

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – IFRN

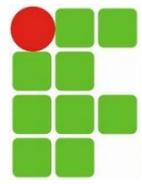
Disciplina: Redes de Computadores

Professor: M. Sc Rodrigo Ronner T. da Silva

E-mail: rodrigo.tertulino@ifrn.edu.br

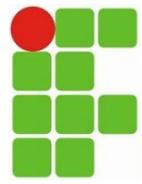


Prof. Rodrigo Ronner - IFRN



Redes wireless

- Redes de computador em que os meios de transmissão não usam cabos físicos
- Usadas em ocasiões ou locais em que as soluções cabeadas não são empregadas
 - Complementam as redes cabeadas
- Motivação: telefones celulares
- Exemplos comuns
 - Infravermelho
 - Bluetooth
 - Wi-Fi
 - WiMAX



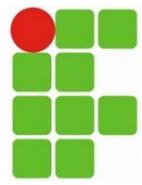
Wireless - Vantagens

- Flexibilidade e mobilidade
- Convenientes na instalação – evita o trabalho de passagem de cabos
 - Reduz custo (dispensa cabeamento)
- Baratas – Equipamentos tem preço acessível
- Pode ser implementada em praticamente qualquer lugar
- Manutenção reduzida



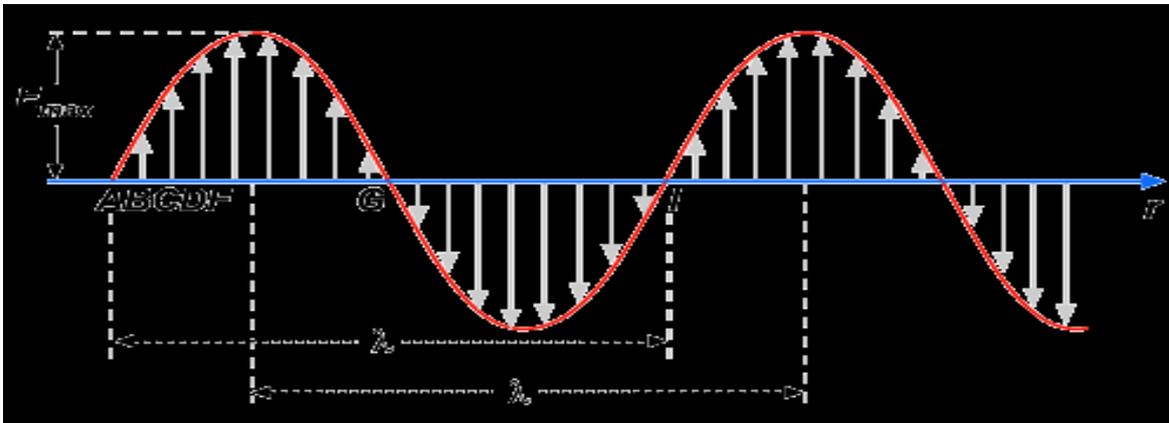
Wireless - Desvantagens

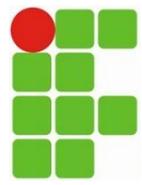
- Largura de banda inferior aos métodos cabeados (Fast e Giga Ethernet)
- Problemas com a segurança da informação
- Qualidade de serviço
 - Força do sinal é decrescente
 - Interferências de outras fontes
 - Propagação multidirecional
- Ligações mais difíceis de estabelecer
 - Necessidade de prot. de correção de erros robusta
 - Partilha do meio de transmissão



Ondas

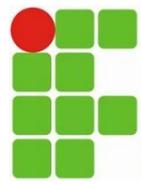
- Ondas eletromagnéticas são ondas cíclicas que se repetem em uma determinada frequência
 - 1 Hz = 1 ciclo por segundo
 - KHz; MHz; GHz
- Viajam à velocidade da luz
- Comprimento de onda diminui quando a frequência aumenta





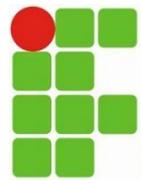
Espectros das redes wireless

Banda	Uso
806-890Mhz	Rede Celular
900 Mhz	Telefone sem fio
2,4Ghz até 2,4835Ghz	Telefones sem fio e redes wireless
4 Ghz – 5 GHz	Antenas parabólicas
5 GHz	Redes wireless (802.11a)



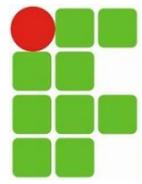
Tecnologia Wi-Fi

- *Wireless Fidelity* – Nome comercial dado à família de padrões 802.11 do IEEE
- Disseminação muito grande nos últimos anos
 - Notebooks e PDAs normalmente já suportam o uso nativamente
- Padrões comerciais
 - 802.11a (5 GHz; 54 Mbps) OFDM
 - 802.11b (2.4 GHz; 11 Mbps) DSSS
 - 802.11g (2.4 GHz; 54Mbps) OFDM
 - 802.11n OFDM



