



AULA – DISPOSITIVOS WIRELESS

1

PC CARD

- Usado somente em notebooks;
- Serve para conectar o notebook a rede wireless;
- Possui antena interna embutida;



PLACAS PCI

- Usado somente em desktops;
- Serve para conectar o desktop a rede wireless;
- Possui antena externa acoplada a saída da placa;



ADAPTADORES USB

- Pode ser usado em notebooks ou desktops;
- Serve para conectar o notebook ou desktop a rede wireless;
- Possui antena interna embutida;



PONTOS DE ACESSO

- Concentra todo o tráfego da rede wireless além das conexões oriundas dos clientes.
- Possui um identificador que identifica a rede chamado **SSID**.
- Interface entre a rede wireless e a rede cabeada por possuir porta **UTP 10 ou 100Mbps**.
- Possui antena interna embutida.
- Suporta a conexão de antenas externas, na maioria dos casos.



GATEWAYS

- Conecta um pequeno número de dispositivos wireless a internet ou outra rede;
- Possui uma porta **WAN** e **várias portas LAN**. Geralmente tem um hub ou switch embutido e possui as funcionalidades de um Ponto de Acesso;



WDS



SEGURANÇA WI-FI

- Riscos maiores de invasão
 - Não é necessário acesso físico à rede para invadir
- Má configuração de Aps
 - Configuração padrão geralmente é insegura – sem criptografia e com SSID de rede padrão
- Clientes/Aps não autorizados
 - Não há autenticação e DHCP concede IP a qualquer um
- Interceptação de tráfego
 - Sniffer sem necessidade de acesso físico à rede
 - Vários protocolos com senha em texto simples (smtp; pop; ftp)



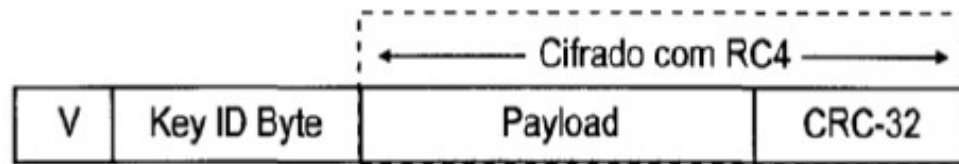
WEP

- WEP (Wired Equivalency Privacy)
 - Princípio: chaves simétricas distribuídas
 - Proposta: proteção contra interceptação (autenticidade; confidencialidade e integridade)
- Autenticação na camada de enlace
 - Chave RC4 – 40 bits (padrão)
 - Chave RC4 - 104 bits



WEP

- Vetor de Inicialização
 - É transmitido em claro
 - Curto: 24 bits
- Key ID Byte: Key Stream
- CRC-32
 - Faz a verificação da integridade dos dados
 - A segurança sugerida não pode ser considerada segura
 - Garante integridade sob ruído



WEP - RESTRIÇÕES

- Somente o cliente é autenticado
 - Aps falsos podem enganar os clientes
- RC4 possui falhas na geração
 - Geração da sequência quando é conhecida uma parte da chave
- Ferramentas de domínio público fazem descoberta de chaves Wep
 - Aircrack
 - WEPCrack



WEP - MELHORIAS

- Chave WEP de 104 bits para alguns fabricantes
- ACL baseado em MAC Address



WPA

- Wi-Fi Protected Access
- Especificado por um grupo de fabricantes chamado “Wi-Fi Alliance”
- Criptografia: TKIP
 - Temporal Key Integrity Protocol – chaves Wep mudam a cada envio de pacotes (RC4 modificado)
 - Chave possui 128 bits
- Autenticação
 - 802.1x e EAP (usuários corporativos)
 - Passphrase (Usuário doméstico)



WPA2

- WPA baseava-se em um draft da norma 802.11i
- Quando a norma foi finalizada, criou algumas melhorias e foi chamada de WPA2
 - Também conhecida por Robust Security Network (RSN)
- Melhorias
 - Mudança na criptografia de TKIP para o AES
 - Abandono do RC4;
 - Uso de CCMP (Protocolo usado para encriptação das mensagens transmitidas.)
- Requer mais mudanças que o WPA no HW e SW dos equipamentos pois é mais “pesado”



WPA2

- WPA2 = WPA + AES
- Criptografia simétrica AES
 - 128/192/256 bits
 - Criptografia de bloco/byte

