# Fundamentos de Redes sem fio

Tecnologia em Redes de Computadores

Aula 08

Prof. Me. Henrique Martins

Fatec Bauru

FUNDAMENTOS DE REDES SEM FIO
Prof. Me. Henrique Martins

# Aula 08

- Soluções VPN
- WPA

# Soluções VPN

- A tecnologia VPN proporciona os meios para dois dispositivos de rede transmitirem dados de forma segura em um meio não seguro.
- O uso mais comum da VPN é na comunicação entre redes de duas empresas distintas ou na comunicação de um cliente com um servidor corporativo via internet.
- Porém existem outras aplicações para a VPN e uma delas é a proteção de dados em uma rede wireless. VPN trabalha criando um túnel no topo de um protocolo como o IP.
- O tráfego dentro do túnel é codificado e totalmente isolado do restante da rede. A tecnologia VPN proporciona três níveis de segurança: autenticação do usuário, criptografia e autenticação dos dados.

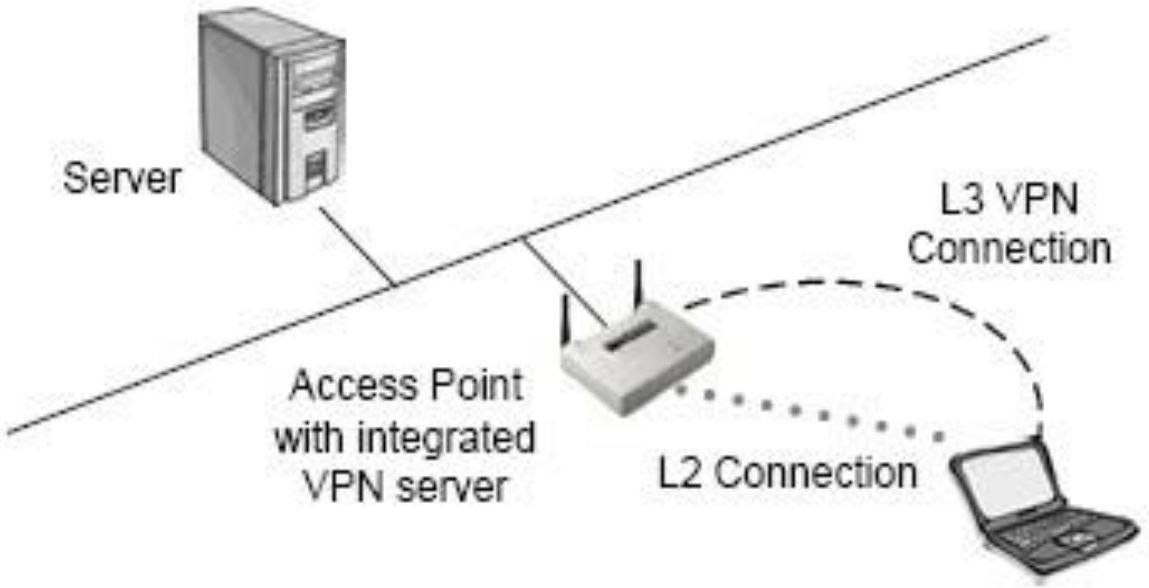
# Soluções VPN

- **Autenticação do Usuário** – Garante que somente usuários autorizados (por um dispositivo específico) são capazes de conectar, enviar e receber dados em uma rede WLAN.

- **Criptografia** – Oferece proteção adicional e garante que transmissões sejam interceptadas, eles não podem ser decodificadas, sem esforço e uma grande demanda de tempo.

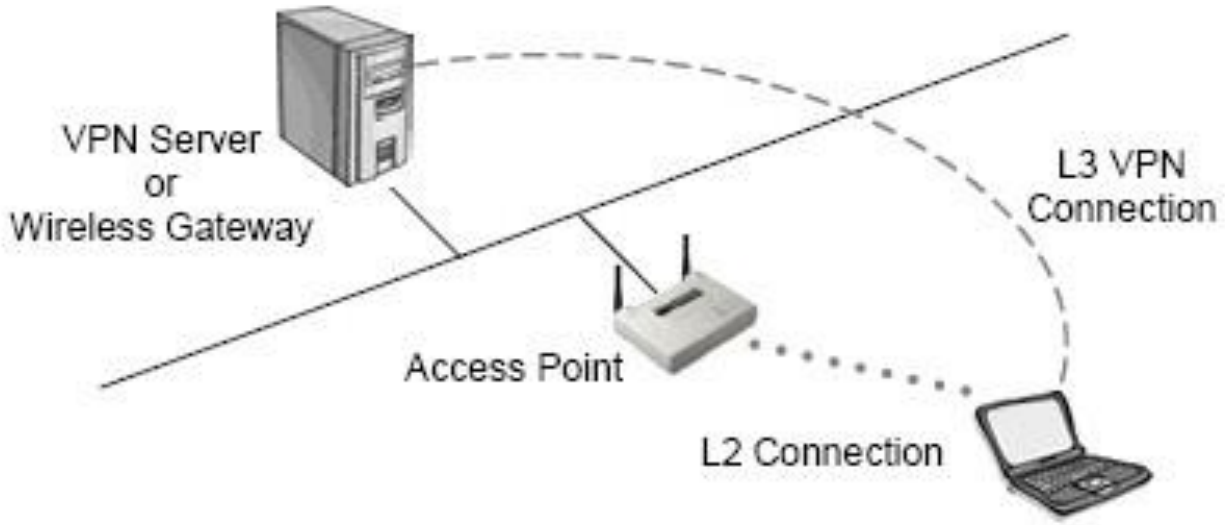
- **Autenticação dos dados** – Garante a integridade dos dados em uma WLAN, dessa forma há a certeza que todo o tráfego provem somente de dispositivos autenticados.

