Fundamentos de Redes sem fio

Tecnologia em Redes de Computadores

Aula 07

Prof. Me. Henrique Martins

Fatec Bauru

FUNDAMENTOS DE REDES SEM FIO
Prof. Me. Henrique Martins

Aula 07

- IEEE e outras Organizações
- Arquitetura de uma rede 802.11
- Métodos de autenticação

Institute of Eletrical and Eletronics Engineers (IEEE)

- O IEEE é o criador de padrões para muitas coisas relacionadas a tecnologia nos Estados Unidos. O IEEE cria seus padrões dentro das leis criadas pelo FCC. O IEEE especifica muitos padrões da tecnologia tais como: Ethernet (IEEE 802.3), Criptografia com chave pública (IEEE 1363) e WLANs (IEEE 802.11).
- Uma de suas missões é desenvolver padrões para operações em WLAN dentro das regras e regulamentações do FCC.
- Os principais padrões para WLANs que estão em uso ou na forma rascunho são: 802.11, 802.11b, 802.11a, 802.11g, 802.11n e 802.11ac.
- Para maiores informações acesse http://www.ieee.org

Outras Organizações

- Enquanto o FCC e o IEEE são responsáveis pela criação de leis e padrões que regulamentam o uso das WLANs nos Estados Unidos, existem outras organizações nos Estados Unidos e em outros países que contribuem para o crescimento e educação no mercado Wireless LAN.

  - Wireless Ethernet Compatibity Alliance (WECA)
  - European Telecommunications Standards Institute (ETSI)
  - Wireless LAN Association (WLANA)

Wireless Ethernet Compatibity Alliance (WECA)

- Responsável por certificar a interoperabilidade de produtos wi-fi (802.11) e promover wi-fi como um padrão global de WLANs através de vários segmentos do mercado.
- Quando um produto satisfaz os requerimentos de interoperabilidade exigidos pela WECA, é garantido a esse produto uma certificação que permite ao vendedor usar o logo wi-fi.
- O logo wi-fi assegura ao usuário final que aquele produto que ele está adquirindo, pode operar com outro produto que também tenha o logo, independente de fabricante.

European Telecommunications Standards Institute (ETSI)

- O ETSI tem as mesmas responsabilidades já vistas com o IEEE, com uma ressalva, é voltado para a Europa.
- Os padrões estabelecidos pelo ETSI para a HiperLAN/2 por exemplo; competem diretamente com aquelas criadas pelo IEEE.
- Como não existe qualquer movimento no sentido de unificar os padrões, o IEEE tentará a interoperabilidade com o HiperLAN/2 com o novo padrão que deverá surgir, o 802.11h.

Wireless LAN Association (WLANA)

- Responsável por prover conhecimento a aqueles que procuram aprender mais sobre WLANs.
- Também é útil na procura de um produto ou serviço especifico. Maiores informações em http://www.wlana.org

Arquitetura de uma rede 802.11

- Muitos dos tópicos que serão descritos a seguir estão definidos diretamente nos padrões do 802.11 e seu entendimento é necessário para o projeto, a implementação e a resolução de problemas em uma WLAN.

Localizando uma WLAN

- Quando instalamos, configuramos e iniciamos um cliente WLAN (Ex.: um cliente USB), o primeiro passo que será executado por ele, será verificar a existência de alguma WLAN dentro do seu alcance.
- Se houver, ele passará a descobrir também se haverá alguma possibilidade de associação com a WLAN em questão.
- Este processo é chamado de scanning, e ocorre antes de qualquer outro, uma vez que é modo como o cliente encontra a rede.

Service Set Identifier (SSID)

- O SSID é um valor único, alfa-numérico, sensível a maiúsculas e minúsculas, com comprimento que varia de 2 até 32 caracteres (depende de fornecedores), que é usado em WLANs como um nome da rede. Esta medida tem basicamente duas finalidades: segmentar as redes como uma maneira de segurança rudimentar e facilitar a associação com a rede.
- O SSID é enviado em vários tipos de frames, tais como: beacons, pedidos e respostas de probe. Um cliente deve estar configurado com o SSID correto para conseguir se associar a uma determinada rede. O mesmo deve ser feito no AP.

