DHCP – Aplicação e Princípios

www.huawei.com

HUAWEI

Prefácio

DHCP é a abreviação de Dynamic Host Configuration Protocol, é uma aplicação para gerenciar centralizadamente a atribuição de endereços dinâmicos. A tecnologia DHCP é usada para garantir a alocação racional de endereços IP, evitando assim o desperdício de endereços IP e melhorando a taxa de utilização do endereço IP.

Objetivo

Após completer está seção você será capaz de:

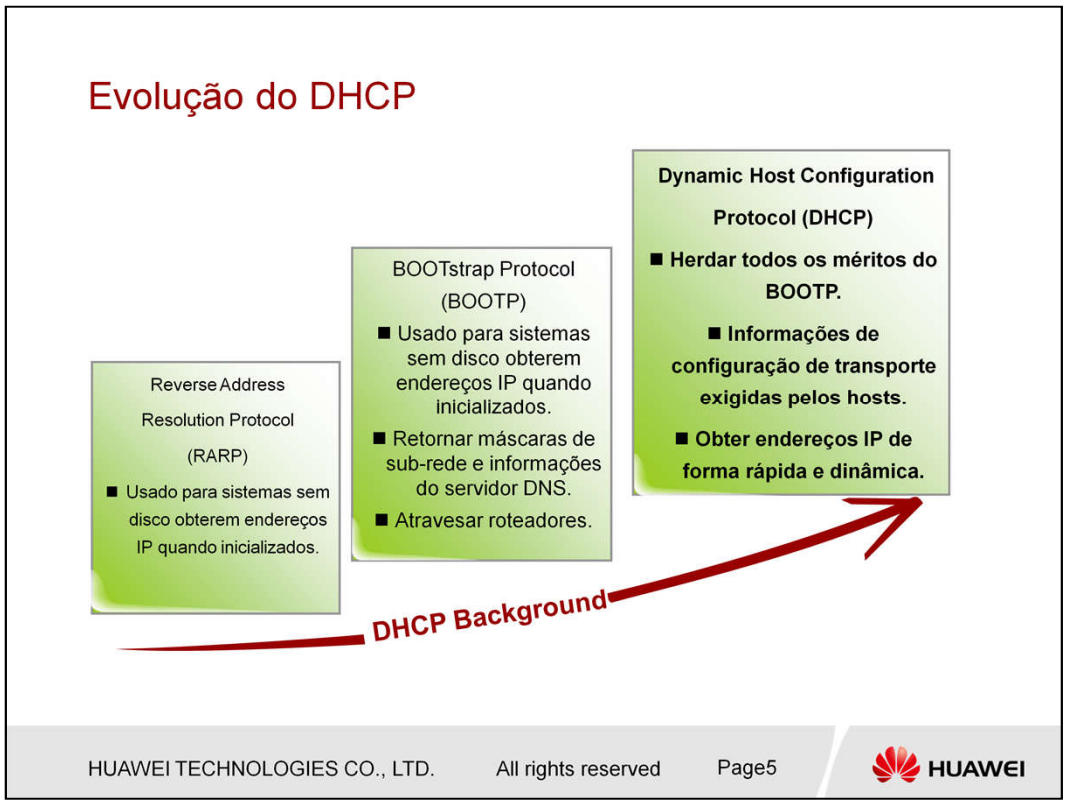
- Explicar os princípios de DHCP
- Entender a operação do DHCP Server
- Entender a função de um DHCP Relay
- Entender a função DHCP Snooping
- Fazer a configuração de DHCP

Conteúdo

Princípios de DHCP

DHCP Snooping

Configuração de DHCP



Origem do DHCP: RARP→BOOTP →DHCP

Protocolo de resolução de endereço reverso (RARP):

O RARP é usado para sistemas sem disco para obter endereços IP quando eles são inicializados. Uma solicitação RARP é transmitida pela rede. O endereço de hardware do remetente é indicado no pacote de solicitação para que um endereço IP seja alocado. A resposta geralmente é retornada no modo unicast. O formato dos pacotes RARP é quase o mesmo que o dos pacotes ARP.

Protocolo BOOTstrap (BOOTP)

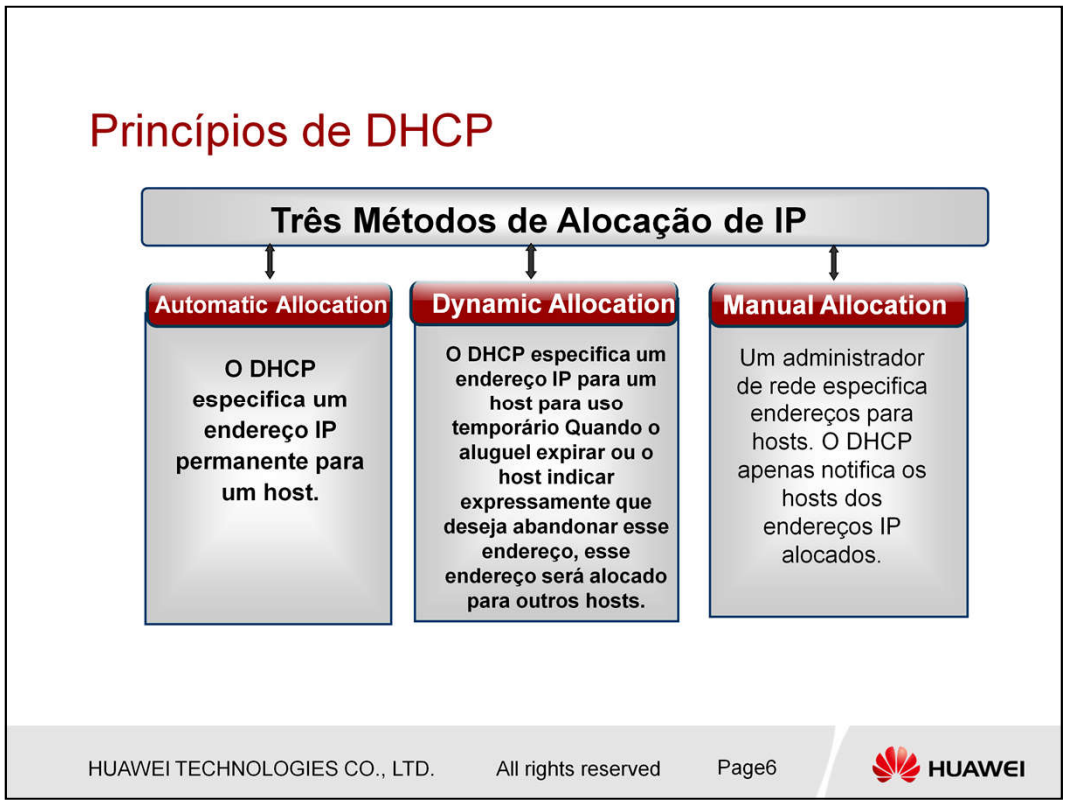
O pacote BOOTP é colocado em um datagrama UDP padrão. O BOOTP permite que um sistema sem disco descubra seu próprio endereço IP. Ele também retorna outros tipos de informações, como o endereço IP de um roteador, a máscara de sub-rede de um cliente e o endereço IP de um servidor DNS. Comparado com o RARP, ele permite a descoberta de mais informações e a travessia de roteadores.

Protocolo de configuração dinâmica de host (DHCP):

O DHCP evolui do BOOTP. Ele herda os méritos do BOOTP. A principal melhoria está na alocação dinâmica.

DHCP é uma extensão para o BOOTP. Primeiro, o DHCP permite que um computador obtenha todas as informações de configuração desejadas por meio de uma mensagem. É por isso que o DHCP é conhecido como protocolo de transporte de configuração. Segundo, o DHCP permite que um computador obtenha rápida e dinamicamente o endereço IP, conhecido como mecanismo de atribuição de endereço IP dinâmico.

O DHCP é baseado no modelo cliente-servidor. O servidor DHCP especificado aloca endereços de rede e parâmetros de configuração de transporte para hosts configurados dinamicamente. Um host pode funcionar como um servidor apenas quando o administrador do sistema o configura como um servidor DHCP.



Modos de alocação de endereço suportados pelo servidor DHCP:

Alocação automática: nesse modo, os endereços IP não são alocados manualmente. Quando um cliente DHCP obtém um endereço IP do servidor DHCP pela primeira vez, esse endereço pertence permanentemente a esse cliente DHCP e não será atribuído a outros clientes.

Alocação dinâmica: quando um cliente DHCP aluga um endereço IP do servidor DHCP, o servidor DHCP atribui um endereço IP temporário ao cliente. Quando o prazo da concessão expira, esse endereço é retornado ao servidor DHCP e disponível para outros clientes. Se o cliente DHCP precisar de um endereço IP posteriormente, talvez seja necessário solicitar outro endereço IP.

Alocação manual: nesse modo, o administrador da rede atribui endereços IP específicos manualmente para clientes DHCP específicos no servidor DHCP. Quando o cliente DHCP solicita um endereço IP para acesso à rede, o servidor DHCP transmite o endereço IP configurado manualmente para o cliente DHCP.

Entre os três modos, apenas a alocação dinâmica de endereços permite a reutilização de endereços IP que foram alocados aos hosts, mas que atualmente não estão em uso. Um endereço precisa ser alocado temporariamente ao host conectado à rede ou a um grupo

de endereços IP limitados.

Os endereços precisam ser alocados aos hosts que não exigem endereços IP permanentes. Quando um novo host precisa acessar uma rede permanentemente e há recursos limitados de endereço IP, a alocação dinâmica é uma boa opção porque o endereço IP do host pode ser recuperado quando este host estiver fora de serviço no futuro.