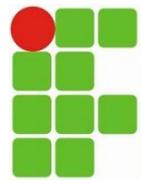
Padrão 802.11 original

- Opera na faixa de frequência 2.4 GHz
- Taxa de transmissão teórica: 1-2 Mbps
 - Taxa real é menor, perto da metade
- Menos suscetível a interferência do meio porque a frequência é usada por poucos aparelhos
- Necessário mais energia a 5 GHz (bateria)
- Maior perda de sinal a 5 GHz
 - Alcance mais curto



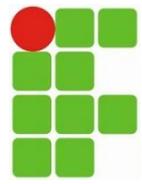
Padrão 802.11a

- Opera na faixa de frequência 5 GHz
- Taxa de transmissão teórica: 54 Mbps
 - Taxa real é menor, perto da metade
- Menos suscetível a interferência do meio porque a frequência é usada por poucos aparelhos
- Necessário mais energia a 5 Ghz (bateria)
- Maior perda de sinal a 5 GHz
 - Alcance mais curto



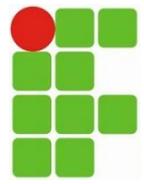
Padrão 802.11b

- Opera na faixa de frequência 2.4 GHz
- Taxa de transmissão teórica: 11 Mbps
- Primeiro padrão a disseminar no Brasil
- Muito suscetível a interferência
 - Opera na faixa de frequência de vários aparelhos
 - Bluetooth; Fornos de microondas; telefones sem fio; equipamentos médicos
- Alcance médio indoor: 35mt



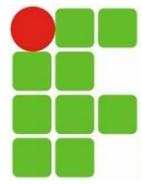
Padrão 802.11g

- Opera na faixa de frequência 2.4 GHz
- Taxa de transmissão teórica: 54 Mbps
- Padrão mais comum na atualidade
- Muito suscetível a interferência
 - Mesma forma do padrão 802.11b
- Suporta comunicação com dispositivos 802.11b, com velocidade setada pelo padrão inferior
- Pode alcançar até 108Mbps com uso de compactação proprietária
- Alcance médio indoor: 25mt



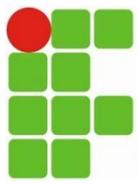
Padrão 802.11n

- Opera na faixa de frequência 5 GHz Ou 2,4Ghz
- Taxa de transmissão teórica: 300 Mbps
- Menos suscetível a interferência
- Alcance médio aparentemente maior que os padrões anteriores



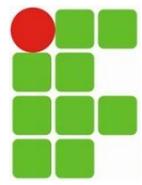
Padrão 802.11ac

- Opera apenas na faixa de 5GHz (que é menos poluída)
- Taxa de transmissão teórica: 1300 Mbps
- Menos suscetível a interferência
- Traz a possibilidade de conversar simultaneamente com diversos aparelhos conectados ao roteador sem qualquer interrupção. Por mais rápido que fosse o padrão "N" só permitia que essa conversa fosse feita com um dispositivo por vez.



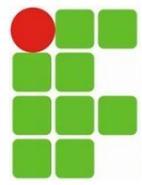
Comparativo 802.11

Padrão	Velocidade máxima	Frequência	Compatível com versões anteriores
802.11a	54 Mbps	5 GHz	Não
802.11b	11 Mbps	2,4 GHz	Não
802.11g	54 Mbps	2,4 GHz	802.11b
802.11n	600 Mbps	2,4 Ghz ou 5 GHz	802.11b/g
802.11ac	1,3 Gbps (1300 Mbps)	2,4 GHz e 5,5 GHz	802.11b/g/n
802.11ad	7 Gbps (7000 Mbps)	2,4 GHz, 5 GHz e 60 GHz	802.11b/g/n/ac



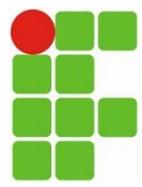
Tipos de dispositivos

- Estações
 - Dispositivo compatível com interface e MAC 802.11
 - Micros, notebooks, Smartphones e etc.
- Access Points
 - Sistema de distribuição para estações associadas
 - Centraliza a comunicação
 - Também chamado de concentrador
- Routers
 - Incorpora funções de switch, roteador, AP e às vezes modem ADSL



