Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Fabricio de Almeida Rodrigues Gonçalves

Análise de Implementações de Gerenciamento de Atribuição de Endereços IPv4 Baseado na Monitoração de Mensagens DHCP

São Paulo

2011

Fabricio de Almeida Rodrigues Gonçalves

Análise de Implementações de Gerenciamento de Atribuição de Endereços IPv4 Baseado na Monitoração de Mensagens DHCP

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, como parte dos requisitos para a obtenção do título de Mestre em Engenharia de Computação

Data da Aprovação: ____/_____/_____

Prof. Dr. Volnys Borges Bernal (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Membros da Banca Examinadora:

Prof. Dr. Volnys Borges Bernal (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr. Sergio Takeo Kofuji (Membro)
USP – Universidade São Paulo

Prof. Dr. Alexandre José Barbieri de Sousa (Membro)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Fabricio de Almeida Rodrigues Gonçalves

Análise de Implementações de Gerenciamento de Atribuição de Endereços IPv4 Baseado na Monitoração de Mensagens DHCP

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, como parte dos requisitos para obtenção do Título de Mestre em Engenharia de Computação

Área de Concentração: Redes de Computadores

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo

Abril/2011

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

G635a **Gonçalves, Fabricio de Almeida Rodrigues**
Análise de implementações de gerenciamento de atribuição de endereços IPv4 baseado na monitoração de mensagens DHCP. / Fabricio de Almeida Rodrigues Gonçalves. São Paulo, 2011.
109 p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

1. GAEIP (Gerenciamento de Atribuição de Endereço IP) 2. DHCP (Dynamic Host Configuration Protocol) 3. Endereço IP 4. Controle de acesso 5. Conflito de IP 6. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Coordenadoria de Ensino Tecnológico II.Título

11-63 CDU 004.738.5.057.4(043)

RESUMO

Com o crescimento da importância das redes IP aumenta a preocupação com segurança e controle do acesso ao ambiente de redes locais. Entre os problemas, incluem-se a configuração não autorizada de endereços IP estáticos por parte dos usuários, o que pode causar conflitos de IP, o uso indevido de recursos computacionais e a falta de rastreabilidade em casos de execução ou tentativa de ataques. Para redes IPv4 uma das alternativas é a utilização de alguns métodos de controle de gerenciamento da atribuição de endereços IP (GAEIP) baseado na monitoração de mensagens DHCP em *switches* ethernet. O tráfego de uma estação é autorizado somente se estiver utilizando endereço IP dinâmico atribuído por um servidor DHCP. Este trabalho avaliou três implementações, sendo duas comerciais e uma própria, com procedimentos de teste em quatro diferentes cenários típicos de organização topológica. A avaliação mostrou que a utilização de GAEIP baseado na monitoração de mensagens DHCP é eficaz quando todos os equipamentos da rede possuem a funcionalidade ativa.

Palavras Chave: Conflito de IP, *Switch*, Endereço IP fixo, Controle do acesso, DHCP.

ABSTRACT

Analysis of Implementation Management IPv4 Address Allocation Based Monitoring DHCP Messages

With the growing importance of IP networks is growing concern with security and access control to the environment of local networks. Among the problems include the configuration of unauthorized static IP addresses for users, which can cause IP conflicts, misuse of computer resources and lack of traceability in cases of execution or attempted attacks. For IPv4 networks some control methods of IP address assigned management (GAEIP) based on DHCP messages in Ethernet switches is one alternative. Traffic from a station is authorized only if it is using a dynamic IP address assigned by a DHCP server. This study evaluated three deployments, two commercial and one of its own with testing procedures in four different scenarios of typical topological organization. The results were evaluated and presented advantages and disadvantages of each of the implementations examined. The evaluate showed that GAEIP based on DHCP messages is effective if all network equipaments have this feature active.

Key words IP conflict, Switch, Static IP Address, Access control, DHCP

Lista de Ilustrações

Lista de Abreviaturas e Siglas

ARP	*Address Resolution Protocol*
BPDU	*Bridge Protocol Data Unit*
CRC	*Cyclic Redundancy Checks*
DDOS	*Distributed Deny of Service*
DHCP	*Dynamic Host Configuration Protocol*
DSAP	*Destination Service Access Point*
FCS	*Frame Check Sequence*
GAEIP	Gerenciamento de atribuição de endereços IP
IEEE	*Institute of Electrical and Eletronic Engineers*
IP	*Internet Protocol*
IANA	*Internet Assigned Numbers Authority*
LLC	*Logical Link Control*
MAC	*Medium Access Control*
MANET	*Mobile ad hoc Network*
NAC	*Network Admission Control*
Mbps	*Megabits per second*
PACL	*Port Access List Control*
RFC	*Request for Comments*
SNMP	*Simple Network Management Protocol*
SNAP	*Secure Network Access Protocol*
SSAP	*Source Service Access Point*
TCP	*Transport Control Protocol*
TTL	*Time to Live*
UDLD	*Unidirectional Link Detection*
UDP	*User Datagram Protocol*
WLAN	*Wireless Local Area Network*

Sumário

1 INTRODUÇÃO

Com o aumento da importância das redes TCP/IP, usadas cada vez mais, por aplicações críticas, aumenta também a preocupação com a monitoração e controle destes ambientes para evitar problemas de disponibilidade, rastreabilidade, controle de acesso e desempenho.

Um dos desafios atualmente são as sub-redes corporativas voltadas aos equipamentos dos usuários: *desktops* e *notebooks*.

A administração da configuração do endereçamento de rede é um dos problemas destas redes, principalmente para evitar o conflito de endereços IP e, também, para viabilizar o rastreamento dos acessos.

Existem duas alternativas principais: configuração estática ou configuração dinâmica do endereçamento utilizando o protocolo DHCP (*Dynamic Host Configuration Protocol*). A configuração estática, além de ser mais custosa e complexa operacionalmente, não impede que um usuário com um *notebook* com privilégio de administrador, configure por conta própria o endereçamento do seu equipamento.

A melhor alternativa é a configuração dinâmica utilizando o protocolo DHCP, porém ainda existe a possibilidade de usuários configurarem endereços IP de forma estática, embora exista um servidor DHCP no ambiente de rede. Além disso, um usuário pode também receber um endereço IP de um servidor DHCP e alterar o endereço trazendo o problema citado a qualquer momento. Isso pode levar a alguns problemas como:

- Perda de rastreabilidade em possíveis ataques e fraudes, pois sem a atribuição de endereços pelo servidor DHCP, não existem registros de qual hardware utilizou um endereço IP que pode ter sido envolvido em algum incidente de segurança;

- Aumento nos custos de serviços de suporte, gerados pelos atendimentos desnecessários ocasionados por conflitos de endereço IP;
- Indisponibilidade de sistemas devido a possíveis conflitos de IP;
- Indisponibilidade de segmentos de rede devido a uma configuração errada feita intencionalmente ou não, tendo o usuário digitado como IP da sua estação o mesmo do *default gateway* do segmento de rede;
- Contorno de restrições de controle de acesso por meio do IP, pois ao se alterar o endereço IP um usuário pode ter acesso não autorizado a sistemas, que tem como controle de acesso o endereço IP de origem.

Dai e Chiang (2007) citam o problema causado pela falta de controle, onde usuários chamados de ilegais alteram seus endereços IP para fixos, e causam interferências na rede, que dependendo do tamanho da rede, a correção pode ser muito difícil.

Conforme Li et al (2008) a falta de controle dos endereços IP de origem, causa perda de desempenho, porque recursos são alocados para pacotes que não são válidos, deixando os válidos na fila para serem encaminhados. Esta invalidade de pacotes pode ser causada por um usuário, que alterando o seu endereço IP, tem acesso a recursos que normalmente não estariam disponíveis para o seu perfil.

1.1 Motivação

As alternativas para controle do problema de gerenciamento da atribuição de endereços IP em redes de usuários são baseadas em funcionalidades existentes nos *switches* (equipamentos tipo *bridge*).

Com a descentralização da responsabilidade pela segurança e pelo controle de acesso, os *switches* nos quais as estações clientes são conectadas, são também exigidos cada vez mais para realizar funções que antes não eram de sua responsabilidade.

Uma maneira para se controlar o endereço IP da estação cliente, é a proibição desta alteração no sistema operacional. Esta ação não pode ser realizada em todos os casos, devido à diversidade dos ambientes e também dos respectivos clientes, tendo como exemplo uma grande corporação que possui, entre seus colaboradores, consultores de diversas empresas. Estes podem ter esta restrição inviabilizada pela política de segurança dos respectivos ambientes de rede. Outra razão para a impossibilidade de se bloquear a permissão de alteração do IP é a necessidade deste recurso para diversos técnicos que tem seus computadores portáteis conectados em diversas redes locais, e algumas sem um servidor DHCP para fornecer o endereço IP.

Controles, como o NAC (*Network Admission Control*) (2009), são implantados no nível de acesso dos ambientes, com a finalidade de aumentar o nível de segurança e de controle. Um destes mecanismos é protocolo IEEE 802.1x, que consiste na autenticação do usuário para permitir o seu acesso à rede, usando a mesma conta e senha para acesso aos recursos computacionais da corporação. Outra funcionalidade usada pelo NAC é a verificação das atualizações de antivírus. Estes controles podem ser também instalados separadamente, dependendo da necessidade do ambiente e da infraestrutura disponível. Para se implementar o NAC, devem ser atendidos vários pré-requisitos, como servidores de antivírus, servidores de autenticação e *switches* de rede com as funcionalidades requeridas para a aplicação do controle, entre outros.

Existem algumas implementações para controle de configuração de endereçamento IP para terminais (desktop, PDA, telefone celular, telefone IP) de usuários, baseadas no protocolo DHCP.

Quando esta funcionalidade de controle de acesso DHCP é aplicada a uma determinada porta de um *switch*, o uso desta é permitido somente após a finalização do processo de obtenção ou renovação de um endereço IP dinâmico, via o protocolo DHCP, por parte do equipamento conectado à respectiva interface.

1.2 Objetivo

O objetivo deste trabalho é avaliar as diferentes implementações de GAEIP (gerenciamento de atribuição de endereço IP) baseado na monitoração de mensagens DHCP e filtragem de pacotes pelo *switch* de acesso, com a finalidade de propiciar um controle maior do uso de endereços IP pelas estações de usuários. Esta funcionalidade de controle de acesso usando o protocolo DHCP pode estar presente nos *switches* ethernet, em *Access Points*, equipamentos tipo *Node B* (Equipamentos de agregação nas redes móveis 3G) e ainda para outras tecnologias como *Wi Max* e 4G (LTE).

Para avaliação da funcionalidade GAEIP foram escolhidas três implementações, são duas implementações de mercado, aqui relacionadas como implementação M1 e M2, e uma implementação tipo prova de conceito.

Como parte do trabalho foi realizada uma implementação de GAEIP com monitoração de mensagens DHCP, tipo prova de conceito, para permitir explorar possíveis problemas nas implementações de mercado, levando em consideração a segurança, desempenho, impacto na disponibilidade e em outras funcionalidades ou protocolos.

Para realização da avaliação foram definidos quatro cenários típicos de uso.

1.3 Escopo

O escopo do trabalho limita-se a redes locais TCP/IP, baseadas nos protocolos Ethernet (IETF, 1984), e IP versão 4 (IETF, 1981). As implementações de mercado avaliadas foram identificadas como M1 e M2 para referência. Uma implementação de teste foi implantada baseada no sistema aberto Linux.

1.4 Organização do trabalho

Os próximos capítulos estão organizados da seguinte forma:

O capítulo 2, Revisão Bibliográfica, apresenta o protocolo DHCPv4 utilizado nos métodos de controle de atribuição de endereços IP avaliados. Além disso, são apresentados outros controles implementados pelos *switches* relevantes ao trabalho. A seção funcionamento de um cliente DHCP analisa o comportamento do cliente DHCP em diversas situações ocorridas no ambiente de rede local, solicitando um novo endereço IP, renovando o mesmo endereço, alterando a configuração do IP para estática, e as alterações realizadas na porta, como a conexão e desconexão de uma estação em uma porta do *switch*.

No capítulo 3, Trabalhos Relacionados, são citados trabalhos relacionados ao controle de endereçamento de atribuição de endereços IP, aumentar o controle do acesso e a segurança das redes locais.

No capítulo 4, Implementações Relacionadas, são analisadas as funcionalidades aplicadas pelos fornecedores de *switches* no mercado. Nesta análise são descritas as implementações, os métodos e as respectivas restrições para o GAEIP. A proposta do Address Guard é apresentada, incluindo a diferença para as implementações de mercado e também suas restrições.

No capítulo 5, Implementação do Address Guard, uma alternativa de implementação é desenvolvida e aplicada para que se possa estudar o comportamento da funcionalidade e possibilitar a aplicação deste controle de acesso em equipamentos de rede como, por exemplo, agregadores de redes móveis 3G, 4G e agregadores de redes sem fio.

No capítulo 6, Metodologia e Cenários de Teste, é apresentada toda metodologia para teste das implementações, incluindo o caderno de testes detalhado com as instruções e procedimentos para realização de cada teste.

O capítulo 7 apresenta os resultados de todos os testes realizados conforme metodologia apresentada no capítulo 6.

No capítulo 8, Avaliação e Comparação dos Resultados, são comparados todos os resultados coletados a partir dos capítulos 5, com as análises realizadas no capítulo 6.

O capítulo 9, Conclusão, apresenta os resultados do trabalho, contribuições e sugestões para pesquisas futuras.

2 CONCEITOS

Neste capítulo são abordados os conceitos sobre redes locais, tendo foco os protocolos de alocação dinâmica de endereços IP (ITEF, 1981), com a finalidade de prover os fundamentos necessários para o desenvolvimento de uma prova de conceito e, também a análise de alternativas de GAEIP (gerenciamento de atribuição de endereço IP) baseado na monitoração das mensagens DHCP.

2.1 Protocolo DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*) (IETF, 1997) foi desenvolvido para possibilitar a atribuição automática de endereços IP. Este tem melhorias em relação ao seu antecessor o BOOTP (IETF, 1997). Uma melhoria é a possibilidade de o nó receber todas as configurações necessárias, como por exemplo endereço IP, máscara e *gateway*, para a sua interoperabilidade com a rede na qual está conectado.

O serviço DHCP permite que sejam utilizadas três tipos de atribuição: manual, automática permanente e automática. Na configuração manual é permitido ao administrador a configuração de um endereço específico para um nó. O DHCP também permite configuração automática, atribuindo um endereço IP permanente para um nó. A terceira maneira seria atribuindo de forma automática, endereços IP temporários. Para a atribuição dinâmica, o DHCP utiliza como identificador da atribuição o endereço MAC do nó solicitante. O modo mais aplicado é aquele que a atribuição é dinâmica e o endereço IP é emprestado para o nó solicitante, por um tempo finito.

Mensagens DHCP são usadas para transportar todas as informações necessárias para o funcionamento do protocolo. No quadro 2.1 são explicadas a função de cada campo da mensagem DHCP, que é ilustrada na figura 2.2.

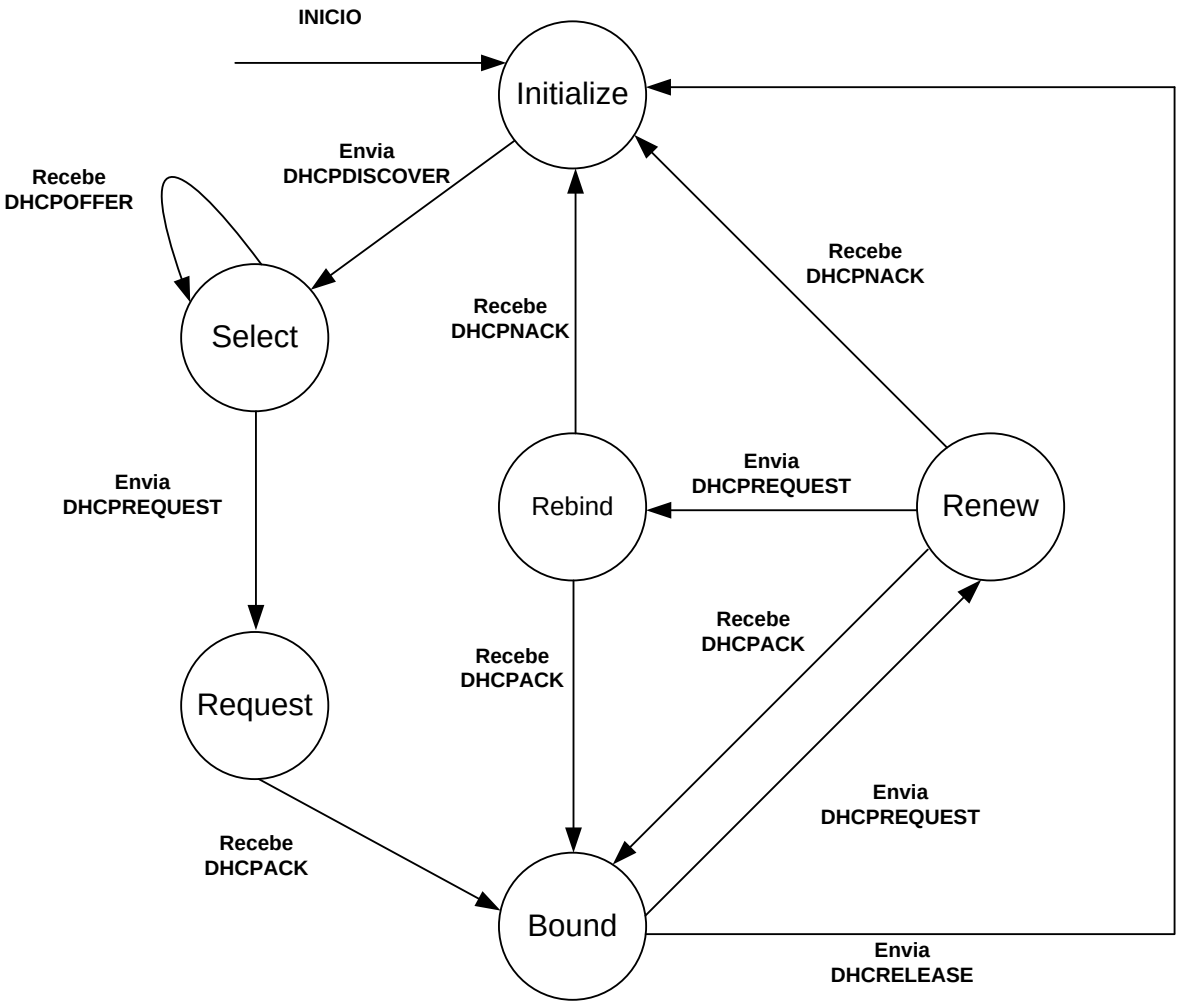


Figura 2.1: Diagrama de estado do cliente DHCP

Fonte: Soares, Lemos e Colcher (2000)

OP	HTYPE	HLEN	HOPS
ID de Transações			
Segundos		Flags	
Endereço IP do Cliente			
Seu Endereço IP			
Endereço IP do Servidor			
Endereço IP do Roteador			
Endereço de Hardware do Cliente (16 octetos)			
Nome do Host do Servidor (64octetos)			
Nome do Arquivo de Partida (128 octetos)			
Opções (varíavel)			

Figura 2.2: Formato da mensagem DHCP

Fonte: Soares, Lemos e Colcher (2000)

A atribuição de um endereço IP segue seis etapas que são observadas no diagrama de estado do protocolo, apresentada na figura 2.1. No estado de INITIALIZE, o cliente envia uma requisição de solicitação de endereço IP, usando a mensagem DHCPDISCOVER que é encapsulada em um datagrama UDP na porta 67 com destino um endereço de *broadcast* (IETF, 1984), conforme figura 2.3. Depois deste envio, a estação passa para o estado SELECT. Todos os elementos do segmento de rede recebem esta mensagem, que é enviada usando o endereço de origem da própria estação e endereço de destino o de *broadcast*. Somente o servidor DHCP responderá a esta solicitação usando a mensagem de DHCPOFFER. A figura 2.4 apresenta os campos de uma mensagem DHCPOFFER capturada.

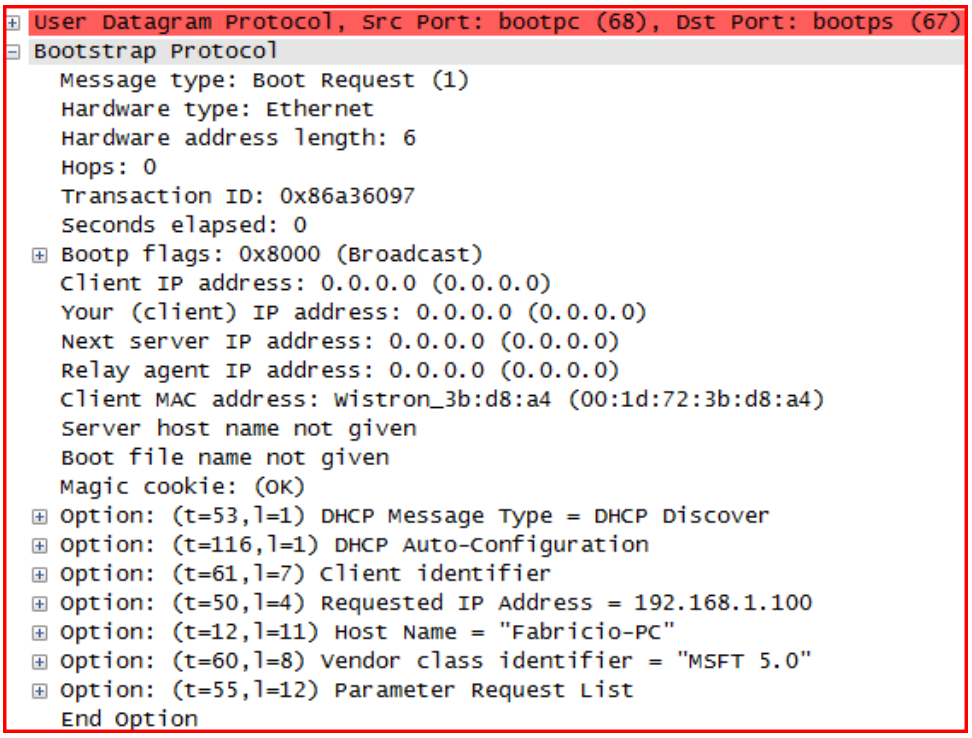


Figura 2.3: Detalhe DHCP DISCOVER

Fonte: Elaborado pelo autor (2010)

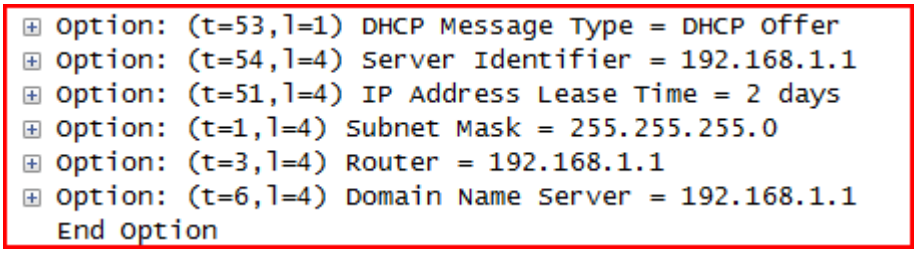


Figura 2.4: Detalhe DHCP OFFER

Fonte: Elaborado pelo autor (2010)

O cliente receberá uma ou mais mensagens de DHCPOFFER, que tem a oferta do endereço IP do servidor DHCP para o cliente, dependendo da quantidade de servidores DHCP na rede. Ao selecionar a primeira mensagem recebida, o cliente responde ao servidor DHCP usando a mensagem de DHCPREQUEST, figura 2.5, e entra no estado de REQUEST. O cliente só poderá usar o endereço IP oferecido pelo servidor DHCP após receber a mensagem DHCPACK, na figura 2.6, que assim entrará no estado de BOUND.