Sequência de atribuição de endereço IP

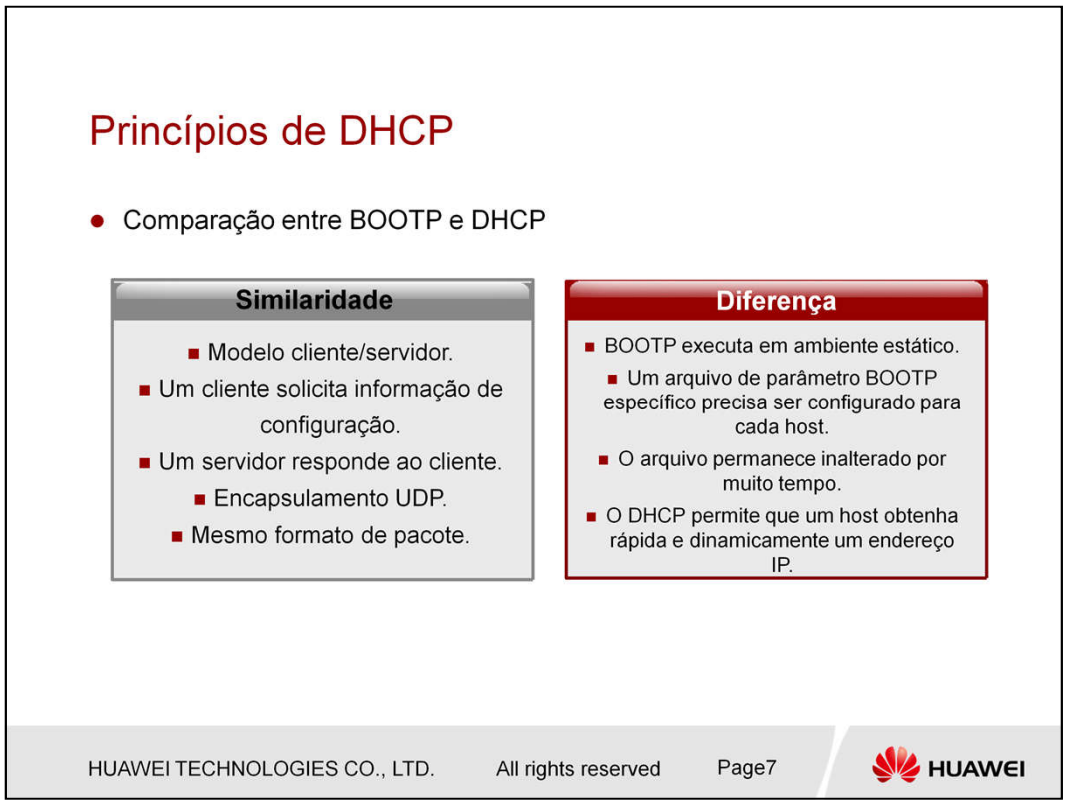
O servidor DHCP atribui endereços IP a um cliente na seguinte sequência:

Endereço IP que está no banco de dados do servidor DHCP e está estaticamente vinculado ao endereço MAC do cliente

Endereço IP atribuído ao cliente antes, ou seja, o endereço IP na opção de endereço IP solicitado do pacote DHCPDISCOVER enviado pelo cliente

Endereço IP encontrado pela primeira vez quando o servidor DHCP pesquisa no pool de endereços DHCP os endereços IP disponíveis

Se o conjunto de endereços DHCP não tiver um endereço IP disponível, o servidor DHCP procurará os endereços IP de tempo limite e os endereços IP conflitantes em busca de um endereço IP não utilizado e, em seguida, atribuirá o endereço IP ao cliente. Se todos os endereços IP forem usados, um erro será relatado.



Comparação entre DHCP e BOOTP:

Semelhante ao BOOTP, o DHCP também funciona no modo cliente / servidor. Um cliente DHCP solicita informações de configuração de um servidor DHCP, incluindo parâmetros como o endereço IP atribuído, a máscara de sub-rede e o gateway padrão. O servidor DHCP responde com as informações de configuração correspondentes com base na política de roteamento. Os pacotes BOOTP e DHCP são encapsulados em pacotes UDP e têm a mesma estrutura de pacotes. O DHCP e o BOOTP usam dois números de porta conhecidos: o número da porta do servidor é 67 e o número da porta do cliente é 68.

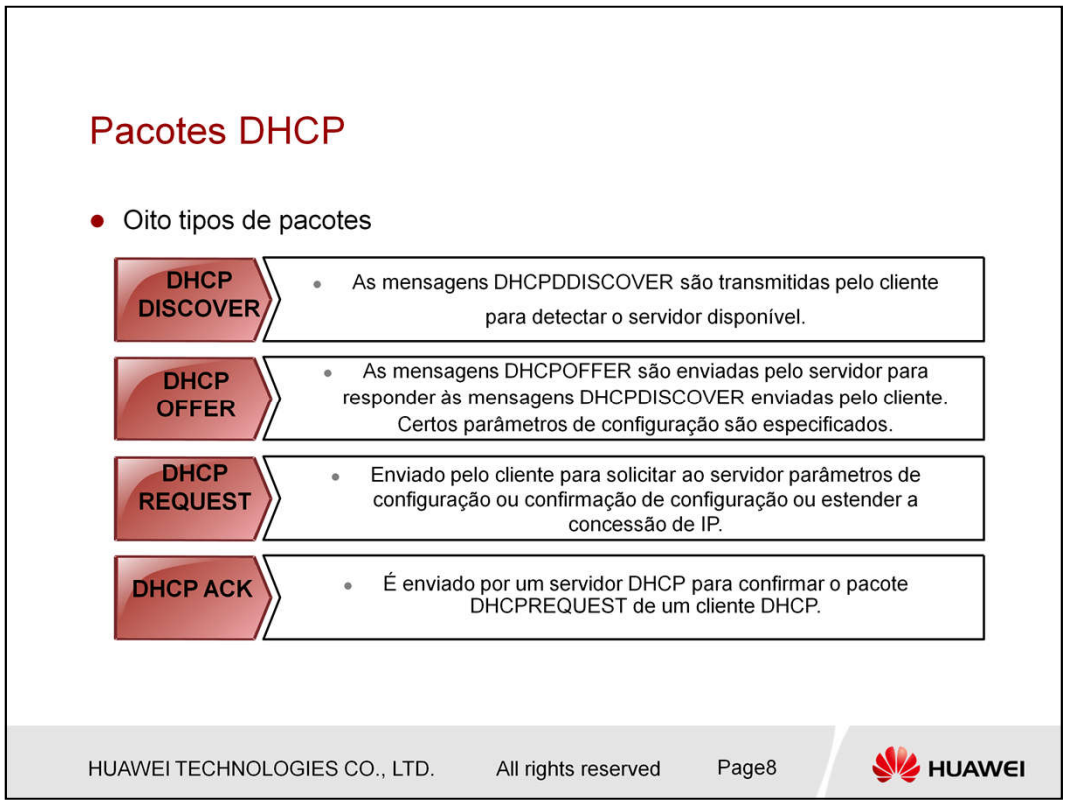
O BOOTP é executado em um ambiente relativamente estático, onde a localização física de cada host é fixa. O administrador configura um arquivo de parâmetro BOOTP específico para cada host. Este arquivo permanece inalterado por um longo período de tempo. O DHCP permite que um host obtenha um endereço IP dinamicamente, em vez de especificar um endereço IP para cada host.

Comparado com o BOOTP, o DHCP tem as seguintes extensões:

O DHCP pode ajudar um host a obter todas as informações de configuração necessárias enviando apenas uma mensagem.

O DHCP permite que um host obtenha um endereço IP

dinamicamente, em vez de especificar um endereço IP para cada host.



Qualquer protocolo dinâmico possui um conjunto de idiomas especificados, ou seja, protocolo. DHCP não é exceção.

Pacotes DHCP têm os seguintes tipos:

DHCP DISCOVER: É o primeiro pacote usado para procurar um servidor DHCP quando um cliente DHCP acessa a rede pela primeira vez.

DHCP OFFER: Enviado pelo servidor para responder às mensagens DHCP Discover enviadas pelo cliente. Certos parâmetros de configuração são especificados.

DHCP REQUEST: enviada pelo cliente para solicitar ao servidor parâmetros de configuração ou confirmação de configuração ou estender a concessão de IP. As funções são as seguintes:

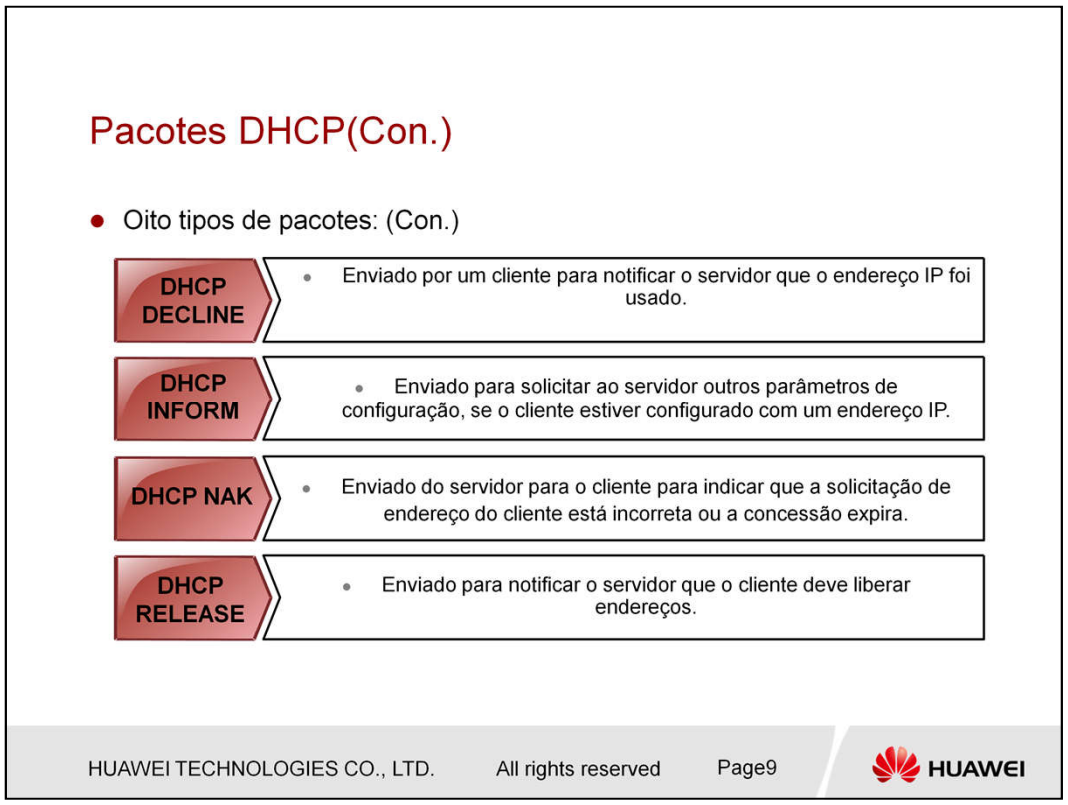
Depois de inicializado, um cliente DHCP transmite um pacote DHCPREQUEST para responder ao pacote DHCPOFFER enviado por um servidor DHCP.