Service Set Identifier (SSID)

- Caso os clientes estejam participando de várias redes, todos os referidos SSID devem estar configurados no cliente.

- É fundamental que o SSID configurado no cliente seja exatamente o mesmo configurado no AP, para que seja possível a associação.

- Se o AP não estiver usando nenhum SSID, a associação de um cliente ao mesmo será automática.

Beacons

- São frames curtos enviados pelos APs a uma estação (modo infraestrutura) ou de uma estação a outra (modo ad-hoc) com o propósito de sincronizar a comunicação em uma WLAN.
- Entre as funções de um beacon, poderíamos destacar:
  - Sincronização do tempo
  - Parâmetros FH ou DS
  - Informação de SSID
  - Mapa de indicação de tráfego(TIM)
  - Taxas suportadas

Beacons

- **Sincronização do tempo** – Quando um cliente recebe o beacon, ele muda seu clock de modo a refletir o clock do AP. Uma vez feita a mudança, os clocks estão sincronizados. Sincronização de clocks em unidades de comunicação, garante que funções dependentes do tempo serão executadas sem erros. Um bom exemplo disso é o pulo da frequência em sistemas FHSS.
- **Parâmetros FH ou DS** – Contém informações direcionadas a tecnologia que estiver sendo utilizada. Em um sistema FHSS, parâmetros de pulo e a sequência do pulo são incluídos. Em sistemas DSSS, informações como o canal sendo utilizado, estarão presentes no beacon.

Beacons

- **Informação de SSID** – Estações procuram no beacon, o SSID da rede que elas querem se associar.
  - Uma vez identificada essa informação, elas enviam um pedido de autenticação para o endereço MAC que originou o beacon, que no nosso caso seria o do AP.
  - Se estações estão configuradas para se associar a qualquer rede (sem SSID especifico), eles se associarão a primeira rede encontrada, no caso de haver mais de um AP, aquele que tiver o sinal mais forte terá preferência.

Beacons

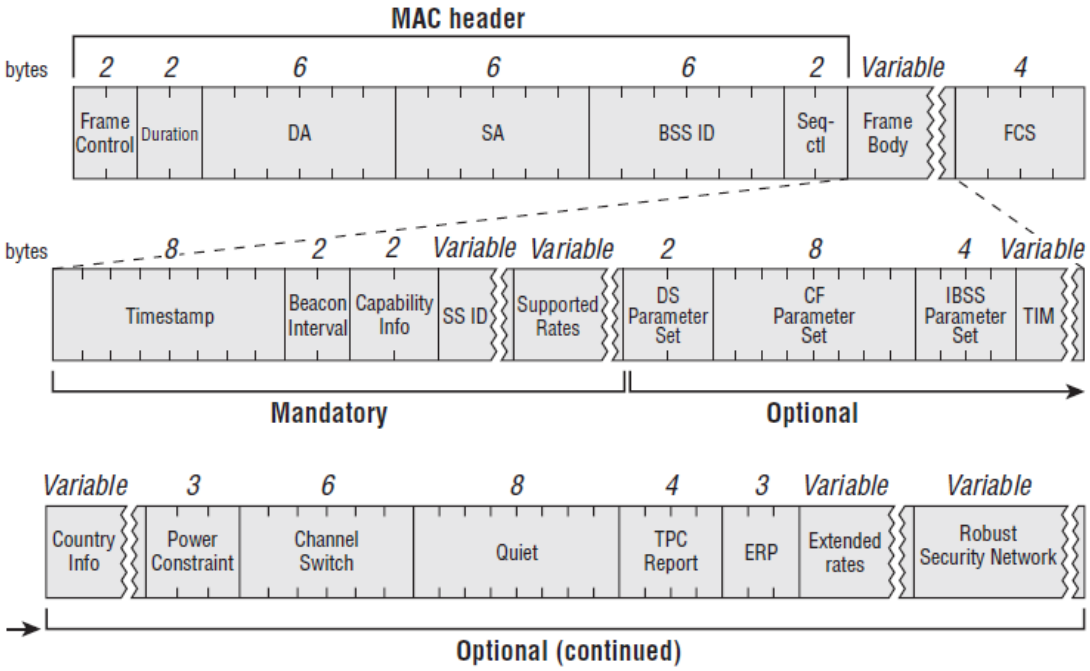
- **Mapa de indicação de tráfego (TIM)** – O TIM nada mais é que uma indicação de quais estações tem pacotes a serem processados, que estão na fila do AP. Esta informação é passada em cada beacon para todas as estações associadas. Quando estão no estado de sleeping, as estações ouvem os beacons e checam o TIM para ver se elas estão presentes na lista, caso não estejam voltam ao estado de sleeping.
- **Taxas suportadas** – Há muitas velocidades suportadas dependendo do padrão do hardware em uso. Esta informação é passada nos beacons para informar quais as velocidades suportadas pelo AP.

