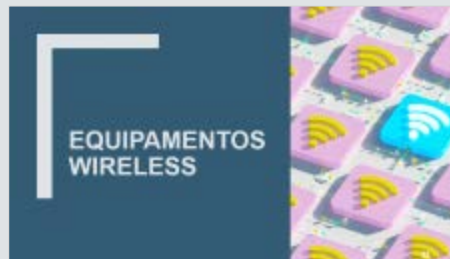


REDES DE COMPUTADORES

Prof. Priscilla Cunha
pcunha@uni9.pro.br

Agenda





REDES SEM FIO – REDES WIRELESS





Sistema flexível de
comunicação



É uma extensão ou
uma alternativa às
redes tradicionais



Dados são
transmitidos em ondas
eletromagnéticas pelo
ar



Sem cabos



Traz mobilidade



Padrão IEEE 802.11



Vantagens:

Fácil de instalar

Barata

Mobilidade

Flexibilidade

Escalabilidade



Desvantagens:

Baixa segurança

Interferências

Velocidades mais baixas

Histórico



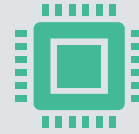
1986

Em 1986 a transmissão digital de sinais foi autorizada para uso militar. Aqui tínhamos a primeira ideia de redes sem fio.



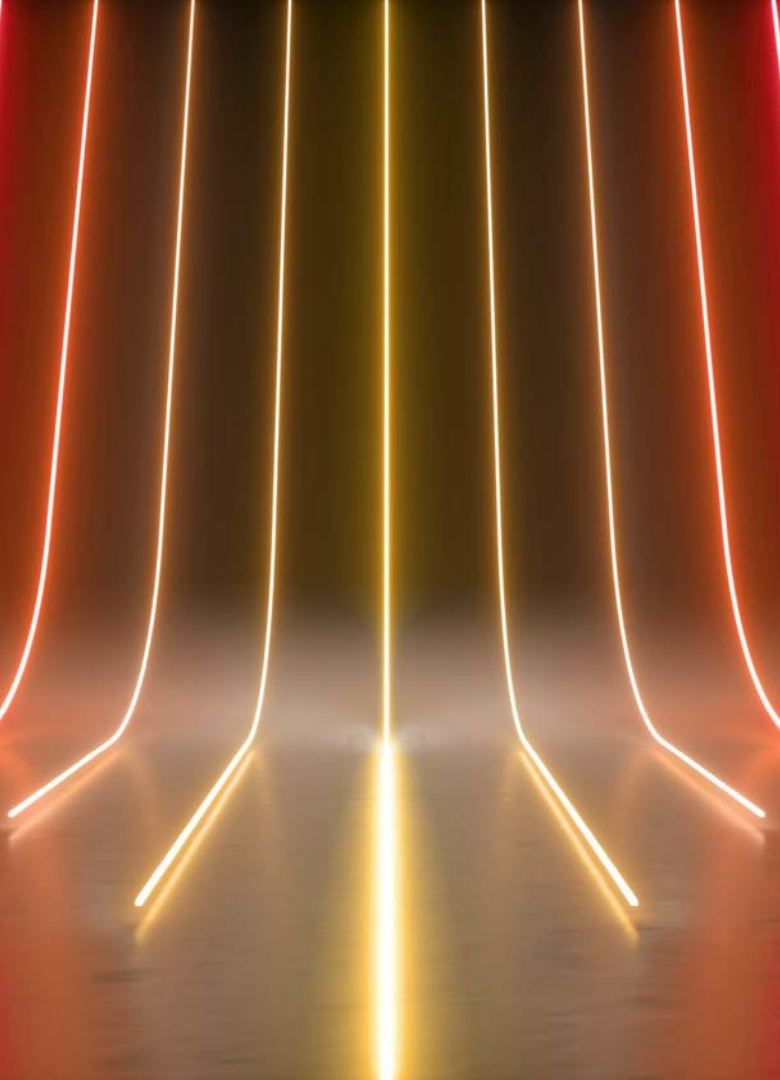
1995

Em 1995 a tecnologia wireless foi lançada pela primeira vez: o Bluetooth (Ericson)



1997

Em 1997 o IEEE lançou o padrão 802.11 para regulamentar as redes sem fio



FUNCIONAMENTO



Cabos e placas de rede ethernet não são necessários



Precisamos de um dispositivo base ou transceptor (access point) que recebe e transmite os sinais entre os hosts

- Também precisamos de placas de rede wireless nos hosts
- Ondas eletromagnéticas são usadas para se comunicar
- Essas ondas são ondas de rádio, que transportam a informação, são conhecidas como portadoras de rádio



Os dados transmitidos são inseridos na onda portadora (modulação), e são extraídos na recepção final (demodulação).