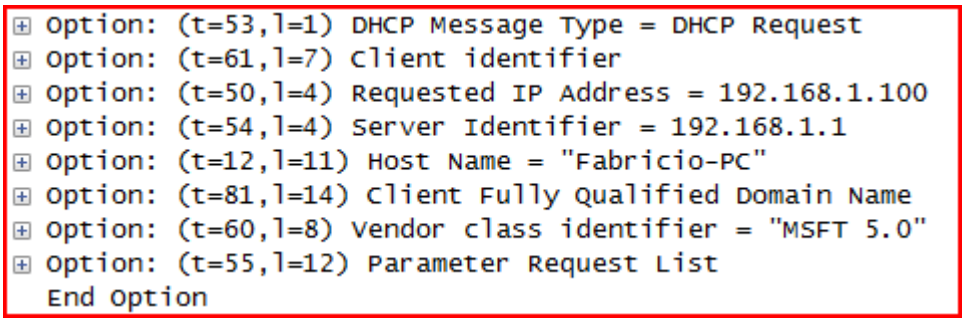


Figura 2.5: Detalhe DHCP REQUEST

Fonte: Elaborado pelo autor (2010)

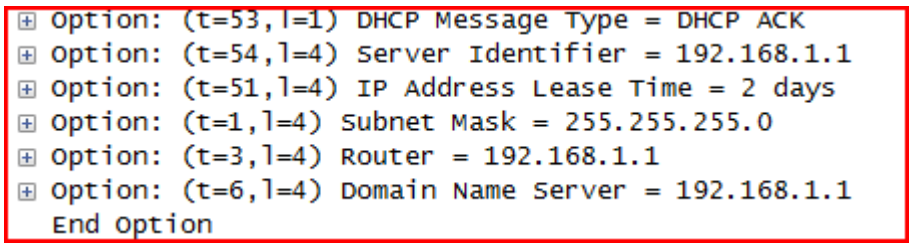


Figura 2.6: Detalhe DHCP ACK

Fonte: Elaborado pelo autor (2010)

O cliente permanece neste estado enquanto estiver usando o endereço IP. Caso não haja mais interesse em usar este endereço, o cliente pode cancelar o uso deste usando a mensagem DHCPRELEASE, apresentada na figura 2.7. Quando esta mensagem é encaminhada o cliente sai do estado de BOUND e volta para o INITIALIZE.

Para a renovação do endereço IP, o cliente ao receber a atribuição, configura três temporizadores que controlarão a primeira tentativa de renovação, uma segunda tentativa e o fim da alocação. Os valores padrões são a metade do tempo do aluguel, um quarto da outra metade do tempo e no final do aluguel. Para tentar renovar o endereço, o cliente envia uma mensagem de DHCPREQUEST, e em seguida entra para o estado de RENEW. Se autorizada a renovação, o servidor enviará um DHCPACK e o cliente voltará para o estado de BOUND. Caso contrário o cliente receberá um DHCPNACK e não utilizará mais o endereço IP. Se o cliente não conseguir renovar no primeiro temporizador, tentará novamente no segundo. Este expirando, o cliente entrará no estado de REBIND, que indica a falha de conectividade

com o servidor DHCP atual. Com isso o cliente voltará a enviar um DHCPREQUEST para toda a rede, procurando qualquer servidor DHCP que possa renovar o endereço IP já em uso. Recebendo uma mensagem DHCPACK volta para o estado de BOUND. O último temporizador atua no estado de vincula novamente REBIND e fará com que o cliente não use mais o endereço IP caso não receba nenhuma resposta, levando para o estado de INITIALIZE forçando o cliente a reiniciar todo o processo.

O quadro 2.1 apresenta os campos de uma mensagem DHCP.

Quadro 2.1: Campos mensagem DHCP.

Campo	Descrição
OP	Indica se a mensagem é uma solicitação ou resposta
HTYPE	Tipo de endereço da camada de enlace
HLEN	Tamanho do endereço do hardware
HOPS	Contagem de passos da rota
ID de Transações	Usado para máquinas sem disco para solicitações e respostas
Segundos	Tempo desde que o cliente fez a solicitação
Flags	Usado para solicitações broadcast
Endereço IP do Cliente	Endereço do cliente em caso de renovação
Seu Endereço IP	Resposta do endereço IP ao cliente em novas alocações
Endereço IP do Servidor	Endereço IP do servidor
Endereço IP do Roteador	Usado para servidores que estão em redes diferentes dos clientes
Endereço de Hardware do Cliente	Endereço físico da interface de rede do cliente
Nome do Host do Servidor	Nome do Servidor usado pelo BOOTP
Nome do Arquivo de Partida	Usado pelo BOOTP para indicar o arquivo inicial das configurações de uma máquina sem disco
Opções	Diversos parâmetros são configurados neste campo, que por exemplo indica o tipo de mensagem DHCP, que com o código 53 e tipos de 1 a 7, indica se é um DHCPREQUEST, OFFER e todas as outras mensagens DHCP.

Todas as mensagens DHCP são diferenciadas no campo de opções, conforme a RFC 2132. A diferenciação entre elas está no campo tipo, todas sob o código 53. Em uma

mesma mensagem DHCP, pode conter mais de uma opção de códigos diferentes. Os tipos de mensagem são mostrados no quadro 2.2.

Quadro 2.2: Campo tipo das mensagens DHCP.

Tipo	Mensagem
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

2.2 Cliente DHCP em algumas situações típicas

O funcionamento do cliente DHCP varia de acordo com a situação na qual se encontra. São descritas algumas situações que podem acontecer em uma operação normal de um ambiente de rede local.

- Nova atribuição de endereço IP dinâmico;
- Alteração de endereço dinâmico para fixo;
- Reinicialização da conexão entre o *switch* e o cliente;
- Renovação do endereço IP.

2.2.1 Atribuição de endereço IP dinâmico

O cliente, quando não possui nenhum endereço IP atribuído anteriormente, envia a mensagem DHCP DISCOVER. Após isto recebe o DHCPOFFER, enviando em seguida o DHCPREQUEST e aguarda a resposta do servidor.

Assim a troca de mensagens DHCP nesta situação segue a ordem: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.

2.2.2 Alteração de endereço dinâmico para fixo

Nos sistemas operacionais, na alteração do endereço IP de dinâmico para fixo, é envia da a mensagem DHCP RELEASE, conforme figura 2.7. De acordo com a RFC 2131, o cliente DHCP quando não necessita mais do endereço IP atribuído pelo servidor DHCP, envia a mensagem de DHCPRELEASE para o servidor DHCP liberando o endereço IP.

Este comportamento pôde ser confirmado pela observação das mensagens DHCP trocadas pelo sistema operacional Windows Vista, que quando o endereço IP foi alterado, a estação envia para o servidor DHCP uma mensagem de DHCPRELEASE.

No DHCP RELEASE, o cliente envia ao servidor DHCP a solicitação para a liberação do endereço IP, identificando qual endereço IP deve ser liberado, pelo endereço físico da respectiva interface.

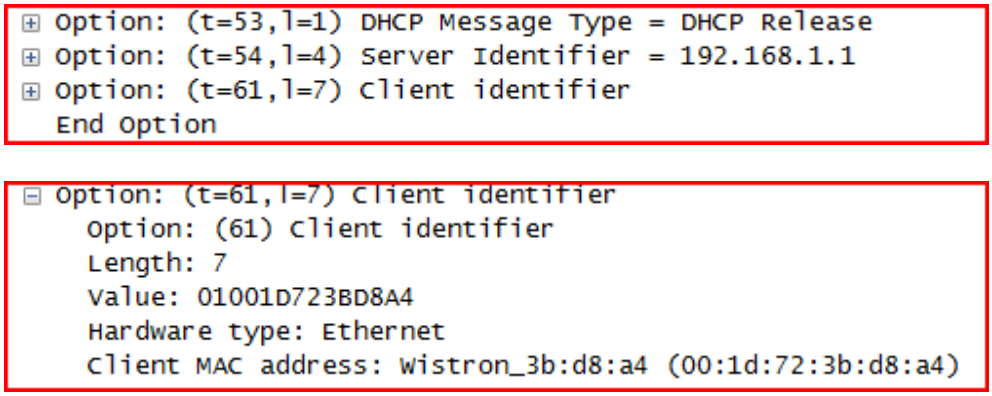


Figura 2.7: Detalhe DHCP RELEASE

Fonte: Elaborado pelo autor (2010)

2.2.3 Reinicialização da conexão entre *switch* e o cliente

Ao desconectar e reconectar o cabo de rede, o cliente DHCP envia uma mensagem DHCP REQUEST, contendo no campo de opções o endereço IP atribuído pelo servidor anteriormente, na tentativa de reutilizá-lo. O servidor responde ainda tendo como

destino o endereço de broadcast, pois o cliente ainda não tem autorização para usar qualquer endereço IP. Esta resposta é um DHCP ACK liberando o endereço para o cliente, que a partir deste momento já pode enviar e receber datagramas IP usando o endereço IP em questão.

A mesma desconexão e reconexão pode acontecer caso o *switch* seja reiniciado.

Em ambas as situações descritas, se o servidor negar o uso do endereço IP com a mensagem DHCPNACK, obriga o cliente a reiniciar todo o processo de obtenção de endereço IP.

Assim, a ordem de mensagens é: DHCPREQUEST e DHCPACK caso o servidor autorize a utilização do endereço IP. Do contrário as seguintes mensagens serão trocadas entre cliente e servidor: DHCPRQUEST, DHCPNACK, DHCPDISCOVER, DHCPOFFER, DHCPREQUEST e DHCPACK.

2.2.4 Renovação do endereço IP

A renovação do endereço IP é solicitada do cliente para o servidor, quando o aluguel do endereço IP alcançar a metade do tempo estabelecido pelo servidor. Caso esta renovação não tenha sucesso por qualquer motivo, o cliente tenta novamente em 75 % do tempo e ainda quando o tempo de aluguel expirar.

O cliente envia a mensagem DHCPREQUEST e aguarda a mensagem DHCPACK. Caso não receba o DHCPACK na última tentativa, toda obtenção do endereço IP inicia como se o cliente não tivesse nenhum endereço IP, já descrito no item 2.2.1.

O tempo de *lease* é enviado na mensagem DHCP ACK. A unidade de tempo usada, seguindo a RFC, é em segundos e tem tamanho de 32 bits.

Na figura 2.8, uma mensagem DHCP ACK, que tem código 53 e tipo 5, tem atrás desta opção diversas outras como a opção 54, que identifica o servidor DHCP, e após esta o tempo de *lease*.

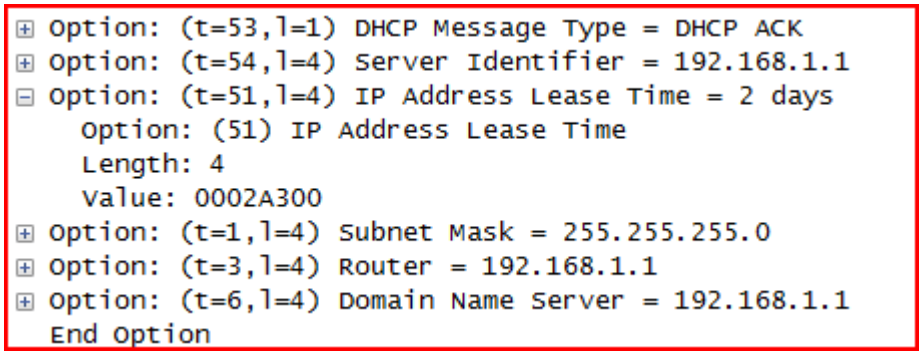


Figura 2.8: Detalhe DHCP *lease time*

Fonte: Elaborado pelo autor (2010)

2.3 Funcionalidades relacionadas ao controle de atribuição de endereço pelo DHCP

2.3.1 IP *Source Guard*

Esta funcionalidade implementada em alguns *switches* como os *switches* das implementações de mercado, é usada para impedir que uma estação envie datagramas IP com um endereço IP de origem diferente do que ela começou a usar, ao se conectar ao *switch*. Isto impede que um usuário mal intencionado realize qualquer tentativa de ataque ou negação de serviço, sem que seja identificado. Isto é, somente o endereço IP atribuído à estação conectada a respectiva interface do *switch*, poderá ser origem dos pacotes encaminhados por esta mesma porta.

2.3.2 Trusted DHCP Server

Com este recurso o *switch* pode, quando habilitada esta funcionalidade, identificar quais as portas podem ser usadas por servidores DHCP, classificando-as como confiáveis. Já

nas portas que não são confiáveis, os *switches* bloqueiam as mensagem de DHCPOFFER, usada pelo servidor DHCP para oferecer um endereço IP à um cliente. Isto garante que ao se instalar um servidor DHCP em um segmento, e este não seja válido, não conseguirá fornecer endereços IP e causar indisponibilidade no ambiente, que é a finalidade desta funcionalidade, também chamada de DHCP *snooping*.

Apesar de também usar mensagens DHCP para manter em uma tabela de estado o IP atribuído para uma estação, a porta e o endereço MAC, não consegue impedir que um cliente tenha acesso a rede sem usar endereços dinâmicos. Além disto, ainda tem pré-requisitos como só funcionar com um hardware específico, com determinadas versões de sistema operacional, sem usar esquemas para alta disponibilidade do *switch*.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta alguns trabalhos relacionados ao tema de gerenciamento da atribuição de endereços IPv4.

O gerenciamento da atribuição de endereços IP representa a monitoração e controle dos endereços IP atribuídos aos equipamentos de uma rede TCP/IP e tem como objetivo evitar que um mesmo endereço IP seja utilizado por mais de um cliente de uma rede TCP/IP, e também garantir que somente clientes tenham acesso ao ambiente de rede caso usem endereço IP dinâmico.

3.1 Shahri et al

O trabalho de Shahri et al (2003) cita que o rápido crescimento das redes de dados e a necessidade por estas interconexões são os dois principais fatores do aumento da preocupação com a segurança destas redes. Os autores defendem o uso de autenticação de usuário para controlar o acesso às redes locais. A mudança de uma arquitetura centralizada para uma descentralizada seria uma alternativa. Para isto é proposto um novo protocolo para autenticação no acesso as redes locais. A mudança para uma arquitetura distribuída seria para aumentar a segurança, confiabilidade e disponibilidade na autenticação dos usuários.

O SNAP (*Secure Network Access Protocol*) é o protocolo sugerido para que a autenticação de usuários na rede local seja feita de forma distribuída. Faz parte deste mecanismo de autenticação um número de servidores que dividem a responsabilidade pela autenticação do usuário, tendo para cada um dos servidores uma parte do código de acesso. Este código de acesso é o que permite ou não o usuário de ter acesso aos recursos de rede. Os servidores de autenticação denominados no SNAP podem ser servidores, roteadores, *gateways* ou qualquer outro componente da rede local.

O usuário solicita autenticação para um servidor de autenticação, que neste caso é denominado nó local. Este nó local, caso o usuário ainda não seja um usuário válido, envia para o usuário a quantidade de partes da chave de autenticação que devem ser obtidas e os respectivos servidores de autenticação. Após isto o usuário inicia comunicação com todos os servidores de autenticação para buscar as partes do código de acesso. Em cada servidor, a autorização do usuário é verificada em sua base local. Ao conseguir todas as partes do código de acesso, o cliente apresenta ao nó local. Com isto o nó local valida o código, concedendo ou não acesso aos recursos de rede.

A análise do trabalho de Shahri et al (2003) demonstra a preocupação com os acessos dos usuários nas redes locais, e com isto a disponibilidade é fundamental para o bom funcionamento das redes locais. Mas um usuário mesmo autenticado pode causar indisponibilidade de alguma comunicação com uma simples mudança de endereço IP.

3.2 Grochla et al

Conforme Grocha et al (2009), um rápido crescimento do interesse de tráfego entre redes sem fio vem sendo observado. Estas redes podem ser de interfaces físicas diferentes como por exemplo 802.11b e 802.11a. Para simplificar o acesso a estas redes, um procedimento de autoconfiguração que provê as configurações mínimas para acesso dos usuários é muito importante.

Uma grande preocupação com esta interoperabilidade entre os ambientes é o uso de um único endereço IP por clientes diferentes, causando um conflito de endereço IP.

Os autores propõem a autoconfiguração dos terminais das redes sem fio, com o uso do protocolo DHCP. Para isto são sugeridas algumas alterações no protocolo, como o uso de algumas opções nas mensagens DHCP para informar o SSID por exemplo. Outra alteração é a na possibilidade de uso de mais de um servidor DHCP para atender a mesma rede. Neste caso os servidores DHCP devem enviar periodicamente mensagens DHCP DISCOVER com a informação de servidor DHCP dentro das opções

da mensagem DHCP. Ao receber esta mensagem o servidor DHCP responde com um DHCP OFFER mantendo a informação de servidor. O método para a eleição do servidor ativo é o maior endereço MAC. Assim quando o servidor DHCP recebe uma mensagem DHCP OFFER com um endereço MAC menor que o seu próprio endereço MAC, este servidor deve enviar uma mensagem de DHCP REQUEST. Ao detectar outro servidor DHCP, o atual, caso perca a eleição, deverá enviar a mensagem de DHCP NACK para todos os clientes com endereços IP em uso para que os mesmos possam solicitar novos endereços IP do servidor vencedor da eleição. A finalidade deste mecanismo é evitar que mais de um servidor DHCP atribua endereço IP para clientes de uma mesma rede, garantindo assim que não ocorra conflito de endereço IP.

A análise do trabalho de Grochla et al (2009) mostra a importância do correto funcionamento do protocolo DHCP, sendo muito crítico para o correto funcionamento das redes TCP/IP. Um conflito de endereço IP pode inviabilizar o correto funcionamento da proposta. Este conflito pode acontecer com uma simples alteração de configuração de um cliente. Nesta proposta, mesmo com as alterações no protocolo DHCP, o problema não consegue ser evitado. O controle para evitar o conflito é feito somente na atribuição do endereço IP.

3.3 Joshi et al

O trabalho de Joshi et al (2009) ressalta a importância da mitigação de problemas com o IP *spoofing* o mais próximo da origem, no caso de redes de banda larga nos concentradores de acesso.

O IP *spoofing* é usado nos ataques mais comuns chamados DoS (*deny of service*), dificultando a identificação da origem, porque a fonte do ataque altera o seu endereço IP.

Como proposta, os autores sugerem algumas melhorias no protocolo DHCP, para que sejam usados nos equipamentos concentradores de acesso de redes de banda larga.

Estas melhorias são algumas mensagens novas no protocolo. Assim o concentrador faria a interceptação da mensagem do cliente, que por sua vez faria a solicitação ao servidor DHCP. O concentrador intercepta as mensagens DHCP ACK, que contém as informações necessárias para um controle mínimo como endereço IP, endereço MAC e o tempo de aluguel do endereço IP. A nova mensagem sugerida é a DHCP LEASEQUERY, que permite ao concentrador consultar os tempos de *lease* em uso por identificador, caso ocorra alguma perda de informações no próprio concentrador. E como resposta da mensagem de DHCP LEASEQUERY, são sugeridas novas mensagens como DHCP LEASEQUERYACTIVE, DHCP LEASEQUERYUNASSIGNED e DHCP LEASEQUERYUNKNOWN. A mensagem DHCP LEASEQUERYACTIVE é uma resposta ao DHCP LEASEQUERY que é enviada pelo servidor DHCP informando que um endereço IP é considerado ativo e válido. O DHCP LEASEQUERYUNASSIGNED para responder se um identificador não é mais válido. Já o DHCP LEASEQUERYUNKNOWN informa que o identificador não existe.

A análise do trabalho de Joshi et al (2008), mostra que estas novas mensagens DHCP permitem uma maior eficiência do controle do uso de endereços IP válidos de uma rede TCP/IP.

3.4 Li et al

Li et al (2008) tratam sobre a verificação do endereço IP de origem com a finalidade de rotear apenas IPs válidos na rede usando um protocolo de autenticação do endereço IP para ser aplicado nos roteadores.

O protocolo SAVE (*Source Address Valid Enforcement*) é proposto para ser usado em roteadores permitindo que aprendam os endereços válidos de cada direção do fluxo de dados, construindo tabelas de entrada de tráfego que são constituídas pelos endereços IP de origem de cada interface do roteador. Com estas tabelas são aplicados filtros nas interfaces encaminhando apenas pacotes que tenham seus endereços citados nas

tabelas. O protocolo SAVE é independente podendo operar com qualquer protocolo de roteamento dinâmico.

Na análise do trabalho de Li et al (2008), o uso de um protocolo que permita verificar e filtrar os pacotes válidos, tendo como base para decisão o endereço IP de origem é subsídio para um bom nível de controle, mas alguns aspectos devem ser observados, como a sua utilização em redes grandes ou AS (*Autonomous Systems*) de trânsito[1], que exigiria uma alta utilização de recursos dos elementos de rede para verificar os novos fluxos que passariam a trafegar pelos elementos de cada AS, como também em caso de convergências de rede. Na internet, além da preocupação com divulgações de redes erradas, que geram a necessidade de filtros e listas de acesso, os administradores deverão se preocupar também com a convergência do protocolo sugerido pelos autores. Assim a aplicabilidade seria para pequenas redes, nunca para redes grandes e *backbones* com uma grande quantidade de elementos de rede.

Esta verificação, para se ter um melhor ganho, deve ser feita no ponto mais próximo da extremidade da rede, visando menor sobrecarga na utilização da infraestrutura, como também uma divisão de carga nos controles de segurança. Ao aplicar controle no *switch* que os clientes são conectados, o tráfego desnecessário é ignorado logo no acesso, não necessitando chegar até o roteador para a decisão de roteá-lo ou não.

3.5 Sue et al

Os autores Shue et al (2009) descrevem a necessidade de proteção das informações nas redes IPv4. Para isto sugerem uma melhoria no protocolo DHCP, através da utilização de certificados para clientes e servidores DHCP. Com isto evitam-se problemas causados por servidores DHCP não oficiais, porque o certificado possibilita realizar a autenticação dos parceiros de comunicação. Assim os clientes sempre

[1] AS de transito é a conexão entre um outro AS e os demais da internet. Geralmente esta função de transito é feita por grandes operadores nacionais e internacionais.

enviam a mensagem DHCPDISCOVER com algumas informações a mais, como por exemplo a chave do domínio que todas as estações tem pré-configuradas.

A análise do trabalho de Sue et al (2009) mostra a criticidade do protocolo DHCP e a preocupação com o correto funcionamento, que garante o bom funcionamento das redes locais TCP/IP. Alguns pontos a serem observados são a necessidade de alterações nos protocolos atuais, uma carga maior nas estações de trabalho na obtenção de endereços IP e, ainda, a dificuldade na utilização de novos clientes de rede, pois precisariam da instalação do certificado. Mas para o correto funcionamento, o cliente deve estar usando o protocolo DHCP. Esta proposta não elimina o problema de conflito de IP causado por uma configuração errada.

3.6 Dai et Chiang

Dai e Chiang (2007) cita que uma das funções do servidor DHCP é evitar a utilização de endereços IP duplicados. Porém, o usuário pode não utilizar o servidor DHCP e configurar o endereço IP de forma manual. Para garantir um controle maior do ambiente de rede, todos os pacotes destes usuários, chamados pelos autores de ilegais, deveriam ser bloqueados garantindo o desempenho do ambiente e também seu controle.

O método sugerido pelos autores usa a tabela ARP do *gateway* da sub-rede[2] e o banco de dados do servidor DHCP. O servidor DHCP deve comparar ambas informações e assim gerar as inconsistências que são notificadas aos elementos de rede, roteador ou *switch*, pelo próprio servidor DHCP. O bloqueio de tráfego dos usuários ilegais é realizado pelo roteador ou *switch* usando regras de filtragem.

A análise do trabalho de Daí e Chiang mostra a preocupação com o uso de endereços IP fixos. Alguns pontos devem ser observados como a comunicação entre o servidor

[2] Neste trabalho o termo sub-rede refere-se à unidade de rede, que é aplicada a uma única rede local virtual, possibilitando a separação dos domínios de broadcast.

DHCP e os roteadores que são *gateways* de cada sub-rede, sendo necessário um protocolo para esta comunicação. Outro item importante é o bloqueio poder ser feito no roteador, permitindo o uso de um endereço IP fixo podendo causar indisponibilidade com algum cliente se acontecer um conflito de endereço IP. Sendo o servidor DHCP o responsável por atualizar todas as listas de acesso, dependendo do tamanho da rede, o servidor poderá ficar sobrecarregado ao fazer tantas verificações entre tabelas ARP e a sua própria tabela, além de ter a responsabilidade de notificar os *switches* e roteadores para realizar os devidos filtros. Desta maneira o tempo entre a detecção de uma alteração e o efetivo bloqueio pode permitir que aconteça um conflito de endereço IP no ambiente de rede.

3.7 Wang et Lee

Wang e Lee (2002) citam que a segurança continua é um dos maiores problemas das redes. Diversos problemas externos, como ataques DDOS (*Distributed Deny of Service)* e problemas internos como conflitos de endereço IP podem trazer indisponibilidade para o ambiente de rede. Quando o protocolo DHCP é usado por estas redes para configuração automática do endereçamento das estações, traz como fragilidade a falta de exigência de que os clientes da rede devam utilizar o protocolo DHCP para ter acesso a rede. Assim um cliente pode acidentalmente ou propositalmente configurar um endereço IP que já esteja em uso por outro cliente DHCP.