# Soluções VPN




**Ponto de acesso com servidor VPN integrado**

# Soluções VPN




**Ponto de acesso com servidor VPN externo**

# Soluções VPN

- A aplicação da tecnologia VPN requer algumas adaptações em relação a LANs quando usada em redes wireless pelas seguintes razões:
  - A função de repetidor inerente aos pontos de acesso automaticamente encaminha o tráfego entre estações WLAN que se comunicam juntas e parecem estar na mesma WLAN.
  - O alcance das redes WLAN geralmente ultrapassa os limites do escritório ou do prédio em que estão, dando aos invasores meios de comprometer a segurança da rede.

# Soluções VPN

- A implementação de uma solução VPN irá variar dependendo das necessidades de cada tipo de ambiente.
- Por exemplo, um hacker que conseguisse a chave WEP usando um sniffer em uma WLAN, teria condições de decodificar os pacotes em tempo real.
- Porém se a rede usasse também uma solução VPN, os pacotes estariam não somente codificados, mas também encapsulados.
- Essa camada extra de segurança fornece muitos benefícios a nível de acesso.

# Segurança

- WEP não proporciona uma segurança robusta para WLANs corporativas.
- Devido ao fato da chave ser estática, não é difícil para um hacker obter a chave sniffando a rede. Isso motivou o surgimento de uma implementação de WEP em que as chaves são fortes e geradas dinamicamente, mas por esse novo mecanismo ser um padrão proprietário, dificulta ou mesmo inviabiliza seu uso em redes que tem dispositivos de vários fabricantes.
- O WPA especificado no padrão 802.1i veio para solucionar esses problemas.

# Segurança

- WPA inclui TKIP (Protocolo de integridade de chave temporal) além dos mecanismos 802.1x. Essa combinação fornece codificação de chave dinâmica e autenticação mutua algo muito necessário em WLANs.
- As seguintes características foram adicionadas ao WEP:
  - **Vetores de inicialização de 48 bits**
  - **Construção e distribuição de chave por pacote**
  - **Código de integridade de mensagem (MIC)**

# Vetores de inicialização de 48 bits

- WEP produz o que é chamado de "agendamento de chave", concatenando a chave compartilhada com um vetor de inicialização de 24 bits gerado aleatoriamente (IV). Com um vetor de 24 bits (IV), WEP evetualmente usa o mesmo IV para diferentes pacotes de dados. Isso resulta na transmissão de frames tendo frames codificados similares o suficiente para um hacker coletar esses frames baseados no mesmo IV e determinar seus valores compartilhados decodificando esses frames.
- WPA com TKIP dificulta e muito o trabalho do hacker devido ao uso de um vetor de 48 bits, o que dificulta a quebra da codificação através da captura de frames.

# Construção e distribuição de chave por pacote

- WPA gera automaticamente e periodicamente uma chave de codificação para cada cliente. Uma única chave para cada frame 802.11 é utilizada. Isso evita que a mesma chave permaneça em uso por semanas ou meses.
- Portanto é muito difícil que alguém mesmo tendo uma cópia da chave pudesse comprometer a maioria dos frames, uma vez que aquela chave não serviria para todos os frames. Mal comparando, seria o mesmo que alguém trocar a fechadura de uma porta toda vez que a fechasse.

# Código de integridade de mensagem (MIC)

- WPA implementa um código de integridade de mensagem para se resguardar de ataques. WEP anexa um código verificador de integridade de 4 bytes (ICV) ao frame 802.11.
- O receptor irá calcular o ICV na recepção do frame para determinar se ele é igual aquele que está no frame. Se for igual há uma grande chance do frame não ter sido interceptado.

# Segurança

- Embora WEP codifique o ICV, um hacker poderia mudar os bits e atualizar o ICV codificado sem ser detectado pelo receptor. WPA soluciona esse problema calculando um MIC de 8 bytes que se localiza antes do ICV.
- Para autenticação o WPA usa uma combinação da autenticação de sistema aberto com o 802.1x. Eis como o processo ocorre:
  - O cliente wireless autentica com o AP, o qual por sua vez, autoriza o cliente a enviar frames.
  - É feito uma autenticação a nível de usuário com o 802.1x. WPA intermédia a comunicação com um servidor de autenticação corporativo (RADIUS ou LDAP) para validar o usuário.

# Segurança

- WPA também é capaz de operar em um modo conhecido como chave pré-compartilhada, caso nenhum servidor de autenticação externo esteja disponível, como nos casos de ambientes domésticos.