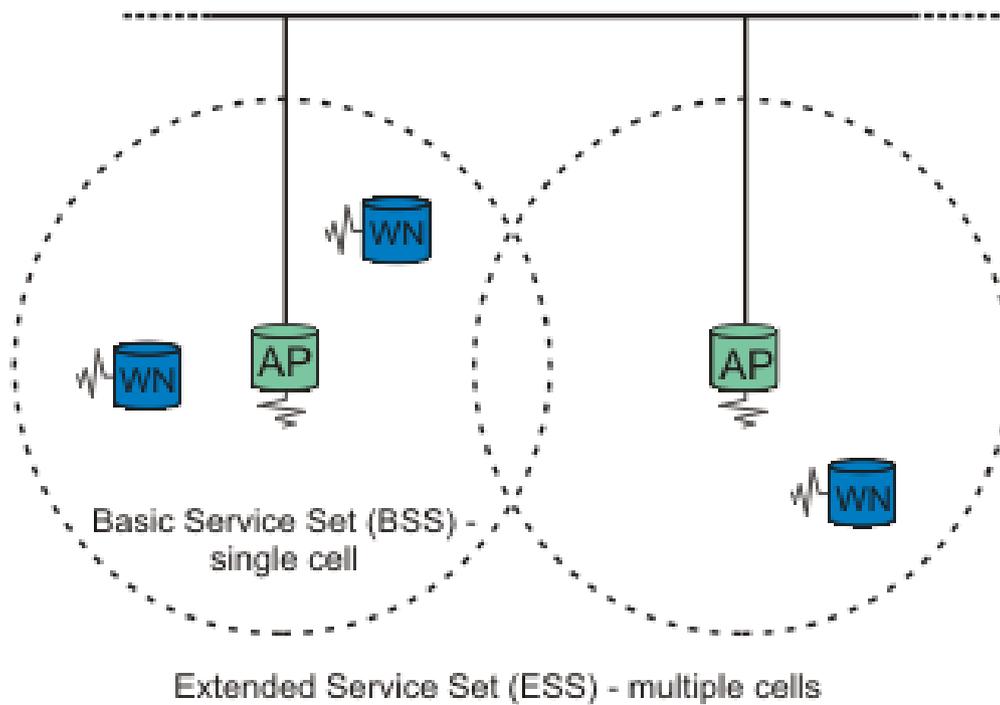
Tipos de redes

- Ad-hoc
 - Comunicação ponto-a-ponto
 - Cada dispositivo da rede comunica-se diretamente com o outro
- Infra-estrutura
 - Dispositivos se conectam a um controlador ou ponto central para retransmitir os sinais
 - Estações se associam ao AP para comunicar com os demais

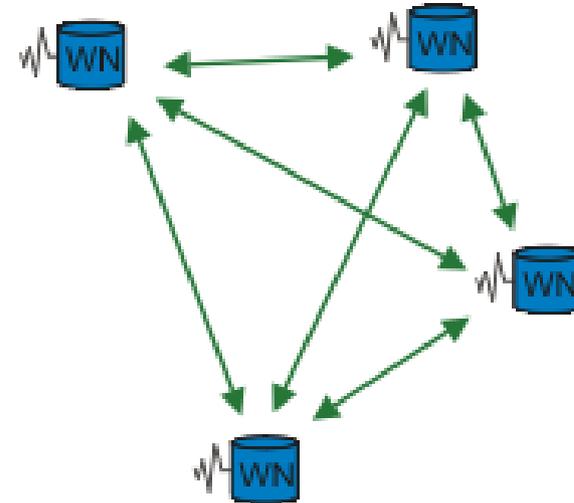


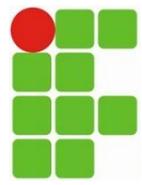
Tipos de redes

Infrastructure Mode:



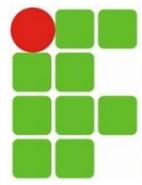
IEEE Ad-hoc Mode:





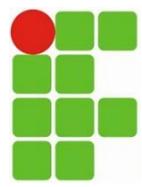
Redes Infra-estrutura

- Conceito de BSA (Basic Service Area)
 - Área em que os dispositivos móveis podem comunicar
- Utiliza dispositivos centralizadores
 - Access Points, intermedeiam as comunicações
 - Um AP é análogo a um hub sem fio
- Área coberta por um AP chama-se célula, composta por BSSs
 - Basic Service Set é o conjunto de serviços básicos de uma célula
 - Um conjunto de BSS chama-se ESS (Extended)
- Em uma rede ESS, é comum o acontecimento de roaming