A sugestão dos autores é o uso da base de dados do servidor DHCP, que contém todos os *leases* de endereços IP atribuídos, para a geração de regras de filtragem a serem aplicadas nos *switches* de rede local. Somente endereços MAC e IP que constem na tabela de *lease* do servidor DHCP, terão o tráfego liberado nos *switches*. Esta tradução é feita com um programa que é executado junto ao servidor DHCP.

A análise do trabalho de Wang e Lee (2002) evidencia um ponto central de processamento. Em ambientes de rede com uma grande quantidade de *switches*, pode trazer problemas ao servidor DHCP, pois dependendo da quantidade de *leases* gerados

em um determinado período de tempo, este servidor poderá sofrer problemas de disponibilidade ou ainda atrasando as atualizações nos *switches*, permitindo assim indisponibilidades para outros clientes.

3.8 Boudjit et al

Nas redes sem fio, chamadas MANET (Mobile ad hoc network), os autores Boudjit et al (2007) citam as dificuldades de atribuição automática de IPs nestas redes, se comparadas às redes locais cabeadas. São indicados como problema a dificuldade de se usar mecanismos que atribuam automaticamente endereços IP neste tipo de rede, e a inviabilidade de se ter um único servidor DHCP para atendimento de todo o ambiente de rede. Todas estas dificuldades estão relacionadas ao tamanho das redes e a instabilidade dos enlaces, instabilidade das conexões e mobilidade. Para resolver as dificuldades apontadas é descrita uma solução para se detectar conflitos de endereços IP, usando um algoritmo de detecção de endereços duplicados. Mas esta detecção ocorre somente no momento da atribuição de qualquer endereço IP por qualquer servidor DHCP.

A análise do trabalho de Boudjit et al (2007) aponta como maior problema o conflito de endereço IP, trazendo indisponibilidade de acesso do cliente à rede. Caso clientes alterem seus endereços IP após estes serem atribuídos por um servidor DHCP, o problema persistirá e não será detectado pelo mecanismo proposto, porque a verificação de duplicidade de endereço IP ocorre somente na atribuição do endereço IP.

3.9 Yang et Mi

Segundo Yang et Mi (2010), o uso do protocolo DHCP traz benefícios para o administrador de rede, mas também problemas de segurança.

São relatadas falhas do protocolo DHCP como a permissão de qualquer servidor poder prover endereços IP. O ponto importante do trabalho é a indicação de que a maior causa dos ataques ao protocolo DHCP é a falta de autenticação dos clientes e servidores. Os autores propõe a utilização de autenticação dos usuários através de uma senha com o endereço de hardware.

Na análise do trabalho de Yang et Mi (2010), em nenhum momento é exigido o uso do protocolo DHCP para se ter acesso a rede, garantindo que o acesso a rede esteja seguro. Toda preocupação com a autenticação dos usuários é feita, mas após esta autenticação um usuário pode de forma proposital ou acidental mudar o endereço IP e causar uma indisponibilidade no ambiente de rede.

3.10 Zuquete

Zuquete (2009) apresenta a necessidade de segurança nas redes locais e comunicações ponto a ponto. Mas de nada adianta isto, se um conflito de endereço IP não permitir que esta conectividade ou transferência seja estabelecida.

A proposta do autor é uma arquitetura de segurança para redes locais, usando o protocolo 802.1x e chaves criando uma política de identificação de novos usuários e um servidor DHCP modificado, forçando assim autenticação das mensagens DHCP. Esta autenticação acontece quando o cliente usa o servidor DHCP, recebe uma chave que é trocada com o ambiente de rede e é usada para autenticar a troca das mensagens do protocolo ARP.

Na análise do trabalho de Zuqete (2009), o esquema garante o momento inicial da conexão de usuários na rede, mas após este instante, um cliente poderá alterar seu endereço IP e ocasionar assim indisponibilidade na conectividade deste e outros clientes da rede IP.

3.11 Brik et al

Brik et al (2004) citam que é pouco eficiente o conhecimento que os servidores DHCP tem dos endereços IP disponíveis, e dizem que seria melhor que os servidores realizassem uma verificação com o envio de pacotes ICMP para realmente constatar se um endereço IP está disponível antes da sua atribuição. Outro problema apontado é a não detecção de problemas de conflitos de IP pelo baixo controle que existe.

Os autores sugerem o desenvolvimento de uma ferramenta para monitorar o uso dos endereços IP baseados em ICMP, ARP e DHCP, gerando um alarme em uma interface para o administrador, em situações de violação das condições configuradas na ferramenta, e ainda sugerindo possíveis correções.

A análise do trabalho de Brik et al (2004) traz uma ferramenta que é completamente passiva, a sugestão dos autores é reativa, com apenas uma recomendação para a solução de um possível problema de conflito de endereço IP. Um conflito pode causar uma indisponibilidade no ambiente de rede sendo muito prejudicial para as mais diversas aplicações.

3.12 Conclusão

Foram analisados diversos trabalhos que tratam da gestão da atribuição de endereços IPv4, quanto de aspectos de segurança, desempenho e disponibilidade. Todos deixam clara a preocupação com a segurança nos ambientes de rede local, principalmente na conexão dos usuários às redes.

As propostas dos autores Wang et Lee (2002) e Dai et Chiang (2007) realizam o gerenciamento de atribuição de endereços IP baseados no serviço DHCP. Ambos

trabalhos sugerem que o servidor DHCP seja responsável pela geração de regras de filtragem, comparando com os endereços em uso na rede ou somente na base de dados do serviço DHCP e enviem estas informações aos equipamentos de rede (*switches* e roteadores) para que sejam aplicados filtros que permitam apenas o tráfego destes endereços IP ou MAC.

Mas estas soluções oneram o servidor DHCP que é o responsável por todas as alterações, atuando na tomada de decisão de quais regras de filtragem devem ser aplicadas nos roteadores e *switches*. Além disto, o tempo de resposta em caso de violação no gerenciamento de atribuição de endereços IP pode não atender aos objetivos propostos que é manter a segurança e disponibilidade dos ambientes de rede IP.

Ainda no trabalho de Dai et Chiang um ponto a ser observado é o local da aplicação das regras de filtragem. Os autores escolhem os roteadores para esta finalidade. Com isto todo o ambiente de rede local fica desprotegido com relação ao gerenciamento da atribuição de endereços IP. Permitindo que um endereço IP seja duplicado, podendo até indisponibilizar toda a rede se o endereço IP configurado por um usuário seja o endereço IP do *default gateway* da rede.

Outros trabalhos, como Li et al, Shari et al e Zuquete, relatam a preocupação com a disponibilidade dos ambientes de rede, propondo melhorias na autenticação entre clientes e servidores DHCP. Estas soluções podem ser usadas em conjunto com o gerenciamento da atribuição de endereços IP para melhor garantir a disponibilidade dos ambientes de rede.

Em nenhum destes trabalhos o ponto de tomada de decisão e o ponto de execução das regras de filtragem estão nos elementos de rede, evitando pontos de gargalo no processamento das alterações, quando uma quantidade excessiva de interações entre clientes e o servidor DHCP é necessária.

4 IMPLEMENTAÇÕES RELACIONADAS

Este capítulo descreve algumas implementações que não possuem representação na literatura acadêmica. São analisadas as implementações de mercado aqui nomeadas como implementação de mercado M1 e implementação de mercado M2. Além disso, também é descrita uma implementação própria denominada Address Guard.

4.1 Descrição da implementação de mercado M1

A implementação de mercado M1, usada para garantir que clientes usem de forma obrigatória endereços fornecidos por um servidor DHCP, é composta pela soma de outras duas funcionalidades, que são o DHCP *snooping* e o IP *source guard*. Não existe uma funcionalidade especifica para gerenciamento da atribuição de endereços IP baseado nas mensagens DHCP.

O DHCP *snooping* inspeciona as portas clientes e permite apenas nas configuradas como confiáveis, o envio de mensagens DHCP OFFER. Isto impede que um servidor DHCP clandestino possa atribuir endereços IP a um cliente. Além deste filtro, também constrói uma tabela com todas as atribuições feitas pelo servidor DHCP usando as mensagens DHCP trocadas entre cliente e servidor.

O IP *source guard* atua como uma ferramenta para evitar um problema de segurança chamado de IP *spoofing*, quando o cliente altera o endereço IP de origem dos pacotes para impedir ou dificultar o rastreamento da origem de acessos e outros incidentes de segurança. Com o uso de filtros, o IP *source guard* permite apenas que pacotes, com um determinado endereço IP, sejam encaminhados.

Com a soma das duas funcionalidades citadas (DHCP *snooping* e IP *source guard*), um *switch* consegue impedir que clientes de uma rede local TCP/IP usem endereços IP que não tenham sido atribuídos por um servidor DHCP.

4.1.1 Resumo do método

O método usado pela implementação de mercado M1 utiliza duas outras funcionalidades com finalidades distintas: DHCP *snooping* e IP *source guard*.

No DHCP *snooping*, o *switch* mantém uma tabela com todos os IPs que foram atribuídos pelo servidor DHCP para as estações que estão conectadas ao *switch*. As mensagens usadas para montar a tabela do DHCP *snooping* são o DHCP ACK, NAK, RELEASE e DECLINE. As tabelas são geradas dependendo da configuração das portas, pois o DHCP *snooping* permite configurar como confiável e não confiável. As portas cuja configuração está como confiável tem permitido o tráfego de mensagens DHCP que seriam enviadas por servidores, por exemplo, DHCP OFFER e DHCP ACK. Já as portas configuradas como não confiáveis tem o tráfego das mensagens DHCP OFFER e DHCP ACK bloqueado. Assim os servidores DHCP devem ser conectados em portas configuradas como confiáveis.

Já o IP *source guard* faz uso da tabela do DHCP *snooping* para a aplicação das regras de filtragem de pacotes em cada porta do *switch*.

A proteção ocorre da seguinte forma: inicialmente todo o tráfego é bloqueado na porta, exceto as mensagens DHCP que são autorizadas pelo DHCP *snooping*. Quando um cliente recebe um endereço IP atribuído por um servidor DHCP, algumas informações da mensagem DHCP ACK são utilizadas para configurar a tabela do DHCP *snooping*. Em seguida é criada uma PACL (*Port Access Control List*) permitindo apenas o encaminhamento de pacotes cujo endereço IP de origem seja igual ao atribuído pelo servidor DHCP.

Ao ser alterado o endereço IP do cliente pelo servidor DHCP, a PACL é alterada e então reaplicada na porta em questão. Ao ser alterado o endereço IP, pelo usuário de forma manual, uma mensagem de DHCP RELEASE é enviada por este cliente. Esta mensagem é detectada pelo DHCP *snooping* que então remove o endereço IP da

tabela do DHCP *snooping*. Essa remoção da tabela causa a execução de uma PACL padrão para bloquear todo o tráfego IP da respectiva porta, exceto para mensagens DHCP.

Uma forma de burlar o controle seria a utilização de um equipamento na própria rede executando um servidor DHCP não oficial, liberando endereços, com mensagens DHCP ACK, não autorizados para estações clientes. Estas mensagens seriam detectadas pelo DHCP *snooping* e teriam o tráfego permitido na respectiva porta. Para impedir isso é possível definir para as portas que não são usadas por servidores DHCP uma configuração de não confiável.

4.1.2 Restrições do método

A maior restrição do método é o fato de usar apenas a mensagem DHCP ACK para considerar como válido um endereço IP teoricamente atribuído para um cliente.

Considerando uma topologia que tem o servidor DHCP conectado em um *switch* que não suporta GAEIP e as estações ligadas em outros *switches* que implementem GAEIP, o controle não pode ser executado na porta de *uplink*, porque a configuração nesta tipo de porta deve ser do modo confiável. O DHCP *snooping* usa duas classificações de porta: confiável e não confiável. No modo não confiável são bloqueadas todas as mensagens DHCP que seriam enviadas por um servidor como (DHCP OFFER e DHCP ACK). Já o modo confiável não filtra qualquer tipo de mensagem DHCP.

Assim toda mensagem DHCP é permitida na porta de *uplink*, não fazendo distinção entre mensagens de um servidor DHCP oficial e mensagens de um possível servidor DHCP clandestino. O fato do método considerar somente a mensagem DHCP ACK, faz com que o conteúdo das mensagens DHCP ACK alimente a tabela do DHCP *snooping*, que responsável pela liberação do tráfego. Assim endereços IP fornecidos pelo servidor DHCP clandestino podem permitir que estações contornem o controle do GAEIP.

4.1.3 Restrições da implementação

As restrições da implementação de mercado M1 são :

- Não é possível usar com outras funcionalidades como PACL;
- Não é recomendado usar em portas trunk;
- Não é recomendado usar em portas com agregação de interfaces físicas;
- Necessidade de manutenção de uma tabela contendo os endereços atribuídos a cada porta, e o tempo para cada atribuição. Em caso de problema com esta tabela, ocasionará indisponibilidade no ambiente;
- Suporta ate 48 IPs por porta, em sistemas operacionais novos. Anteriormente este limite era de 10;
- Se em um ambiente o tempo de *lease* for muito baixo, pode gerar uma carga maior no *switch* pois a tabela estará em constante alteração. Este aumento do uso dos recursos pode trazer impactos no desempenho do ambiente;
- No caso de uma possível implementação do serviço DHCP para servidores, com *lease* muito alto, e em interfaces que sejam conectadas servidores usando virtualização, este mecanismo pode não funcionar corretamente;
- Nos *switches* L2 não existe a funcionalidade de IP *source guard*.

Os testes realizados com um *switch* desta implementação de mercado M1 mostraram que o objetivo de não permitir o acesso de clientes com IPs que não foram atribuídos pelo servidor DHCP é atingido com algumas restrições, como o *switch* atuar na camada 3.

Isto obriga que, para aplicar esta funcionalidade, deverão ser adquiridos *switches* mais caros e maiores, sem a utilização plena das funcionalidades disponíveis.
Mesmo nos *switches* L3, ainda existem algumas restrições de hardware e software.

As configurações usadas no laboratório para o teste do funcionamento o DHCP *snooping* com o IP *source guard*, como pode-se observar na figura 4.1

```
DHCP Snooping
int range xxx
!
no ip dhcp snooping trust
!
ip verify source vlan dhcp-snooping port-security
```

Figura 4.1 : Configuração usada na implementação de mercado M1

Fonte: Elaborado pelo autor (2010)

4.2 Descrição da implementação de mercado M2

A implementação de mercado M2 também é composta por duas funcionalidades distintas: DHCP *snooping* e o IP *source guard*. O DHCP *snooping* armazena em uma tabela as informações recebidas do servidor DHCP como o endereço MAC, a porta cujo cliente está conectado e a VLAN desta porta.

O IP *source guard*, que aplica filtros para restringir o tráfego tendo como base os endereços IP e MAC relacionados na tabela do DHCP *snooping*.

4.2.1 Resumo do método

O método usado pela implementação de mercado M2 é similar ao método usado pela implementação de mercado M1, que soma duas funcionalidades com funções distintas para evitar o uso de endereços falsos, mais conhecido como IP *spoofing*, e para evitar falsos servidores DHCP no ambiente de rede.

O método conta com a busca e identificação das mensagens DHCP para alimentar a tabela da funcionalidade DHCP *snooping*. Esta tabela contém os endereços MAC, IP e

o tempo de *lease* em segundos. Com as informações desta tabela a funcionalidade complementar, chamada IP *source guard* aplica filtros de regras de filtragem.

Somente a mensagem DHCP ACK é utilizada para popular a tabela do DHCP *snooping*.

4.2.2 Restrições do método

A restrição do método é o uso de somente a mensagem DHCP ACK para verificar se um cliente está usando um endereço IP fornecido pelo servidor DHCP. O problema da liberação do tráfego causado pelo uso de mensagens DHCP oriundas de servidor DHCP clandestino, conforme descrito no capítulo 4.1.2.

4.2.3 Restrições da implementação

A funcionalidade apresentada pela implementação de mercado M2 possui as seguintes restrições de implementação:

- Não é recomendada a aplicação desta funcionalidade em portas agregadas, como por exemplo o uso do IEEE 802.3ad (Ethernet Channel);
- A criação de entradas estáticas requer cuidados e traz problemas como a indisponibilidade do tráfego de um ou mais clientes;
- Não deve ser utilizada em portas de *uplink.*

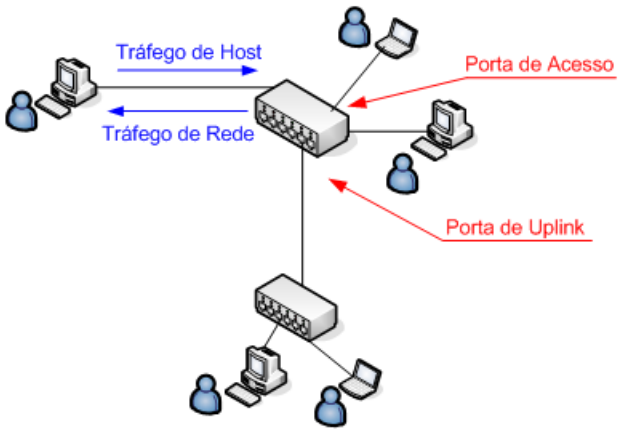
4.3 Proposta Address Guard

Este trabalho apresenta uma proposta alternativa para gerenciamento da atribuição dos endereços IP baseados nas mensagens DHCP. A partir da proposta foi realizada uma implementação tipo prova de conceito que será incluída na análise das implementações realizadas neste trabalho.

4.3.1 Descrição técnica

A funcionalidade Address Guard, nome usado para a prova de conceito, é voltada para *switches* (equipamentos tipo *bridge*) (IETF, 2004) para permitir somente o uso de endereços IP dinâmicos nas portas cuja configuração estiver aplicada. Ao habilitar a funcionalidade em uma porta de acesso, o *switch* de rede local permitirá o tráfego de quadros somente após a atribuição e uso de um endereço IP dinâmico designado por um servidor DHCP.

Ao habilitar a funcionalidade em uma porta de *uplink* (conexão entre *switch* e outro elemento de rede que tenha mais de uma porta, como por exemplo outro *switch* ou um *hub*) ilustrada na figura 4.2, o tráfego é restrito somente aos destinatários com endereços IP atribuídos dinamicamente.



Legenda:

- Porta de Acesso – Porta onde as estações de trabalho e servidores são conectadas. Normalmente, tem apenas um endereço MAC.
- Porta de Uplink – Porta que são usadas para interconectar os switches de uma rede local.
- Tráfego de Host – Tráfego de entrada em uma porta de acesso ou uplink
- Tráfego de Rede – Tráfego de saída em um porta de acesso ou uplink

Figura 4.2 : Definições Tráfegos e Portas

Fonte: Elaborado pelo autor (2011)

Conforme a RFC 2131 (IETF, 1997), todos os clientes DHCP que sofrerem qualquer alteração nos parâmetros de rede local, como uma reinicialização ou desconexão com a rede, deverão revalidar ou solicitar novamente sua configuração ao servidor DHCP.

Ao fazer a verificação das mensagens DHCP REQUEST e ACK, o tempo de *lease* é extraído da mensagem DHCP e usado para a determinação do tempo que este é válido e quando o filtro deverá ser aplicado para bloquear o tráfego, caso não ocorra nenhuma renovação.

O Address Guard também permite o uso de endereços IP fixos que podem ser usados em impressoras e outros equipamentos como *scanners*. Quando existir esta necessidade o endereço deste elemento será inserido manualmente na regra de filtragem que permitirá todo o tráfego oriundo deste determinado endereço MAC e endereço IP.

4.3.2 Escopo

O escopo da implementação é restrito à pilha TCP/IP e o protocolo IPv4.

4.3.3 Controle nas portas de acesso

Nas portas de acesso, figura 4.4, ocorre a filtragem somente do tráfego de entrada (no sentido de host para o *switch*), quando este tráfego for autorizado.

A monitoração de mensagens DHCP ocorre sempre que a porta estiver encaminhando tráfego. O mapa de estado da proposta, conforme figura 4.3, ilustra o funcionamento proposto para a porta de acesso.

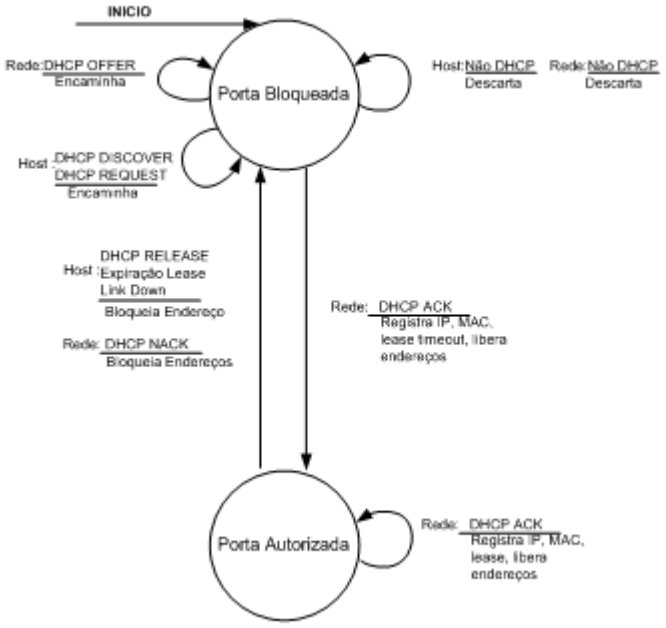


Figura 4.3: Diagrama de estado para porta de acesso

Fonte: Elaborado pelo autor (2010)

O mecanismo do Address Guard monitora a passagem das mensagens DHCP e, quando receber uma sequência com as mensagens de DHCPREQUEST e DHCPACK, estando relacionadas a uma mesma estação, o tráfego de pacotes será liberado para esta porta. Caso o mecanismo não identifique esta comunicação, o filtro de quadros continuará aplicado, permitindo apenas o tráfego de mensagens DHCP além das mensagens para o endereço de *broadcast*.

Mesmo com o tráfego liberado são permitidos apenas quadros na entrada da porta do *switch* que tenham o mesmo endereço físico e endereço IP do solicitante do endereço IP ao servidor DHCP, além do tráfego de *broadcast* e *multicast*. Isto acontece com o uso de regras de filtragem. Mesmo com o tráfego liberado, todas as mensagens DHCP são coletadas e analisadas. Na detecção das mensagens DHCP RELEASE e DHCP NACK, o filtro é aplicado para bloquear tráfego do endereço físico.

O Address Guard bloqueia o tráfego na porta em caso do *lease* expirado ou ainda na detecção da mensagem de DHCP RELEASE ou DHCP NACK. Este bloqueio impede que qualquer quadro ou pacote seja encaminhado se tiver respectivamente um determinado endereço MAC e um determinado endereço IP.

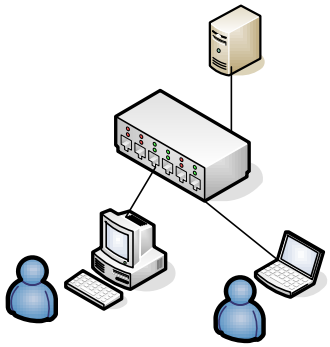


Figura 4.4: Diagrama conexão porta acesso

Fonte: Elaborado pelo autor (2009)

Se uma interface permanecer ativa e com o tráfego liberado, o Address Guard continuará em operação para o caso do usuário alterar a modalidade de configuração do endereçamento para IP fixo, e garantir que ao término do tempo de *lease* do IP, o cliente faça uma nova requisição ao servidor DHCP. Nesta situação inspecionará outras mensagens como DHCPREQUEST, DHCP ACK e DHCPRELEASE que são utilizadas na renovação do endereço IP e quando é encerrado o modo de operação DHCP na estação cliente, ou seja, quando é configurado um IP fixo manualmente.

Para evitar que uma estação altere seu endereço IP de forma manual sem que ocorra o envio da mensagem DHCP RELEASE, o Address Guard usa uma tabela que contém os endereços IP, MAC e também o tempo de lease do endereço IP. Com a tabela o Address Guard sabe qual o tempo máximo de validade do endereço IP atribuído, o endereço IP atribuído à estação conectada na porta em questão e também o endereço MAC da estação para o qual o endereço IP foi atribuído.
Como o servidor DHCP atribuiu o endereço IP com um tempo de *lease*, este endereço não será atribuído para outro cliente até que este tempo esteja encerrado. Assim há a garantia que não acontecerá qualquer conflito de endereço IP.

Outra característica do funcionamento da porta de acesso é a remoção da permissão do tráfego na regra de filtragem aplicada na porta. Este comportamento não interfere no funcionamento da rede porque quando um cliente restabelece sua conexão física com o *switch*, precisa fazer uma nova validação do endereço IP recebido previamente, usando para isto a mensagem DHCP REQUEST. Assim o servidor DHCP responde com a mensagem DHCP ACK.

