1.Segurança em encaminhamento de tráfego

1.1 Man-in-the-Middle em Camada 2

Os ataques Man-in-the-Middle, também conhecidos como MitM, são uma classe de ameaças em que um invasor se posiciona entre a comunicação entre dois dispositivos, agindo como intermediário. Para ilustrar, imagine uma conversa entre Alice e Bob, que estão trocando informações pela rede.

O invasor, chamado de atacante, se insere no meio dessa comunicação e intercepta as mensagens enviadas por Alice, depois as reenvia para Bob, e vice-versa, fazendo com que pareça que a comunicação está ocorrendo normalmente, mas, na verdade, o atacante está controlando todo o fluxo.

1.2 Clonagem de MAC

O MAC Cloning, também conhecido como clonagem de endereço MAC, é uma técnica utilizada em ataques de segurança de redes para falsificar o endereço físico (MAC) de um dispositivo de rede. O objetivo desse ataque é enganar o sistema de autenticação da rede e se passar por um dispositivo legítimo, permitindo ao atacante acessar recursos e informações restritas da rede. Veja como é implementado:

- **Observação do alvo:** O atacante começa observando o tráfego de rede para identificar os dispositivos ativos na rede, especialmente aqueles com permissões e acesso privilegiado. Isso pode ser feito por meio de ferramentas de análise de rede ou sniffers, que permitem ao atacante visualizar os pacotes de dados enviados e recebidos pelos dispositivos na rede.
- **Identificação do alvo:** Com base nas informações obtidas no passo anterior, o atacante seleciona o dispositivo legítimo que deseja se passar. Isso pode ser um roteador, um computador ou qualquer outro dispositivo com acesso restrito que o atacante queira imitar.
- **Coleta do endereço MAC do alvo:** O atacante coleta o endereço MAC do dispositivo legítimo escolhido. O endereço MAC é uma sequência única de 48 bits atribuída à placa de rede de cada dispositivo, e é utilizado para identificá-lo de forma exclusiva em uma rede.
- **Configuração do endereço MAC clonado:** Com o endereço MAC do dispositivo legítimo em mãos, o atacante configura seu próprio dispositivo para usar esse endereço MAC clonado. Essa etapa é crucial, pois é aqui que o atacante engana a rede fazendo-a acreditar que seu dispositivo é o dispositivo legítimo escolhido no passo 2.
- **Conexão à rede:** Após configurar o endereço MAC clonado em seu dispositivo, o atacante se conecta à rede. A rede, ao receber o pacote de dados do atacante, reconhece o endereço MAC clonado como sendo do dispositivo

legítimo e, assim, concede acesso aos recursos e informações restritas destinadas ao dispositivo original.

1.3 Inundação de MAC (MAC flooding)

O MAC Flooding, ou inundação de MAC, é uma técnica de ataque em redes locais (LANs) que visa sobrecarregar a tabela de endereços MAC de um switch. Esse tipo de ataque aproveita uma vulnerabilidade comum em switches que usam uma tabela limitada para armazenar os endereços MAC dos dispositivos conectados à rede. Ao inundar essa tabela com informações falsas de endereços MAC, o atacante pode causar uma falha no funcionamento do switch, resultando em uma situação conhecida como "*flooding*" (inundação) de tráfego.

Funcionamento:

- **Identificação do switch e porta:** O atacante começa identificando o switch e a porta a serem atacados. Geralmente, o atacante realiza uma varredura na rede para detectar switches e dispositivos conectados a eles, buscando vulnerabilidades para explorar.
- **Criação de pacotes:** Em seguida, o atacante gera uma grande quantidade de pacotes falsificados com endereços MAC aleatórios, geralmente, com o objetivo de esgotar a capacidade da tabela de endereços MAC do switch.
- **Envio dos pacotes falsos:** O atacante envia os pacotes falsos para o switch através da porta selecionada, fazendo com que o switch adicione cada endereço MAC falso à sua tabela. Como a tabela do switch tem um tamanho limitado, ela eventualmente fica cheia, resultando em uma situação de "flooding" de tráfego. 4.
- **Comportamento anômalo do switch:** À medida que a tabela de endereços MAC fica cheia, o switch entra em um estado chamado "modo de falha aberto", onde ele não consegue mais associar endereços MAC aos respectivos dispositivos físicos corretos. Como resultado, o switch passa a enviar todo o tráfego de rede para todas as portas, em vez de direcioná-lo apenas para o destino correto, causando uma sobrecarga da rede e interrompendo sua operação normal.

