IMPACTA– Curso: Ciência da Computação

Redes de Computadores – Professor: Rodolfo Riyoei Goya

AC 4 – Redes de Computadores

Nome: André Lucas Fabbris de Toledo

RA - 1902777

1. As diferenças entre as redes LAN, MAN e WAN é que na categoria LAN, em geral, atinge tamanhos de construções, como edifícios, residências, etc. Já a rede MAN, atinge tamanhos de uma cidade, ou campus, com uma única operadora e com tecnologia homogênea, enquanto a tecnologia WAN atinge já múltiplas cidades, países ou até continentes, sem limites, com múltiplas operadoras e tecnologia heterogênea.
2. O endereçamento físico não é usado pois as redes são distribuídas geograficamente, ou seja, de longa distância.
3. O cabeçalho TCP é feito começando com a aplicação de origem do pacote IP, o Source Port e a aplicação de destino do pacote IP, o Destinatio Port, ambos com 16 bits, sendo que os números de port para estas aplicações estão na faixa entre 0 e 1023, para aplicações Server, e acima dos 1023, para aplicação Client.

Além deles, contém o Sequencie Number, onde o TCP do remetente divide os dados recebidos da aplicação em pacotes e cria um numero de sequencia para cada pacote baseado na posição correta dentro do fluxo, com um número de sequência de 32 bits.

Já o Ackonowledge Number, com um valor de 32 bits, serve para enviar mensagens de reconhecimento para confirmar os pacotes recebidos, e quando não recebe o reconhecimento após o timeout, retransmite o pacote.

O HLEN, com tamanho de 4 bits, indica o tamanho do cabeçalho do pacote TCP, em blocos de 32 bits.

O Flags, com 6 bits, faz o controle de fluxo dos pacotes como o PSH, avisando que o pacote deve ser entregue imediatamente para a aplicação, o SYN, o qual o pacote é de sincronização, o FIN, que é de finalização, URG, ACK e RST.

O Window size, com um valor de 16bits, tem a função de evitar que cada uma das partes não passe a quantidade máxima de dados que a outra parte possa processar, isto é, cada parte envia um valor X para sinalizar para outra este valor máximo, sendo assim, não podendo ultrapassar este valor, e vice versa.

E o checksum, com tamanho de 16 bits, faz a verificação de integridade e retransmissão de pacotes com erros ou perdidos.

