



# PROTOCOLOS DE CONTROLE

## Principais protocolos de controle

### Protocolo de controle da Internet

O protocolo IP é o responsável por manter a unidade de toda a Internet, porém, ele não consegue realizar sozinho todo o trabalho necessário. Para auxiliá-lo nessa tarefa, foram desenvolvidos protocolos auxiliares na camada de rede, conhecidos como protocolos de controle.

Neste módulo, estudaremos os principais protocolos de controle que trabalham em conjunto com o protocolo IP.

### **ARP (*Address Resolution Protocol*)**

Embora na Internet cada hospedeiro possua um ou mais endereços IP, na verdade eles não podem ser usados diretamente para o envio de informações pela rede, pois o hardware da camada de enlace de dados não entende os endereços Internet.

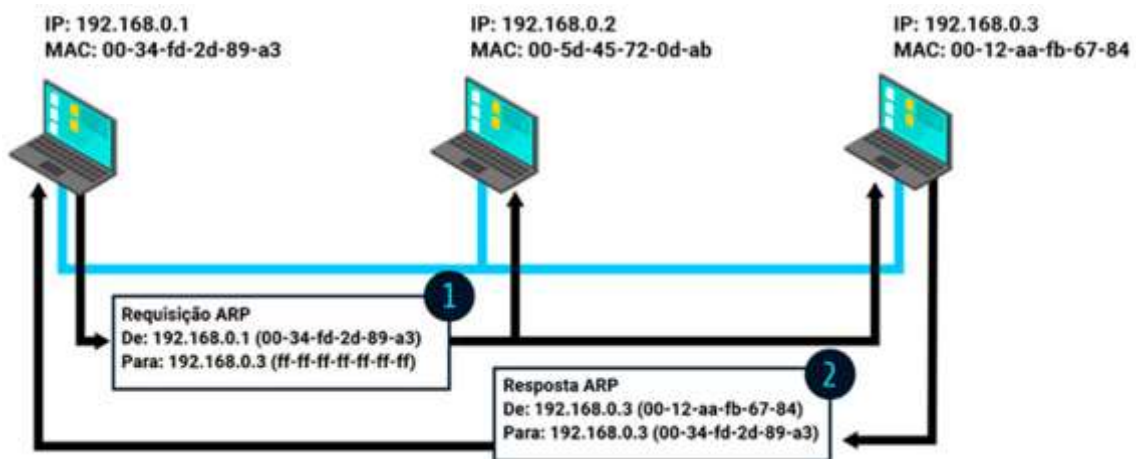


Suponha que você esteja utilizando um notebook e que ele enviará dados para um servidor na mesma rede. O software IP do notebook receberá os dados a serem enviados e construirá um pacote com o endereço IP do servidor no campo ENDEREÇO DESTINO do datagrama para transmissão. O software IP descobrirá que o servidor está em sua própria rede e que, portanto, deverá transmitir os dados diretamente a ele.

Neste ponto existe um problema. A placa de rede trabalha com endereços físicos da camada de enlace, ela não reconhece endereços IP. Logo, é necessário encontrar uma forma de mapear os endereços de rede nos endereços de enlace.

A solução adotada é fazer com que o hospedeiro que precise descobrir o endereço de enlace do destinatário envie um pacote por difusão perguntando: “A quem pertence o endereço IP A.B.C.D?”. Então, o hospedeiro destinatário responderá com seu endereço de enlace. O protocolo que faz essa pergunta e obtém a resposta é o ARP (*Address Resolution Protocol*, que é definido na RFC 826).

No exemplo da imagem a seguir, a requisição ARP é enviada para o endereço de enlace ff-ff-ff-ff-ff-ff, o que permite que a camada de enlace promova uma difusão (entregue a requisição a todos os hospedeiros ligados ao meio de transmissão).



Continuando em nosso exemplo, o software IP do notebook constrói um quadro de enlace endereçado ao servidor, coloca o pacote IP no campo de carga útil e o envia. A placa de rede do destinatário detecta esse quadro, reconhece-o como um quadro destinado a ela e o recolhe. O software de enlace extrai o pacote IP da carga útil e o repassa para o software IP, que verifica se ele está corretamente endereçado e o processa.