# Service Sets

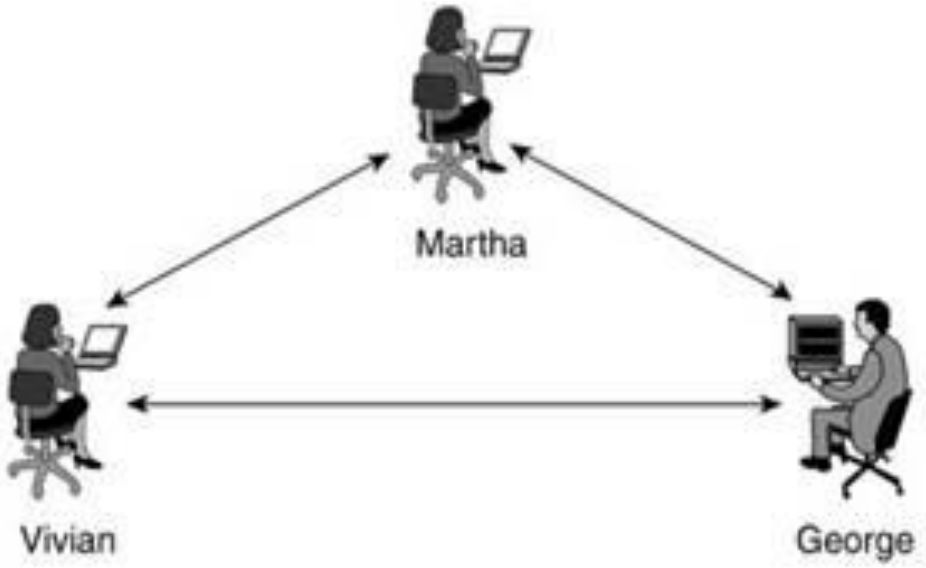
- Um **service set** é um termo usado para descrever os componentes básicos de uma WLAN operacional, pode ser também referenciado como topologia de uma WLAN.
- As WLANs podem ser classificadas em 3 categorias: IBSS, BSS e ESS.
- WLANs fazem o broadcast de um sinal através de uma portadora de RF. A estação pode estar na faixa de vários transmissores, mas como o sinal carrega o SSID do transmissor, a estação receptora usa esse SSID (que deve ser o mesmo do seu) para filtrar os sinais recebidos de um determinado transmissor e localizar a célula de onde ela faz parte.

# IBSS (Independent Basic Service Sets)

- Um IBSS consiste de um grupo de estações 802.11 se comunicando diretamente umas com as outras. IBSS é também chamado de AD-HOC, porque ele é essencialmente uma rede peer to peer. Não há um ponto central que controle a rede.
- Redes IBSS são geralmente pequenas e não tem interfaces com redes cabeadas. Não há um limite pré-estabelecido para o número máximo de estações. Porém a medida que a rede cresce, problemas de comunicação podem ocorrer devido ao problema do nó escondido. Como não há um elemento central que faça o controle na rede, ou seja, para determinar qual estação tem autorização para transmitir naquele momento, essa autorização é controlada de uma maneira distribuída.

# IBSS (Independent Basic Service Sets)

- Se a transmissão de dados para fora do IBSS é necessária, um dos clientes deve atuar como gateway ou roteador usando uma solução de software para esse propósito.



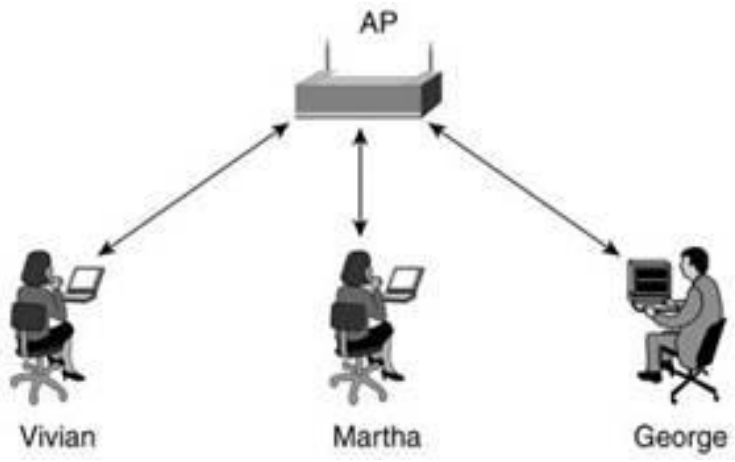

**WLAN IBSS ou AD-HOC**

# BSS (Basic Service Sets)

- Um BSS consiste de um grupo de estações 802.11 se comunicando umas com as outras através de um dispositivo central conhecido como ponto de acesso ou AP. Diferentemente do IBSS, em um BSS, as estações não se comunicam diretamente umas com as outras. Elas podem se comunicar somente com o AP e este encaminha os frames para a estação destino. Um ponto de acesso possui uma porta para conexão a uma estrutura cabeada (um backbone Ethernet por exemplo) e por isso é também chamado de infraestrutura BSS.
- Uma rede BSS possui um thgrouput melhor que uma IBSS, devido a presença de um dispositivo que gerencia todo o tráfego.

