1) **Endereço IP**:

* **Definição**: Identificador numérico para dispositivos em uma rede que usa o Protocolo de Internet (ex.: 192.168.0.1 para IPv4).
* **Função**: Identifica e localiza dispositivos para comunicação entre redes, permitindo o roteamento de dados.

**Endereço MAC**:

* **Definição**: Identificador único atribuído a interfaces de rede, usado em redes locais, composto por 48 bits em formato hexadecimal (ex.: 00:1A:2B:3C:4D:5E).
* **Função**: Identifica dispositivos fisicamente na rede local, assegurando a entrega correta de pacotes de dados na camada de enlace.

**Propósito**:

* **IP**: Identificação lógica global (entre redes).
* **MAC**: Identificação física local (dentro de redes).

2) **Uso Combinado**:

* **IP (Endereçamento Lógico)**: Identifica dispositivos globalmente para roteamento de dados entre redes.
* **MAC (Endereçamento Físico)**: Identifica dispositivos localmente para entrega precisa dos pacotes na rede local.

**Processo de Comunicação**:

1. **Resolução com ARP**: Dispositivo usa ARP para mapear o IP de destino ao seu endereço MAC correspondente.
2. **Envio de Dados**: Pacotes incluem endereços IP e MAC do destino para garantir que os dados cheguem ao dispositivo correto.
3. **Roteamento e Comutação**: Roteadores usam IPs para direcionar entre redes; switches usam MACs para entrega local.

**Exemplo**:

* Um computador A (IP: 192.168.1.2, MAC: 00:1A:2B:3C:4D:5E) quer acessar um servidor (IP: 192.168.1.10, MAC: 00:5E:4D:3C:2B:1A):
  1. A usa ARP para obter o MAC do servidor.
  2. A envia dados com ambos os endereços IP e MAC do servidor.
  3. O switch entrega os pacotes usando o MAC do servidor.

Os endereços IP roteiam os pacotes, enquanto os endereços MAC garantem a entrega na rede local.

3) **Configuração de Endereços:**

* **IP**:
  + - **Estático**: Configurado manualmente no dispositivo.
    - **Dinâmico (DHCP)**: Atribuído automaticamente pelo servidor DHCP.
* **MAC**:
  + - Atribuído de fábrica e geralmente fixo, usado para identificar fisicamentedispositivos na rede.

**Ferramentas de Rede:**

1. **ipconfig (Windows)**:
   * + Exibe informações de rede, incluindo IP e MAC.
     + Exemplo: ipconfig /all mostra todos os detalhes.
2. **ifconfig (Linux/Unix)**:
   * + Usado para ver e configurar endereços IP e MAC.
     + Exemplo: ifconfig -a exibe todas as interfaces de rede.
3. **Wireshark**:
   * + Captura e analisa pacotes de rede em tempo real.
     + Permite filtrar por endereços IP ou MAC para inspeção detalhada.

**Simulação:**

* **Cisco Packet Tracer/GNS3**: Simulam redes para visualizar e testar configurações de IP e MAC, usando comandos como ipconfig ou ifconfig e capturando tráfego com Wireshark.

**4) Implicações Práticas:**

1. **Gerenciamento de Rede**: IPs ajudam na identificação de dispositivos entre redes, enquanto MACs são usados para controle de acesso local e segmentação de tráfego.
2. **Diagnóstico de Problemas**: Ferramentas como ipconfig, ifconfig e Wireshark ajudam a identificar conflitos de IP e problemas de conectividade relacionados a endereços MAC.
3. **Otimização de Desempenho**: IPs otimizam o roteamento entre redes; MACs facilitam comutação eficiente dentro da rede local.

**Questões de Segurança e Mitigação:**

1. **Filtragem de MAC**:

* **Risco**: Pode ser burlada com spoofing de MAC.
* **Mitigação**: Usar autenticação adicional como 802.1X.

1. **Spoofing de IP**:

* **Risco**: Usado para ataques como DDoS e bypass de firewalls.
* **Mitigação**: Filtragem de pacotes e uso de sistemas de prevenção de intrusões (IPS).

1. **Spoofing de MAC**:

* **Risco**: Permite acesso não autorizado ou interceptação de tráfego.
* **Mitigação**: Port Security em switches e monitoramento de rede.

**Segurança de Rede**:

* Implementar múltiplas camadas de segurança, incluindo criptografia, segmentação e políticas de segurança robustas, para proteger contra ameaças associadas a IP e MAC.