Sistemas de Conectividade

Aula 09 - Além do Ethernet: redes sem fio 802.11 - parte 1

Apresentação

Olá, pessoal!

Nas aulas 7 e 8 vimos que o padrão Ethernet é a tecnologia mais utilizada atualmente nas redes locais das edificações. Entretanto, existem diversos outros padrões de redes. Embora a maioria desses outros padrões seja definida para redes locais cabeadas, as redes sem fio têm se tornado cada vez mais presentes em nossas vidas.

Nesta e na próxima aula, você vai estudar em detalhes o principal padrão de redes sem fio utilizado atualmente, o 802.11, e verá que a sua utilização ocorre normalmente em conjunto com o Ethernet. Você aprenderá como ele funciona e quais os benefícios que essa tecnologia nos proporciona. Também verá as principais formas de interligar redes diferentes, como uma matriz e suas filiais.

Objetivos

- Entender o funcionamento das redes Wi-Fi;
- Conhecer os dois modos da arquitetura 802.11;
- Compreender o papel e o funcionamento de um Access Point (AP);
- Conhecer os detalhes de frequência e velocidades em redes 802.11.

Redes Sem Fio

As tecnologias que permitem a comunicação sem fio têm conquistado cada vez mais lugar no mercado. Algumas das principais vantagens desse tipo de tecnologia são: a simplicidade para instalação, uma vez que não são necessários cabos; a liberdade para mover o equipamento de um lugar para outro; e as altas taxas de transmissão conseguidas atualmente pelas tecnologias sem fio.

É importante observar que existem várias tecnologias de comunicação sem fio, como Bluetooth, Wi-Fi (802.11), WiMax, redes de telefonia celular, etc., e cada uma tem uma finalidade diferente. Como o foco desta aula é a criação de LANs (*Local Area Network*) sem fio e conexões WAN (*Wide Area Network*), explicaremos em detalhes apenas o padrão 802.11, por se enquadrar nesse contexto e ser a tecnologia mais utilizada atualmente. Você estudará as outras tecnologias de redes sem fio na aula 11.

Redes Wi-Fi

O padrão que estudaremos agora se chama 802.11 e é o padrão definido pelo IEEE (*Institute of Electrical and Eletronics Engineers*) para as LANs sem fio. Antes de qualquer coisa, precisamos entender qual a diferença entre os termos 802.11 e Wi-Fi, que você já deve ter ouvido falar. O termo Wi-Fi, que surgiu como uma abreviação de *wireless fidelity*, ou “fidelidade sem fio”, foi criado por uma organização chamada Wi-Fi Alliance como uma forma de mostrar que um dado equipamento que utiliza tecnologia de transmissão sem fio segue o padrão 802.11. Assim, quando você olhar um equipamento e ele tiver o logotipo Wi-Fi mostrado na **Figura 1**, poderá ter certeza de que ele foi testado pela Wi-Fi Alliance e, portanto, funciona de acordo com o padrão 802.11.

Figura 01 - Logotipo Wi-Fi que garante ao equipamento conformidade ao padrão 802.11.

Fonte: http://www.wi-fi.org

Arquitetura da Rede 802.11

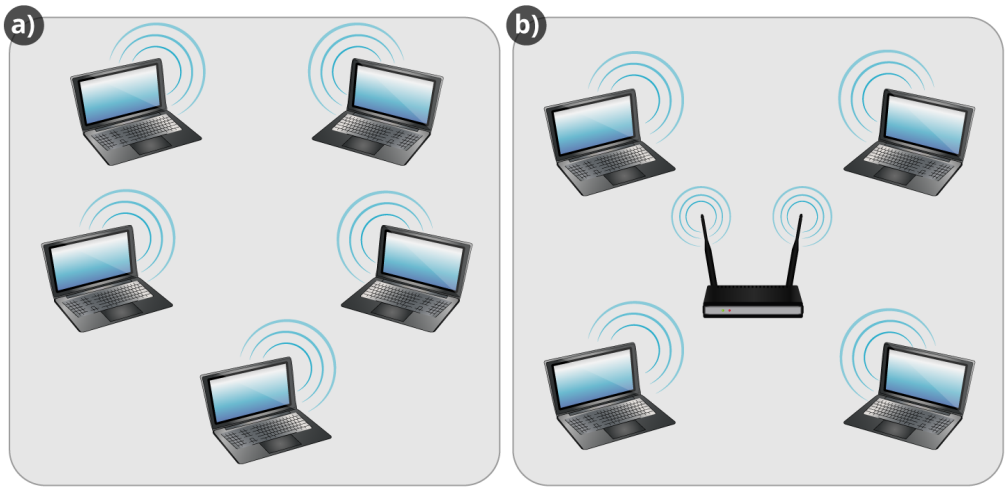
Os equipamentos interconectados por meio da rede 802.11 são organizados em um grupo chamado *Basic Service Set* (Conjunto de Serviços Básicos – BSS). Um BSS pode ser organizado de dois modos: **modo infraestrutura** e **modo Ad Hoc**. O modo mais popular é o de infraestrutura, pois é usado para conectar clientes (como *laptops*, *tablets* e *smartphones*) a uma outra rede, geralmente a LAN da empresa ou a Internet.