# BSS (Basic Service Sets)

- O BSS cobre uma simples célula ou área RF em torno do ponto de acesso com várias zonas de taxas de dados (círculos concêntricos) de diferentes velocidades. As velocidades nesses círculos dependerá da tecnologia sendo utilizada. Se o BSS é feito de equipamentos 802.11b, então os círculos poderiam ter velocidades de 11, 5.5, 2 e 1 Mbps. As velocidades se tornam menores a medida que os círculos se afastam do ponto de acesso. Um BSS tem um único SSID.

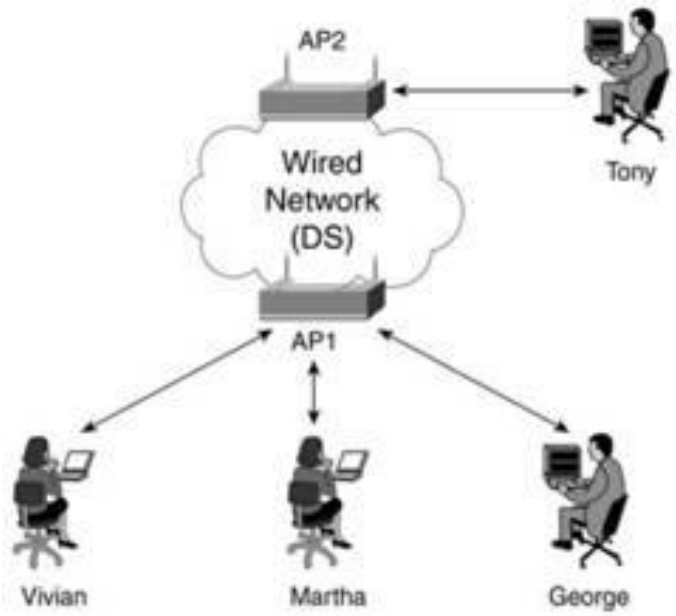


# ESS (Extended Service Sets)

- Dois ou mais BSS podem ser conectados via suas interfaces de uplink formando uma estrutura ESS. A interface de uplink conecta o BSS a um sistema de distribuição (DS).
- O uplink para o sistema de distribuição pode ser uma conexão cabeada ou wireless, mas na maioria das vezes é uma conexão cabeada, geralmente ethernet.

# ESS (Extended Service Sets)

- De acordo com o padrão 802.11, um ESS cobre múltiplas células e permite (mas não requer) capacidades de roaming e não necessita que as células tenham o mesmo SSID.



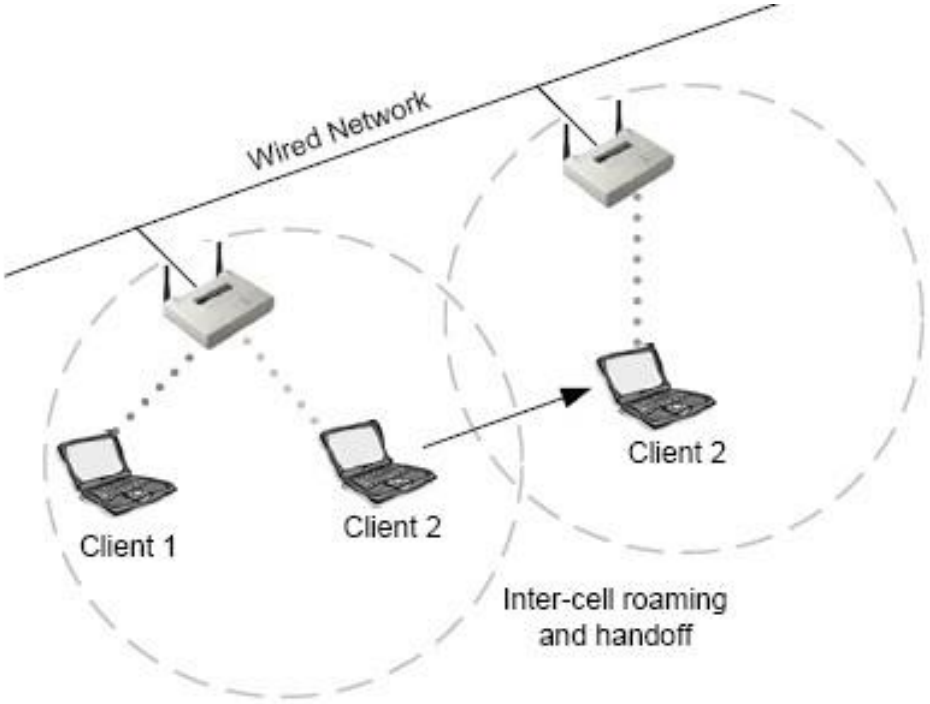

**Uma estrutura ESS**

# Roaming

- É a habilidade de um cliente em se mover de uma célula para a outra sem perder a conectividade com a rede. Os pontos de acesso envolvidos nos BSS são os grandes responsáveis por esse processo que é transparente para o cliente.
- Quando qualquer área em um prédio está dentro do alcance de um ou mais pontos de acesso, as células se sobrepõem. Áreas de cobertura sobrepostas são um aspecto importante no setup de WLANs, porque isto habilita o roaming entre elas.
- Um usuário com um notebook, poderia circular livremente entre essas células sem perder a conexão com a rede.

# Roaming

- Vários pontos de acesso podem proporcionar uma cobertura de roaming para um campus ou um prédio inteiro.




