Redes Sem Fio

Planejamento e Projeto de Redes Sem Fio 802.11x

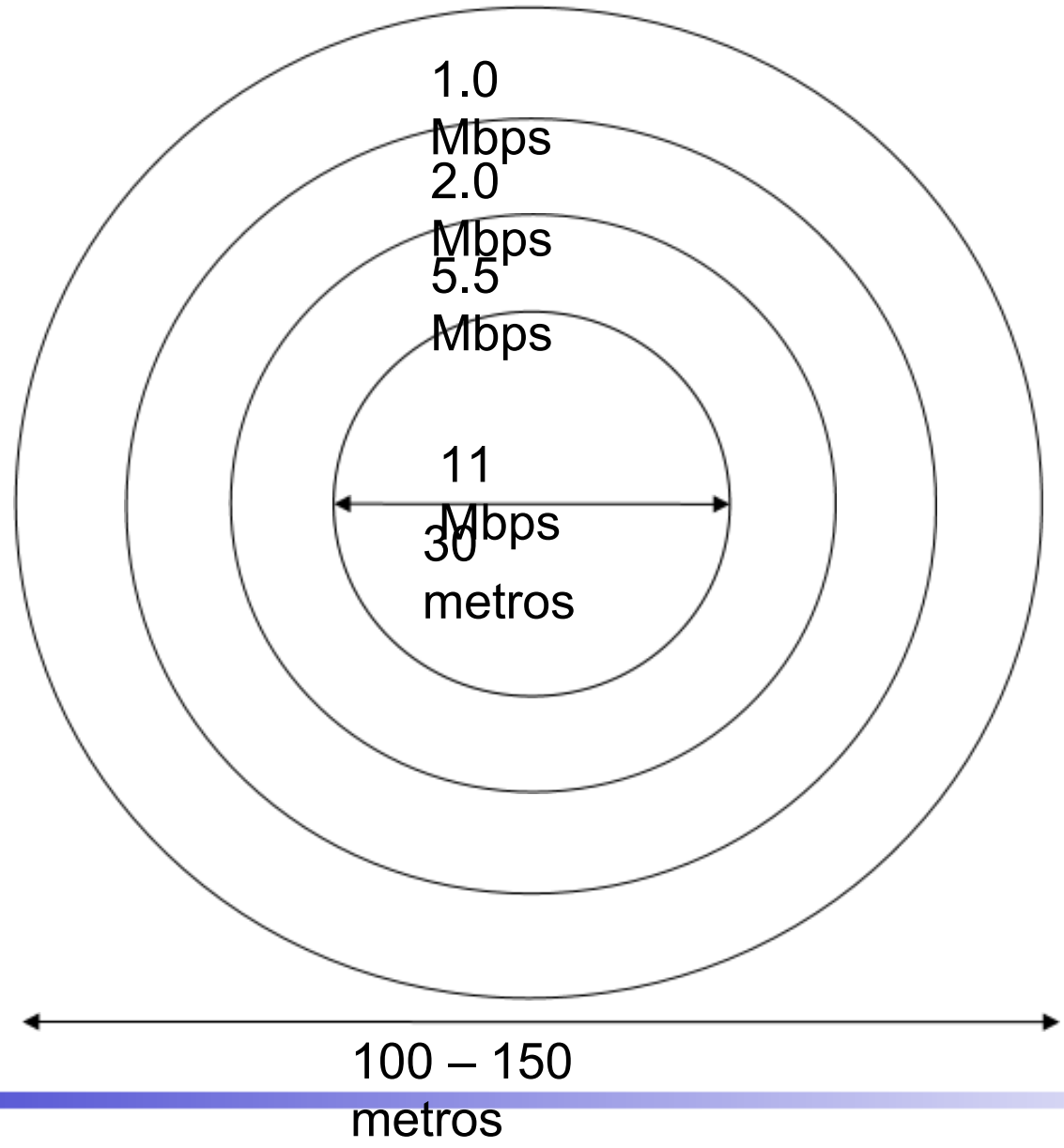
Sumário

- Considerações gerais sobre o projeto de redes sem fio
- Análise dos requisitos de capacidade e cobertura
- Realização de Site Surveys
- Aspectos de segurança