No **modo infraestrutura**, cada cliente está associado ao *Access Point* (Ponto de Acesso – AP), um equipamento que desempenha função especial no controle das comunicações. Normalmente, o AP utiliza antenas omnidirecionais, que emitem e recebem sinal num raio de 360 graus, para tentar criar uma área de cobertura circular. O AP também pode ser ligado a uma antena externa do tipo direcional, quando se pretende fazer enlaces sem fio ponto a ponto.

Quando o BSS é formado apenas pelas máquinas dos usuários, que se comunicam diretamente umas com as outras, a rede é dita operar em **modo Ad Hoc** (*Independent Basic Service Set* – IBSS). Esse modo não possui ponto de acesso e serve basicamente para comunicações isoladas entre um conjunto de computadores.

A **Figura 2** ilustra os dois tipos de BSS (infraestrutura e *ad hoc*). Nesta aula, estudaremos as redes com infraestrutura, que são as mais utilizadas atualmente.

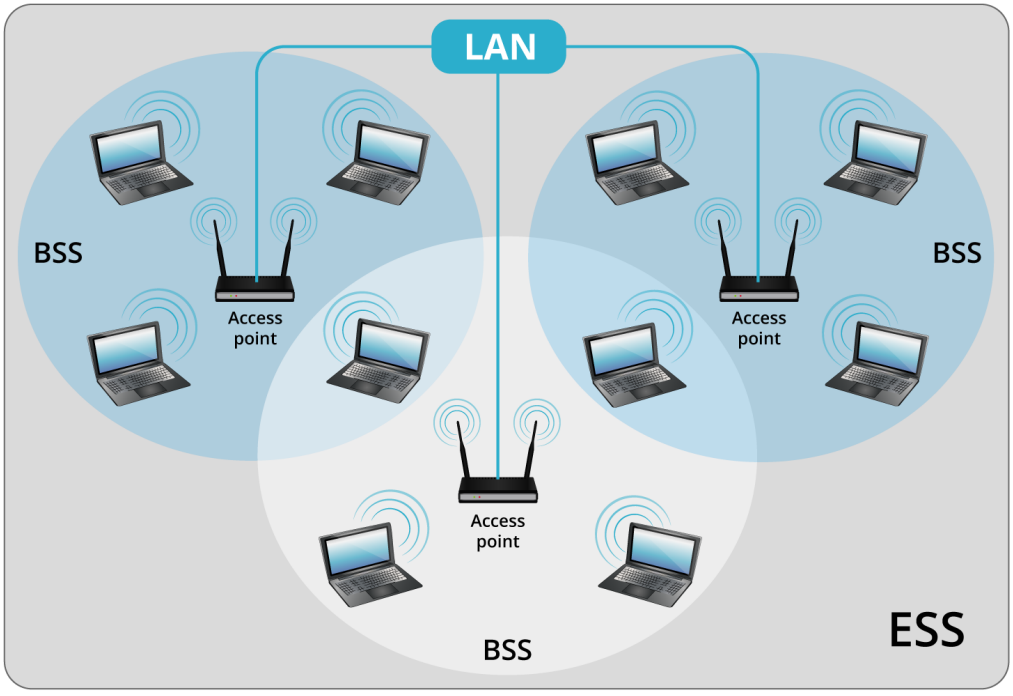
Figura 02 - BSS em modo Ad Hoc (a) e em modo infraestrutura (b).



Fonte: Elaborado pelo Autor (2016).