4.3.4 Controle nas portas de *uplink*

Na porta de *uplink* ilustrada na figura 4.6, ocorre a liberação de tráfego dos quadros que tenham seus endereços atribuídos por um servidor DHCP. O bloqueio do tráfego também é feito por endereço MAC e IP, da mesma forma das portas de acesso, descrito no capítulo 4.3.3. O comportamento do Address Guard em portas de *uplink* é mostrado na figura 4.5.

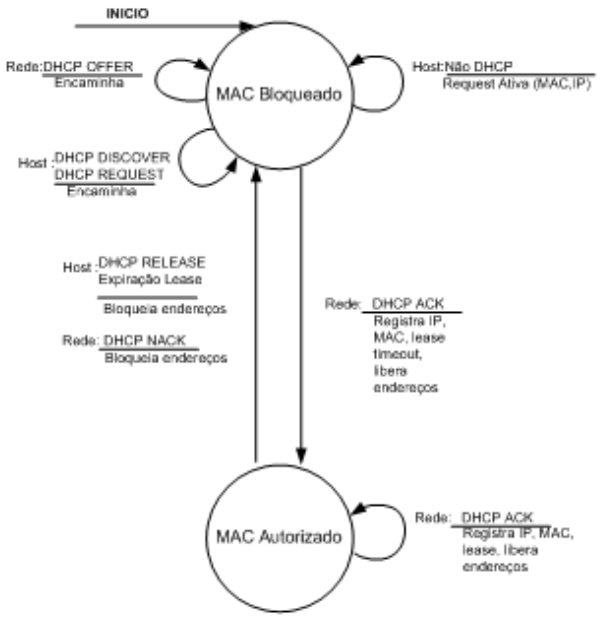


Figura 4.5: Diagrama de estado para porta *uplink*

Fonte: Elaborado pelo autor (2010)

O Address Guard mantém o estado MAC bloqueado desde quando a porta começa a funcionar. Na detecção das mensagens DHCP REQUEST e DHCP ACK, estando estas mensagens relacionadas a um mesmo endereço MAC, o estado do endereço MAC e IP vai para o estado de MAC Autorizado. Neste estado o tráfego é liberado. O tráfego voltará ao estado de MAC Bloqueado quando na monitoração das mensagens DHCP forem detectadas uma das mensagens DHCP NACK ou DHCP RELEASE; ou também quando o tempo de *lease* expirar.

Endereços IP fixos para elementos como servidores são suportados pelo Address Guard, que nestes casos, tem os respectivos endereços IP e endereços MAC inseridos na tabela da porta de *uplink* de forma manual.

A questão mais relevante nas portas de *uplink* está nas situações de reiniciação dos *switches*, quando as tabelas usadas pelo Address Guard são perdidas, bloqueando todo o tráfego. Outra preocupação é na reiniciação das portas de *uplink* (que pode acontecer devido a uma falha no cabo de conexão ou na reiniciação do *switch* que está conectado na outra ponta da porta de *uplink*) não devendo descartar o conteúdo das tabelas de controle.

Estas preocupações existem porque a atuação do Address Guard em portas de *uplink* deve ser habilitada quando o *switch* ou hub da outra ponta não suportar GAEIP. Assim, problemas nas permissões para encaminhamento do tráfego podem impactar completamente no acesso dos usuários conectados nos equipamentos sem o Address Guard ou similar.

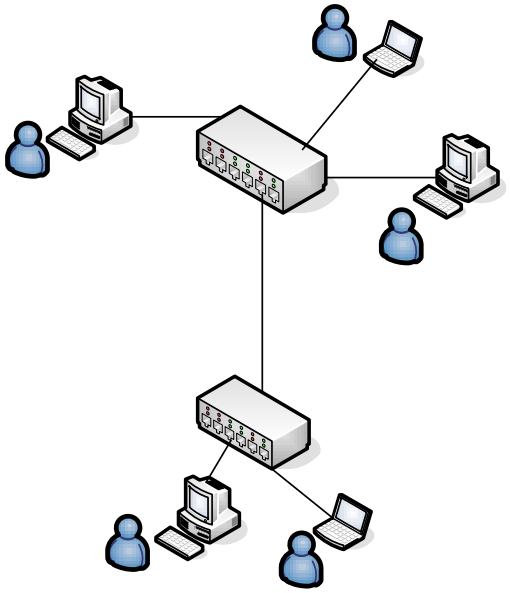


Figura 4.6: Diagrama conexão *uplink*

Fonte: Elaborado pelo autor (2009)

Na tentativa de evitar o bloqueio dos pacotes nestas situações, foram avaliadas duas possíveis soluções:

- Novas mensagens DHCP;
- Armazenar em um arquivo a tabela do Address Guard.

O uso de novas mensagens, conforme proposto por Joshi et al (2009), para viabilizar uma consulta para saber se um endereço é válido ou não, gera uma complexidade muito grande pois além de necessitar todo o desenvolvimento no protocolo DHCP, gera uma necessidade de desenvolvimento nos *switches* para o envio e recebimento de novas mensagens DHCP. Outro ponto importante é dependência da troca de mensagens entre o servidor DHCP para que o tráfego de uma determinada estação seja liberado.

Para resolver os problemas apontados neste capítulo, o Address Guard mantém a tabela com os endereços MAC, IP e tempo de *lease* de cada estação que está usando

um endereço IP fornecido pelo servidor DHCP. Isto é feito armazenando todas estas informações em um arquivo que por sua vez é salvo na memória não volátil.

Este armazenamento na memória não impacta na operação do *switch*, porque seu tamanho não precisa ser muito grande, e também porque a escrita neste arquivo não precisa ser condicionada a nenhum outro processo do *switch*. O Address Guard salva as informações dos endereços MAC, IP e tempo de *lease* periodicamente.

Com isso nas situações de reiniciação do *switch*, a primeira tarefa do Address Guard é carregar seu respectivo arquivo da memória não volátil.

Uma entrada só será removida da tabela, quando o Address Guard detectar a passagem da mensagem DHCP RELEASE, ou quando o tempo de *lease* expirar.

4.3.5 Diferenças para outras implementações

O Address Guard tem algumas mudanças em relação as implementações de mercado M1 e M2. A primeira mudança é o uso de uma mensagem DHCP a mais para que um endereço possa ser considerado atribuído pelo servidor DHCP e consequentemente este tráfego seja liberado. Este mensagem adicional é o DHCP REQUEST. As implementações de mercado M1 e M2 usam apenas o DHCP ACK, já o Address Guard usa as mensagens DHCP REQUEST e o DHCP ACK, existindo uma dependência entre ambas para que o tráfego de um determinado endereço IP seja liberado.

Outra alteração é a realização do controle nas portas de *uplink*, para atender outros elementos que não suportam GAEIP. As implementações de mercado M1 e M2 armazenam as informações dos endereços atribuídos pelo servidor DHCP em uma memória volátil, independente se a porta é de acesso ou de *uplink*. A implementação de mercado M2 informa que a funcionalidade para GAEIP não é suportada em portas de *uplink*. O Address Guard salva as informações em uma memória não volátil que permite seu funcionamento para portas de *uplink*. Esta restrição é devida a uma possbilidade de

problema caso o *switch* com GAEIP seja reiniciado sem que o *switch* sem GAEIP seja reiniciado também. Nesta situação as estações de clientes conectados no *switch* sem GAEIP teriam seu tráfego e funcionamento interrompidos.

4.3.6 Restrições da Implementação

As restrições da implementação do Address Guard estão relacionadas ao funcionamento em determinadas topologias com equipamentos que suportam e não GAEIP.

Com uma topologia onde existem equipamentos que suportam e que não suportam GAEIP, a verificação para as estações conectadas nos *switches* sem GAEIP é feita na porta de *uplink* no *switch* com GAEIP.

O primeiro cenário que demonstra uma restrição do Address Guard está na figura 4.7. Neste topologia são encontrados dois problemas. O primeiro problema está na conexão do servidor DHCP a um *switch* sem suporte a GAEIP. O segundo problema está na conexão entre dois *switches* sem GAEIP. O primeiro problema está relacionado a incapacidade do Address Guard proteger o ambiente contra servidores DHCP não autorizados, porque as conexões dos outros *switches* a este não podem ter o Address Guard habilitado. Assim não há qualquer controle de mensagens DHCP nestas conexões. O outro problema está na conexão entre dois *switches* sem GAEIP, que aumenta a abrangência de um possível problema de conflito de endereço IP, podendo afetar uma quantidade maior de clientes.

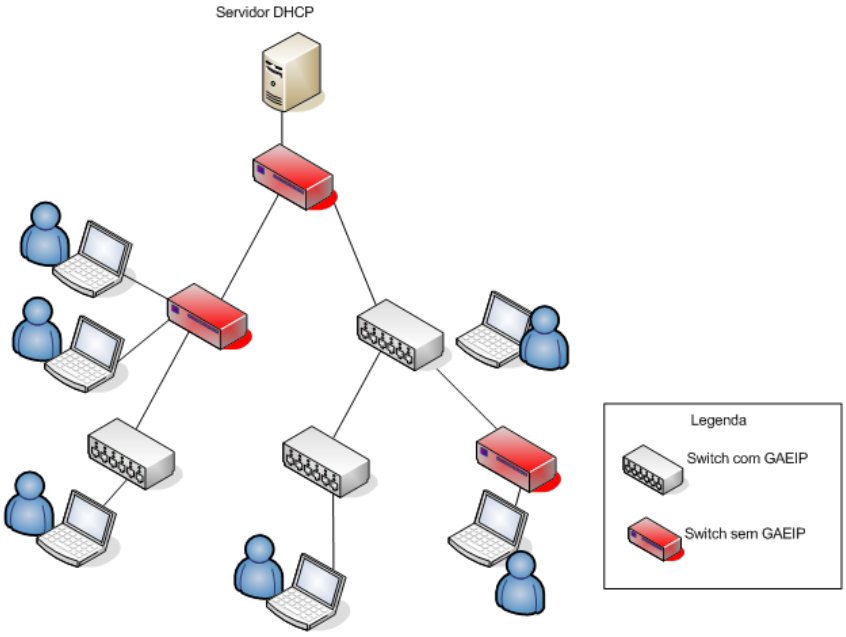


Figura 4.7: Restrição de topologia do Address Guard – Cenário 1

Fonte: Elaborado pelo autor (2011)

No segundo cenário representado pela figura 4.8 o problema da conexão do servidor DHCP foi resolvido, mas ainda existem dois *switches* sem GAEIP conectados, que pode causar um impacto maior em um caso de conflito de IP. Quanto maior a quantidade de *switches* sem GAEIP conectados diretamente, maior pode ser o impacto em situações de problema.

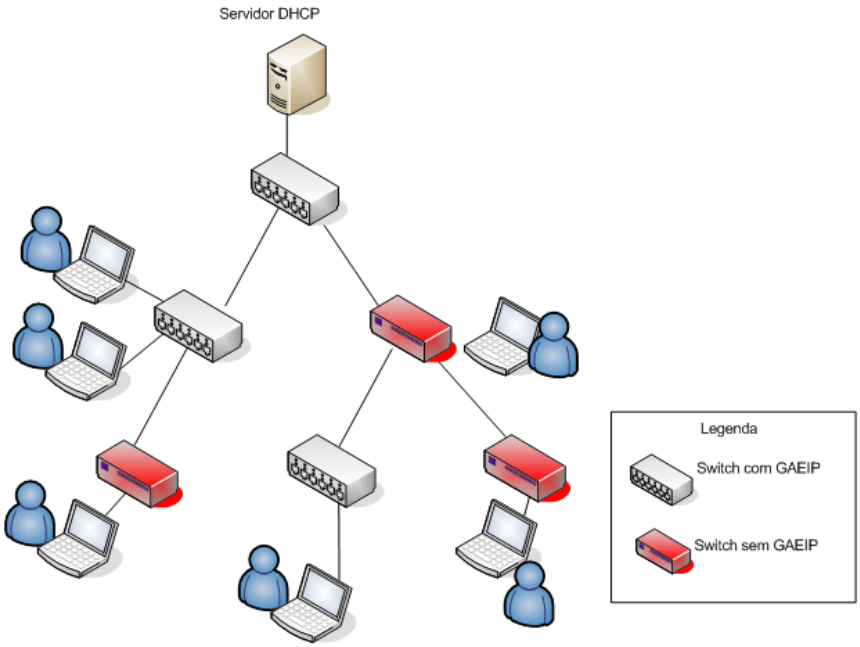


Figura 4.8: Restrição de topologia do Address Guard – Cenário 2

Fonte: Elaborado pelo autor (2011)

As restrições de topologia do Address Guard são:

- Servidor DHCP deve ser conectado em um *switch* com GAEIP
- Dois ou mais *switches* sem GAEIP nunca podem estar conectados diretamente. Entre eles deve haver um *switch* com GAEIP.

5 IMPLEMENTAÇÃO DO ADDRESS GUARD

Este capítulo apresenta a implementação tipo prova de conceito com nome de Address Guard. Os componentes utilizados como hardware, software e *scripts* de configuração são citados e demonstrados.

5.1 Componentes de hardware e software utilizados

Para a implementação do Address Guard foi usado o sistema operacional Linux Ubuntu por ser um software aberto com grande quantidade de aplicativos e a facilidade de se criar *scripts*. Como o intuito da prova de conceito é mostrar o conceito em funcionamento, os pontos citados foram fundamentais para a decisão de qual sistema operacional usar.

Na estação que simula o funcionamento do *switch*, o Linux na distribuição Ubuntu foi instalado em uma estação com duas interfaces de rede. Estas duas interfaces foram colocadas em modo *bridge*, usando comandos apresentados na figura 5.1.

```
Ifconfig eth0
Ifconfig eth1
Ifconfig eth2
Brctl addbr br0
Brctl addif br0 eth0
Brctl addif br0 eth1
Brctl addif br0 eth2
Ifconfig br0 up 192.168.1.200
```

Figura 5.1: *Script bridge* portas Address Guard

Fonte: Elaborado pelo autor (2010)

Para servidor DHCP foi usado um roteador Linksys, atribuindo apenas o range de 192.168.1.101 até o 192.168.1.139

A rede configurada foi 192.168.1.0, com a máscara 255.255.255.0, sendo o servidor DHCP com o 192.168.1.1

Para as estações foi usado o sistema operacional Windows. Para a simulação da porta de *uplink* foi usado um hub permitindo o uso de mais de uma estação pela mesma porta.

Os pacotes usados na instalação foram:

- Dhcp3-server: Servidor DHCP;
- *Bridge*-util: *Bridge* entre 2 ou mais interfaces de rede;
- Ebtables: Filtro de quadros;
- PHP: Linguagem de Programação.

5.2 Implementação

Com a finalidade de realizar uma prova de conceito sobre a funcionalidade proposta, nomeada de Address Guard, foi usado o PHP para a implementação, com dois módulos principais: o módulo de detecção e o módulo de bloqueio.

5.2.1 Mecanismo de detecção

O mecanismo de detecção foi divido na captura das mensagens e procura das mensagens desejadas nos pacotes capturados.

5.2.1.1 Captura das mensagens

Para detecção das mensagens DHCP foi usado o tcpdump, conforme parâmetros na figura 5.2, que é uma ferramenta que permite a captura de pacotes de uma interface de rede. Sua aplicação acontece nas portas da estação que simula o funcionamento do *switch*, inspecionando todos os quadros recebidos e enviados nas interfaces, filtrando

apenas as mensagens UDP nas portas 67 e 68. Estas mensagens são então encaminhadas para o arquivo de nome captura.

```
tcpdump -vnles0 -i eth0 port 67 and port 68 > captura
```

Figura 5.2: *Script* captura mensagens DHCP

Fonte: Elaborado pelo autor (2010)

5.2.1.2 Procura das mensagens desejadas nos pacotes capturados

Em paralelo é executado o monit.php. Este *script* é composto por um laço principal e suas funções. O laço principal é executado a cada dez segundos, buscando o arquivo captura e verificando a quantidade de linhas. Se existir uma quantidade de linhas maior que o contador atual, realiza uma busca nestas linhas aplicando as funções `request()`, `reply()`, `release()` e `nack()`.

Cada função tem por objetivo verificar se as mensagens que interessam ao Address Guard, como DHCP REQUEST, ACK, RELEASE e NACK. Se alguma função encontrar a respectiva mensagem, executará o mecanismo de bloqueio ou liberação do tráfego.

Para garantir que o cliente está usando um endereço IP atribuído por um servidor DHCP, a liberação do tráfego só acontece com a identificação das mensagens DHCP REQUEST e DHCP ACK, quando os endereços MAC de origem da mensagem DHCP REQUEST e endereço MAC de destino do DHCP ACK são os mesmos.

No momento da liberação o tempo de *lease* é extraído das mensagens DHCP. Com esta informação o Address Guard soma o valor com o tempo do sistema, no caso do sistema operacional. Quando o valor deste contador for menor que do sistema, o mecanismo de bloqueio é acionado.

Todos os valores são armazenados em um vetor, contendo o endereço MAC e o tempo de *lease*. Sendo criado um vetor para cada endereço IP detectado e atribuído pelo servidor DHCP.

O tempo de validade de um endereço IP é calculado com a soma do tempo de *lease* extraído da mensagem DHCP em segundos com o tempo do sistema, chegando assim no tempo do sistema final, que caso não seja renovado, o respectivo endereço MAC e IP devem ser retirados da tabela que permite o tráfego destes endereços. O único pré-requisito para o correto funcionamento é o *switch* ter o horário atualizado por um servidor de tempo.

A geração do *script* seguiu todos os pontos citados no item 5.2.1.2, e é apresentado no Apêndice B contendo todas as linhas usadas no Address Guard para o GAEIP.

5.2.2 Mecanismo de bloqueio

O bloqueio é feito com o pacote ebtables. Este pacote possibilita a filtragem de quadros na camada 2 e também na camada 3. Alguns recursos desta ferramenta são usados como a possibilidade de filtrar quadros que não tenham um determinado endereço MAC e/ou endereço IP e não permitir seu encaminhamento.

São criados dois *scripts* em shell, chamados de libera_eth1 e bloqueia_eth1. Todas as interfaces ao serem ligadas, começam com o bloqueia_eth1. Este permite apenas o encaminhamento de mensagens DHCP, nas portas UDP 67 e 68.

Caso as mensagens DHCP sejam identificadas, é executado imediatamente o libera_eth1. Esta regra permite o tráfego dos quadros que tenham como endereço de origem, o endereço MAC do cliente que solicitou e recebeu o endereço IP do servidor DHCP.

O conteúdo do *script* libera_eth1 foi inserido na função reply, porque caso esta mensagem seja encontrada e associada com o request, o tráfego deve ser liberado, mas somente para os endereços MAC e IP contidos dentro destas mensagens, e para isto devem ser coletadas algumas variáveis para permitir a aplicação da regra de filtragem.

Se alguma mensagem DHCP RELEASE ou DHCP NACK for detectada na porta, o bloqueio é executado imediatamente, executando novamente o bloqueia_eth1. O *script* para bloqueio do tráfego é demonstrado na figura 5.3 e para a liberação do tráfego é demonstrado na figura 5.4

```
ebtables -F FORWARD
ebtables -A FORWARD -p ipv4 -i eth1 --ip-proto udp --ip-destination-port 67:68 -j
ACCEPT
ebtables -A FORWARD -p arp -i eth1 -j ACCEPT
ebtables -A FORWARD -i eth1 -j DROP
```

Figura 5.3: *Script* bloqueio tráfego

Fonte: Elaborado pelo autor (2011)

```
ebtables -F FORWARD
ebtables -A FORWARD –j CONTINUE  -s <mac address>
ebtables –A FORWARD –j ACCEPT –p ipv4 –ip- source <IP>
ebtables -A FORWARD -i eth1 -j DROP
```

Figura 5.4: *Script* liberação tráfego

Fonte: Elaborado pelo autor (2011)

Antes da aplicação de qualquer filtro o comando ebtables –F, para que qualquer outra configuração que exista seja removida, evitando assim uma sobreposição de comandos que possa comprometer o funcionamento do Address Guard.

6 METODOLOGIA E CENÁRIOS DE TESTES

Este capítulo descreve a metodologia utilizada nos testes de avaliação das implementações para gerenciamento de atribuição de endereçamento IPv4.

Para a realização dos testes de avaliação, foram definidos quatro cenários, cada um suportando escopos de operação distintos.

6.1 Descrição dos cenários

Para realizar todos os experimentos necessários, a metodologia dos testes utiliza quatros cenários, cada um representando uma topologia típica. O primeiro é um cenário simples onde uma estação é conectada a um *switch*. No segundo cenário um outro *switch* é conectado para verificação do comportamento entre os elementos de rede, sendo que ambos *switches* suportam GAEIP. No terceiro cenário os dois *switches* são mantidos, mas agora o *switch* onde o servidor DHCP não está conectado, não suporta GAEIP. O quarto e último cenário é similar ao terceiro, mas agora o *switch* que não suporta GAEIP é onde o servidor DHCP está conectado.

6.1.1 Cenário A

6.1.1.1 Objetivo

O objetivo do cenário A é testar o funcionamento básico do sistema do GAEIP baseado na monitoração de mensagens DHCP. Este cenário compreende a situação mais simples no qual existe somente um *switch*.

São usados para cada teste os *switches* das implementações de mercado M1, M2, e a implementação tipo prova de conceito.

6.1.1.2 Descrição

O cenário A compreende a configuração apresentada na figura 6.1, com um *switch*, um servidor DHCP, uma estação cliente e um tap para duplicar o tráfego da estação cliente para o *sniffer*. O servidor DHCP está configurado para atribuir endereços IP para clientes na faixa de 192.168.1.100/24 até 192.168.1.130/24.

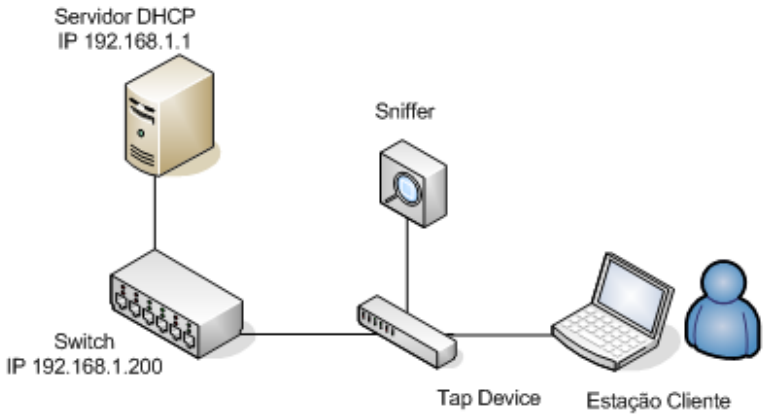


Figura 6.1: Topologia do Cenário A

Fonte: Elaborado pelo autor (2011)

Este cenário representa a situação mais simples de conectividade, que permite a realização dos testes funcionais.

6.1.2 Cenário B

6.1.2.1 Objetivo

O objetivo deste cenário é verificar o funcionamento do GAEIP em sub-redes com mais de um *switch*, e todos suportando GAEIP.

6.1.2.2 Descrição

Neste cenário todos os *switches* suportam a funcionalidade GAEIP. As configurações de controle de endereço IP serão feitas somente nas portas de acesso. Como todos os *switches* suportam a funcionalidade GAEIP não é necessário habilitar configuração GAEIP na porta de *uplink*, como ilustrado na figura 6.2. Um teste para avaliar a resistência contra servidor DHCP não autorizado também é feito, sendo este servidor conectado no *switch* A. O problema do servidor DHCP não autorizado é este enviar endereços IP sem que o cliente tenha solicitado, usando as mensagens ACK, causando problemas para o GAEIP baseado na monitoração de mensagens DHCP. Isto pode acontecer para que um cliente possa realizar um acesso indevido a um sistema, sem que possa ser rastreado, ou ainda podendo causar um conflito de IP.