Após ser reiniciado, um cliente DHCP transmite um pacote DHCPREQUEST para confirmar a correção do endereço IP alocado anteriormente.

Depois de vinculado a um endereço IP, um cliente DHCP envia um pacote DHCPREQUEST unicast para estender a concessão do

endereço IP.

DHCP ACK: É enviado por um servidor DHCP para confirmar o pacote DHCPREQUEST de um cliente DHCP. Depois de receber um pacote DHCPACK, o cliente DHCP obtém as informações de configuração, incluindo o endereço IP.



Quatro outros tipos de pacotes DHCP:

DHCP DECLINE: É enviado por um cliente DHCP para notificar o servidor DHCP de que o endereço IP atribuído está em conflito com os outros endereços IP. Em seguida, o cliente DHCP aplica-se ao servidor DHCP para outro endereço IP.

DHCP NAK: É enviado por um servidor DHCP para recusar o pacote DHCPREQUEST enviado por um cliente. Geralmente, o pacote DHCPNAK é usado nos seguintes casos:

DHCP INFORM: Após obter um endereço IP, um cliente envia esse pacote para obter outras informações de configuração de rede, como o endereço do gateway e o endereço do servidor DNS, do servidor.

DHCP RELEASE: É enviado por um cliente DHCP para liberar ativamente o endereço IP atribuído por um servidor DHCP. Depois de receber um pacote DHCPRELEASE, o servidor DHCP atribui esse endereço IP a outro cliente DHCP.

Pacotes DHCP(Con.)

- Formato dos Pacotes DHCP

OP (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4)			
Secs (2)		Flags (2)	
Client IP address (4)			
Your IP address (4)			
Server IP address (4)			
Gateway IP address (4)			
Client Hardware Address (16)			
Server Name (64)			
File (128)			
Options (variable)			

OP: código de operação (1 = solicitação de inicialização, 2 = resposta de inicialização)

Htype: tipo de endereço de hardware (1 = 10mb ethernet)

Hlen: comprimento do endereço de hardware (10 para Ethernet)

Hops: indica o número de agentes de retransmissão DHCP pelos quais um pacote DHCP passa. Este campo é definido como 0 pelo cliente. O valor desse campo é aumentado em 1 cada vez que o pacote DHCP passa um relé DHCP. Este campo é usado para limitar o número de agentes de retransmissão DHCP pelos quais um pacote DHCP pode passar. O número de retransmissões DHCP entre um servidor e um cliente não deve ser maior que 4. Ou seja, o número de saltos não deve ser maior que 4. Caso contrário, o pacote DHCP será descartado.

Xid: ID de transmissão, selecionado por um cliente para interação com o servidor.

Secs: tempo decorrido desde a última vez que o endereço IP usado por um cliente foi obtido ou atualizado.

Flags: Este campo está reservado e não é usado no BOOTP. No DHCP, indica um sinalizador. Somente o bit mais significativo do campo Flags é importante e outros bits são definidos como 0. O bit mais à esquerda do campo Flags é o sinalizador de resposta de

transmissão. Os significados dos valores são os seguintes:

0: indica que o cliente solicita que o servidor envie um pacote de resposta no modo unicast.

1: indica que o cliente solicita que o servidor envie um pacote de resposta no modo de transmissão.

Client IP Address: usado apenas quando o cliente está nos estados BOUND, RENEW ou REBOUND e puder responder a solicitações ARP.

Your IP Address: endereço IP do cliente alocado pelo servidor DHCP.

Server IP Address: indica o endereço IP de um servidor.

Gateway IP Address: indica o endereço IP do primeiro agente de retransmissão DHCP. Depois que um cliente envia um pacote DHCPREQUEST, o primeiro agente de retransmissão DHCP preenche seu endereço IP nesse campo ao encaminhar esse pacote DHCPREQUEST se o servidor e o cliente estiverem em diferentes segmentos de rede. O servidor determina o endereço do segmento de rede com base nesse campo e, em seguida, seleciona o pool de endereços para atribuir um endereço IP ao cliente. O servidor também retorna um pacote DHCPREPLY para o primeiro agente de retransmissão DHCP. O agente de retransmissão DHCP encaminha o pacote DHCPREPLY para o cliente. Se a solicitação passar mais de uma retransmissão DHCP antes de chegar ao servidor DHCP, as não-primeiras retransmissões DHCP aumentam os saltos em 1 em vez de alterar esse campo.

Client Hardware Address: indica o endereço MAC de um cliente. Este campo deve ser consistente com os campos Tipo de hardware e Comprimento do hardware. Ao enviar um pacote de solicitação DHCP, o cliente preenche seu endereço de hardware neste campo. Para uma Ethernet, esse campo deve ser preenchido com um endereço MAC Ethernet de 6 bytes quando os valores dos campos Tipo de Hardware e Comprimento do Hardware forem 1 e 6, respectivamente.

Server name: indica o nome do servidor no qual um cliente obtém informações de configuração. Este campo é opcional e é preenchido pelo servidor DHCP. Se o campo for preenchido, deverá ser uma sequência de caracteres que termine com 0. Por padrão, o valor está vazio.

File: indica o nome do arquivo de inicialização. O nome completo é fornecido no pacote DHCPOFFER.

Options: indica o campo Opções de DHCP. Ele deve ter no mínimo 312 bytes. Este campo contém informações de configuração atribuídas por um servidor a um cliente, incluindo os endereços IP do gateway e do servidor DNS e a concessão do endereço IP disponível para o cliente.

Pacotes DHCP (Con.)

- Formato dos Pacotes DHCP
  - ⇨ O campo de opção nas mensagens DHCP usa o modo CLV.
    - − Código: identificador de um byte para identificar exclusivamente o conteúdo da informação.
    - − Comprimento: indica o comprimento do conteúdo da informação, contendo um byte.
    - − Valor: indica o conteúdo da informação, cujo comprimento é determinado pelo campo Comprimento. É expresso em bytes.

  HUAWEI

O campo de opção de um pacote DHCP é construído no modo CLV. Especificamente:

Código: identificador de um byte para identificar exclusivamente o conteúdo da informação.

Comprimento: indica o comprimento do conteúdo da informação, contendo um byte.

Valor: indica o conteúdo da informação, cujo comprimento é determinado pelo campo Comprimento. É expresso em bytes.

Este é um formato flexível. Quando novas informações são necessárias, basta solicitar uma nova opção neste modo. O modo CLV é extensível e, portanto, amplamente utilizado em protocolos.

Tipos de opções comuns:

Tipo de pacote: C = 53, L = 1, V = 1-8, indicando um tipo de pacote DHCP.

IP do roteador: C = 3, L = comprimento do endereço IP, V = endereço IP do gateway padrão de um cliente

IP DNS: C = 6, L = múltiplo do tamanho do endereço IP, V = sequência de endereços IP do servidor DNS de um cliente

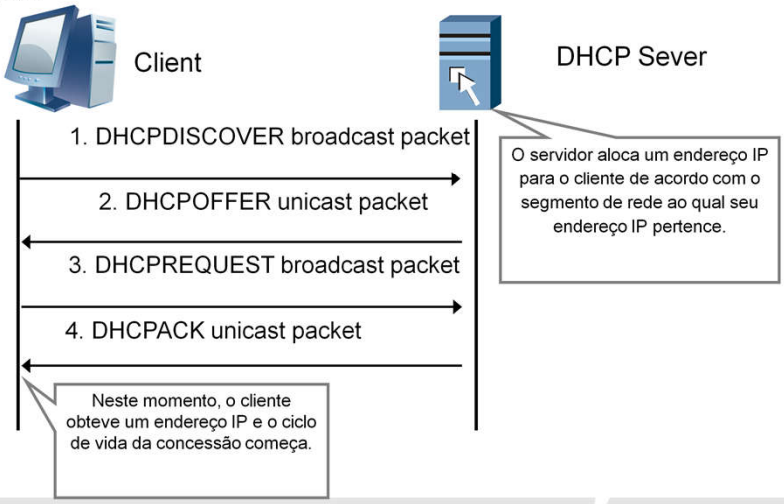
IP WINS: C = 44, L = múltiplo do tamanho do endereço IP, V = IP

sequência de endereços do servidor WINS de um cliente

O DHCP fornece uma estrutura para a transmissão de parâmetros de configuração em uma rede TCP / IP. Entre os clientes DHCP e o servidor DHCP, os parâmetros de configuração e as informações de controle acordados por ambas as partes são transmitidos por meio de códigos de opção.

Funcionamento do DHCP

- Um cliente solicita a um servidor um endereço IP através do DHCP em quatro etapas:



Procedimento de trabalho DHCP:

O cliente envia um pacote de difusão DHCPDISCOVER, com 255.255.255.255 como o endereço de destino, para encontrar um servidor DHCP na rede.

Todos os servidores DHCP que recebem o pacote DHCPDISCOVER na rede respondem à solicitação no modo de transmissão. Eles selecionam um dos endereços IP disponíveis e o alocam ao cliente DHCP enviando um pacote DHCPOFFER que contém o endereço IP para concessão e outras informações de configuração.

Após o recebimento dos pacotes DHCPOFFER, o cliente envia um pacote DHCPREQUEST, que contém o endereço IP solicitado por um servidor DHCP específico. Como existem vários servidores DHCP, o cliente transmite o pacote DHCPREQUEST e notifica todos os servidores DHCP de que aceitará o endereço IP fornecido por um servidor DHCP específico.

Após o recebimento do pacote DHCPREQUEST, o servidor DHCP envia um pacote de resposta ACK ao cliente.

Posteriormente, quando o cliente DHCP efetua login na rede novamente, não precisa enviar uma mensagem DHCPDISOVER novamente. Em vez disso, envia a mensagem DHCPREQUEST contendo o último endereço IP alocado. Quando o servidor DHCP

recebe essa mensagem, ele tenta fazer com que o cliente DHCP continue usando o endereço IP original e responde com uma mensagem DHCPACK.

Se esse endereço IP não estiver disponível (por exemplo, foi alocado para outro cliente DHCP), o servidor DHCP responderá com uma mensagem DHCPNAK ao cliente. Após receber a mensagem DHCPNAK, o cliente deve reenviar uma mensagem DHCPDISOVER para solicitar um novo endereço IP.