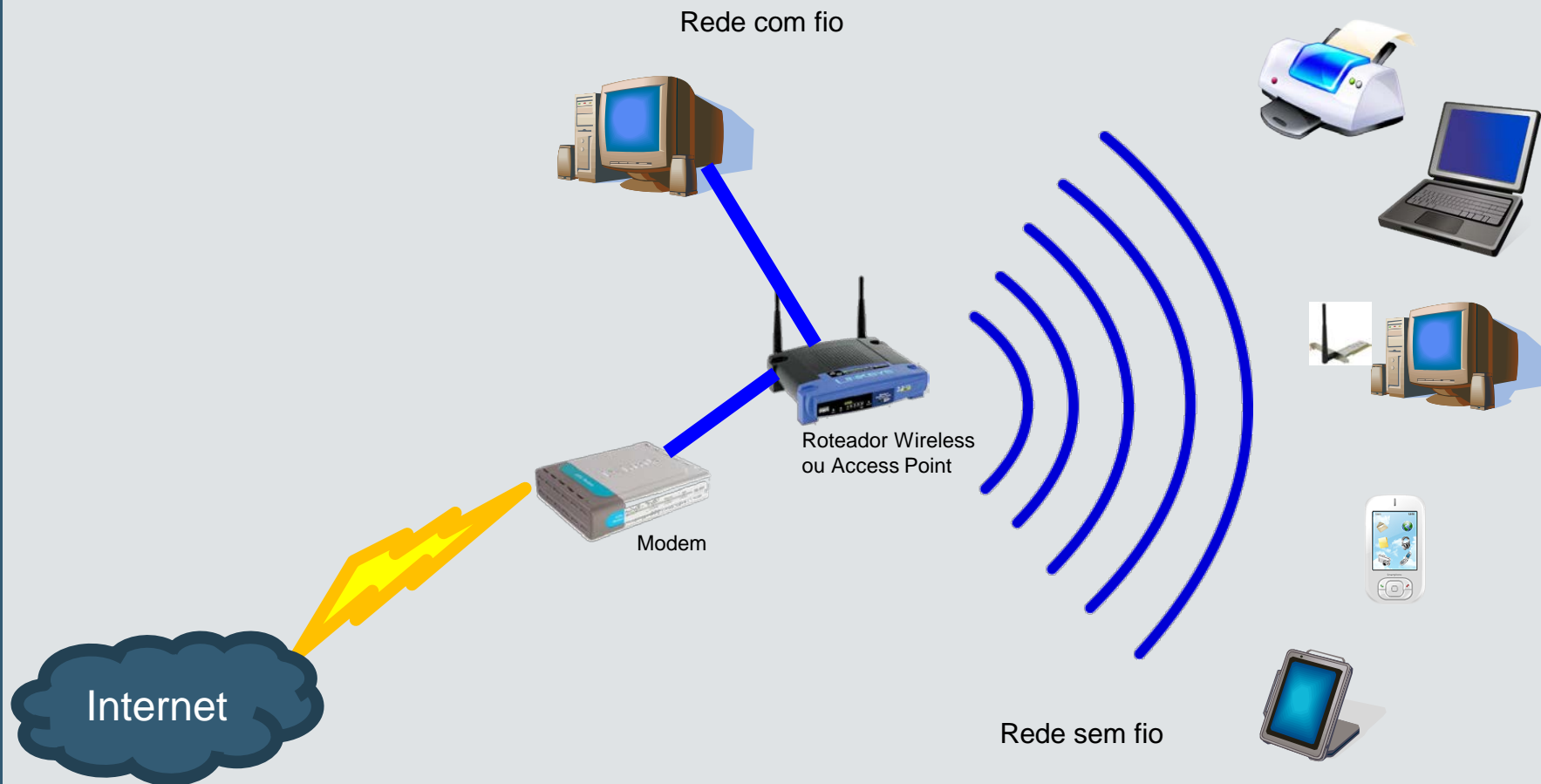
O access point retransmite os dados para hosts wireless, para outros AP's e também pode transmitir para a rede cabeada, pois o AP pode ter hosts ligados a ele via cabo



Usamos um cabo par trançado para ligar o