Alunos :

Matheus Holanda Matos
Paulo Henrique Araujo Nobre
Moises Moura Rabelo

1 - Diferencie a subcamada LLC da camada MAC do Ethernet.

A subcamada LLC trata da comunicação entre as camadas superiores e as camadas inferiores, além disso, o LCC é implementado no software, e sua implementação não depende do hardware. Em um computador, o LLC pode ser considerado o software do driver para a placa de rede.

Já a subcamada MAC constitui a subcamada inferior da camada de enlace de dados, além disso, o MAC é implementado pelo hardware, normalmente na placa de rede do computador.

2 - Descreva as funções dos campos de um quadro Ethernet.

Preâmbulo: é usado para a sincronização da temporização em Ethernet assíncrona de 10 Mbps e em implementações mais lentas;

Delimitador de Início de Quadro: consiste em um campo de um octeto que marca o final das informações de temporização;

Endereço de Destino: contém um endereço de destino MAC;

Endereço de Origem: contém um endereço de origem MAC;

Comprimento: indica o número de bytes de dados que vêm depois desse campo;

Tipo: especifica o protocolo da camada superior que recebe os dados;

Dados: Informações a serem transferidas;

Enchimento: inserido imediatamente após os dados do usuário, quando não houver dados de usuário suficientes para que o quadro satisfaça o comprimento mínimo para o quadro;

FCS: contém um valor que permite a verificação de erros com base em cálculos.

3 - Quais são as duas partes de um endereço MAC?

A primeira metade de um endereço MAC denota o fabricante do dispositivo de hardware. Já a segunda metade de um endereço MAC denota o número de série do dispositivo individual.

4 - Como o switch aprende sobre onde estão os hosts da LAN Ethernet?

O switch aprende os dispositivos que estão conectados às suas portas através da leitura do endereços MAC de origem no Quadro Ethernet que cruza suas portas.

5 - Quando o switch faz uma inundação de quadros Ethernet?

O switch faz uma inundação de quadros Ethernet quando ele não conhece o MAC de destino ou esse destino é um broadcast ou multicast. Outra situação de inundação é quando o número máximo de MACs é atingido, nesse caso o switch acaba se comportando como um HUB.

6 - Diferencie portas full-duplex da half-duplex de switches Ethernet.

A comunicação em half duplex depende do fluxo de dados unidirecional

quando o envio e o recebimento de dados não são executados ao mesmo tempo. Isso é semelhante à forma de funcionamento de walkie-talkies ou rádios bidirecionais à medida que apenas uma pessoa pode falar por vez. Se alguém fala com outra pessoa já falando, ocorre uma colisão. Dessa forma, a comunicação em half duplex implementa CSMA/CD para ajudar a reduzir o potencial de colisões e as detectar quando elas acontecerem.

Já na comunicação full duplex, como o fluxo de dados é bidirecional, os dados podem ser enviados e recebidos ao mesmo tempo. O suporte bidirecional aprimora o desempenho, reduzindo o tempo de espera entre as transmissões. Grande parte das placas de rede Ethernet, Fast Ethernet e Gigabit Ethernet vendidas atualmente oferecem recursos em full duplex. No modo full duplex, o circuito de detecção de colisões é desabilitado. Os quadros enviados pelos dois nós finais conectados não podem colidir porque os nós finais usam dois circuitos separados no cabo de rede.

7 - Como um host conhece o endereços MAC a partir de um endereço IP.

Um host conhece o endereço MAC a partir de um endereço IP através do protocolo ARP, esse protocolo fornece resolução dinâmica de endereços, que é um mapeamento entre as duas firmas de endereçamento distintas: endereços IP, e qualquer outro tipo de endereço usado na camada de enlace. No caso dos quadros Ethernet, a camada de enlace usa o MAC Address (Media Access Control), endereço físico da interface.

8 - Descreva o ataque ARP Spoofing.

ARP Spoofing é uma técnica pela qual um invasor envia mensagens falsas do ARP para uma rede local. Geralmente, o objetivo é associar o endereço MAC do atacante ao endereço IP de outro hospedeiro, como o gateway padrão, fazendo com que qualquer tráfego destinado a esse endereço IP seja enviado ao atacante.

A falsificação ARP pode permitir que um atacante intercepte quadros de dados em uma rede, modifique o tráfego ou interrompa todo o tráfego. Geralmente, o ataque é usado como uma abertura para outros ataques, como DoS, man-in-the-middle ou session hijacking.

O ataque só pode ser usado em redes que usam ARP e exige que o invasor tenha acesso direto ao segmento de rede local a ser atacado.