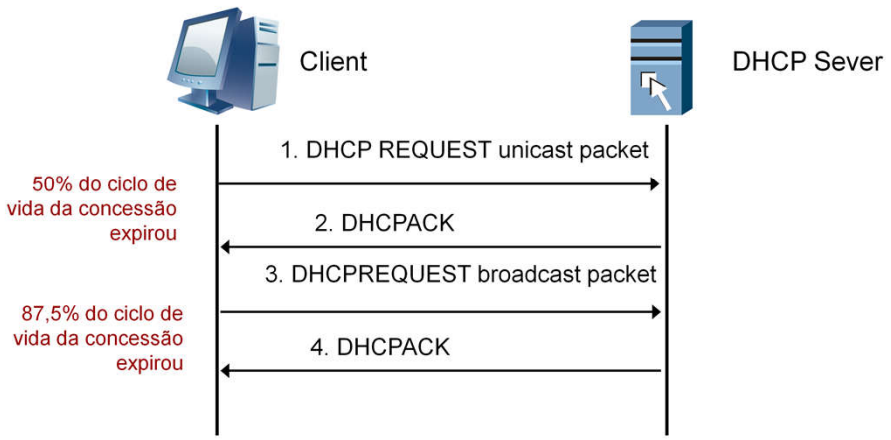
Comparado com o de um cliente DHCP, o comportamento de um servidor DHCP é mais simples, totalmente controlado pelo cliente DHCP. O servidor apenas responde a diferentes pacotes DHCP de acordo com os pacotes de solicitação recebidos de um cliente DHCP.

Princípio de alocação de endereço IP: Após o recebimento de um pacote de solicitação DHCP, o servidor DHCP primeiro verifica se o valor do campo giaddr (endereço IP do gateway) é 0. Caso contrário, ele aloca um endereço IP do pool de endereços correspondente de acordo com a rede segmento ao qual o endereço IP do gateway pertence. Se o valor do campo giaddr (endereço IP do gateway) for 0, o servidor DHCP pensará que o cliente está na mesma sub-rede e, em seguida, alocará um endereço IP ao cliente do pool de endereços correspondente, de acordo com o segmento de rede onde o seu próprio O endereço IP pertence.

Um servidor DHCP também pode implementar o gerenciamento de pool de endereços.

Funcionamento do DHCP

- Um cliente renova uma concessão de endereço IP em quatro etapas :



  HUAWEI

Todos os endereços IP obtidos pelos clientes têm um ciclo de vida de concessão. Se um cliente não renovar uma concessão que expirou, o endereço IP do cliente será recuperado pelo servidor.

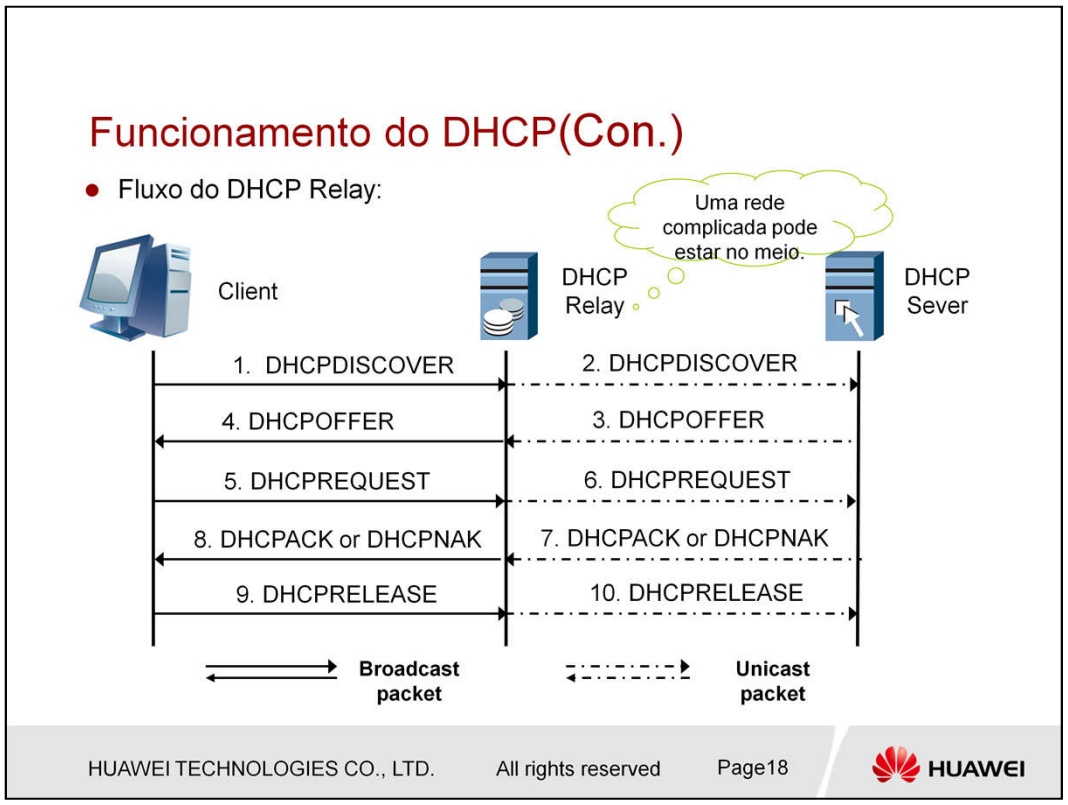
O processo é como se segue:

Quando 50% do ciclo de vida da concessão expirou, o cliente envia um pacote DHCPREQUEST para renovação da concessão. Como as informações sobre o servidor DHCP foram obtidas anteriormente, desta vez o pacote DHCPREQUEST é unicast.

Após o recebimento do pacote DHCPREQUEST, o servidor envia uma mensagem de resposta e redefine o ciclo de vida da concessão.

Se o servidor falhar ao receber um pacote DHCPREQUEST quando 50% do ciclo de vida da concessão expirar, o ciclo de vida da concessão do endereço IP não será redefinido. Se nenhuma resposta ao pacote DHCPREQUEST (enviada quando 50% do ciclo de vida da concessão expirar) for recebida quando 87,5% do ciclo de vida da concessão expirar, o cliente assumirá que o servidor DHCP original não está disponível e começará a transmitir um pacote DHCPREQUEST. Qualquer servidor DHCP na rede pode responder a essa solicitação com um pacote DHCPACK ou DHCPNAK.

Se o cliente receber um pacote DHCPACK, ele retornará ao estado de ligação e redefinirá os cronômetros de atualização de concessão e de religação do servidor.
Se todos os pacotes recebidos pelo cliente forem pacotes DHCPNAK, o cliente retornará ao estado de inicialização. Ao mesmo tempo, o cliente deve parar de usar esse endereço IP imediatamente. Depois de voltar ao estado de inicialização, o cliente pode solicitar novamente um endereço IP.
Se o cliente não receber nenhuma resposta antes que o cronômetro de expiração da concessão expire, o cliente deverá parar de usar o endereço IP atual imediatamente e retornar ao estado de inicialização para solicitar um novo endereço IP.
Após receber a solicitação de renovação de concessão, o servidor DHCP envia uma mensagem DHCPACK como resposta e redefine o ciclo de vida da concessão do cliente.



Ambiente de aplicação da DHCP relay:

Os protocolos DHCP anteriores são aplicáveis apenas à situação em que os clientes DHCP e o servidor DHCP estão no mesmo segmento de rede. Muitos campos, como giaddr e hop, não estão disponíveis nos pacotes DHCP. Posteriormente, o protocolo DHCP foi estendido. Portanto, é necessário configurar um servidor DHCP em cada segmento de rede para a configuração dinâmica do host. Esta operação, no entanto, é antieconômica.

A função de DHCP relay é assim introduzida para solucionar esse problema. Por meio de um agente DHCP Relay, um cliente DHCP pode solicitar ao servidor DHCP em outro segmento de rede um endereço IP válido. Dessa maneira, os clientes DHCP em vários segmentos de rede podem compartilhar um servidor DHCP. Isso economiza custos e facilita o gerenciamento centralizado.

Os pacotes DHCP geralmente são transmitidos e não podem atravessar várias sub-redes. Quando um pacote DHCP precisa atravessar várias sub-redes, são necessários DHCP Relay.

O DHCP Relay pode ser um roteador ou host. Em uma palavra, o DHCP relay deve escutar todos os pacotes UDP cujo destino seja a porta 67.

Ao receber esse pacote, o DHCP relay determina primeiro se é um pacote de solicitação de um cliente. Se for e o valor do campo giaddr (endereço IP do gateway) for 0, o relay preenche seu próprio endereço IP nesse campo e envia o pacote em um servidor DHCP real, permitindo que o pacote DHCP atravesse várias sub-redes.

Se o DHCP relay descobrir que é um pacote de resposta do servidor DHCP, a DHCP relay transmite ou envia o pacote encapsulado ao cliente DHCP, dependendo do bit do sinalizador de transmissão no campo Flag.

O procedimento de trabalho do DHCP relay é o seguinte:

Um cliente transmite um pacote DHCPDISCOVER para encontrar um servidor DHCP.

Após o recebimento do pacote DHCPDISCOVER, o DHCP relay preenche seu próprio endereço IP no campo giaddr e, em seguida, preenche o endereço IP do servidor no campo Servidor DHCP antes de enviar a solicitação ao servidor DHCP.

Após o recebimento do pacote DHCPDISCOVER, o servidor DHCP envia um pacote DHCPOFFER que contém o endereço IP do servidor DHCP para o DHCP relay.

O DHCP relay envia o pacote DHCPOFFER recebido ao cliente.

Depois de encontrar o servidor DHCP, o cliente DHCP envia um pacote DHCPREQUEST para solicitar um endereço IP.

Após o recebimento desta solicitação, o DHCP relay preenche seu próprio endereço IP no endereço giaddr e envia o pacote DHCPREQUEST ao servidor DHCP.

Após o recebimento da solicitação, o servidor DHCP aloca um endereço IP ao cliente enviando um pacote DHCPACK. Se o endereço IP solicitado não estiver disponível, o servidor envia um pacote DHCPNAK para o DHCP relay. No pacote enviado para o DHCP Relay, o servidor preenche o endereço IP alocado ao cliente no campo Seu endereço IP.

Após o recebimento do pacote de resposta do servidor DHCP, a DHCP relay encaminha esse pacote para o cliente DHCP.