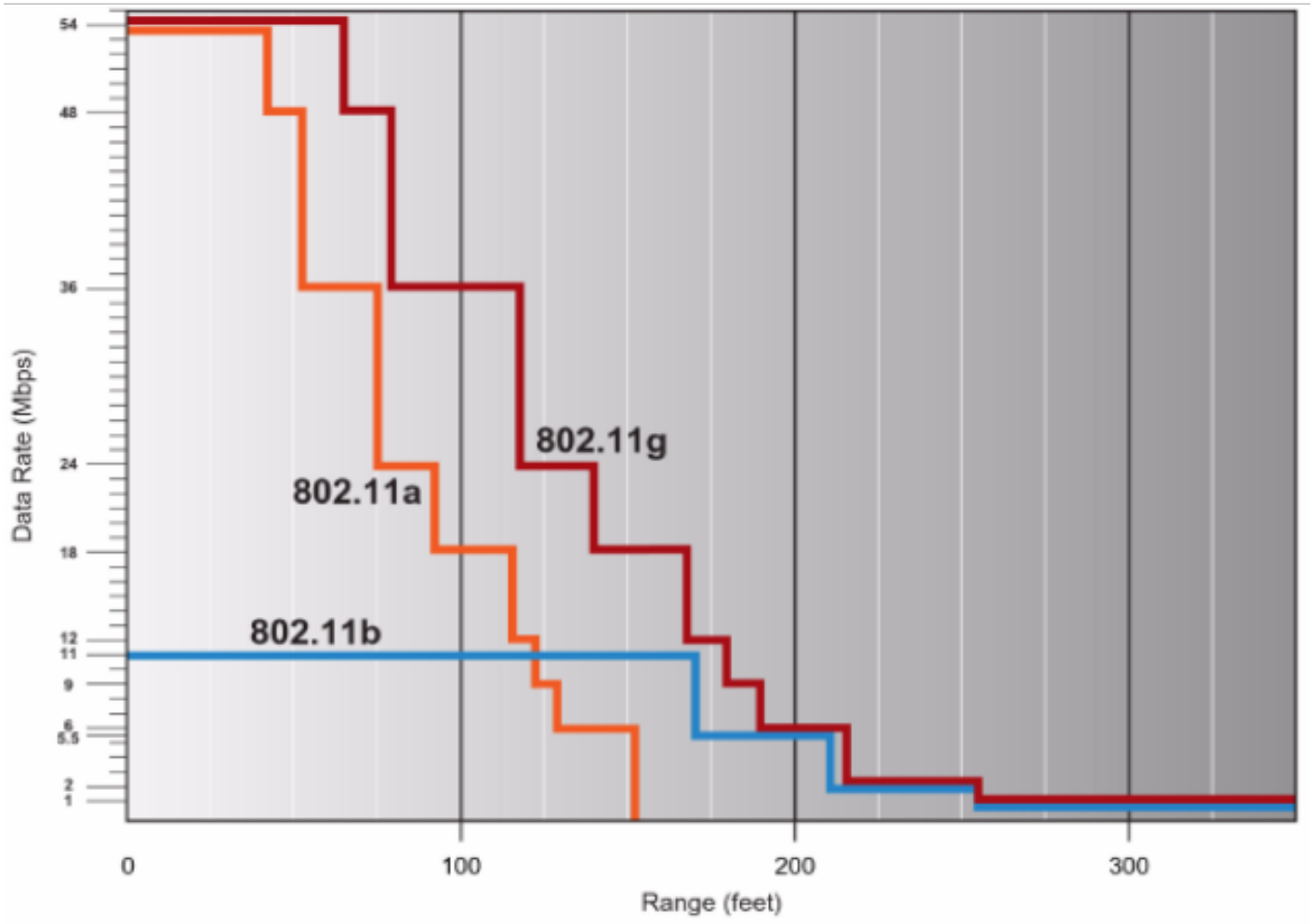
Questões relacionadas com o uso de RF

- Outros dispositivos competindo pela mesma faixa de freqüência
  - **dispositivos Bluetooth, telefones sem fio, forno microondas**
- Distâncias
  - **A força do sinal decresce com o quadrado da distância**
  - **Perdas na integridade do sinal e na largura de banda**
  - **Distância máxima depende do ganho da antena**
    - **padrão: 30m *indoors* e 100m *outdoors***
  - **802.11b: perda de 50% da largura de banda a cada 30m**
    - **o AP reduz a freqüência do sinal para facilitar sua penetração através de obstáculos; utiliza uma codificação mais robusta**
  - **Se houver uma única estação distante, a taxa é**