AP ao modem ADSL se quisermos ter acesso a internet pela rede wireless



Um AP suporta alguns hosts e, se necessário, podemos usar mais AP's para aumentar seu alcance



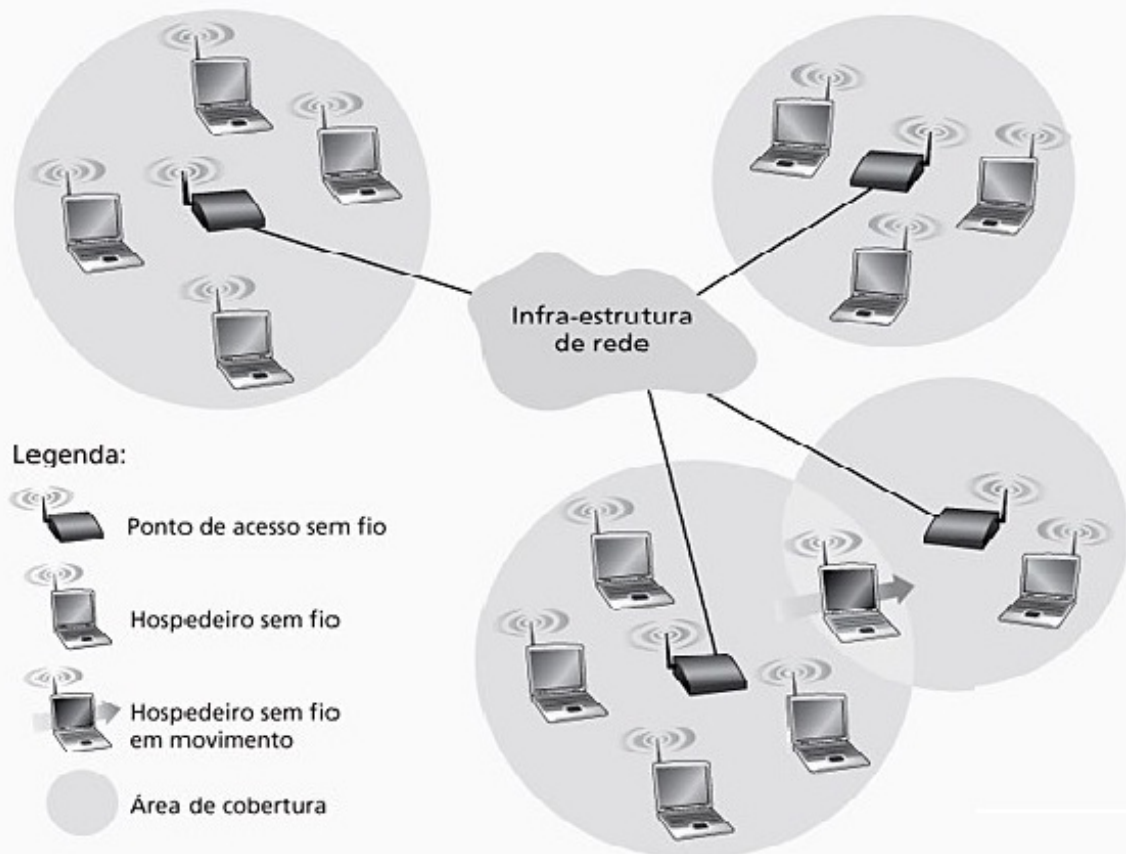
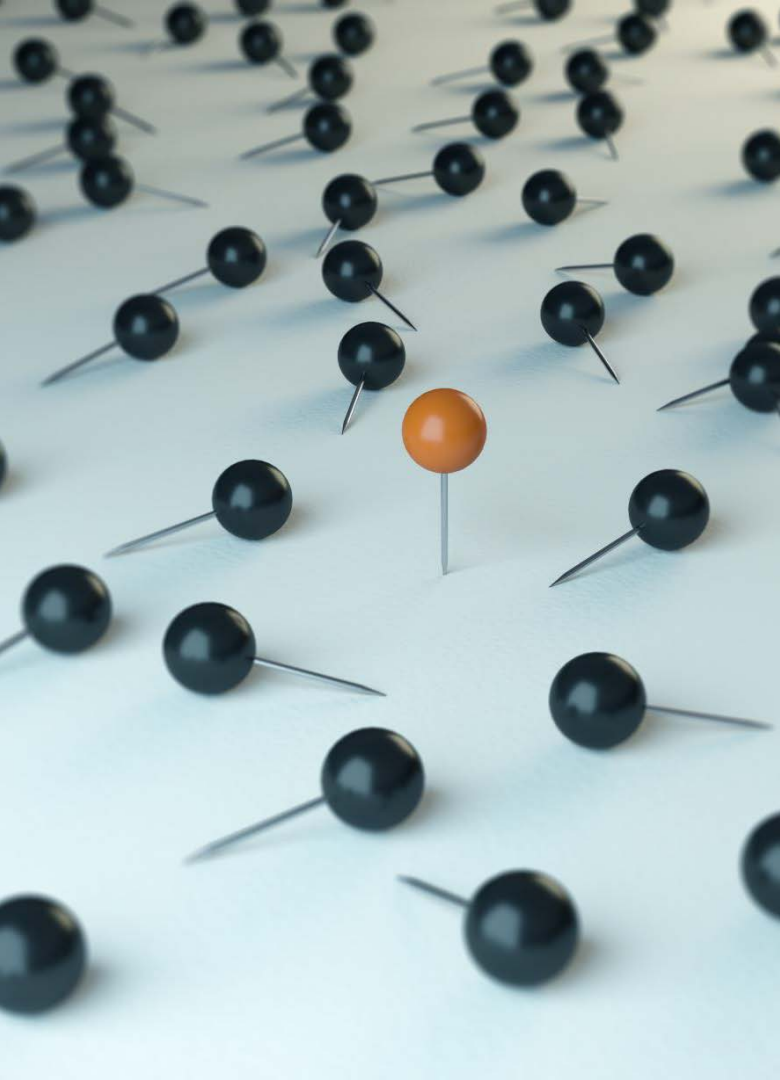