No modo infraestrutura, vários APs podem ser interconectados através de um Sistema de Distribuição que pode ser formado por qualquer tecnologia IEEE 802, por exemplo, o Ethernet. Na **Figura 3** temos uma rede 802.11 estendida, na qual dois ou mais BSSs estão interconectados formando um *Extented Service Set* – ESS.

Figura 03 - Vários BSSs formando um ESS.



Fonte: Elaborado pelo Autor (2016).

O interior das elipses corresponde à área de cobertura de cada AP. Tipicamente, em uma organização existem diversos pontos de acesso, e cada um deles está conectado a algum switch, através de cabos Par-Trançado. Desse modo, se todos os APs estão conectados à mesma rede Ethernet, essa rede passa a ser o Sistema de Distribuição. Observe que os APs têm uma interface Wireless e uma (ou mais) Ethernet. Embora existam APs que também são roteadores, por definição os APs são equipamentos que atuam como pontes, ou seja, trabalham na camada de enlace. Portanto, para formarem um ESS, todos os APs devem atuar com pontes.

Curiosidade!

Enquanto nas empresas é muito comum a utilização de APs que atuam como pontes (fazendo com que as estações sem fio pertençam à mesma rede cabeada a qual estão ligadas), os APs utilizados nas residências para compartilhar a conexão de Internet normalmente atuam como roteadores.

Atividade 01

1. Qual a diferença entre uma antena direcional e uma antena omnidirecional?
2. Qual das antenas é utilizada em um Access Point (AP) indoor, isto é, que esteja dentro de uma edificação?

Respostas

Respostas

1. Uma antena direcional tem seu feche de ondas eletromagnéticas direcionado para um determinado ponto. Já a antena omnidirecional propaga suas ondas em todas as direções criando uma área de cobertura circular.

2. Em edificações, o Access Point (AP) utiliza antenas omnidirecionais, pois o AP deve ser posicionado o mais próximo possível do centro do prédio de forma que a cobertura circular cubra todos os compartimentos da edificação.

Funcionamento do *Access Point*

A função do AP é controlar toda a comunicação das estações sem fio. Desse modo, sempre que uma estação quer realizar uma transmissão, ela envia o quadro para o AP que, por sua vez, o reencaminha para a estação de destino. Os APs também são encarregados de informar sobre a existência da rede sem fio. Você já deve ter observado que quando é ligado um computador que possui conexão sem fio e é pedido para que ele localize as redes Wi-Fi, aparece uma ou mais redes que possuem, cada uma, um nome que as identifica. Esse nome é configurado pela pessoa que instalou o AP e se chama *Service Set Identifier* (**SSID**). Em um ESS, o SSID às vezes também é referido como *Extended Service Set Indentifier* (ESSID), mas o chamaremos apenas de SSID. É importante lembrar que, em um ESS, todos os APs possuem o mesmo SSID.

Na próxima aula estudaremos os formatos dos quadros transmitidos em uma rede 802.11. Por enquanto, é importante que você saiba da existência dos três tipos de quadros: a) quadros de dados, b) quadros de gerenciamento e c) quadros de controle.

O AP envia periodicamente um quadro de gerenciamento especial, chamado *Beacon*, que contêm diversas informações importantes sobre a rede, como as velocidades suportadas, além de informações a respeito do tempo necessário para

que as estações sincronizem seus relógios com o AP. Tipicamente, um AP envia um *Beacon* a cada 100ms, o que significa que são enviados 10 *Beacons* por segundo. No entanto, esse tempo pode ser configurado.

Para que os computadores possam descobrir as redes sem fio, duas abordagens podem ser utilizadas. A primeira refere-se à abordagem padrão, em que o AP informa o SSID no quadro de *Beacon*. Desse modo, tudo o que o computador precisa fazer é escutar o meio para receber os SSIDs. Na segunda abordagem, por sua vez, os APs não informam seus SSIDs, pois são os computadores que enviam um tipo de quadro de gerenciamento perguntando pelas redes existentes. Eles podem procurar pelo AP com um SSID específico (informado pelos próprios computadores) ou perguntar se existe alguma rede disponível. Nessa segunda abordagem as redes ficam “escondidas”, e só conseguirão conectar a elas os computadores que já souberem da sua existência.

Note que um computador pode estar ao alcance de sinal de dois ou mais APs e, por isso, pode identificar várias redes sem fio. O 802.11 não define um método automático para escolha da rede à qual a máquina irá se associar (veja a próxima seção para uma definição mais detalhada de associação). Entretanto, depois que o usuário escolhe manualmente a qual rede se associar, sempre que ela estiver disponível, o sistema se associará automaticamente a ela. Vale ressaltar, contudo, que isso é um recurso do sistema operacional, e não do 802.11.

