Instituto Politécnico Cávado do Ave

Redes e Segurança Informática

ICMP

Hugo Azevedo, a25431

Braga, 2023

Índice

1. Introdução

Os protocolos de rede são responsáveis por permitir a comunicação entre dispositivos de rede e garantir que os dados sejam transmitidos de forma confiável e segura.

O protocolo ICMP (Internet Control Message Protocol) é um protocolo fundamental para o funcionamento da Internet e tem um papel importante na comunicação e monitoramento da rede. Como parte do protocolo IP, o ICMP é responsável por enviar mensagens de erro e notificação de volta aos dispositivos de origem quando ocorrem problemas durante a transmissão de dados. Essas mensagens são essências para manter a integridade e a segurança da rede além de ajudar os administradores de rede a identificar e corrigir problemas de conexão.

Neste relatório, serão apresentados a história, descrição, aplicações e exemplos de aplicações que usam o protocolo ICMP.

2. História do Protocolo ICMP

O ICMP é um protocolo de rede usado para enviar mensagens de controle e erro através de uma rede IP. Foi criado em 1981, juntamente com o Protocolo Internet (IP), como parte fundamental do conjunto de protocolos TCP/IP que formam a base da Internet moderna.

O objetivo inicial do ICMP era fornecer informações de rastreamento e erro, como mensagens de confirmação e roteamento, para ajudar a manter a rede IP funcionando corretamente. O protocolo foi projetado para permitir que os dispositivos de rede se comuniquem entre si para resolver problemas, identificar falhas e garantir que os dados possam ser entregues com êxito.

Desde o seu lançamento inicial, o ICMP passou por diversas atualizações e melhorias. Em 1985, o ICMPv2 foi introduzido para fornecer recursos adicionais de controle de congestionamento e roteamento. Esta versão foi atualizada em 1989 com a adição de mensagens de autenticação e segurança.

Com o tempo, o ICMP tornou-se parte integrante da Internet, desempenhando um papel fundamental no diagnóstico de problemas de rede, na comunicação entre dispositivos de rede e na gestão do tráfego de rede. O protocolo é frequentemente usado na ferramenta de diagnóstico "ping", que envia uma mensagem de solicitação de eco ICMP para um dispositivo na rede e aguarda uma resposta. O tempo de resposta é então medido, permitindo que os administradores de rede determinem a latência e a qualidade da conexão.

Além disso, o ICMP é usado em muitas aplicações do dia-a-dia, como navegação na web, envio de e-mails, videoconferências, transações bancárias e muito mais. Sem o ICMP, muitas dessas atividades simplesmente não funcionariam.

4. Descrição do Protocolo

4.1. Descrição detalhada do Protocolo ICMP

O principal objetivo do ICMP é o relatório de erros. Quando dois dispositivos se conectam pela internet, o ICMP gera erros para compartilhar com o dispositivo de envio, caso algum dos dados não chegue ao destino pretendido. Por exemplo, se um pacote de dados for muito grande para um router, o router descartará o pacote e enviará uma mensagem ICMP de volta para a fonte original dos dados.

As mensagens ICMP são enviadas dentro de pacotes IP e são identificadas por um campo Tipo e Código. Existem vários tipos de mensagens ICMP, incluindo mensagens de erro, mensagens de solicitação e resposta de eco, mensagens de redirecionamento, mensagens de tempo excedido, mensagens de destino inacessível, entre outras.

As mensagens ICMP podem ser usadas para uma variedade de fins, como indicar erros de rede, testar a conectividade entre dispositivos, enviar informações de roteamento, controlar o congestionamento da rede e muito mais.

Um uso secundário do protocolo ICMP é realizar diagnósticos de rede; os utilitários de terminal traceroute e ping comumente usados operam usando ICMP. O utilitário traceroute é usado para exibir o caminho de roteamento entre dois dispositivos de Internet. O caminho de roteamento é o caminho físico real dos routers conectados pelo qual uma solicitação deve passar antes de chegar ao seu destino. A viagem entre um router e outro é conhecida como "hop" e uma traceroute também informa o tempo necessário para cada salto ao longo do caminho. Isso pode ser útil para determinar fontes de atraso de rede.

4.2. Mensagens ICMP

Mensagens de erro:

- As mensagens de erro ICMP são usadas para informar um dispositivo de origem de que ocorreu um erro no processo de entrega de um pacote IP. Existem vários tipos de mensagens de erro ICMP, incluindo "Destino inacessível", "Tempo excedido", "Redirecionamento" e muito mais. Essas mensagens são enviadas pelo dispositivo de destino para informar o dispositivo de origem do erro e podem incluir informações adicionais sobre o erro, como por que o destino está inacessível ou a rota correta para chegar ao destino.

Mensagens de solicitação e resposta de eco:

- As mensagens de solicitação e resposta de eco ICMP são usadas para testar a conectividade entre dispositivos em uma rede IP. O dispositivo de origem envia uma mensagem de solicitação de eco para o dispositivo de destino, que responde com uma mensagem de resposta de eco. Este tipo de teste é frequentemente utilizado para verificar se um dispositivo está ligado e acessível na rede IP.

