Redes sem Fio

Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Redes IEEE802.11

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

IEEE 802.11

A especificação IEEE 802.11 tem como objetivo a definição das camadas física e de enlace de dados do modelo de referência OSI para redes locais sem fio (WLAN).

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

História

- Em 1997 surge o padrão IEEE 802.11. Ele foi especificado para operar na faixa de frequência de 2,4 GHz com taxa de dados de 1 Mbps e 2 Mbps.
- Em 1999, o IEEE publicou os suplementos 802.11a e 802.11b, que estenderam a taxa de transmissão para 54 e 11 Mbps, respectivamente. O 802.11b mantém a operação a 2,4 GHz, enquanto que o 802.11a passa a operar na frequência de 5 GHz.
- Em 2003, o IEEE publicou o 802.11g que opera com taxa de transmissão de 54 Mbps usando a frequência de 2,4 GHz;

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

História

- Em 2004, a especificação 802.11i aumentou consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia;
- Em 2009, o IEEE publicou o 802.11n que opera nas faixas de frequência de 2,4GHz e 5GHz e atingindo velocidades de até 450 Mbps;
- Em 2012, é lançado o IEEE 802.11ac operando na frequência de 5GHz atingindo velocidades de até 1,3 Gbps.

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

Wi-Fi

A especificação IEEE 802.11 original apresentava problemas de interoperabilidade entre fabricantes. Dessa forma, vários fabricantes se juntaram com o objetivo de criar uma aliança sem fins lucrativos para garantir a interoperabilidade entre dispositivos. Essa aliança ficou conhecida como WECA (*Wireless Ethernet Compatibility Alliance*). A organização lançou um certificado chamado Wi-Fi (*Wireless Fidelity*) para garantir que dispositivos de comunicação sem fio estava operante com os outros dispositivos também certificados. Posteriormente, o padrão IEEE 802.11 passou a ser conhecido como de Wi-Fi.

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

Arquitetura

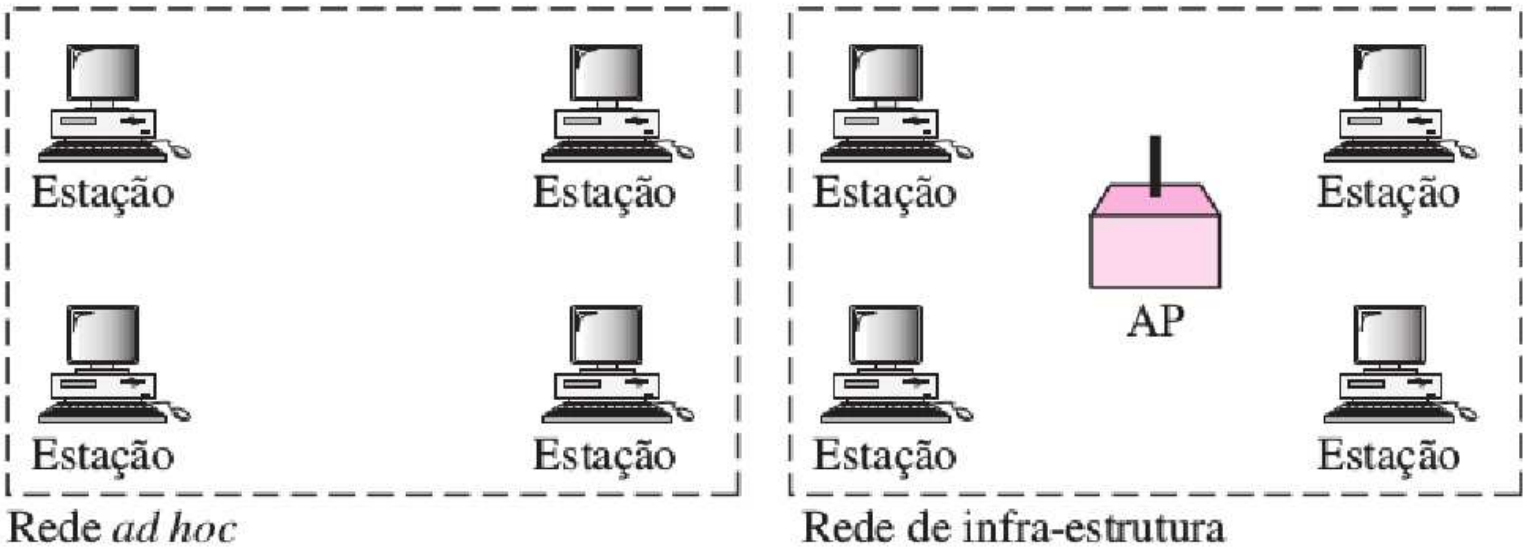
O padrão define dois tipos de serviços:

- BSS (*Basic Service Set*), também chamada de rede infraestruturada, é definido como um conjunto de estações (STAs) que conseguem se comunicar com o auxilio de um ponto de acesso (AP).
- IBSS (Independent BSS), também chamado de *ad hoc*, é uma BSS sem um AP, ou seja, as estações se comunicam diretamente;
- ESS (*Extended Service Set*) é formada por duas ou mais BSSs com APs. Nesse caso, as BSSs são conectadas por meio de um sistema de distribuição que normalmente é uma LAN com fio.

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

Arquitetura – BSS e IBSS

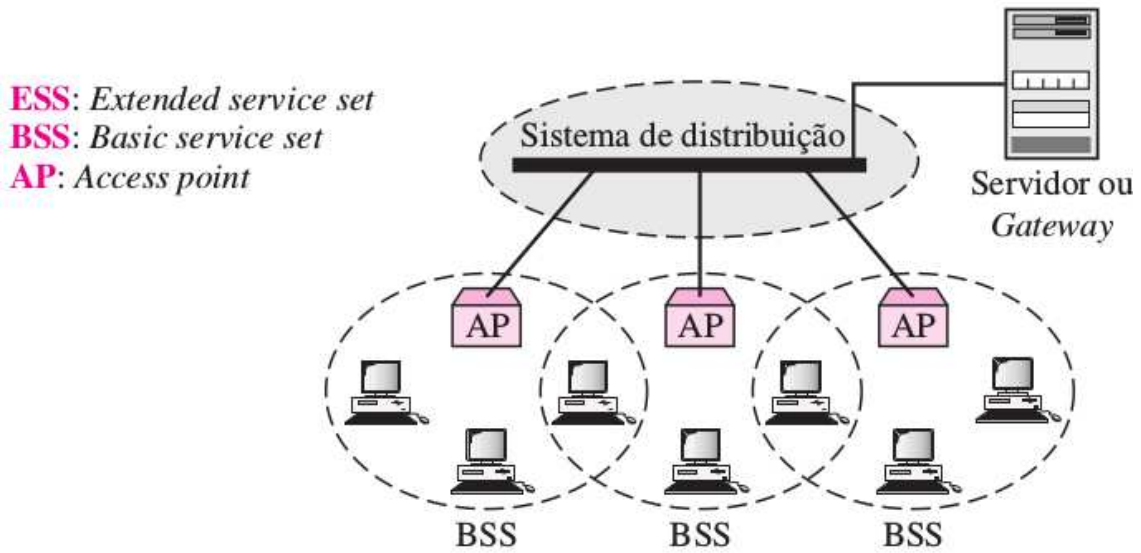
O modo sem infraestrutura (ad hoc) serve para a troca ocasional de informações. O modo com infraestrutura serve para estender uma rede com fio, a comunicação entre um nó da rede sem fio e outro nó qualquer sempre passará pelo AP.



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

Arquitetura – ESS

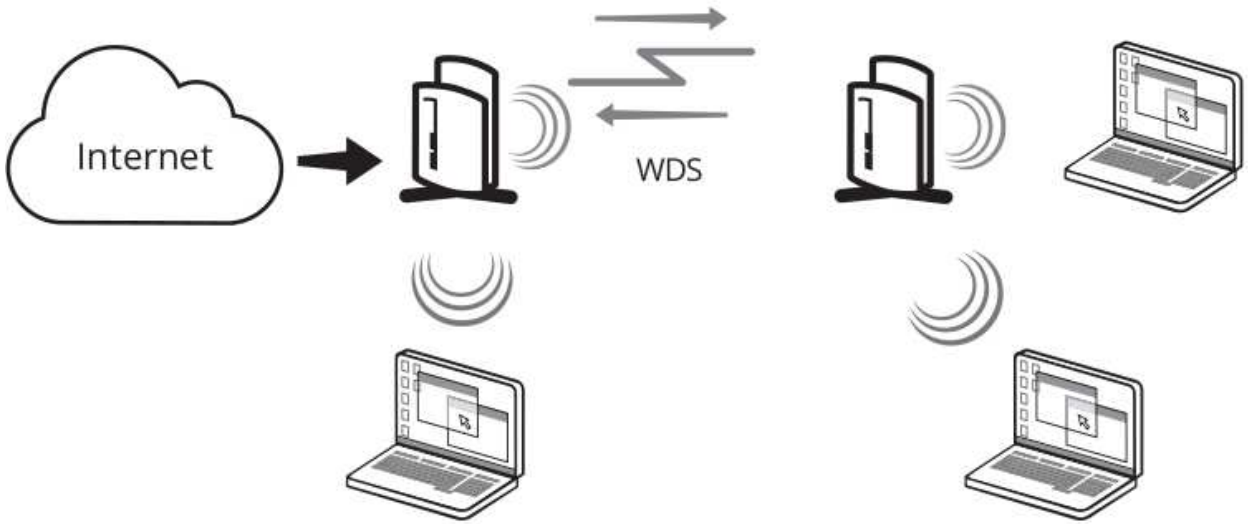
Um único BSS pode não ser suficiente para cobrir uma área extensa, ou pode haver a necessidade de colocar mais APs para servir a mais usuários. Nesse caso, é necessário interligar os BSSs para que estações possam falar entre si através da ESS.