No caso de um ESS (visto na Figura 3), em que a rede utiliza mais de um AP para aumentar a área de cobertura do sinal, todos os APs estão com o mesmo SSID, e cada máquina tipicamente irá se associar ao AP que lhe fornece a melhor qualidade de sinal, ou seja, do qual ele receber o sinal “mais forte”.

Associação e Controle de Acesso

Antes de fazer parte do BSS para ter acesso aos serviços básicos de rede e poder transmitir qualquer coisa, os computadores precisam se associar ao AP (ao se associar ao AP, o computador se conecta à rede). No entanto, quando a estação não deseja mais participar do BSS (vai ser desligada, por exemplo), ela pode, também, se

desassociar do AP. A associação é basicamente um registro das estações no AP e permite tanto que o AP saiba quem faz parte da sua rede, como impõe algum tipo de controle de acesso para que a estação entre na rede.

Desse modo, os APs podem exigir que os usuários se autentiquem para que possam fazer parte do BSS. Essa autenticação pode ser baseada no endereço MAC, em nome de usuário e senha, ou através de uma senha compartilhada. Nesse último caso, a pessoa que instala o AP cadastra uma senha neste, e cada máquina que desejar se associar a ele deverá informar a mesma senha. Você já viu algo assim, correto?

Normalmente, o sistema operacional da máquina grava essa senha associada ao nome da rede sem fio para que você não precise informá-la sempre que for conectar à rede. Suponha, por exemplo, que você tem um notebook por meio do qual acessa uma rede sem fio em casa e outra no trabalho. Na primeira vez que conectar em cada uma dessas redes, terá de informar a sua respectiva senha.

A partir daí, quando chegar ao trabalho o computador detectará que a rede sem fio disponível é a do trabalho e se associará automaticamente ao AP usando a senha dessa rede. Assim como quando chegar à casa e for usar a rede, o computador utilizará a senha da rede de casa para se associar ao AP desta.

O método de proteção original do mecanismo de autenticação do 802.11 chamava-se *Wired Equivalent Privacy* (WEP), e pretendia, inicialmente, fornecer às redes sem fio o mesmo nível de segurança das redes cabeadas. Este protocolo utiliza uma senha compartilhada para criptografar os pacotes que são trocados numa rede sem fios a fim de tentar garantir confidencialidade aos dados trafegados. No entanto, após vários estudos e testes realizados com este protocolo, encontraram-se algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade. Atualmente, o padrão dos mecanismos de autenticação mais utilizado no 802.11 é chamado 802.11i, e a Wi-Fi Alliance criou o termo *Wi-Fi Protected Access* (WPA) para designar os equipamentos que incorporam esse padrão.

A segunda versão do protocolo 802.11i (WPA2) pode operar em dois modos. O primeiro modo, assim como no WEP, utiliza uma senha compartilhada (*Pre-Shared Key* - PSK) pelo AP e pelas estações, dando origem ao termo WPA2-PSK. O segundo método de autenticação do 802.11i, por sua vez, chama-se *WPA Enterprise* e utiliza

uma infraestrutura de autenticação 802.1x, baseada em servidor de controle de acessos, sendo este, geralmente, um servidor RADIUS (*Remote Authentication Dial in User Service*), o qual é usado para validar as informações dos usuários, tais como login e senha.

Atividade 02

---

1. Geralmente, os Access Points corporativos conseguem definir diferentes redes sem fio para uso simultâneo por diferentes tipos de usuários. Como é possível distinguir uma rede sem fio de outra a partir do mesmo AP?

2. Pelo que você já observou ao usar diferentes redes sem fio que requerem autenticação, qual método é o mais utilizado?

Respostas

Respostas

1. A identificação de uma determinada rede sem fio é feita pelo SSID (Service Set IDentifier), que é um nome qualquer que possa definir o propósito daquela rede. Por exemplo, no IMD poderíamos ter as redes sem fio “IMD Alunos” e “IMD Professores”, caso quiséssemos separar em redes sem fio distintas os equipamentos dos alunos dos equipamentos dos professores a fim de aplicar políticas de acesso e usos diferentes para cada uma. Existem APs corporativos que permitem criar até 8 redes sem fio (SSID), cada uma com suas configurações distintas.