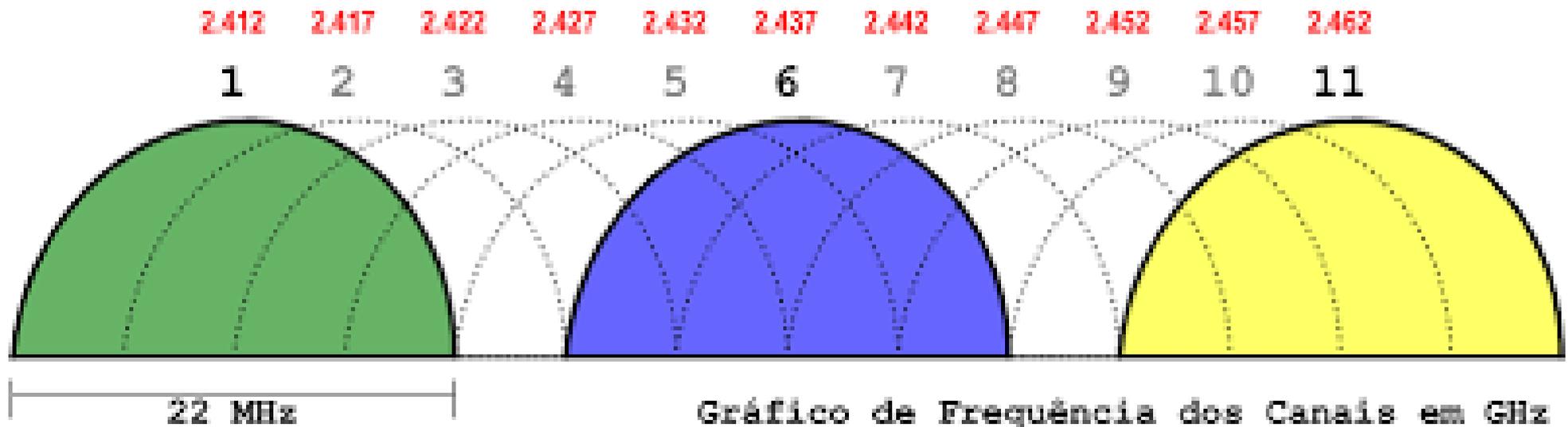


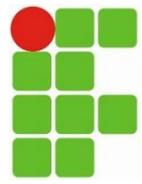
Redes Ad-hoc

- Não há controle centralizado
- Análogo à ligação direta de dois computadores com cabo *crossover*
- Máquinas podem se comunicar livremente, desde que dentro do alcance de sinal
- Alcance do sinal é menor
 - Antenas dos dispositivos é menos potente
- Usado apenas em redes de pequeno porte
- Conceito de IBSS (Independent)
 - BSS sem um AP
 - Uma das estações pode assumir a função de coordenação



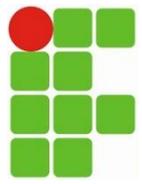
802.11 – Canais





Identificação da rede

- Service Set Identifier (SSID)
- Nome da rede, com caracteres alfanuméricos e tamanho máximo de 32 caracteres
- Uma rede possui um único SSID
 - Mesmo que possua mais de um AP (ESS)
- Basic Service Set Identifier (BSSID)
 - Identificador da célula.
 - Valor é o MAC ad. do AP
 - Composto por 12 algarismos Hexa
 - Um BSS possui um único BSSID

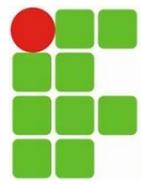


MÉTODOS DE ACESSO AO MEIO



Métodos de acesso ao meio

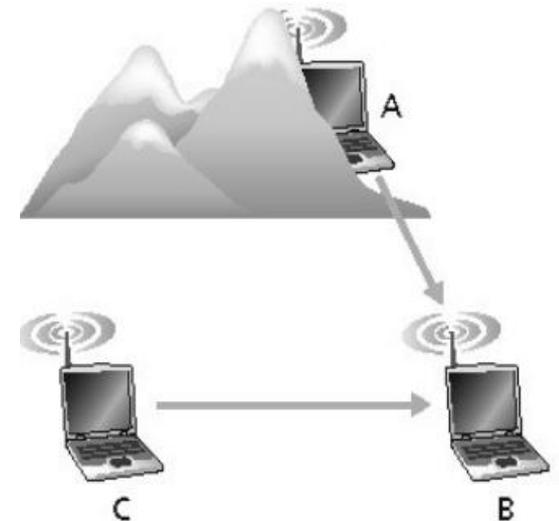
- **CSMA/CA (Carrier sense multiple access with collision avoidance - Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão)**
 - Dispositivo “escuta” o meio e, se o meio estiver livre por tempo determinado (DIFS) ; transmite; senão backoff.
 - Tempo de backoff é randômico, para evitar colisões
 - Uso de ACK para verificar entrega