Beacons

- Site detalha o funcionamento de um Beacon Frame

https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/

FIGURE 4.5 Beacon frame structure



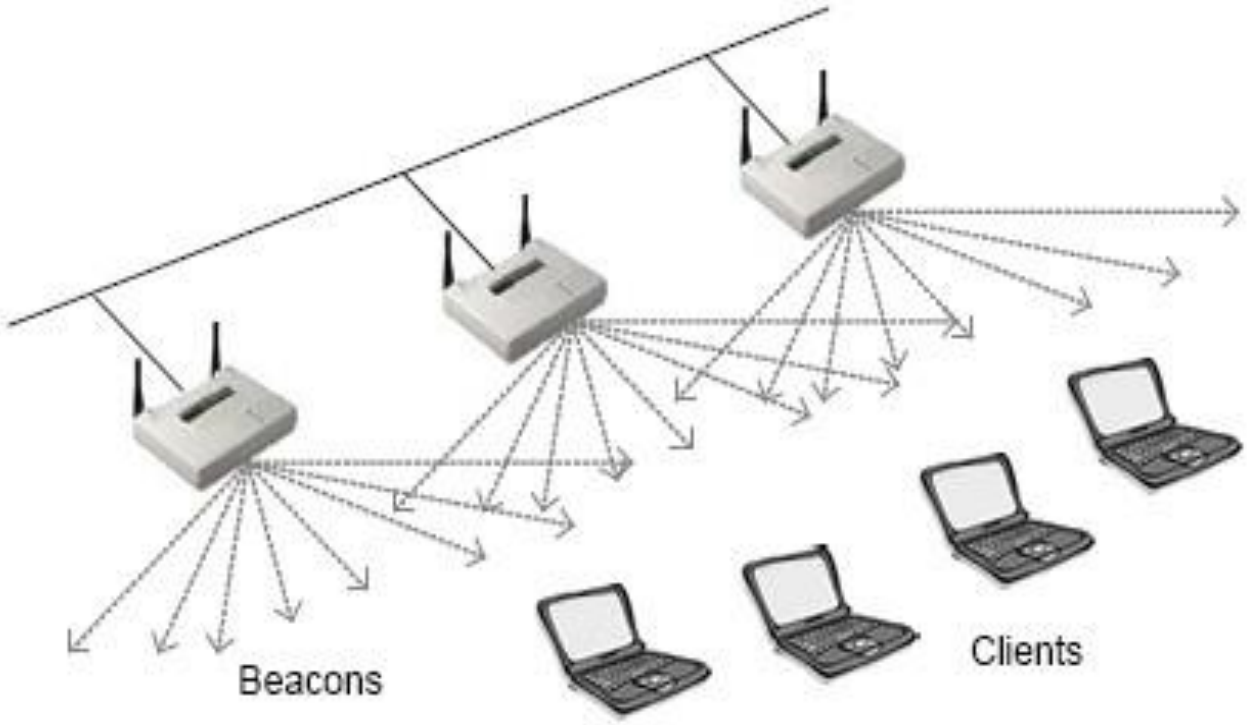
Scanning Passivo

- É o processo pela qual estações procuram por beacons em cada canal por um determinado período de tempo, tão logo a estação tenha sido inicializada.
- Os beacons são enviados pelo AP e as estações procuram nesses beacons se o SSID da rede que eles desejam entrar está listado.
- Se estiver, a estação então tenta entrar na rede através do AP que enviou o beacon. Em configurações em que há vários APs, vários beacons serão enviados, a estação tenta entrar na rede através do AP que tiver o sinal mais forte.