WPS (WIFI PROTECTED SETUP)

- é um padrão criado pela Wi-Fi Alliance que dá aos usuários residenciais e de pequenas empresas uma maneira fácil de configurar a segurança Wi-Fi Protected Access.
- **PBC:** Com a Configuração de botão de ação, um botão (real ou virtual) é pressionado no ponto de acesso, ou registro da rede, e outro botão é pressionado no novo dispositivo sem fio que habilita a criptografia dos dados.
- **PIN:** Um rótulo com um número de identificação pessoal é fornecido em cada novo dispositivo sem fio que ingressa na rede. O PIN pode ser gerado dinamicamente na tela do dispositivo. Quando o novo dispositivo é detectado, você é solicitado a inserir o PIN no ponto de acesso sem fio ou registro da rede. Esse é o modelo base obrigatório que todo produto certificado para WPS deve seguir.

WPS (WIFI PROTECTED SETUP)

- **NFC:** Os leitores de comunicação em curta distância transferem as configurações da rede para um novo dispositivo sem a inserção manual do PIN. Quando um novo dispositivo sem fio se movimenta dentro da área de alcance do ponto de acesso, ou registro da rede, uma comunicação é estabelecida à curta distância permitindo que o PIN seja transferido.
- UFD:** Uma unidade flash USB também pode ser usada para transferir dados entre o novo dispositivo sem fio e o ponto de acesso, ou registro da rede. O suporte a esse modelo pelos fabricantes de dispositivos WPS é opcional.

- Fonte: <http://support.pt.kodak.com.br/>

POTÊNCIA DE TRANSMISSÃO E ALCANCE

- O alcance típico de uma rede 802.11g é de **30 metros** em espaços fechados (como uma casa ou um prédio, onde existem paredes e outros obstáculos) e **150 metros em campo aberto**, sem obstáculos.
- A potência total da transmissão é medida em **dBm (decibel milliwatt)**, enquanto o ganho da antena é medido em **dBi (decibel isotrópico)**.
- No caso da potência de transmissão, o parâmetro de comparação é um sinal de **1 milliwatt**.

UNIDADES DE POTÊNCIA - WATT

- Unidade básica de potência. É definido como 1 ampere(A) de corrente em 1 volt (V), logo:
- **potência = volt x ampere ($P=VA$).**
- O FCC permite no máximo **4 watts** de potência a ser radiado de uma antena em uma WLAN ponto multiponto sobre a frequência de 2.4Ghz.
- Pode não parecer muita potência, mas é o suficiente para enviar sinais RF claros por quilômetros.

UNIDADES DE POTÊNCIA - MILIWATT

- Em WLANs, níveis de potência são comumente expressos em **miliwatts(mw)**, ou seja **(1/1000w)**.
- Em um segmento WLAN típico indoor, os níveis de potência raramente ultrapassam 100mw;

DECIBEL

- **O DECIBEL** é uma relação logarítmica entre duas potências ou intensidades.
 - $P_{dB} = 10 \log_{10} (P_1/P_0)$ ou $I_{dB} = 10 \log_{10} (I_1/I_0)$
- Para isso foi introduzida uma razão de compressão logarítmica, o decibel (dB).
 - Ex.: O **decibel** é a unidade usada para medir a intensidade de um som.

DECIBEL MILLIWATT - DBM

- **dBm** ou **dBmW** (decibel miliwatt) é uma unidade de medida utilizada principalmente em telecomunicações para expressar a frequência absoluta mediante uma relação logarítmica. Define-se como o nível de potência em decibéis em relação ao nível de referência de um 1 mW.