São possíveis várias otimizações para tornar o arp mais eficaz. Em primeiro lugar, depois que uma máquina executa o ARP, ela armazena o resultado em um cache.

Em muitos casos, o destinatário precisará enviar uma resposta, o que forçará também a execução do ARP para determinar o endereço de enlace do transmissor. Essa difusão do ARP pode ser evitada fazendo-se com que o destinatário inclua em sua tabela o mapeamento entre os endereços de rede e de enlace do transmissor.

Se um hospedeiro precisar enviar dados para outro hospedeiro que se encontra em uma sub-rede diferente da sua, esse sistema de entrega direta não funcionará. Nesse caso, o hospedeiro transmissor precisará enviar seus dados para um roteador, que deverá providenciar o encaminhamento do datagrama para a sub-rede do destinatário. Poderá ser necessário que o protocolo ARP seja utilizado mais de uma vez ao longo do caminho.

## Configuração automática de endereços

### **DHCP (*Dynamic Host Configuration Protocol*)**

Para ter acesso à Internet, um hospedeiro precisa ser configurado com alguns parâmetros.

Os parâmetros mínimos a serem configurados são:

#### **Endereço IP**

Para permitir que o hospedeiro possa ser endereçado e receber dados de outro hospedeiro.

#### **Máscara de sub-rede**

Para que o hospedeiro possa determinar qual a sua sub-rede.

#### **Endereço do gateway (roteador)**

Para que o hospedeiro possa enviar informações para fora de sua sub-rede.

#### **Endereço do servidor DNS**

Para que o hospedeiro possa acessar outros hospedeiros por seus nomes em vez de precisar conhecer seus endereços IP.

Esses parâmetros devem ser configurados em todos os hospedeiros da organização, o que pode ser feito manualmente pelos administradores da rede. Isso funcionaria muito bem em um ambiente relativamente estático onde os hospedeiros raramente fossem mudados de lugar ou trocados.

E no caso de ambientes onde existe uma grande variação nos hospedeiros presentes na rede?

Imagine, por exemplo, como seria na praça de alimentação de um shopping que oferece acesso à Internet. Seria viável solicitar que todo o dispositivo móvel que chegasse nesse shopping e quisesse acessar a Internet fizesse um pré-cadastro para poder ter esse acesso? Como cada dispositivo precisa de um endereço único no momento do acesso, como seria administrar essa distribuição por todos os possíveis clientes?



Para facilitar a distribuição de endereços IP e demais parâmetros de rede entre os vários hospedeiros que podem estar presentes em uma rede, e administrar a atribuição desses parâmetros de forma automatizada, a IETF desenvolveu o DHCP, cuja especificação encontra-se na RFC 2131.

Para utilizar o mecanismo dinâmico de alocação de endereços do DHCP, o administrador do sistema deve configurar um servidor fornecendo um grupo de endereços IP. Sempre que um novo computador se conecta à rede, entra em contato com o servidor e solicita um endereço. O servidor opta por um dos endereços especificados pelo administrador e aloca tal endereço para o computador.

De modo geral, o **DHCP** permite três tipos de atribuição de endereços:

## 1. Configuração manual

O administrador especifica o endereço que cada hospedeiro receberá quando se conectar à rede.

## 2. Configuração automática

O administrador permite que um servidor DHCP atribua um endereço quando um hospedeiro se conectar pela primeira vez à rede. A partir desse momento, esse endereço estará reservado para esse hospedeiro para sempre.

