Implementação de uma Rede Wi-Fi

N. G. Rodrigues
Departamento de Informática e Comunicações da Escola Superior de Tecnologia e de Gestão.
Instituto Politécnico de Bragança,
5301-854 BRAGANÇA,
Portugal,
nuno@ipb.pt

RESUMO

N. G. Rodrigues. 2004. Implementação de uma Rede WiFi. Congresso Brasileiro de Ciência da Computação, Itajaí, 2004, 835 – 848. Itajaí, SC – Brasil, ISSN 1677-2822

Pretende-se com o presente documento abordar as diferentes questões técnicas associadas à implementação de uma Rede WiFi à escala de um Campus Universitário, utilizando como *case study* o Projecto Campus Virtual do Instituto Politécnico de Bragança - IPB. Será feita uma introdução às redes sem fios e analisadas as mais recentes normas da família IEEE 802.11. Segue-se uma abordagem a aspectos práticos como a extensão da Rede de cablagem guiada do Campus para suporte aos equipamentos WiFi, a Autenticação dos utilizadores, a questão da Segurança nesta nova infra-estrutura e novas perspectivas de serviços possíveis com uma infra-estrutura deste tipo.

PALAVRAS DE INDEXAÇÃO ADITIONAIS: *Rede sem fios, 802.11b, 802.11g, 802.11a, Campus Virtual.*

INTRODUÇÃO

A "Era da Informação" que actualmente vivemos caracteriza-se pela elevada dependência da tecnologia, que estabelece a ponte entre as pessoas e a informação, pelos Espaços Virtuais e em constante mutação e por conceitos como a globalização e desregulamentação. Surge, neste contexto, a Internet, como elo agregador destas características.

Comparativamente à evolução "Era Industrial" -> "Era da Informação", também a própria Internet e o acesso à Informação de uma forma mais genérica têm caminhado no sentido da globalização e ubiquidade – disponibilidade em todo o lado e a toda a hora.

Neste contexto, as redes sem fios têm-se desenvolvido recentemente de forma bastante acentuada, enquadrando-se como elementos importantes de suporte à mobilidade no acesso à informação. O seu desenvolvimento tem-se baseado em dois tipos de necessidades:

a) de interligação de redes locais (LAN's), através de ligações ponto-a-ponto sem fios;

b) interligação de computadores num ambiente de rede local (dando origem ao conceito Wireless LAN – WLAN).

Esta segunda situação pode ocorrer quando a instalação de uma rede de cablagem guiada não se justifica (por motivos económicos, arquitectónicos, de funcionalidade, elevada mobilidade dos sistemas, etc) ou também como extensão de uma rede local estruturada tradicional.

TECNOLOGIAS *WIRELESS LAN* (WLAN)

As redes de área local sem fios (WLAN - *Wireless LAN*'s) podem definir-se como redes com um alcance local, que utilizam o ar como meio de transmissão.

Por rede sem fios entendemos uma rede que utiliza ondas electromagnéticas como meio de transmissão da informação, através de um canal que interliga os diferentes equipamentos móveis presentes na mesma "(MONTEIRO, 2000)".

Estas ligações são normalmente implementadas através de tecnologias de rádio-frequência ou de infravermelhos.

Uma rede local sem fios é um sistema flexível de comunicações, que pode ser implementado como uma extensão ou directamente como uma alternativa a uma rede de cablagem guiada.

Este tipo de infra-estruturas proporciona grande mobilidade aos utilizadores, sem perder conectividade.

Outras vantagens encontram-se ao nível da facilidade de instalação e na economia associada à supressão dos meios de transmissão guiados.

A primeira rede local sem fios publicamente conhecida foi implementada durante a década de 70, por investigadores da Universidade do Hawaii, ficando conhecida por rede ALOHA. Era objectivo da altura ultrapassar as barreiras naturais que impossibilitavam a ligação via cabo à rede Arpanet, então em desenvolvimento. No entanto, de acordo com KHAN "(2003)", já durante a II Guerra Mundial o exército Norte Americano usou sinais rádio para transmissão cifrada de dados, embora todos os desenvolvimentos militares nesta área se tenham mantido secretos por muitos anos.

Em Março de 1985, a Comissão Federal de Comunicações Americana - FCC, (organismo com competências na área da regulação das telecomunicações nos Estados Unidos), atribuiu aos sistemas WLAN as gamas de frequência 902-928 Mhz, 2.400-2.4835 Ghz e 5.725-5.850 Ghz.

Estas gamas de frequências, que ficaram conhecidas como bandas ISM - *Industrial Científica e Médica*, podem ser utilizadas sem necessidade de licenciamento prévio por parte das entidades reguladoras.

Embora a atribuição da FCC seja seguida na maior parte dos países, existem pequenas variantes, como se pode ver na Tabela 1 para a banda dos 2.4 GHz.

Tabela 1 – Alocação global do espectro de frequências na bandas dos 2.4 GHz

Região	Espectro alocado (GHz)
Espanha	2.4450 – 2.4750
Estados Unidos da América	2.4000 – 2.4835
Europa	2.4000 – 2.4835
França	2.4465 – 2.4835
Japão	2.4710 – 2.4970

Tipos de tecnologias usadas nas WLAN

As redes WLAN são suportadas por três categorias base de tecnologias:

- Microondas: as redes baseadas neste tipo de tecnologias funcionam normalmente na banda dos 5.8 GHz, oferecendo débitos elevados mas com um alcance limitado.

- Rádio Frequência (RF): trata-se da tecnologia actualmente mais divulgada nas WLAN, operando tipicamente nas bandas dos 2.4 GHz ou 5GHz. As implementações mais comuns utilizam técnicas de modulação de *Spread Spectrum*, onde a energia dos sinais é repartida de igual forma ao longo de toda a largura de banda disponível, em vez de a concentrar à volta de uma portadora concreta. Existem actualmente duas técnicas de *Spread Spectrum* usadas nas redes de RF "(VINES, 2002)":

  - *Direct Sequence Spread Spectrum* - DSSS: distribui o sinal ao longo de toda a gama de frequências disponível, reorganizando posteriormente os pacotes no receptor.

  - *Frequency Hopping Spread Spectrum* - FHSS: envia segmentos curtos de dados que são transmitidos através de frequências específicas, controlando o fluxo com o receptor. Este negoceia velocidades menores, comparativamente às velocidades oferecidas pela técnica DSSS mas menos susceptíveis a interferências.

Implementações mais recentes utilizam uma técnica baseada em multiplexagem por divisão de frequência, denominada *Orthogonal Frequency Division Multiplexing* (OFDM). Esta técnica divide os sinais de rádio numa espécie de múltiplos sub-sinais, que são de seguida transmitidos simultaneamente em diferentes frequências.

- Tecnologia de Infravermelhos: os sistemas de infravermelhos posicionam-se em altas frequências, imediatamente abaixo da faixa de frequências da luz visível. Assim, as propriedades dos infravermelhos são as mesmas da luz visível, o que faz com que estes não possam passar através de objectos opacos. Podem no entanto reflectir-se em determinadas superfícies. Esta tecnologia aplica-se tipicamente em ambientes interiores, para a criação de ligações ponto-a-ponto de curto alcance.

Configurações WLAN

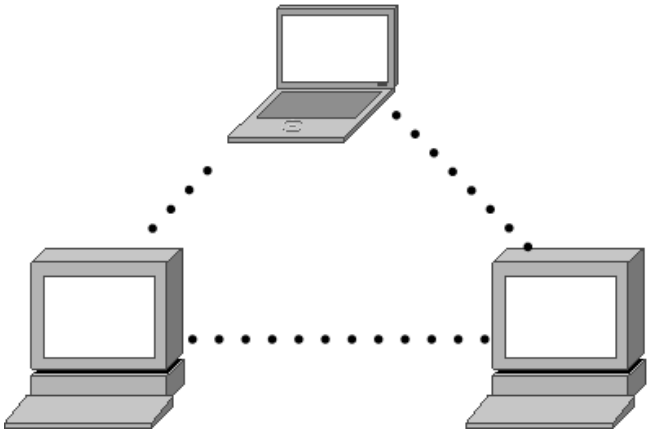
O grau de complexidade de uma rede local sem fios é variável, dependendo das necessidades a satisfazer.

O equivalente sem fios a um segmento de rede guiada é a célula. Estas células são designadas por BSA - *Basic Service Area*, dependendo o seu tamanho das características do ambiente e da potência dos transmissores/receptores usados nas estações (designadas por BSS – *Basic Service Set*).

Entre as topologias mais comuns, destacam-se as seguintes:

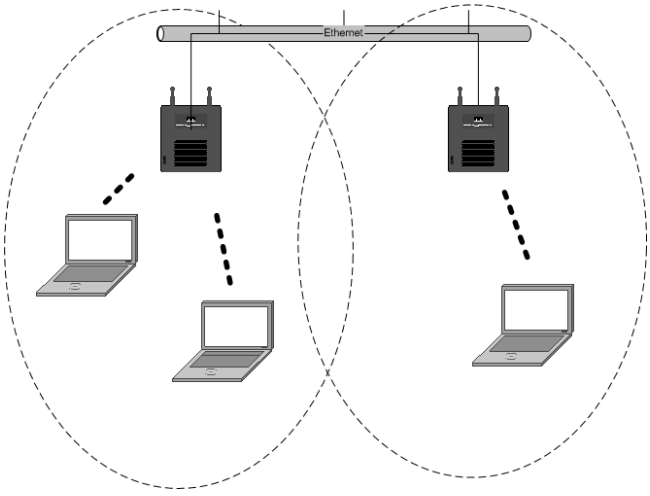
- Redes sem infra-estrutura (*ad-hoc*): correspondem à topologia mais simples, sendo constituídas por um conjunto de equipamentos terminais móveis, equipados com uma placa adaptadora sem fios (Figura 1). Para a comunicação ser possível, é necessário que todas as estações estejam no raio de cobertura radioeléctrica umas das outras. Trata-se de redes muito simples de implementar e que não requerem grandes recursos de administração.