O MAC Flooding pode ser um ataque eficaz em redes que utilizam switches com tabelas de endereços MAC pequenas e não possuem proteções adequadas contra esse tipo de ataque. Para mitigar esse tipo de ameaça, é recomendável implementar medidas de segurança, como limitar o número de endereços MAC aprendidos por porta, utilizar switches com capacidade de detecção de ataques de flooding e, em algumas situações, a utilização de VLANs (Redes Locais Virtuais) para segmentar o tráfego de rede.

2.Spanning Tree Protocol (STP)

É um protocolo de rede utilizado em redes Ethernet para evitar loops de caminho em topologias comutadas. A presença de loops em uma rede pode causar problemas, como tempestades de broadcast e congestionamentos, afetando negativamente o desempenho e a estabilidade da rede. O STP trabalha eliminando esses loops, mantendo caminhos redundantes, mas bloqueando-os de forma inteligente para garantir a convergência da rede em uma topologia sem loops.

Funcionamento:

- **Eleição do bridge raiz (root bridge):** O primeiro passo do STP é a eleição do Bridge Raiz. Todos os switches na rede disputam essa posição, e o switch com o menor valor de prioridade (Bridge ID) se torna o Bridge Raiz. Caso haja empate na prioridade, o switch com o menor endereço MAC assume a posição de Bridge Raiz. O Bridge Raiz é o ponto de referência para a construção da árvore de expansão.
- **Cálculo dos caminhos mais curtos:** Após a eleição do Bridge Raiz, cada switch determina os caminhos mais curtos até o Bridge Raiz. Para isso, os switches trocam informações entre si por meio de mensagens BPDU (Bridge Protocol Data Unit). As BPDU contêm informações sobre o Bridge Raiz, o custo do caminho e o identificador do switch que as envia. Com base nas informações das BPDU, cada switch calcula o caminho mais curto até o Bridge Raiz.
- **Escolha das portas designadas e bloqueadas:** Uma vez que os caminhos mais curtos são calculados, cada switch seleciona as portas designadas e bloqueadas para evitar loops. A porta designada é a que oferece o caminho mais curto para o Bridge Raiz, enquanto as portas bloqueadas são aquelas que formam loops e são desativadas para prevenir problemas na rede.
- **Atualizações contínuas como BPDUs:** O STP é dinâmico e se adapta às mudanças na rede. Ele continua a trocar BPDUs regularmente para atualizar a topologia da rede. Se ocorrerem alterações, como falhas de links ou adição de novos switches, o STP recalcula as portas designadas e bloqueadas para garantir que a topologia da rede permaneça livre de loops.
- **Tempo de convergência:** O STP pode levar alguns segundos para convergir após uma alteração na rede, durante os quais as portas podem ser bloqueadas ou desbloqueadas. Durante esse período, o tráfego pode ser redirecionado temporariamente, mas a rede se estabilizará assim que o STP concluir suas atualizações.

Com o Spanning Tree Protocol, as redes Ethernet conseguem fornecer redundância e disponibilidade enquanto evitam loops. No entanto, o STP pode causar uma subutilização de links redundantes, especialmente em topologias de rede complexas. Por esse motivo, outras versões aprimoradas do STP, como o Rapid Spanning Tree Protocol (RSTP) e o Multiple Spanning Tree Protocol (MSTP), foram desenvolvidas para otimizar a convergência da rede e permitir um melhor aproveitamento dos links redundantes.