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

Arquitetura – WDS

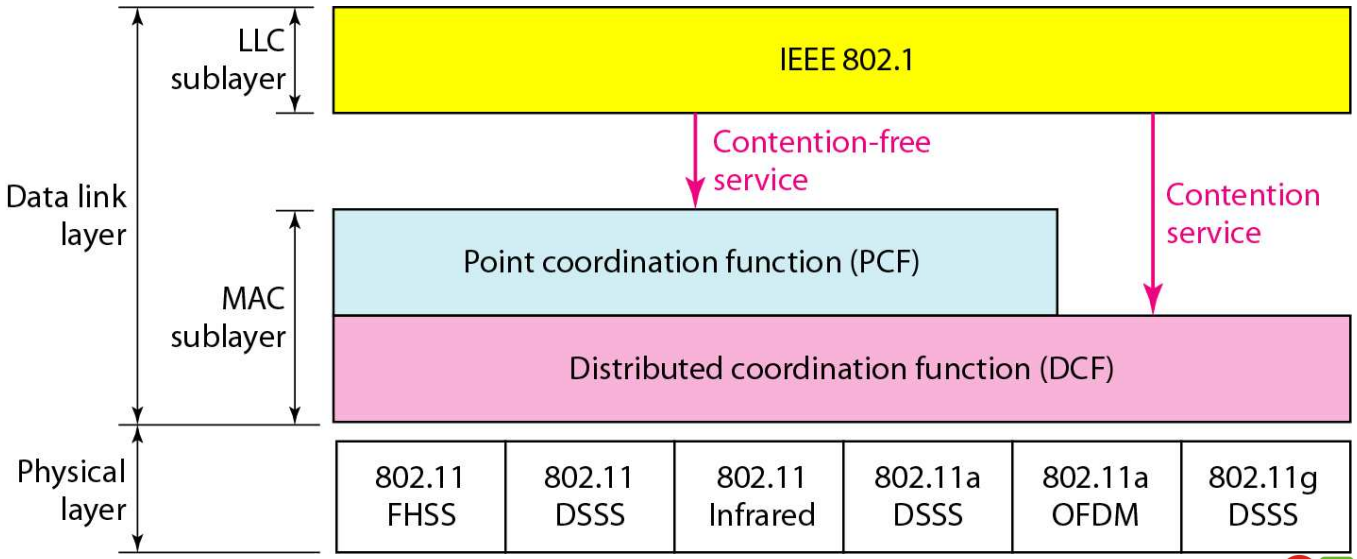
O sistema de distribuição sem fio (Wireless Distribution System - WDS) é uma maneira de interligar BSSs sem usar cabeamento, usando rádio para a interligação dos Aps.



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

IEEE 802.11 – Camadas

O padrão IEEE 802.11 descreve a várias camadas físicas e uma camada de enlace. A camada de enlace é subdividida em subcamada de controle (LLC) e subcamada de acesso (MAC).



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

Camada Física

A camada física é responsável pela codificação, modulação, espalhamento espectral e transmissão dos dados no meio físico. Ao longo de sua evolução, o padrão IEEE 802.11 incorporou uma série de técnicas de modulação e codificação distintas, sendo que as mais importantes:

- 802.11: infravermelho, FHSS (2,4 GHz) e DSSS (2,4 GHz);
- 802.11b: DSSS (2,4 GHz);
- 802.11a: OFDM (5 GHz);
- 802.11g: OFDM com CCK (diversos) (2,4 GHz);
- 802.11n: MIMO-OFDM (2,4 GHz e 5 GHz);
- 802.11ac: MU-MIMO (5 GHz).

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

Faixas ISM

Redes 802.11 utilizam duas faixas do espectro de uso não licenciado, chamadas Industrial, Scientific and Medical (ISM) e, como o nome indica, são reservadas para uso industrial, médico e científico. Ela podem ser usadas por qualquer dispositivo, contanto que a potência transmitida não ultrapasse certos valores legais.

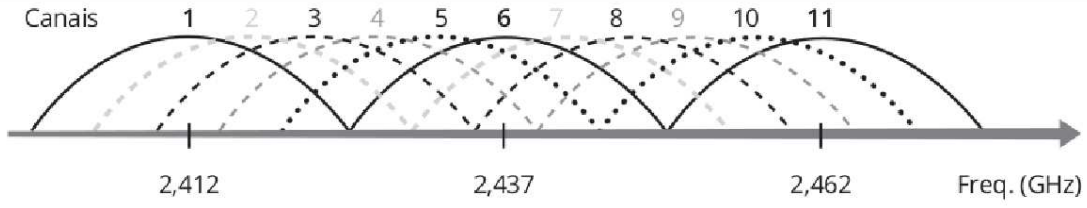
- A primeira é a chamada banda S-ISM, que abrange as frequências entre 2,4 e 2,5 GHz.
- A segunda faixa do espectro utilizada por dispositivos 802.11 é chamada banda C-ISM e abrange as frequências entre 5 e 5,875 GHz.

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

Canais na faixa de 2.4 GHz

Na faixa de 2.4 GHz, cada canal está separado por 5 MHz. Assim, o canal 1 tem a frequência central em 2.412 MHz, enquanto a frequência central do canal 2 é 2.417 MHz (2.412 + 5), no total de 11 canais.

É sugerido o uso dos canais 1, 6 e 11, chamados canais ortogonais ou não interferentes, quando se pretende a instalação de várias redes ou pontos de acesso próximos.

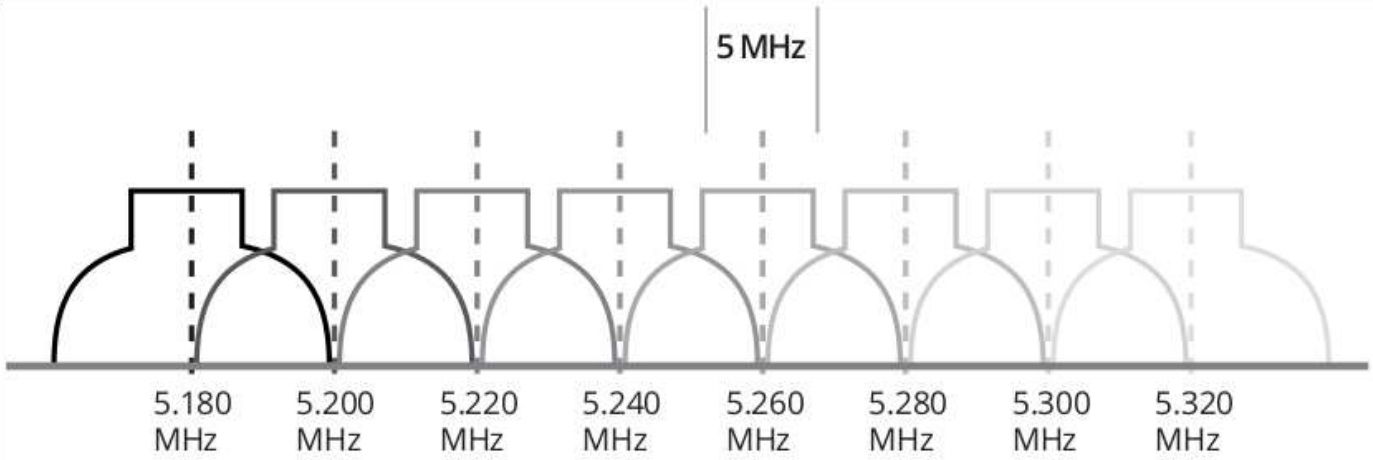


Canal	1	2	3	4	5	6	7	8	9	10	11
Frequencia Central (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462

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

Canais na faixa de 5 GHz

Na faixa de 5 GHz, o padrão 802.11, utilizam canal com 20 MHz de largura, criando no total 8 canais ortogonais alocados entre 5.150 MHz e 5.350 MHz, sendo o primeiro o canal 36 (frequência central 5.180 MHz), seguido pelos canais 40, 44 e assim por diante, até o canal 64.



