

NEaD

Núcleo de Educação a Distância

CYBER SECURITY

F a c u l d a d e
IMPACTA

5

Comunicação sem fio

Alex Sandro da Silva Feitosa

Resumo

Neste texto falaremos sobre redes wireless, ou redes sem fio, que permitem a comunicação entre dispositivos sem a necessidade de cabos físicos, utilizando sinais de rádio para transmitir dados. Esse tipo de rede oferece mobilidade, flexibilidade e facilidade de instalação, sendo amplamente utilizada em ambientes domésticos, empresariais e públicos.

A LAN (Local Area Network) é uma rede local, geralmente cabeada, que conecta computadores e outros dispositivos dentro de um espaço físico limitado, como uma casa, escritório ou escola. Já a WLAN (Wireless Local Area Network) é uma variação da LAN que utiliza tecnologia sem fio (geralmente baseada no padrão Wi-Fi) para conectar os dispositivos, mantendo a estrutura lógica de uma LAN, mas sem a necessidade de fios.

Introdução

As redes wireless permitem a comunicação entre dispositivos sem o uso de cabos, utilizando sinais de rádio para a transmissão de dados. Elas oferecem vantagens como mobilidade, praticidade e fácil instalação, sendo comuns em diferentes ambientes. As LANs são redes locais cabeadas, enquanto as WLANs são redes locais sem fio que utilizam tecnologias como o Wi-Fi. Ambas possuem estruturas semelhantes, mas diferem na forma de conexão entre os dispositivos.

1.1. Comunicação sem fio

1.1.1 LAN versus WLAN

As WLANs usam Frequências de Rádio (RF) em vez de cabos na camada física e na subcamada MAC da camada de link de dados.

O IEEE adotou o portfólio 802 LAN/MAN de padrões de arquitetura de rede de computadores, que inclui dois grupos de trabalho dominantes 802.3 Ethernet, que definiu Ethernet para LANs com fio e 802.11 que definiu Ethernet para WLANs.

As WLANs também diferem das LANs com fio da seguinte forma:

As WLANs conectam clientes à rede por meio de um ponto de acesso sem fio (AP) ou roteador sem fio, em vez de um switch Ethernet.

As WLANs conectam dispositivos móveis que geralmente são alimentados por bateria, em vez de dispositivos LAN conectados. As placas de rede sem fio tendem a reduzir a duração da bateria de um dispositivo móvel.

WLANs suportam hosts que disputam acesso na mídia de RF (bandas de frequência).

As WLANs usam um formato de quadro diferente das LANs Ethernet com fio. As WLANs exigem informações adicionais no cabeçalho da Camada 2 do quadro.

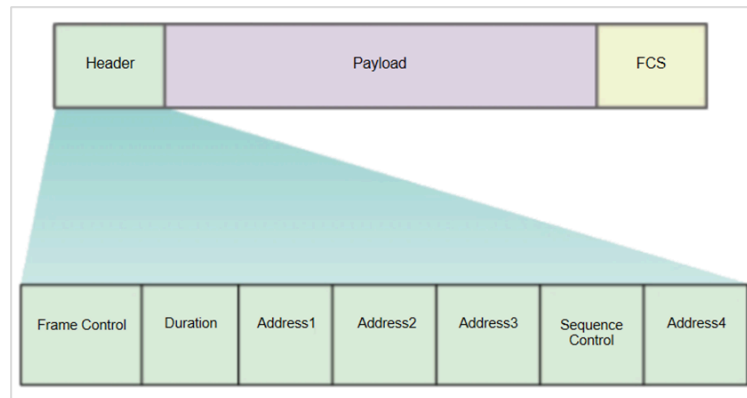
As WLANs levantam mais problemas de privacidade porque as frequências de rádio podem chegar fora das instalações.

A diferença entre WLAN e LAN com fio é resumida na tabela a seguir.

Característica	802.11 LAN sem fio	802.3 LANs Ethernet com fio
Camada física	Frequência de rádio (RF)	Cabos físicos
Acesso à mídia	Prevenção de colisão	Detecção de colisão
Disponibilidade	Qualquer pessoa com uma placa de rede sem fio ao alcance de um ponto de acesso	Conexão de cabo físico necessária
Interferência de sinal	Sim	Mínima
Regulamentações	Regulamentos diferentes por país	O padrão IEEE dita

Todos os quadros sem fio 802.11 contêm os seguintes campos:

Figura 1.1. Estrutura do quadro 802.11



Fonte: CCNA Cyber OPS Associate v1, 2020.