2.1 Bridge Protocol Data Unit (BPDU) Guard

O Bridge Protocol Data Unit (***BPDU***) Guard é uma medida de segurança utilizada em switches para evitar problemas causados pela recepção de mensagens BPDU (Bridge Protocol Data Unit) em portas que não deveriam receber essas informações. As BPDU são utilizadas pelo STP para calcular os caminhos mais curtos e evitar loops em topologias de rede comutadas.

Funcionamento:

- **Portas de acesso e portas tronco:** Os switches de rede possuem diferentes tipos de portas, como portas de acesso e portas tronco. As portas de acesso são aquelas usadas para conectar dispositivos finais, como computadores e impressoras, enquanto as portas tronco são usadas para interconectar switches e permitir o tráfego entre diferentes VLANs.
- **BPDU Guard para Portas de Acesso:** O BPDU Guard é ativado em portas de acesso. Quando o BPDU Guard está habilitado em uma porta, ela monitora a recepção de BPDUs. Caso a porta detecte a chegada de uma BPDU, ela imediatamente entra em estado de erro (errdisable) e é desativada, bloqueando o tráfego para prevenir a formação de loops na rede.
- **Cenário de Porta Bloqueada:** O cenário ideal para a utilização do BPDU Guard em portas de acesso é quando um switch é conectado a uma porta de acesso em vez de um dispositivo final. Isso poderia acontecer por acidente ou intencionalmente. Sem o BPDU Guard, o switch conectado poderia enviar BPDUs para a rede, fazendo com que os switches em toda a rede recalculem o Spanning Tree, causando uma interrupção temporária na comunicação da rede.
- **Recuperação da Porta:** Quando uma porta é colocada em estado de erro (errdisable) pelo BPDU Guard, ela permanece nesse estado até que um administrador de rede intervenha para solucionar o problema. Após o problema ser resolvido, a porta pode ser reativada manualmente.

3.Filtragem de endereços MAC

A Filtragem de Endereços MAC (***MAC Filtering***) é uma técnica de segurança usada em redes para controlar quais dispositivos são permitidos ou bloqueados de

acessar a rede com base em seus endereços MAC. Cada dispositivo de rede possui um endereço MAC único e, ao utilizar o MAC Filtering, é possível configurar o roteador ou switch para permitir apenas dispositivos com endereços MAC específicos a se conectarem à rede.

Funcionamento:

- **Coleta dos endereços MAC autorizados:** Para implementar o MAC Filtering, o administrador da rede deve coletar os endereços MAC dos dispositivos que deseja autorizar a se conectar à rede. Isso pode ser feito manualmente, identificando os dispositivos e obtendo seus respectivos endereços MAC.
- **Configuração no roteador ou switch:** Com os endereços MAC autorizados em mãos, o administrador configura o roteador ou switch com as informações de MAC Filtering. Essa configuração é realizada no dispositivo que controla o acesso à rede, geralmente, o roteador ou switch principal.
- **Escolha do modo de filtragem:** Existem dois modos de filtragem de MAC comuns: "*Permitir*" e "*Bloquear*". No modo "*Permitir*", apenas os endereços MAC listados são autorizados a acessar a rede, enquanto, no modo "*Bloquear*", todos os dispositivos são permitidos, exceto aqueles com endereços MAC listados.
- **Autenticação dos dispositivos:** Quando um dispositivo tenta se conectar à rede, ele envia seu endereço MAC para o roteador ou switch. O dispositivo de rede verifica se o endereço MAC está na lista de MAC Filtering configurada e toma a decisão de permitir ou bloquear o acesso com base nessa verificação.
- **Segurança e limitações:** Embora o MAC Filtering seja uma medida de segurança adicional, é importante lembrar que o endereço MAC pode ser facilmente falsificado por um atacante experiente. Portanto, o MAC Filtering não é uma solução invulnerável e deve ser usado em conjunto com outras medidas de segurança, como criptografia de rede (WPA2/WPA3 em redes Wi-Fi) e autenticação de dispositivos.