802.11a Channels

Canal	36	40	44	48	52	56	60	64
Frequencia Central (MHz)	5180	5200	5220	5240	5260	5280	5300	5320

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

IEEE 802.11 Legado

O padrão IEEE 802.11 original incorpora três descrições de camada física, sendo que uma delas, que utiliza luz infravermelha, e suportaria apenas a taxa de 1 Mbps, nunca chegou a ser implementada.

As outras duas PHYs usam sinais de radiofrequência (RF) e a técnica de espalhamento espectral (spread spectrum), Frequency-Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS).

Apresenta taxas de transmissão de 1 e 2 Mbps.

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

IEEE 802.11a

O padrão 802.11a, apesar de oferecer taxas mais altas, não alcançou a mesma do que o 802.11b. As taxas oferecidas pela emenda "a" são: 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. Para isso, utilizada a técnica Orthogonal Frequency-Division Multiplexing (OFDM).

As frequências utilizadas por esse padrão estão entre 5,725 e 5,875 GHz. Nessa faixa de frequência mais alta, o sinal é mais susceptível a perdas de propagação, diminuindo seu alcance em comparação à faixa utilizada pelo IEEE 802.11b.

Toda a banda é dividida em 52 subfaixas, sendo 48 para dados e 4 para controle. A modulação é a PSK (18 Mbps) e QAM (54 Mbps).

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

IEEE 802.11b

Uma nova proposta de camadas físicas permitiram aumentar o desempenho das redes sem fio. Trouxe a técnica de modulação DSSS com taxa de 5.5 Mbps e uma variante chamada High Rate Direct Spread Spectrum (HR/DSSS) foi empregada para alcançar taxas de 11 Mbps. Opera na faixa de 2,4 GHz.

A modulação é a BPSK (1 Mbps), QPSK (2Mbps), BPSK com CCK de 4 bits (5,5 Mbps) e QPSK com CCK de 8 bits (11 Mbps).

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

IEEE 802.11g

Sua grande vantagem foi elevar as taxas de transmissão até o patamar de 54 Mbps utilizando a codificação OFDM na faixa de frequências ISM de 2,4 GHz.. A rigor, o IEEE 802.11g oferece um conjunto de especificações de camada física agrupadas sobre o que se convencionou chamar Extended-Rate PHY (ERP): ERP-DSSS e ERP-CCK (1, 2, 5,5 e 11 Mbps) e ERP-OFDM (6, 9, 12, 18, 24, 36, 48 e 54 Mbps).

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

IEEE 802.11n

Alcança taxas de transmissão de 600 Mbps (HT-MIMO-OFDM com modulação 64-QAM) incluindo o uso de até quatro antenas simultaneamente (chamada de multiplexação espacial, que permite a transmissão de informações independentes em cada antena de transmissão), o aumento da largura do canal (para 40 MHz) e a possibilidade de agregação de quadros

MIMO usa múltiplas antenas no transmissor e receptor para aumentar a sensibilidade do sistema, através de um mecanismo chamado de "diversidade" e outro chamado de "multiplexação espacial".

Opera nas faixas de 2,4 GHz e 5 GHz.

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

IEEE 802.11ac

Poderá alcança taxas de transmissão de até 6,77 Gbit/s (MU-MIMO com 8 antenas e modulação 256-QAM). Também aumenta da largura do canal (para 160 MHz) e a possibilidade de agregação de quadros.

Opera nas faixas de 5 GHz.

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

Camada de Enlace

O padrão 802 define duas subcamadas:

- Subcamada MAC: controle de acesso ao meio, de forma que a transmissão não sofra interferência das outras estações que também disputam o meio.
- Subcamada LLC: serviços de endereçamento, reconhecimento de quadros, controle de erros, controle de fluxo e interface para camada superior.

O LLC provê um protocolo único para o controle do enlace de dados de todas as LANs IEEE. Enquanto que, a subcamada MAC é específico para os diferentes tipos de LANs.

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

Subcamada MAC

O padrão IEEE 802.11 estabelece duas subcamadas MAC:

- *Distributed Coordination Function* (DCF): usa o CSMA/CA como método de acesso ao meio físico;
- *Point Coordination Function* (PCF): implementado em redes de infra-estrutura, utiliza o método de acesso centralizado por meio de *polling*, livre de contenção.

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

IEEE 802.11 – Subcamada DCF

O *Distributed Coordination Function* (DCF) usa o CSMA/CA modificado como método de acesso ao meio. A decisão de transmitir é tomada em cada estação, há possibilidade de colisão e pode ser utilizada tanto em redes com infraestrutura quanto *ad-hoc*. O CSMA/CA funciona da seguinte forma:

1. Antes de transmitir, a estação "escuta" o meio usando uma estratégia de persistência com back-off (tentativa);
2. Após constatar que o canal está livre, a estação espera um período DIFS (*Distributed Interface Space*). Em seguida, envia um quadro de controle RTS (*Request to Send*);

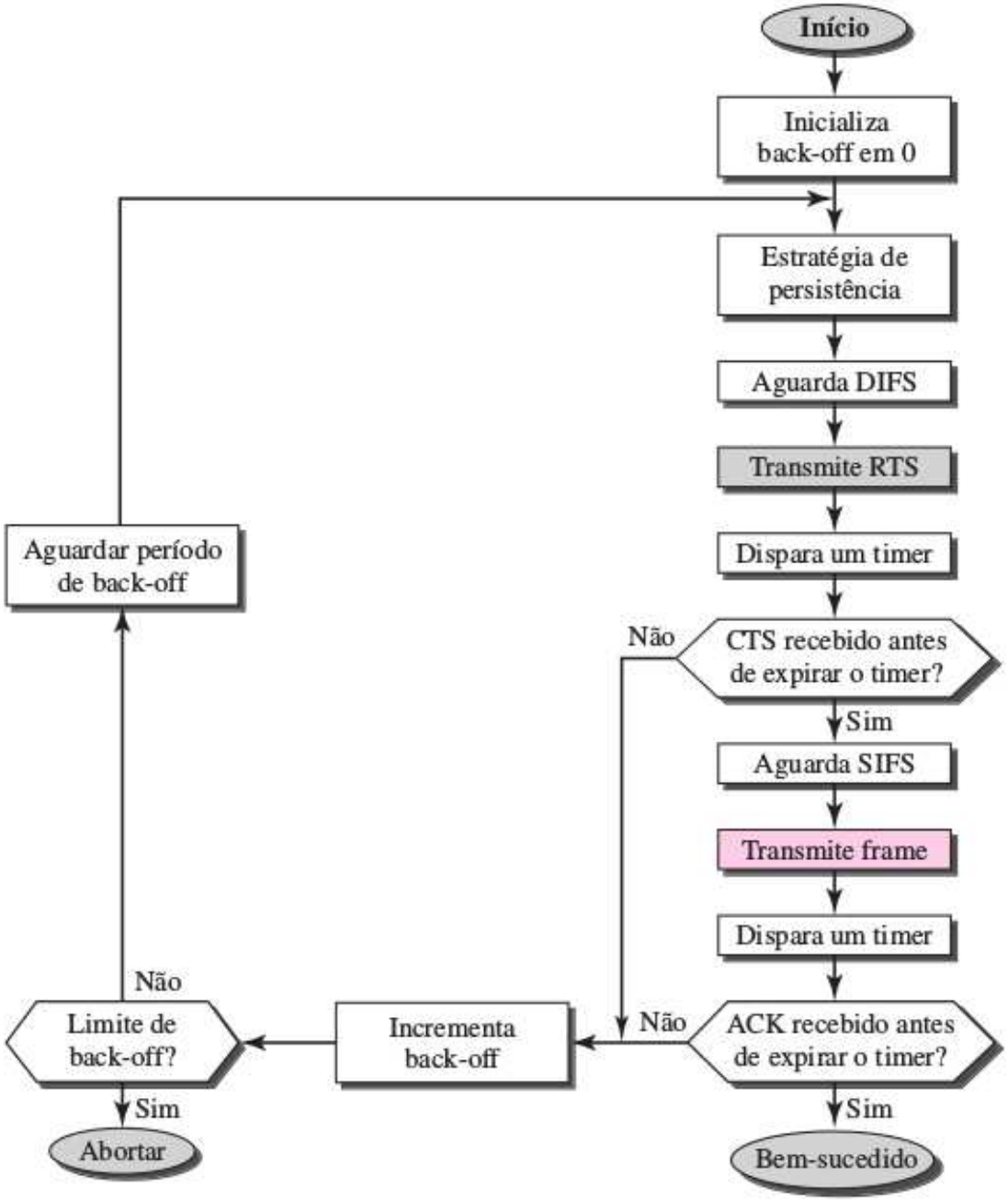
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IEEE 802.11 – Subcamada DCF

3. Após receber o RTS, a estação de destino envia um *frame* de controle CTS (*Clear to Send*), para a estação de origem;
4. A estação de origem envia os frames de dados após aguardar um período SIFS (*Short Interframe Space)*;
5. A estação de destino, envia um ACK (confirmação) para indicar que o quadro foi recebido com sucesso.
6. Fim da trasmissão.