Se o cliente quiser liberar o endereço IP, ele envia um pacote DHCPRELEASE, cujo campo Endereço IP do Cliente é preenchido com o endereço IP obtido.

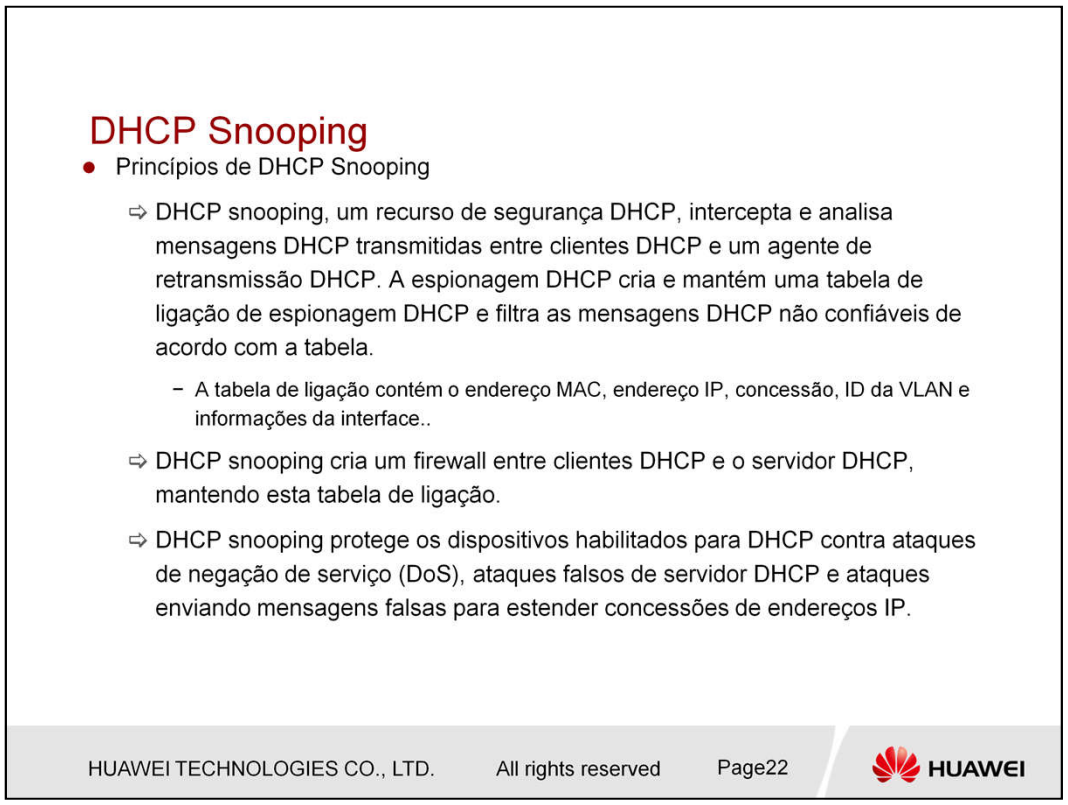
Após o recebimento do pacote DHCPRELEASE, o DHCP relay preenche seu próprio endereço IP no campo giaddr e envia o pacote ao servidor DHCP. Após receber a solicitação, o servidor DHCP libera o endereço IP alocado anteriormente.

Conteúdo

Princípios de DHCP

DHCP Snooping

Configuração do DHCP



A espionagem DHCP registra uma tabela de ligação DHCP, que contém os endereços IP e MAC do cliente, número da porta e ID da VLAN da interface que recebeu a solicitação do cliente no processo de alocação de endereço. Quando um cliente é conectado, a tabela de ligação é criada para o cliente. Quando o cliente fica offline, esta tabela de ligação é excluída.

Quando ou após uma tabela de ligação ser gerada, a espionagem DHCP verifica os pacotes DHCP e compara os campos no pacote com os da tabela de ligação DHCP. Se um ataque de DHCP for detectado, este pacote será descartado, impedindo o ataque de DHCP.

Além disso, a espionagem do DHCP distingue interfaces confiáveis e interfaces não confiáveis. As interfaces que se conectam ao servidor DHCP (na rede de uma operadora de telecomunicações) são definidas como Confiável e outras interfaces configuradas para receber mensagens de fora da rede da operadora de telecomunicações são definidas como Não Confiáveis. O endereço IP de retransmissão é adicionado apenas para dispositivos de retransmissão DHCP. Pacotes de retransmissão DHCP cujo giaddr arquivado não é 0 de interfaces não confiáveis não são processados para evitar ataques falsos ao servidor DHCP.

As entradas de espionagem DHCP podem ajudar a impedir a

falsificação de endereço IP e a falsificação de ARP.

DHCP Snooping (Con.)

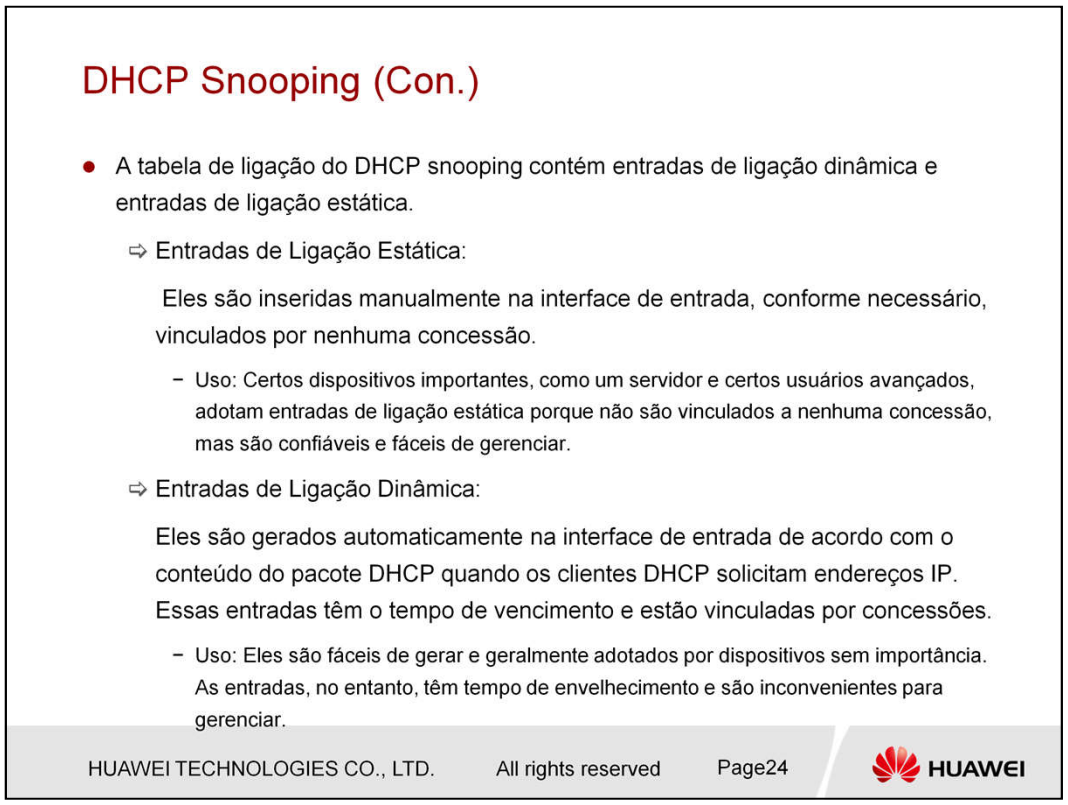
- Principais técnicas adotadas no DHCP Snooping
  - ⇨ Interface Confiável / Não Confiável: Geralmente, as interfaces que se recebem processam mensagens oriundas do servidor DHCP são definidas como Confiável e outras interfaces que não devem processar mensagens oriundas de servidor são definidas como Não-Confiável..
  - ⇨ Tabela de ligação: estabelece os relacionamentos de ligação entre endereços MAC, endereços IP, IDs de VLAN e números de porta.
  - ⇨ Opção 82: uma das opções relacionadas aos pacotes DHCP, para registrar o tipo de interface de entrada, o número da porta, as informações da VLAN e o endereço MAC da ponte. É essencial para a geração de uma tabela de ligação.

  HUAWEI

O campo giaddr nos pacotes DHCP destinados a zonas confiáveis não é 0. O campo giaddr nos pacotes DHCP recebidos de zonas não confiáveis é 0.

A espionagem DHCP é usada principalmente para impedir ataques de negação de serviço (DoS), ataques falsos de servidor DHCP, ataques de intermediários ARP e ataques de falsificação de IP / MAC quando o DHCP está ativado no dispositivo.

A espionagem DHCP pode ser aplicada aos dispositivos de rede das camadas 2 e 3.



Ligação estática:

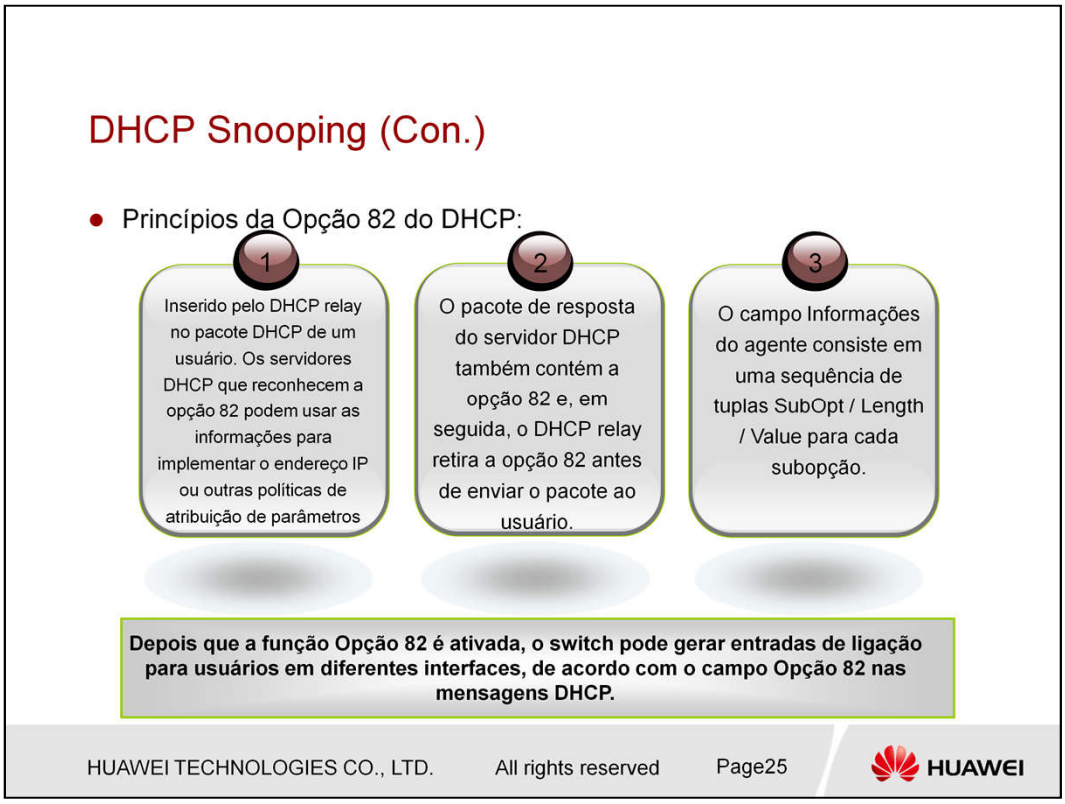
Se endereços IP estáticos estiverem alocados para clientes, você poderá configurar entradas de ligação estática para esses endereços IP alocados para impedir que certos usuários roubem esses endereços IP estáticos. Caso um grande número de clientes precise de endereços IP estáticos, você precisará configurar endereços IP para eles, um por um. Caso contrário, os usuários ilegais não poderão ser impedidos de roubar endereços IP estáticos.