Frame Control ou Controle do quadro - Identifica o tipo de quadro sem fio e contém subcampos para versão do protocolo, tipo de quadro, tipo de endereço, gerenciamento de energia e configurações de segurança.

Duration ou Duração - Normalmente usado para indicar a duração restante necessária para receber a próxima transmissão de quadro.

Address1 ou Endereço 1 - Endereço MAC do dispositivo sem fio receptor ou AP.

Address2 ou Endereço 2 - Endereço MAC do dispositivo sem fio transmissor ou AP.

Address3 ou Endereço 3 - Endereço MAC do destino, como a interface do roteador com o AP conectado.

Sequence Control - Controle de sequência - Contém informações para controlar o sequenciamento e os quadros fragmentados.

Endereço 4 - Geralmente está ausente, pois é usado apenas no modo ad hoc.

Payload ou Carga útil - contém os dados para transmissão.

FCS – Usado para controle de erros da camada 2.

CSMA/CA

As WLANs trabalham na estrutura de transmissão half-duplex.

Half-duplex significa que apenas um cliente pode transmitir ou receber dados a qualquer momento.

O meio compartilhado significa que todos os clientes sem fio podem transmitir e receber no mesmo canal de radiofrequência.

Isso gera um problema porque um cliente sem fio não pode escutar enquanto está enviando, tornando assim impossível detectar uma colisão.

Como resolvemos esse problema?

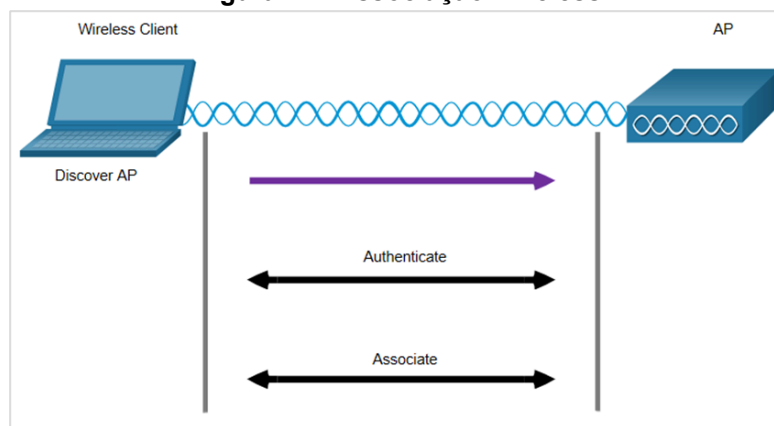
As WLANs usam o método CSMA/CA - Carrier Sense Multiple Access com Collision Avoidance, determinando assim como e quando enviar dados na rede

Um cliente sem fio faz o seguinte:

- Escuta o canal para ver se ele está ocioso. O canal também é chamado de portadora.
- Envia uma mensagem Ready To Send (RTS) ao AP para solicitar acesso dedicado à rede.
- Recebe uma mensagem Clear To Send (CTS) do AP concedendo acesso para enviar.
- Se o cliente sem fio não receber uma mensagem CTS, ele aguardará um período aleatório antes de reiniciar o processo.
- Depois de receber o CTS, ele transmite os dados.
- Todas as transmissões são confirmadas.

Associação de cliente sem fio e ponto de acesso.

Figura 1.2. Associação Wireless



Fonte: CCNA Cyber OPS Associate v1, 2020.

Para que os dispositivos de rede sem fio possam se comunicar, eles devem primeiro se associar a um Access Point ou roteador wifi.

Uma parte importante do processo 802.11 é descobrir uma rede WLAN e conectar-se a ela.

Os dispositivos de rede sem fio concluem o seguinte processo de três estágios, conforme mostrado na figura:

- Descobrir um novo AP sem fio.
- Autenticar-se no ponto de acesso
- Associar-se ao ponto de acesso

Para conseguir uma associação bem-sucedida, um cliente de rede sem fio e um access point devem concordar com parâmetros específicos. Os parâmetros devem ser configurados no AP e no cliente. Os parâmetros da rede sem fio configuráveis incluem:

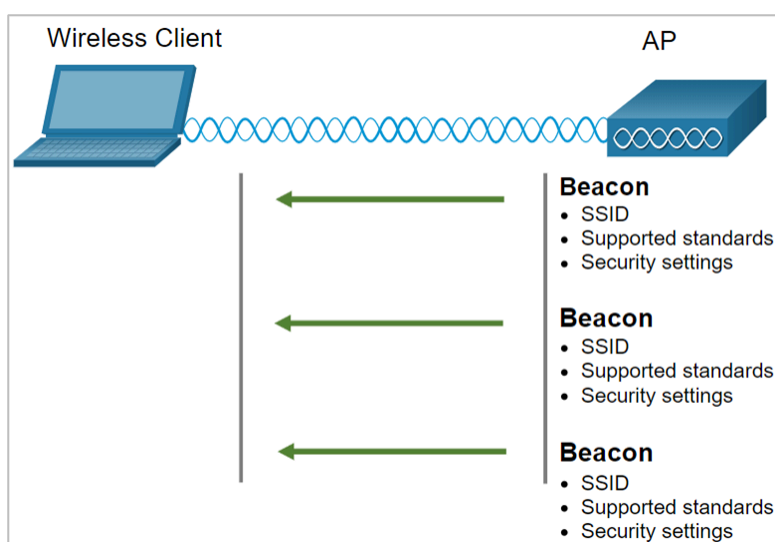
- SSID - O nome SSID aparece na lista de redes wireless disponíveis em um cliente.
- Senha - É necessário senha, no cliente wifi, para se autenticar no ponto de acesso.
- Modo de rede - Refere-se aos padrões de WLAN 802.11a/b/g/n/ac/ad.

- Modo de segurança - Isso se refere às configurações de parâmetros de segurança, como WEP, WPA ou WPA2. Sempre habilite o nível de segurança mais alto suportado.
- Configurações do canal - Refere-se às bandas de frequência usadas para transmitir dados na rede sem fio.

Modo de descoberta passiva e ativa

Os dispositivos da rede sem fio devem encontrar e conectar-se a um access point ou roteador wireless. Os clientes sem fio se conectam ao AP usando um processo de varredura (sondagem), como passivo e ativo.

Figura 1.3. Modo de descoberta passiva



Fonte: CCNA Cyber OPS Associate v1, 2020.

Modo passivo

Nesse modo, o AP anuncia abertamente sua rede, enviando periodicamente informações sobre seu SSID, padrões suportados e configurações de segurança.

O objetivo principal do beacon é permitir que os clientes da rede sem fio aprendam quais redes e access point estão disponíveis em uma determinada área.

Isso permite que os clientes sem fio escolham qual rede e ponto de acesso usar.

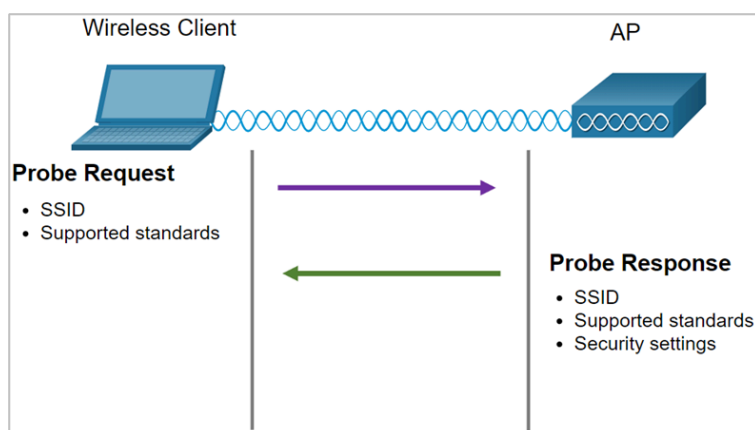
Modo Ativo

Neste modo, os clientes sem fio devem saber o nome do SSID.

O cliente da rede sem fio inicia o processo transmitindo um quadro de solicitação de investigação em vários canais, incluindo o nome SSID e os padrões suportados.

Os pontos de acesso configurados com o SSID enviarão uma resposta do “probe” que inclui o SSID, os padrões suportados e as configurações de segurança.

Figura 1.3. Modo de descoberta ativa



Fonte: CCNA Cyber OPS Associate v1, 2020.

O modo ativo pode ser necessário se um AP estiver configurado para não transmitir quadros de beacon.

Um cliente sem fio também pode enviar uma solicitação de análise sem um nome SSID para descobrir redes WLAN próximas. Os pontos de acesso configurados para transmitir quadros de beacon responderiam ao cliente sem fio com uma resposta do “probe” e forneceriam o nome SSID.

Conclusão

Compreender a diferença entre LAN e WLAN é essencial para reconhecer as diversas formas de conexão em redes atuais. As redes wireless se destacam por sua flexibilidade e ampla aplicação, sendo uma evolução prática das redes locais tradicionais. Mesmo com suas diferenças, ambas as redes desempenham papéis importantes na comunicação digital do dia a dia.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em <<https://www.netacad.com>>.

SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes: primeiros passos**. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security: applications and standards**. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002: Tecnologia da informação**.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000.