**Roaming em um ESS**

# Roaming

- Quando as áreas de cobertura de dois ou mais pontos de acesso se sobrepõem, as estações nessa área sobreposta podem estabelecer a melhor conexão possível com um dos APs e ao mesmo tempo estar procurando pelo melhor AP.
- Para minimizar a perda de pacotes durante o chaveamento, os APs novo e antigo se comunicam para coordenar o processo de roaming.

# Padrões

- O padrão 802.11 não define a forma como o roaming deve ser feito, mas define os conceitos principais. Nesses conceitos estão incluídos um scanning passivo e ativo e um processo de reassociação. Toda vez que um cliente migrar de um AP para o outro, um processo de re-associação deverá ocorrer entre o cliente e o novo AP.
- O padrão permite a migração de um cliente entre vários APs operando ou não no mesmo canal.
- Para satisfazer as necessidades de comunicação de rádios móveis, o padrão deve ser tolerante com conexões sendo perdidas e re-estabelecidas. O padrão tenta garantir o mínimo de prejuízo a entrega dos dados e fornece algumas características para caching e encaminhamento de mensagens entre BSSs.

# Padrões

- O padrão 802.11 deixa a cargo dos fabricantes muitos aspectos da operação detalhada dos sistemas de distribuição. Esta decisão foi uma decisão deliberada de parte dos desenvolvedores de padrões, porque eles estavam preocupados com o fato de tornar o padrão independente de qualquer padrão de rede existente.
- Como resultado, a maioria de WLANs 802.11b usando topologias ESS estão conectadas a LANs Ethernet e fazem uso do TCP/IP.

# Conectividade

- A camada MAC 802.11 é responsável pela forma com que um cliente se associa a um AP.
- Quando um cliente 802.11 entra no alcance de um ou mais pontos de acesso, ele escolhe um AP para se associar, baseado no nível do sinal e na taxa de erro de pacotes. Uma vez associado com o AP, o cliente periodicamente faz um survey em todos os canais na tentativa de encontrar um AP com melhor performance (melhor nível de sinal). Uma vez encontrado esse AP, o cliente se re-associa com o novo AP mudando para o canal na qual o AP está configurado.

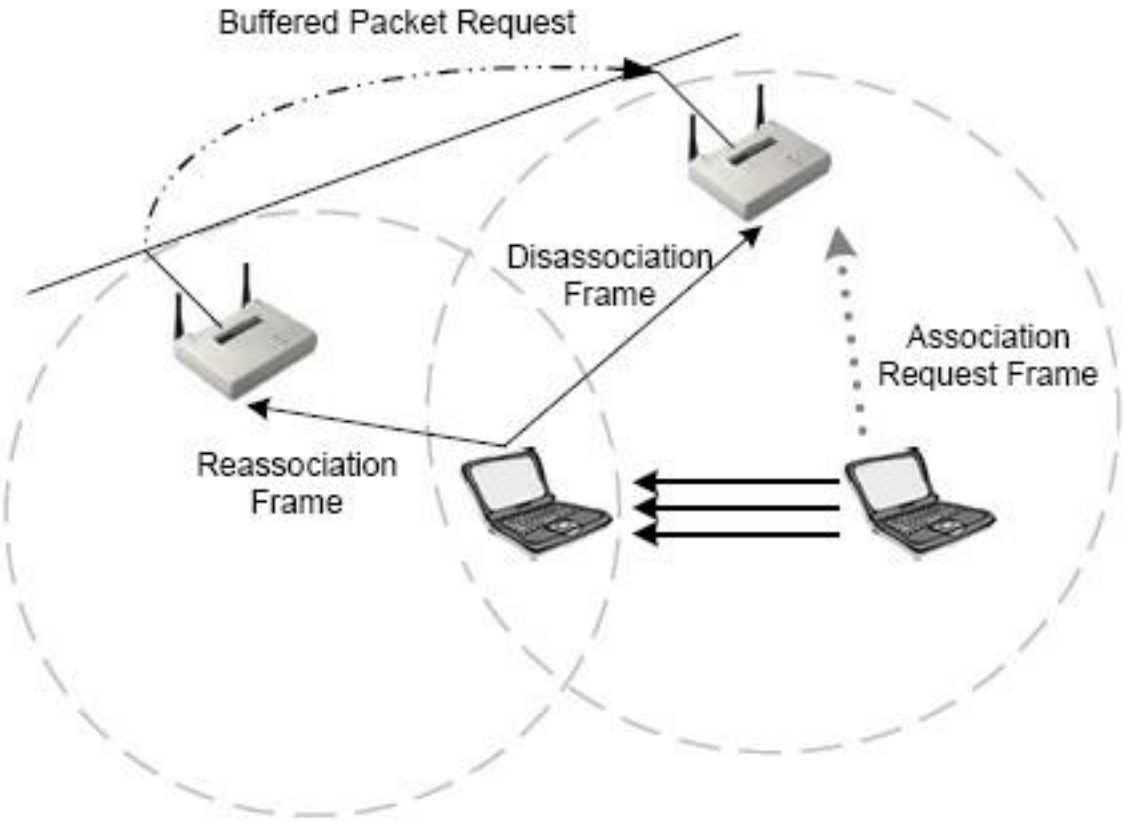
# Re-associação

- Re-associação geralmente ocorre porque o cliente se afastou demasiadamente do AP original levando a um enfraquecimento no sinal. Mas existem outros casos em que a re-associação pode ocorrer. Um caso muito comum é quando há um alto tráfego na rede no AP original.
- Neste caso isso funciona também como balanceamento de carga, uma vez que a ideia principal é distribuir uniformemente a carga por toda a infraestrutura WLAN disponível.

