O IP (Internet Protocol)

---

1. Introdução

O IP foi desenvolvido como um protocolo com baixa sobrecarga, fornecendo apenas as funções necessárias para enviar um pacote e uma origem a um destino por um sistema interconectado de redes. As características básicas do IP são:

- **Sem conexão:** Não há conexão com o destino estabelecido antes do envio de pacotes de dados, o que significa que nenhuma conexão ponta a ponta dedicada é criada pelo IP antes que os dados sejam enviados.
- **Melhor esforço:** O IP é inerente e não confiável, porque a entrega de pacotes não é garantida. Os remetentes não sabem se os dispositivos de destino estão presentes e funcionais ao enviar pacotes, nem sabem se o destino recebe o pacote ou se o dispositivo de destino pode acessar e ler o pacote.
- **Independente da mídia:** A operação é independente do meio que carrega os dados.

Existe uma característica importante que a camada de rede considera, e esta é o tamanho máximo da PDU que cada meio consegue transportar. Essa característica também é chamada de ***Unidade Máxima de Transmissão*** (***MTU***). Parte das comunicações de controle entre a camada de enlace de dados e a camada de rede é a definição de um tamanho máximo para o pacote. A camada de enlace de dados passa o valor da MTU para a camada de rede. A camada de rede então determina o tamanho que os pacotes podem ter.

Um dispositivo intermediário, geralmente um roteador, deve dividir um pacote IPv4 ao encaminhá-lo de um meio para outro com uma MTU menor. Esse processo é chamado de fragmentação do pacote ou apenas fragmentação. O IP encapsula o segmento da camada de transporte ou outros dados adicionando um cabeçalho IP. Este cabeçalho é usado para entregar o pacote ao host de destino.

O cabeçalho IP é examinado por dispositivos de Camada 3 (roteadores/switches) à medida que viaja através de uma rede até seu destino. As informações de endereçamento IP permanecem as mesmas desde o momento em que o pacote sai do host de origem até chegar ao host de destino, exceto quando traduzido pelo dispositivo que executa NAT para IPv4.

Os roteadores implementam protocolos de roteamento para rotear pacotes entre redes. O roteamento realizado por esses dispositivos intermediários examina o endereçamento da camada de rede no cabeçalho do pacote. Em todos os casos, a parte de dados do pacote (PDU) da camada de transporte permanece inalterada durante o processo da camada de rede.

O pacote TCP/IP fornece mensagens de erro e mensagens informativas ao se comunicar com outro dispositivo IP denominado serviços do ICMP. O objetivo dessas mensagens é dar feedback sobre questões relativas ao processamento de pacotes IP sob certas condições, e não tornar o IP confiável. As mensagens ICMP não são necessárias e muitas vezes não são permitidas por questões de segurança.

O ICMP está disponível tanto para IPv4 como para IPv6. ICMPv4 é o protocolo de mensagens para o IPv4. O ICMPv6 fornece os mesmos serviços para o IPv6, mas inclui funcionalidade adicional.

As mensagens ICMP comuns ao ICMPv4 e ICMPv6 e discutidas neste módulo incluem: acessibilidade do host, destino ou serviço inalcançável e tempo excedido.

Uma mensagem de eco ICMP pode ser usada para testar a capacidade de acesso de um host em uma rede IP. O host local envia uma solicitação de eco ICMP para um host. Se o host estiver disponível, o host de destino enviará uma resposta de eco.

Alguns dos códigos de Destino inacessível para o ICMPv4 são os seguintes:

- 0 = ***Rede inalcançável***
- 1 = ***Host inalcançável***
- 2 = ***Protocolo inalcançável***
- 3 = ***Porta inalcançável***

Alguns dos códigos de Destino inacessível para o ICMPv6 são os seguintes:

- 0 = ***Nenhuma rota para o destino***
- 1 = ***A comunicação com o destino é administrativamente proíbida (firewall)***
- 2 = ***Além do escopo do endereço de origem***
- 3 = ***Endereço inacessível***
- 4 = ***Porta inalcançável***

Uma mensagem ICMPv4 de tempo excedido é usada por um roteador para indicar que um pacote não pode ser encaminhado porque o campo ***Vida Útil*** (***TTL***) do pacote foi reduzido a 0. Se um roteador recebe um pacote e o campo TTL do pacote IPv4 diminui para zero, ele descarta o pacote e envia uma mensagem de tempo excedido para o host de origem. O ICMPv6 também enviará uma mensagem de tempo excedido se o roteador não conseguir encaminhar um pacote IPv6 porque o pacote expirou. As mensagens ICMPv6 são encapsuladas no IPv6.