Antes de encaminhar os dados dos usuários aos quais são atribuídos endereços IP estaticamente, um comutador não pode aprender automaticamente os endereços MAC dos usuários ou gerar entradas de tabela de ligação para esses usuários. Você precisa criar a tabela de ligação manualmente.

Ligação dinâmica:

As entradas dinâmicas na tabela de ligação de espionagem DHCP não precisam ser configuradas. Eles são gerados automaticamente quando a espionagem DHCP está ativada. Para endereços IP alocados dinamicamente a clientes, o dispositivo habilitado para DHCP aprende automaticamente os endereços MAC dos clientes e cria uma tabela de

relacionamento de ligação. Nesse caso, uma tabela de ligação não precisa ser configurada.



A RFC 3046 (opção de informações do agente de retransmissão DHCP) propõe a aplicação da opção 82. Ele é inserido pelo agente de retransmissão DHCP ao encaminhar pacotes DHCP originados pelo cliente para um servidor DHCP. Os servidores que reconhecem a opção Informações do agente de retransmissão podem usar as informações para implementar o endereço IP ou outras políticas de atribuição de parâmetros. O servidor DHCP faz eco da opção de volta literalmente ao agente de retransmissão nas respostas de servidor para cliente, e o agente de retransmissão retira a opção antes de encaminhar a resposta ao cliente. O campo Informações do agente consiste em uma sequência de tuplas SubOpt / Length / Value para cada sub-opção. Atualmente, duas sub-opções são definidas da seguinte maneira:

1 Subopção de ID do circuito do agente: identifica o circuito de um usuário.

2 Subopção de identificação remota do agente: identifica o host na extremidade remota do circuito.

Quando a função Opção 82 está ativada em um relé DHCP, se a Opção 82 construída por um usuário não contém informações de interface, a tabela de ligação gerada não possui essas informações. Isso pode causar:

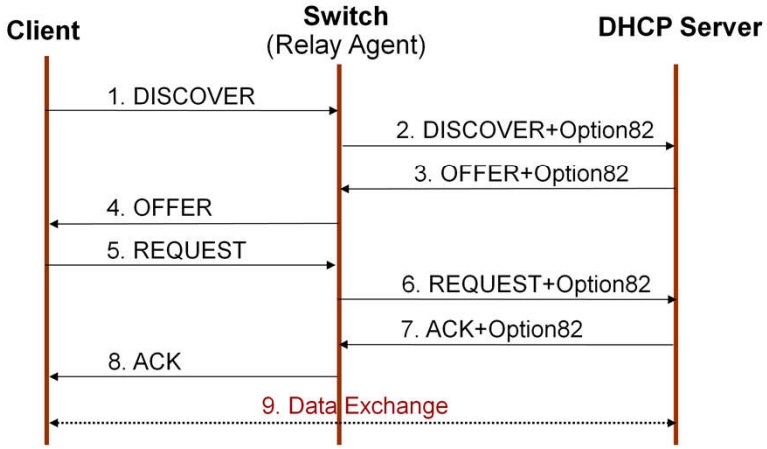
Pacotes de resposta DHCP de servidores a serem ouvidos pelos usuários sob outras interfaces na mesma VLAN.

Depois que o usuário fica on-line, se outro usuário sob uma interface diferente na mesma VLAN fabricar um endereço IP e um endereço MAC, esse usuário falso pode se disfarçar de usuário legal.

Quando o espião DHCP é usado na Camada 2, as informações da interface podem ser obtidas para a tabela de ligação se a função Opção 82 não estiver configurada.

DHCP Snooping (Con.)

- Procedimento de funcionamento da opção 82 do DHCP:



Um cliente envia um pacote DHCPDISCOVER para encontrar um servidor DHCP.

Após o recebimento do pacote DHCPDISCOVER, o switch que funciona como agente de retransmissão DHCP adiciona informações da Opção 82 ao pacote e as encaminha para o servidor DHCP.

Após o recebimento do pacote DHCPDISCOVER, o servidor DHCP responde com um pacote DHCPOFFER que contém as informações da Opção 82 adicionadas anteriormente.

Após o recebimento da resposta do servidor DHCP, o switch que funciona como agente de retransmissão DHCP retira as informações da Opção 82 e encaminha esse pacote ao cliente.

Agora, o cliente descobriu o servidor DHCP e começa a enviar um pacote DHCPREQUEST para solicitar um endereço IP.

Após o recebimento do pacote DHCPREQUEST, o switch que funciona como agente de retransmissão DHCP adiciona informações da Opção 82 ao pacote e as encaminha para o servidor DHCP.

Após o recebimento do pacote DHCPREQUEST que contém informações da Opção 82, o servidor DHCP aloca um endereço IP para o cliente. Se o endereço IP solicitado não estiver disponível ou o ciclo de vida da concessão expirar, o servidor responderá com um pacote DHCPNAK. Caso contrário, o servidor responderá com um

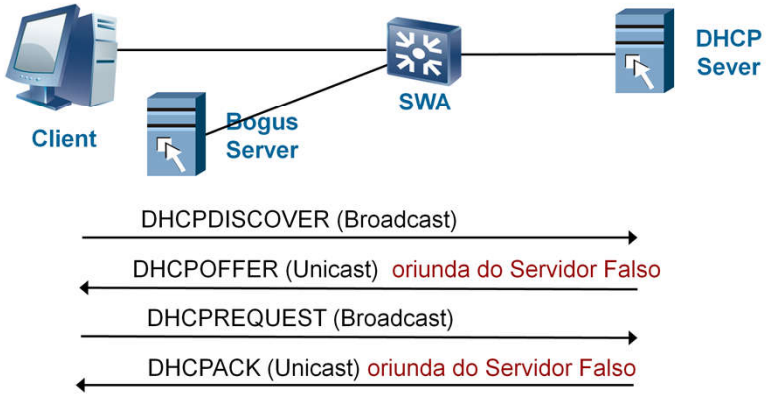
pacote DHCPACK, que contém informações da Opção 82.

Após o recebimento do pacote DHCPACK que contém informações da Opção 82, o switch que funciona como agente de retransmissão DHCP retira as informações da Opção 82 e encaminha o pacote DHCPACK ao cliente.

Após a conclusão do processo de solicitação de endereço, o cliente pode trocar dados com outras pessoas.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping(1)
  - ⇨ Ataque de Servidor DHCP Falso

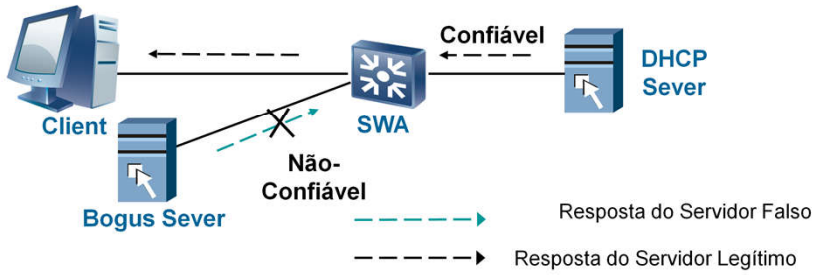


  HUAWEI

Pacotes DHCP REQUEST são enviados no modo de transmissão. O servidor DHCP falso pode, assim, ouvir os pacotes de solicitação de DHCP. O servidor DHCP falso responde com pacotes incorretos com o endereço IP incorreto do gateway, servidor DNS incorreto e endereço IP incorreto para o cliente DHCP. Isso causa a negação de serviço (DoS).

DHCP Snooping (Con.)

- Aplicação de DHCP Snooping (1)
  - ⇨ Solução para ataques de servidor DHCP falso

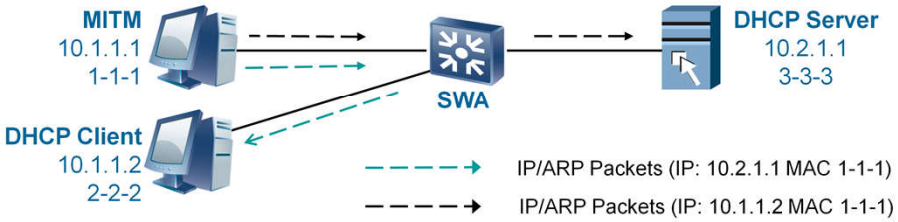


- Geralmente, interfaces conectando-se ao servidor DHCP (interfaces do lado da rede conectando-se a uma intranet) para Trusted e outras interfaces (interfaces do lado do usuário conectando-se a uma extranet) ao Não-confiável.