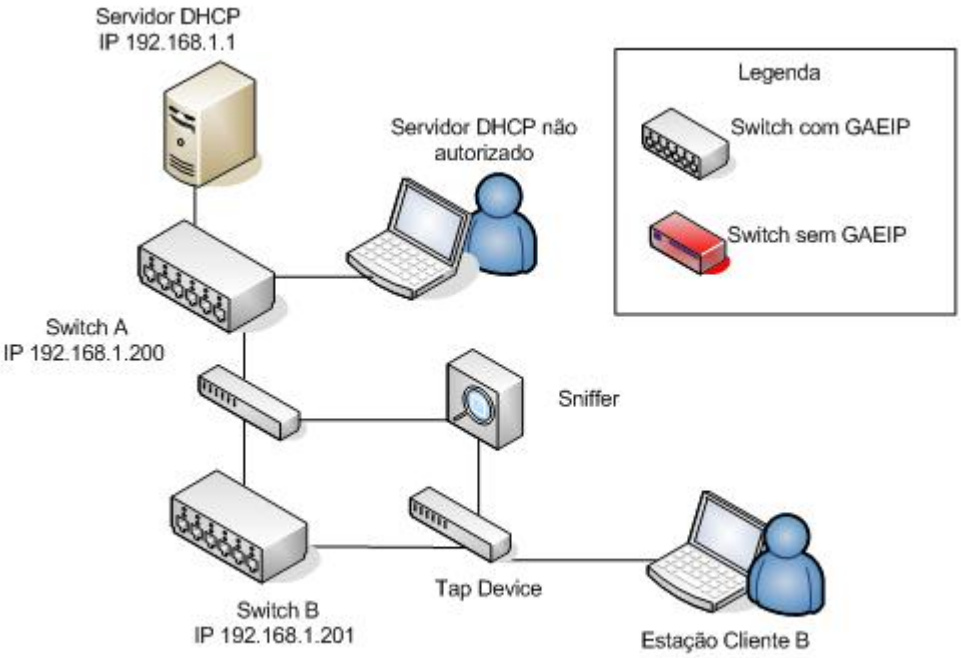


Figura 6.2: Topologia do Cenário B

Fonte: Elaborado pelo autor (2011)

6.1.3 Cenário C

6.1.3.1 Objetivo

O objetivo deste cenário é testar o funcionamento do GAEIP em sub-redes com topologia de equipamentos de rede de camada 2 (*hubs* e *switches)* com e sem funcionalidade GAEIP.

Este cenário representa uma possível situação de ambiente de rede onde nem todos os *switches* são gerenciados, e também um ou mais *switches* podem não suportar o GAEIP.

6.1.3.2 Descrição

Similar ao cenário B, mas com a alteração no *switch* B que agora não suporta GAEIP. Além disto, uma outra estação cliente é conectada no *switch* A, conforme figura 6.3.

Assim a verificação deverá ser feita na porta de conexão entre os *switches*, ou *switch* e hub. O escopo do servidor DHCP continua configurado como no cenário A, que atribui IPs para clientes na faixa de 192.168.1.100/24 até 192.168.1.130/24.

A resistência contra servidor DHCP não autorizado é testada com este servidor conectado no *switch* B.

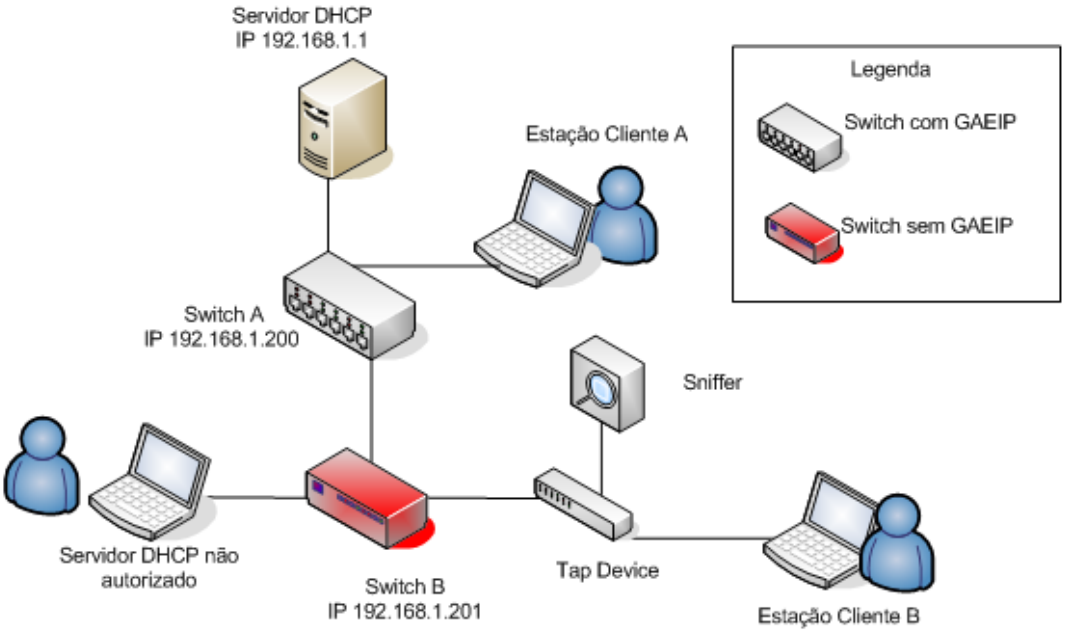


Figura 6.3: Topologia do Cenário C

Fonte: Elaborado pelo autor (2011)

O cenário C contempla uma possível topologia real onde existam *switches* heterogêneos, sendo que alguns suportem GAEIP e outros não suportem GAEIP. Esta situação pode acontecer em diversos ambientes onde equipamentos novos são conectados a equipamentos mais antigos. Neste caso o controle deve ser feito na porta de *uplink*.

6.1.4 Cenário D

Este cenário representa, da mesma forma que o cenário C no item 6.1.3, uma possível situação de ambiente de rede onde nem todos os *switches* são gerenciados, e também um ou mais *switches* podem não suportar o GAEIP.

6.1.4.1 Objetivo

O objetivo do cenário D é verificar a resistência contra servidor DHCP não autorizado em um ambiente onde o servidor DHCP está conectado em um *switch* que não suporta GAEIP baseado nas mensagens DHCP.

Na tentativa de burlar ou contornar a funcionalidade, uma máquina de forma não autorizada gera mensagens DHCP não verdadeiras.

Uma outra estação, diferente da estação cliente, fazendo uso de uma ferramenta de geração de pacotes, simula a atribuição via DHCP de endereço IP para uma determinada porta. Com isto será alterado o IP na estação para fixo, usando qualquer outro IP que fora enviado pelo tráfego DHCP não oficial. A verificação do funcionamento é feita com o envio de ICMP Request para o servidor DHCP.

6.1.4.2 Descrição

Similar ao cenário 2, mantendo uma estação que simula o funcionamento do cliente e um servidor DHCP.

Com a mesma quantidade de elementos do cenário C, trocando apenas a posição física entre os dois *switches*, de acordo com a figura 6.4. O *switch* que suporta a funcionalidade agora é usado para a conexão das estações. O *switch* que não suporta a funcionalidade de gerenciamento da atribuição de endereços IP baseado nas mensagens DHCP, agora é usado para conectar o servidor DHCP.

O escopo do servidor DHCP continua configurado como no cenário A, que atribui IPs para clientes na faixa de 192.168.1.100/24 até 192.168.1.130/24.

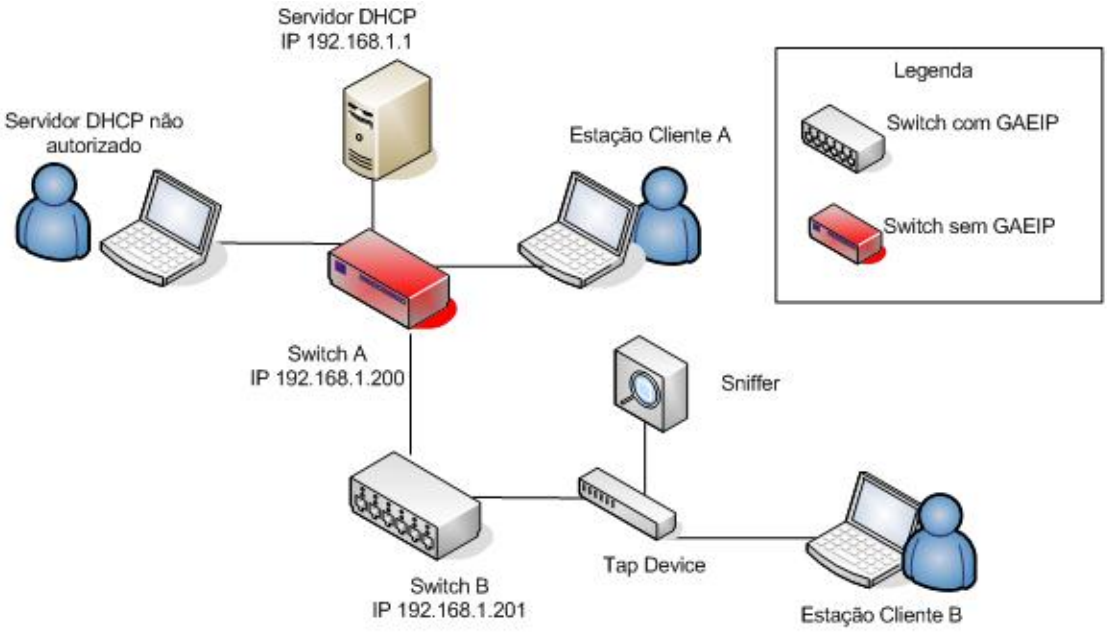


Figura 6.4: Topologia do Cenário D

Fonte: Elaborado pelo autor (2011)

6.2 Metodologia dos testes

Os procedimentos de todos os testes necessitam de alguns passos prévios que serão apresentados em todos os testes como a conectividade entre todos os elementos. Os passos contemplados na conectividade entre todos os elementos são:

- Ligar todos os elementos, incluindo *switches* e servidor DHCP;
- Conectar o tap device e o *sniffer*;
- Realizar as conexões físicas, desde que esta deva ser feita no andamento do teste.

6.2.1 Cenário A

O cenário A possui os seguintes testes funcionais:

- Conexão de um novo cliente via DHCP (quadro 6.1);

- Conexão de um novo cliente utilizando IP fixo (quadro 6.2);
- Alteração do IP de dinâmico para fixo (alterando e mantendo o mesmo IP) (quadro 6.3);
- Alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP Release (quadro 6.4);
- Renovação do aluguel do endereço IP (quadro 6.5);
- Alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP e com o tempo de aluguel do endereço IP expirado (quadro 6.6);
- Desconexão e reconexão do ponto de rede à mesma máquina (quadro 6.7);
- Substituição da estação por outra na mesma porta (quadro 6.8);
- Reinicialização do cliente (quadro 6.9);
- Reinicialização do *switch* (quadro 6.10).

Quadro 6.1: Teste conexão de um novo cliente via DHCP.

Nome do Teste	Conexão de um novo cliente via DHCP
Descrição	Este teste tem como objetivo a observação do comportamento da funcionalidade, com a conexão de um novo cliente a um *switch* que tem em suas portas de acesso a funcionalidade de GAEIP baseado em mensagens DHCP configurada. Para verificar a conectividade será utilizado o comando ping (pacotes ICMP Echo Request são enviados da estação para o servidor DHCP e ICMP Echo Reply são recebidos). Na captura do tráfego é usado um tap device para fazer o espelhamento de todo o tráfego em uma outra porta que por sua vez é analisado por um *sniffer*.
Procedimento	Na estação cliente: Iniciar o comando ping com destino o IP do servidor DHCP (192.168.1.1) e o IP do switch (192.168.1.200); Na estação cliente: Configurar a estação para utilizar o protocolo DHCP; Conectar o cabo entre a estação e o switch ; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	A porta deverá estar liberada para o tráfego, caso o cliente use um IP atribuído pelo servidor DHCP.

Quadro 6.2: Teste conexão de um novo cliente utilizando IP fixo.

Nome do Teste	Conexão de um novo cliente utilizando IP fixo
Descrição	Testar a conexão de um novo cliente com configuração de IP fixo.
Procedimento	No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar o IP 192.168.1.101; Conectar o cabo entre a estação e o *switch* ; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	Como o cliente tem IP fixo, não existe a troca de mensagens DHCP. Nesta situação o tráfego não será liberado.

Quadro 6.3: Teste alteração do IP de dinâmico para fixo.

Nome do Teste	Alteração do IP de dinâmico para fixo
Descrição	Alteração do endereço IP atribuído dinamicamente via DHCP para o mesmo endereço IP fixo na mesma rede, e também um outro endereço IP fixo na mesma rede.
Procedimento	No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para utilizar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Na estação cliente: Configurar o IP 192.168.1.100; No *switch* : Verificar o funcionamento do comando ping; Na estação cliente: Configurar o IP 192.168.1.105; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	Na alteração de IP dinâmico para fixo, o cliente DHCP deve enviar um DHCPRELEASE. Neste instante, a funcionalidade deve detectar a presença desta mensagem e assim, bloquear o tráfego.

Quadro 6.4: Teste alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP.

Nome do Teste	Alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP Release
Descrição	Alteração do endereço IP atribuído dinamicamente via DHCP para o mesmo endereço IP fixo na mesma rede, e também um outro endereço IP fixo na mesma rede. Neste teste, após a aquisição do IP será filtrada a troca de mensagens para o servidor DHCP, para que não seja enviada pelo cliente e mensagem de DHCP Release após a alteração para IP fixo.
Procedimento	No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Na estação cliente: Inserir uma entrada na tabela ARP para o endereço IP 192.168.1.1 com o mesmo endereço físico da estação cliente; Na estação cliente: Configurar o IP 192.168.1.101; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	O tráfego é liberado após o recebimento do endereço IP fornecido pelo servidor DHCP. Como a mensagem de DHCP Release, enviada após a configuração do IP fixo, é bloqueada ao ser desviada para o mesmo endereço físico da estação cliente, a funcionalidade não detecta a mesma e consequentemente o tráfego não é bloqueado.

Quadro 6.5: Teste renovação do aluguel do endereço IP.

Nome do Teste	Renovação do aluguel do endereço IP
Descrição	Testar o comportamento na renovação do endereço IP, após o prazo da utilização do IP ter se esgotado.
Procedimento	Na estação cliente: Iniciar o comando ping com destino o IP do switch (192.168.1.200) e também para o IP do servidor DHCP (192.168.1.1); Conectar o cabo entre a estação e o switch; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP, principalmente a renovação do endereço IP; No *switch* : Verificar o funcionamento do comando ping; No *switch* : Verificar o funcionamento da funcionalidade.
Comportamento Esperado	O endereço IP é renovado com as mensagens DHCP REQUEST e o tráfego continua sendo encaminhado, sem impacto para o cliente.

Quadro 6.6: Teste alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP Release e com o tempo de alugle expirado.

Nome do Teste	Alteração do IP de dinâmico para fixo com filtragem da mensagem DHCP Release e com o tempo de aluguel expirado
Descrição	Alteração do endereço IP atribuído dinamicamente via DHCP para o mesmo endereço IP fixo na mesma rede, e também um outro endereço IP fixo na mesma rede. Neste teste, após a aquisição do IP será filtrada a troca de mensagens para o servidor DHCP, para que não seja enviada pelo cliente e mensagem de DHCP RELEASE e após a alteração para IP fixo. Após a troca o tempo de aluguel do endereço IP será expirado no servidor DHCP.
Procedimento	Na estação cliente: Iniciar o comando ping com destino o IP do switch (192.168.1.200) e para o IP do servidor DHCP (192.168.1.1.); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; Na estação cliente: Verificar o funcionamento do comando ping; Na estação cliente: Inserir uma entrada na tabela ARP para o endereço IP 192.168.1.1 com o mesmo MAC da estação cliente; Na estação cliente: Configurar o IP 192.168.1.101; No *switch* : Verificar o funcionamento da funcionalidade ; Aguardar o tempo de expiração do endereço IP; No *switch* : Verificar o funcionamento da funcionalidade; Na estação cliente: Verificar o funcionamento do comando ping.
Comportamento Esperado	O tráfego é liberado após o recebimento do endereço IP fornecido pelo servidor DHCP. Como a mensagem de DHCP Release, enviada após a configuração do IP fixo, é bloqueada ao ser desviada para o mesmo endereço físico da estação cliente, a funcionalidade não detecta a mesma e consequentemente o tráfego não é bloqueado. Após a expiração do IP a funcionalidade que monitora o tempo de aluguel, bloqueia o tráfego pois não consegue detectar as mensagens DHCP.

Quadro 6.7: Teste desconexão e reconexão do ponto de rede à mesma máquina.

Nome do Teste	Desconexão e reconexão do ponto de rede à mesma máquina
Descrição	Desconectar e conectar novamente o cabo no switch com a mesma estação cliente. Isto leva a necessidade da troca de mensagens DHCP entre o cliente e o servidor DHCP para que o tráfego seja liberado nesta porta do switch.
Procedimento	No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Desconectar o cabo da estação cliente; No *switch* : Verificar o funcionamento do comando ping; Conectar o cabo da estação cliente no *switch* ; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	O tráfego da estação cliente só é liberado com a troca de mensagens DHCP entre o cliente e o servidor. Ao desconectar o cabo o tráfego é interrompido e a autorização cancelada. Após conectar novamente o cabo, com a troca de mensagens DHPC a autorização é novamente aprovada e o tráfego volta a ser encaminhado pela porta do switch.

Quadro 6.8: Teste substituição da estação por outra na mesma porta.

Nome do Teste	Substituição da estação por outra na mesma porta
Descrição	Desconectar uma estação cliente e conectar outra estação na mesma porta do switch, com o objetivo de tentar ter acesso a rede sem usar endereço IP dinâmico. Com a desconexão do cabo, há a necessidade da troca de mensagens DHCP entre o cliente e o servidor DHCP para que o tráfego seja liberado nesta porta do *switch* .
Procedimento	No *switch* : Iniciar o comando ping destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Desconectar o cabo da estação cliente; No *switch* : Verificar o funcionamento do comando ping; Conectar o cabo de uma outra estação cliente no *switch* ; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Na estação cliente: Alterar o endereço IP da estação que está desconectada para usar o mesmo IP do cliente conectado ao *switch* . Desconectar a estação cliente, que usa IP dinâmico; Conectar a estação que está com o IP fixo; Verificar o funcionamento do comando ping.
Comportamento Esperado	O tráfego da estação cliente só é liberado com a troca de mensagens DHCP entre o cliente e o servidor. Ao desconectar o cabo o tráfego é interrompido e a autorização cancelada. Após conectar o cabo desta porta a uma outra estação independente se a mesma está usando o mesmo IP ou qualquer outro, o tráfego só é liberado mediante a troca de mensagens DHCP entre o cliente e o servidor DHCP.

Quadro 6.9: Teste reinicialização do cliente.

Nome do Teste	Reinicialização do cliente
Descrição	O cliente ao reiniciar, pode não enviar o DHCPRELEASE, mantendo o endereço IP reservado para o seu endereço MAC. Quando o cliente volta a funcionar, envia um DHCP REQUEST solicitando a autorização para continuar usando o endereço IP que ele tinha recebido anteriormente. O servidor DHCP verifica na sua tabela e assim envia o DHCPACK com a permissão de uso do endereço IP.
Procedimento	No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para uso do protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping; Na estação cliente: Reiniciar o sistema operacional; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping.
Comportamento Esperado	Após a reinicialização do cliente, o tráfego é liberado quando detectada a troca de mensagens DHCP.

Quadro 6.10: Teste reinicialização do *switch.*

Nome do Teste	Reinicialização do *switch*
Descrição	Um *switch* pode reiniciar, devido a falha de energia elétrica, e também após uma alteração do sistema operacional.
Procedimento	Na estação cliente: Iniciar o comando ping para o IP do switch 192.168.1.200; Na estação cliente: Configurar a estação para uso do protocolo DHCP; Conectar o cabo entre a estação e o switch; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; Na estação cliente: Verificar o funcionamento do comando ping; Reiniciar o *switch* , desligando e ligando novamente; No *sniffer* : Acompanhar o fluxo de mensagens DHCP; Na estação cliente: Verificar o funcionamento do comando ping.
Comportamento Esperado	Como todas as portas são desligadas, os clientes conectados neste switch, devem tentar renovar o endereço IP que já está configurado nas respectivas interfaces de rede. A funcionalidade deverá identificar a troca de mensagens entre cliente e servidor, e assim permitir o tráfego.

O cenário A também apresenta o teste de carga, conforme quadro 6.11 e o teste de impacto na funcionalidade de lista de controle de acesso (quadro 6.12).

Quadro 6.11: Teste de carga.

Nome do Teste	Teste de carga
Descrição	Com a inspeção de todos os quadros que passam pelas portas de um switch, este pode ter seu desempenho reduzido por todas estas verificações que deverão ser feitas enquanto a porta estiver ligada. Todo ambiente de teste pode ser observado na figura 6.5. Este teste analisa o impacto no desempenho e disponibilidade do switch. O desempenho será medido com um analisador de protocolo ou sniffer, que medirá o tempo de encaminhamento do quadro pelo switch, desde a porta de entrada até a porta de saída. Ainda neste teste, o envio e recebimento de ICMP Request e Response serão usados, para que se possa ser melhor ilustrado, e ainda certificar que a medição do sniffer está correta. Com a união destes dois testes poderá ser verificado se acontece um aumento no retardo do encaminhamento. Estes testes serão realizados com a funcionalidade ligada e desligada no switch. Para verificar se há impacto na disponibilidade, os recursos do switch de CPU e memória são testados com a funcionalidade em execução, recebendo e enviando um tráfego alto, de aproximadamente 100 Mbps, que é criado usando um gerador de tráfego, dentro de uma estação cliente. Também é usado um gerador de pacotes para simular as situações de diversas mensagens DHCP sendo geradas simultaneamente. Estas mensagens são de clientes enviando diversos DHCP DISCOVER e DHCP REQUEST, e o servidor respondendo DHCP OFFER e DHCP ACK.
Procedimento	Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No sniffer: Acompanhar todo fluxo de mensagens DHCP; Na estação cliente: Iniciar o comando ping com destino o IP do servidor DHCP (192.168.1.1); Na estação cliente: Verificar o funcionamento do comando ping; Na estação cliente: Coletar o tempo de retardo inserido pelo switch; No switch: Verificar a utilização de CPU e memória do switch; Na estação cliente: Iniciar a geração de tráfego; Nas estações geradoras: Iniciar a geração de tráfego e de mensagens DHCP; Na estação cliente: Verificar o funcionamento do comando ping; Na estação cliente: Coletar o tempo de retardo inserido pelo switch; No switch: Verificar a utilização de CPU e memória do switch.
Comportamento Esperado	Não deve haver impacto pelo uso da funcionalidade GAEIP

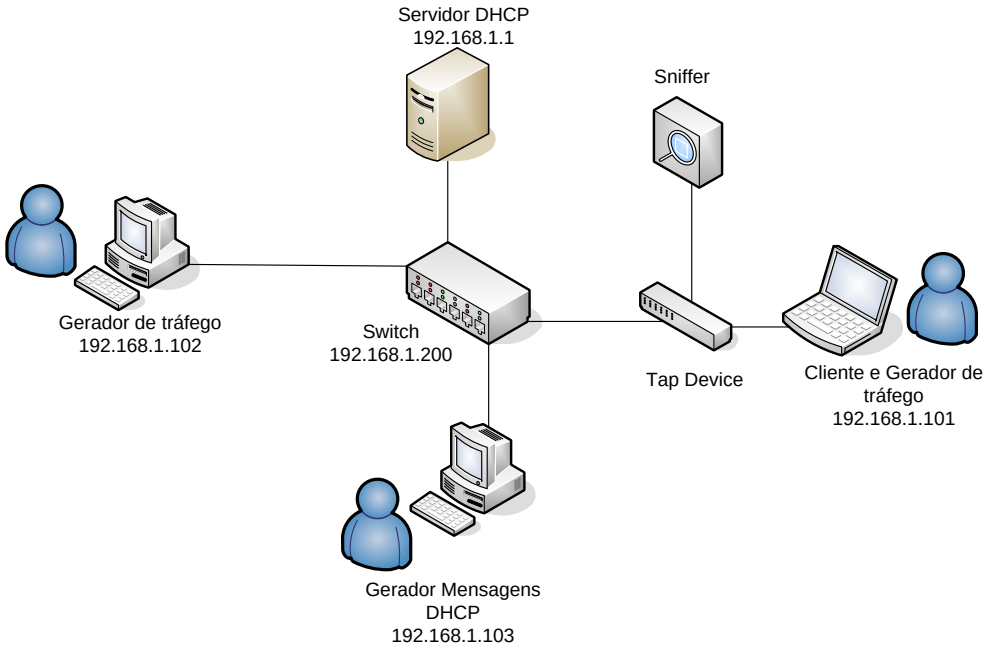


Figura 6.5: Topologia do Cenário 1 – Teste de Carga

Fonte: Elaborado pelo autor (2011)

Quadro 6.12: Teste impacto na funcionalidade de lista de controle de acesso.