a) Convertendo mw para dBm

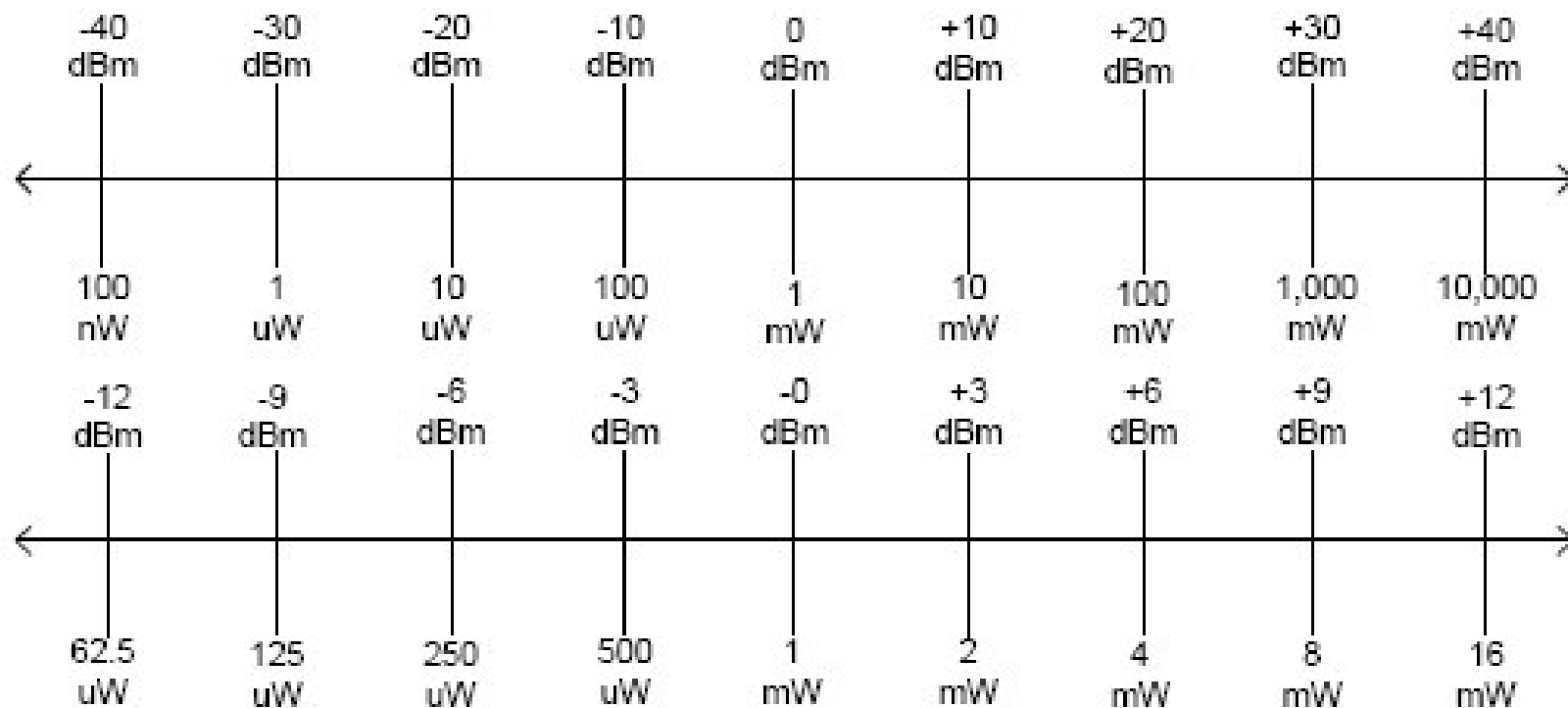
$$P_{dbm} = 10 \log P_{mW}$$

b) Convertendo dBm para mw:

$$P_{mW} = \log^{-1} \left(\frac{P_{dbm}}{10} \right)$$

0 dBm	1 milliwatt
3 dBm	2 milliwatts
6 dBm	4 milliwatts
9 dBm	7.9 milliwatts
12 dBm	15.8 milliwatts
15 dBm	31.6 milliwatts
18 dBm	61.1 milliwatts
21 dBm	125.9 milliwatts
24 dBm	251.2 milliwatts
27 dBm	501.2 milliwatts
30 dBm	1000 milliwatts
60 dBm	1000000 milliwatts