Caso algum erro, não receber o CTS ou ACK ou estourar o temporizador, é aumentado o back-off (tentativa), verifica se não estourou o limite de tentativas, espera um tempo e tenta novamente a transmissão.

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



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

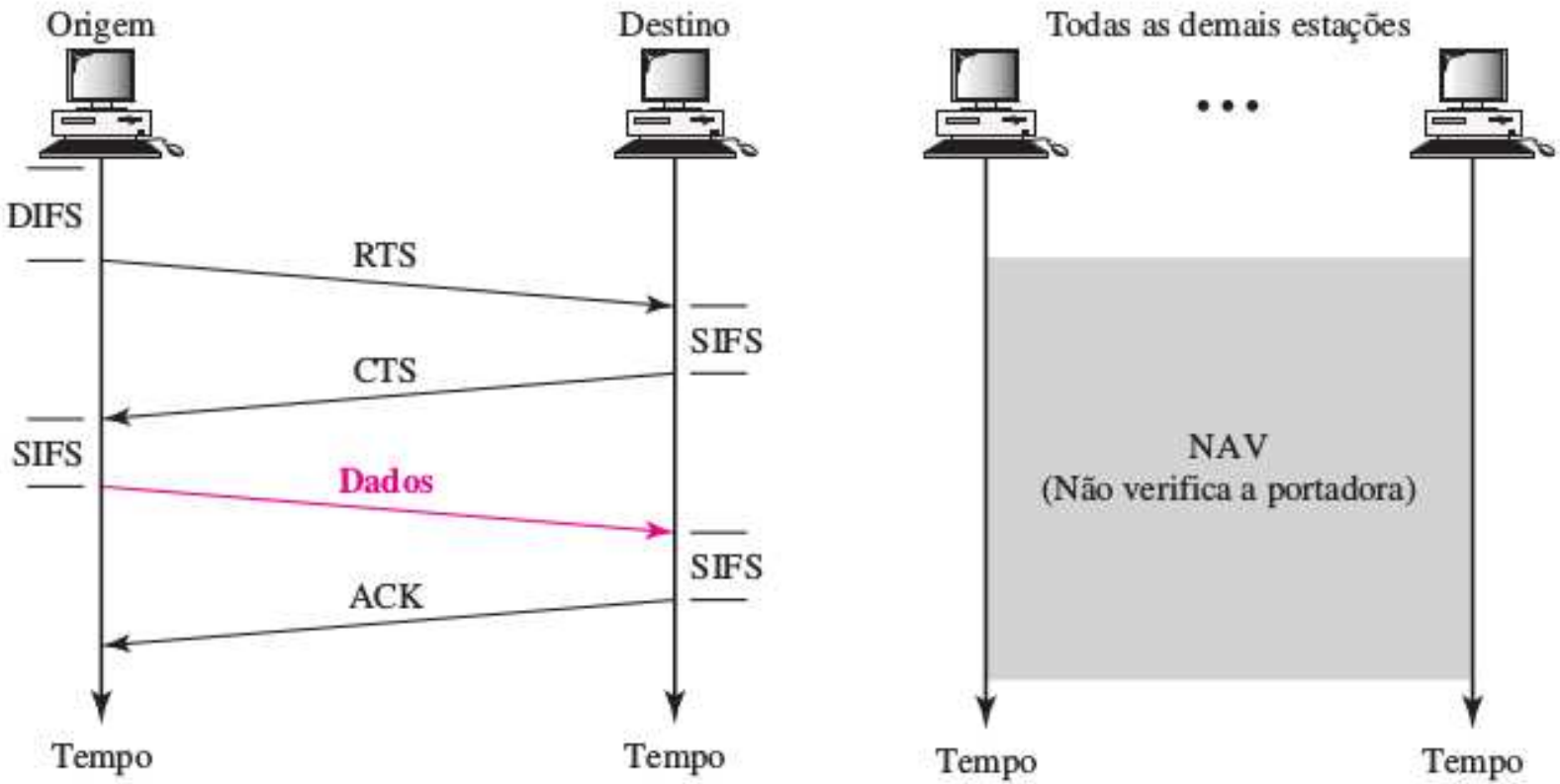
IEEE 802.11 – Subcamada DCF (NAV)

Quando uma estação manda um frame RTS, ela inclui quanto tempo será necessário ocupar o canal (transmissão e confirmação de recebimento pelo destinatário). As estações que estão na rede e não irá receber os dados, inicializam um *timer*, chamado de Network Allocation Vector (NAV), que mostra quanto tempo as estações irão esperar para verificar novamente se o canal está livre.

Quando receber o RTS o receptor envia de volta um quadro CTS. Este quadro também informa o tempo necessário para a transmissão. As estações que não escutarem o RTS, mas escutam o CTS, também irão entrar no mecanismo NAV, e a colisão será evitada.

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

IEEE 802.11 – Subcamada DCF (NAV)



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

IEEE 802.11 – Subcamada PCF

O PCF (*Point Coordination Function*) é um método que só pode ser implementado em rede com infra-estrutura. Ele oferece suporte à transmissão sensíveis ao atraso, como voz e vídeo. O PCF é implementado com um controle centralizado (pelo AP) por meio de *polling*, dessa forma, não existe a possibilidade de colisão. O AP faz varredura (*polling*) em todas as estações perguntando a cada uma se desejam transmitir.