4.DHCP snooping

É uma medida de segurança utilizada em redes para proteger contra ataques de Dynamic Host Configuration Protocol (DHCP) falsificado. O DHCP é um protocolo que permite aos dispositivos obterem automaticamente endereços IP e outras configurações de rede, tornando o processo de configuração de redes mais simples e dinâmico.

No entanto, o DHCP pode ser explorado por atacantes para fornecer informações de configuração de rede incorretas ou prejudiciais a dispositivos legítimos. Funcionamento abaixo:

- **O DHCP falsificado:** É um ataque em que um dispositivo malicioso se passa pelo servidor DHCP legítimo e responde às solicitações de dispositivos na rede. O dispositivo malicioso pode fornecer informações incorretas, como um endereço IP inválido ou mesmo um endereço IP pertencente a um servidor malicioso controlado pelo atacante.
- **Ativação do DHCP snooping:** Para evitar o DHCP Falsificado, o administrador da rede ativa o DHCP Snooping no switch de rede. O DHCP Snooping é uma funcionalidade de segurança que monitora o tráfego DHCP na rede e valida as respostas do servidor DHCP antes de permitir que sejam encaminhadas para os dispositivos clientes.
- **Criação de uma tabela DHCP snooping:** Quando o DHCP Snooping está ativo, o switch cria uma tabela de DHCP Snooping que armazena informações sobre quais portas estão autorizadas a enviar ou receber pacotes DHCP. Inicialmente, todas as portas são marcadas como não confiáveis, o que significa que não podem enviar pacotes DHCP para a rede.
- **Identificação de portas confiáveis e não confiáveis:** Através do DHCP Snooping, o switch pode distinguir quais portas são confiáveis e quais são não confiáveis. Portas confiáveis são aquelas conectadas a servidores DHCP legítimos, como o servidor DHCP do roteador ou servidor da rede. Portas não confiáveis são aquelas em que dispositivos finais, como computadores e dispositivos móveis, estão conectados.
- **Aprendizado de informações de DHCP snooping:** Quando o DHCP Snooping está em funcionamento, o switch aprende quais endereços MAC estão associados a cada porta do switch. As portas confiáveis são autorizadas a enviar pacotes DHCP e outras informações de configuração de rede, enquanto as portas não confiáveis são bloqueadas para evitar que enviem pacotes DHCP falsificados.
- **Prevenção de ataques de DHCP falsificado:** Com o DHCP Snooping em ação, o switch pode diferenciar entre as respostas legítimas do servidor DHCP e as respostas falsificadas de um atacante. Quando uma resposta DHCP é recebida em uma porta não confiável, o switch a descarta, evitando assim que as informações de configuração de rede incorretas sejam distribuídas aos dispositivos clientes.

5.Port-based Network Access Control (PNAC)

Também conhecido como ***Controle de Acesso Baseado em Porta***, é uma técnica de segurança usada em redes para controlar o acesso de dispositivos aos recursos de rede com base nas portas físicas do switch em que eles estão conectados. Essa abordagem é comum em switches Ethernet e é amplamente utilizada para restringir o acesso a recursos de rede apenas a dispositivos autorizados.

Funcionamento:

- **Identificação dos dispositivos e portas:** O primeiro passo do PNAC é identificar os dispositivos que desejam acessar a rede e as portas físicas dos switches em que esses dispositivos estão conectados. Os dispositivos podem ser computadores, impressoras, telefones IP ou qualquer outro dispositivo de rede que precise se comunicar na rede.
- **Definição das políticas de acesso:** Com base na identificação dos dispositivos, o administrador de rede define políticas de acesso que indicam quais dispositivos estão autorizados a acessar a rede e quais tipos de acesso eles têm. Por exemplo, alguns dispositivos podem ter acesso completo à rede, enquanto outros podem ter acesso limitado a determinados recursos.
- **Configuração no switch:** Após definir as políticas de acesso, o administrador configura o switch para aplicar essas políticas nas portas físicas relevantes. Essa configuração é realizada no switch que controla o acesso à rede, normalmente no nível da camada 2 (camada de enlace) do modelo OSI.
- **Métodos de autenticação:** O PNAC pode ser implementado com diferentes métodos de autenticação, dependendo do nível de segurança desejado. Alguns métodos comuns de autenticação incluem o uso de endereços MAC ou autenticação baseada em portas 802.1x (802.1x Port-Based Authentication), que envolve o uso de um servidor de autenticação externo.
- **Verificação do acesso:** Quando um dispositivo é conectado a uma porta do switch, o PNAC verifica se ele está autorizado a acessar a rede, com base nas políticas de acesso configuradas. Se o dispositivo for autorizado, ele receberá acesso conforme definido na política. Caso contrário, o acesso será negado.
- **Monitoramento e manutenção:** O PNAC também inclui recursos de monitoramento e manutenção para garantir que as políticas de acesso sejam aplicadas corretamente. Inclui registros de atividade de rede e a capacidade de atualizar ou modificar as políticas conforme necessário.

6.IP Spoofing

É uma técnica de ataque cibernético que envolve a falsificação do endereço IP de origem em um pacote de dados para mascarar a verdadeira identidade do remetente. Isso permite que o atacante envie pacotes de dados com um endereço IP

forjado, fazendo-os parecer originados de uma fonte confiável ou autorizada. Essa técnica é frequentemente utilizada em ataques de negação de serviço distribuídos (DDoS) e em outras atividades maliciosas para evitar a identificação do verdadeiro remetente.

Funcionamento:

- **Identificação do alvo:** O atacante começa identificando o alvo do ataque, que pode ser um servidor, um roteador ou outro dispositivo na rede. O objetivo é enviar pacotes de dados falsificados ao alvo, aparentando que eles vêm de uma origem legítima.
- **Captura do tráfego de rede:** Para obter informações sobre o tráfego de rede entre o atacante e o alvo, o atacante pode usar ferramentas de sniffing ou análise de pacotes. Isso permite que ele observe o tráfego existente e identifique endereços IP legítimos na rede.
- **Escolha do endereço IP falsificado:** Com base nas informações obtidas, o atacante escolhe um endereço IP falso para utilizar no ataque. Geralmente, ele seleciona um endereço IP que pertence a uma fonte confiável ou que não esteja em uso na rede, para evitar a detecção.
- **Criação do pacote forjado:** Com o endereço IP falso escolhido, o atacante cria pacotes de dados falsificados, incluindo o endereço IP de origem forjado. Esses pacotes podem conter comandos maliciosos, dados falsos ou até mesmo serem vazios, dependendo do objetivo do ataque.
- **Envio dos pacotes falsificados:** O atacante envia os pacotes de dados falsificados ao alvo. Como os pacotes parecem originados de um endereço IP legítimo ou autorizado, o alvo pode processá-los sem suspeitar de sua autenticidade.
- **Consequências do IP spoofing:** As consequências do IP Spoofing podem ser graves. O atacante pode usar essa técnica para executar ataques DDoS, onde múltiplos dispositivos enviam pacotes falsificados ao alvo, sobrecarregando seus recursos e causando indisponibilidade de serviços. Além disso, o IP Spoofing pode ser usado para evitar a detecção ou rastreamento de atividades maliciosas, uma vez que a fonte real do ataque é mascarada com um endereço IP falso.

7.Balanceamento de carga

Um Balanceador de Carga (***Load Balancer***) é um dispositivo ou software que distribui o tráfego de rede de forma equilibrada entre vários servidores ou recursos para otimizar o desempenho, evitar sobrecargas e melhorar a disponibilidade dos serviços.

