

Prof. Esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp
- **Consultor de Tecnologia - [aXR6] Cyber Security e NtecSoftware**
- **Professor no Senac (contratado)**
- **Professor na Wyden Facimp (contratado)**
 - **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor na Wyden Facimp (Efetivado)**
 - **Graduação:** Análise e desenvolvimento de sistemas - Wyden Facimp

Redes sociais:

- **Linkedin:** <https://www.linkedin.com/in/thalles-canela/>
- **YouTube:** <https://www.youtube.com/aXR6CyberSecurity>
- **Facebook:** <https://www.facebook.com/axr6PenTest>
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** <https://github.com/ThallesCanela>
- **Github:** <https://github.com/aXR6>
- **Twitter:** <https://twitter.com/Axr6S>

Protocolo DHCP

- **O protocolo DHCP é um protocolo de cliente/servidor que fornece automaticamente um host ip (protocolo IP) com seu endereço IP e outras informações de configuração relacionadas, como a máscara de sub-rede e o gateway padrão.**

Obs.: As RFCs 2131 e 2132 definem o DHCP como um padrão de IETF (Força-Tarefa de Engenharia da Internet) com base no protocolo BOOTP, um protocolo com o qual o DHCP compartilha muitos detalhes de implementação. O DHCP permite que os hosts obtenham informações de configuração TCP/IP necessárias de um servidor DHCP.

Observações - Part. 1

- Entender com detalhes o funcionamento do protocolo DHCP pode ajudar você na identificação de problemas nos endereços IP dos seus computadores.
- O correto mapeamento dos seus ativos de rede é valioso quando ocorrem incidentes, visto que ajudam na restauração dos serviços críticos sem gerar impactos negativos no seu negócio.

Observações - Part. 2

- O DHCP combinado com diferentes protocolos de rede permite endereços IP diferentes para cada conexão de internet. Utiliza-se, para tanto, as arquiteturas do modelo cliente-servidor.

Observações - Part. 3

- Primeiramente, o cliente se conecta a uma rede e envia um pacote com um pedido de configuração de endereço IP. O servidor DHCP gerencia uma faixa fixa de endereços disponíveis com os parâmetros: gateway padrão, nomes de domínios e DNS.

Observações - Part. 4

- O DHCP é integrável com várias plataformas e é uma solução bem eficaz para os administradores de rede. Entender o seu correto funcionamento pode evitar muitas brechas de segurança na sua infraestrutura.

Observações - Part. 5

- Vale lembrar que o servidor DHCP distribui os endereços IP e serve de base para todos os pedidos DHCP dos computadores clientes. Logo, esse servidor precisa de um IP fixo.

Observações - Part. 6

- Quando se inicializa uma máquina, não há nenhuma configuração de rede definida ainda. Então, utiliza-se o broadcast para encontrar e se comunicar com o servidor DHCP. O computador envia um pacote broadcast com os parâmetros tipo de pedido e portas de conexão da rede local.

Observações - Part. 7

- Ao receber esse pacote, o servidor DHCP devolve ao cliente outro pacote broadcast com todas as informações pedidas. Não dá para contatar o cliente diretamente.

Há vários tipos de pacotes DHCP trocados entre clientes e servidor.

- **DHCPDISCOVER:** serve para encontrar quais servidores DHCP estão disponíveis.
- **DHCPOFFER:** uma resposta do servidor para os pacotes DHCPDISCOVER que têm os primeiros parâmetros da conexão.
- **DHCPREQUEST:** pedidos dos clientes para prolongar o tempo de aluguel do endereço IP.
- **DHCPACK:** uma resposta do servidor com os parâmetros e o IP do computador do cliente.
- **DHCPNAK:** uma resposta do servidor para informar o término do aluguel ou uma configuração inadequada da rede.
- **DHCPDECLINE:** uma mensagem do cliente para informar ao servidor que já houve uso do endereço IP.
- **DHCPRELEASE:** uma liberação do endereço IP pelo cliente.
- **DHCPINFORM:** um pedido pelo cliente com endereço IP dos parâmetros locais.

Como funciona?

1. O primeiro pacote que o cliente envia é o DHCPDISCOVER. O servidor responde com um DHCPOFFER, que apresenta um IP ao cliente.
2. O cliente define a sua configuração e realiza um DHCPREQUEST para validar o endereço IP. Trata-se de um pedido broadcast, pois o DHCPOFFER não carrega o endereço IP.
3. O servidor responde com um DHCPACK, com o endereço IP que confirma a atribuição do IP ao computador do cliente. No geral, bastam esses passos para o cliente configurar sua máquina na rede. O processo pode demorar mais um pouco se o cliente não aceitar o endereço IP.