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

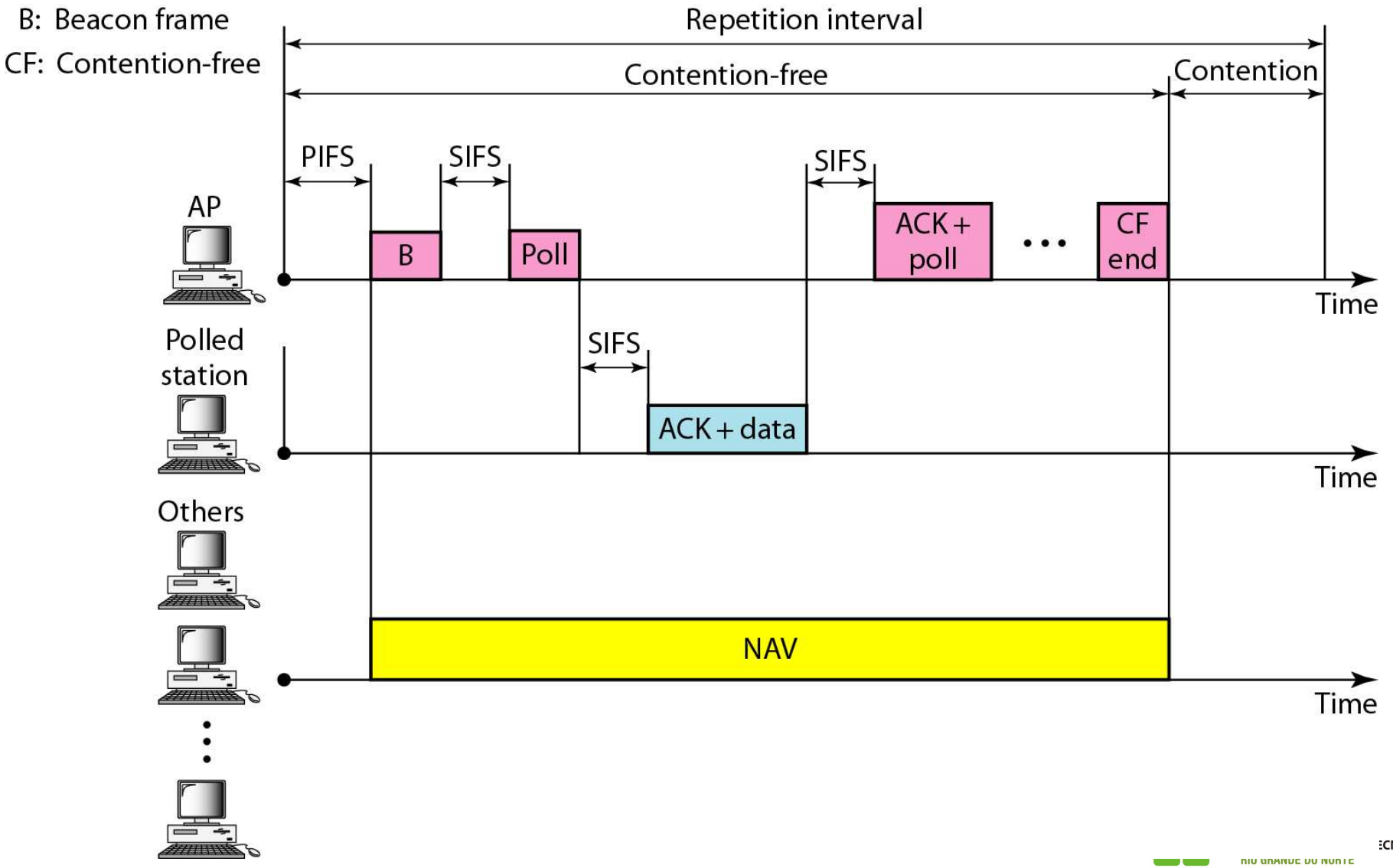
IEEE 802.11 – Subcamada PCF

O PCF é implementado em conjunto com o DCF (através de intervalos de repetição), entretanto o PCF tem prioridade. Essa prioridade é feita através de temporizadores (PIFS e SIFS). O SIFS é o mesmo que o do PCF, mas o PIFS é mais curto.

No intervalo de repetição, inicia com uma quadro de controle **beacon** (sinalização). O AP pode enviar um frame de pool, receber dados, transmitir ACKs. Ao final do período de contenção (PCF), o AP envia um quadro CF, informando o fim do PCF. Agora as demais estações baseadas em DCF podem utilizar o meio de transmissão.

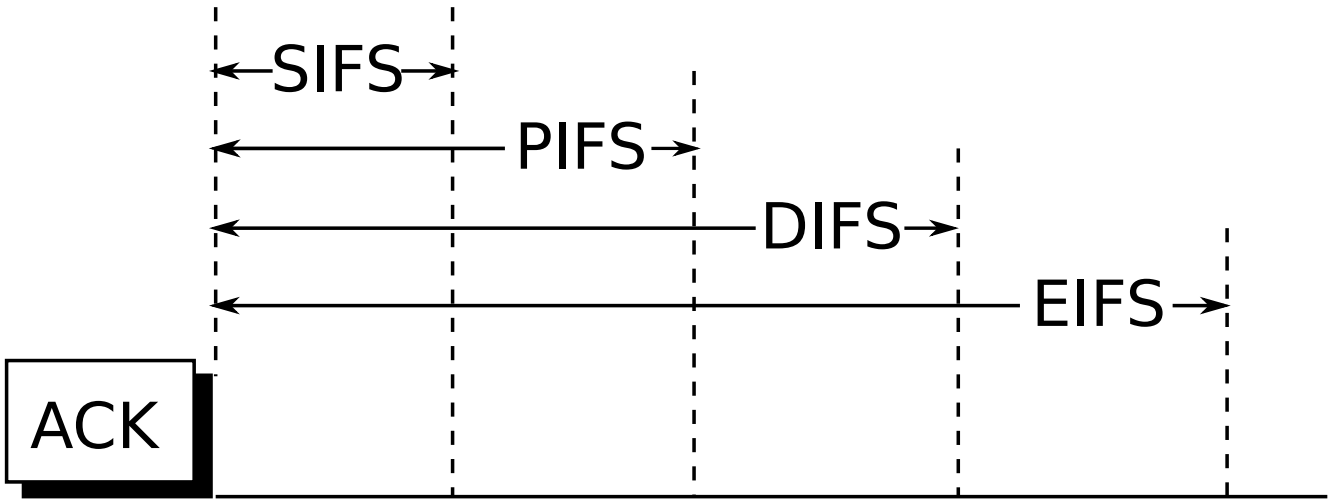
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IEEE 802.11 – Subcamada PCF



IEEE 802.11 - PCF e DCF

Os quatro intervalos entre *frames* estão representados na figura:

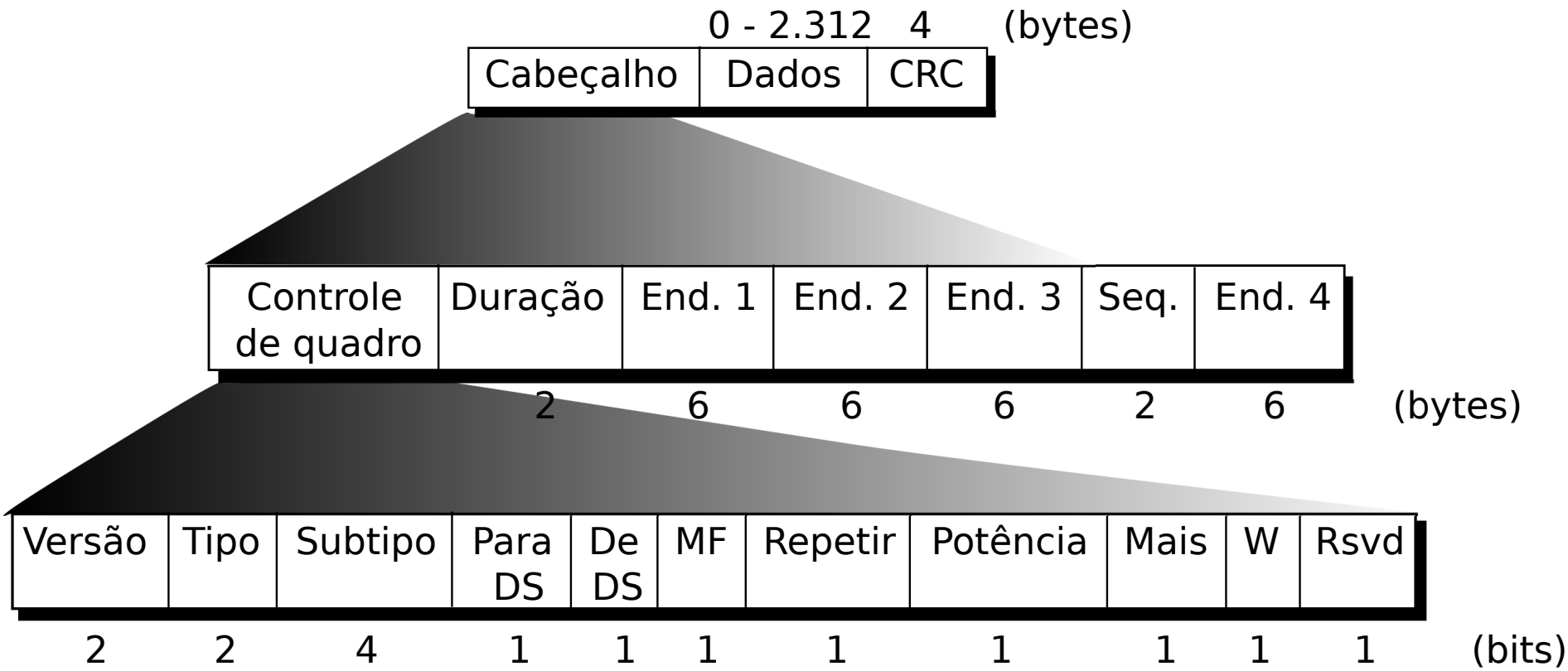


IEEE 802.11 - Temporização

- SIFS (*Short InterFrame Spacing*): é usado para permitir que as partes de um único diálogo tenham a chance de transmitir primeiro. Por exemplo, permite ao receptor enviar um CTS, a fim de responder a um RTS, ou ACK relativo a um dado;
- PIFS (*PCF InterFrame Spacing*): permite ao AP enviar um quadro *beacon* ou um quadro de *polling*;
- DIFS (*DCF InterFrame Spacing*): qualquer estação poderá tentar adquirir a posse do canal para enviar um novo quadro. O controle de aesso é feito através do CSMA/CA;
- EIFS (*Extended InterFrame Spacing*): é usado por uma estação que tenha acabado de receber um quadro defeituoso ou desconhecido, a fim de informar sobre a presença do quadro defeituoso.