O objetivo principal do Load Balancer é garantir que cada servidor receba uma quantidade justa de solicitações de clientes, evitando que um servidor específico fique sobrecarregado e causando atrasos ou falhas no atendimento. Existem dois tipos principais de Load Balancer:

- **Balanceador de carga de camada 4 (layer 4 load balancer):** Opera na camada 4 (camada de transporte) do modelo OSI. Ele toma decisões de balanceamento de carga com base em informações contidas nos cabeçalhos dos pacotes de rede, como endereços IP de origem e destino, portas de origem e destino, e informações do protocolo de transporte (como TCP ou UDP).
- **Balanceador de carga de camada 7 (Layer 7 load balancer):** Atua na camada 7 (camada de aplicação) do modelo OSI. Além das informações disponíveis no Layer 4, ele examina o conteúdo do tráfego de aplicação, permitindo tomar decisões de balanceamento de carga com base em informações mais detalhadas, como URL, cabeçalhos HTTP e dados do payload.

8.Ataque Distribuído de Negação de Serviço (DDoS)

Um Ataque Distribuído de Negação de Serviço ou ***Distributed Denial of Service*** (***DDoS***) Attack, é uma forma de ataque cibernético projetada para sobrecarregar um servidor, serviço ou infraestrutura de rede, tornando-os inacessíveis a usuários legítimos. Nesse tipo de ataque, um grande volume de tráfego malicioso é direcionado ao alvo, inundando seus recursos e causando uma negação de serviço para os usuários legítimos que tentam acessá-lo.

Funcionamento:

- **Recrutamento de botnets:** Os atacantes geralmente não possuem recursos suficientes para lançar ataques DDoS sozinhos. Por isso, eles recrutam uma rede de dispositivos comprometidos, conhecida como botnet. Esses dispositivos podem ser computadores, servidores, roteadores, câmeras IP ou outros dispositivos conectados à internet que foram infectados com malware e estão sob o controle do atacante.
- **Preparação do ataque:** O atacante configura e prepara a botnet para lançar o ataque DDoS. Isso pode incluir o uso de kits de ferramentas especializados para controlar os dispositivos comprometidos e direcionar o tráfego ao alvo. O atacante também pode dividir a botnet em vários grupos, cada um encarregado de atacar diferentes partes do alvo, o que torna o ataque mais complexo de ser mitigado.
- **Ataques - enchendo a tubulação:** Uma vez que a botnet está pronta, o ataque começa. Os dispositivos comprometidos enviam uma enorme quantidade de

tráfego malicioso ao servidor ou serviço alvo. Esse tráfego pode ser do tipo TCP, UDP, HTTP ou até mesmo pacotes ICMP, dependendo do tipo de ataque DDoS.

- **Sobrecarga de recursos:** Com o volume massivo de tráfego malicioso, os recursos do servidor alvo, como CPU, memória e largura de banda, são rapidamente sobrecarregados. Isso impede que o servidor responda a solicitações legítimas dos usuários, resultando em uma negação de serviço. O objetivo do atacante é tornar o serviço inacessível ou desativá-lo completamente.

9.Clustering

O ***clustering*** em balanceamento de carga é uma técnica que combina múltiplos servidores (nós) em um grupo, conhecido como cluster, para distribuir a carga de trabalho de forma equilibrada entre eles. O objetivo é melhorar o desempenho, a escalabilidade e a disponibilidade dos serviços, permitindo que os servidores trabalhem em conjunto para atender às solicitações dos clientes de forma mais eficiente.

Funcionamento

- **Criação do cluster:** Os servidores físicos ou virtuais são agrupados em um único cluster. Os servidores do cluster podem estar fisicamente próximos ou distribuídos em diferentes locais geográficos, dependendo dos requisitos de redundância e disponibilidade.
- **Distribuição da carga:** Quando os clientes enviam solicitações para os serviços hospedados pelo cluster, um dispositivo de balanceamento de carga é colocado em frente ao cluster para distribuir a carga de trabalho entre os servidores. O *load balancer* pode usar diferentes algoritmos, como Round Robin (distribuição sequencial), Least Connections (encaminhamento para o servidor com menos conexões) ou Hashing (encaminhamento com base em informações dos pacotes), para determinar para qual servidor direcionar cada solicitação.
- **Monitoramento e gerenciamento:** O cluster geralmente possui um mecanismo de monitoramento que verifica o status de cada servidor em tempo real. Caso um servidor falhe ou apresente problemas, o *load balancer* redireciona automaticamente as solicitações para os servidores restantes, garantindo que os serviços permaneçam disponíveis, mesmo em caso de falha de um dos nós.
- **Escalabilidade e disponibilidade:** Com o clustering em balanceamento de carga, é possível adicionar ou remover servidores do cluster conforme a demanda, o que permite ajustar a capacidade de processamento de acordo com

