PADRÃO IEEE 802.11

Institute of Electrical and Electronics Engineers

Gabriel Nunes de Almeida

PADRÃO IEEE 802.11
WI-FI

O padrão IEEE 802.11, criado pelo Institute of Electrical and Electronics Engineers (IEEE), define as regras de funcionamento das redes locais sem fio (WLAN), conhecidas mundialmente como Wi-Fi.

Ele permite a transmissão de dados por meio de ondas de rádio, eliminando o uso de cabos e proporcionando mobilidade, praticidade e conectividade entre diferentes dispositivos — como notebooks, smartphones, tablets e até aparelhos domésticos inteligentes.

EVOLUÇÃO HISTÓRICA DO WI-FI

- 1997: 802.11 — 2 Mbps (primeira versão).
- 1999: 802.11a/b — até 54 Mbps.
- 2003: 802.11g — popularização do Wi-Fi.
- 2009: 802.11n — uso de múltiplas antenas (MIMO).
- 2013: 802.11ac — Wi-Fi 5 (até 6,9 Gbps).
- 2019: 802.11ax — Wi-Fi 6 (mais eficiência).
- 2024: 802.11be — Wi-Fi 7 (até 46 Gbps).

- Os diferentes padrões do Wi-Fi variam conforme a frequência de operação, a largura de banda e o alcance do sinal.
- As redes de 2,4 GHz têm maior alcance, pois o sinal atravessa melhor paredes e obstáculos, porém oferecem menor velocidade.
- Já as redes de 5 GHz e 6 GHz oferecem altas velocidades e menor interferência, mas o alcance é mais limitado.
- A largura de banda (como 20, 40, 80 ou 160 MHz) define a capacidade de transmissão: quanto maior, mais dados podem ser enviados simultaneamente.

INFRA-ESTRUTURADAS VS. AD-HOC

Existem dois modos principais de operação das redes Wi-FI

Rede infraestruturada

é a mais comum. Utiliza um ponto de acesso (Access Point) ou roteador, que gerencia todas as conexões e fornece acesso à Internet. É mais estável, organizada e segura

Rede ad-hoc

conecta os dispositivos diretamente entre si, sem precisar de um roteador. É útil em situações temporárias, como transferir arquivos entre dois notebooks

A principal diferença está na presença do ponto de acesso, que centraliza o tráfego na rede infraestruturada, enquanto na ad-hoc a comunicação é descentralizada.

SSID (SERVICE SET IDENTIFIER)

- O SSID é o nome identificador de uma rede Wi-Fi, aquele que aparece quando procuramos redes disponíveis no celular ou computador.
- Ele permite que os usuários reconheçam e escolham a rede correta para se conectar.
- Cada rede possui um SSID único, que pode ser visível, sendo transmitido automaticamente, ou oculto, quando o administrador decide não exibir o nome para aumentar a segurança.
- Exemplos de SSID: “Casa_5G”, “Campus_WiFi”, “Convidados_Unifor”.
- Mesmo redes diferentes podem usar o mesmo SSID, mas pertencendo a roteadores distintos.