DECIBEL MILLIWATT – TABELA DE RELAÇÕES



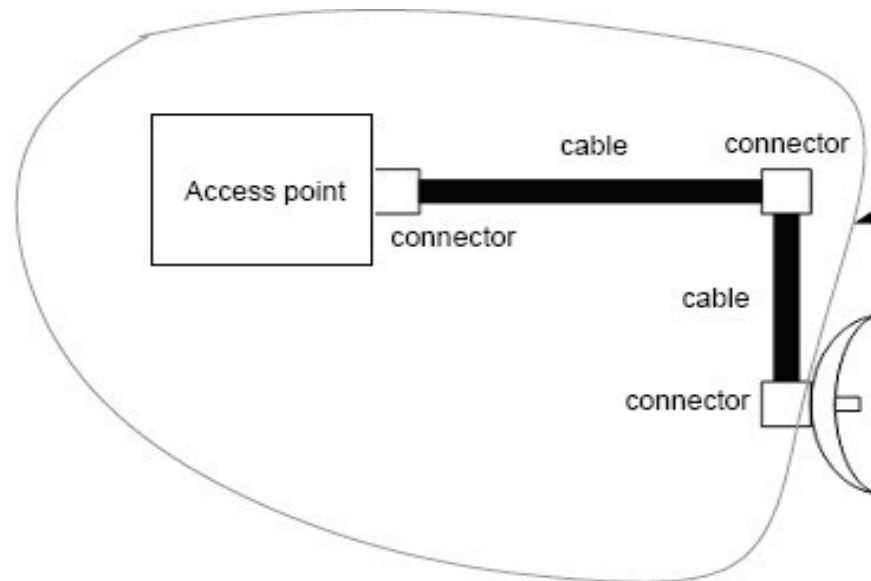
ANTENA ISOTRÓPICA

- O **ganho da antena** é medido em relação a um radiador isotrópico.
- A antena isotrópica é uma **antena virtual**, na prática não existe, a antena que mais se aproxima de uma isotrópica é a **dipolo**.
- As **antenas isotrópicas** tem por função um comparativo entre as antenas reais e as ideais.
- Na prática não possui o mesmo desempenho em todas as direções;
- É um elemento pontual no espaço;
 - Irradia igualmente para todas as direções;
 - Gera padrão de irradiação esférica;

DECIBEL ISOTRÓPICO - DBI

- Ao quantificarmos o ganho de uma antena, comumente a expressamos em dBi, que é uma medida relativa.
- O “i” se refere apenas a uma antena isotrópica.
- Conforme vimos anteriormente, uma antena isotrópica é teoricamente um transmissor ideal que irradia sinal em todas as direções com a mesma intensidade, com 100 % de eficiência em três dimensões. dBi é usado em RF da mesma maneira que DB.
- Considere uma antena de 10 dBi com um 10 miliwatts de potência aplicada:
 - $10\text{mw} + 10\text{ dBi (acrécimo de 10 vezes)} = 100\text{ mw}$

EXEMPLO



Potência de saída do Access Point	100mw
Ganho da antena	12 dBi
Perdas	
Primeiro conector	- 3 dB
Segundo conector	- 3 dB
Terceiro conector	- 3 dB

EXEMPLO

- Para designar o nível de potência em vários pontos do circuito, faremos:
- **P1** – Potência de saída do Access point;
- **P2** – Potência irradiada pela antena;
- **P3** – Potência do sinal antes de chegar a antena;

EXEMPLO

- Primeiramente vamos transformar a potência de saída do Access point para facilitar o calculo :

$$P \text{ (dBm)} = 10 \log 100$$

$$P1 = 10 \times 2 = \mathbf{20 \text{ dBm}}$$

- Agora calculamos o sinal resultante computando as perdas causadas pelos conectores e o ganho da antena.

$$P2 = \text{Potência do AP} - \text{perdas dos conectores} + \text{ganho da antena}$$

$$P2 = 20 - 3 - 3 - 3 + 12 = \mathbf{23 \text{ dBm} = 200 \text{ mw}}$$

- Observe que o ganho real foi de 3 dB (o dobro) em relação ao sinal que sai do AP.

EXEMPLO

- Para calcularmos o sinal que chega a antena, fazemos:

$P_3 = \text{Potência do AP} - \text{perdas dos conectores}$

$P_3 = 11 \text{ dBm}$.

GANHO EM RELAÇÃO À ANTENA ISOTRÓPICA

- Todas as antenas concentram o sinal em determinadas direções, sendo que quanto mais concentrado é o sinal, maior é o ganho. Uma antena de **3 dBi**, por exemplo, irradia o sinal com o dobro de potência que um radiador isotrópico, porém irradia em um ângulo **duas vezes menor**.
- Uma antena de **6 dBi** oferece um sinal quatro vezes mais concentrado, porém para um **ângulo 4 vezes mais estreito**, e assim por diante. De uma forma geral, quanto maior é o ganho desejado, maior precisa ser a antena; justamente por isso as antenas **omnidirecionais e yagi** de alto ganho são muito maiores que as antenas padrão de **2.2 dBi** dos pontos de acesso.