Figura 1 – Rede *ad-hoc*



- Extensão das células básicas – modo de infra-estrutura: Para aumentar o alcance de uma rede do tipo anterior, torna-se necessário instalar um Ponto de Acesso - AP (*Access Point*). Os Pontos de Acesso são estações especiais, responsáveis pela captura das transmissões realizadas pelas estações da sua célula, destinadas a estações localizadas em outras células, e retransmitindo-as através de um sistema de distribuição. Com este novo elemento, a distância máxima permitida deixa de ser entre estações, passando a ser a distância entre cada estação e o AP. Ao mesmo tempo, os pontos de acesso podem ser interligados a outras redes, nomeadamente a redes fixas, às quais o utilizador móvel passa a poder ter acesso (Figura 2). Para fornecer cobertura a zonas maiores, torna-se necessário instalar mais pontos de acesso. A ligeira sobreposição das diferentes células de cobertura vai permitir também o deslocamento dos utilizadores móveis ao longo de toda essa área sem perder conectividade.

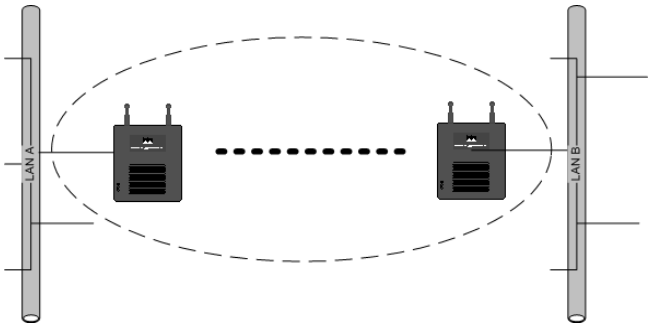
Figura 2 – Rede sem fios com infra-estrutura



- Interligação entre duas ou mais rede LAN: Esta opção permite a interligação de diferentes LAN's (por exemplo de edifícios separados, etc) usando redes sem fios. Neste caso, as soluções mais simples passam pela instalação de uma antena direccional em cada extremo, apontando-se mutuamente (Figura 3). Ao mesmo

tempo, cada uma destas antenas está ligada à rede local do seu lado, através de um Ponto de Acesso.

Figura 3 - Interligação de LANs por Redes sem fios



Em situações mais complexas, são utilizadas, hoje em dia, antenas omni-direccionais ligadas a encaminhadores (que substituem os Pontos de Acesso), que por sua vez se ligam às respectivas redes locais.

Desta forma é possível extender o conceito de Redes Locais Sem Fios para Redes Metropolitanas Sem Fios, que interligam redes locais à escala de uma cidade, por exemplo "(AMARO, 2000)".

Principais Normas WLAN

Tal como em outras áreas tecnológicas, também nesta área das redes sem fios se fez sentir a necessidade de criar normas internacionais de interoperabilidade entre sistemas de diferentes fabricantes. Entre as normas mais divulgadas, destacam-se as apresentadas nas próximas sub-secções.

Bluetooth

O Bluethooth "(BISDIKIAN, 2001)" é um protocolo baseado na especificação IEEE 802.15 (*Wireless Personal Area Networks* – WPAN), especialmente vocacionado para comunicações ponto-a-ponto simples entre pequenos equipamentos móveis, nomeadamente telemóveis, PDA's, impressoras, computadores portáteis, etc. Usa o intervalo de frequências 2.4 – 2.5 GHz com tecnologia FHSS. Uma rede Bluetooth pode acomodar até oito dispositivos, disponibilizando um débito que pode ir até um Mbps a distâncias que variam entre os 10 e os 30 metros, dependendo da potência do sinal.

HomeRF

Sendo o nome HomeRF uma abreviatura de *home radio frequency*, retira-se daí o seu principal mercado alvo: a utilização em ambiente doméstico "(LANSFORD, 1999)". Funciona na banda de frequências dos 2.4 GHz e utiliza a técnica FHSS. Tem por objectivo disponibilizar um meio de comunicação sem fios para equipamentos domésticos de entretenimento e automação, suportando velocidades de até 1.6 Mbps na versão 1.0 e até 10 Mbps na versão 2.0. A tecnologia HomeRF utiliza o protocolo SWAP – *Shared – Wireless Access Protocol*, desenvolvido pelo *HomeRF Working Group* do IEEE.

HiperLAN - *High-Performance Radio Local Area Networks*

Conjunto de normas similares às normas IEEE 802.11 (referidas adiante), desenvolvidas pelo ETSI – *European Telecommunications Standards Institute* e adoptadas em alguns países Europeus.

A primeira versão da norma – HiperLAN/1 – suporta débitos até 20 Mbps, enquanto a segunda versão – HiperLAN/2 – permite atingir os 54 Mbps. Ambas as versões operam na banda de frequências dos 5 GHz.

O HiperLAN/2 utiliza um protocolo orientado à conexão, do tipo *Time Division Protocol* – TDM, que lhe permite a implementação de mecanismos adicionais suporte a Qualidade de Serviço – QoS.

Conjunto de normas IEEE 802.11

Dada a importância da norma IEEE 802.11 e subsequentes evoluções para as WLAN, a próxima secção será dedicada à sua apresentação mais detalhada.

A Norma IEEE 802.11 e evoluções

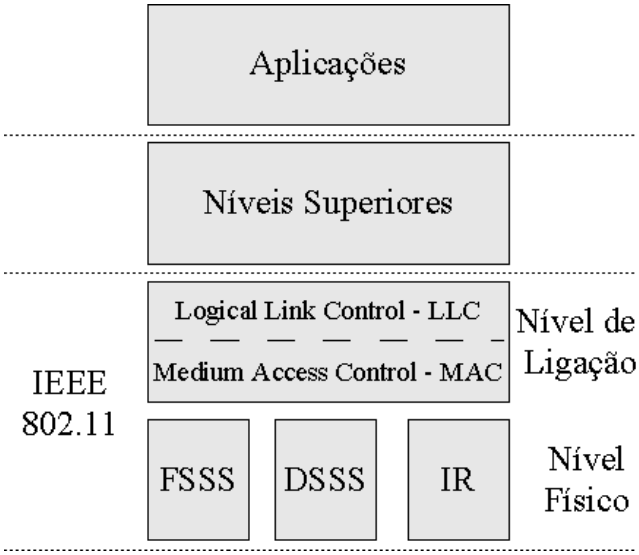
Após trabalhos de aproximadamente 7 anos, em 1997 o IEEE rectificou a norma IEEE 802.11, que veio estabelecer um ponto de referência para a implementação deste tipo de redes ao nível da arquitectura dos níveis físico e de ligação de dados "(ISO/IEC, 1999)".

Tal como os restantes protocolos IEEE 802x, também esta norma intervém ao nível das camadas mais baixas do Modelo OSI, com especificações para os níveis Físico e de *Medium Access Control* – MAC (Figura 4).

As restantes camadas mantém-se semelhantes às definidas para as LAN's da família IEEE 802, nomeadamente a sub-camada superior do nível lógico (*IEEE 802.2 Logical Link Control* – LLC), a estrutura de endereçamento de 48 bits e todos os níveis superiores até à camada de aplicação.

No nível físico são tratadas apenas as transmissões com radiofrequência (RF) e por infravermelho (IR). Na prática, apenas as transmissões por radiofrequência são utilizadas, com recurso às técnicas DSSS ou FHSS.

Figura 4 – Arquitectura Protocolar do IEEE 802.11



No nível de ligação de dados (mais propriamente no sub-nível MAC), o IEEE definiu uma arquitectura constituída por duas funcionalidades básicas: a Função de Coordenação Pontual (PCF - *Point Coordination Function*) e a Função de Coordenação Distribuída (DCF - *Distributed Coordination Function*).

Uma função de Coordenação pode ser definida como sendo a funcionalidade que determina, dentro de um conjunto básico de serviços (BSS), quando uma estação pode transmitir e/ou receber dados do protocolo do nível MAC, através do meio sem fios.

A função de coordenação distribuída é implementada na parte inferior do sub-nível MAC. O seu funcionamento baseia-se em técnicas de acesso aleatório ao meio de transmissão. O tráfego transmitido ao abrigo desta função tem um carácter assíncrono, já que estas técnicas de disputa pelo meio introduzem atrasos aleatórios e não perceptíveis nem toleráveis por serviços síncronos.

O algoritmo básico de acesso a este nível é semelhante ao CSMA/CD[1] implementado na norma IEEE 802.3, sendo aqui designado por CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance* "(BRENER, 1997)".

Por cima da funcionalidade DCF, situa-se (opcionalmente) a função de coordenação pontual (PCF), associada às transmissões livres de disputa, que utilizam técnicas de acesso determinísticas.

A norma IEEE 802.11 define uma técnica de interrogação circular, a partir do ponto de acesso, para este nível. Destina-se ao suporte de serviços síncronos, que não suportam atrasos aleatórios no acesso ao meio.

Estes dois métodos de acesso podem funcionar em conjunto dentro da mesma célula ou conjunto de serviços básicos, recorrendo a uma estrutura denominada super-trama.

Neste caso, a função de coordenação pontual assume o controlo da transmissão, para evitar a ocorrência de colisões.

Uma parte da super-trama é atribuída ao período de disputa pelo meio, permitindo ao subconjunto de estações que funcionam desta forma efectuar transmissões.

Uma vez terminado este período, o ponto de acesso toma posse do meio de transmissão, iniciando-se um período livre de disputa, no qual podem transmitir o resto das estações da célula que utilizam técnicas determinísticas.

O IEEE 802.11 especifica uma taxa de transmissão entre 1 e 2 Mbps. Opera na banda de frequências 2.400-2.4835 GHz, podendo funcionar com FHSS ou DSSS.