Métodos de acesso ao meio

- **Terminal escondido**

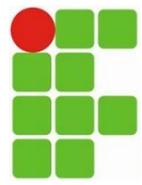
- Mecanismo de reserva para evitar terminal escondido.
- O problema é ilustrado com três terminais
- A e C não se encontram ao alcance um do outro, pelo que não se conseguem escutar mutuamente, mas estão ambos ao alcance de B
- Caso A e C transmitam para B, ocorrerá uma colisão
- O terminal A está “escondido” (em relação a C), se estiver ao alcance rádio do receptor (neste caso B) mas não de outro emissor (neste caso C), o mesmo se passando com C em relação a A





Métodos de acesso ao meio

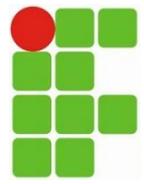
- **O problema é parcialmente resolvido com recurso a tramas de controlo RTS (Request to Send) e CTS (Clear to Send), sendo este mecanismo opcional.**
 - O emissor (A) e o receptor (B) trocam tramas RTS e CTS antes de A transmitir a trama de dados (podem naturalmente ocorrer colisões durante este processo).
 - Ao escutar a trama CTS enviada por B, C não iniciará uma transmissão (a menos que já o tenha feito)



Métodos de acesso ao meio

DCF (Distributed Coordination Function)

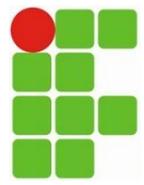
1. As estações competem pelo entre si pelo meio
2. A DCF trabalha semelhantemente a função CSMA/CD da tecnologia de rede local cabeada (Padrão Ethernet 802.3)
3. Uso de CSMA/CA
4. A estação sente o meio para determinar se outra estação já está transmitindo.
5. Se o meio estiver livre há pelo menos um intervalo de tempo DIFS, a estação transmite seu quadro imediatamente, caso contrário, ela aguarda DIFS novamente, cada estação escolhe um tempo aleatório de retirada (Back-off time) e atrasa esse tempo aleatório sua tentativa de acesso ao meio. Se ao terminar seu tempo de back-off a estação encontrar o meio livre, ela transmitirá.
6. Após cada transmissão com ou sem colisão, a rede fica em um modo onde as estações só podem começar a transmitir em intervalos de tempo a elas pré-alocados.
7. Ao concluir uma transmissão, as estações alocadas ao primeiro intervalo têm o direito de transmitir. Se não o fazem, o direito passa as estações alocadas ao segundo intervalo, e assim sucessivamente até que ocorra uma transmissão, quando todo o processo reinicia.
8. Se todos os intervalos não são utilizados, a rede entra então no estado onde o CSMA comum é usado para acesso, podendo dessa forma ocorrer colisões.



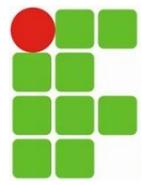
Métodos de acesso ao meio

PCF (Point Coordination Function)

- É Opcional;
- AP escuta estações em turnos para verificar se há frames;
- Elimina Colisões;
- Coexiste com DCF em uma rede;



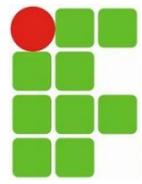
TIPOS DE MODULAÇÃO



Spread Spectrum

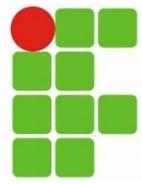
Para lembrar:

- SS é um **tipo de modulação** que espalha a transmissão de dados por toda a frequência disponível
- Esse espalhamento traz maiores resistências a
 - Interceptação
 - Ruído
 - Interferência
- Vários usuários podem compartilhar a mesma banda
 - Telefonia Celular



FHSS

- Frequency Hopping Spread Spectrum
- Transmissão ocorre em várias frequências pseudo aleatórias
- Transmissor e receptor mudam de frequência de forma sincronizada
 - Usa 79 canais separados entre 2.402 e 2.480 Mhz
 - Muda o canal a cada 0.1s
 - Problemas em certa frequência afetam poucos bits
- Muitas redes podem ocupar a mesma área
- Usa menos energia e é mais barato do que o DSSS



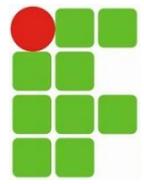
DSSS

- Sinal é modulado com uma sequência de 11 bits (código de spreading)
- Usado por 802.11b
- Um pouco mais suscetível a ruído do que o FHSS
- Permite apenas três redes na mesma área (canais)