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

IEEE 802.11 – Quadro



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

IEEE 802.11 - Estrutura do *Frame*

- Controle de quadro:
  - Versão: define a versão atual do protocolo (atualmemte é 0);
  - Tipo: define o tipo da informação: 00 (gerenciamento), 01 (controle), 10 (dados) e 11 (reservado);
  - Subtipo: define o subtipo para cada tipo de *frame*, por exemplo: 1011 (RTS), 1100 (CTS) e 1101 (ACK);
  - Para DS e De DS: define o modo de endereçamento;
  - MF: indica se existem mais fragmentos;
  - Repetir: indica que o frame é de uma retransmissão;
  - Potência: significa que a estação está no modo de gerenciamento de energia;
  - Mais: significa que a estação tem mais dados a serem transmitidos;
  - W: indica que os dados estão criptografados;
  - Rsvd: reservado para uso futuro.

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

IEEE 802.11 - Estrutura do *Frame*

- Duração: define a duração do quadro e da sua confirmação. Este campo é usado no mecanismo de NAV;
- Endereços: depende do valor dos subcampos Para DS e De DS:

Para DS	De DS	End. 1	End. 2	End. 3	End.4
0	0	Destino	Origem	ID da BSS	-
0	1	Destino	AP transmissor	Origem	-
1	0	AP receptor	Origem	Destino	-
1	1	AP receptor	AP transmissor	Destino	Origem

- Seq.: define o número de seqüência do *frame*, ou seja, permite que os fragmentos sejam numerados;
- CRC: 4 bytes para detecção de erros.

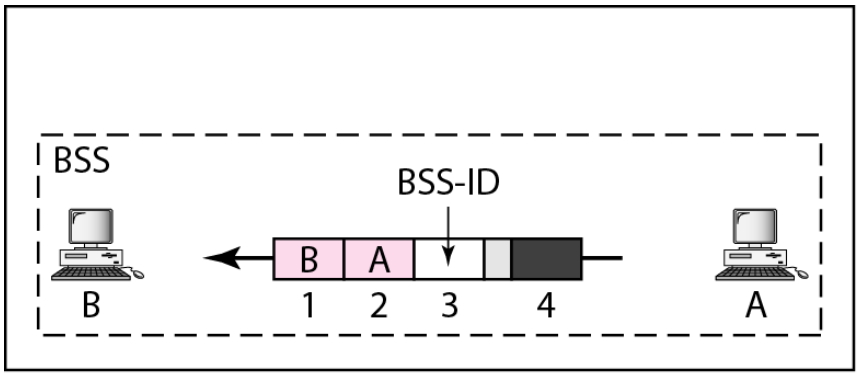
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IEEE 802.11 - Mecanismo de Endereçamento

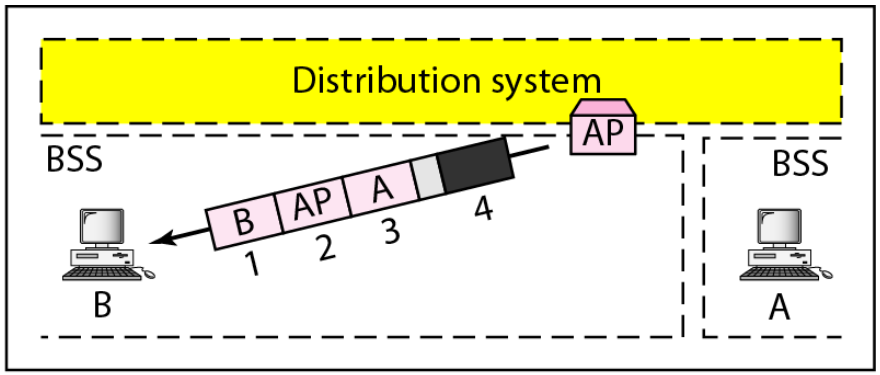
- Caso 1: os subcampos "Para DS = 0" e "De DS = 0". O *frame* vai de uma estação para outra sem passar por um sistema de distribuição;
- Caso 2: os subcampos "Para DS = 0" e "De DS = 1". O *frame* vem de um sistema de distribuição (AP) e indo para uma estação. O endereço 3 contém o endereço da estação emissora original do *frame*;
- Caso 3: os subcampos "Para DS = 1" e "De DS = 0". O *frame* está indo para um sistema de distribuição (AP) e foi originado por uma estação. O endereço 3 contém o endereço do destino final do *frame*;
- Caso 4: os subcampos "Para DS = 1" e "De DS = 1". Usado quando o sitema de distribuição também é *wireless*. O *frame* vai de um AP para outro AP. Os endereços irão definir o emissor original, o destino final e os dois APs intermediários.

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

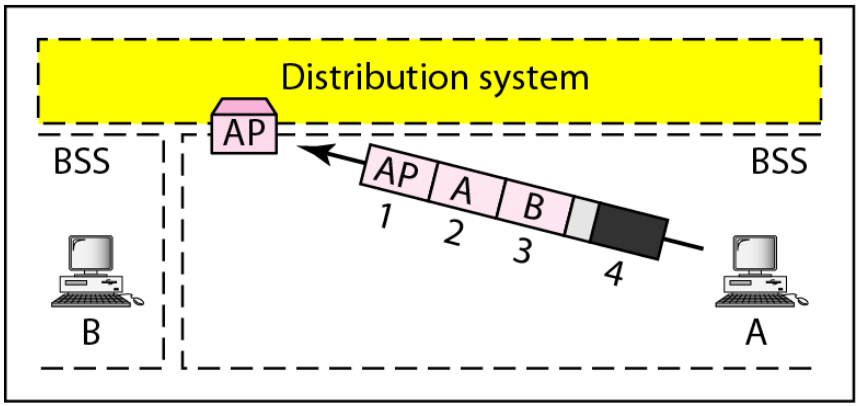
IEEE 802.11 - Mecanismo de Endereçamento



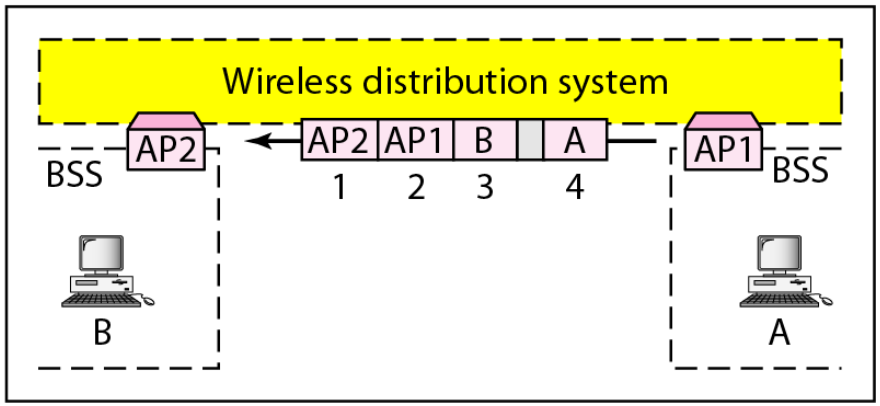
a. Case 1



b. Case 2



c. Case 3



d. Case 4

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

IEEE 802.11 - Associação

O processo de associar um computador (estação) e a rede (através de um ponto de acesso) tem vários passos:

- Encontrar os pontos de acesso, através de uma varredura;
- Escolher o ponto de acesso desejado;
- Identificar-se na rede;
- Associar-se ao ponto de acesso.

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

IEEE 802.11 - Varredura

O processo de encontrar os pontos de acesso disponíveis é chamado de varredura, porque a estação muda seu canal para descobrir pontos de acesso em todos os canais, varrendo a faixa de frequência destinada ao IEEE 802.11.

A varredura é **ativa** se a estação envia um pacote especial (**probe request**) para identificar a existência de redes nas proximidades do usuário, ou **passiva**, se a estação apenas escuta pacotes especiais enviados pelos pontos de acesso (**beacons**)