Numa rede IEEE 802.11 típica, as estações sem fios (designadas STA) associam-se a Pontos de Acesso (AP), que por sua vez actuam como uma espécie de pontes para a rede de cabos.

A combinação de um AP com as STA's associadas designa-se por *Basic Service Set* – BSS.

Cada rede sem fios é identificada univocamente por um *Service Set Identifier* – SSID. O SSID é um número de 32 bits que é adicionado ao cabeçalho dos pacotes que circulam na WLAN, funcionando também como método básico de autenticação dos clientes perante um Ponto de Acesso.

IEEE 802.11b

Em 1999, o IEEE apresentou uma versão melhorada da norma IEEE 802.11, que designou IEEE 802.11b.

Esta versão, que especifica taxas de transmissão de 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps, trouxe um novo fôlego a este tipo de redes, traduzido numa crescente aceitação do mercado. Uma boa parte das WLAN usadas actualmente são baseadas nesta norma.

Funciona na mesma banda de frequências do IEEE 802.11 (2.400-2.4835 GHz), usando neste caso apenas DSSS, já que a técnica FHSS não suporta velocidades acima dos 2 Mbps sem violar as disposições da FCC. Neste sentido, o IEEE 802.11b apenas mantém compatibilidade com sistemas da norma IEEE 802.11 que utilizam DSSS.

O intervalo de frequências referido é dividido em canais (13 nos países que adoptam as especificações do ETSI), apenas se podendo utilizar 3 num mesmo espaço físico, com um intervalo de 5 canais entre cada (Figuras 5 e 6).

[1] CSMA/CD - *Carrier Sense Multiple Access with Collision Detection*

Em espaço aberto, é possível estabelecer ligações a 11 Mbps até 300 a 400 metros de distância, sem antenas de ganho adicionais. Em espaço fechado, esta distâncias diminui para 30 a 50 metros, dependendo das condições do local.

Para suportar distâncias superiores ou ambientes com maior influência de ruído, esta norma utiliza degradação dinâmica do débito. Quando um terminal se afasta do alcance óptimo do Ponto de Acesso, a norma degrada a transmissão para velocidades inferiores, primeiro para 5.5 Mbps, 2 Mbps e por último 1 Mbps. Quando o terminal se aproxima, verifica-se o processo inverso.

Figura 5 – Gama de frequências e respectivos canais disponíveis numa rede IEEE 802.11b

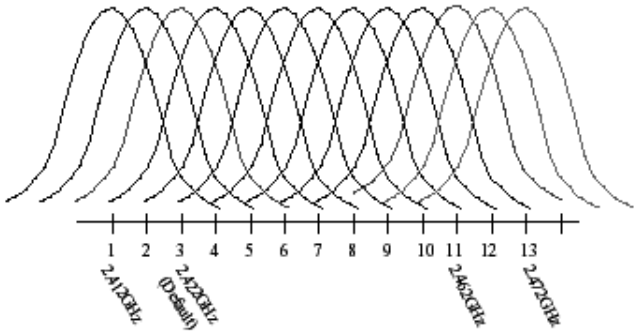
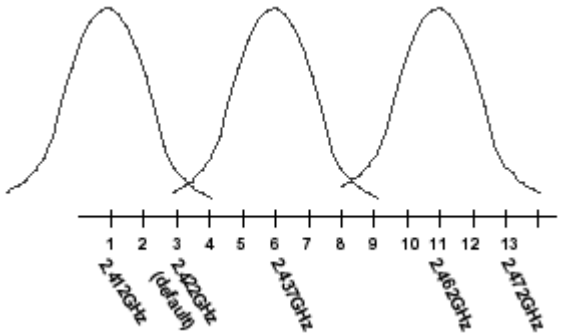


Figura 6 – Canais simultâneos disponíveis numa rede IEEE 802.11b



IEEE 802.11a

A norma IEEE 802.11a foi aprovada aproximadamente na mesma altura da norma IEEE 802.11b, em Dezembro de 1999. Trata-se de mais uma evolução da norma IEEE 802.11 mas com uma diferença fundamental em relação a esta: opera na banda de frequências dos 5 GHz.

Suporta débitos até 54 Mbps para distâncias até 50 metros, com valores intermédios para 6, 12, 18, 24, 36 e 48 Mbps.

Ao nível físico, esta norma usa *Orthogonal Frequency Division Multiplexing* – OFDM, já abordado anteriormente.

A banda de frequências dos 5 GHz é, na generalidade, actualmente ainda muito menos utilizada que a banda dos 2.4 GHz. Por um lado este aspecto apresenta-se como uma vantagem para o IEEE 802.11a, já que a probabilidade de ocorrência de interferências com outros equipamentos a operar na mesma gama de frequências diminui substancialmente. No entanto, por outro lado acaba por se traduzir também numa desvantagem, dada a falta de regulamentação que ainda existe em muitos países para a utilização deste espaço do espectro electromagnético.

Enquanto na banda de frequências dos 2.4 GHz apenas podemos ter 3 canais sobrepostos, o IEEE 802.11a suporta até 12 canais simultâneos, permitindo assim o aumento da largura de banda disponível para os utilizadores, através do incremento de Pontos de Acesso com células sobrepostas. O número real de canais disponíveis para utilização varia de país para país.

Os equipamentos IEEE802.11a não são directamente compatíveis com equipamentos das normas antecessoras (IEEE 802.11 e IEEE 802.11b), por dois motivos:

- funcionamento em bandas de frequências diferentes
- utilizam diferentes tecnologias de *spread spectrum*. O IEEE 802.11a funciona com OFDM enquanto as outras duas normas funcionam com FHSS ou DSSS.

Apesar destas condicionantes, existe interoperabilidade entre os equipamentos das três normas ao nível MAC, já que todas utilizam, a este nível, o algoritmo CSMA/CA da especificação original do IEEE 802.11.

IEEE 802.11g

A norma IEEE 802.11g foi rectificada em 2003, tendo este desfecho sido aguardado com imensa expectativa pelo mercado. Percebe-se facilmente porquê: O IEEE 802.11g promete uma performance comparável ao IEEE 802.11a, com débitos de até 54 Mbps, enquanto mantém compatibilidade retroactiva com a norma IEEE 802.11b. Há quem compare esta combinação de performance e compatibilidade retroactiva com a evolução da Ethernet de 10 Mbps para os 100 Mbps da norma Fast-Ethernet, nas Redes Locais.

Esta norma opera na mesma banda de frequências do IEEE 802.11b (2.4 GHz), estando igualmente limitada ao máximo de três canais sobrepostos.

Um dos requisitos obrigatórios nesta norma é a total compatibilidade com o IEEE 802.11b, sendo visto como um importante factor de protecção de investimento para a actual base instalada.

Por outro lado, tal como o IEEE 802.11a, utiliza OFDM para a transmissão de dados a débitos mais elevados. Quando entra em modo de compatibilidade com a norma IEEE 802.11b, passa automaticamente a utilizar DSSS (Tabela 2).

Tabela 2 – Débitos e tipos de transmissão do IEEE 802.11g

Débito (Mbps)	Tipo de Transmissão
54	OFDM
48	OFDM
36	OFDM
24	OFDM
18	OFDM
12	OFDM
11	DSSS
9	OFDM
6	OFDM
5.5	DSSS
2	DSSS
1	DSSS

Os dispositivos 802.11b não têm capacidade para detectar as transmissões OFDM usadas nos débitos mais elevados do IEEE 802.11g. Assim, esta norma inclui mecanismos de protecção para garantir a compatibilidade retroactiva, o que degrada a performance da rede IEEE 802.11g quando esta inclui clientes IEEE 802.11b.

Breve comparação da capacidade entre as normas IEEE 802.11a, b e g

No contexto das WLAN, a capacidade da rede é medida através do produto do débito real (*throughput*) vezes o número de canais disponíveis.

Nas redes IEEE 802.11b/a/g, o *throughtput* obtido apresenta tipicamente valores bastante abaixo da Taxa Máxima de Transferência anunciada pelas normas. Isto deve-se à utilização, ao nível MAC, do protocolo CSMA/CA e de um mecanismo de protecção denominado *Request to Send/Clear to* Send (RTS/CTS).

Como referido atrás, a performance de uma rede IEEE 802.11g depende, não só das condições ambientais, mas também da presença ou não de clientes IEEE 802.11b.

Tabela 3 – Comparação do *Throughput* entre as normas IEEE 802.11a, b e g

Norma	Débito (Mbps)	*Throughput* (Mbps)	Canais (n.º)	Capacidade (Mbps)
802.11b	11	6	3	18
802.11g (com presença de clientes 802.11b)	54	7	3	21
802.11g(sem presença de clientes 802.11b)	54	22	3	66
802.11a	54	25	12	300

De acordo com as regras da física, existe uma relação inversamente proporcional entre o comprimento de onda e o alcance. Mantendo todas as restantes condições, um sinal transmitido a uma baixa frequência alcança uma maior distância que um sinal transmitido numa frequência mais elevada, atravessando também mais facilmente obstáculos sólidos.

Neste sentido, as normas IEEE 802.11b e IEEE 802.11g apresentam-se em vantagem relativamente à norma IEEE 802.11a.

Por outro lado, outra regra fundamental diz que, à medida que aumenta a taxa de transmissão, o alcance diminuirá.

Assim, supostamente, os débitos mais elevados do IEEE 802.11g deveriam ter um alcance menos que os do IEEE 802.11b. No entanto, como a técnica OFDM é mais eficiente que a técnica DSSS, esta diferença acaba por se esbater significativamente (Tabela 4).

Tabela 4 – Alcance comparativo num ambiente interior "(CISCO, 2003)".

