**NICOLE DE JESUS ALCANTARA**

**1. Definição e Função**

**Endereço IP (Internet Protocol Address):**

* **Definição:** Um endereço IP é um identificador único atribuído a cada dispositivo em uma rede que usa o protocolo IP para comunicação. Existem duas versões principais: IPv4 (por exemplo, 192.168.1.1) e IPv6 (por exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
* **Função:** O endereço IP permite que dispositivos se localizem e se comuniquem uns com os outros através de uma rede. Ele fornece a localização lógica e pode mudar conforme o dispositivo se conecta a diferentes redes.

**Endereço MAC (Media Access Control Address):**

* **Definição:** Um endereço MAC é um identificador único atribuído à interface de rede de um dispositivo (por exemplo, 00:1A:2B:3C:4D:5E). É geralmente um número hexadecimal de 48 bits.
* **Função:** O endereço MAC é usado para identificar dispositivos de forma física na rede local. Ele é atribuído pelo fabricante da interface de rede e permanece constante.

**2. Funcionamento**

**Como Endereços IP e MAC Trabalham Juntos:**

* **Estabelecimento de Comunicação:**
  1. **Resolução de Endereço:** Quando um dispositivo deseja se comunicar com outro, ele usa o endereço IP do destinatário. No nível da rede local, o dispositivo usa o protocolo ARP (Address Resolution Protocol) para mapear o endereço IP para um endereço MAC.
  2. **Transmissão de Dados:** O dispositivo envia pacotes de dados com o endereço IP do destinatário. Esses pacotes são encapsulados em quadros de dados que incluem o endereço MAC do destinatário. O switch de rede usa os endereços MAC para encaminhar o quadro para o dispositivo correto dentro da rede local.

**Exemplo:**

* Suponha que um computador (Com A) quer se comunicar com um servidor (Serv B) em uma rede local. Com A conhece o endereço IP de Serv B, mas precisa do endereço MAC para enviar os dados na camada de enlace. O ARP é usado para descobrir o endereço MAC correspondente ao IP de Serv B. Depois de resolver o endereço MAC, Com A pode encapsular os dados com o endereço MAC de Serv B e enviá-los através do switch.

**3. Configuração e Ferramentas**

**Configuração:**

* **Endereços IP:** Podem ser configurados manualmente (estático) ou atribuídos automaticamente por um servidor DHCP. Em sistemas operacionais, isso é feito através das configurações de rede.
* **Endereços MAC:** São atribuídos pela fabricante da interface de rede e não são configuráveis pela maioria dos usuários finais. Contudo, em alguns casos, é possível alterar o endereço MAC por software (spoofing).

**Ferramentas de Rede:**

* **ipconfig (Windows) e ifconfig (Linux):** Estas ferramentas mostram o endereço IP e o endereço MAC de um dispositivo. Exemplos de comandos:
  + ipconfig /all (Windows) ou ifconfig (Linux) exibe os endereços IP e MAC.
* **Wireshark:** Um analisador de pacotes que captura e exibe pacotes de rede, incluindo endereços IP e MAC dos dispositivos envolvidos na comunicação.

**4. Implicações Práticas e de Segurança**

**Implicações Práticas:**

* **Gerenciamento de Rede:** Endereços IP são usados para gerenciar a comunicação e roteamento de dados em uma rede maior, enquanto endereços MAC são usados para a comunicação dentro de uma rede local.
* **Diagnóstico de Problemas:** Problemas de rede podem ser diagnosticados observando o tráfego com ferramentas como Wireshark para identificar se há problemas com os endereços IP ou MAC.
* **Otimização de Desempenho:** Conhecer e configurar corretamente endereços IP e MAC pode ajudar a otimizar o desempenho da rede, evitando conflitos e melhorando o roteamento de tráfego.

**Questões de Segurança:**

* **Filtragem de MAC:** Pode ser usada para restringir o acesso a uma rede local. Contudo, a segurança baseada apenas em MAC pode ser insuficiente, pois endereços MAC podem ser falsificados.
* **Spoofing de IP:** Ocorre quando um atacante falsifica um endereço IP para se passar por outro dispositivo. Isso pode ser mitigado com a utilização de técnicas de autenticação e filtragem.
* **Mitigação:** Implementar medidas de segurança como VLANs (Virtual LANs), firewalls, e técnicas de criptografia pode ajudar a proteger a rede contra ataques que exploram endereços IP e MAC.