Para evitar ataques falsos ao servidor DHCP, você pode configurar interfaces confiáveis e não confiáveis.
Você pode definir uma interface física ou VLAN como Confiável ou Não Confiável. As mensagens de resposta do DHCP (mensagens OFERTA, ACK ou NAK) recebidas de uma interface não confiável são descartadas diretamente, para que os ataques do servidor DHCP falso possam ser evitados.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping (2)
  - ⇨ Ataques do homem-do-meio e falsificação IP/MAC



Exibir entradas ARP do cliente DHCP e do servidor DHCP. As seguintes informações são exibidas:

Entrada ARP no cliente DHCP: 00-01-00-01-00-01

Entrada ARP no servidor DHCP: 00-01-00-01-00-01

  HUAWEI

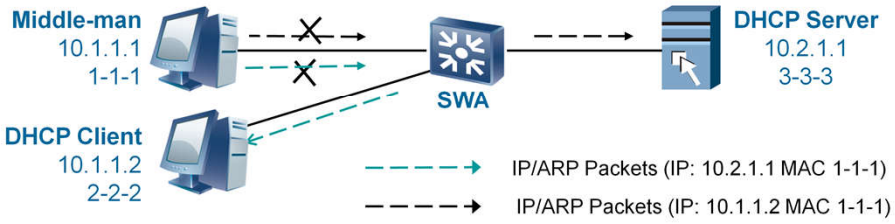
Conforme mostrado na figura, um MITM faz com que o servidor DHCP aprenda o endereço IP do cliente DHCP, 10.1.1.2, e seu próprio endereço MAC, 1-1-1, enviando um pacote IP ou ARP. Da perspectiva do servidor DHCP, todos os pacotes são de ou para o cliente DHCP, embora todos os pacotes sejam processados pelo MITM.

O MITM reenvia um pacote IP ou ARP, fazendo com que o cliente DHCP aprenda o endereço IP do servidor DHCP, 10.2.1.1, e seu próprio endereço MAC, 1-1-1. Da perspectiva do cliente DHCP, todos os pacotes são de ou para o servidor DHCP, embora todos os pacotes sejam processados pelo MITM.

Dessa maneira, o MITM se disfarça de servidor DHCP e cliente DHCP e obtém informações de interação entre o servidor DHCP e o cliente DHCP.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping(2)
  - ⇨ Solução para ataques do homem-do-meio e falsificação IP/MAC



Para impedir o ataque MITM ou o spoofing IP / MAC, você pode configurar a função de DHCP snooping no switch. A função de tabela de ligação do DHCP snooping permite o encaminhamento de um pacote recebido somente seja feto quando seu conteúdo é consistente com o da tabela de ligação. Se o conteúdo for inconsistente, o pacote será descartado.

  HUAWEI

Quando o switch recebe um pacote ARP ou IP em uma interface, ele combina o endereço IP de origem e o endereço MAC de origem do pacote com as entradas na tabela de ligação de espionagem DHCP. Quando a política forte é configurada, o switch descarta o pacote IP se nenhuma entrada correspondente for encontrada.

Um usuário que usa um endereço IP estático não possui uma entrada de ligação de DHCP snooping correspondente no switch porque o usuário não obtém o endereço IP enviando uma mensagem de solicitação de DHCP. Portanto, os pacotes ARP ou IP enviados desse usuário são descartados para impedir que o usuário use recursos de rede. Para permitir que os usuários com endereços IP alocados estaticamente acessem a rede, você deve configurar uma tabela de ligação de espionagem DHCP estática.

Um usuário que desvie um endereço IP válido de outro cliente também obtém o endereço IP sem enviar uma mensagem de solicitação DHCP; portanto, o endereço MAC e a interface deste usuário não correspondem à entrada correspondente ao endereço IP na tabela de ligação de espionagem DHCP. Em seguida, os pacotes IP enviados pelo fraudador são descartados e o fraudador não pode acessar a rede.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping(3)
  - ⇨ Ataque de exaustão DHCP
    - Princípio do ataque: em um ataque de exaustão do DHCP, o atacante muda constantemente o endereço físico, tentando esgotar todos os endereços IP no pool de endereços do servidor DHCP e fazendo com que outros usuários normais não consigam obter endereços IP.
    - Solução: A função de limitação de endereço MAC pode impedir o ataque de exaustão do DHCP. Limitar o número máximo de endereços MAC que podem ser aprendidos na interface do switch pode impedir que os usuários enviem solicitações substantivas de DHCP alterando o endereço MAC e limitando o número de usuários conectados a uma interface.

  HUAWEI

A função de limitação de endereço MAC geralmente é implantada em um dispositivo de camada 2. Limitar o número máximo de endereços MAC que podem ser aprendidos na interface do switch pode impedir que os usuários enviem solicitações substantivas de DHCP alterando o endereço MAC e limitando o número de usuários conectados a uma interface.

Limitação de endereço MAC no modo QinQ:

Na prática, um cliente se conecta a uma rede através de um DSLAM (Digital Subscriber Line Access Multiplexer). O DSLAM isola clientes configurando VLANs diferentes para clientes. Além disso, para evitar a limitação do número total de VLAN (4094), o recurso QinQ é adotado para encapsular duas camadas de tags em pacotes dos clientes. Depois disso, se a função de limitação de endereço MAC for implantada no gateway, o gateway poderá limitar o número de endereços MAC com base nas tags de duas camadas.

DHCP Snooping (Con.)

- Aplicação de DHCP Snooping (4)
  - ⇨ Ataque de exaustão do DHCP alterando o Endereço de Hardware do Cliente (CHADDR)
    - − O invasor pode alterar o campo CHADDR carregado nas mensagens DHCP, mas não o endereço MAC de origem no cabeçalho do quadro para solicitar endereços IP continuamente. Se o dispositivo apenas verificar a validade dos pacotes com base no endereço MAC de origem no cabeçalho do quadro, o limite do endereço MAC poderá não ter efeito.
    - − Solução: Você pode configurar o DHCP Snooping no switch para verificar o campo CHADDR carregado em uma mensagem de Solicitação DHCP. Se o valor do campo em um pacote corresponder ao endereço MAC de origem no cabeçalho do quadro de dados, o pacote será encaminhado. Caso contrário, o pacote será descartado.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping (5)
  - ⇨ Princípio dos ataques ARP
    - − Os ataques ao ARP são de vários tipos e em vários modos. Os ataques podem ter como alvo um host ou um gateway. Os ataques podem ser realizados através de falsificação de endereços ou outros ataques. Os ataques podem se originar de vírus ou software ilegítimo.
    - − Causa dos ataques ARP: o protocolo ARP é inerentemente simples e aberto demais, sem nenhum meio de segurança, deixando muitas oportunidades para ataques de hackers.
    - − Impactos de ataques ARP: os ataques de falsificação de endereço ARP geralmente têm como alvo hosts individuais ou hosts em um escopo especificado. Portanto, o impacto é comparativamente pequeno. Os ataques ARP DDoS direcionados a dispositivos de gateway, no entanto, forçariam um grande número de usuários offline devido à localização especial de gateways em uma rede.

DHCP Snooping (Con.)

- Aplicação do DHCP Snooping(5)
  - ⇨ Solução para os Ataques ao ARP:
    - − No ambiente de rede em que o servidor DHCP é aplicado, crie portas confiáveis, cujos pacotes DHCP são monitorados para obter a tabela de ligação de endereço IP / MAC. Essa é uma base importante para o DHCP Snooping verificar ameaças à segurança IP / ARP. Na verdade, essa é uma mudança do foco de segurança, convertendo os problemas de segurança do ARP em outros problemas de segurança.
    - − O DHCP Snooping filtra todos os pacotes IP / ARP incompatíveis com base em tabelas de ligação geradas em portas confiáveis, verificando todos os pacotes IP / ARP. Isso melhora significativamente a capacidade anti-ataque.

Em um ambiente de rede em que o servidor DHCP é aplicado, o DHCP Snooping alcança um efeito melhor na prevenção de ataques. Isso ocorre porque o DHCP snooping muda o objeto de segurança do APR que não possui meios de segurança para o DHCP. O ambiente de aplicativos do servidor DHCP é mais seguro que o ambiente de aplicativos host. Portanto, portas confiáveis podem ser criadas e os pacotes DHCP dessas portas são monitorados para obter a tabela de ligação de endereço IP / MAC. Essa é uma mudança do foco de segurança, convertendo os problemas de segurança do ARP em outros problemas de segurança.

Conteúdo

Princípios de DHCP

DHCP Snooping

Configuração do DHCP

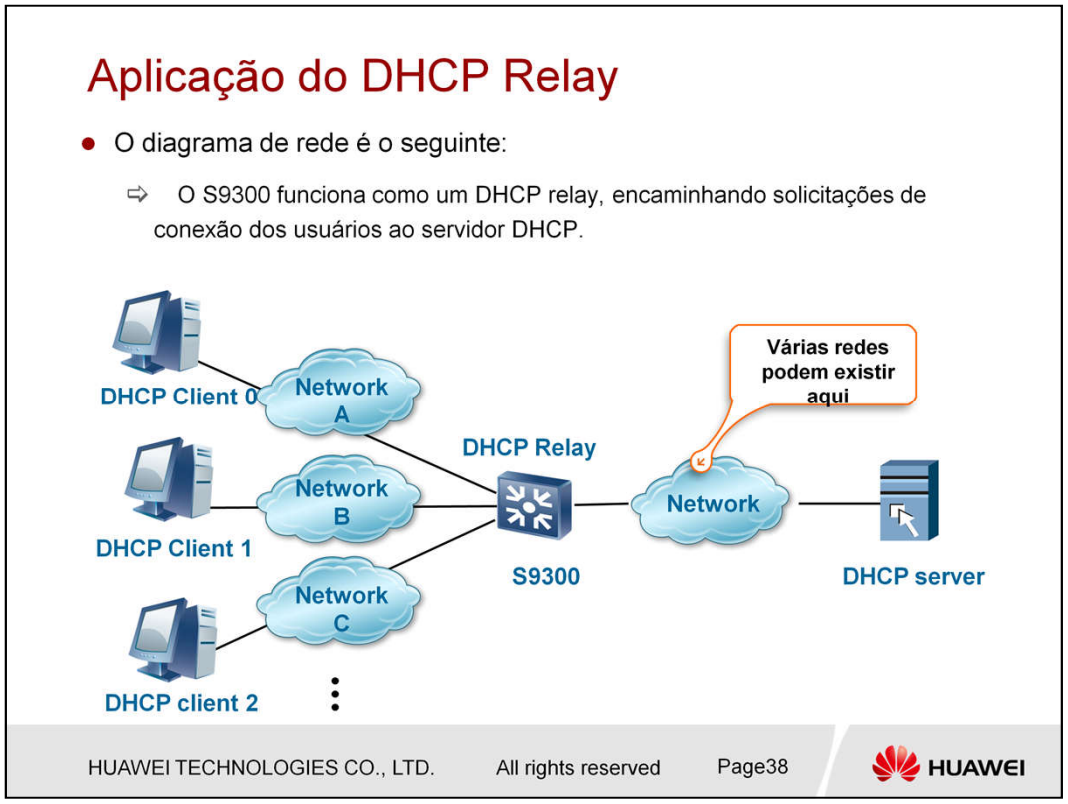
Conteúdo

Configuração do DHCP

3.1 Configuração do DHCP Relay configuration

3.2 Configuração de Servidor DHCP

3.3 Configuração do DHCP Snooping



Cenário de uso da retransmissão DHCP

Se nenhum servidor DHCP estiver configurado em uma rede, a função de retransmissão DHCP poderá ser ativada em um S9300. Dessa maneira, o pacote de Solicitação DHCP dos clientes pode ser transmitido ao servidor DHCP em outra rede através do agente de retransmissão DHCP. Para permitir que os clientes obtenham endereços IP, o servidor DHCP deve usar um pool de endereços global. Ou seja, a interface do servidor conectado ao agente de retransmissão DHCP não pode ser configurada com nenhum pool de endereços.