2. Se você observar as redes sem fio que usa, perceberá que a maioria dessas redes as quais utilizam chaves para permitir a sua entrada (associação) utilizam, ainda, o protocolo WPA2 com chave compartilhada PSK (Pre-Shared Key).

Camada Física do 802.11

O padrão 802.11 inicial, criado em 1999, especificava duas camadas físicas diferentes para a transmissão dos sinais na faixa de frequências de rádio. Ambas utilizavam a faixa de frequência de 2,4 GHz, que é uma faixa não licenciada. Isso significava que qualquer pessoa podia fazer transmissão nessa frequência, e, portanto, as comunicações estavam sujeitas a interferências de outras fontes, como os telefones sem fio e os fornos de micro-ondas. Além, evidentemente, de outras redes sem fio 802.11 que estivessem na mesma área. Esses dois padrões iniciais de transmissão sem fio chamavam-se *Frequency Hopping Spread Spectrum* (FHSS) e *Direct Sequence Spread Spectrum* (DSSS), e transmitiam a velocidades de 1 ou 2 Mbps. Atualmente, o método mais utilizado é o *Orthogonal Frequency-Division Multiplexing* (OFDM), com transmissões que chegam até 54 Mbps.

Em 1999, foram criados, também, os padrões chamados 802.11a e 802.11b e, em 2003, o padrão 802.11g. Em dezembro de 2009, após sete anos de trabalho, foi concluído o processo de padronização do 802.11n. Esse último utiliza duas ou mais antenas no transmissor e no receptor, chamadas MIMO (*Multiple Input* – entrada múltipla e *Multiple Output* – saída múltipla), para realizar transmissões em paralelo (simultâneas) e, com isso, obter taxas de transmissão muito superiores às obtidas pelos padrões anteriores.

Todos esses novos padrões de camada física procuraram melhorar a qualidade das transmissões, o alcance dos sinais e, principalmente, as velocidades de transmissão. A Tabela 1 mostra as velocidades máximas suportadas por esses padrões, a faixa de frequência utilizada e a técnica para transmissão dos sinais.

Padão	**Faixa de Frequência**	**Técnica de Transmissão**	**Taxa de Transferência de dados**
802.11	2,4Ghz	FHSS e DSSS	2 Mbps
802.11a	5Ghz	OFDM	54 Mbps

Padão	Faixa de Frequência	Técnica de Transmissão	Taxa de Transferência de dados
802.11b	2,4Ghz	HD-DSSS	11 Mbps
802.11g	2,4Ghz	OFDM	54 Mbps
802.11n	2,4Ghz e/ou 5Ghz	MIMO-OFDM	600Mbps (300 Mbps na prática)

Tabela 1 - Faixas de frequência e velocidades dos padrões Wi-Fi.
Fonte: https://standards.ieee.org/about/get/802/802.11.html

Observe que, embora a faixa de 5GHz também não seja licenciada, existem menos equipamentos que trabalham nessa faixa de frequência do que na de 2,4GHz, de modo que a faixa de 5GHz apresenta menos interferência.

Observe, também, que, embora o 802.11n possa, em tese, atingir 600 Mbps, a maior parte dos equipamentos atuais oferece taxas próximas a apenas 300 Mbps, o que, ainda assim, já é um aumento de velocidade considerável em relação aos padrões anteriores. Um dos motivos para isso é que, para atingir a velocidade de 600 Mbps, os equipamentos teriam um custo maior, pois precisariam utilizar o número máximo de antenas e ter mais capacidade de processamento.

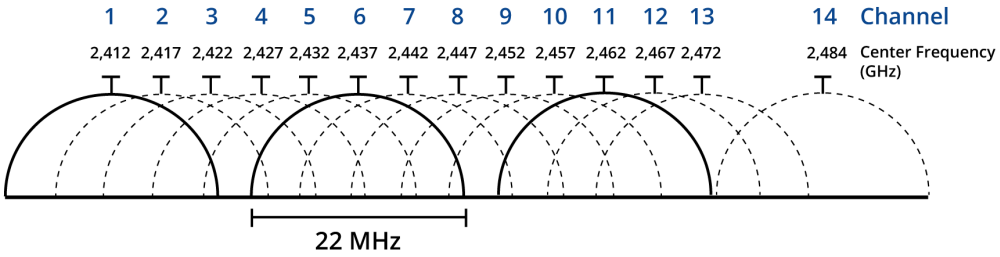
Curiosidades!