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

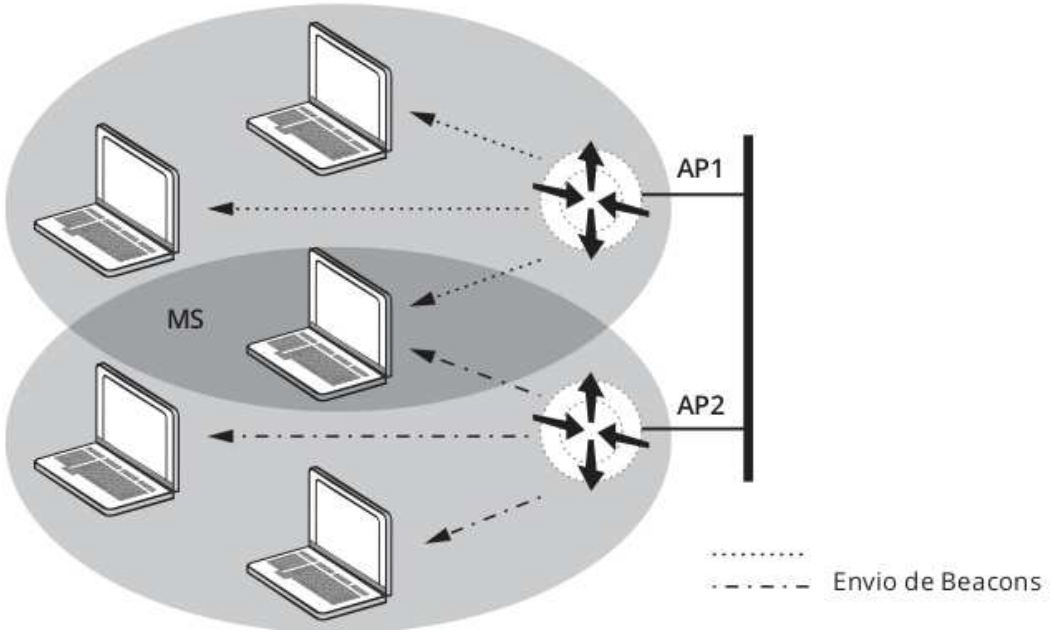
IEEE 802.11 - Varredura Passiva

A varredura passiva refere-se ao processo de procurar por beacons em cada canal. Estes beacons são enviados pelos APs, ou estações (no caso de redes ad-hoc), para que estações obtenham informações sobre as redes disponíveis (como o valor do SSID da rede). A estação fazendo a varredura tenta, então, se associar com o BSS utilizando o SSID e outras informações encontradas.

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

IEEE 802.11 - Beacon

Beacons são quadros enviados periodicamente pelos APs para avisar de sua presença e passar algumas informações necessárias para as estações que podem querer se associar a eles, por exemplo, o nome (SSID) da rede e o método de segurança (WEP, WPA) usado pela rede, ou indica se a rede é aberta.



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

IEEE 802.11 - Varredura Ativa

Na varredura ativa, a estação envia um quadro do tipo probe request. Esse mecanismo ativo é utilizado pelas estações clientes para assegurar a presença de uma rede com a qual desejem se associar. Esse quadro costuma conter o valor do SSID requerido pela estação cliente. Se o SSID for vazio, todos os pontos de acesso que ouvirem o probe request responderão.

Todos os APs que recebem um probe request com parâmetros compatíveis respondem com um probe response. Este tem campos similares do quadro de beacon, que permite que uma estação comece o processo de associação.

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

IEEE 802.11 - Autenticação

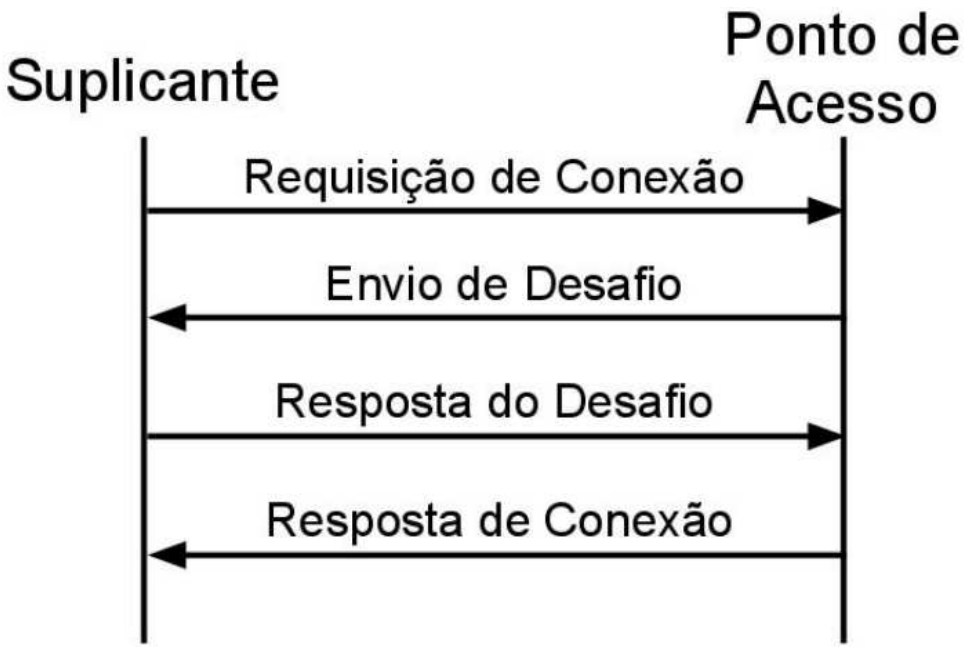
É a primeira etapa para conectar na rede. A autenticação requer que um dispositivo móvel (estação) estabeleça sua identidade com um ponto de acesso (AP). O padrão 802.11 define dois tipos de autenticação:

- Sistema aberto: sem uma chave compartilhada ou senha;
- Chave compartilhada: com uma chave compartilhada ou senha, é definida manualmente no dispositivo móvel e no AP. Vários tipos de autenticação de chave compartilhada estão disponíveis, por exemplo, WEP, WPA e WPA2.

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

IEEE 802.11 - Autenticação

A autenticação de chave compartilhada, utilizada na criptografia simétrica, faz uso de cifras baseado em desafio/resposta. Nela é enviado um desafio por uma das partes, normalmente um Ponto de Acesso, e o outro devolvê-lo crifrando o desafio com a chave compartilhada.



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

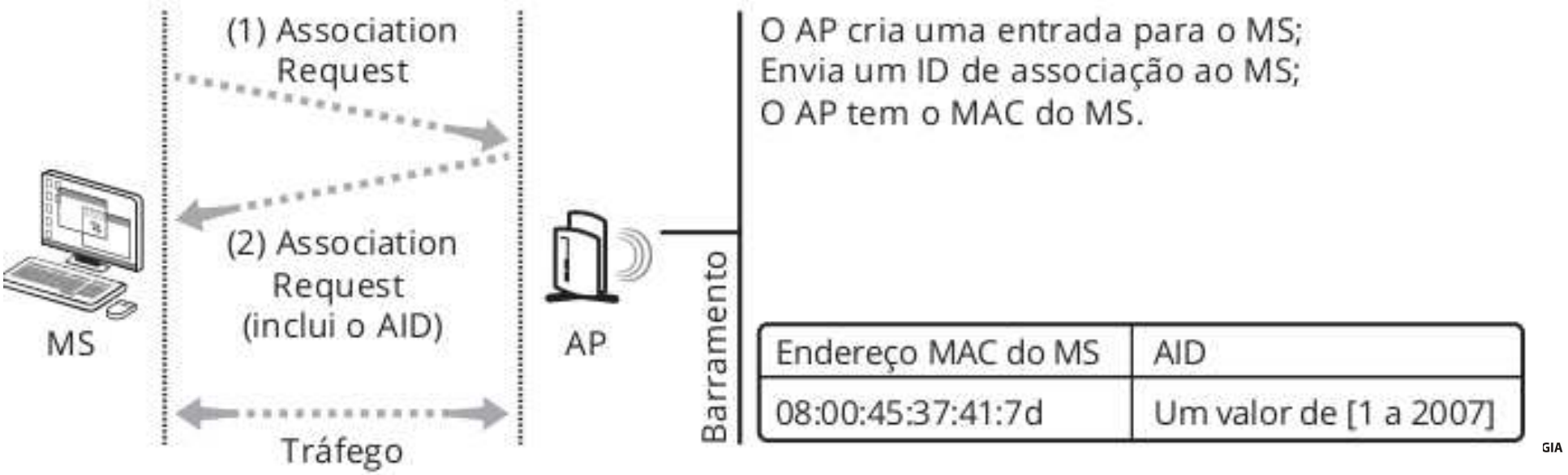
IEEE 802.11 - Associação

Uma vez que a autenticação está completa, os dispositivos móveis podem associar (registrar) com um AP para ganhar o acesso à rede, enviando um quadro de association request. Associação ocorre apenas em redes de infra-estrutura, não no ad-hoc.

A estação móvel pode se associar somente a uma única BSS de cada vez.

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

O primeiro passo é enviar uma requisição de associação (Association Request) ao AP. Recebendo essa requisição e a aceitando, o AP cria uma entrada para o MS e envia uma mensagem ARP na rede cabeada com o endereço MAC da estação, fazendo o registro nos elementos ativos (switches). Em seguida, envia uma identificação (AID) de associação para o MS, através de um quadro association response. Uma vez associados, AP e MS começam a trocar dados.



WEP

O Wired Equivalent Privacy (WEP) é parte do padrão IEEE 802.11 original, de 1997. Ele faz uso de uma senha configurada no ponto de acesso e distribuída para todos os usuários, chamada de (Pre Shared Key - PSK). O algoritmo de criptografia escolhido foi o RC4.