POTÊNCIA DE UM RÁDIO

- A maioria dos modelos domésticos de pontos de acesso trabalham com 17.5 dBm (56 milliwatts) ou 18 dBm (63 milliwatts) de potência, mas existem modelos com apenas 15 dBm (31.6 milliwatts) e, no outro extremo, alguns modelos com até 400 milliwatts (26 dBm), como o *Senao ECB-3220* e o *OVISLINK WL-5460*:



POTÊNCIA DE UM RÁDIO

- Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer depende também da qualidade e do tipo da antena usada.
- As antenas **dipole** utilizadas por padrão nos pontos de acesso são pequenas, práticas e baratas, mas existe a opção de utilizar antenas mais sofisticadas para aumentar o alcance da rede.
- O alcance típico de uma rede **802.11g é de 30 metros em espaços fechados (como uma casa ou um prédio, onde existem paredes e outros obstáculos) e 150 metros em campo aberto, sem obstáculos.**

POTÊNCIA DE UM RÁDIO

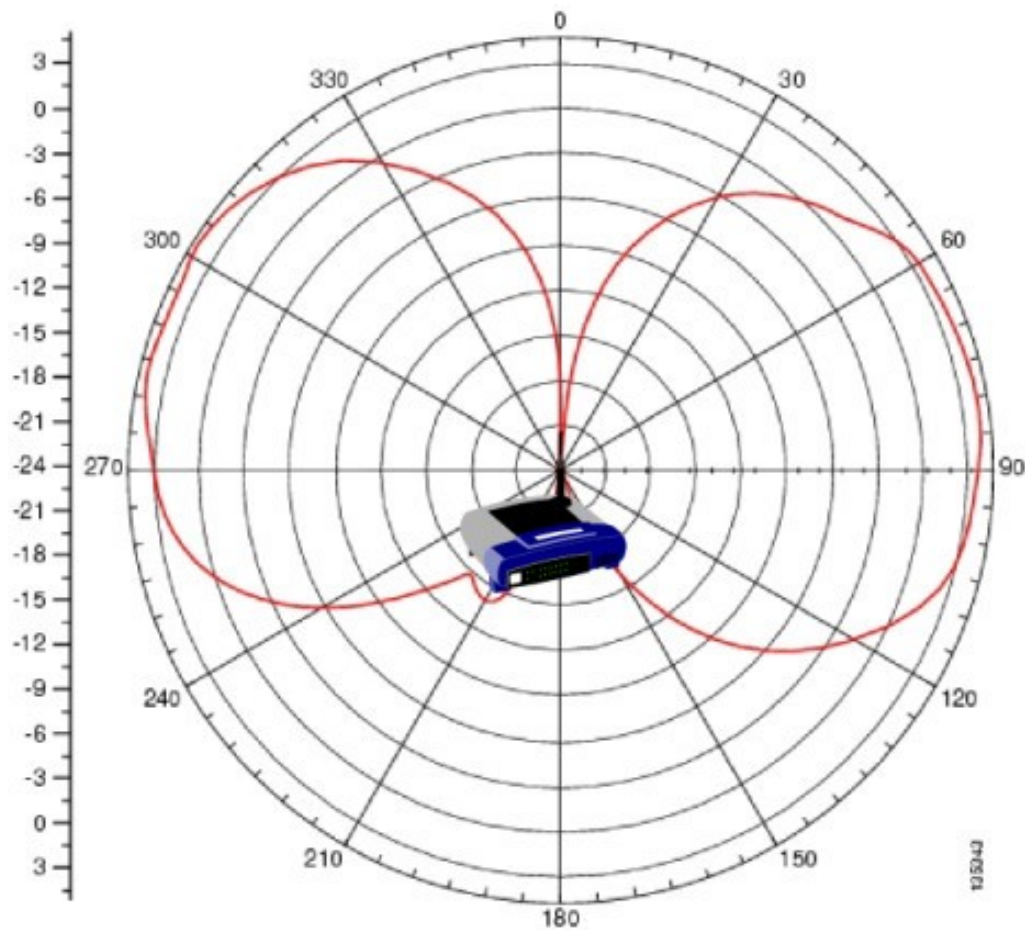
- Entretanto, como vimos anteriormente, a distância máxima e a qualidade do sinal (e, conseqüentemente, a velocidade de transmissão) podem variar bastante de um modelo de ponto de acesso para outro, de acordo com a qualidade e potência do transmissor e do ganho da antena usada pelo fabricante, sem contar os obstáculos presentes entre o ponto de acesso e o cliente. Vamos então a dicas de como aumentar o alcance da sua rede e criar links de longa distância.