Imagem do livro Redes de Computadores e a Internet – J. F. Kurose

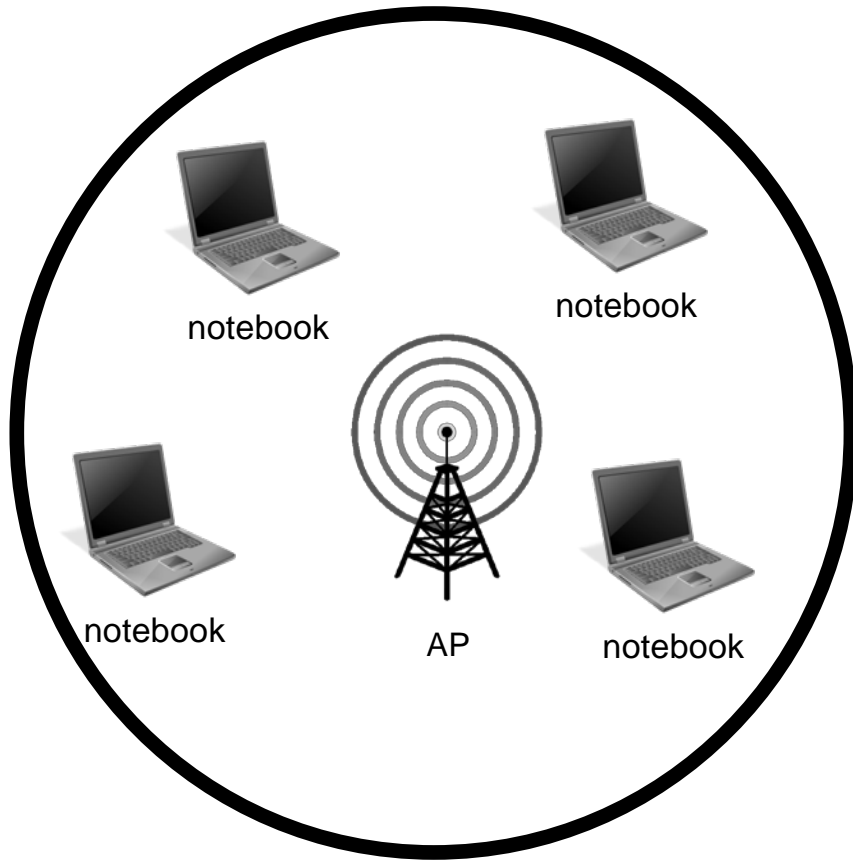


TOPOLOGIAS

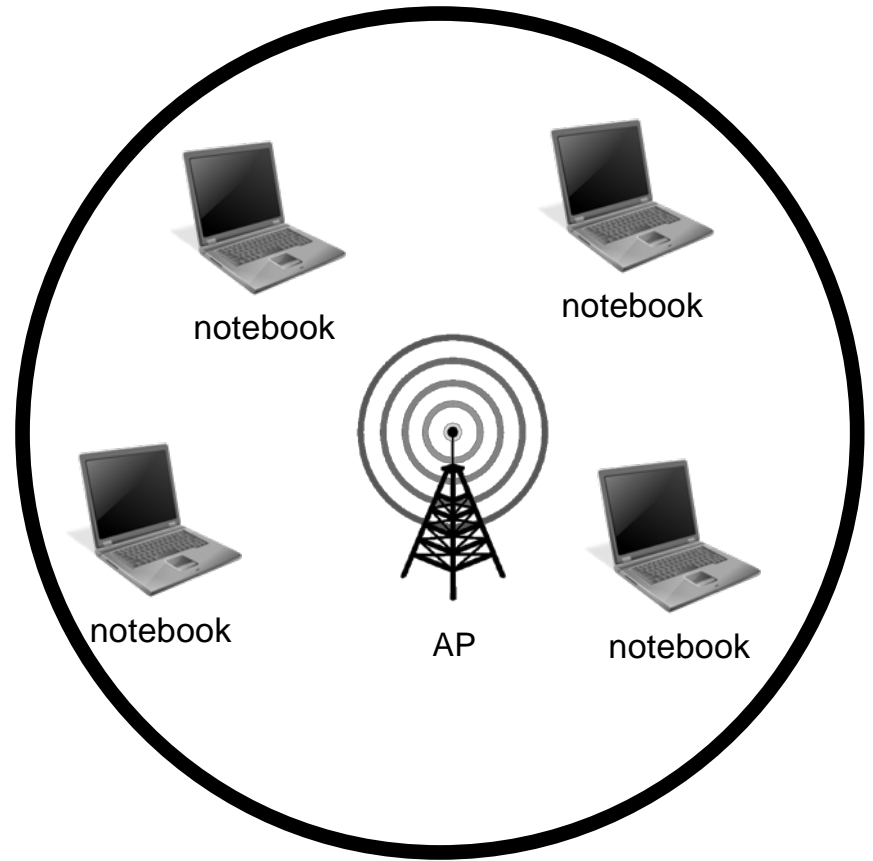
- O IEEE, quando definiu o padrão 802.11 de redes wireless, fundamentou a arquitetura a divisão da área coberta pela rede em células.
- Essas células são chamadas BSA (Basic Service Area) e seu tamanho depende de fatores como o ambiente e a potência dos dispositivos envolvidos na comunicação.

- Um grupo de hosts se comunicando em uma BSA constitui um BSS (Basic Service Set – conjunto básico de serviço).

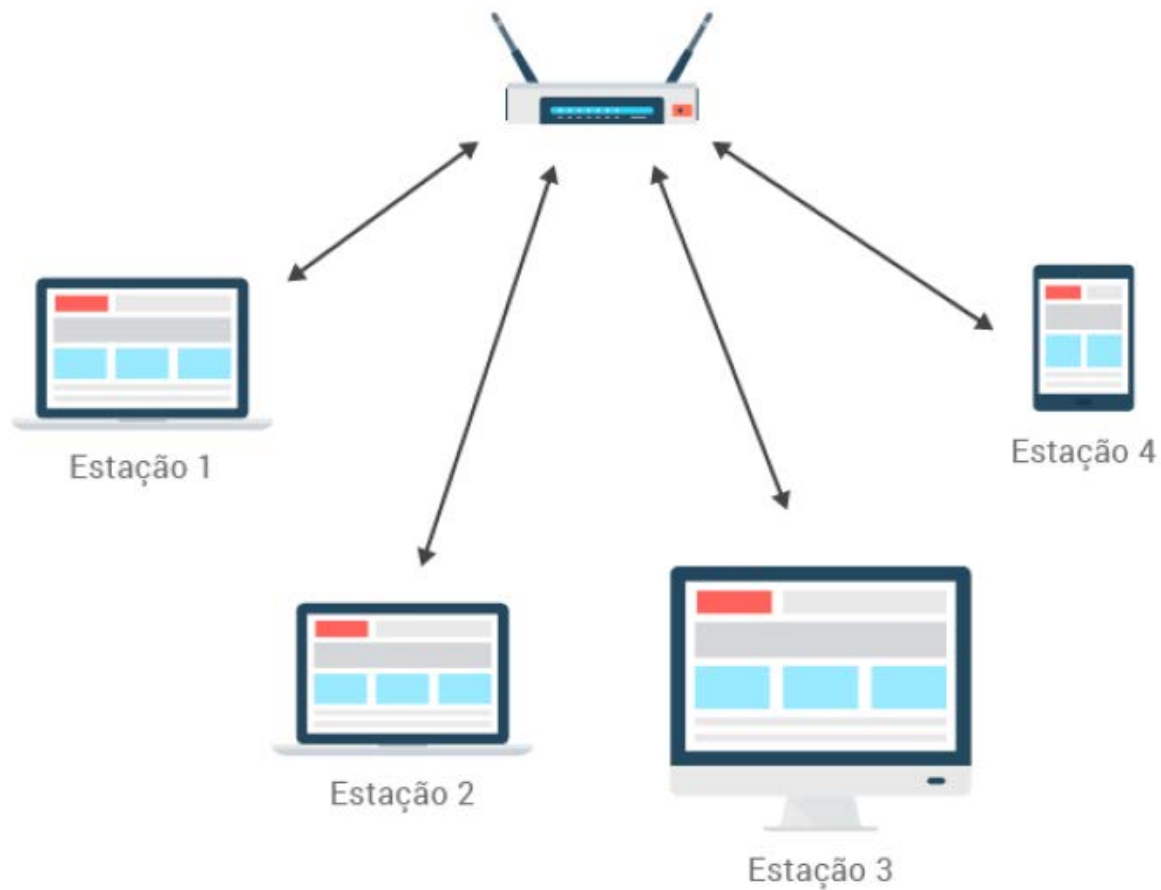
- BSS – Basic Service Set
 - Hosts se comunicam através de um ponto comum, o Access Point
 - Comunicação não ocorre sem passar pelo AP
 - Tem dois ou mais hosts wireless e o AP