OFDM - Spread Spectrum Orthogonal Frequency-Division Multiplexing

- Usada pelos padrões mais rápidos (802.11 a/g)
- Tipo de FDM que divide uma única transmissão em múltiplos sinais com menor ocupação do espectro de frequência
 - Sinal possui maior resistência a interferência
- Utiliza todos os canais **ao mesmo tempo**
 - Trabalha com várias “subportadoras” moduladas de forma convencional (QAM ou PSK)
 - Nos demais métodos, ele alterna o uso dos canais
 - Vários pequenos canais ao invés de um grande canal
 - Melhor imunidade à interferência

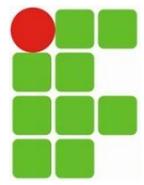


ANTENAS



Antenas

- Omnidirecional
 - Transmitem em todas as direções (360°)
 - Ex. WiFi
- Setorial
 - Transmitem em uma única direção, mas com ângulo de irradiação aberto
 - Ex. Celulares
- Direcional
 - Transmitem em uma única direção, com ângulo de irradiação fechado
 - Ex. Parabólicas



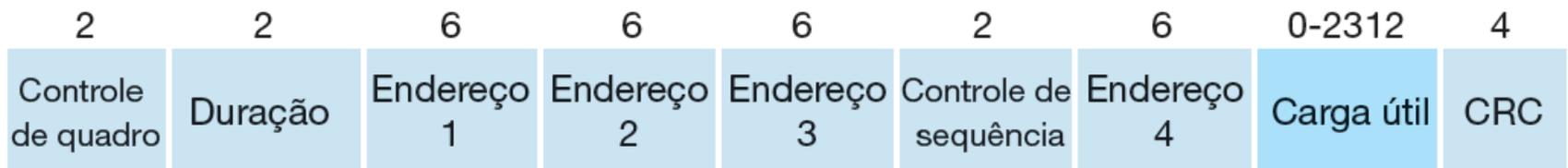
O QUADRO



O quadro IEEE 802.11

- O quadro 802.11

Quadro (os números indicam o comprimento do campo em bytes):



Detalhamento do campo de controle do quadro (os números indicam o comprimento do campo em bits):

