**Definição e Função:**

Endereços IP (Internet Protocol) são identificadores numéricos atribuídos a dispositivos em uma rede para roteamento de dados entre eles, enquanto endereços MAC (Media Access Control) são identificadores únicos atribuídos a interfaces de rede para comunicação dentro de uma rede local. O endereço IP facilita a comunicação entre redes diferentes, e o endereço MAC é essencial para a comunicação dentro da mesma rede local.

**Funcionamento:**

Endereços IP e MAC trabalham juntos para permitir a comunicação entre dispositivos. Quando um dispositivo envia dados, ele utiliza o endereço IP para encaminhar os pacotes através de diferentes redes e o endereço MAC para entregar os pacotes ao dispositivo correto dentro da rede local. Por exemplo, em uma rede Ethernet, o ARP (Address Resolution Protocol) mapeia o endereço IP para o endereço MAC correspondente para garantir que os pacotes sejam entregues corretamente.

**Configuração e Ferramentas:**

Endereços IP são configurados manualmente ou automaticamente através de DHCP (Dynamic Host Configuration Protocol). Endereços MAC são definidos pelo hardware e geralmente não mudam. Ferramentas como `ipconfig` (Windows) e `ifconfig` (Linux) permitem visualizar e configurar endereços IP. O Wireshark é usado para capturar pacotes e analisar endereços IP e MAC em tráfego de rede, identificando e diagnosticando problemas.

**Implicações Práticas e de Segurança:**

Endereços IP e MAC distintos são essenciais para gerenciamento de rede e diagnóstico de problemas, como identificar dispositivos e otimizar o tráfego. No entanto, questões de segurança incluem o spoofing de IP (onde um atacante finge ter um IP legítimo) e a falsificação de MAC (onde o atacante altera o endereço MAC para burlar filtros de segurança). Para mitigar esses riscos, é crucial implementar políticas de segurança como filtragem de MAC, uso de criptografia e monitoramento de tráfego para detectar comportamentos anômalos.