PROBLEMAS DA ESTAÇÃO OCULTA E ESTAÇÃO EXPOSTA /PROTOCOLO CSMA/CA

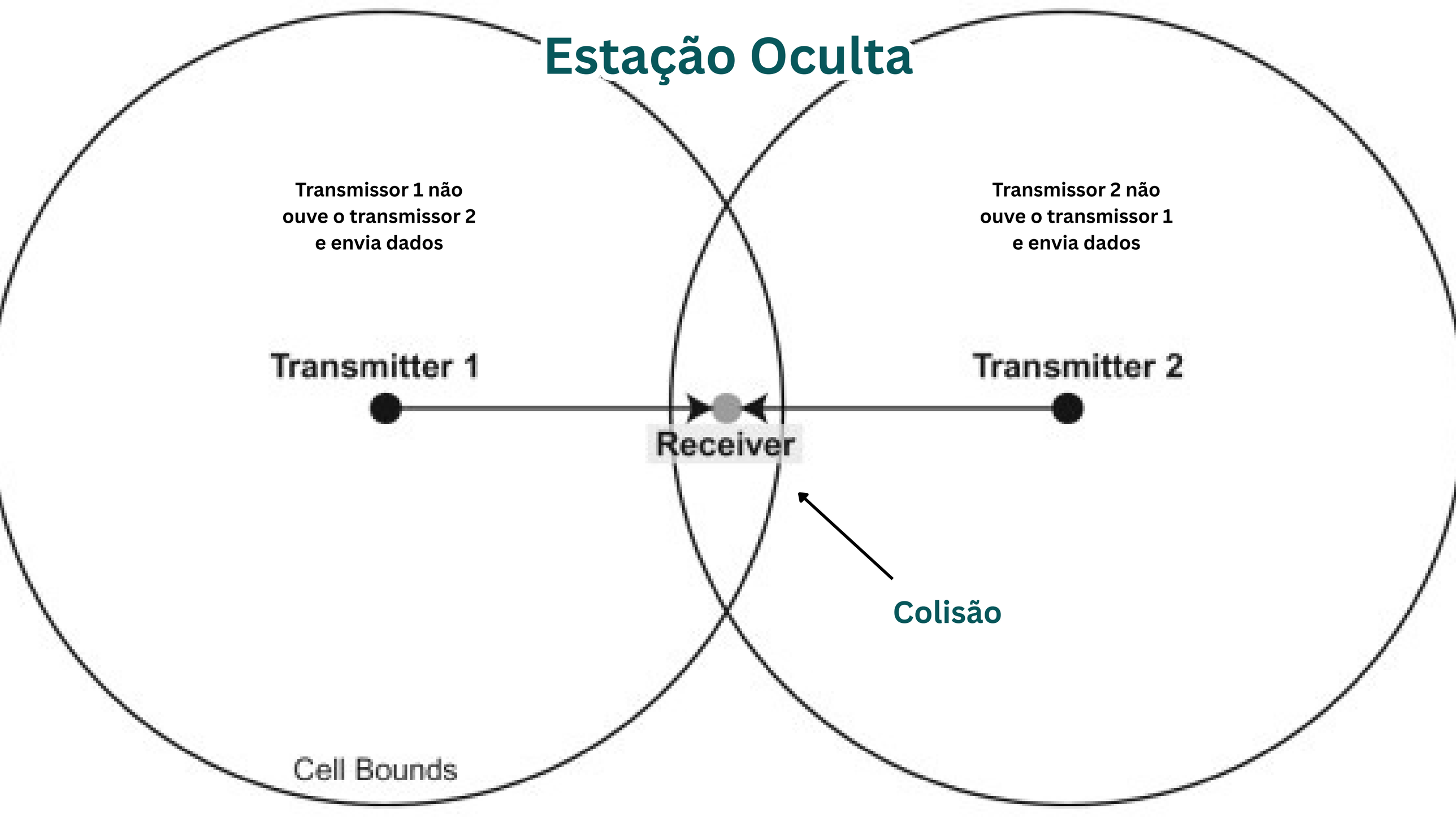
Em redes Wi-Fi, os dispositivos compartilham o mesmo meio de transmissão (o ar), o que pode causar colisões de dados.

Estação Oculta: ocorre quando duas estações não conseguem "se ouvir" porque estão fora do alcance uma da outra, mas ambas conseguem enviar dados ao mesmo ponto de acesso, gerando colisões.

Estação Exposta: acontece quando uma estação ouve outra transmitindo e, por precaução, deixa de enviar dados, mesmo que sua transmissão não causaria interferência.

Para lidar com isso, o Wi-Fi usa o protocolo CSMA/CA, que evita colisões verificando se o canal está livre antes de transmitir. Além disso, o método RTS/CTS (Request to Send / Clear to Send) ajuda a coordenar o envio de dados, reduzindo o risco de conflitos.

Estação Oculta



Estação Exposta

B ouve a transmissão de A e deixa de transmitir por precaução, mesmo que sua transmissão não cause interferência.