Scanning Passivo

- O processo de scanning continua mesmo depois da estação ter entrado na rede. Isso economiza tempo na reconexão a rede, caso a estação tenha perdido a conexão por algum motivo. Esse processo só é possível, porque é através dos Beacons que as estações mantém uma lista de APs disponíveis e catalogam informações sobre os APs, tais como: canal, nível de sinal, SSID entre outras.
- Uma estação migrará de uma célula para outra, quando o nível de sinal do AP ao qual ela está conectada cair abaixo de um determinado nível. Essa migração ocorrerá sem o conhecimento do usuário, mas para que isso seja possível, as células devem se sobrepor em 20-30%.

Scanning Passivo



- No scanning passivo são os APs que iniciam o processo, através do envio de beacons.

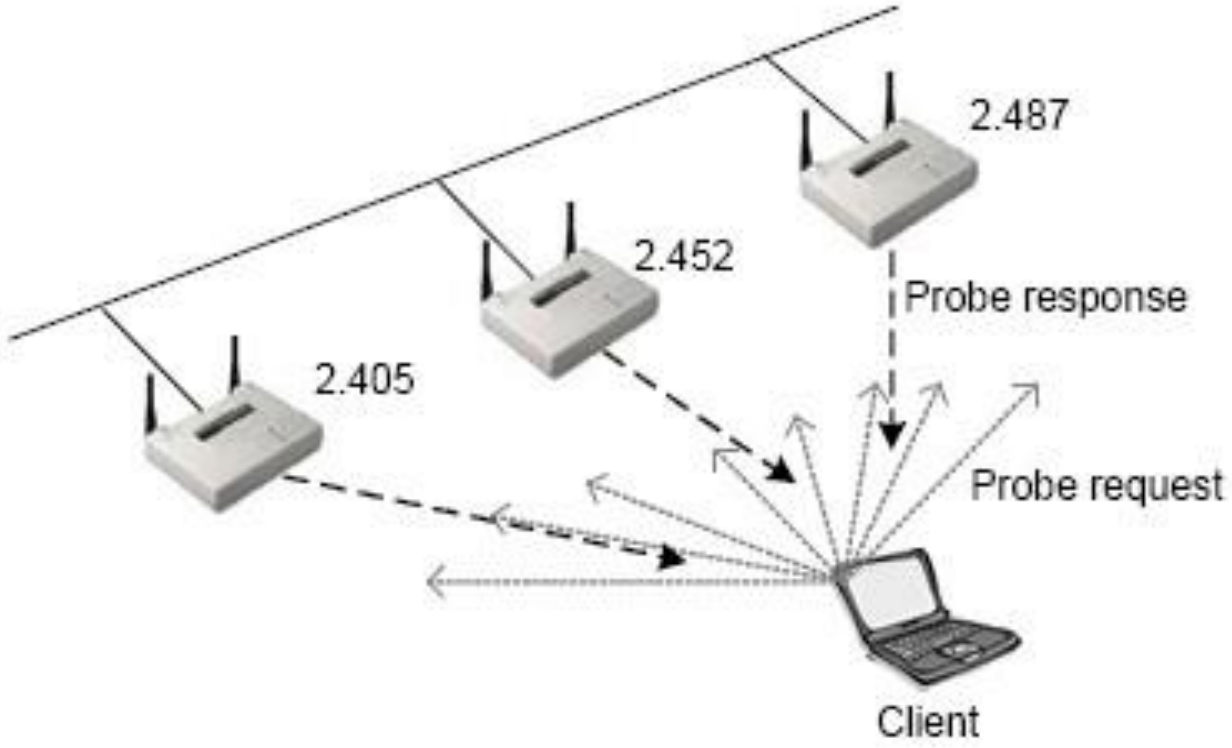
Scanning Ativo

- Diferentemente do processo anterior, no scanning ativo, são as estações que iniciam o processo, tornando-se portanto parte ativa do mesmo.
- Quando a estação está procurando por uma rede, ela envia um frame chamado **probe request**, contendo o SSID da rede que ela procura ou uma rede qualquer. O AP que tiver o SSID em questão, envia um **probe response**. Se houver vários APs, somente aquele que tiver aquele SSID envia o probe response. Por outro lado, se o SSID de broadcast, que indica: qualquer rede, for enviado no probe request, todos os APs enviarão um probe response.