Débito (Mbps)	802.11b *	802.11a **	802.11g ***
54		13 metros	27 metros
48		15 metros	29 metros
36		19 metros	30 metros
24		26 metros	42 metros
18		33 metros	54 metros
12		39 metros	64 metros
11	48 metros		48 metros
9		45 metros	76 metros
6		50 metros	91 metros
5.5	67 metros		67 metros
2	82 metros		82 metros
1	124 metros		124 metros

* 100 mW de potência com antena de 2.2 dBi
** 40 mW de potência com antena de 6 dBi
*** 30 mW de potência com antena de 2.2 dBi

Como se pode constatar pela tabela anterior, para iguais débitos, as normas IEEE 802.11b e IEEE 802.11g atingem o mesmo alcance, já que nesses casos, utilizam ambas a técnica DSSS.

***Wi-Fi* - Wireless Fidelity**

Com o objectivo de garantir a interoperabilidade entre produtos da família IEEE 802.11 de diferentes fabricantes, foi criada uma organização internacional independente, denominada *Wireless Ethernet Compatibility Alliance* – WECA. Esta associação, também denominada *Wi-Fi Alliance*, tem como afiliados os principais fabricantes de equipamento WLAN, tendo como principais funções a certificação dos equipamentos conformes com as normas IEEE 802.11b, IEEE 802.11a e IEEE 802.11g, atribuindo-lhes o selo *Wi-Fi Certified*.

Evoluções futuras das normas IEEE 802.11

Dado o sucesso das normas da família IEEE 802.11, nomeadamente da variante IEEE 802.11b, o IEEE tem criado vários grupos de trabalho, com o objectivo de dar continuidade ao desenvolvimento de novas versões e de novas funcionalidades. Entre os principais, destacam-se "(ZAHARIADIS, 2004)":

- grupo de trabalho 802.11d: tenta adaptar o IEEE 802.11b a outras gamas de frequências, para uso em países onde a banda dos 2.4 GHz não está disponível.
- grupo de trabalho 802.11e: desenvolve trabalho no desenvolvimento de um novo protocolo para o nível MAC das normas 802.11, que suporte mecanismos de Qualidade de Serviço e de segurança adicionais.
- grupo de trabalho 802.11f: tem por objectivo introduzir melhorias no suporte ao *roaming* dos utilizadores entre Pontos de Acesso ligados a redes diferentes.
- grupo de trabalho 802.11h: procura adaptar os requisitos da potência do sinal e da selecção de canais do IEEE 802.11a aos regulamentos Europeus.
- grupo de trabalho 802.11i: trabalha no desenvolvimento de uma *framework* avançada de segurança para as redes IEEE 802.11b/a/g. Este assunto será novamente abordado mais à frente.
- grupo de trabalho 802.11j: desenvolve trabalho na compatibilização das normas IEEE 802.11a e HIPERLAN/2.

SEGURANÇA NUMA REDE WI-FI

A segurança das redes sem fios reveste-se de importância especial, em virtude de o canal de comunicação ser público e partilhado por múltiplos utilizadores.

Estas redes estão especialmente vulneráveis a vários tipos de ameaças, nomeadamente à confidencialidade e integridade da informação e à disponibilidade da própria rede.

A eliminação destas vulnerabilidades passa por dois aspectos fundamentais: autenticação e cifragem dos dados.

Entre os principais requisitos que um mecanismo de autenticação de uma rede deste tipo deve assegurar, destacam-se:

- Autenticação mútua: a rede tem de autenticar o cliente que se vai associar a esta, mas este também deve ter capacidade de autenticar o próprio autenticador.

- Auto-protecção: o cliente e a rede devem proteger o canal de comunicação, já que o meio físico não é seguro.

- Imunidade a ataques de dicionário.

- Utilização de chaves de sessão, para autenticação, confidencialidade e protecção de integridade.

A norma IEEE 802.11 define um mecanismo opcional de cifragem denominado Wired Equivalent Privacy – WEP. Para além de alguns problemas de desenho, recentemente foram descobertas algumas vulnerabilidades que tornaram este mecanismo inseguro como meio de protecção das redes Wi-Fi actuais.

Na tentativa de ultrapassar estas limitações, têm vindo recentemente a ser estudadas alternativas e desenvolvidas novas normas, nomeadamente a *framework* de autenticação 802.1x, o protocolo *Temporal Key Integrity Protocol* – TKIP e o protocolo *Advanced Encryption Standard* – AES, integrado na nova norma IEEE 802.11i.

Estas alternativas serão analisadas mais detalhadamente nas próximas secções, após uma breve referência ao WEP.

Wired Equivalent Privacy - WEP

O mecanismo WEP faz parte da norma IEEE 802.11 original, como mecanismo base de protecção dos dados numa rede sem fios.

Principais funcionalidades deste mecanismo:

- Controlo de acesso à rede sem fios, através de autenticação. Apenas os utilizadores com a chave correcta se conseguem associar à rede.
- Fornecer privacidade nos dados que circulam na rede sem fios. Apenas os utilizadores que conhecem as chaves correctas poderão decifras os dados.

É implementado tendo como base o algoritmo RC4, com cifragem de 40 bit.

Utiliza para tal um esquema simétrico, onde a mesma chave e algoritmo são usados para cifrar e decifras os dados.

Métodos de Autenticação WEP

Numa rede protegida por WEP, um cliente só fica definitivamente associado à rede depois de se autenticar. A norma IEEE 802.11b define dois tipos de autenticação:

- Autenticação Aberta: método de autenticação por defeito numa rede 802.11. Tal como o nome indica, com este tipo de autenticação o Ponto de Acesso aceita qualquer cliente que solicite a junção à rede, processando-se o processo de autenticação e a troca de dados posterior completamente em claro. Tal significa que na prática este tipo de autenticação corresponde a uma autenticação nula, sendo completamente insegura.
- Autenticação com Chave Partilhada: com este método, existe uma chave secreta, partilhada entre os clientes e o Ponto de Acesso. Neste caso, apenas os clientes que fornecerem a chave correcta se conseguem associar à rede. Após este processo, os dados trocados são cifrados usando esta mesma chave secreta, dificultando assim o acesso não autorizado aos mesmos (Figura 9).

Falhas de segurança do WEP

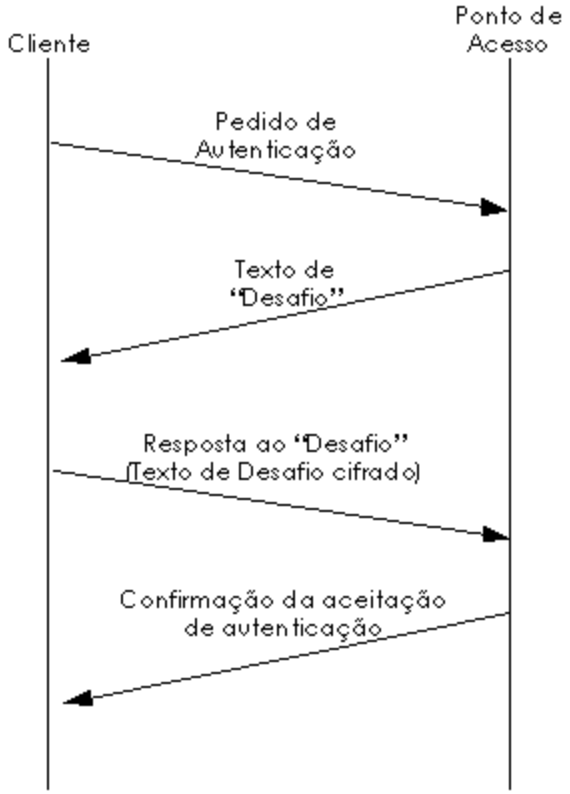
O WEP depende da utilização de uma chave secreta para cifragem e decifragem dos dados. Sendo actualmente o RC4 considerado um algoritmo criptograficamente não seguro, o WEP tem sofrido por tabela as consequências.

Quando o WEP está activo numa rede sem fios, cada pacote é separadamente cifrado usando o algoritmo RC4 com uma chave de 64 bits. Esta chave é composta por um vector de inicialização de 24 bits mais a chave WEP de 40 bits. O pacote cifrado é obtido a partir de uma operação XOR (OU exclusivo) do pacote original com a sequência RC4.

Na sequência deste princípio de funcionamento, têm sido apontadas ao WEP várias falhas de segurança, entre as quais:

- Tamanho e método de gestão das chaves: dado que a norma que institui o WEP não define regras para a gestão das chaves (troca, rotatividade, etc), estas tendem a ser de longa duração e de fraca qualidade. Por outro lado, o próprio tamanho das chaves (40 bits) é actualmente considerado demasiado pequeno, para as capacidades computacionais existentes. Alguns fabricantes têm tentado ultrapassar esta falha aumentando o tamanho da chave para 104 bits, que a juntar ao vector de inicialização perfaz um total de 128 bits.
- Tamanho do vector de inicialização é demasiado pequeno.
- As mensagens de autenticação podem ser facilmente forjadas.

Figura 7 – Processo de autenticação WEP com chave partilhada



***Framework* de Autenticação 802.1x**

O 802.1x foi inicialmente desenvolvido como uma framework de autenticação e controlo de acesso para redes Ethernet cabladas, para tentar limitar algumas das principais vulnerabilidades de segurança no acesso físico a estas redes.

Foi entretanto aproveitado para as WLAN, fornecendo, em combinação com um protocolo de autenticação, controlo de acesso *port-based* e autenticação mútua entre clientes (denominados suplicantes, neste contexto) e Pontos de Acesso, através de um Servidor de Autenticação. Fornece também um método de distribuição dinâmica de chaves para os clientes sem fios, resolvendo assim um dos problemas do WEP com a rotação das chaves.