ANTENAS OMNIDIRECIONAIS

- As antenas usadas por padrão nos pontos de acesso são chamadas de **dipole ou omnidirecionais** pois irradiam o sinal em todas as direções, permitindo que você se conecte à rede a partir de qualquer ponto na área em torno do ponto de acesso.
- Na verdade, o "**em todas as direções**" é uma figura de linguagem, pois as antenas concentram o sinal na horizontal, **em um raio de 360 graus**, irradiando, em compensação, pouco sinal na vertical.
- Você pode imaginar que, ao utilizar uma **antena ominidirecional**, o sinal emitido pelo ponto de acesso tem formato de um donut, como você pode ver neste gráfico;

ANTENAS OMNIDIRECIONAIS



ANTENAS OMNIDIRECIONAIS

- Por não irradiar muito sinal na vertical, concentrando-o na horizontal, uma antena omnidirecional típica oferece um ganho de **2.2 dBi**, o que equivale a um aumento de 65% na potência de transmissão (e também na qualidade da recepção) em relação a uma antena (teórica) que irradiasse o sinal igualmente em todas as direções.
- A partir daí, é possível aumentar a potência de transmissão do ponto de acesso de duas maneiras:
 - Usando um amplificador de sinal, de forma a aumentar a potência de transmissão do ponto de acesso.
 - Substituindo a antena padrão por uma antena de maior ganho, ou seja, por uma antena que concentre o sinal, permitindo que ele atinja distâncias maiores.

ANTENAS OMNIDIRECIONAIS

- Usar um amplificador é uma forma de resolver o problema na base da força bruta. Usando um amplificador, é possível aumentar a potência de transmissão do ponto de acesso (ou da placa wireless) para até 1 watt, que é o máximo permitido pela legislação.

ANTENAS OMNIDIRECIONAIS

- A grande maioria dos pontos de acesso trabalha com menos de 100 milliwatts de potência de transmissão, de forma que 1 watt significa um ganho considerável.
- Ao usar um amplificador, é importante escolher um amplificador bidirecional (que amplifica nas duas direções, atuando também sobre sinal recebido dos clientes), caso contrário o alcance prático da rede ficará limitado pela potência de transmissão dos clientes (afinal, se o ponto de acesso não recebe o sinal do cliente, não é possível abrir o canal de comunicação).



ANTENAS OMNIDIRECIONAIS



ANTENAS DIRECIONAIS

- Em seguida temos as antenas direcionais, que além de concentrarem o sinal na vertical, concentram-no também na horizontal, fazendo com que, em vez de um ângulo de 360 graus, o sinal seja concentrado em um ângulo de 90 graus ou menos.

ANTENAS DIRECIONAIS

- As primeiras em ordem hierárquica são as **antenas setoriais**, que concentram o sinal em um ângulo de aproximadamente **90 graus**, ou seja, um quarto de um círculo completo.
- Se instaladas no canto de um galpão ou cômodo, elas distribuem o sinal em todo o ambiente, deixando pouco sinal vazar no outro sentido.
- A maioria das antenas setoriais trabalham com ganho de **12 a 17 dBi**. Embora no papel a diferença possa parecer pequena, uma antena de **17 dBi** trabalha com uma potência de transmissão pouco mais de 3 vezes maior que uma de **12 dBi**.



ANTENAS SETORIAIS

- Duas variações das antenas setoriais são as **patch antennas** (antenas de painel) e as **round patch antennas** (antenas circulares).
- As **patch antennas** são antenas quadradas, que contêm internamente uma folha de metal.
- Elas trabalham com um ângulo de cobertura mais aberto do que as antenas setoriais, mas em compensação oferecem menos ganho, servindo como uma espécie de meio-termo entre elas e as antenas omnidirecionais:

ANTENAS SETORIAIS



ANTENNAS ROUND PATCH

- As antenas **round patch** seguem o mesmo princípio, mas são redondas. Devido a isso, elas são muitas vezes instaladas no teto (como se fosse um soquete de lâmpada) de forma a irradiar o sinal igualmente por todo o cômodo.