Nome do Teste	Impacto na funcionalidade de lista de controle de acesso
Descrição	A funcionalidade de access-list pode ser impedida de funcionar se o controle de acesso baseado em mensagens DHCP for ativado.
Procedimento	No *switch* : Configurar uma access-list negando o tráfego de origem 192.168.1.0/24, destino 192.168.1.1, protocolo ICMP; Conectar o *sniffer* para captura do tráfego; No *switch* : Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; Na estação cliente: Iniciar o comando ping com destino o IP do servidor DHCP; No *sniffer* : Acompanhar todo fluxo de mensagens DHCP; No *switch* : Verificar o funcionamento do comando ping do switch para a estação; Na estação cliente: Verificar o funcionamento do comando ping da estação para o servidor DHCP.
Comportamento Esperado	Funcionamento normal de ambas as funcionalidades.

6.2.2 Cenário B

O cenário B traz dois testes sendo o primeiro da conexão de um novo cliente, conforme quadro 6.13 e um segundo teste para verificar a resistência contra servidor DHCP não autorizado, no quadro 6.14.

Quadro 6.13: Teste conexão de um novo cliente – Cenário B.

Nome do Teste	Conexão de um novo cliente
Descrição	Testar a necessidade de realizar o controle nas portas de *uplink* quando todos os *switches* suportam GAEIP
Procedimento	Iniciar o comando ping com origem o IP da estação cliente e destino o IP do switch que a estação cliente está conectada; Conectar o cabo entre a estação e o *switch* B; Ligar a estação de trabalho; Iniciar o comando ping com origem o IP da estação cliente B e destino o IP do *switch* A que o servidor DHCP está conectado; Certificar que a estação está configurada para pegar IP de um servidor DHCP; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Conectar o tap e o *sniffer* na porta de *uplink*; Configurar o IP 192.168.1.101 na estação cliente; Verificar o funcionamento do comando ping.
Comportamento Esperado	Todo o controle será feito na porta de acesso do cliente conectado no switch B, conforme figura 6.2. Se o cliente B não estiver usando um IP dinâmico não será observado nenhum pacote na porta de uplink entre os switches A e B. A estação cliente B ao conectar e pegar um IP do DHCP terá seu tráfego liberado. Para comprovar serão enviados ICMP Request e consequentemente os ICMP Response serão recebidos pela estação. A partir do momento que o cliente alterar seu endereço IP para fixo, não receberá mais os pacotes ICMP Response. Simultaneamente o tráfego na porta de *uplink* será capturado para constatar que nenhum pacote está sendo encaminhado.

Quadro 6.14: Teste resistência contra servidor DHCP não autorizado – Cenário B.

Nome do Teste	Resistência contra servidor DHCP não autorizado
Descrição	Testar o comportamento de uma topologia onde o servidor DHCP está conectado em um switch que suporta GAEIP
Procedimento	No *switch*: Iniciar o comando ping com destino o IP da estação, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; No *switch*: Verificar o funcionamento do comando ping; No servidor DHCP não autorizado: Iniciar a geração de pacotes DHCP Ack da estação geradora de mensagens DHCP, com destino a primeira estação cliente, oferecendo os endereços IP 192.168.1.150 e 192.168.1.151; No *sniffer*: Acompanhar o fluxo de mensagens DHCP; No *switch*: Verificar a operação da funcionalidade; Na estação cliente: Alterar o IP da estação para 192.168.1.151; Verificar se há conectividade entre a estação e a rede, usando o IP fixo.
Comportamento Esperado	Como todos os *switches* suportam GAEIP, o servidor DHCP não autorizado não causará nenhum impacto ao ambiente de rede.

6.2.3 Cenário C

Todos os testes citados deverão ser realizados novamente, pois agora o cliente está conectado em um *switch* que não suporta GAEIP, conforme diagrama do item 6.1.3. Agora o comportamento da funcionalidade será observado na porta de *uplink*, que faz a conexão entre os *switches*.

- Conexão de um novo cliente em *switch* sem GAEIP (quadro 6.15);
- Alteração do IP de dinâmico para fixo (alterando ou mantendo o mesmo IP) (quadro 6.16);
- Reinicialização da porta (desconexão e conexão) do cliente (quadro 6.17);
- Reinicialização da porta de conexão entre *switches* (quadro 6.18);
- Reinicialização do *switch* com GAEIP (quadro 6.19);
- Reinicialização do *switch* sem GAEIP (quadro 6.20);
- Impacto em outros protocolos (quadro 6.21);
- Resistência contra servidor DHCP não autorizado para clientes no *switch* A (quadro 6.22);
- Resistência contra servidor DHCP não autorizado para clientes no *switch* B (quadro 6.23)

Quadro 6.15: Teste conexão de um cliente no *switch* sem GAEIP.

Nome do Teste	Conexão de um cliente no switch sem GAEIP
Descrição	Nem todos os switches de uma rede local podem suportar o controle de configuração de IP baseado em mensagens DHCP. Assim este teste permite visualizar o funcionamento da conexão de um cliente em um *switch* que não suporte esta funcionalidade. O comportamento operacional é verificado na porta de *uplink*, que conecta ambos switches.
Procedimento	No *switch* A: Iniciar o comando ping com destino o IP da estação B, que será provavelmente o primeiro IP do DHCP (192.168.1.100); Na estação cliente: Iniciar o comando ping para o IP do switch B (192.168.1.201); Na estação cliente: Configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação cliente B e o *switch* B; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; Na estação cliente: Verificar o funcionamento do comando ping.
Comportamento Esperado	Com o uso do IP dinâmico, o tráfego é liberado na porta de *uplink* para a estação cliente B. Esta verificação de conectividade é realizada com o protocolo ICMP. Usando o comando ping são enviados ICMP Requests para o servidor DHCP, e com a resposta do servidor é possível ver que o tráfego está autorizado na porta de *uplink*.

Quadro 6.16: Teste alteração da configuração do IP de dinâmico para fixo – Cenário C.

Nome do Teste	Alteração da configuração do IP de dinâmico para fixo
Descrição	Mesmo estando em um switch que não suporte a configuração, quando o endereço IP é alterado de dinâmico para fixo, a funcionalidade deve bloquear somente o tráfego desta estação para o resto da rede. Como esta estação está conectada em um switch que não suporta a funcionalidade, somente o tráfego local deste switch funcionará para esta estação cliente.
Procedimento	Iniciar o comando ping com origem o IP da estação cliente A e destino o IP do switch B (192.168.1.201); Iniciar o comando ping da estação cliente B para o IP do switch B sem GAEIP (192.168.1.201); Certificar que a estação está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação cliente B e o switch B; Ligar a estação cliente B; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping. Alterar o endereço IP da estação cliente B para 192.168.1.131; Verificar o funcionamento do comando ping.
Comportamento Esperado	A estação cliente ao usar o IP dinâmico envia e recebe tráfego de toda a rede. No momento que o endereço IP é alterado para fixo, os quadros desta estação começam a ser bloqueados pela funcionalidade na porta de uplink. O tráfego interno ao switch que não suporta a funcionalidade continua funcionando. Outros tráfegos continuam funcionando pela porta de uplink.

Quadro 6.17: Teste reinicialização da porta (desconexão e conexão) do cliente.

Nome do Teste	Reinicialização da porta (desconexão e conexão) do cliente
Descrição	Teste de acesso do cliente que está conectado no switch B, que não suporta a funcionalidade, na desconexão e conexão do cabo de rede.
Procedimento	Iniciar o comando ping com origem o IP da estação cliente A com a funcionalidade e destino o IP da estação B; Iniciar o comando ping da estação cliente B para o IP do switch B (192.168.1.201); Certificar que a estação está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Desconectar o cabo entre a estação cliente e o switch que não suporta a funcionalidade; Verificar se a permissão de acesso ainda existe no uplink; Conectar o cabo que foi desconectado anteriormente; Verificar o funcionamento do comando ping .
Comportamento Esperado	Após a conexão o tráfego é novamente liberado, não havendo qualquer impacto para o cliente.

Quadro 6.18: Teste reinicialização da porta de *uplink.*

Nome do Teste	Reinicialização da porta de uplink
Descrição	A reinicialização da porta de *uplink,* que é usada para conectar os *switches* que suportam ou não a funcionalidade, pode ocasionar a paralização do funcionamento do tráfego da estação cliente, mesmo que esteja usando um endereço IP atribuído pelo servidor DHCP.
Procedimento	Iniciar o comando ping com origem o IP do *switch* A e destino o IP da estação cliente B; Certificar que a estação cliente B está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação cliente B e o switch B; Ligar a estação cliente B; Iniciar o comando ping da estação cliente B para o IP do switch B (192.168.1.201); Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Desconectar o cabo de uplink entre os switches; Verificar o funcionamento do comando ping; Conectar o cabo de uplink; Verificar o funcionamento do comando ping; Verificar a permissão de acesso da funcionalidade; Desconectar e conectar o cabo da estação cliente; Verificar o funcionamento do comando ping; Reiniciar o switch que suporta a funcionalidade; Verificar o funcionamento do comando ping.
Comportamento Esperado	Após a reiniciação do switch todas as permissões de encaminhamento de datagramas IP devem ser mantidas. Com isto as estações devem continuar funcionando.

Quadro 6.19: Teste reinicialização do *switch* com GAEIP.

Nome do Teste	Reinicialização do *switch* com GAEIP.
Descrição	Com o ambiente em operação, o *switch* que suporta o GAEIP é reiniciado para verificar o funcionamento do gerenciamento da atribuição dos endereços IP.
Procedimento	Iniciar o comando ping com origem o IP da estação cliente B e destino o IP do *switch* A (192.168.1.200); Iniciar o comando ping com origem o IP da estação cliente B para o IP do *switch* B (192.168.1.201); Certificar que a estação está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação e o *switch;* Ligar a estação de trabalho; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Reinicializar o *switch* que o servidor DHCP está conectado; Verificar o funcionamento do comando ping.
Comportamento Esperado	Após a reinicialização do switch A, todas as estações que estão conectadas devem continuar funcionando.

Quadro 6.20: Teste reinicialização do *switch* sem GAEIP.

Nome do Teste	Reinicialização do *switch* sem GAEIP
Descrição	Com o ambiente em operação, o *switch* que não suporta o GAEIP é reiniciado para verificar o funcionamento do controle de acesso nesta situação.
Procedimento	Iniciar o comando ping com origem o IP da estação cliente A e destino o IP do *switch* B (192.168.1.201); Iniciar o comando ping com origem o IP da estação cliente B e destino o IP do *switch* B (192.168.1.201); Iniciar o comando ping da estação cliente A para a estação cliente B; Certificar que a estação está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação e o *switch* ; Ligar a estação de trabalho; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Reinicializar o *switch* que a estação cliente está conectada; Verificar o funcionamento do comando ping.
Comportamento Esperado	Após a reinicialização do *switch* , todas as estações que estão conectadas devem solicitar novamente os respectivos endereços IP já em uso com o DHCP Request. Após o fluxo de mensagens DHCP o tráfego é liberado na porta de *uplink* do *switch* que tem a funcionalidade configurada.

Quadro 6.21: Teste impacto em outros protocolos.

Nome do Teste	Impacto em outros protocolos
Descrição	No caso do spanning-tree, a preocupação é com o não encaminhamento de BPDUs nas portas de *uplink*, uma vez que nesta conexão o tráfego é permitido por endereço de origem, que por sua vez só é liberado com a condição deste endereço ser atribuído por um servidor DHCP. Se as BPDUs não forem encaminhadas entre *switches* o qualquer outro tráfego for liberado um loop na camada 2 ocasionará a indisponibilidade do ambiente de rede local.
Procedimento	Iniciar o comando ping com origem o IP da estação cliente B e destino o IP do switch A (192.168.1.200); Certificar que a estação está configurada para pegar IP de um servidor DHCP; Conectar o cabo entre a estação e o *switch*; Ligar a estação de trabalho; Acompanhar todo fluxo de mensagens DHCP; Verificar o funcionamento do comando ping; Conectar um segundo cabo de *uplink* em outra porta que também tenha a funcionalidade configurada; Verificar o comportamento do protocolo Spanning Tree; Verificar o funcionamento do comando ping.
Comportamento Esperado	Como a funcionalidade permite a passagem de quadros com o endereço de multicast 01:80:C2:00:00:00 (endereço de multicast para o STP), não haverá nenhum impacto no protocolo STP.

Quadro 6.22: Teste resistência contra servidor DHCP não autorizado para clientes conectados no *switch* A.

Nome do Teste	Resistência contra servidor DHCP não autorizado para clientes conectados no *switch* B
Descrição	Testar o comportamento de uma topologia onde o servidor DHCP está conectado em um switch com GAEIP, o servidor DHCP não autorizado está conectado em um *switch* que não suporta GAEIP e os clientes estão em um *switch* que suporta GAEIP.
Procedimento	Na estação cliente B: Iniciar o comando ping com destino o IP da estação cliente A; Na estação cliente: configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; No *switch*: Verificar o funcionamento do comando ping; No servidor DHCP não autorizado: Iniciar a geração de pacotes DHCP Ack da estação geradora de mensagens DHCP, com destino a estação cliente A, oferecendo os endereços IP 192.168.1.150 e 192.168.1.151; No *sniffer*: Acompanhar o fluxo de mensagens DHCP; No *switch*: Verificar a operação da funcionalidade; Na estação cliente A: Alterar o IP da estação para 192.168.1.151; Verificar se há conectividade entre a estação cliente A e a rede;
Comportamento Esperado	Como o servidor DHCP autorizado está conectado no switch que suporta GAEIP, a atribuição falsa feita pelo servidor DHCP não oficial não funcionará. Assim a estação cliente A, ao alterar seu IP para fixo, perderá acesso à rede.

Quadro 6.23: Teste resistência contra servidor DHCP não autorizado para clientes conectados no *switch* B.

Nome do Teste	Resistência contra servidor DHCP não autorizado para clientes conectados no *switch* B
Descrição	Testar o comportamento de uma topologia onde o servidor DHCP está conectado em um switch com GAEIP, o servidor DHCP não autorizado está conectado em um *switch* que não suporta GAEIP e os clientes estão em um *switch* que suporta GAEIP.
Procedimento	Na estação cliente A: Iniciar o comando ping com destino o IP da estação cliente B; Na estação cliente: configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; Na estação cliente B: Iniciar o comando ping com destino o IP do switch B (192.168.1.201); No servidor DHCP não autorizado: Iniciar a geração de pacotes DHCP Ack da estação geradora de mensagens DHCP, com destino a estação cliente A, oferecendo os endereços IP 192.168.1.150 e 192.168.1.151; No *sniffer*: Acompanhar o fluxo de mensagens DHCP; No *switch*: Verificar a operação da funcionalidade; Na estação cliente B: Alterar o IP da estação para 192.168.1.151; Verificar se há conectividade entre a estação cliente B e a rede;
Comportamento Esperado	Como a estação B está conectada no switch B que não suporta GAEIP, esta poderá usar o IP 192.168.1.151. Mas este tráfego ficará restrito ao switch B, pois no switch A, o GAEIP não vai identificar a atribuição do endereço IP. Se houver mais uma estação cliente no switch B, ela poderá se cominucar com a estação cliente B pelo endereço IP fixo 192.168.1.151.

6.2.4 Cenário D

O cenário D mostra dois testes de resistência contra servidor DHCP não autorizado, nos quadros 6.24 e 6.25, sendo respectivamente para clientes conectados no switch A e clientes conectados no switch B.

Quadro 6.24: Teste resistência contra servidor DHCP não autorizado para clientes conectados no *switch* A.

Nome do Teste	Resistência contra servidor DHCP não autorizado para clientes conectados no *switch* A
Descrição	Testar o comportamento de uma topologia onde os servidores DHCP autorizado e não autorizado estão conectados em um switch sem GAEIP, e os clientes estão no mesmo switch. Também existe cliente conectado a um switch com GAEIP.
Procedimento	Na estação cliente B: Iniciar o comando ping com destino o IP da estação cliente A; Na estação cliente: configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; No *switch*: Verificar o funcionamento do comando ping; No servidor DHCP não autorizado: Iniciar a geração de pacotes DHCP Ack da estação geradora de mensagens DHCP, com destino a estação cliente A, oferecendo os endereços IP 192.168.1.150 e 192.168.1.151; No *sniffer*: Acompanhar o fluxo de mensagens DHCP; No *switch*: Verificar a operação da funcionalidade; Na estação cliente A: Alterar o IP da estação para 192.168.1.151; Verificar se há conectividade entre a estação cliente A e a rede;
Comportamento Esperado	Como os servidores e a estação cliente A estão conectados no *switch* A, sem GAEIP, todo e qualquer endereço IP usado pela estação A terá seu tráfego liberado para alcançar, por exemplo, a estação cliente B que ela está conectada no *switch* com GAEIP.

Quadro 6.25: Teste resistência contra servidor DHCP não autorizado para clientes conectados no *switch* B.

Nome do Teste	Resistência contra servidor DHCP não autorizado para clientes conectados no *switch* B
Descrição	Testar o comportamento de uma topologia onde os servidores DHCP autorizado e não autorizado estão conectados no *switch* sem GAEIP, e a estação cliente está conectada no *switch* com GAEIP.
Procedimento	Na estação cliente A: Iniciar o comando ping com destino o IP da estação cliente B; Na estação cliente: configurar a estação para usar o protocolo DHCP; Conectar o cabo entre a estação e o switch; Ligar a estação de trabalho; No *sniffer*: Acompanhar todo fluxo de mensagens DHCP; Na estação cliente B: Iniciar o comando ping com destino o IP do switch B (192.168.1.201); No servidor DHCP não autorizado: Iniciar a geração de pacotes DHCP Ack da estação geradora de mensagens DHCP, com destino a estação cliente B, oferecendo os endereços IP 192.168.1.150 e 192.168.1.151; No *sniffer*: Acompanhar o fluxo de mensagens DHCP; No *switch*: Verificar a operação da funcionalidade; Na estação cliente B: Alterar o IP da estação para 192.168.1.151; Verificar se há conectividade entre a estação cliente B e a rede;
Comportamento Esperado	Como a estação cliente B está conectada no *switch* com GAEIP, somente o endereço IP solicitado e respondido pelo servidor DHCP autorizado terá o tráfego liberado.

7 REALIZAÇÃO DOS TESTES E RESULTADOS

Neste capítulo são apresentados os ambientes dos testes e resultados apresentados, seguindo a metodologia do capítulo 5.

7.1 Equipamentos utilizados

Para os testes foram usados os seguintes equipamentos:

- *Switch* Cisco Catalyst 2950;
- *Switch* Cisco Catalyst 3750;
- *Switch* 3Com/HP 4210 versão 3.10;
- Hub Encore ESH-708;
- Tap Device NetOptics – 10/100 CU Teeny Tap;
- Laptop Acer Extensa 4420;
- Laptop Lenovo R61;
- Laptop Acer Aspire One.

7.2 Execução dos testes

Todos os testes seguiram a mesma metodologia para todos os fabricantes testados, e também para a prova de conceito.

O resultado dos testes está apresentado no quadro 7.1. Neste quadro o resultado sim indica que o comportamento esperado foi atingido e não quando o resultado esperado não foi atingido.

Quadro 7.1: Comparativo dos testes realizados.

	Teste	M1	M2	Address Guard
Cenário A	Conexão novo cliente DHCP	Sim	Sim	Sim
	Conexão de um novo cliente utilizando IP fixo	Sim	Sim	Sim
	Alteração do IP de dinâmico para fixo	Sim	Sim	Sim
	Alteração do IP de dinamico para fixo com filtragem da mensagem DHCP Release	Sim	Sim	Sim
	Renovação do aluguel do endereço IP	Sim	Sim	Sim
	Alteração do IP de dinamico para fixo com filtragem da mensagem DHCP Release e com o tempo de aluguel expirado	Sim	Sim	Sim
	Desconexão e reconexão do ponto de rede à mesma máquina	Sim	Sim	Sim
	Substituição da estação por outra na mesma porta	Não	Sim	Sim
	Reinicialização do cliente	Sim	Sim	Sim
	Reinicialização do switch	Sim	Sim	Sim
	Teste de Carga	Sim	Sim	Sim
	Teste de Impacto em outra Funcionalidade	Sim	Sim	Sim
Cenário B	Conexão de um novo cliente	Sim	Sim	Sim
	Resistência contra servidor DHCP não autorizado	Sim	Sim	Sim
Cenário C	conexão de um novo cliente no switch sem o address guard	Sim	Sim	Sim
	alteração do IP de dinâmico para fixo	Sim	Sim	Sim
	reinicialização da porta	Sim	Sim	Sim
	reinicialização da porta de uplink	Sim	Sim	Sim
	reinicialização do switch sem GAEIP	Sim	Sim	Sim
	reinicialização do switch com GAEIP	Não	Não	Sim
	Impacto em outro protocolo	Sim	Sim	Sim
	Resistência contra servidor DHCP não autorizado para clientes conectados no switch A	Sim	Sim	Sim
	Resistência contra servidor DHCP não autorizado para clientes conectados no switch B	Não	Não	Não
Cenário D	Resistência contra servidor DHCP não autorizado para clientes conectados no switch A	Não	Não	Não
	Resistência contra servidor DHCP não autorizado para clientes conectados no switch B	Não	Não	Sim

Legenda	
Sim	Resultado do teste atendeu ao esperado
Não	Resultado do teste não atendeu ao esperado

7.3 Resultados relevantes

São apresentados e detalhados os resultados que se destacaram por não atender ao objetivo de garantir o gerenciamento da atribuição dos endereços IP baseados nas mensagens DHCP, e também os resultados que apesar de alcançar o objetivo se destacam pelo funcionamento.

7.3.1 Substituição da estação por outra na mesma porta

No teste de substituição da estação por outra na mesma porta, a implementação de mercado M1 liberou o tráfego normalmente após a obtenção do endereço IP de um servidor DHCP pela estação 1. Em seguida com a desconexão da estação 1 e conexão da estação 2, com o mesmo endereço IP da estação 1 configurado previamente, o tráfego foi encaminhado, o que não era esperado.

Com o Address Guard e a implementação de mercado M2, a estação 2 não teve o tráfego encaminhado.

7.3.2 Reinicialização do *switch* com GAEIP

No teste de reinicialização do *switch* com GAEIP as implementações de mercado M1 e M2, ao terem o *switch* reiniciado, não mantiveram a tabela de controle do DHCP *snooping* que impediu o encaminhamento do tráfego após o *switch* voltar ao funcionamento.

No teste com o Address Guard não ocorreu a interrupção do tráfego entre as estações e a rede, após a reinicialização.

7.3.3 Resistência contra servidor DHCP não autorizado

O teste de resistência contra servidor DHCP não autorizado foi feito nos cenários B, C e D, conforme capítulo 6. Esta repetição foi feita para analisar no detalhe a eficácia das implementações de mercado e do Address Guard em algumas possíveis topologias de rede. Sendo este um problema importante a ser avaliado.

Nos testes do cenário C para clientes conectados no *switch* B e do cenário D para clientes conectados no *switch* A, todas as implementações testadas não obtiveram sucesso no controle porque as estações e o servidor DHCP não autorizado estão conectados no *switch* sem GAEIP. Desta forma estas estações clientes puderam usar qualquer endereço IP.

No teste do cenário C para clientes conectados no *switch* A, todas as implementações de mercado e o Address Guard obtiveram sucesso no controle, pois o servidor DHCP está conectado no *switch* com GAEIP e o servidor DHCP não autorizado está conectado no *switch* sem GAEIP. Como a porta de *uplink* não tem autorização para encaminhar as mensagens DHCP OFFER e DHCP ACK, os endereços não conseguem ser atribuídos pelo GAEIP executado nas implementações de mercado e no Address Guard. Para as portas não confiáveis, a porta UDP 68 (usada por servidores DHCP) é bloqueada como porta de origem, permitindo que somente a porta UDP 67 (usada por clientes DHCP).

Já no teste do cenário D para clientes conectados no *switch* B, o servidor envia uma mensagem forjada DHCP ACK à estação cliente, sem esta ter solicitado um endereço IP. Neste cenário o servidor DHCP não autorizado está conectado em um *switch* sem GAEIP e todo o controle é feito na porta de *uplink* do outro *switch* que suporta GAEIP. Nesse momento as implementações de mercado M1 e M2 aceitaram esta resposta como de um servidor autorizado ou válido habilitando a porta do *switch* para receber tráfego com este endereço IP.

A prova de conceito Address Guard não cadastrou este endereço IP como válido para uma estação ou porta, porque não detectou a mensagem DHCP REQUEST da estação solicitando ao servidor DHCP.

8 AVALIAÇÃO E COMPARAÇÃO DOS RESULTADOS

Neste capítulo são avaliados e comparados os resultados dos testes realizados nas implementações de mercado M1 e M2, e no Address Guard.