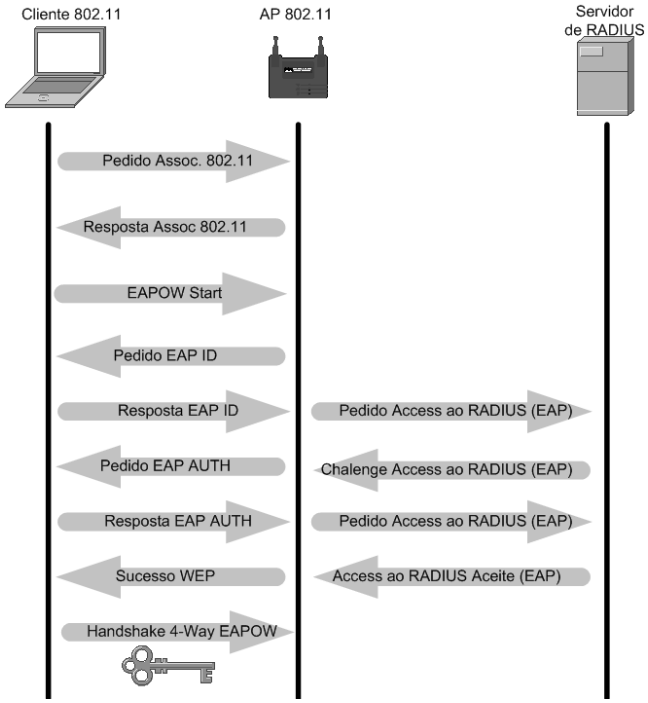
A especificação dos mecanismos de autenticação do 802.1x estão incluídos no draft mais recente do grupo de trabalho IEEE 802.11i, que tem como objectivo fundamental introduzir melhorias de segurança no nível MAC das normas IEEE 802.11.

A framework de segurança 802.1x disponibiliza um conjunto de serviços de autenticação forte no nível 2 do modelo OSI.

Com o objectivo de eliminar algumas das principais vulnerabilidades do WEP, foi desenvolvido um novo protocolo, denominado *Extensible Authentication Protocol* – EAP, sobre o qual foram desenvolvidos diferentes métodos de autenticação. O EAP actua como uma espécie de envelope que transporta um desses métodos.

A figura 8 apresenta o processo de autenticação 802.1x com um protocolo de autenticação da família do EAP.

Figura 8 – Processo de autenticação 802.1x



Assim, sobre esta framework 802.1x, quer na componente de rádio, quer sobre Servidores de Autenticação Radius (iniciais de *Remote Authentication Dial-In User Service*) na rede cablada, podem ser implementados diferentes métodos de EAP. Mais adiante apresentam-se os principais métodos de autenticação EAP disponíveis actualmente.

TKIP – *Temporal Key Integrity Protocol*

O protocolo TKIP, inicialmente conhecido como sendo WEP2, foi a solução de curto prazo encontrada para solucionar o problema da reutilização das chaves WEP.

Um processo TKIP começa com uma chave temporal de 128 bits, partilhada entre os clientes e os Pontos de Acesso. O protocolo combina esta chave temporal com o endereço MAC do cliente, adicionando a seguir um vector de inicialização para produzir a chave com a qual vai cifrar os dados. Este procedimento assegura que cada estação usa diferentes sequências de chaves para cifrar os dados.

Tal como o WEP, o TKIP utiliza RC4 para proceder à cifragem. Apresenta no entanto uma diferença fundamental! Ao contrário do WEP, altera as chaves temporais a cada 10000 pacotes, fornecendo assim um método de distribuição dinâmica que incrementa de forma significativa a segurança no canal de comunicação.

***Advanced Encryption Standard* – AES**

O protocolo AES foi desenvolvido com o objectivo de fornecer um mecanismo de cifragem extremamente forte, tendo sido aprovado como standard oficial pelo Secretário do Comércio Norte-americano em 2002. Prevê-se que venha a substituir o protocolo DES – *Data Encryption Standard*, desde à longo tempo usado como protocolo oficial de cifragem nos mais variados domínios.

Apresenta no entanto uma desvantagem importante, ao requerer a disponibilidade de hardware de processamento adicional. Ou seja, é necessário substituir uma boa parte da base instalada de Pontos de Acesso e placas de rede cliente para implementar o AES.

Atendendo no entanto às taxas previsíveis de crescimento do mercado das WLAN nos próximos tempos, é de esperar que os novos equipamentos comecem a surgir no mercado com suporte para AES.

Métodos de Autenticação EAP

A *framework* de autenticação 802.1x especifica a forma de utilização do EAP directamente sobre um protocolo de ligação de dados (nível 2 do modelo OSI).

De entre os diferentes métodos de autenticação que podem ser usados com este protocolo, alguns recorrem a certificados de chave pública e ao protocolo TLS – *Transport Layer Security*.

Apresentam-se de seguida os principais métodos usados actualmente.

EAP-TLS

O método EAP-TLS utiliza um mecanismo de autenticação baseado em certificados TLS de chave pública.

Disponibiliza autenticação mútua do cliente perante o Ponto de Acesso e vice-versa, precisando ambos de certificados digitais assinados por Autoridade de Certificação (CA) em que ambos confiem.

Entre as principais funcionalidades deste método, destacam-se:

- Autenticação mútua entre cliente e Ponto de Acesso.
- Troca de chaves, para utilização de chaves WEP ou TKIP dinâmicas.
- Fragmentação e reassemblagem de mensagens EAP muito longas, se necessário.
- Rápida recuperação de ligação perdida.

***Protected Extensible Authentication Protocol* - PEAP**

O algoritmo PEAP é actualmente um draft do IETF, tendo sido desenvolvido conjuntamente pela RSA Security, Cisco Systems e Microsoft Corporation.

Adiciona um nível TLS no topo do EAP para autenticar o Servidor de Autenticação no cliente, mas não o inverso.

Trata-se assim de um protocolo que requer apenas certificados digitais do lado do Servidor de autenticação, para a realização desta tarefa. É considerado um protocolo bastante flexível, pelos métodos de autenticação do cliente suportados (par login/password e *One Time Passwords*) e pela capacidade de integração com diversas bases de dados externas com informação de autenticação dos clientes (LDAP, NDS, etc), dependendo da implementação.

Disponibiliza as seguintes funcionalidades:

- Autenticação de mensagens.
- Cifragem de mensagens.
- Autenticação do servidor para o Cliente.
- Troca de chaves, para utilização de chaves WEP ou TKIP dinâmicas.
- Fragmentação e reassemblagem de mensagens EAP muito longas, se necessário.
- Rápida recuperação de ligação perdida.

A Microsoft implementou uma versão de PEAP que suporta autenticação do cliente apenas com MS-CHAP-V2, o que limita as bases de dados com a informação de autenticação às que suportam este protocolo (Domínios Windows NT e Active Directory).

A Cisco desenvolveu também uma variante de PEAP, com autenticação do cliente através de *One-Time Password* – OTP ou par login/password, armazenados em Servidores externos (LDAP, NDS, etc).

Adicionalmente, a implementação da Cisco protege o login do utilizador enquanto o túnel TLS cifrado é estabelecido.

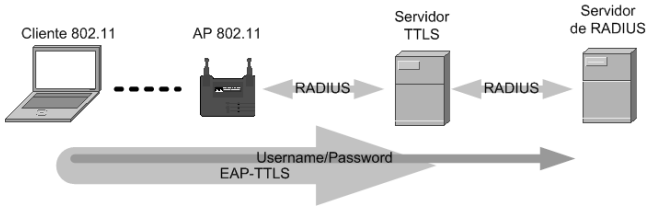
***Tunneled Transport Layer Security* - EAP-TTLS**

O EAP-TTLS é actualmente um draft do IETF, com autoria das organizações Funk Software e Certicom.

É um protocolo muito semelhante ao PEAP, na medida em que procura estabelecer um túnel seguro para autenticação entre o cliente e o servidor.

Tal como o PEAP, também este método estabelece um túnel seguro de TLS iniciado do lado do servidor, o que faz com que não seja necessária a utilização de certificados por parte do cliente (Figura 9).

Figura 9 – Princípio de funcionamento do EAP-TTLS



A grande diferença entre estes dois métodos está no modo como lidam com a autenticação do utilizador. No caso do PEAP é utilizado um método adicional de EAP, por exemplo EAP-GTC para *One Time Passwords* ou EAP-MD5 com login/password. No EAP-TTLS, depois da autenticação do lado do servidor (TLS), são implementados métodos de autenticação do tipo EAP ou então também podem ser usados outros mecanismos de autenticação tradicionais, como seja PAP ou CHAP com login/password.

***Lightweight Extensible Authentication Protocol* - LEAP**

O LEAP é mais um algoritmo de autenticação, desenvolvido pela Cisco Systems para correr sobre 802.1x. Dada a predominância deste fabricante no mercado das redes de computadores, trata-se actualmente de um método bastante utilizado nas funções para as quais foi desenhado.

Disponibiliza um conjunto alargado de funcionalidades, entre as quais:

- autenticação mútua;
- chaves WEP dinâmicas, geradas dinamicamente por utilizador/sessão e periodicamente renegociadas;
- suporta o protocolo TKIP – *Temporal Key Integrity Protocol*.

Sendo um método baseado em autenticação por par login/password em vez de certificados digitais, está mais vulnerável a ataques de dicionário, como comprovaram alguns problemas recentemente detectados. Na sequência dos mesmos, a Cisco está a recomendar aos utilizadores que procedam à

aplicação de chaves fortes ou, em alternativa, que procedam à migração para outro método sem estes problemas.

Breve comparação entre os diferentes métodos EAP

Na tabela 5 é apresentado um breve resumo comparativo entre os diferentes métodos EAP abordados atrás.

Tabela 5 – Comparação de diferentes métodos EAP

	Autenticação do Servidor	Autenticação do Cliente	Chaves Dinâmicas	Riscos de Segurança
EAP-TLS	Chave Pública (certificado)	Chave Pública (certificado ou Smart Card)	Sim	Identidade exposta
PEAP	Chave Pública (certificado)	EAP-MSCHAPv2 ou Chave Pública	Sim	Ataque *man-in-the midle*
EAP-TTLS	Chave Pública (certificado)	CHAP, PAP, MSCHAPv2, EAP	Sim	Ataque *man-in-the midle*
LEAP	Password	Password	Sim	Identidade exposta; ataques de dicionário

WPA – Wi-Fi Protected Access e 802.11i

O grupo de trabalho do IEEE 802.11i rectificou recentemente a norma WPA – *Wi-Fi Protected Access* "(COHEN, 2003)", considerando-o como um sub-conjunto dos mecanismos de segurança incluídos na futura norma IEEE 802.11i (também designada de WPA2).