# Re-associação

- Associação e re-associação diferem quanto ao seu uso. Frames de pedido de associação são usados quando o cliente tenta entrar na rede pela primeira vez. Frames de pedido de re-associação são usados quando o cliente migra entre APs.
- No segundo caso, o novo AP tem conhecimento dos frames buferizados do AP antigo e deixa o sistema de distribuição saber que o cliente se moveu.

# Re-associação




Roaming com re-associação

# Re-associação

- Esse processo de associação e re-associação dinâmica permite configurar WLANs com áreas de cobertura muito larga criando uma série de células sobrepostas através de um prédio ou campus. Para a implementação ser bem sucedida, deve-se usar a reutilização de canal, tomando o cuidado de configurar cada AP com um canal que não venha a interferir com aquele utilizado pelo seu vizinho.
- Devemos lembrar que há somente 3 canais no DSSS que não se sobrepõem, e estes é que devem ser usados para implementações multi-células. Se dois APs são configurados para usar o mesmo canal e estão próximos um do outro, isto causará interferência entre eles e a largura de banda na área da sobreposição das células sofrerá uma drástica redução.

# Uso da VPN

- Soluções de VPN wireless podem ser implementadas de duas formas. A primeira delas, através do uso de um servidor de VPN externo centralizado.
- Este servidor de VPN, poderia ser uma solução de hardware proprietário ou um servidor com uma aplicação de VPN rodando nele.
- Este servidor de VPN atua como gateway e firewall entre o usuário wireless e o núcleo da rede e fornece um nível de segurança similar as VPNs em LANs.

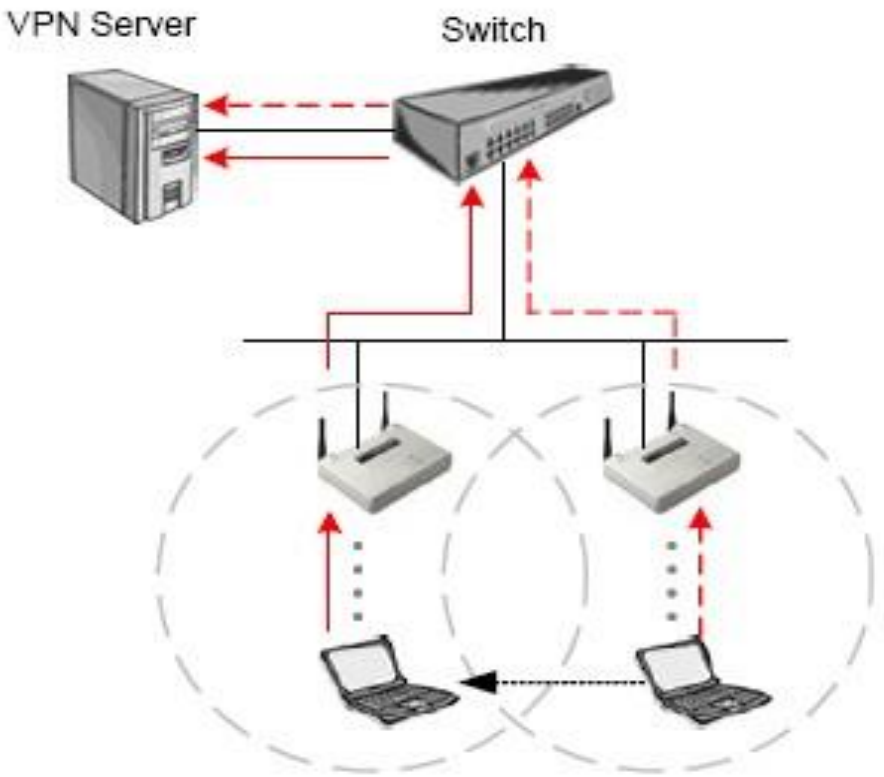
# Uso da VPN

- A segunda delas, através de um set distribuído de servidores VPN. Alguns fabricantes implementam funcionalidades de VPN em seus pontos de acesso.
- Este tipo de solução seria adequada para organizações de pequeno e médio portes, uma vez que não há um mecanismo de autenticação externo como o RADIUS.
- Muitos desses pontos de acesso além de serem servidores VPN também suportam RADIUS.

# Uso da VPN

- Quando o cliente migra de uma célula para outra, na verdade o cliente está migrando entre pontos de acesso (supondo que eles não tem funcionalidade VPN e não há servidores VPN externos), este é um processo que ocorre dentro da camada 2.
- Porém, quando essa mesma migração ocorre e há servidores de VPN envolvidos, túneis são construídos para o ponto de acesso ou servidor de VPN centralizado e o processo agora ultrapassa os limites da camada 2 e passa a ser de camada 3.
- Nesse caso, deve haver algum mecanismo que mantenha o túnel vivo quando ele ultrapassa os limites da camada 2.