Alguns padrões 802.11 são compatíveis com outros. Por exemplo: um AP 802.11g suporta a associação de estações 802.11b, e um AP 802.11n suporta estações 802.11g.

Conheça um pouco mais sobre as novas redes sem fio de alta velocidade 802.11ac clicando no link: http://www.tecmundo.com.br/wi-fi/23964-wi-fi-802-11ac-as-redes-sem-fio-de-alta-velocidade-vem-ai.htm

Cada padrão utiliza sua faixa de frequência de um modo. Os padrões 802.11b/g/n, por exemplo, dividem sua faixa de frequência de largura 84 MHz, que vai de 2,4 GHz até 2,484 GHz, em 14 canais de 22 MHz cada, como pode ser visto na **Figura 4**. Esses canais se sobrepõem parcialmente, de modo que só não há sobreposição entre dois canais se eles estiverem separados por quatro ou mais canais.

Figura 04 - Representação gráfica da sobreposição dos canais da banda de 2,4GHz



Fonte: https://en.wikipedia.org/wiki/List_of_WLAN_channels. Acesso em: 20 jul. 2016.

Então, na hora de configurar dois APs, deve-se saber escolher os canais de maneira que eles não se sobreponham. O único conjunto de três canais que não se sobrepõem nos padrões 802.11b/g/n, por exemplo, é formado pelos canais 1, 6 e 11. O canal a ser utilizado pelo AP pode ser modificado, a fim de utilizar o que apresente menos interferência ou a fim de permitir a utilização de mais de um AP na mesma área.

Algo muito importante que você precisa observar é o fato de que os padrões 802.11 utilizam transmissão por sinais de rádio e, por isso, temos algumas consequências. As principais são:

- Os sinais de rádio são atenuados (perdem força) quando atravessam objetos, por exemplo, paredes. Isso reduz o alcance do sinal;

- Os objetos presentes em um determinado ambiente interferem na propagação dos sinais de rádio, fazendo com que percorram caminhos diferentes até o destino (receptor do sinal);

- Outros equipamentos podem gerar interferência, como é o caso dos aparelhos de telefone sem fio e micro-ondas (conforme explicado anteriormente);

- Como a probabilidade de erros durante uma transmissão sem fio é muito maior do que em redes cabeadas, o 802.11 utiliza quadros de confirmação (no Ethernet isso não é feito);

- Os sinais de todos os dispositivos sem fio compartilham o mesmo meio de transmissão (o ar). Podemos dizer, então, que o enlace é multiponto. Sendo assim, a banda de rede é dividida entre todos os equipamentos. Desse modo, ter um AP trabalhando a 54 Mbps com 10 computadores associados significa, a grosso modo, que cada uma tem, disponível para si, em torno de 5,4 Mbps. Isso é diferente do que ocorre em uma rede cabeada (utilizando switch), na qual cada máquina tem um canal exclusivo.

Curiosidade!

Devido às características de propagação dos sinais de rádio, observe que, embora seja simples criar uma rede sem fio, o mesmo não se pode dizer acerca da garantia da qualidade do sinal que chega a cada máquina. Mudanças no ambiente, bem como colocação de divisórias ou movimentação de armários podem comprometer a qualidade do sinal em um determinado lugar.

Handoff (Mobilidade entre APs)

É importante observarmos que uma rede sem fio não precisa ser necessariamente uma rede em que existe mobilidade, isto é, onde os dispositivos acessem a rede enquanto estão em movimento. Poderá, por exemplo, ter uma rede sem fio em casa e ter um desktop conectado a essa rede. Ou ter, então, um notebook que é sempre utilizado em cima de uma mesa. Um dia você pode usá-lo no seu quarto e outro dia na sala, mas ele é ligado somente após ser colocado em uma mesa e só é retirado desta após ser desligado. Pode, ainda, levá-lo para o trabalho e fazer a mesma coisa lá, ou seja, utilizá-lo apenas em uma mesa. Nesses casos, não houve mobilidade, visto que o notebook não foi movido da mesa onde foi utilizado.