Tal como outras normas referidas atrás, o WPA está estruturado em duas componentes: autenticação e cifragem do canal sem fios.

Ao nível da autenticação, o WPA implementa 802.1x, com um dos diferentes métodos disponíveis (PEAP, EAP-TTLS, LEAP, etc).

Ao nível da cifragem, o WPA é um substituto do WEP, recorrendo para tal às funcionalidades do TKIP. Apresenta-se na tabela seguinte um breve resumo comparativo dos dois mecanismos.

Tabela 6 – Breve comparação entre o WEP e o WPA

	WEP	**WPA**
Cifragem	Com falhas; segurança quebrada por cientistas e hackers	Resolve todas as falhas do WEP
	Chaves de 40 bits	Chaves de 128 bits
	Chave estática, usada por todos os utilizadores da rede	Chaves dinâmicas de sessão. Chaves por sessão, por utilizador e por pacote
	Distribuição manual das chaves	Distribuição automática das chaves
Autenticação	Com falhas	Autenticação forte por utilizador, utilizando 802.1x e EAP

IMPLEMENTAÇÃO DE UMA REDE WI-FI NUM CAMPUS UNIVERSITÁRIO

Redes Wi-Fi na Educação

Tal como em outros domínios de intervenção, as redes Wi-Fi podem-se traduzir num significativo valor acrescentado no meio académico.

De acordo com o paradigma tradicional, o aluno desloca-se à escola e à sala de aula para desenvolver os seus estudos. No futuro, serão as ferramentas de estudo a deslocar-se com o aluno, com a crescente disponibilidade da informação em qualquer altura e em qualquer lugar que este se encontre.

A disponibilidade de redes Wi-Fi nos Campus Universitários permitirá que os alunos se inscrevam nos cursos, nas disciplinas e nos exames, consultem as sebentas, sumários e exercícios online, a partir do bar, da cantina, da biblioteca ou de qualquer outro espaço público do Campus.

A implementação de uma rede Wi-Fi num Campus Universitário tipicamente vem complementar a infra-estrutura de comunicações cablada existente, potenciando o conceito de ubiquidade – acesso para todos (docentes, alunos, visitantes…), em qualquer hora e em qualquer lugar (na sala de aula, biblioteca, bar, jardim, parque de estacionamento, etc).

Entre os principais benefícios deste tipo de infra-estruturas, destacam-se:

- Mobilidade no acesso à informação e aos recursos: Facilita a implementação de aplicações que requeiram ligação permanente à rede em ambientes que envolvam movimentação do utilizador no campus.
- Aumento da produtividade: As WLANs permitem aos seus utilizadores serem mais produtivos, já que possibilitam o acesso à Internet, e-mail, bases de dados e a ficheiros de rede, em qualquer lugar do campus, bem como permitem introduzir novos serviços (ex: Instant Messaging) que ajudem em tempo útil no suporte à decisão;
- Redução de custos: Face a uma utilização mais eficiente dos recursos e infra-estruturas;
- Flexibilidade: É mais fácil adicionar, retirar ou modificar clientes que usem a tecnologia de acesso wireless, nomeadamente em infra-estruturas de rede temporárias. Os utilizadores podem ainda trabalhar em vários locais sem necessidade de grandes configurações por parte dos administradores da rede.
- Trabalho colaborativo: Facilidade de acesso a ferramentas de partilha de ficheiros, e-mail, Instant Messaging e Groupware a partir de qualquer localização.

Dada a dimensão destes projectos, a fase de planeamento é fundamental para o sucesso desta tarefa, tornando-se fundamental uma análise prévia dos requisitos a diversos níveis, nomeadamente:

- Definição da tecnologia a utilizar: IEEE 802.11b, g ou a ou uma combinação das mesmas.
- Determinação das áreas de cobertura através da realização de *site survey* com equipamentos similares aos que se pretende usar na implementação.
- Determinação das possíveis falhas de segurança na rede e elaboração de um plano com as medidas e mecanismos de

segurança a implementar, em conjunto com os mecanismos de autenticação dos utilizadores.
- Análise cuidada das infra-estruturas de backbone disponíveis e levantamento das necessidades ao nível de eventuais actualizações necessários na mesma para suporte à nova rede. Alguns aspectos importantes a este nível tem a ver com o suporte ou não à criação de diferentes VLAN's, suporte a diferentes níveis de qualidade de serviço, etc.
- Identificação das necessidades de mobilidade relacionadas com o *roaming* dos utilizadores.
- Mecanismos de Gestão e manutenção preventiva da nova infra-estrutura.

Considerações prévias à fase de instalação

***Site Survey* e escolha da tecnologia e equipamentos**

Caso a escolha dos equipamentos recaia sobre Pontos de Acesso conformes com a norma IEEE 802.11b, é fundamental a verificação da possibilidade de uma migração posterior para a tecnologia IEEE 802.11g sem custos adicionais significativos.

Atendendo à larga experiência, divulgação e versatilidade na selecção de antenas da norma IEEE 802.11b, em primeiro lugar a escolha deve recair na utilização de Pontos de Acesso 802.11g ou 802.11b. Dadas as vantagens anteriormente identificadas da norma IEEE 802.11g, a escolha de equipamentos baseados na norma 802.11a deve ainda ser considerada como uma segunda alternativa, para ambientes que estejam sujeitos a um nível elevado de interferências na faixa dos 2.4 GHz.

O número de Pontos de Acesso utilizado na implementação de uma rede Wi-Fi depende das conclusões tiradas do *Site Survey* efectuado, bem como da previsível distribuição dos utilizadores no respectivo Campus e débitos de comunicação requeridos para suporte das aplicações.

Por questões de segurança física estes equipamentos deverão ser instalados, sempre que possível, em tectos falsos ou em zonas de difícil acesso. O número de utilizadores / ligações simultâneas, por zona de cobertura de uma determinada célula, depende do tipo de aplicações suportadas, tempos de resposta adequados para as mesmas e modelo de Ponto de Acesso/antenas seleccionado. Desta forma, em zonas de grande concentração de utilizadores, recomenda-se uma maior cobertura de Pontos de Acesso, dentro dos limites impostos pela tecnologia, nomeadamente quanto ao número de canais sobrepostos.

Por questões relacionadas com a facilidade de instalação, estes equipamentos devem permitir a alimentação através do cabo Ethernet, de acordo com a norma IEEE 802.3af (*Power over Ethernet*), sendo para isso possível utilizar, *Power Injectores* e/ou switches de concentração de Pontos de Acesso com *Inline Power*.

Numa rede Wi-Fi com infra-estrutura, onde vários Pontos de Acesso têm por objectivo disponibilizar conectividade sem fios em espaços contíguos, a disposição destes equipamentos deve ser feita tendo em atenção:

- ligeira sobreposição entre as células de Pontos de Acesso contíguos para permitir a mobilidade dos utilizadores entre células;

- a não sobreposição de canais, pelo que nenhum local pode ter cobertura simultânea de mais do que três Pontos de Acesso (Figuras 10 e 11).

Figura 10 – Disposição de células Wi-Fi sem interferências entre os canais

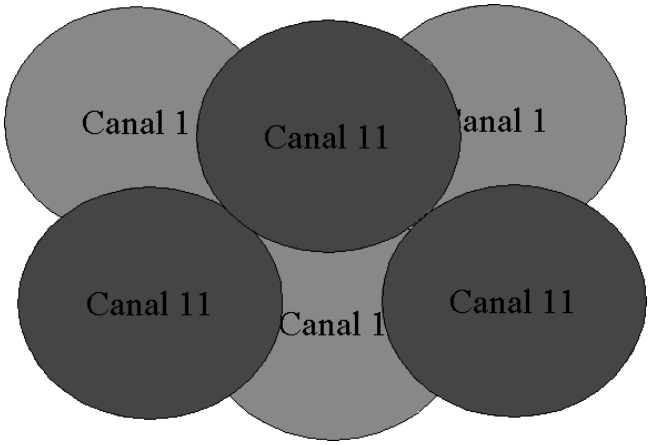
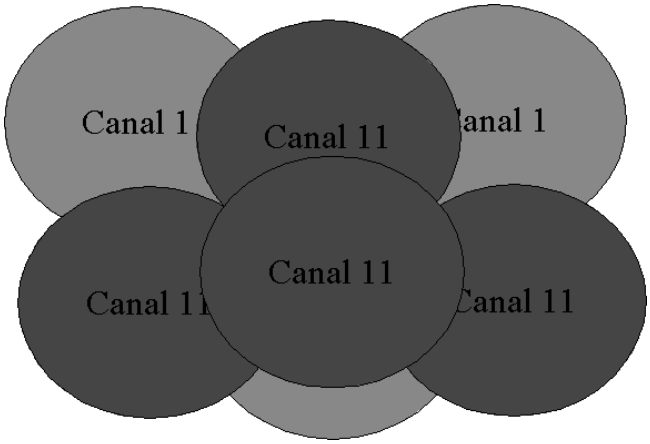


Figura 11 – Disposição de células Wi-Fi com interferências entre os canais



Modelo de Autenticação e Segurança

A instalação de uma infra-estrutura deste tipo vai-se traduzir num aumento do número de pontos de acesso à rede, o que torna necessariamente as infra-estruturas da rede interna mais vulneráveis a ataques de utilizadores não autorizados.