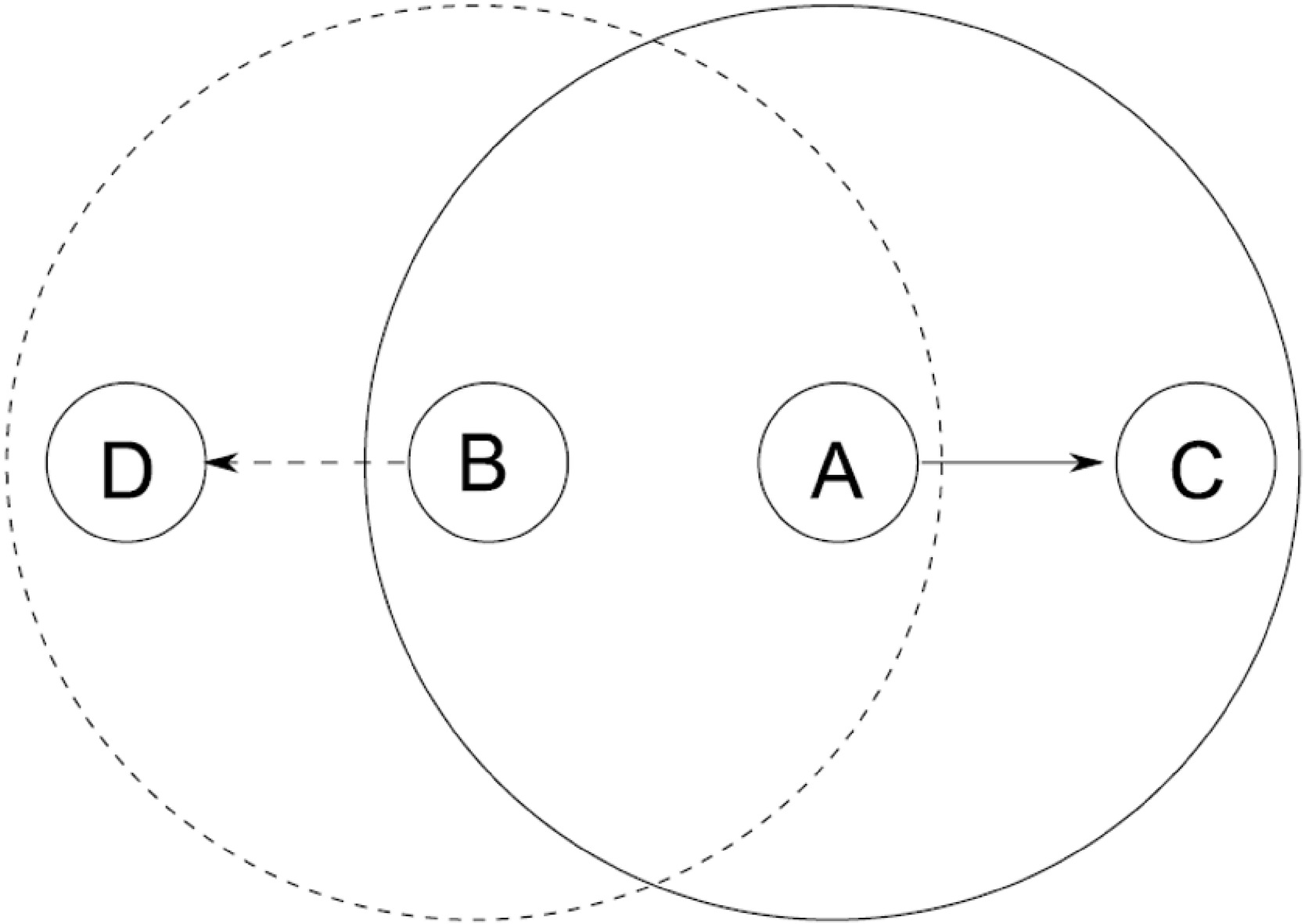


Figure 2: B is an exposed node.

PROBLEMAS DA ESTAÇÃO OCULTA E ESTAÇÃO EXPOSTA /PROTOCOLO CSMA/CA

O CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), para evitar colisões de dados antes que elas ocorram. Ele funciona primeiro verificando se o canal de transmissão está livre, esperando se necessário. Se o canal estiver ocioso, ele utiliza outros mecanismos, como o envio de uma mensagem de "pronto para enviar" (RTS) e recebimento de uma confirmação "limpo para enviar" (CTS), antes de realmente enviar os dados.

- **Carrier Sense (Detecção de Portadora):** Antes de iniciar a transmissão, um dispositivo verifica se o meio de comunicação (o canal sem fio) está livre. Se o canal estiver ocupado, ele espera.
- **Multiple Access (Acesso Múltiplo):** Vários dispositivos podem acessar o mesmo meio de transmissão, e o protocolo gerencia o acesso para evitar que todos transmitam ao mesmo tempo.
- **Collision Avoidance (Prevenção de Colisões):** Em redes sem fio, a detecção de colisões (CSMA/CD) é difícil. Por isso, o protocolo foca na prevenção. Para evitar colisões, os dispositivos podem:

SEGURANÇA NAS REDES WI-FI

A segurança é um aspecto fundamental das redes Wi-Fi, e seus protocolos evoluíram ao longo dos anos para proteger os usuários contra invasões.

- **WEP (1997): usava criptografia RC4, mas era facilmente quebrável. Foi rapidamente substituído.**
- **WPA (2003): introduziu o TKIP e trouxe pequenas melhorias de segurança.**
- **WPA2 (2004): passou a utilizar o padrão AES (Advanced Encryption Standard), muito mais robusto, e tornou-se o mais usado por mais de uma década.**
- **WPA3 (2018): trouxe o protocolo SAE (Simultaneous Authentication of Equals), que protege contra ataques de força bruta e oferece criptografia individual para cada conexão.**

Essa evolução garantiu que as redes Wi-Fi se tornassem cada vez mais seguras e confiáveis para usuários domésticos e corporativos.

O WI-FI É MAIS DO QUE UMA TECNOLOGIA — É O ELO INVISÍVEL QUE CONECTA O MUNDO MODERNO.

OBRIGADO PELA ATENÇÃO