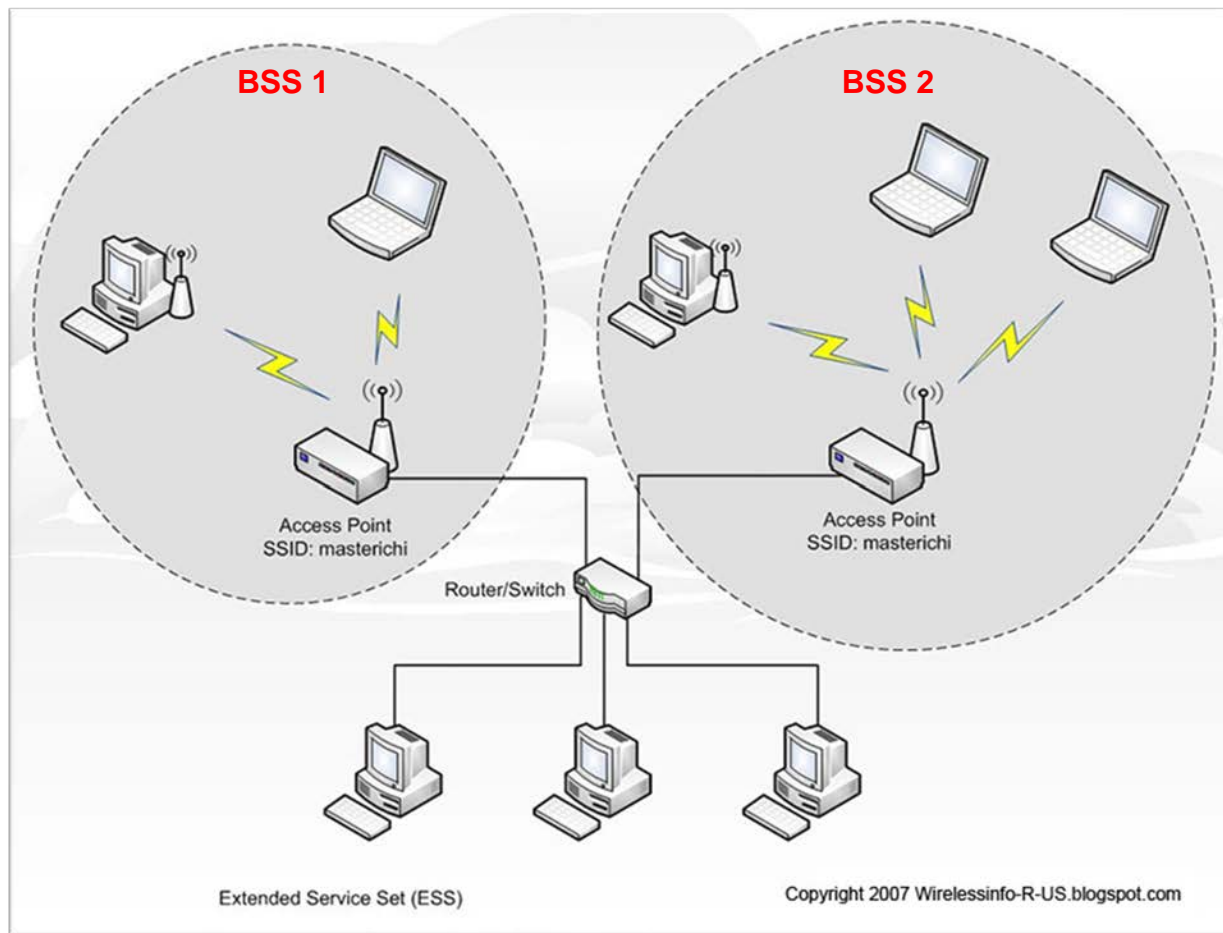
BSS 1

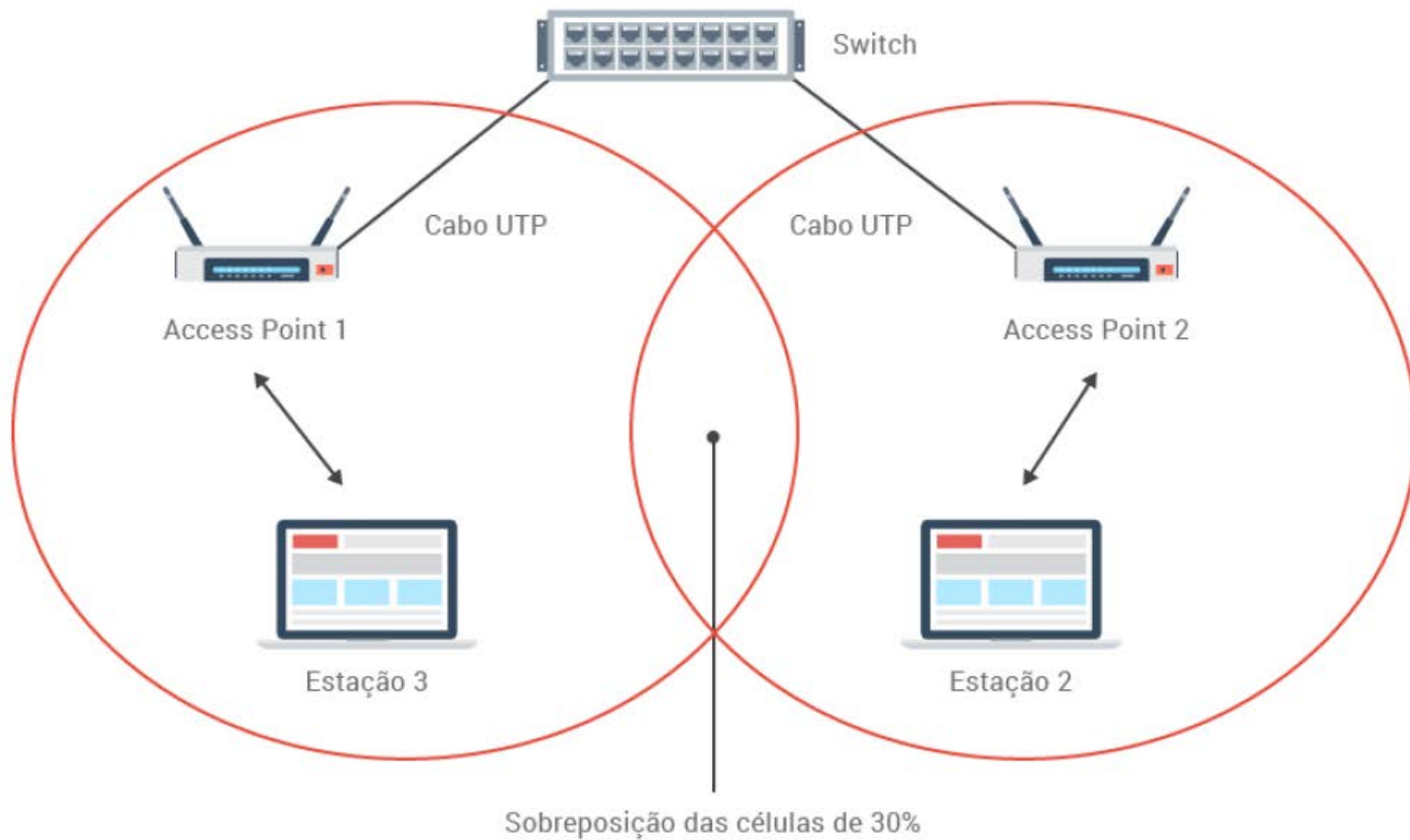


BSS 2

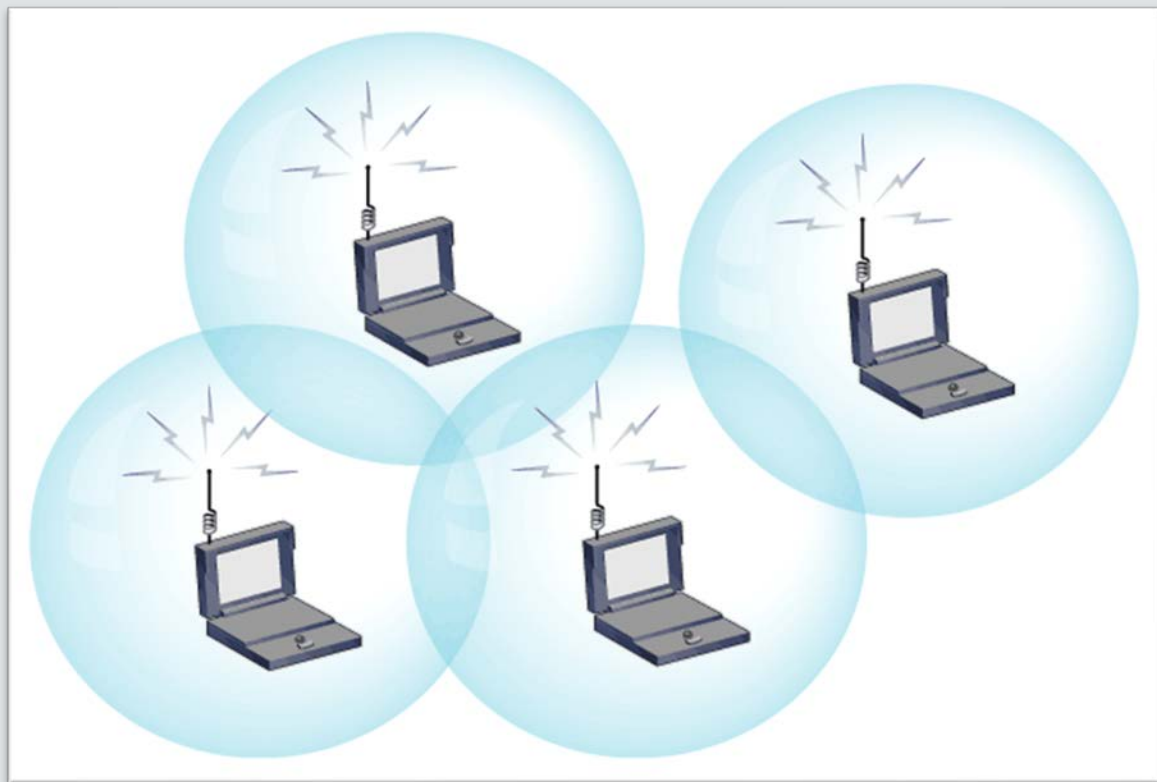


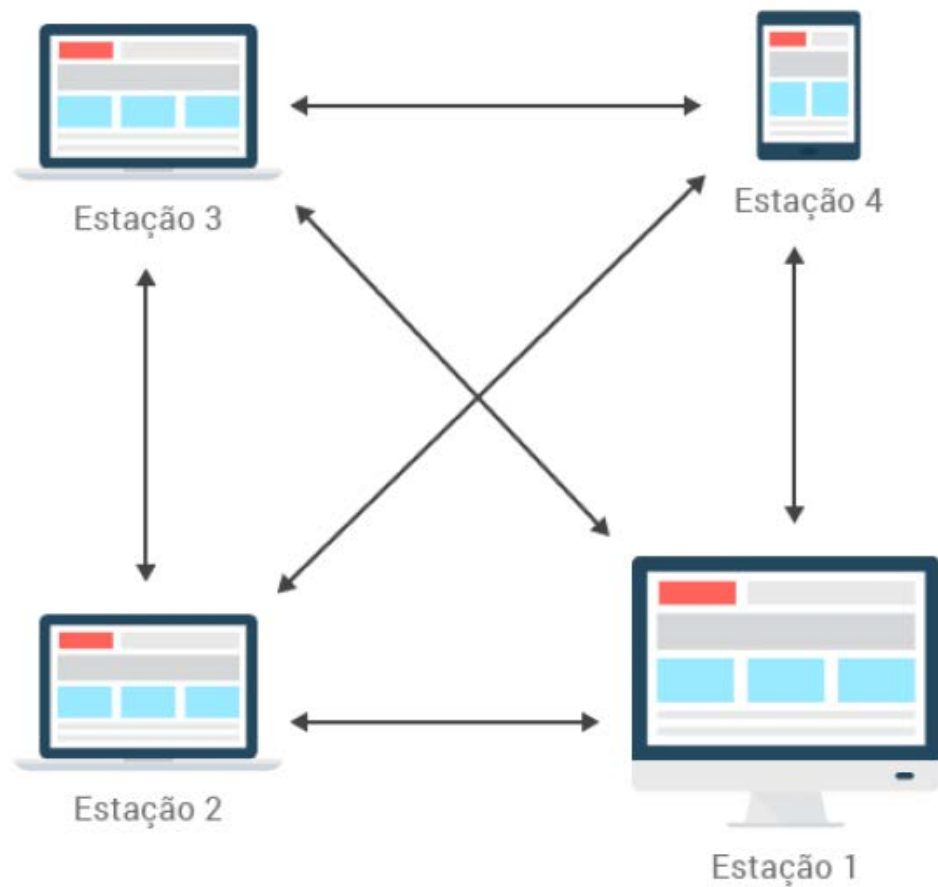
- ESS – Extended Service Sets
 - Conjunto estendido de serviços
 - Composto por vários BSS's, com os access points conectados a um DS (Distribution System – Centro de Distribuição)
 - Os APs geralmente se conectam ao DS via rede ethernet (cabeada)
 - Essas várias BSSs interligadas através de um DS é que são chamadas de ESS