## 3. Configuração dinâmica

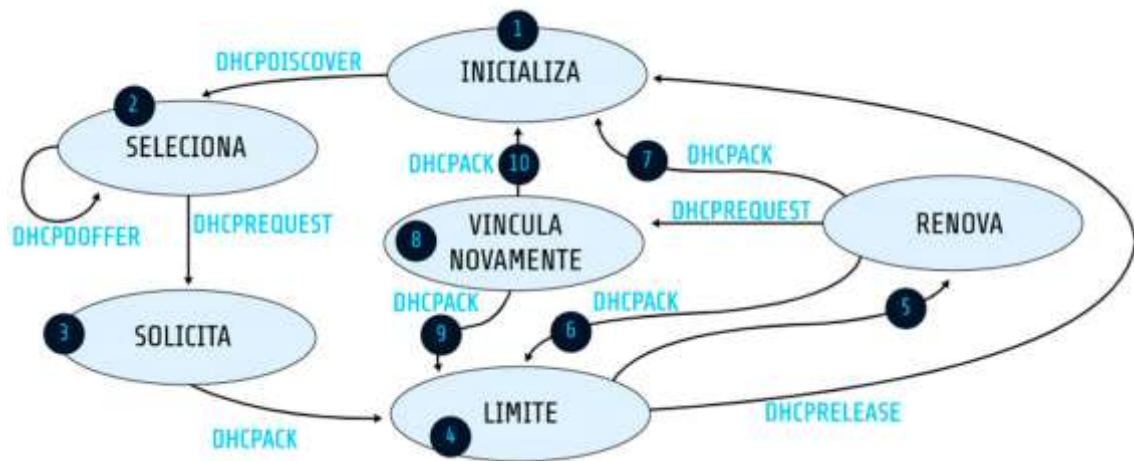
O servidor “empresta” um endereço a um hospedeiro, por um tempo limitado. Quando o hospedeiro não estiver mais utilizando esse endereço, ele poderá ser alocado a outro hospedeiro.

Um servidor DHCP empresta um endereço para o hospedeiro por um período de tempo determinado que ele especifica ao alocar o endereço. Durante esse período, o servidor não alocará o mesmo endereço a outro cliente, entretanto, quando a alocação terminar, o cliente deverá renová-la ou cancelar o uso do endereço.

O período ideal de alocação depende da rede e das necessidades de um hospedeiro em particular. O DHCP não especifica uma quantidade de tempo para o período de alocação. O protocolo permite que um cliente solicite um tempo de alocação específico e que um servidor informe ao cliente quanto tempo de alocação lhe será concedido. Fica a cargo do administrador determinar esse tempo.

## Funcionamento do DHCP

A figura mostra os seis estados em que um cliente DHCP pode estar:



Entenda o que ocorre em cada etapa:

## 1. Inicializa

Quando um cliente faz a primeira inicialização, ele entra no estado INICIALIZA. Para dar início à aquisição de um endereço IP, o cliente primeiro entra em contato com todos os servidores DHCP da rede local difundindo uma mensagem DHCPDISCOVER, utilizando para isso a porta 67 do protocolo UDP, que é o protocolo de transporte da Internet sem conexões.

## 2. Selecciona

Após, ele passa para o estado SELECIONA. Os servidores da rede local recebem a mensagem e enviam, cada um, uma mensagem DHCPOFFER. As mensagens DHCPOFFER contêm informações de configuração e o endereço IP oferecido pelo servidor.

O cliente, assim, selecciona um dos servidores e lhe envia uma mensagem DHCPREQUEST, solicitando uma alocação.

## 3. Solicita

Em seguida, vai para o estado SOLICITA. O servidor responde com a mensagem DHCPACK, dando início à alocação. O cliente segue então para o estado LIMITE, que é o estado normal de operação.

## 4. Limite

Uma vez no estado LIMITE, o cliente configura três temporizadores que controlam a renovação, a revinculação e o fim da alocação. Um servidor DHCP pode especificar os valores explícitos para os temporizadores, caso contrário o cliente utiliza o padrão. O valor padrão para o primeiro temporizador é a metade do valor do tempo total da alocação.

## 5. Renova

Quando o temporizador ultrapassar o tempo determinado pela primeira vez, o cliente deverá tentar renovar a alocação. Para solicitar uma renovação, o cliente transmite uma mensagem DHCPREQUEST ao servidor que lhe fez a alocação. Em seguida, muda para o estado RENOVA para aguardar uma resposta.

O servidor pode responder de dois modos: instruindo o cliente a não utilizar mais o endereço ou autorizando-o a prolongar o uso.