o tráfego e evitar sobrecargas. Além disso, a redundância fornecida pelo cluster melhora a disponibilidade, uma vez que, se um servidor falhar, os outros servidores podem assumir a carga e manter o serviço ativo.

Existem duas principais configurações de clustering em balanceamento de carga:

- **Active/Passive (A/P) Clustering:** No A/P Clustering, apenas um dos servidores é designado como ativo (active), enquanto os demais servidores são designados como passivos (passive). O servidor ativo é responsável por processar todas as solicitações de clientes, enquanto os servidores passivos permanecem ociosos, em modo de espera, monitorando continuamente o servidor ativo. Caso o servidor ativo falhe, um dos servidores passivos é ativado automaticamente pelo *load balancer* para assumir a carga e garantir a continuidade dos serviços.
- **Active/Active (A/A) Clustering:** No A/A Clustering, todos os servidores do cluster estão ativos e participam ativamente do processamento das solicitações dos clientes. O *load balancer* distribui a carga de trabalho de forma equilibrada entre todos os servidores ativos, garantindo que cada servidor contribua igualmente para o atendimento das solicitações. Essa configuração oferece melhor utilização dos recursos, permitindo que todos os servidores estejam envolvidos no processamento do tráfego.

10.QoS

O ***Quality of Service*** (***QoS***), ou Qualidade de Serviço, é uma técnica de gerenciamento de tráfego em redes de computadores que prioriza e controla a entrega de dados com base em suas necessidades de desempenho e requisitos de serviço. O objetivo do QoS é garantir uma distribuição justa e eficiente da largura de banda e recursos de rede entre diferentes tipos de tráfego, como voz, vídeo, dados críticos e aplicativos em tempo real.

Funcionamento:

- **Classificação de tráfego:** O primeiro passo para implementar o QoS é classificar o tráfego em categorias ou classes, com base em suas características e requisitos de desempenho. Por exemplo, o tráfego de voz de uma chamada VoIP é classificado como uma classe de alta prioridade, enquanto o tráfego de transferência de arquivos pode ser classificado como uma classe de baixa prioridade.
- **Marcação de pacotes:** Após a classificação, os pacotes de dados são marcados com informações que indicam sua prioridade de QoS. Essas informações são

adicionadas aos cabeçalhos dos pacotes e podem ser interpretadas por roteadores e switches da rede para aplicar as políticas de QoS.

- **Priorização de tráfego:** Com os pacotes devidamente marcados, o QoS permite que os dispositivos de rede, como roteadores e switches, priorizem o tráfego com base nas marcações. Os pacotes marcados com alta prioridade têm tratamento preferencial e são encaminhados antes dos pacotes com prioridade mais baixa.
- **Gerenciamento de largura de banda:** O QoS também controla a alocação de largura de banda para diferentes classes de tráfego. Isso pode ser feito por meio de técnicas como "*bandwidth reservation*" (reserva de largura de banda) e "*bandwidth policing*" (policiação de largura de banda). O objetivo é garantir que as classes de tráfego com alta prioridade tenham acesso a recursos suficientes para atender às suas necessidades de desempenho.
- **Controle de congestionamento:** QoS também é usado para evitar congestionamentos na rede. Quando a demanda por largura de banda é alta, o QoS pode acionar mecanismos de controle de congestionamento, como "*traffic shaping*" (moldagem de tráfego) ou "*traffic policing*" (policiação de tráfego), para limitar a taxa de transmissão de pacotes e evitar que a rede fique sobrecarregada.
- **Benefícios do QoS:** A implementação do Quality of Service oferece diversos benefícios para as redes de computadores