- IBSS – Independent Basic Service Set
 - Também conhecida como redes ad hoc
 - É uma conexão ponto a ponto
 - Topologia wireless em que os 2 hosts se comunicam sem o uso do access point
 - Tem que configurar as placas de rede (usando o sistema operacional)
 - Velocidade é a mesma
 - Alcance do sinal é menor







PADRÃO 802.11



O quadro é o mesmo das redes ethernet



Pode se comunicar a até 100m



Temos 5 padrões definidos pelos IEEE:
802.11a, 802.11b, 802.11g e 802.11n,
802.11ac

- Foi criado por um grupo do IEEE em 1990
- Em 1997 foi aprovado p padrão 802.11 (1 a 2 Mbps)
- Em 1999 surgiram os padrões 802.11a (54 Mbps) e 802.11b (11 Mbps)
 - O padrão b surgiu alguns meses antes, e apesar de sua velocidade menor, ganhou mais mercado

- Em 1999 criou-se um comitê que tinha como objetivo alcançar a interoperabilidade
- Em 2000 surgiram os primeiros hot spots públicos e o termo wi-fi
- Em 2003 surgiu o padrão 802.11 g
- Em 2006 surgiu o padrão 802.11 n
- Em 2012 surgiu o padrão 802.11 ac



IEEE 802.11a

- Velocidade de até 54 Mbps
- Frequência: 5 GHz
- Suporta até 64 hosts por AP
- Sem interferências
- Incompatível com os padrão b e g



IEEE 802.11b

- Velocidade de até 11 Mbps
- Frequência: 2,4 GHz (mesma de telefones móveis, microondas e bluetooth)
- Suporta até 32 hosts por AP
- Baixo custo
- Devido a sua faixa de frequência, sofre muitas interferências



IEEE 802.11g

- Velocidade de até 54 Mbps
- Frequência: 2,4 GHz
- Compatível com dispositivos do padrão 802.11b
- Possui o mesmo problema de interferências do 802.11b



IEEE 802.11n

- Velocidade de até 104 Mbps
- Frequência: 2,4 e 5 GHz
- Pode atingir até 600 Mbps com configuração MIMO (Multiple Input, Multiple Output)
- Compatível com os demais padrões



IEEE 802.11ac

- Desenvolvido entre 2011 e 2013
- Pode chegar a 1 Gbps, a depender da quantidade de antenas no AP
- Trabalha na frequência de 5 GHz
- APs suportam até 8 antenas
- Compatível com os demais padrões, mas funciona melhor com dispositivos de padrão ac
- Ainda é bem caro

- O padrão ac trabalha com a tecnologia Beamforming, que oferece emissão inteligente, reforçando o sinal nos locais onde há dispositivos conectados
- Com esse recurso os problemas com os pontos cegos, ou seja os locais aonde o sinal não chegava são parcialmente resolvidos

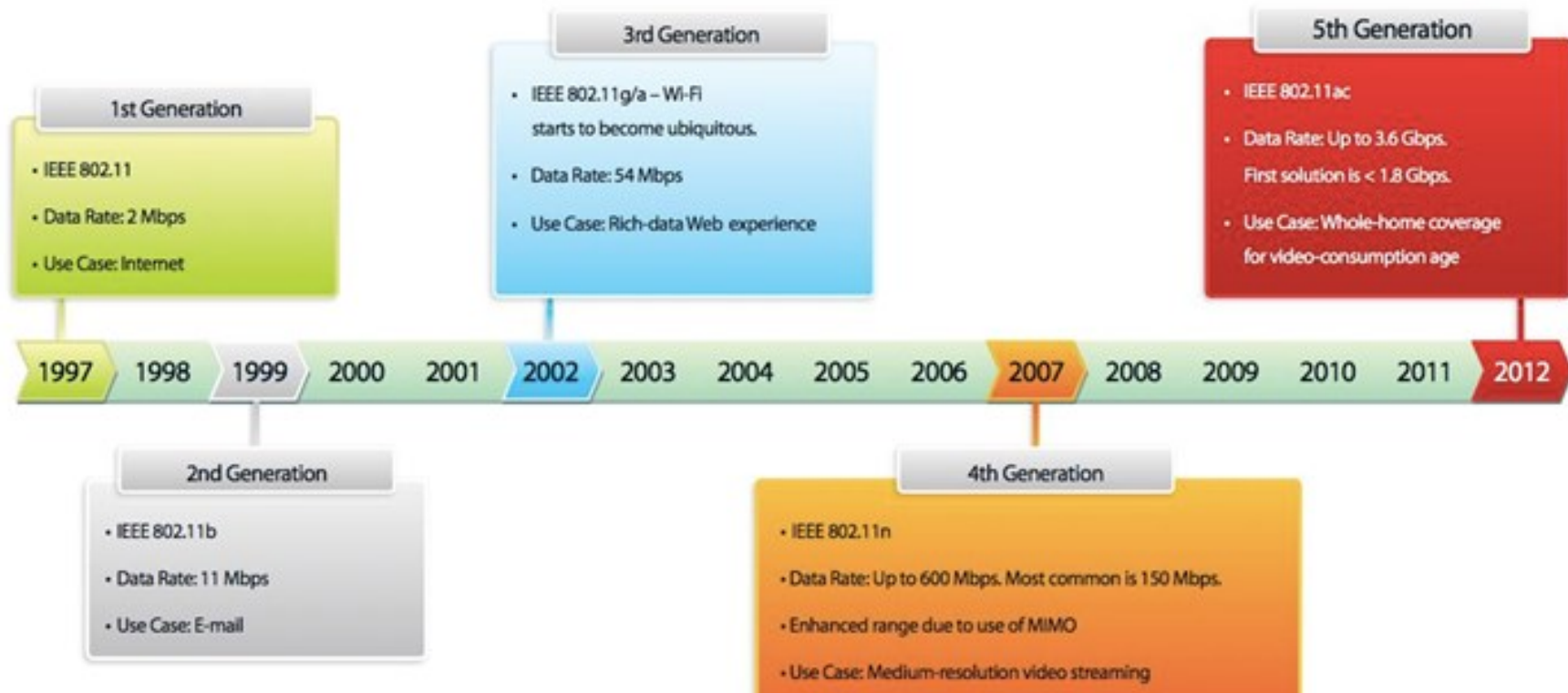


Today's WiFi



802.11ac Beamforming Technology

- Vale destacar que essa é a transferência de dados entre os dispositivos na rede e não a velocidade da Internet, que depende do provedor.
- Isso se aplica a todos os padrões