Desta forma há necessidade de estruturar a solução de modo a implementar mecanismos de segurança eficazes que cumpram os seguintes objectivos:

- Fornecer a segurança adequada: Garantir que os utilizadores só têm possibilidade de aceder a determinados recursos, de acordo com o seu perfil, e proteger a infra-estrutura de outros acessos não autorizados;
- Fácil administração: Os sistemas devem garantir um método fácil para a manutenção dos mecanismos de segurança ao longo do tempo;
- Transparência para o utilizador: Devem ser evitados mecanismos de segurança extremamente difíceis de operar e de ser activados pelo utilizador.

No sentido de concretizar os objectivos anteriormente delineados, a autenticação / autorização dos utilizadores deverá ser assegurada através da utilização de servidores de autenticação baseados no protocolo RADIUS, nos quais são inseridos os vários perfis dos utilizadores.

Quando o número de utilizadores autorizados a utilizar a rede é muito elevado, é aconselhável implementar um Serviço de

Directório baseado no protocolo LDAP – *Lightweight Directory Access Protocol* podendo funcionar como repositório central de autenticação para os mais variados serviços:

- Autenticação na rede Wi-Fi, com recurso a 802.1x através de um servidor de RADIUS;
- Serviço de correio electrónico;
- Autenticação WEB no portal da instituição, etc.

Para além do processo de autenticação, também os dados que circulam na rede sem fios devem ser protegidos por mecanismos fortes de cifragem. Aconselha-se neste sentido a adopção da norma WPA como mecanismo base de protecção da rede.

Uma alternativa à utilização de um mecanismo de cifragem como o WEP ou o WPA, passa pelo recurso a serviços de VPN – *Virtual Private Networking* para protecção do canal de comunicação sem fios.

Neste caso, a infra-estrutura central tem de ser equipada com um Concentrador de VPN's, para onde o utilizador móvel estabelecerá um túnel seguro, a partir do seu equipamento terminal. Desta forma, torna-se indiferente se o canal sem fios está ou não protegido, já que os dados entre o utilizador móvel e a infra-estrutura cablada circularão pelo canal seguro criado pela VPN.

Para protecção da informação contida nas respectivas infra-estruturas centrais, além dos servidores de autenticação referidos anteriormente, é aconselhável a instalação de um sistema de firewall que permita a criação de um perímetro de segurança e de controlo de todo o tráfego que entra ou sai desse mesmo perímetro.

Os níveis de segurança disponibilizados pelos sistemas de firewall assentam fundamentalmente em mecanismos de segurança defensivos não sendo nestes contemplada a vigilância activa do perímetro protegido pelo correspondente equipamento, por exemplo, em termos da detecção de actividades de intrusão, pela análise de padrões de ataque ou de assinaturas digitais de ficheiros. Para que tal seja implementado é necessário utilizar software adequado para a análise do tráfego em tempo real, nomeadamente ao nível da detecção de ataques, usando sondas sondas IDS.

Infra-estruturas de backbone e QoS

A utilização de mecanismos que assegurem a qualidade de serviço (QoS) numa infra-estrutura é essencial para a implementação com sucesso de algumas aplicações mais recentes, como por exemplo soluções de e-learning ou VoIP (voz sobre IP). Estas aplicações exigem, além de uma grande largura de banda disponível, um serviço diferenciado. Em muitos casos, é preciso garantir que a transmissão de dados é feita sem interrupção ou perda de pacotes.

Tradicionalmente as redes locais utilizam uma filosofia de *best effort* para efectuarem a comutação dos pacotes IP nos quais estão encapsulados os dados aplicacionais. Os referidos pacotes são encaminhados da melhor forma possível, conforme as rotas existentes e a largura de banda disponível no momento. Quando ocorre uma situação de congestionamento, os pacotes são descartados sem distinção do tipo de serviço suportado.

Para solucionar este problema é fundamental que os equipamentos activos utilizados para constituir a infra-estrutura da rede de comunicações, nomeadamente os equipamentos de backbone, tenham a capacidade de utilização de mecanismos de QoS baseados nos protocolos IEEE 802.1p *Class of Service* (CoS) e *IETF Differentiated Service* (DiffServ). A utilização destes mecanismos permite que se efectue a marcação dos pacotes IP para distinguir os vários tipos de serviços, possibilitando assim aos equipamentos de rede encaminhar os pacotes IP de acordo com os níveis de prioridade definidos nos mesmos.

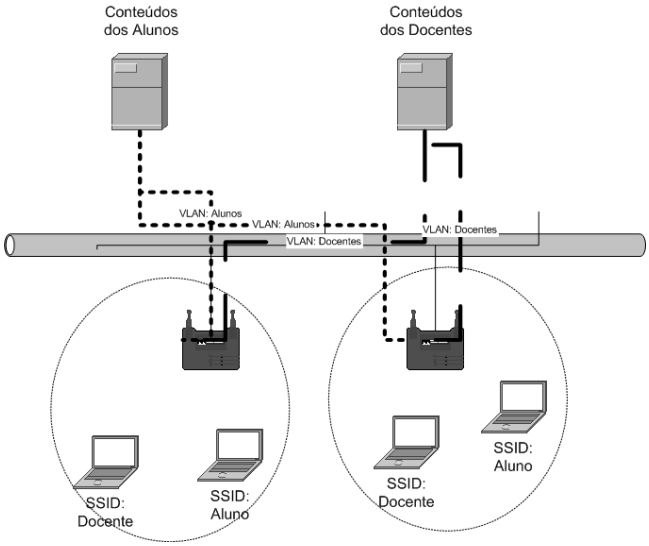
Em redes WLAN é igualmente importante que os Pontos de Acesso tenham a capacidade de analisar o tipo de tráfego e, em função do mesmo, efectuar a prioritização de acordo com o tipo de aplicações, de forma a garantir a qualidade de serviço necessária numa infra-estrutura desta natureza. A arquitectura destes equipamentos deverá ainda permitir actualizações de hardware e de software para possibilitar a inclusão de novas funcionalidades à medida que estas vão sendo normalizadas/disponibilizadas, nomeadamente o suporte de novos standards como o IEEE 802.11e.

Adicionalmente os equipamentos a utilizar para a implementação da infra-estrutura de comunicações devem ter a capacidade de criar VLANs baseadas no standard IEEE 802.1Q para permitir que numa única infra-estrutura física sejam criadas várias redes virtuais distintas, possibilitando desta forma a associação de cada grupo de utilizadores a uma VLAN determinada.

Os fluxos de tráfego entre as várias VLANs devem ser controlados preferencialmente por sistemas de firewall.

A associação dos utilizadores da rede Wi-Fi a diferentes VLAN's pode ser feita recorrendo a um mapeamento SSID/VLAN. Alguns dos mais recentes Pontos de Acesso Wi-Fi já suportam mapeamentos de múltiplos SSID/VLAN, o que significa na prática que um mesmo equipamento suporta mais do que uma rede lógica WLAN. Para implementar estas funcionalidades, é necessário que a infra-estrutura de backbone dê continuidade às VLANs criadas nos Pontos de Acesso Wi-Fi (Figura 12).

Figura 12 – Mapeamento SSID/VLAN



Mobilidade e Roaming dos utilizadores

Uma das maiores vantagens que uma solução WLAN apresenta é sem dúvida o facto de permitir uma maior mobilidade dos seus utilizadores. No entanto, para esta liberdade de movimentos ser real, é necessário que quando um utilizador abandona a zona de cobertura de uma célula e passa a estar inserido na área de cobertura de uma outra célula, a transição da sessão estabelecida com o primeiro equipamento seja transferida para o segundo de uma forma completamente transparente para o utilizador.

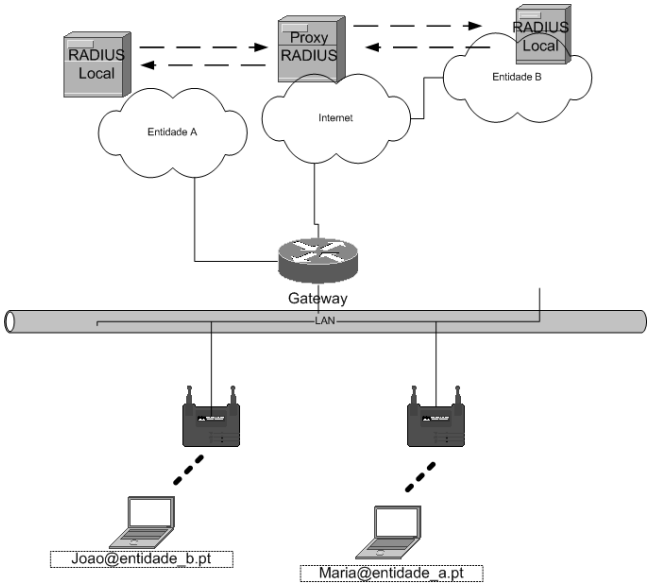
Este objectivo só será efectivamente alcançado através da utilização de equipamentos que suportem mecanismos de roaming entre os diversos Pontos de Acesso. Desta forma a área a cobrir pela solução WLAN deve estar isenta de zonas sem sinal.

Esta condição é atingida com um planeamento eficaz da distribuição de Pontos de Acesso, selecção adequada dos canais de operação e respectiva potência de transmissão destes equipamentos. Deve garantir-se ainda a sobreposição (*overlapping*) das áreas de cobertura dos Pontos de Acessos entre 10% - 15%, tendo sempre em conta que o número máximo de canais que podem ser sobrepostos sem que ocorram interferências, e consequentemente degradação da performance da rede, são três nas normas IEEE 802.11b e IEEE 802.11g. Este planeamento deve ser assegurado durante a fase de *Site Survey*, referida anteriormente.

Adicionalmente o conceito de *roaming* pode ser estendido a horizontes mais alargados, permitindo o acesso dos utilizadores registados num campus da Entidade quando se deslocam para outro campus dessa mesma Entidade, ou aos utilizadores de uma determinada Entidade a partir de qualquer outra, desde que devidamente autenticado e autorizado.