PATCH ANTENNA



ANTENNAS YAGI

- Em seguida temos as antenas **yagi**, que oferecem um ganho ainda maior, mas em compensação são capazes de cobrir apenas uma pequena área, para a qual são diretamente **apontadas (normalmente em um raio de 24 x 30 graus, ou mais estreito)**. Você pode imaginar que uma antena yagi emite o sinal em um ângulo similar ao de um cone, resultando em um padrão de transmissão similar ao do diagrama abaixo:
- O foco concentrado resulta em um ganho muito maior do que o das antenas setoriais. A maior parte das antenas yagi à venda oferecem ganho de **14 a 19 dBi**, mas não é incomum ver antenas com até **24 dBi**.

ANTENNAS YAGI

- Estas antenas são úteis para cobrir alguma área específica, longe do ponto de acesso, ou interligar duas redes distantes. Usando duas antenas yagi de alto ganho é possível criar links de **até 25 km, o que é mais de 150 vezes o alcance inicial.**
- Para melhores resultados, uma antena deve ficar apontada exatamente para a outra, cada uma no topo de um prédio ou morro, de forma que não exista nenhum obstáculo entre as duas. Em instalações profissionais é usado um laser para fazer um ajuste fino no final da instalação, "mirando" as duas antenas

ANTENNAS YAGI

- As **yagi** são também o melhor tipo de antena a usar quando é preciso concentrar o sinal para **"furar" um obstáculo** entre as duas redes, como, por exemplo, um prédio bem no meio do caminho. Nestes casos a distância atingida será sempre mais curta, naturalmente.
- Uma solução muito adotada nestes casos é usar um repetidor instalado em um ponto intermediário, permitindo que o sinal desvie do obstáculo. Existem até mesmo pontos de acesso extremamente robustos, desenvolvidos para uso industrial, que além de um gabinete reforçado utilizam placas solares e baterias, que permitem a eles funcionar de forma inteiramente autônoma

ANTENNAS YAGI



ANTENAS PARABÓLICAS

- Continuando, temos as antenas **parabólicas**, que também captam o sinal em apenas uma direção, de forma ainda mais concentrada que as yagi, permitindo que sejam atingidas **distâncias ainda maiores**. A maioria das antenas parabólicas destinadas a redes **WI-FI utilizam uma grelha metálica** no lugar de um disco sólido, o que reduz o custo e evita que a antena seja balançada pelo vento, saindo de sua posição ideal. Por causa disso, elas são também chamadas de antenas de grelha, ou grid antennas, em inglês.
- Usar uma antena de maior ganho aumenta tanto a capacidade de transmissão quanto de recepção do ponto de acesso, permitindo tanto que o sinal transmitido se propague por uma distância maior quanto que ele seja capaz de captar o sinal fraco de clientes distantes, desde que eles sejam instalados dentro do foco da antena (que se torna cada vez mais estreito conforme aumenta o ganho).

ANTENAS PARABÓLICAS

- Ao criar links de longa distância, é necessário usar antenas de alto ganho tanto no ponto de acesso quanto no cliente, o que soma o ganho das duas antenas, aumentando exponencialmente o alcance. Em situações ideais, é possível criar links **com 25 ou até mesmo 30 km**, combinando duas antenas de alto ganho, perfeitamente alinhadas.
- Uma curiosidade é que alguns fabricantes estão passando também a incorporar placas wireless USB às antenas, de forma a torná-las mais atrativas, permitindo que você instale a placa com a antena diretamente em uma porta USB disponível, sem precisar se preocupar com pigtails e conectores. Como os adaptadores wireless USB estão cada vez mais baratos, isso tende a se tornar mais comum.

ANTENAS PARABÓLICAS



REFERÊNCIAS

- www.guiadohardware.com.br
- Wikipedia: DBI, DBM
- <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless005.asp>
- [http://support.pt.kodak.com.br/app/answers/detail/a_id/24114/~/o-que-%C3%A9-wi-fi-protected-setup-\(wps\)%3Fselected=true](http://support.pt.kodak.com.br/app/answers/detail/a_id/24114/~/o-que-%C3%A9-wi-fi-protected-setup-(wps)%3Fselected=true)