Scanning Ativo

- Uma vez que o AP com o SSID específico tenha sido encontrado, a estação inicia os passos de autenticação e associação para entrar na rede através daquele AP.
- A informação passada nos probes responses pelos APs é idêntica aos beacons, com exceção do TIM.
- O nível de sinal informado nos probes responses ajuda ao cliente determinar qual AP ela tentará se associar. Geralmente a estação escolhe o AP com o melhor nível de sinal e menor taxa de erro (BER). O BER é basicamente uma comparação de pacotes corrompidos em comparação a pacotes bons, tipicamente determinada pela relação sinal-ruido.

Scanning Ativo



Métodos de autenticação

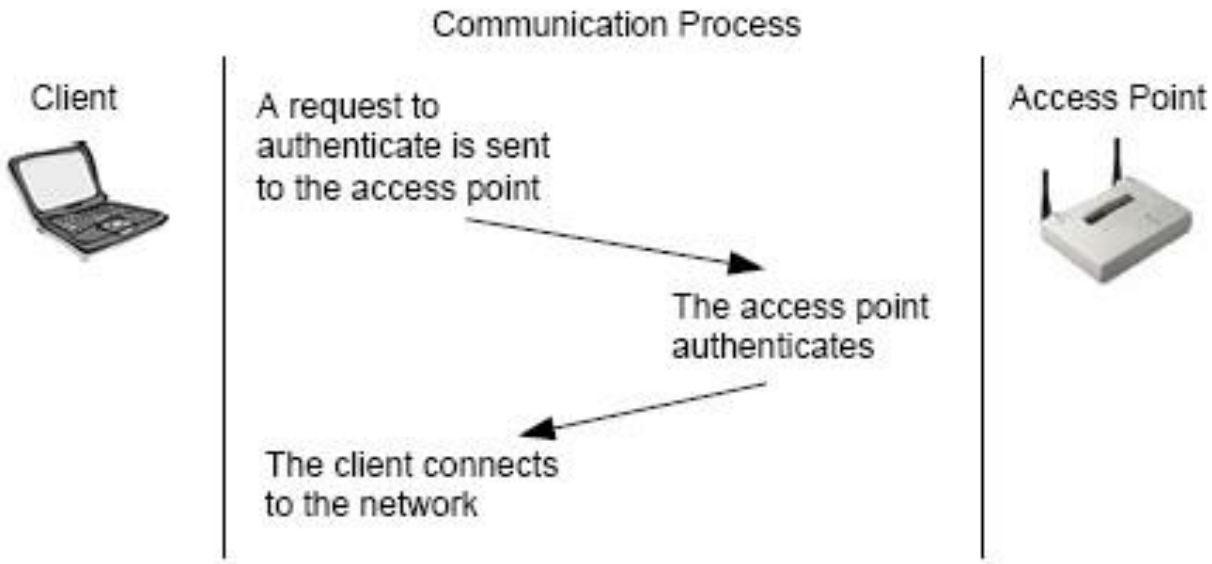
- O padrão IEEE 802.11 especifica dois métodos de autenticação:
  - Autenticação de sistema aberto e
  - Autenticação de chave compartilhada.
- O mais simples e mais seguro dos dois é a autenticação de sistema aberto.
- Para se tornar autenticado o cliente deve caminhar por uma série de passos durante esse processo, esses passos variam de um método para o outro.

Autenticação de sistema aberto

- É o método padrão usado nos equipamentos wireless.
- Usando este método uma estação pode se associar com qualquer AP que também use o método.
- Este método de autenticação é baseado no SSID, ou seja, basta que a estação e o AP tenham o mesmo SSID para que a autenticação ocorra.
- O processo de autenticação de sistema aberto é usado de forma eficaz tanto em ambientes seguros quanto não seguros.

Autenticação de sistema aberto

- O cliente faz um pedido para se associar ao AP.
- O AP toma conhecimento desse pedido, envia uma resposta positiva e autentica o cliente.