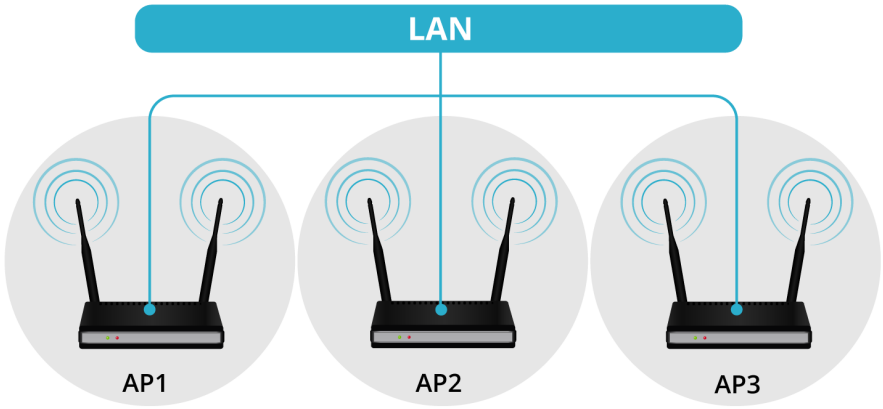
Contudo, suponha que você estava no quarto com o seu notebook, baixando um arquivo da Internet enquanto estudava com ele e, no entanto, alguém ligou a televisão. Como o ambiente da sala estava mais silencioso, você, então, resolveu ir para lá com o notebook ainda ligado. Dessa forma, enquanto você estiver dentro do alcance do sinal do seu AP, poderá se movimentar livremente que não haverá problema nenhum, pois continuará conectado à rede.

A situação anterior foi simples porque você tinha apenas um AP. Suponha, agora, que uma situação semelhante ocorreu em seu trabalho e que você precisou sair de sua sala para mostrar alguma coisa no notebook ao seu chefe. Enquanto ia à sala dele, um arquivo também estava sendo baixado. Como a área da empresa não podia ser atendida por apenas um AP, imagine que você estava em um BSS e a sala do seu chefe em outro BSS.

À medida que você passava do seu BSS para outro vizinho, era importante que sua máquina se associasse automaticamente ao novo AP e que suas conexões de rede fossem mantidas. Esse processo se chama handoff, e é simples de ser realizado quando os dois computadores estão na mesma rede IP, pois consiste basicamente em fazer com que os APs saibam que a estação está associada a outro AP.

Atividade 03

1. Considere que você tenha sido contratado para instalar uma rede 802.11 estendida com AP utilizando o padrão 802.11g, conforme a figura abaixo. Qual canal deve ser configurado em qual AP para que tenha o mínimo de interferência?



Resposta

Respostas

1. Nas redes Wi-Fi b/g/n que utilizam a faixa de 2.4GHz, os únicos canais que não se sobrepõem entre si são os canais 1, 6 e 11. Assim, algumas possibilidades de uso desses canais nos três APs da questão seriam:
    - AP1 com canal 1, AP2 com canal 6, AP3 com canal 11;
    - AP1 com canal 6, AP2 com canal 1, AP3 com canal 6;
    - AP1 com canal 11, AP2 com canal 6, AP3 com canal 11;

Leitura Complementar

- IEEE 802.11™: Wireless LANs.
- IEEE 802.11.

Resumo

Nesta aula, você iniciou o estudo do padrão 802.11 (Wi-Fi), que consiste em uma rede sem fio na qual normalmente se utiliza um (ou mais) Ponto de Acesso (AP) em que as estações dos usuários se associam. Conheceu os detalhes da camada física desse padrão, observando as frequências de rádio e as velocidades de transmissão suportadas. Conheceu também alguns mecanismos de controle de acesso utilizados no Wi-Fi nos quais são usadas senhas para fazer a autenticação. Na próxima aula continuaremos o estudo do 802.11, conhecendo o seu protocolo de acesso ao meio físico, o formato dos quadros e alguns outros aspectos relevantes dessa tecnologia.

Autoavaliação

1. Para que servem as redes Wi-Fi?
2. Quais as frequências e velocidades suportadas pelo 802.11?

Respostas

Respostas

1. Para criar redes locais sem fio, especialmente dentro de edificações, estendendo a rede cabeada e provendo mobilidade nas conexões com a rede.

2. A tabela 1 desta aula apresenta todas as frequências e velocidades suportadas pelo padrão 802.11.

Referências

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 3. ed. São Paulo: Addison Wesley, 2006.

SOARES, L. F. G. **Redes de computadores das LANs, MANs e WANs às redes ATM**. 2. ed. São Paulo: Editora Campus, 1995.

TELECO. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_1.asp>. Acesso em: 9 maio 2012.