Mensagens de redirecionamento:

- As mensagens de redirecionamento ICMP são usadas para informar um dispositivo de origem de que ele deve enviar pacotes para outro dispositivo em vez do destino original. Essas mensagens são enviadas pelo dispositivo de roteamento para o dispositivo de origem e podem ser usadas para otimizar o tráfego em uma rede IP.

Mensagens de tempo excedido:

- As mensagens ICMP com tempo excedido são usadas para informar um dispositivo de origem de que um pacote IP foi descartado porque excedeu o tempo máximo permitido para chegar ao destino. Essas mensagens são enviadas pelo dispositivo de roteamento para o dispositivo de origem e podem ser usadas para diagnosticar problemas de rede.

Mensagens de destino inalcançáveis:

- As mensagens de destino inacessíveis ICMP são usadas para informar um dispositivo de origem de que o destino especificado em um pacote IP está inacessível. Essas mensagens são enviadas pelo dispositivo de roteamento para o dispositivo de origem e podem incluir informações adicionais sobre por que o destino está inacessível.

4.3. Parâmetros ICMP

Os parâmetros ICMP existem no cabeçalho do pacote e ajudam a identificar os erros no pacote IP a que pertencem. Os parâmetros são como uma etiqueta de envio em uma embalagem. Eles fornecem informações de identificação sobre o pacote e os dados que ele contém. Dessa forma, os protocolos e ferramentas de rede que recebem a mensagem ICMP sabem como lidar com o pacote.

1 - Type

- Os primeiros 8 bits são os tipos de mensagem. Alguns tipos de mensagem comuns incluem o seguinte:
    - Type 0 -- Echo reply
    - Type 3 -- Destino inacessível
    - Type 8 -- Eco
    - Type 5 – Redirecionamento

- O tipo fornece uma breve explicação sobre para que serve a mensagem para que o dispositivo da rede recetora saiba por que está recebendo a mensagem e como tratá-la. Por exemplo, um *Type* 8 Echo é uma consulta que um host envia para ver se um sistema de destino potencial está disponível. Ao receber uma mensagem Echo, o dispositivo recetor pode enviar de volta uma Echo Reply (*Type* 0), indicando que ela está disponível.

2 - Code

- Os próximos 8 bits representam o código do tipo de mensagem, que fornece informações adicionais sobre o tipo de erro.

3 - Checksum

- Os últimos 16 bits fornecem uma verificação de integridade da mensagem. O *checksum* mostra o número de bits em toda a mensagem e permite que a ferramenta ICMP verifique a consistência com o cabeçalho da mensagem ICMP para garantir que todo o intervalo de dados foi entregue.

4 - Pointer

- A próxima parte do cabeçalho ICMP é o *Pointer*. É composto por 32 bits de dados que apontam o problema na mensagem IP original. Especificamente, o *Pointer* identifica o local do byte na mensagem IP original que causou a geração da mensagem de problema. O dispositivo recetor examina essa parte do cabeçalho para identificar o problema.

5 - Datagram

- A seção final do pacote ICMP é o *Datagram* original. Ele consiste em até 576 bytes em IPv4 e 1.280 bytes em IPv6 e inclui uma cópia da mensagem IP original contendo erros.

4.4. Modo de Funcionamento do Protocolo ICMP

O ICMP funciona enviando mensagens de controle e feedback entre dispositivos de rede. Quando um dispositivo envia dados pela rede, o ICMP pode enviar mensagens de erro de volta para o dispositivo de origem se ocorrerem problemas durante a transmissão de dados. Além disso, o ICMP pode ser usado para enviar mensagens de consulta para dispositivos de rede, permitindo que os dispositivos verifiquem a disponibilidade de outros dispositivos na rede ou calculem a latência da conexão.

As mensagens ICMP são encapsuladas em pacotes IP e usam o campo Tipo e Código para identificar o tipo de mensagem que está sendo enviada. Existem vários tipos de mensagens ICMP, incluindo mensagens de erro, mensagens de solicitação e resposta de eco, mensagens de redirecionamento, mensagens de tempo excedido, mensagens de destino inacessível, entre outras.

Ao contrário do protocolo Internet (IP), o ICMP não está associado a um protocolo de camada de transporte, como TCP ou UDP. Isso torna o ICMP um protocolo sem conexão: um dispositivo não precisa abrir uma conexão com outro dispositivo antes de enviar uma mensagem ICMP. O tráfego IP normal é enviado usando TCP, o que significa que quaisquer dois dispositivos trocando dados executarão primeiro um handshake TCP para garantir que ambos os dispositivos estejam prontos para receber dados. O ICMP não abre uma conexão dessa forma. O protocolo ICMP também não permite que você direcione uma porta específica em um dispositivo.

Um exemplo comum de como o ICMP funciona é quando um dispositivo tenta enviar um pacote de dados para outro dispositivo na rede IP. Se o dispositivo de destino estiver inacessível ou não existir, o ICMP enviará uma mensagem de erro "Destino inacessível" para o dispositivo de origem. Essa mensagem pode incluir informações adicionais, como por que o destino está inacessível, como um endereço IP inválido ou uma rota de rede incorreta.