Processo de autenticação de sistema aberto

Autenticação de sistema aberto

- Existe ainda a opção de se usar WEP (não é obrigatório) para criptografar o processo. Porém a criptografia não é feita durante o processo de autenticação em si, ou seja, a chave WEP não é verificada por ambos os lados durante a autenticação, mas para criptografar os dados depois que o cliente já estiver autenticado e associado.
- Este método de autenticação é usado em diversos cenários, mas há duas razões principais para isso:
  - É considerado mais seguro dos dois métodos disponíveis.
  - Já é usado por padrão nos dispositivos wireless, o que não requer configuração adicional.

Autenticação de chave compartilhada

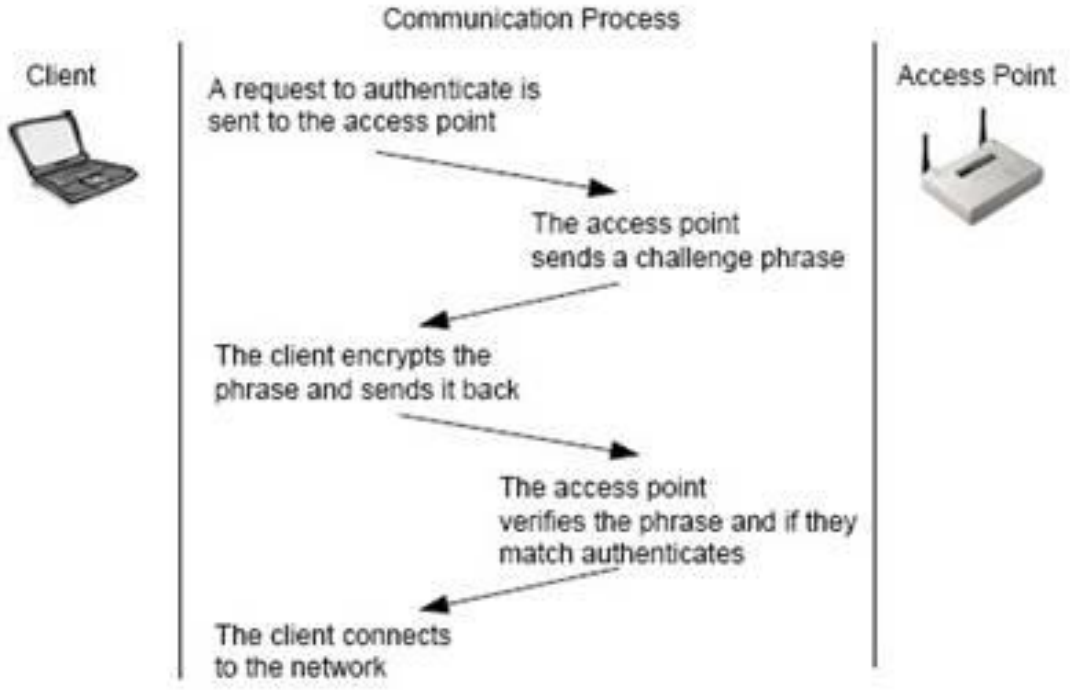
- Neste método o uso da criptografia é obrigatório.
- A criptografia WEP usa chaves tanto no cliente quanto no AP, e elas devem ser as mesmas para que o WEP possa operar.
- Essas chaves são configuradas manualmente.

Autenticação de chave compartilhada

- O cliente faz um pedido de associação ao AP (Esse passo é o mesmo da autenticação de sistema aberto)
- O AP envia uma pergunta ao cliente. Essa pergunta é um texto gerado aleatoriamente e enviado ao cliente na forma de texto puro.
- O cliente responde a essa pergunta. A chave WEP do cliente é usada para criptografar a pergunta e por fim a mesma é enviada já codificada de volta ao AP.
- O AP responde a resposta do cliente. A resposta codificada enviada pelo cliente é então decodificada usando a chave WEP do AP, verificando assim se o cliente tem a mesma chave. Se a chave do cliente é a correta, o AP responderá positivamente e autenticará o cliente. Se a chave do cliente não for a correta, o AP responderá negativamente e não autenticará o cliente.

Autenticação de chave compartilhada

- Diferentemente do que possa parecer, o processo de autenticação de chave compartilhada não é mais seguro que o processo de autenticação de sistema aberto. O processo de chave compartilhada, abre uma porta para hackers.



Referência

- Fonte: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless020.asp