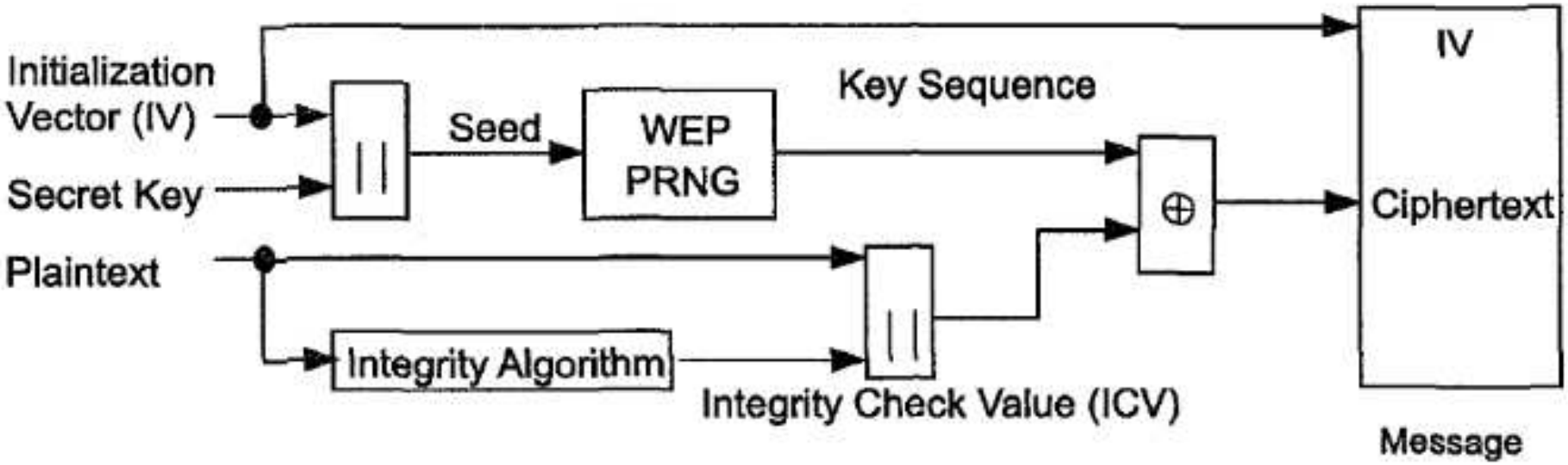
Para garantir que o conteúdo do quadro não foi adulterado, os quadros WEP incorporam um campo Cyclic Redundancy Check (CRC) de 32 bits.

As chaves que podem ser de 64 ou 128 bits, para a codificação dos dados são utilizados 40 ou 104 bits respectivamente, porque em ambos os casos 24 bits são usados no pacote como vetor de iniciação (IV).

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

WEP

A chave é concatenada a um vetor de inicialização (IV) e usada em um gerador de números pseudo-aleatórios (PRNG). É feito um XOR bit a bit da sequência de saída do PRNG com o texto pleno concatenado com um código de integridade (CRC). O texto cifrado resultante é concatenado com o IV mantido às claras (pois ele é necessário para a decriptação) e o resultado é enviado.



WEP

Atualmente é possível extrair a chave (independentemente de qual ela seja) de uma rede sem fio que utiliza o protocolo WEP em menos de cinco minutos.

Chaves de 40 bits são demasiadamente curtas. Mesmo as de 104 bits não são fortes o suficiente.

Outro problemas do WEP está ligada a um elemento chamado Vetor de Inicialização. Esse campo do quadro WEP é transmitido em texto plano (sem criptografia) e consiste nos primeiros 24 bits da chave criptográfica. Revelar uma parte da chave auxilia no processo de criptoanálise (ataque à criptografia).

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

WPA

Uma vez reconhecidas as falhas do WEP, o IEEE estabeleceu o TGi para tornar as redes Wi-Fi mais seguras.

Uma preocupação do comitê foi garantir que os dispositivos Wi-Fi já vendidos ainda pudessem ser aproveitados. A ideia era, portanto, criar melhorias que ainda pudessem ser utilizadas pelos dispositivos lançados com WEP, bastando uma alteração de software.

A retrocompatibilidade implicava em continuar usando a cifragem RC4, que estava presente no hardware das placas Wi-Fi.

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

WPA

Para alcançar maior grau de segurança, o novo protocolo batizado de Temporal Key Integrity Protocol (TKIP) incorporou uma série de mudanças. Em primeiro lugar, o CRC foi substituído por um novo esquema mais forte chamado de Michael Integrity Check (MIC), muito mais eficiente na identificação de adulterações do quadro.

O esquema de uso dos vetores de inicialização também foi alterado para dificultar a criptoanálise e o sistema passou a usar chaves temporárias, derivadas da chave original, e diferentes para cada quadro transmitido.

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

WPA

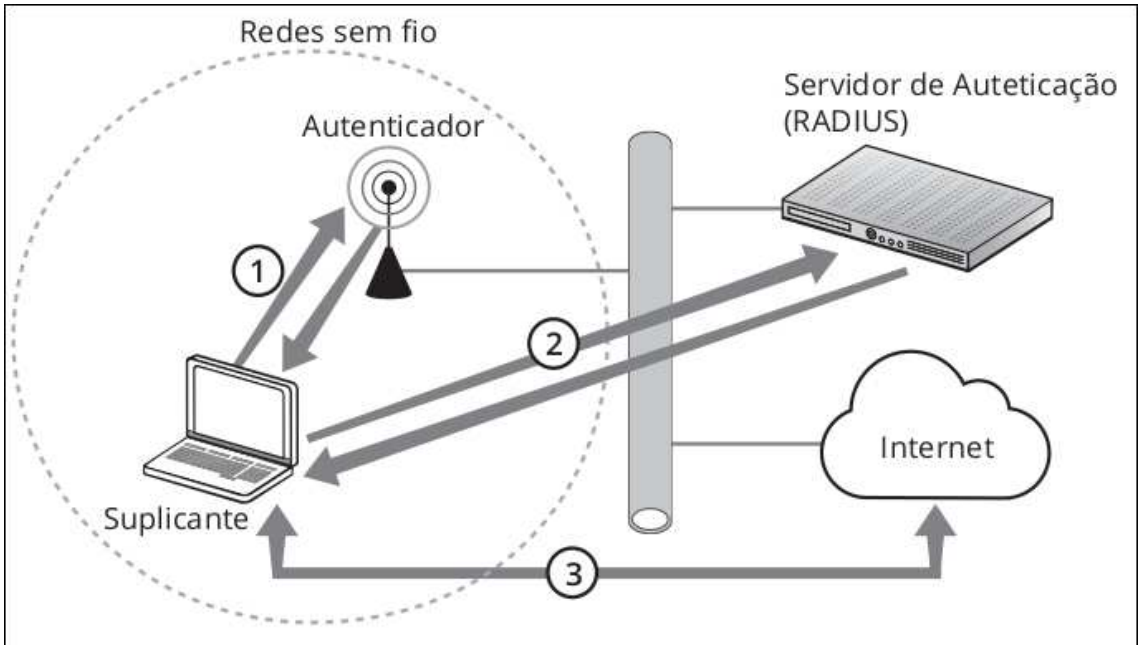
Uma característica do WEP que o WPA ainda preserva é o esquema de chaves pré-compartilhadas. Mas uma alternativa também foi oferecida pelo padrão: o uso de servidores de autenticação.

Um servidor de autenticação recebe pedidos de autenticação dos usuários e os valida ou não. Nesse caso, os usuários têm senhas individuais, além da chave da rede, provendo uma camada adicional de segurança.

Para implementar o servidor de autenticação, o IEEE escolheu o protocolo Remote Authentication Dial In User Service (RADIUS).

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

O elemento que deseja se autenticar (suplicante) inicia todo o processo logo após a associação ao ponto de acesso (autenticador). O papel do autenticador é permitir a conexão do suplicante com o servidor de autenticação e bloquear todo o tráfego do suplicante que não seja referente a autenticação. Se o servidor de autenticação liberar o acesso, o suplicante poderá usufruir de todos os serviços da rede. Caso contrário, será desassociado pelo ponto de acesso.



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

WPA2

Lançado em 2004, o WPA2 reconstrói o sistema de segurança do Wi-Fi sem nenhuma preocupação com a retrocompatibilidade. Definido pelo padrão IEEE 802.11i, chamada Robust Security Network (RSN).

O WPA2 utiiza o sistema de criptografia Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP), passando a utilizar um algoritmo de criptografia por blocos (block cipher) chamado Advanced Encryption Standard (AES), com chaves de 128 bits.

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

WPA2

Assim como o WPA, o WPA2 pode ser usado nas vertentes com chaves pré-compartilhada (Personal) e utilizando servidor de autenticação RADIUS (Enterprise).

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