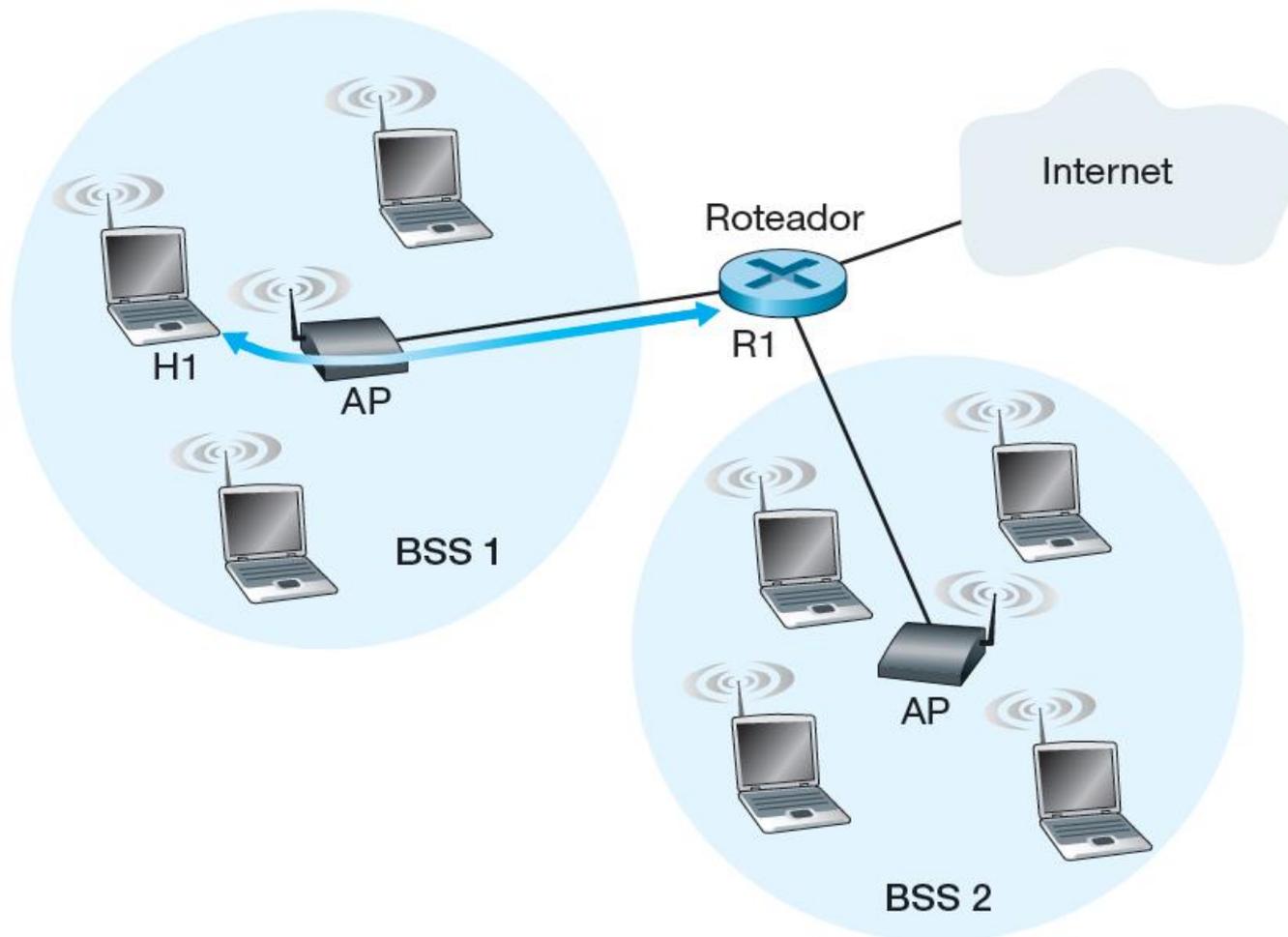


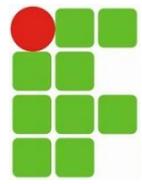


O quadro IEEE 802.11

- No coração do quadro está a carga útil, que consiste, tipicamente, em um datagrama IP ou em um pacote ARP.
- Talvez a diferença mais marcante no quadro 802.11 é que ele tem quatro campos de endereço e cada um pode conter um endereço MAC de 6 bytes.
- A figura a seguir mostra a utilização de campos de endereço em quadros 802.11: movendo um quadro entre H1 e R1.

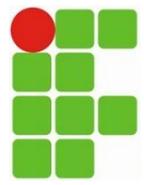
O quadro IEEE 802.11



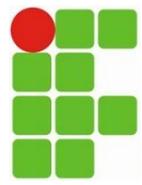


O quadro IEEE 802.11

- Os campos *tipo* e *subtipo* são usados para distinguir os quadros de associação, RTS, CTS, ACK e de dados.
- Os campos *de* e *para* são usados para definir os significados dos diferentes campos de endereço.
- O campo *WEP* (*Wireless Equivalent Privacy*) indica se está sendo ou não utilizada criptografia.

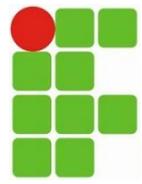


SEGURANÇA



Segurança Wi-fi

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



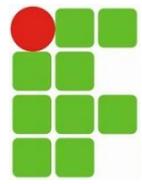
WEP

- WEP (Wired Equivalency Privacy)
 - Princípio: chaves simétricas distribuídas
 - Proposta: proteção contra interceptação (autenticidade; confidencialidade e integridade)
- Autenticação na camada de enlace
 - não é fim-a-fim
- Modos
 - Open system – modo default
 - Shared key – chave wep para mecanismo challeng-response
- Chave RC4 – 40 bits



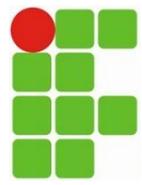
WEP - restrições

- Somente o cliente é autenticado
 - Aps falsos podem enganar os clientes
- Integridade dos dados não é garantida
 - CRC32 é função linear e o conteúdo da mensagem pode ser alterado sem conhecimento prévio da chave Wep
- RC4 possui falhas na geração
 - Geração da sequência quando é conhecida uma parte da chave
- Ferramentas de domínio público fazem descoberta de chaves Wep
 - Aircrack-ng
 - WEPCrack



WPA

- Wi-Fi Protected Access
- Especificado por um grupo de fabricantes chamado “Wi-Fi Alliance”
- Criptografia: TKIP
 - Temporal Key Integrity Protocol – chaves Wep mudam de tempos em tempos
 - Chave possui 128 bits
 - Chaves de sessão dinâmicas: Por usuário, por sessão ou até por pacote
- Autenticação
 - 802.1x e EAP (usuários corporativos)
 - Passphrase (Usuário doméstico)



WPA2

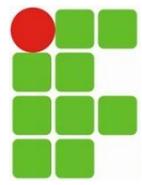
- WPA baseava-se em um draft da norma 802.11i
- Quando a norma foi finalizada, criou algumas melhorias e foi chamada de WPA2
 - Também conhecida por Robust Security Network (RSN)
- Melhorias
 - Mudança na criptografia de TKIP para AES
 - Abandono do RC4, com uso de CCMP
- Requer mais mudanças que o WPA no HW e SW dos equipamentos