8.1 Testes do cenário A

No cenário A, somente um teste apresentou uma não conformidade: a substituição de uma estação por outra na mesma porta. Neste teste a implementação de mercado M1 alcançou parcialmente o controle necessário, pois quando uma nova estação já com o endereço IP, obtido pela estação anterior, configurado de forma manual é conectada ao *switch* tem seu tráfego encaminhado normalmente, o que não era esperado, pois o *switch* deveria impedir o tráfego desta estação nesta porta. No teste com a implementação de mercado M2 e com o Address Guard, o filtro é feito pelo endereço IP e pelo endereço MAC, que assim não permitiu o funcionamento da nova estação cliente.

Todos os outros testes apresentaram resultado satisfatório com o comportamento similar ao esperado, relacionados no capítulo 6. Somente as estações que obtiveram o endereço IP do servidor DHCP, tiveram acesso aos recursos da rede.

No cenário A que contempla apenas um *switch*, sem conexões de *uplink* e outros elementos de rede, os resultados foram satisfatórios atendendo ao GAEIP (gerenciamento de atribuição de endereços IP).

8.2 Testes do cenário B

Os resultados obtidos no cenário B, mostram que não é necessário aplicar o GAEIP em portas de *uplink* entre dois *switches* com GAEIP ativo em todas as portas de acesso. O uso do GAEIP em portas de *uplink* pode servir como um mecanismo adicional para

garantir o gerenciamento da atribuição dos endereços IP, que será usado em caso de falha deste mecanismo já em execução em outros *switches*.

No teste de resistência contra servidor DHCP não autorizado, o controle é realizado pois o servidor DHCP não autorizado está conectado no *switch* que suporta GAEIP. Assim as mensagens de servidor DHCP são filtradas na porta de acesso, impedindo que este envie mensagens que podem ser usadas pela funcionalidade GAEIP.

8.3 Testes do cenário C

Apenas um teste deste cenário não apresentou conformidade com o resultado esperado nas implementações de mercado M1 e M2: a reinicialização do *switch* com GAEIP. Após a reiniciação do *switch*, suas tabelas de controle do GAEIP foram perdidas, fazendo com que todo o tráfego das estações que estavam conectadas no *switch* sem GAEIP fossem bloqueados

Na implementação Address Guard a tabela associada às portas de *uplink* é mantida em memória persistente.

Os testes de resistência contra servidor DHCP não autorizado mostraram que, conforme exposto no capítulo 4.3.6, os servidores DHCP devem ser conectados sempre em *switches* com GAEIP. Os resultados dos testes onde esta condição foi atendida apresentaram resposta satisfatória, mas quando o servidor DHCP não autorizado foi conectado a um *switch* sem GAEIP, nenhuma das implementações incluindo a prova de conceito, o resultado não foi satisfatório.

8.4 Testes do cenário D

No cenário D, o servidor DHCP estava conectado em um *switch* que não suportava o Address Guard, que por sua vez estava conectado a outro *switch* com o Address Guard

configurado. Ainda neste *switch* do servidor DHCP e sem o Address Guard, uma outra estação foi conectada simulando um DHCP não autorizado que enviou para diversos endereços MAC diversos endereços IP da mesma rede que estava em produção.

Nas implementações de mercado M1 e M2, os endereços IP atribuídos de forma ilegal foram cadastrados nos filtros aplicados nas portas dos clientes, permitindo que estas estações pudessem alterar seus endereços IP e continuar tendo acesso a rede.

No Address Guard isto não aconteceu porque como a estação cliente não solicitou o endereço IP, este não foi permitido para o tráfego.

Esta diferença de comportamento deve-se ao fato do Address Guard usar as mensagens DHCP ACK e REQUEST para inserir o endereço IP no filtro aplicado a porta, porque um endereço só pode ser recebido em uma estação cliente se o mesmo tiver sido solicitado a um servidor DHCP. Já nas outras implementações é usada somente a mensagem DHCP ACK.

8.5 Vantagens e desvantagens das implementações

Os assuntos relacionados à precisão do controle, disponibilidade em situação de problema, armazenamento e impacto em outros protocolos, podem ser avaliados com a comparação dos resultados dos testes de todos os cenários.

Em relação à eficácia do GAEIP, a implementação de mercado M1 tem como pontos negativos a não verificação do endereço MAC e a utilização de uma única mensagem DHCP para fazer a verificação se uma estação usa ou não endereço IP fornecido por um servidor DHCP. A implementação de mercado M2 faz a verificação do MAC, mas ainda usa uma única mensagem DHCP. Já o Address Guard verifica também o MAC e usa além da mensagem DHCP ACK, também a DHCP REQUEST, garantindo que uma estação só pode receber um IP se a mesma fez esta solicitação.

Considerando um problema de uma reiniciação do *switch* que suporte a funcionalidade, sendo o cenário 3 como no capítulo 6.1.3, somente o Address Guard consegue manter o ambiente funcionando. As implementações de mercado M1 e M2 tem problemas de manter os estados de liberação de tráfego realizados antes da reiniciação.

Em relação ao armazenamento, o Address Guard necessita que a tabela do controle GAEIP da porta de *uplink* seja armazenada em memória persistente.

Nenhuma das implementações apresentaram impacto no protocolo Spanning-tree e na filtragem de pacotes, que foram usados como exemplo para verificar se haveria algum problema em outros protocolos e funcionalidades.

O quadro 8.1 compara as vantagens e desvantagens das implementações de mercado M1, M2, e Address Guard. As vantagens são indicadas com uma seta para cima e as desvantagens com uma seta para baixo.

Quadro 8.1: Comparativo das implementações.

Item Avaliado	M1	M2	Address Guard
Precisão do Controle	↓	↓	↑
Disponibilidade após reiniciação de switch	↓	↓	↑
Não necessidade de memória persistente	↑	↑	↓
Não impacto em outros protocolos	↑	↑	↑

Embora o Address Guard tenha a desvantagem de depender de uma memória persistente, esta desvantagem é causada para mitigar um problema existente nas implementações de mercado M1 e M2. Na comparação as vantagens do Address Guard superam as implementações de mercado M1e M2. O tamanho das tabelas do Address Guard e da implementação de mercado M2 é o mesmo, e maiores que o

tamanho da tabela da implementação de mercado M1. A principal diferença é que no Address Guard o armazenamento deve ser feito em memória persistente.

A quantidade máxima de entradas na tabela GAEIP é igual a quantidade de pontos existentes da sub-rede (levando em consideração *switches* e *hubs*), incluindo neste cálculo *switches* virtuais de sistemas virtualizados.

A figura 8.1 ilustra a comparação das três implementações avaliadas nos critérios de eficácia do controle de GAEIP e no tamanho da tabela de controle para GAEIP. A implementação M1 tem um tamanho menor porque não armazena o endereço MAC. Já as implementações M2 e Address Guard tem o mesmo pois armazenam as mesmas informações. A diferença está no tipo de armazenamento, que na implementação M2 é feito em memória não persistente e no Address Guard em memória persistente, garantindo para o Address Guard uma maior eficácia no controle.

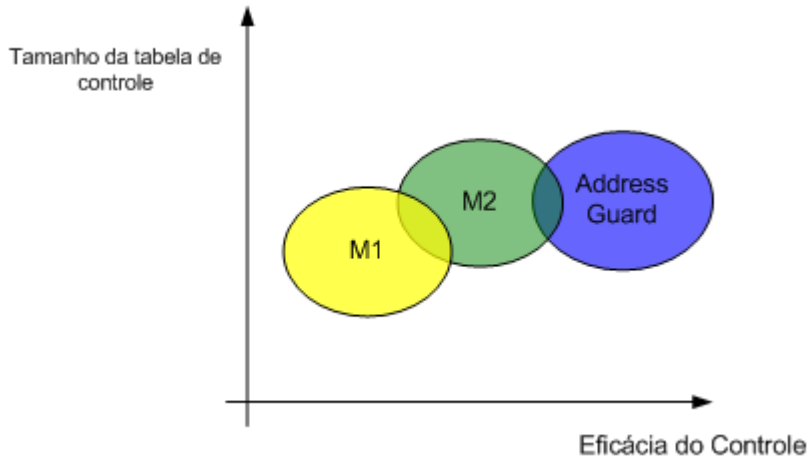


Figura 8.1: Comparativo Implementações

Fonte: Elaborado pelo autor (2011)

9 CONCLUSÃO

O gerenciamento de atribuição de endereços IP (GAEIP) baseado na monitoração das mensagens DHCP é uma das alternativas para se manter a disponibilidade dos ambientes de rede de acesso de usuários , pois evita o conflito de IP, além de oferecer rastreabilidade de endereços IP.

O objetivo deste trabalho foi de avaliar algumas implementações de GAEIP. O escopo do trabalho foram as redes locais TCP/IP, baseadas nos protocolos Ethernet e IP versão 4.

Foram selecionadas duas implementações de mercado para avaliação do GAEIP através da monitoração das mensagens DHCP. Embora estas implementações usem a junção de duas funcionalidades para suportar o GAEIP (DHCP *snooping* e IP *source guard*), este resultado é alcançado com algumas restrições de implementação e do método usado. Como não existe uma funcionalidade especificamente para monitorar as mensagens DHCP e gerenciar os IPs atribuídos, algumas situações propositais ou não, podem trazer problemas de disponibilidade ou ainda de perda de rastreabilidade.

Para auxiliar nas analises, foi realizada uma implementação tipo prova de conceito. O Address Guard foi proposto não somente para facilitar a configuração nos *switches*, como também para testar outras alternativas de implementação do GAEIP.

As análises foram realizadas sobre 4 cenários, seguindo uma metodologia de testes.

Os resultados mostram que o GAEIP é eficaz quando todos os equipamentos de nível 2 suprtam GAEIP. Porém quando existem equipamentos de rede de nível 2 com e sem GAEIP, dependendo da topologia, da localização do servidor DHCP e da estação cliente o controle do GAEIP é limitado, possibilitando a configuração manual de

endereço IP, a inserção de servidor DHCP não autorizado entre outros problemas, infelizmente comprometendo toda a sub-rede, pois possibilita a ocorrência de conflito de IP. A implementação Address Guard através da monitoração de mais uma mensagem DHCP, mitiga o problema em uma determinada situação, mas não elimina o problema.

Os testes com as duas implementações de mercado apresentaram um problema quando o *switch* com GAEIP é renicializado. O tráfego das estações clientes, que estavam conectadas pela porta de *uplink* do *switch* com GAEIP, não foi restabelecido após o *switch* voltar ao funcionamento normal. Já com a implementação Address Guard isto não ocorreu pois mesmo com a reinicialização do *switch*, todas as informações da tabela com endereços IP e tempos de aluguel é armazenada em uma memória não volátil, que quando o *switch* volta ao funcionamento normal, estas informações são recuperadas e implementadas pelo *switch*. Com isto o tráfego das estações cliente é restabelecido após a reinicialização. Todavia este armazenamento gera uma maior necessidade de memória para armazenamento das informações.

9.1 Contribuições

O trabalho contribui com a apresentação de alguns possíveis problemas das implementações de mercado M1 e M2, sendo úteis para que administradores de rede tenham ciência que em algumas situações o gerenciamento da atribuição de endereços IP baseado na monitoração de mensagens DHCP pode não ser completamente eficaz. Outra contribuição do trabalho é a proposta de implementação que usa um método diferente, chamada Address Guard. O Address Guard mostrou que pode resolver problemas de implementação e de método apontados nas outras implementações.

9.2 Trabalhos futuros

Com base nos estudos realizados no trabalho e os resultados coletados, tem-se como sugestão de novos trabalhos:

- Adaptação dos Address Guard para redes wireless, que usam roteamento/Nat/redes internas para acesso externo. Esta situação acontece com roteadores/APs wireless, que fazem NAT para permitir o acesso de diversos clientes, usando apenas um único endereço IP. Talvez monitorando ao invés de mensagens DHCP algum outro tipo de mensagem que consiga distinguir que diversos acessos estão sendo feitos com o uso de um único endereço IP;

- Adequação do Address Guard para o IPv6, estuando o comportamento dos protocolos IPv6 e DHCPv6.

REFERÊNCIAS

BOUDJIT, S.; ADJIH, C.; MUHLETHALER, P.; LAOUITI, A. **Duplicate Address Detection and Autoconfiguration in OLSR**. Journal of Universal Computer Science [S.I.], v.13, n.1, p.4-31, 2007.

BRIK, V.; STROIK, J.; BENERJEE, S. **Debugging DHCP Performance**, Sigcom Internet Measurement Conference.Itália, out. 2004.

COMER, D. E. **Interligação em Rede com TCP/IP.** 5 ed. Rio de Janeiro: Editora Campus, 2006. 468p.

DAI, J.; CHIANG, L.; **A New Method to Detect Abnormal IP Address on DHCP**. TENCON 2007 – 2007 IEEE Region 10 Conference. Taiwan, nov. 2007.

DROMS, R.; LEMON, T. **The DHCP Handbook**. 2 ed. [S.l.]:Sams, 2002. 624p.

LI, J.; MIRKOVIC, J.; EHRENKRANZ, T.; WANG, M.; REIHER, P.; ZHANG, L.; **Learning the valid incoming direction of IP packets**. The International Journal of Computer and Telecommunications Networking [S.l.], v.52, n.2, p.399-417, 2008.

GROCHLA, K.; BUGA, W.; DZIERSEGA, J.; PACYNA, P.; SEMAN, A. **Autoconfiguration procedures for multiradio wireless mesh networks based on DHCP protocol.** World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium, ISBN 978-1-4244-4440-3 , 2009.

JOSHI, B.; KURAPATI, P.; RAO, D.T.V.R. **Spoofing Challenges Faced by Broadband Access Concentrators.** Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International, ISBN 978-1-4244-2912-7 , 2009.

SEIFERT, R. **The *Switch* Book: The Complete Guide to LAN *Switch*ing Technology.** 1ed. [S.l.]: Wiley, 2000. 720p.

SHAHRI, A.F.; SMITH D.G.; IRVINE J.M. **A Secure Network Access Protocol (SNAP)**. França**:** Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), ISBN 978-3-540-25338-9, 2003.

SHUE, C.A.; KALAFUT, A.J.; GUPTA, M. **A Unified Approach to Intra-Domain Security**. Computational Science and Engineering, 2009. CSE '09. International Conference, ISBN: 978-1-4244-5334-4 , 2009.

THE INTERNACIONAL ENGINEERING TASK FORCE. **Dynamic Host Configuration Protocol**, 1997 [S.l.] . Disponível em <http://www.ietf.org/rfc/rfc2131.txt>. Acesso em 17 fev. 2008.

THE INTERNACIONAL ENGINEERING TASK FORCE. **Internet Protocol**, 1981 [S.l.] . Disponível em <http://www.ietf.org/rfc/rfc791.txt>. Acesso em 05 abr.2010.

THE INTERNACIONAL ENGINEERING TASK FORCE. **A Standard for Transmission of IP Datagrams over Ethernet Networks**, 1984 [S.l.]. Disponível em < http://tools.ietf.org/html/rfc894>. Acesso em 04 abr.2010.

THE INSTITUTE OF ELECTRICAL AND ELETRONIC ENGINEERS. **Standard for Local and metropolitan area networks Media Access Control (MAC) *Bridges***, 2004 [S.l.] . Disponível em < http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=29062&arnumber=1309630&punumber=9155>. Acesso em 23 mar. 2008.

YANG,Y.; MI,J. **Design of DHCP protocol based on access control and SAKA encryption algorithm**. 2010 2nd International Conference on Computer Engineering and Technology , ISDN 978-1-4244-6347-3 , 2010.

WANG, J.; LEE, T. **Enhanced Intranet Management in a DHCP-Enabled Environment**. 26th Annual International Computer Software and Applications Conference. Estados Unidos, 2002.

ZUQUETE, A. **Protection of LAN-wide, PSP interactions: a holistic approach**. International Journal of Communication Networks and Distributed Systems Sicience [S.I.], v.3, n.4, 2009.

REFERÊNCIAS COMPLEMENTARES

CISCO SYSTEMS. **How LAN *Switches* Works**, 2007 [S.l.]. Disponível em < http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a00800a7af3.shtml>. Acesso em 16 fev. 2008.

CISCO SYSTEMS. **Configuring DHCP Snooping and IP Sourge Guard**, 2009 [S.I.]. Disponível em < http://www.cisco.com/en/US/docs/*switches*/lan/catalyst6500/catos/8.x/configuration/guide/dhcp.html>. Acesso em 04 abr. 2010.

CISCO SYSTEMS. **Cisco Network Admission Control (NAC) Executive Overview,** 2009 [S.I.]. Disponível em < http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd80557152.html>. Acesso em 10 abr 2011

HP NETWORKS. How to configure DHCP Snooping on ProCurve *switches*, 2008 [S.I.]. Disponível em <http://h40060.www4.hp.com/procurve/uk/en/pdfs/application-notes/AN-S12_ProCurve-DHCP-snooping-final.pdf>. Acesso em 06 mar. 2011.

HUCABY, D. CCNP **BCMSN Official Exam Certification Guide**. 4 ed. Indianapolis: Cisco Press. 631p.

SOARES, L.F.G.; LEMOS G.; COLCHER, S. **Redes de Computadores das LANs, MANs e WANs às Redes ATM.** 2 ed. Rio de Janeiro: Editora Campus. 740p.

APÊNDICE A

O apêndice A apresenta os resultados mais relevantes dos testes realizados:

- Desconexão e reconexão do ponto de rede à máquinas diferentes
- Resistência contra servidor DHCP não autorizado
- Reinicialização do *switch* com GAEIP

A.1 - Teste de substituição da estação por outra na mesma porta

No teste de substituição da estação por outra na mesma porta, capítulo 6.2.1 , a figura A.1 mostra o momento da desconexão do cabo da estação cliente 1, que com isto o comando ping parou de funcionar. Na implementação de mercado M1 a estação cliente 2, usando o mesmo endereço IP da estação 1 teve seu tráfego permitido na porta, ilustrado na figura A.2. A figura A.3 mostra a troca de mensagens DHCP da estação 1 quando recebeu o endereço IP do servidor DHCP. A figura A.4 traz o comportamento do DHCP *snooping* e também a situação da porta quando a estação 1 foi desconectada.

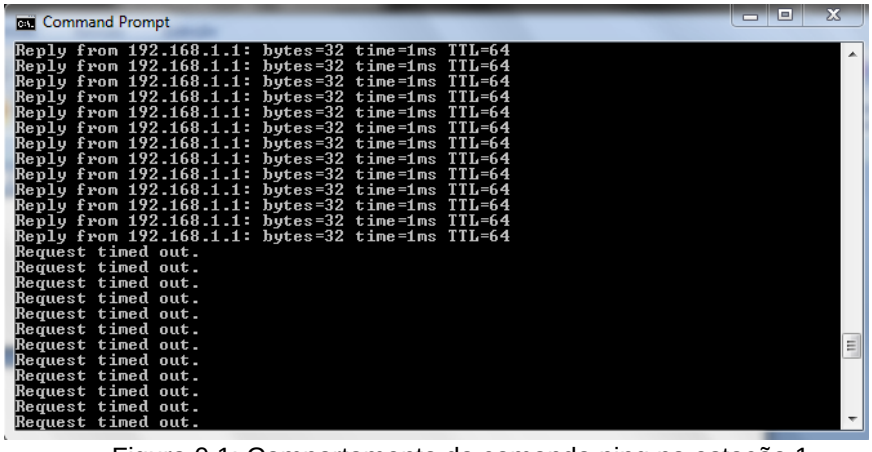


Figura 0.1: Comportamento do comando ping na estação 1

Fonte: Elaborado pelo autor (2011)

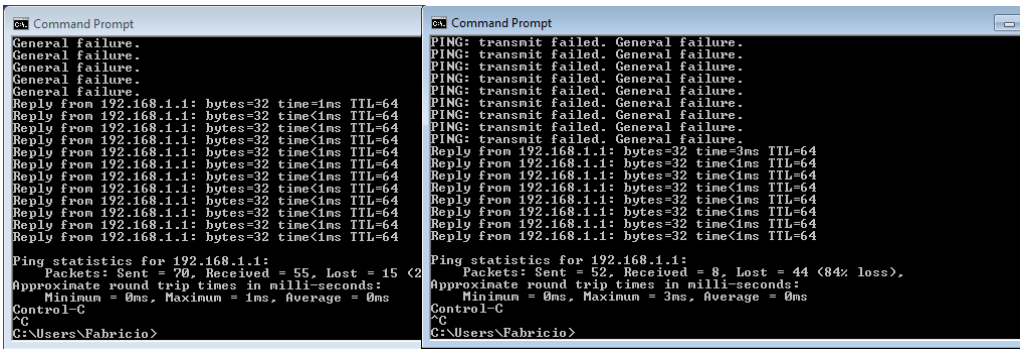
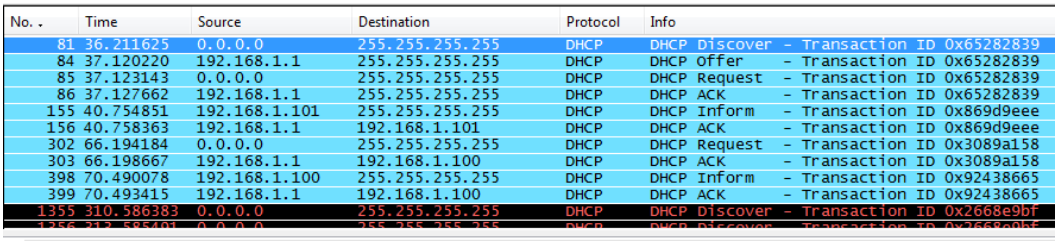


Figura 0.2: Comportamento da estação 2 usando DHCP e usando o mesmo IP fixo da estação 1

Fonte: Elaborado pelo autor (2011)



No.	Time	Source	Destination	Protocol	Info
81	36.211625	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x65282839
84	37.120220	192.168.1.1	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x65282839
85	37.123143	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x65282839
86	37.127662	192.168.1.1	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x65282839
155	40.754851	192.168.1.101	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x869d9eee
156	40.758363	192.168.1.1	192.168.1.101	DHCP	DHCP ACK - Transaction ID 0x869d9eee
302	66.194184	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3089a158
303	66.198667	192.168.1.1	192.168.1.100	DHCP	DHCP ACK - Transaction ID 0x3089a158
398	70.490078	192.168.1.100	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x92438665
399	70.493415	192.168.1.1	192.168.1.100	DHCP	DHCP ACK - Transaction ID 0x92438665
1355	310.586383	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x2668e9bf

Figura 0.3: Coleta do tráfego pelo *sniffer*

Fonte: Elaborado pelo autor (2011)

```
Teste#sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:1D:72:3B:D8:A4   192.168.1.100   172412      dhcp-snooping  5     FastEthernet1/0/3
00:1C:25:44:21:42   192.168.1.101   172769      dhcp-snooping  5     FastEthernet1/0/7
Total number of bindings: 2

Teste#sh int f1/0/3
FastEthernet1/0/3 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0015.623f.5f05 (bia 0015.623f.5f05)
  MTU 1546 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:19, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1952 packets input, 258384 bytes, 0 no buffer
     Received 707 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 395 multicast, 0 pause input
     0 input packets with dribble condition detected
     1115 packets output, 121891 bytes, 0 underruns
```

Figura 0.4: Comportamento da funcionalidade e estado da porta durante a desconexão e reconexão

Fonte: Elaborado pelo autor (2011)

A.2 – Resistência contra servidor DHCP não autorizado

No teste de resistência contra servidor DHCP não autorizado para o cenário D, capítulo 6.2.4, algumas etapas são ilustradas conforme figuras abaixo, relacionadas as implementação de mercado M1 e M2

- Comportamento do comando ping na estação cliente (figura A.5);
- Programa para gerar mensagens DHCP não autorizadas (figura A.6);
- Envio das mensagens DHCP não autorizadas (figura A.7);
- Comportamento do ping na alteração do IP para o fixo liberado pelo servidor DHCP não autorizado (figura A.8);
- Comportamento da funcionalidade GAEIP na implementação de mercado M1 (figura A.9);
- Comportamento da funcionalidade GAEIP na implementação de mercado M2 (figura A.10);
- Alteração do IP de dinâmico para fixo na estação cliente (figura A.11);
- Captura do tráfego pelo *sniffer*, no recebimento das mensagens do servidor DHCP não autorizado (figura A.12).