O ICMPv6 inclui quatro novos protocolos como parte do protocolo ND ou NDP.

- **RS:** Mensagem de solicitação de roteador
- **RA:** Mensagem de anúncio de roteador
- **NS:** Mensagem de solicitação de vizinho
- **NA:** Mensagem de anúncio de vizinho

2. Mensagem RA

As mensagens de RA são enviadas por roteadores habilitados para IPv6 a cada 200 segundos para fornecer informações de endereçamento para hosts habilitados para IPv6. A mensagem RA pode incluir informações de endereçamento para o host, como prefixo, comprimento do

prefixo, endereço DNS e nome de domínio. Um host que usa a Configuração Automática de Endereço sem Estado (SLAAC) definirá seu gateway padrão para o endereço local do link do roteador que enviou o RA

2.1 Mensagem RS

Um roteador habilitado para IPv6 também enviará uma mensagem RA em resposta a uma mensagem RS. Na figura abaixo, PC1 envia uma mensagem RS para determinar como receber suas informações de endereço IPv6 dinamicamente.

2.2 Mensagem NS

Quando um dispositivo recebe um endereço IP unicast global ou unicast local de link, um dispositivo pode receber DAD (***Detecção de Endereço Duplicado***) para garantir que o endereço IPv6 seja exclusivo.

2.3 Mensagem NA

É usada quando um dispositivo na LAN sabe o endereço IPv6 unicast de um destino, mas não seu endereço MAC Ethernet. Para determinar o endereço MAC destino, o dispositivo enviará uma mensagem de NS para o endereço do nó solicitado. A mensagem incluirá o endereço IPv6 (destino) conhecido. O dispositivo que tem o endereço IPv6 alvo responderá com uma mensagem de NA contendo seu endereço MAC Ethernet.

Para testar a conectividade com outro host em uma rede, uma solicitação de eco (***echo request***) é enviada ao endereço do host usando o comando **ping**. O ping tem um valor de tempo limite para a resposta. Se a resposta não é recebida dentro do tempo de espera, o ping mostra uma mensagem informando que a resposta não foi recebida. Isso pode indicar que há um problema, mas também pode indicar que os recursos de segurança que bloqueiam as mensagens de ping foram ativados na rede.

3. Tempo de ida e volta (RTT)

O uso do traceroute fornece tempo de ida e volta para cada salto ao longo do caminho e indica se um salto falha na resposta. O tempo de ida e volta é o tempo que um pacote leva para alcançar o host remoto e retornar a resposta do host. Um asterisco (*) é usado para indicar um pacote perdido ou não respondido.

4. Limite de salto IPv4 TTL e IPv6

O comando ***Traceroute*** utiliza uma função do campo TTL no IPv4 e do campo Limite de saltos no IPv6 nos cabeçalhos da camada 3, junto com a mensagem ICMP Time Exceed.

O tipo de testes de conectividade realizados com **ping** incluem o seguinte:

- Fazendo ping no loopback local
- Fazendo ping no gateway padrão
- Fazendo ping em um host remoto

O ping pode ser usado para testar a configuração interna do IPv4 ou IPv6 no host local. Para executar este teste, **ping** o endereço de loopback local 127.0.0.1 para IPv4 (:: 1 para IPv6). Uma resposta vinda de 127.0.0.1 para IPv4 (ou ::1 para IPv6) indica que o IP está instalado corretamente no host. Essa resposta vem da camada de rede.

Você também pode usar **ping** para testar a capacidade de um host de se comunicar na rede local. Isso geralmente é feito através do ping do endereço IP do gateway padrão do host. Um êxito **ping** no gateway padrão indica que o host e a interface do roteador servindo como gateway padrão estão operacionais na rede local. Se o gateway padrão ou outro host responder, o host local poderá se comunicar com êxito pela rede local. Se o gateway padrão não responder, mas outro host, isso pode indicar um problema com a interface do roteador servindo como gateway padrão.

O host local pode fazer ping em um host IPv4 operacional de uma rede remota. Se esse ping tiver êxito, a operação de uma grande parte da rede interconectada poderá ser verificada. Um êxito **ping** na rede confirma a comunicação na rede local, a operação do roteador que serve como gateway padrão e a operação de todos os outros roteadores que possam estar no caminho entre a rede local e a rede do host remoto.

Traceroute (***tracert - Windows***) é um utilitário que gera uma lista de saltos que foram alcançados com sucesso ao longo do caminho. Essa lista pode dar informações importantes para a verificação e a solução de erros.