1. Pois para não haver dois hosts com o mesmo endereço, os endereços são gerenciadas pela IANA, Internet Assigned Numbers Authority, definindo as redes CIDR, com um padrão sem as regras das classes, acrescentando um “/N” ao final do endereço, entre 0 e 32, definindo as máscaras, rede e broadcast dos endereços, aumentando a quantidade de combinações de endereços dentro de uma rede, num total de mais de 4 bilhões de combinações no IPV4 e um numero muito maior no IPV6.
2. O protocolo ARP é usado cada vez que deseja uma comunicação com uma maquina onde o endereço MAC é desconhecido porém com um IP conhecido, enviando uma mensagem de broadcast (ARP Request) contendo o endereço IP desejado e o computador de destino responde (ARP Reply) com seus endereços IP e MAC.
3. Os dados que fazem parte do cabeçalho IP são: Vers, HLEN, Type of Service, Total Length, identifier, Source IP address, Destination IP address, Flags, Fragment offset, Time to live, Protocol e Header Checksum.
4. Os campos do cabeçalho IP que são alterados a cada roteador que o pacote atravessa são os dados do Fragment offset, flags, Time to live e o Header Checksum
5. A função do Time to live do cabeçalho IP é para evitar que pacotes fiquem passando de roteador em roteador indefinidamente pela internet
6. A função do Protocol é especificar o protocolo dos dados contidos no pacote
7. A função do Checksum é somar todos os campos do cabeçalho IP ajustando para 16 bits, sendo recalculado a cada roteador para comparar com o armazenado no campo do cabeçalho.
8. O protocolo de rede IP tem 8 bits, variando de 0 a 255, e se diz que executa o melhor esforço pois é ele que especifica os tipos dos dados, como por exemplo se é TCP, UDP, entre outros.
9. MTU é o tamanho máximo de frame que pode passar por um enlance.
10. Fragmentação é quando um pacote é maior que o MTU e se divide e remontagem é quando remontam essas fragmentações no equipamento de destino.
11. Ao passar de um enlance para outro de MTU menor, o pacote pode ser fragmentado, ou seja, o pacote é dividido para que consiga passar e dar continuidade até o endereço destino e remontado apenas no equipamento de destino.
12. O pacote será fragmentado em 3, com tamanhos de 500, 500(sendo 20 de cabeçalho) e 240(sendo 20 de cabeçalho).
13. Será fragmentado em mais 2, com tamanhos de 300 bytes 220 bytes na primeira e na segunda fragmentação, sendo assim 5 fragmentos, dois de 300 bytes, dois de 220 bytes e um de 240 bytes.
14. O ICMP, Internet Control Message Protocol, são 17 mensagens padronizadas para o IPV4, ampliada para o IPV6, no qual são mensagens para teste, informação de estado e mensagens de erro.
15. O cabeçalho é formado pelo Type, Code e Checksum
16. Os principais tipos de mensagens são: o Echo request (do tipo 8), que solicita que o equipamento de destino envie uma resposta, o Echo Reply(do tipo 0), respondendo o Echo request, o Source Quench (do tipo 4), que envia uma mensagem sinalizando que descartou um pacote por congestionamento, o Time exceeded (do tipo 11), mostrando que o campo Time to Live do cabeçalho IP chegou a zero durante o transito ou durante a remontagem no destino, o Timestamp Request e Reply (do tipo 13 e 14, respectivamente), que obtém a hora no host de destino, o Address Mask Request e Reply (do tipo 17 e 18, respectivamente), que obtém a mascara de rede da estação de destino, o Redirect (do tipo 5), informando o remetente que um outro roteador deve ser usado para o roteamento deste pacote, o Router Request (do tipo 10), mensagem solicitando a identificação de roteadores em uma rede, o Router Advertisement (do tipo 9), mensagem em resposta a um router request com a identificação de roteadores, e o Destination unreachable (do tipo 3).
17. São as camadas de enlances.
18. No modelo ISO/OSI divide as redes em 7 camadas: a camada de aplicação, que executa a logica de negócios e a interface com usuários; a camada de apresentação, que especifica como representar dados, resolvendo as diferenças nas representações internas de dados entre diferentes computadores; a camada de sessão, que especifica como estabelecer uma sessão de comunicação com um sistema remoto, como o login; a camada de transporte, que especifica como tratar dos detalhes de transferência de dados confiáveis entre dois hosts; a camada de rede, que especifica como são atribuídos os endereços distintos e globais aos hosts; a camada de enlance, que especifica como os dados são organizados em frames e transmitidos; e a camada física que corresponde ao hardware da rede.
19. No modelo TCP/IP, as redes são divididas em 4: camada de aplicação, onde executa efetivamente a logica de negócios e interface com usuários, sendo elas, aplicações clientes, que originam conexões com servidores, e servidoras, aplicações que ficam sempre em execução e aguardam serem chamados pelas aplicações clientes para oferecerem seus serviços; camada Hosto to Host, que especifica como tratar dos detalhes de transferência de dados entre dois hosts; camada Internet, que especifica o endereçamento IP e como dados são encaminhados de uma ponta a outra, a comunicação fim a fim; e a camada Interface de Rede, que corresponde ao hardware da rede.
20. A camada de Aplicação no TCP/IP corresponde às camadas aplicação, apresentação e sessão no modelo ISO/OSI, a camada host to host no TCP/Ip equivale a camada transporte no ISO/OSI, a camada Internet corresponde à camada rede no ISO/OSI e a interface de rede corresponde às camadas enlace e física no ISO/OSI.
21. Os cabeçalhos introduzidos em cada camada do protocolo aparecem antes da área de dados.