O pool de endereços da interface tem precedência sobre o pool de endereços global. Se um conjunto de endereços estiver configurado em uma interface, os clientes obterão endereços IP preferencialmente do conjunto de endereços da interface, mesmo que um conjunto de endereços global esteja configurado.

Você pode configurar até 64 grupos de servidores DHCP no sistema,

Você pode configurar no máximo oito servidores DHCP em um grupo de servidores DHCP. Se nenhum índice for especificado, o sistema alocará automaticamente um índice inativo.

Depois que a função de retransmissão DHCP está ativada na interface VLANIF do S9300, a interface VLANIF retransmite os pacotes ao agente de retransmissão DHCP.

O número de retransmissões de pacotes DHCP entre um servidor DHCP e um cliente DHCP não pode exceder 4. Caso contrário, o pacote DHCP será descartado.

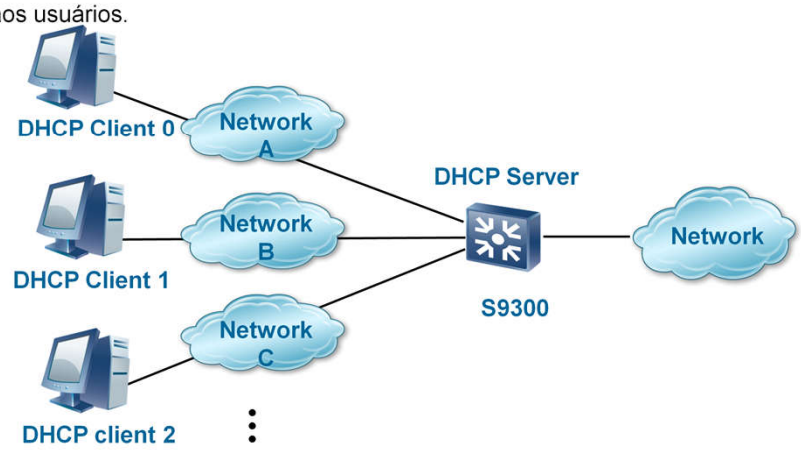
Se a retransmissão DHCP estiver ativada em uma super VLAN, a espionagem DHCP não poderá ser ativada nessa super VLAN.

Um grupo de servidores DHCP pode corresponder a várias interfaces VLANIF, enquanto apenas um grupo de servidores DHCP pode ser especificado para uma interface VLANIF. Ou seja, as mensagens de solicitação de DHCP em uma interface VLANIF podem ser retransmitidas para apenas um servidor DHCP.

Aplicação do Servidor DHCP

- O diagrama de rede é o abaixo:

O S9300 funciona como um servidor DHCP, alocando endereços IP aos usuários.



Implante serviços perto de usuários na rede distribuída. Como ponto de convergência, o S9300 atribui endereços IP aos usuários por meio do servidor DHCP local ou do servidor DHCP remoto para finalizar os clientes no S9300.

Configuração do Servidor DHCP

- Configure o servidor DHCP no S9300:

```
⇨dhcp enable
```

Ative o DHCP.

```
⇨interface vlanif 10
    ip address 192.168.1.1 24
    dhcp select global
```

Configure o servidor DHCP com base no pool de endereços global.

(Configure o pool de endereços global se o servidor DHCP com base no pool de endereços global for usado.)

  HUAWEI

Quando o S9300 funciona como um servidor DHCP, você pode definir o modo de processamento dos pacotes DHCP cujos endereços de destino são o endereço IP do dispositivo local. O S9300 pode atribuir endereços IP através do pool de endereços global ou do pool de endereços da interface.

O cliente e o S9300 precisam estar localizados na mesma sub-rede e cada interface pode ser configurada com apenas um modo de processamento.

Configuração do Servidor DHCP (Con.)

- Configure o servidor DHCP no S9300 : (con.)

```
⇨interface vlanif 10
    ip address 192.168.1.1 24
    dhcp select interface
```

Configure o servidor DHCP com base no pool de endereços de uma interface VLANIF.

(O pool de endereços da interface tem precedência sobre o pool de endereços global.)

```
dhcp server ping packets 5
```

(Opcional) Impedir a alocação repetitiva de um endereço IP.

Se um servidor DHCP baseado em um pool de endereços global estiver configurado, os usuários que estiverem online através de qualquer interface poderão obter endereços IP do pool de endereços global.

Configure o conjunto de endereços global:

ip pool 1

gateway-list 10.1.1.126

network 10.1.1.0 mask 255.255.255.128

dns-list 10.1.1.2Se um servidor DHCP baseado em um conjunto de endereços da interface estiver configurado, todos os usuários que estiverem online através dessa interface obterão endereços IP do conjunto de endereços da interface. O endereço do gateway é o endereço IP desta interface.

O pool de endereços da interface tem precedência sobre o pool de endereços global. Se um conjunto de endereços estiver configurado em uma interface, os clientes obterão endereços IP preferencialmente do conjunto de endereços da interface, mesmo que um conjunto de endereços global esteja configurado.

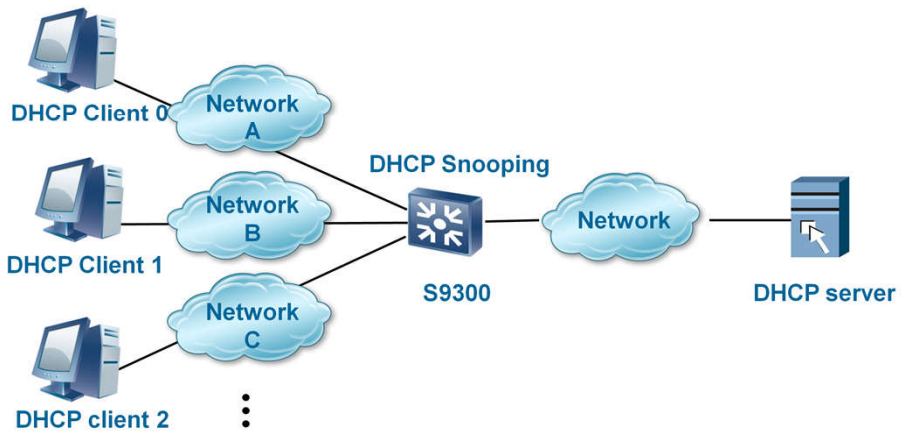
O servidor DHCP pode enviar pacotes de ping para verificar se um endereço IP está em uso. Isso evita a alocação repetitiva de um IP.

Por padrão, o número máximo de pacotes de ping é 5 e o maior tempo de espera de resposta de cada pacote de ping é 0.

Aplicação do DHCP Snooping

- O diagrama é o seguinte:

Habilite o DHCP snooping no S9300 para evitar ataques falsos ao servidor DHCP.



  HUAWEI

A função do switch da camada 2 e o recurso de roteamento da camada 3 são suportados. Nos dois cenários de aplicativos, o DHCP snooping pode ser configurado.
Quando o S9300 é implantado em uma rede da camada 2 ou funciona como um DHCP relay, a ativação do espião DHCP pode impedir ataques de DHCP. A única diferença na configuração é que o S9300 como um DHCP relay suporta a interação ARP e DHCP, que não está disponível quando o S9300 é implantado na camada 2.

Configuração do DHCP Snooping

- Configure a espionagem de DHCP no S9300 (contra ataques de servidor DHCP falsos):

```
⇨ dhcp enable
  # Ative o DHCP globalmente.
⇨ dhcp snooping enable
  # Ative a Opção 82 do DHCP e oDHCP snooping em uma interface.
⇨ interface GigabitEthernet3/0/0
  dhcp option82 insert enable
  dhcp snooping enable
  #  Ative o DHCP snooping em uma interface ou uma VLAN.
⇨ interface GigabitEthernet3/0/0
    dhcp snooping trusted
  # Configure uma interface como confiável.
```


Para habilitar a espionagem DHCP, você precisa seguir a seguinte sequência:

Habilite o DHCP globalmente.
Habilite a espionagem de DHCP globalmente.
Habilite a espionagem DHCP em uma interface ou em uma VLAN.

Questões

1. Qual a função básica do DHCP?
2. Como funciona o DHCP e quais são os pacotes básicos?
3. Qual a função do DHCP snooping?
4. Qual a função da Opção 82?

  HUAWEI

1. O princípio básico do DHCP é que o host obtenha a configuração de rede e o endereço IP correspondentes por meio da interação dinâmica de pacotes.

2. Procedimento básico do DHCP: Um host envia um pacote DHCPDISCOVER para encontrar um servidor DHCP. O servidor DHCP responde com um pacote DHCPOFFER. Em seguida, o host envia um pacote DHCPREQUEST para solicitar um endereço IP. Após o recebimento da solicitação, o servidor responde com um pacote DHCPACK. Quando 50% do ciclo de vida da concessão expirou, o host envia um pacote DHCPREQUEST para renovar a concessão. Se a solicitação de renovação de concessão for rejeitada, ele envia um pacote DHCPREQUEST novamente para renovar a concessão quando 87,5% do ciclo de vida da concessão expirar.

3. Evitar que DHCP ilegítimos possa emprestar IP para clientes dentro de uma rede.

4. A função da opção 82 é encapsular informações de localização para a implementação de políticas de segurança e QoS.

Thank you

www.huawei.com