# Uso da VPN




Roaming dentro de túneis VPN

# Uso da VPN

- O problema aqui é que normalmente cada ponto de acesso está em uma subnet IP diferente, e quando o cliente migra de uma célula para outra ele vai estar com novo IP, e com isso perderá a conexão aos servidores e aplicações.

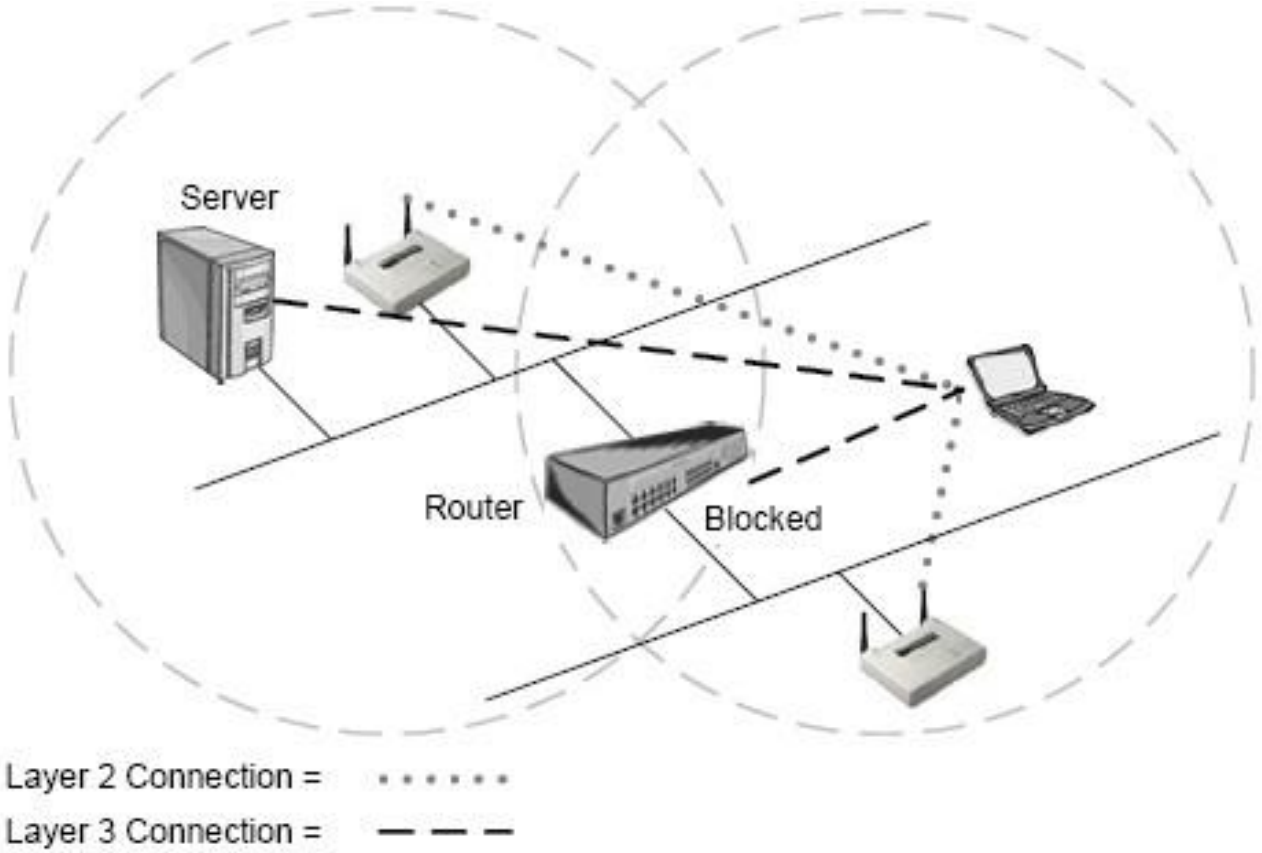
# Uso da VPN

- Empresas que tem muitos prédios, muitas vezes implementam uma LAN em cada prédio e conectam essas LANs com roteadores ou switches-routers. Isto é uma segmentação de camada 3 e tem duas vantagens. A primeira é o bloqueio de broadcasts entre os segmentos e a segunda, um controle de acesso entre os segmentos da rede. Este tipo de segmentação pode ser feita também usando VLANs em switches.
- É como se partíssemos um switch em várias partes e cada parte vira uma subrede separada (VLAN), lembrando que uma VLAN não se comunica com outra sem o uso de roteamento. Essa segmentação de camada 2, segmenta a rede completamente.

# Uso da VPN

- Quando roteadores são usados, usuários devem ser capazes de ultrapassar os limites do roteador sem perder sua conectividade de camada 3. A conexão de camada 2 é mantida pelo AP, mas como houve uma mudança na subnet IP durante a migração, a conexão para os servidores (por exemplo) será quebrada. Uma boa medida para evitar esse problema seria colocar todos os APs na mesma subnet IP, porém essa não é uma solução muito prática nem tão pouco simpática.
- Mesmo com o uso de VLANs, teríamos o mesmo tipo de problema porque o switch veria essa migração de usuários como uma mudança de uma VLAN para outra.