Este serviço de *roaming* é conseguido à custa da implementação de dois níveis de servidores de RADIUS "(GUIDO, 2004)". O servidor de autenticação de cada Entidade irá ter uma dependência de um servidor de RADIUS central quando o domínio dos utilizadores que se querem autenticar não seja o da própria Entidade onde estão a aceder à rede WLAN. O servidor central será responsável pelo encaminhamento do pedido de autenticação (proxy RADIUS) para o servidor da Entidade a que os utilizadores pertencem (Figura 13).

Figura 13 – Utilização de um Proxy RADIUS para suporte de a mobilidade entre redes



REDES WI-FI – NOVOS SERVIÇOS

A criação de uma infra-estrutura deste tipo apresenta duas vantagens importantes: disponibilidade em locais até então inacessíveis e possibilidade de utilização por novos utilizadores, até então sem meios ou permissões de acesso à infra-estrutura tradicional cablada.

Entre os principais serviços tipicamente disponibilizados sobre estas redes, destaca-se o acesso:

- à World Wide Web e a portais aplicacionais internos, como por exemplo serviços de consulta de notas, realização de matrículas, portais de e-learning, etc.
- ao Correio Electrónico;
- a serviços de *Instant Messaging*;
- a ferramentas de trabalho colaborativo e workflow, etc.

Para além destes serviços tradicionais, dadas as vantagens da disponibilidade em novos locais e para novos utilizadores, é possível desenvolver novos e inovadores serviços sobre estas infra-estruturas.

A título de exemplo, apresentam-se a seguir alguns exemplos de novos serviços potenciais.

Telefonia IP

A Telefonia IP é uma tecnologia baseada no VoIP – *Voice ver* IP e na norma ITU-T H323, que permite a transmissão de voz em redes IP com níveis de funcionalidade aproximados aos dos serviços tradicionais de voz. Precisa no entanto de requisitos muito específicos ao nível de alguns parâmetros de qualidade de serviço, ainda não acessíveis a algumas redes IP.

Apesar disso, começa a impor-se hoje em dia em alguns mercados específicos. Principalmente na Ásia há já operadores de telecomunicações que prestam este tipo de serviço e que permite levantar algumas das limitações do serviço de voz tradicional.

Com as recentes evoluções nas redes Wi-Fi, ao nível do débito, segurança e qualidade de serviço, é de esperar evoluções positivas na utilização futura deste tipo de infra-estruturas para este serviço.

Actualmente já começam a surgir fabricantes com soluções de terminais Wi-Fi móveis com suporte para Telefonia IP, o que permite aos utilizadores navegarem por um conjunto de *hotspots* tendo a possibilidade de fazer chamadas telefónicas e um conjunto de serviços adicionais avançados.

Tele-vigilância

Tradicionalmente, este tipo de serviços requer a instalação de infra-estruturas dedicadas e tipicamente dispendiosas.

Com a disponibilidade de um canal alternativo de comunicação em locais até então inacessíveis, passa a ser possível implementar sistemas de tele-vigilância com investimentos menos onerosos e com maior flexibilidade na escolha dos equipamentos, baseados em normas abertas.

O CASO DO CAMPUS VIRTUAL DO IPB

Breve descrição do IPB

O Instituto Politécnico de Bragança – IPB - é uma Instituição Portuguesa de Ensino Superior Politécnico, frequentada actualmente por mais de 5500 alunos, apoiados por mais de 400 docentes.

Integra actualmente cinco Escolas – Escola Superior Agrária, Escola Superior de Educação, Escola Superior de Tecnologia e de Gestão de Bragança, Escola Superior de Saúde e Escola Superior de Tecnologia e Gestão de Mirandela, onde são ministrados mais de 30 cursos de licenciatura e alguns de mestrado, nas áreas da Educação, Ciências Agrárias, Informática, Gestão, Engenharias e Saúde.

As três primeiras escolas estão sediadas no principal Campus da Instituição - Campus de Santa Apolónia (Figura 14) -, em Bragança, onde também se localizam os Serviços Centrais do Instituto e os Serviços de Acção Social. Estes últimos têm como missão a prestação de serviços de apoio social aos alunos, com a

gestão e manutenção de uma cantina central, três residências estudantis e diversos equipamentos desportivos.

Figura 14 – Campus de Santa Apolónia, em Bragança

A Escola Superior de Saúde está também sediada na mesma cidade, junto ao Hospital Distrital de Bragança e portanto fora do Campus de Santa Apolónia.

A Escola Superior de Tecnologia e Gestão de Mirandela está sediada nesta cidade, a aproximadamente 50 quilómetros da cidade de Bragança. Encontra-se actualmente distribuída por três edifícios distintos, espalhados pela cidade de Mirandela.

O Projecto "Campus Virtual do IPB"

O projecto "Campus Virtual do IPB" começou a ser desenvolvido em Março de 2003, após o lançamento da *Iniciativa Campus Virtuais – e-U*[2], pela Unidade de Missão Inovação e Conhecimento (UMIC) do Governo Português.

Esta iniciativa tem como principais objectivos criar uma rede nacional de partilha de conhecimento e acesso a informação entre todas as instituições portuguesas de ensino superior, com três vertentes fundamentais:

- criação de uma rede Wi-Fi em cada Campus Universitário do país, onde os docentes e alunos passarão a ter acesso aos mais diversos serviços electrónicos;
- potenciar a informatização e webização dos serviços administrativos, académicos e pedagógicos das instituições de ensino superior. Desta forma, os alunos poderão realizar as mais diversas acções administrativas através da WEB. Entre outros, destacam-se serviços como a consulta de notas, alteração de dados pessoais, matricula nas disciplinas e em exames, pagamentos por via electrónica, etc. Nesta vertente pretende-se também promover a publicação em formato electrónico de sebentas e outro material pedagógico, para ser possível a sua partilha e fácil acesso por toda a comunidade académica nacional.
- Promover a aquisição de equipamento informático, especialmente computadores portáteis, junto dos alunos e docentes.

Atendendo a que, em relação à segunda vertente da iniciativa, o IPB já à algum tempo vinha a desenvolver um trabalho sólido, apresentou a sua candidatura a esta iniciativa em Abril de 2003, contemplando apenas a componente da rede Wi-Fi e algumas melhorias na ferramenta de apoio pedagógico – e-learning -, entretanto já desenvolvida internamente.

Actualmente em fase final de instalação, a rede Wi-Fi do IPB contempla a cobertura da totalidade dos espaços interiores da instituição, bem como alguns espaços exteriores de referência (parques, praças, etc). É constituída por um total de 130 Pontos de Acesso conformes com a norma IEEE 802.11g, recentemente rectificada.

Vai permitir o acesso aos mais variados serviços a todos os alunos e docentes da instituição, bem como a visitantes de outras instituições de ensino que também estejam presentes na rede nacional do e-U.

Todos os alunos, docentes e restantes funcionários da Instituição possuem uma conta num Servidor Central LDAP, a partir do qual é efectuada a autenticação para acesso à rede e aos diversos serviços aplicacionais disponibilizados por via electrónica.

De entre os Serviços para alunos e docentes já actualmente disponíveis na WEB, destacam-se:

- Serviços de Comunicações:
  - Correio Electrónico para todos os docentes, alunos, e restantes funcionários, com acesso por POP3S, IMAPS ou interface Webmail.
  - Listas de Correio, disponíveis para comunicação em grupo, quer entre os alunos, quer entre os docentes.
- Serviços Académicos:
  - Consulta e alteração dos dados pessoais.
  - Consulta de notas.
  - Matricula nos cursos, em disciplinas e nos exames
  - Pagamento de propinas através de sistemas de pagamento automático (Multibanco), com referência e valor gerados automaticamente.
- Apoio às Aulas e E-Learning:
  - Consulta de sebentas, exercícios práticos e outro material multimédia online.
  - Fóruns de discussão por disciplina.

Atendendo ao ambiente de enorme expectativa que tem rodeado a instalação da rede Wi-Fi por parte dos alunos e docentes do IPB, parece-nos que a sua entrada em funcionamento pleno (prevista para a segunda quinzena de Março) vai potenciar decisivamente a criação de novos hábitos de relacionamento e partilha de informação entre toda a comunidade académica desta Instituição.

LITERATURA CITADA

AMARO, J.; LOPES. R. **Rede Digital Comunitária: uma Rede sem fios metropolitana**. CRC'2000 – 3ª Conferência sobre Redes de Computadores, Viseu: Instituto Politécnico de Viseu, 2000.

BISDIKIAN, C. **An overview of Bluetooth Wireless Technology**. IEEE Communications Magazine, 2001.

BRENER, P. **A Thechnical Tutorial on the IEEE 802.11 Protocol**. Breesecom Wireless Communications, 1997.

COHEN, D. **Wi-Fi Protected Access**. Networld+Interop, 2003.

GUIDO, L. **Campus Virtuais: Arquitectura de Roaming Nacional**. Lisboa: FCCN, 2003.

KHAN, L.; KHWAJA, A. **Building Secure Wireless Networks with 802.11**. Indianapolis: Wiley Publishing, Inc, 2003.

[2] Sítio da iniciativa em www.e-u.pt

VINES, R. **Gíreles Security Essentials – Defending Mobile Systems from Data Piracy**. Indianapolys: Wiley Publishing, Inc, 2002.

LANSFORD, J. **HomeRF: Bringing Wireless Connectivity Home**. Intel Labs, 1999.

MONTEIRO, E.; BOAVIDA, F. **Engenharia de Redes Informáticas**. Lisboa: FCA – Editora de Informática, Lda, 2000.

ISO/IEC, **IEEE 802.11 Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical (PHY) Specifications**, ISO/IEC 8802-11, 1999.

CISCO, **Capacity, Coverage and Deployment Considerations for IEEE 802.11g,** White Paper, Cisco Systems, 2003.

ZAHARIADIS, T. **Evolution of the Wireless PAN and LAN standards**. Computer Standards & Interfaces 26 – pp 175-185. Elsevier, 2004.