## 6. Limite

Caso aprove a renovação, o servidor transmite um DHCPACK, o que faz o cliente retornar ao estado LIMITE e continuar com o uso do endereço.

## 7. Inicializa

Se um servidor não aprovar a renovação do endereço, ele envia um DHCPNACK, que faz com que o cliente interrompa imediatamente o uso do endereço e retorne ao estado INICIALIZA.

## 8. Vincula novamente

Caso o cliente esteja no estado RENOVA e não chegue nenhuma resposta, provavelmente o servidor que concedeu a alocação estará fora de alcance. Para contornar essa situação, o DHCP conta com um segundo temporizador, que expira após 87,5% do período da alocação e faz com que o cliente mude o estado VINCULA NOVAMENTE.

## 9. Limite

Ao fazer essa transição, o cliente passa a difundir a mensagem DHCPREQUEST para qualquer servidor da rede local. Caso receba uma resposta positiva, o cliente retorna ao estado LIMITE e reconfigura os temporizadores.

## 10. Inicializa

Se a resposta for negativa, o cliente deve mudar para o estado INICIALIZA e interromper imediatamente o uso do endereço IP.

Quando um cliente não precisa mais da alocação, o DHCP permite que ele a encerre sem precisar esperar que o prazo da validade termine. Para isso, o cliente envia uma mensagem DHCPRELEASE ao servidor. Depois de enviar a mensagem, o cliente deixa o estado LIMITE e volta ao estado INICIALIZA.

## ICMP (*Internet Control Message Protocol*)

Durante o tráfego de informações pela rede, podem ocorrer **erros ou situações anormais** que precisam ser do conhecimento dos hospedeiros. Para permitir a troca desse tipo de informação, foi criado o **protocolo ICMP**. Com ele, hospedeiros conseguem enviar mensagens de controle e erros para outros hospedeiros. O erro sempre é reportado ao sistema que gerou o datagrama.

Além de oferecer a possibilidade de troca de informações sobre erros e de controle, o ICMP inclui um mecanismo de envio e resposta (echo) para testar quando um destino é alcançável ou não. O comando ping utiliza esse protocolo.

O ICMP é definido na RFC 792.

Uma mensagem ICMP é carregada dentro de um datagrama IP, ou seja, **as mensagens ICMP são transportadas pelo protocolo IP**. Existem diversas mensagens ICMP. **As mais importantes são:**

- *Destination unreachable* (destino inalcançável): datagrama não pode ser entregue. Usada quando a sub-rede ou um roteador não pode localizar o destino, ou um datagrama com o bit DF não pode ser entregue porque há uma rede de pacotes pequenos no caminho.
- *Time exceeded* (tempo excedido): campo tempo de vida do IP chegou a zero. Enviada quando um pacote é descartado porque seu contador chegou a zero. Esse evento é um sintoma de que os datagramas estão entrando em loop, de que há congestionamento ou de que estão sendo definidos valores muito baixos para o temporizador.
- *Parameter problem* (problema de parâmetro): campo de cabeçalho inválido. Essa mensagem indica existência de um problema no software IP do hospedeiro transmissor ou no software de um roteador pelo qual o pacote transitou.



- *Source quench* (redução de origem): conhecida como pacote regulador. Usada para ajustar os hospedeiros que estejam enviando pacotes demais a fim de controlar o congestionamento na rede.
- *Redirect* (redirecionar): usada quando um roteador percebe que o pacote pode ter sido incorretamente roteado. É usada pelo roteador para informar ao hospedeiro transmissor a respeito do provável erro.
- *Echo request* (solicitação de eco): perguntar a um hospedeiro se ele está ativo. Ao receber a mensagem *echo request*, o destino deve enviar de volta uma mensagem *echo reply*.
- *Echo reply* (resposta de eco): confirmação de que o hospedeiro está ativo.
- *Timestamp request* (solicitação de carimbo de data e hora): mesmo que *echo request*, mas solicita que a hora da chegada da mensagem e da partida da resposta sejam registradas na mensagem de resposta.
- *Timestamp reply* (resposta de carimbo de data e hora): resposta à mensagem *timestamp request*.