# Uso da VPN

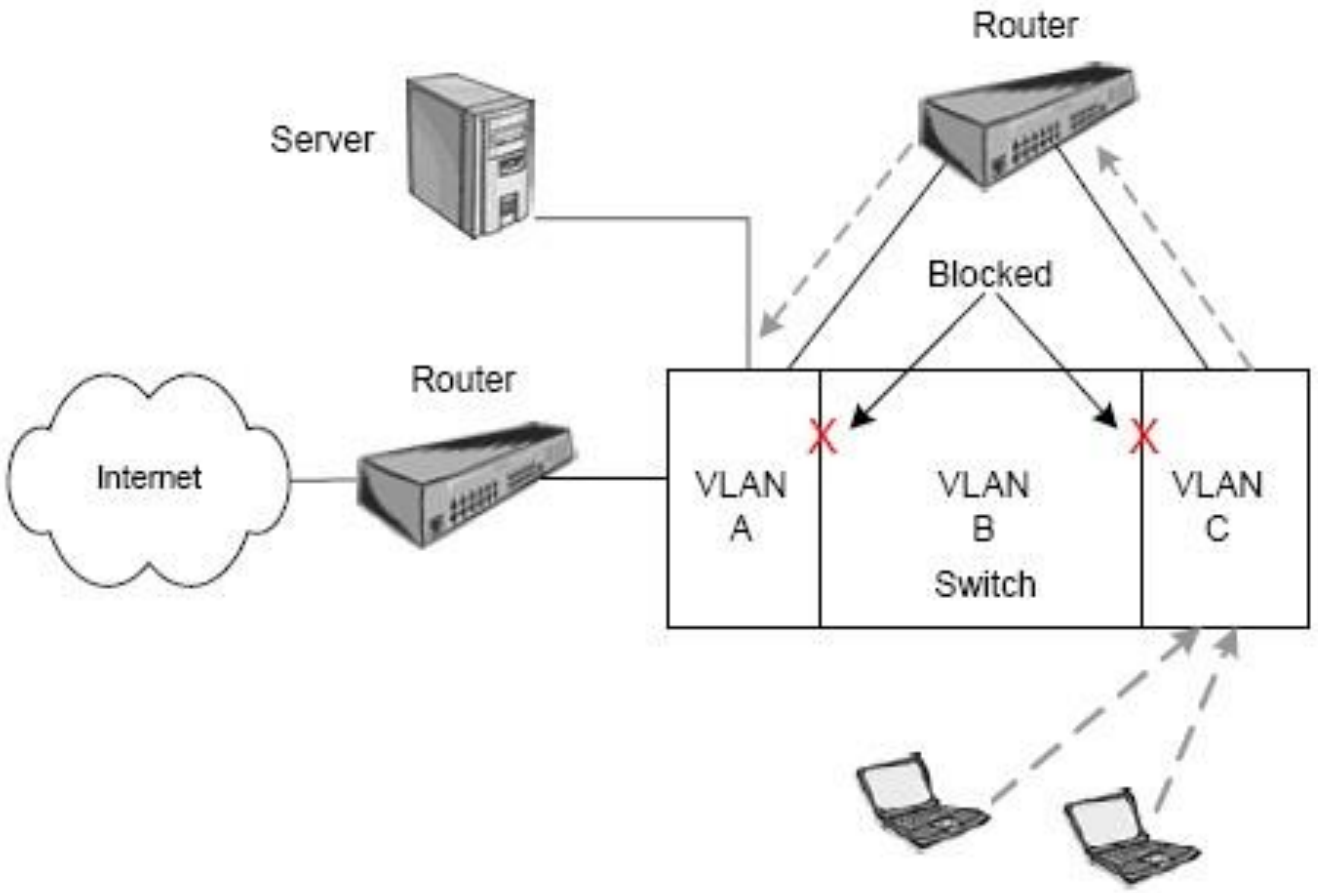



Roaming com roteador envolvido

# Uso da VPN

- A solução de hardware definitiva para esse problema seria colocar todos os APs em uma única VLAN. Dessa forma evitando a mudança de IP durante o roaming dos usuários, e ainda nesse caso, um servidor DHCP não seria necessário. Usuários seriam então roteados como um grupo para dentro da rede corporativa usando um firewall e um roteador. Essa solução pode ser difícil de implementar, mas é aceita como uma metodologia padrão.
- Existem ainda muitas soluções no mercado em que o AP possui um servidor de VPN embutido e executa roteamento, inclusive protocolos de roteamento como o RIP.

# Uso da VPN




Roaming entre VLANs

# Balanceamento de Carga

- Áreas congestionadas com muitos usuários e alta carga de trafego por unidade, necessita de uma estrutura multi-célula. Nessa estrutura dois ou mais APs cobrem a mesma área o que aumenta o throughput agregado.
- Clientes dentro dessa área de cobertura comum, geralmente se associam com o AP menos carregado e que tem melhor qualidade de sinal. A eficiência é maximizada porque todos os APs estão trabalhando no mesmo nível de carga.
- Em muitos casos o balanceamento de carga é configurado no AP e nas estações.

# Referência

- Fonte: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless022.asp