As concessões ativas do DHCP

- Para racionalizar os recursos da rede, são emitidos endereços IP com datas de início e fim — esse é o processo de concessão.
- Ao perceber que a concessão do endereço IP chegou ao fim, o cliente pode solicitar ao servidor DHCP um prolongamento por meio do pacote DHCPREQUEST. Da mesma forma, se o servidor observar que uma concessão de IP já terminou, ele pode enviar um pacote DHCPNAK para perguntar ao cliente se quer prolongá-la.
- Caso o servidor não receba uma resposta válida, ele torna o endereço IP disponível para atribuição. Algumas bibliografias chamam a concessão de aluguel.

As concessões ativas do DHCP

- O detalhe do DHCP é que conseguimos otimizar a atribuição dos endereços IP aos computadores de acordo com o tempo de duração das concessões. Se não houver liberação de endereços IP depois de um certo tempo, não será possível atender aos outros pedidos por não haver endereços para distribuir.
- Em redes com muitos dispositivos fixos, as concessões de longa duração já atendem. Vale lembrar que o DHCP opera via broadcast, e isso pode sobrecarregar a banda larga em redes pequenas com alta atividade.

Quais são os modos de funcionamento do DHCP?

- Quando o servidor DHCP recebe o pedido, ele disponibiliza os endereços e as configurações para a máquina do cliente. Opera-se de 3 formas: automática, dinâmica e manual.

Automática

- No modo automático, define-se uma quantidade de endereços IP de uma faixa para se utilizar na rede — de 192.168.0.51 a 192.168.0.90, por exemplo. Sempre que um computador solicita uma conexão, designa-se um IP que não está em utilização por outra máquina.

Dinâmica

- A configuração dinâmica tem um funcionamento bem parecido com o da automática. A diferença é que a conexão do computador com um endereço IP tem um limite de tempo predefinido, que varia conforme as configurações montadas pelo administrador de rede.
- Independentemente do endereço MAC do computador, atribui-se um endereço IP disponível. A ideia é tornar essa configuração mais rápida mesmo.

Manual

- Na configuração manual, o protocolo DHCP aloca os IPs de acordo com o MAC (Medium Access Control) das placas de rede. Cada computador utiliza apenas esse endereço IP. A ideia é usar o DHCP manual apenas quando as máquinas precisam de um endereço IP fixo.
- Os administradores de redes configuram tabelas no servidor ou nos roteadores que contêm os endereços IP associados a cada endereço MAC. Se apenas os MAC conhecidos forem ligados aos IP e não houver regras adicionais, os computadores desconhecidos não vão receber um IP da rede, o que pode dificultar acessos indevidos por pessoas não cadastradas.

Por que usar o DHCP?

- Parâmetros de configuração TCP/IP válidos para todos os clientes na rede.
- Endereços IP válidos, mantidos em um pool para atribuição a clientes, bem como endereços excluídos.
- IP Reservado endereços associados a clientes DHCP específicos. Isso permite a atribuição consistente de um único endereço IP para um único cliente DHCP.
- A duração da concessão ou o período de tempo para o qual o endereço IP pode ser usado antes que uma renovação de concessão seja necessária.
- Um cliente habilitado para DHCP, após aceitar uma oferta de concessão, recebe:
- Um endereço IP válido para a sub-rede à qual ela está se conectando.
- Opções DHCP solicitadas, que são parâmetros adicionais que um servidor DHCP está configurado para atribuir aos clientes. Alguns exemplos de opções de DHCP são Roteador (gateway padrão), Servidores DNS e Nome de Domínio DNS.

Benefícios do DHCP

- **Configuração de endereço IP confiável.** O DHCP minimiza os erros de configuração causados pela configuração manual de endereço IP, como erros tipográficos ou conflitos de endereço causados pela atribuição de um endereço IP a mais de um computador ao mesmo tempo.

Benefícios do DHCP

- **Administração de rede reduzida.** O DHCP inclui os seguintes recursos para reduzir a administração de rede:
 - Configuração TCP/IP centralizada e automatizada.
 - A capacidade de definir configurações de TCP/IP de um local central.
 - A capacidade de atribuir um intervalo completo de valores de configuração TCP/IP adicionais por meio de opções DHCP.
 - O tratamento eficiente de alterações de endereço IP para clientes que devem ser atualizados com frequência, como aqueles para dispositivos portáteis que se movem para locais diferentes em uma rede sem fio.
 - O encaminhamento de mensagens DHCP iniciais usando um agente de retransmissão DHCP, que elimina a necessidade de um servidor DHCP em cada sub-rede.

Atividade:

- Qual é o seu papel nas empresas de TI?