Antenas



- Para que possamos aumentar o alcance de nossa rede wireless, podemos usar 3 tipos de antenas:

Yagi

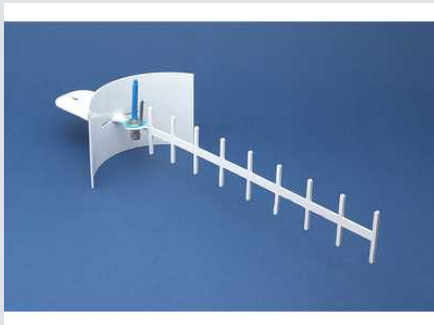
- Maior alcance que a antena original do AP (pode passar 500m)
- Cobrem apenas a área para onde estão apontadas

Omnidirecionais

- Cobrem uma área circular ao redor da antena
- Pode-se usar uma antena da potência desejada (alcance na casa de kms)

Miniparabólicas

- Transmitem e recebem apenas na direção que estão apontadas
- Seu alcance é o maior dos 3 tipos



YAGI



OMNIDIRECIONAL



MINIPARABÓLICA



SEGURANÇA EM REDES WIRELESS

- As redes sem fio são bastante vulneráveis quando se trata do assunto segurança, pois como o sinal trafega em forma de ondas eletromagnéticas, e controlar sua abrangência e acesso é bastante complicado.

- Seu alcance pode ultrapassar as barreiras de sua empresa e sua informação estar trafegando por aí, possibilitando seu acesso por pessoas não autorizadas.

- Além de as redes sem fio serem relativamente novas (se comparadas às redes cabeadas), elas são muito mais fáceis de instalar e configurar, sendo uma realidade na vida de todos e não apenas das empresas.
- Com isso, é fácil perceber que devemos proteger as redes sem fio, seja em nossa residência ou nas empresas.

- Principais problemas de segurança das redes sem fio:
 - Sem controle de acesso
 - Sem comunicação criptografada
 - Uso de senha padrão
 - Uso de nome de rede padrão

- Podemos usar para proteger as redes sem fio:
 - SSID
 - WEP
 - WPA (e WPA 2)

SSID

- Código alfanumérico que identifica a rede (é o nome da sua rede) e os access points
- Quando o SSID não é alterado e fica como padrão de fábrica (em geral o nome do fabricante), o acesso indevido aos equipamentos e a rede é mais fácil, pois com isso é fácil descobrir o endereço IP padrão (e que permite acessar as configurações do AP)



WEP

- Método de segurança mais antigo usado em redes wireless, criado em 1999
- Fornece autenticação e criptografia de dados trocados pelo host e pelo AP
- Ao habilitar o WEP, uma chave de segurança passa a ser requerida para se conectar na rede wireless



- Ele é vulnerável, mas melhor do que nada. Quando associado a troca do SSID já é um primeiro passo na segurança
- Dispositivos mais antigos só possuem esse método de segurança

WPA

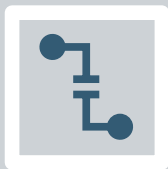
- Método de segurança mais seguro que o WEP, foi criado em 2003
- Trabalha com criptografia mais segura, com chaves maiores
- Equipamentos que trabalham com WPA podem não trabalhar com dispositivos WEP



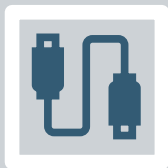
- Supri os problemas do WEP
- Teve uma evolução, o WPA2, que foi criado em 2006 e que implementou ainda mais segurança na comunicação wireless, mas também não funciona com os dispositivos antigos

EQUIPAMENTOS WIRELESS





Como já falamos, as redes sem fio não se limitam a computadores.



Temos os mais diversos dispositivos nessas redes, como notebooks, tablets, smartphones, e até televisão.

- Se um computador sem dispositivo wireless precisar ser incluído numa rede sem fio, será necessário o uso de uma placa wireless ou um adaptador USB wireless



- Já roteadores wireless (os Access Points), existem aos montes no mercado, de diversos modelos e fabricantes, para ambientes domésticos ou empresariais, com uma ou várias antenas, e nos mais variados padrões.

- Antes de comprar o seu equipamento wireless, seja para montar uma rede, seja para fazer com que um dispositivo acesse uma, é importante conhecer as características de cada aparelho para fazer a aquisição certa.
- Por exemplo, pode ser um desperdício comprar uma placa Wi-Fi 802.11n e um access point 802.11g.

The background of the image is a collage of film-related elements. On the left, a large, detailed film reel is visible. On the right, a clapperboard is partially shown, with text including 'PRODUCTION', 'DIRECTOR', 'CAMERA', 'SCENE', and 'TAKE'. A semi-transparent blue rectangle is centered over the image, containing the main text.

VÍDEOS E PARA SABER MAIS



Vídeo

- Entenda o WI-FI de uma VEZ por TODAS! -
<https://www.youtube.com/watch?v=V2XW8nxNjcc>
- A história do WiFi - TecMundo -
<https://www.youtube.com/watch?v=ko2IGeRtXZw>



Padrão 802.11 ax

- <https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/07/wi-fi-80211-ax-entenda-como-sera-o-proximo-padrao-de-conexao-sem-fio.html>
- <https://macmagazine.com.br/post/2018/01/08/vem-ai-um-novo-padrao-wi-fi-o-802-11ax/>
- <https://olhardigital.com.br/2017/09/05/noticias/asus-revela-roteador-com-a-nova-geracao-do-wi-fi-saiba-do-que-ele-e-capaz/>

Dúvidas???