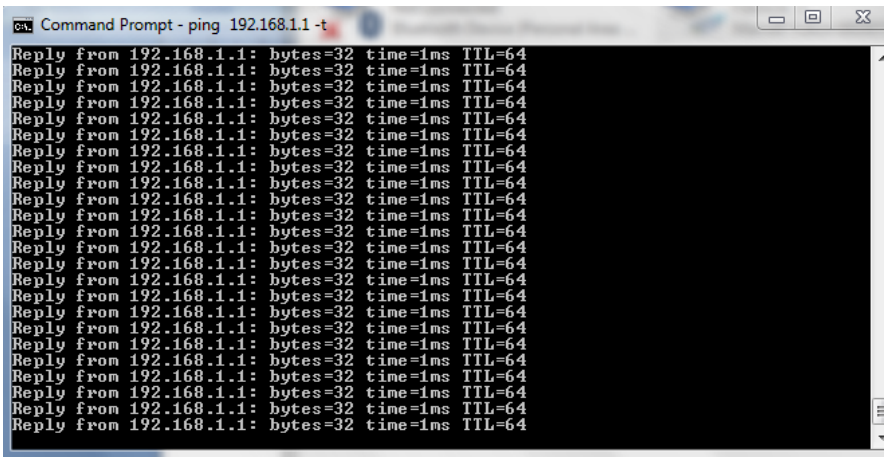


Figura 0.5: Comportamento do comando ping na estação

Fonte: Elaborado pelo autor (2011)

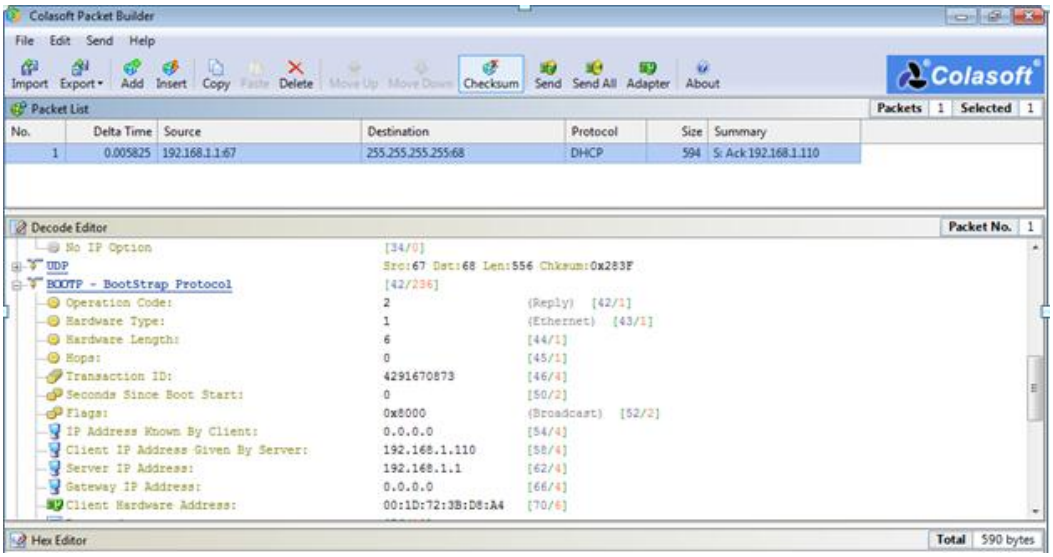


Figura 0.6: Tela da mensagem DHCP ACK gerada pelo servidor DHCP não autorizado

Fonte: Elaborado pelo autor (2011)

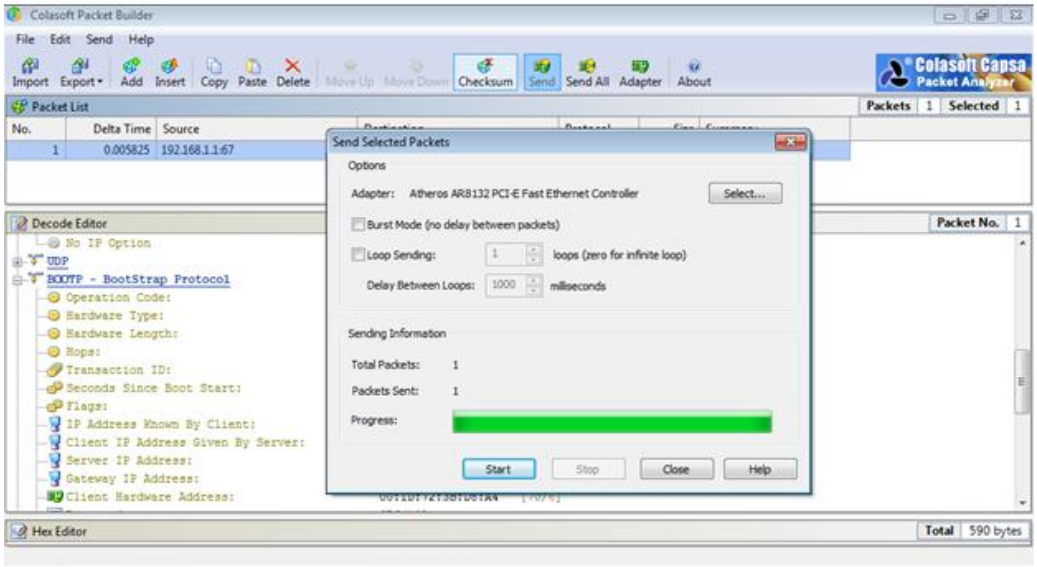


Figura 0.7: Tela com o envio das mensagens DHCP não autorizadas

Fonte: Elaborado pelo autor (2011)

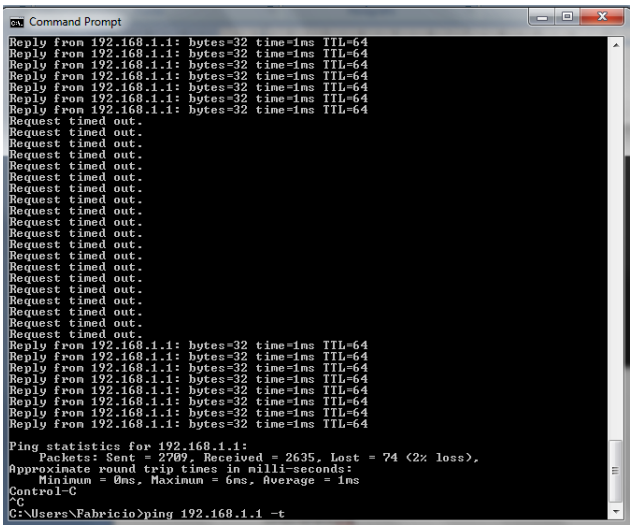


Figura 0.8: Comportamento do comando ping na alteração dos endereços IP

Fonte: Elaborado pelo autor (2011)

```
Switch#sh debugging
Ip source guard:
 Ip source guard debug packet debugging is on
Switch#
06:09:20: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.110, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add flag: 0.
06:09:20: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 0.
06:09:20: IP_SOURCE_GUARD: mac binding is removed, port: FastEthernet1/0/11, vlan: 5, mac: 001D.723B.D8A4.
06:09:20: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.100, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add fla
Switch#g: 1.
06:09:20: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 1.

Switch#
06:11:53: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.100, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add flag: 0.
06:11:53: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 0.
06:11:53: IP_SOURCE_GUARD: mac binding is removed, port: FastEthernet1/0/11, vlan: 5, mac: 001D.723B.D8A4.
06:11:53: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.110, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add fla
Switch#g: 1.
06:11:53: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 1.

Switch#
06:20:37: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.110, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add flag: 0.
06:20:37: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 0.
06:20:37: IP_SOURCE_GUARD: mac binding is removed, port: FastEthernet1/0/11, vlan: 5, mac: 001D.723B.D8A4.
06:20:37: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.100, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add fla
Switch#g: 1.
06:20:37: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 1.
Switch#sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:1D:72:3B:D8:A4   192.168.1.100   172793      dhcp-snooping  5     FastEthernet1/0/11
70:5A:B6:34:A3:48   192.168.1.101   166297      dhcp-snooping  5     FastEthernet1/0/9
Total number of bindings: 2

Switch#
06:20:54: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.100, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add flag: 0.
06:20:54: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 0.
06:20:54: IP_SOURCE_GUARD: mac binding is removed, port: FastEthernet1/0/11, vlan: 5, mac: 001D.723B.D8A4.
06:20:54: IP_SOURCE_GUARD: dhcp snooping binding update, ip: 192.168.1.110, vlan: 5, port: FastEthernet1/0/11,
mac: 001D.723B.D8A4, add fla
Switch#g: 1.
06:20:54: IP_SOURCE_GUARD: get per port/vlan ip binding, port: FastEthernet1/0/11, vlan: 5, number of bindings: 1.
Switch#sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:1D:72:3B:D8:A4   192.168.1.110   172794      dhcp-snooping  5     FastEthernet1/0/11
70:5A:B6:34:A3:48   192.168.1.101   166280      dhcp-snooping  5     FastEthernet1/0/9
```

Figura 0.9: Comportamento da funcionalidade no *switch* da implementação de mercado M1

Fonte: Elaborado pelo autor (2011)

```
*0.1866588 4210 SC/8/SC_DETAIL::- 1 -SC_DHCP_NotifyNewIp :input IpAddr:192.168.1.100 ,mac:001d-
723b-d8a4
*0.1869726 4210 DHCP-SNP/8/debug_ipcheck:- 1 -
 DEL rule: Driver return 0

*0.1869817 4210 DHCP-SNP/8/debug_ipcheck:- 1 -
 DEL rule: The bindingitem's IP = 192.168.1.100, MAC = 0000-0000-0000, VLAN = 0, PortIndex = 1, flag
= 1, ret = 0

[4210-Ethernet1/0/4]
*0.1935684 4210 DHCP-SNP/8/debug_ipcheck:- 1 -
 Do not findthe static item

*0.1935784 4210 DHCP-SNP/8/debug_ipcheck:- 1 -
 ADD rule: Driver return 0

*0.1935875 4210 DHCP-SNP/8/debug_ipcheck:- 1 -
 ADD rule: The bindingitem's IP = 192.168.1.110, MAC = 0000-0000-0000, VLAN = 0, PortIndex = 1, flag
= 1, ret = 0

*0.1936085 4210 SC/8/SC_DETAIL::- 1 -SC_DHCP_NotifyNewIp :input IpAddr:192.168.1.110 ,mac:001d-
723b-d8a4
```

Figura 0.10: Comportamento da funcionalidade no *switch* da implementação de mercado M2

Fonte: Elaborado pelo autor (2011)

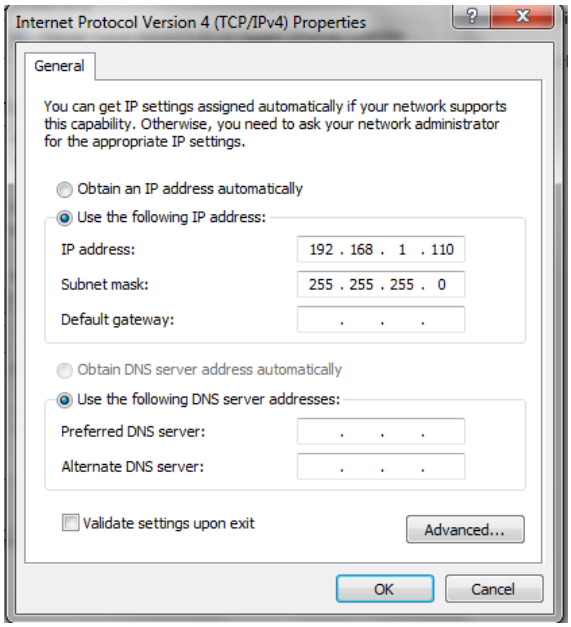


Figura 0.11: Configuração do cliente na alteração para IP fixo

Fonte: Elaborado pelo autor (2011)

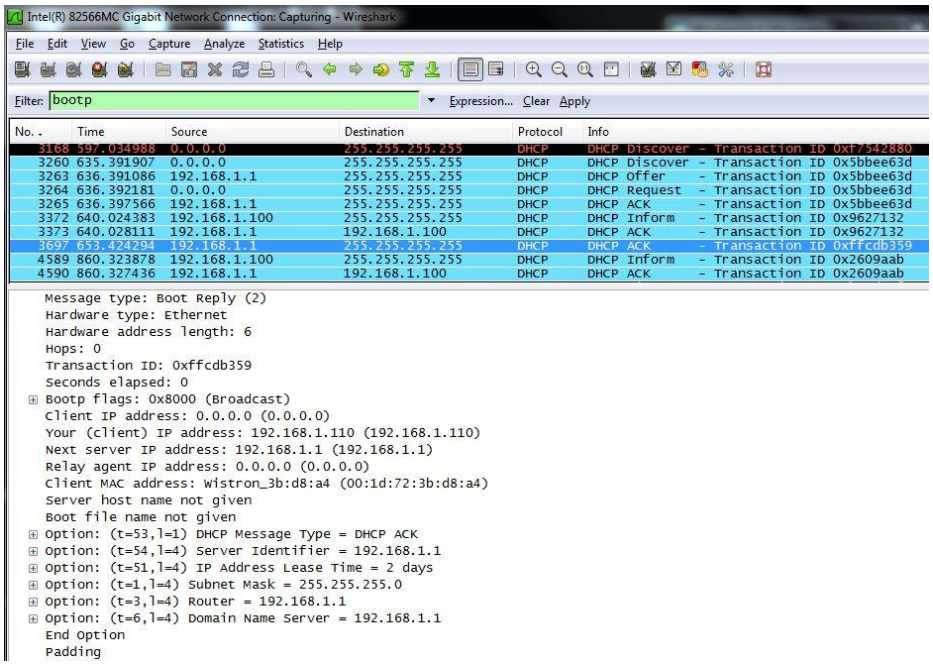


Figura 0.12: Captura de tráfego pelo *sniffer*

Fonte: Elaborado pelo autor (2011)

A.3 – Reinicialização do *switch* com GAEIP

No teste de reinicialização do *switch* com GAEIP, capítulo 6.2.3, a figura A.13 mostra o funcionamento do comando ping com o Address Guard. Já a figura A.14 ilustra o funcionamento do comando ping com as implementações de mercado M1 e M2. A captura das mensagens DHCP no *switch* com a funcionalidade é ilustrada na figura A.15.

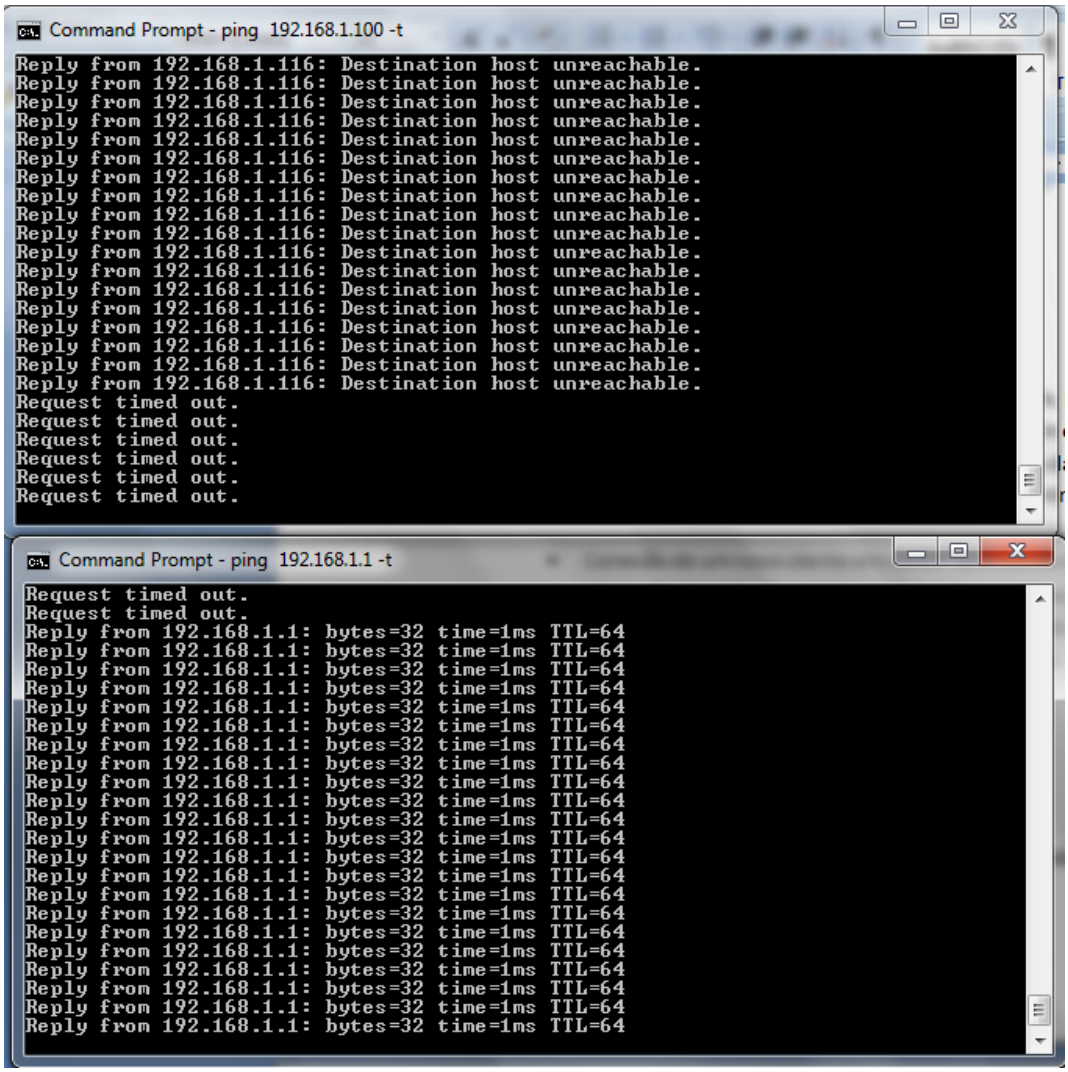


Figura 0.13: Comportamento do comando ping para uma estação que está no *switch* sem GAEIP e para o servidor DHCP

Fonte: Elaborado pelo autor (2011)

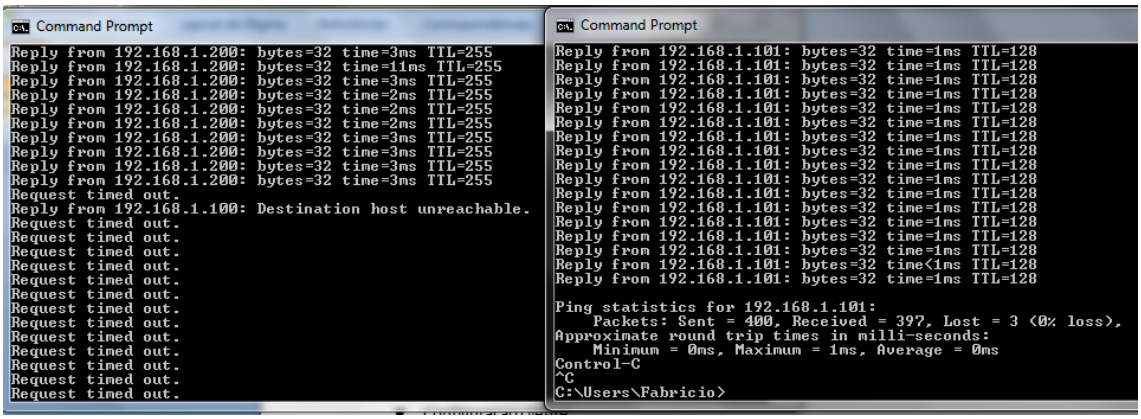


Figura 0.14: Comportamento do comando ping para uma estação que está no *switch* sem GAEIP e para o servidor DHCP, nas implementações de mercado M1 e M2.

Fonte: Elaborado pelo autor (2011)

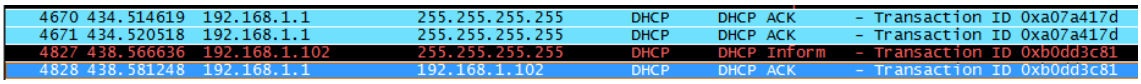


Figura 0.15: Captura de tráfego pelo *sniffer* no *switch* com GAEIP

Fonte: Elaborado pelo autor (2011)

APÊNDICE B

No apêndice B é apresentado o *script* usado pelo Address Guard em PHP.

```
<?
error_reporting(E_ALL);
ini_set('display_errors', '1');

$pol=10;
$file='captura';
$novas_linhas=0;
$linhas_processadas=0;
$dhcp_req=null;

function verifica_lease()
{
	global $dhcp_reply;
	foreach ($dhcp_reply as $val1)
	foreach ($val1 as $val2)
	foreach ($val2 as $val3)
	{
	   $agora=time();
	   echo "Valor arr $val3\r\n";
	   echo "Agora $agora\r\n";
	   //echo "n";
	   if ($val3 < $agora)
	      echo "REMOVER DO IPTABLES MAC!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!";
	}
	reset ($dhcp_reply);
}

function verifica_request($linha)
{
	global $dhcp_req;
	$msg1='Request from';
	$pos = strstr($linha, $msg1);
	if ($pos === false)
	{
	//echo "n";
	} else {
	   $pos=substr($pos, 13, 17);
	   $dhcp_req[]=$pos;
	   //echo"\\r\\n Request from: $pos \\r\\n";\
	}

}

function verifica_reply($linha)
{
	global $dhcp_req;
	global $dhcp_reply;
	global $conteudo_processar;
```

```
        global $j;
        $msg1='BOOTP/DHCP, Reply';
        $pos = strstr($linha, $msg1);
        if ($pos === false)
        {
        //echo "n";\
        } else {
           $pos = strstr($conteudo_processar[$j-1], ">");
           $pos=substr($pos, 2, 17);

           if (in_array($pos, $dhcp_req))
           {

              $ip = strstr($conteudo_processar[$j+1], "IP");
              $ip = substr($ip, 3);
              $lease = strstr($conteudo_processar[$j+9], ":");
              $lease = substr($lease, 2);
              $dhcp_reply[$pos][$ip][$lease]=time() + ($lease);

                   echo "\r\n IP $ip com MAC $pos permitido!\r\n";
                   shell_exec('ebtables -F FORWARD');
                   shell_exec("ebtables -A FORWARD -j CONTINUE -s $pos");
                   shell_exec("ebtables -A FORWARD -j ACCEPT -p ipv4 --ip-source $ip");
                   shell_exec('ebtables -A FORWARD -i eth1 -j DROP');
                   print_r($pos);
           }
        }
}

function verifica_release ($linha)
{
                        global $dhcp_release;
                        $msg1='Release';
                        $pos= strstr($linha, $msg1);
                        if ($pos === false)
                        {
                        } else {
                                //shell_exec ( 'ebtables -A FORWARD -i eth1 -j DROP');
                                shell_exec('./bloqueia_eth1.c');
                                }
}

function verifica_nack ($linha)
{
                        global $dhcp_nack;
                        $msg1='Nack';
                        $pos= strstr($linha, $msg1);
                        if ($pos === false)
                        {
                                } else {
                                        shell_exec('./bloqueia_eth1.c');
                                        }
}
shell_exec('./bloqueia_eth1.c');
for($i=1; ;$i++)
{
```

```
        $total_linhas=shell_exec("wc -l $file | cut -d \" \" -f1");
        $total_linhas=trim($total_linhas);
        // Entra aqui se novas linhas forem detectadas\
    if ($total_linhas>$linhas_processadas)
        {
              $novas_linhas= ($total_linhas - $linhas_processadas);
              $conteudo_processar=shell_exec("tail -$novas_linhas $file");
        $conteudo_processar=explode("\n", $conteudo_processar);
        //print_r($conteudo_processar);\
              //Processar o conteudo aqui!!\
           for($j=0; $j < $novas_linhas; $j++)
        {
           verifica_request($conteudo_processar[$j]);
           verifica_reply($conteudo_processar[$j]);
                                verifica_release($conteudo_processar[$j]);
                                verifica_nack($conteudo_processar[$j]);
        }

    }

    if (count($dhcp_reply) >=1)
           verifica_lease();
        echo "-----------------------------------------------------\r\n";
        echo "Iteracao Numero: $i \r\n";
        echo "Total de linhas do arquivo: $total_linhas \r\n";
        echo "Quantidade de linhas ja processadas: $linhas_processadas \r\n";
        echo "Quantidade de linhas novas: $novas_linhas \r\n";
                    //echo "$pos \r\n";
        //echo "Conteudo das novas linhas: \\r\\n $conteudo_processar\\r\\n";\
    print_r($dhcp_req);
    print_r($dhcp_reply);
        echo "-----------------------------------------------------\r\n";
        //Update de variaveis\
        //Limpar pois o conteudo j\'e1 foi processado\
        $conteudo_processar='';
  //update das linhas j\'e1 processadas\
        $linhas_processadas=$total_linhas;
        //novas linhas volta a ser zero\
        $novas_linhas=0;

        //Espera $pol segundos a cada iteracao do laco\
        sleep($pol);
}

?>
```