Recursos avançados em 802.11

Adaptação da taxa 802.11

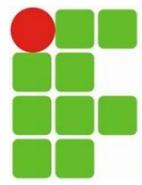
- Algumas execuções de 802.11 possuem uma capacidade de adaptação de taxa que seleciona, de maneira adaptável, a técnica de modulação da camada física sobreposta a ser usada com base em características atuais ou recentes do canal.
- A adaptação da taxa 802.11 e o controle de congestionamento TCP são semelhantes à criança: está sempre exigindo mais e mais de seus pais até eles por fim dizerem “Chega!” e a criança desistir.



Recursos avançados em 802.11

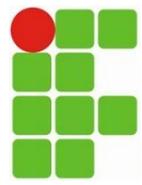
Gerenciamento de energia

- O padrão 802.11 provê capacidades de gerenciamento de energia, permitindo que os nós 802.11 minimizem o tempo de suas funções de:
- percepção,
- transmissão e recebimento, e
- outros circuitos necessários para “funcionar”.



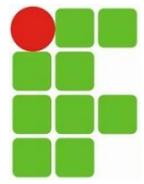
Redes pessoais: Bluetooth e Zigbee

- As camadas de enlace e física do 802.15.1 são baseadas na especificação do **Bluetooth** anterior para redes pessoais.
- Redes 802.15.1 operam na faixa de rádio não licenciada de 2,4 GHz em modo TDM, com intervalos de tempo de $625 \mu s$.
- Redes 802.15.1 são redes *ad hoc*.
- Dispositivos 802.15.1 são primeiro organizados em uma picorrede (piconet: pequena rede) de até oito dispositivos ativos.



Redes pessoais: Bluetooth e Zigbee

- **Zigbee** é voltada para aplicações de menos potência, menor taxa de dados e menor ciclo de trabalho do que Bluetooth.
- Zigbee define taxas de canal de 20, 40, 100 e 250 Kbits/s, dependendo da frequência do canal.
- Os nós em uma rede Zigbee podem ser de dois tipos.
- Os chamados “dispositivos de função reduzida” operam como escravos controlados por um único “dispositivo de função completa”, assim como dispositivos Bluetooth escravos.

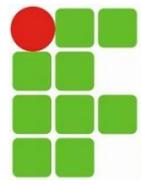


TIPOS DE REDES WIRELESS



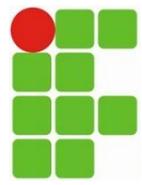
WMAN

- Desafio: Prover acesso banda larga à Internet, sem uso de fios
- Instalação de tecnologias com fio pode ser mais complicada
 - DSL, Cabo, ISDN
- Wireless MAN (WMAN)
 - Conexão wireless para hotspots
 - Acesso internet banda larga para usuários móveis
 - Sucessor do DSL para residências e companhias
 - Backbone wireless



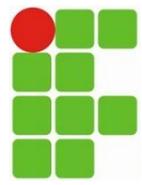
O padrão 802.16

- Especificações de camadas física e de enlace (MAC) na freq. 10 – 66 GHz
- Line-of-sight (LOS) é necessário
 - Pouca ou nenhuma mobilidade
- Usa frequências licenciadas ou não
- Otimizado para comutação por pacotes
- Suporte a QoS
- Largura de banda variável



A família 802.16

- Há muitos variantes (802.16a até m)
 - Algumas variações dos protocolos
 - Outros mecanismos de coexistência e gerência
- 802.16
 - 10-66Ghz; Não móvel; Velocidade 32-134Mbit/s
 - Distância típica – 1.5 até 5km
- 802.16a
 - 2-11Ghz; Não móvel; Velocidade até 75 Mbit/s
 - Distância típica: 7-10km
- 802.16e
 - 5-6Ghz; mobilidade pedestre; Vel. Até 15 Mbit/s
 - Distância típica: 1.5 até 5 km



Comparativo

	802.16	802.16a	802.16e
Frequency range	10 - 66 GHz	2 - 11 GHz	5 - 6 GHz
Transmission	LOS	NLOS	NLOS
Data rate	32 - 134 MBit/s	up to 75 MBit/s	up to 15 MBit/s
Modulation	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM
Mobility	no	no	„pedestrian mobility“
Typical cell size	1.5 - 5 km ; 50 km is maximum size	7 - 10 km; 50 km is maximum size	1.5 - 5 km
Application area	Connection of stationary users of a region	Fast connection of hotspots, Mesh topology	Enhancement by user mobility