4.5. ICMP em Ataques DDoS

Em ataques DoS distribuídos (DDoS), os atacantes sobrecarregam o alvo com tráfego indesejado para que o alvo não possa fornecer serviço aos seus utilizadores. Há várias maneiras pelas quais um invasor pode usar o ICMP para executar esses ataques, incluindo o seguinte:

- *Ping of death*: O invasor envia um pacote IP maior do que o número de bytes permitido pelo IP. No caminho para o destino pretendido, o pacote de grandes dimensões é fragmentado. No entanto, quando o dispositivo destinatário o remonta novamente, o tamanho excede o limite, causando um estouro de buffer e a máquina recetora congelar ou falhar. Os dispositivos mais recentes têm defesas contra esse ataque de tipo mais antigo, mas os dispositivos de rede herdados ainda são vulneráveis a ele.

- *ICMP flood attack:* Às vezes chamado de *ping flood attack*, o objetivo desse ataque é sobrecarregar o dispositivo alvo com pacotes de solicitação de eco. Cada pacote de solicitação de eco deve ser processado pelo destino e respondido com mensagens de resposta de eco. Isso suga todos os recursos do computador de destino e causa uma negação de serviço para quaisquer outros utilizadores do computador de destino.

- *Smurl attack*: Em um ataque *Smurf*, o invasor envia um pacote ICMP com um endereço IP de origem falsificado e o equipamento da camada de rede responde ao pacote, enviando ao endereço falsificado uma enxurrada de pacotes. Como o *Ping of death*, os ataques *Smurf* são mais propensos a trabalhar em equipamentos legados não defendidos.

5. Aplicações

5.1. Aplicações que usam o protocolo ICMP no dia a dia

Ping

- O ping usa dois códigos ICMP: 8 (echo request) e 0 (echo reply). Quando se emite o comando Ping no prompt, o programa Ping envia um pacote ICMP contendo o código 8 no campo *Type*. A resposta terá um *Type* de 0. O programa divide o intervalo entre o envio do pacote de solicitação de eco e a chegada da resposta. Assim, pode-se obter o "tempo de ida e volta" de um pacote para a rede de destino dada e de volta.

- O pacote de solicitação de eco é incomum, pois é o único pacote ICMP que é enviado sem ser causado por um erro. Assim, o Ping não precisa emular uma condição de erro para receber uma mensagem ICMP de volta. O ping tem duas opções que permitem especificar uma lista de endereços para o caminho que a transmissão deve tomar. Estes são "-j", que sugere uma rota e "-k", que dita a rota.

Tracerout

- O programa *Traceroute* começa enviando um pacote com um TTL de 0. Isso será descartado pelo primeiro router que o receber, que geralmente é o gateway de rede. Esse router envia de volta um pacote ICMP. As únicas informações que o *Traceroute* deseja dessa resposta são o tempo necessário para retornar e o endereço de origem do pacote. Isso informa ao *Traceroute* o endereço do primeiro router no caminho para o destino. O programa então envia um pacote com um TTL de 1. Isso passa pelo gateway, o que diminui o TTL em 1. O router que recebe o pacote em seguida vê que o TTL é zero, descarta o pacote e envia de volta um pacote ICMP. Assim, o segundo router no caminho é revelado e o *Traceroute* anota o tempo que levou para que essa resposta chegasse. Ao aumentar o TTL em 1 a cada transmissão, o *Traceroute* eventualmente constrói um mapa de todos os links através da internet para o endereço fornecido.

6. Conclusão

O Protocolo ICMP é um elemento essencial da arquitetura de rede e desempenha um papel importante na comunicação entre dispositivos. Ele permite que os dispositivos transmitam informações sobre conectividade de rede, verifiquem a disponibilidade do dispositivo e identifiquem problemas de entrega de pacotes de dados. Além disso, o ICMP também é usado em muitas ferramentas de segurança de rede, como firewalls e sistemas de deteção de intrusão.

Ao longo do tempo, o ICMP evoluiu para uma ferramenta forte e confiável que ajuda a manter a conectividade e a segurança das redes em todo o mundo. No entanto, é importante lembrar que o uso indevido do ICMP pode resultar em problemas de segurança, como ataques de negação de serviço. Por isso, é essencial ter um conhecimento aprofundado sobre o protocolo e utilizá-lo com cuidado e cautela.

Compreender o ICMP é uma parte importante para garantir que as redes permaneçam seguras, estáveis e eficientes. Para aqueles envolvidos na administração de redes ou segurança de rede, é fundamental ter um conhecimento sólido deste protocolo e suas funcionalidades.

7. Bibliografia

https://www.comparitech.com/net-admin/what-is-icmp/#The_history_of_ICMP

https://www.techtarget.com/searchnetworking/definition/ICMP

https://www.cloudflare.com/pt-br/learning/ddos/glossary/internet-control-message-protocol-icmp/

https://www.techtarget.com/searchnetworking/definition/ICMP

https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/