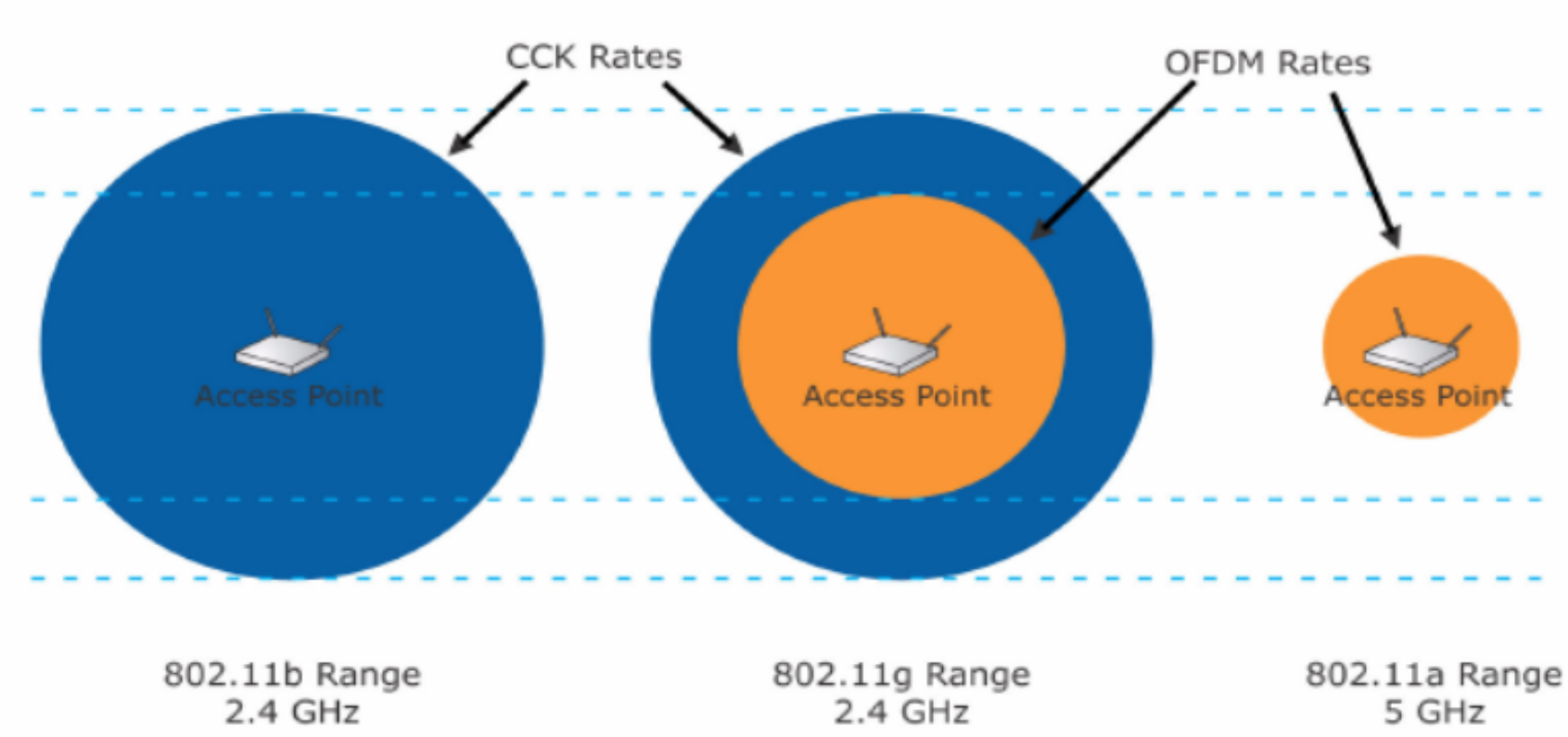
Raio de Cobertura vs. Taxa de Dados



Comparação: 802.11a/b/g



Comparação: 802.11a/b/g



Questões relacionadas com o uso de RF

- "Caixas de Metal"
  - **objetos metálicos ou magnéticos bloqueiam e absorvem o sinal**
- Objetos estacionários
  - **paredes, árvores e vegetação em geral, mobiliário**
  - **bloqueio e reflexão do sinal**
- Largura de banda compartilhada
  - **todos os dispositivos ativos em uma WLAN competem entre si pela largura de banda disponível**
  - **muitos dispositivos associados a um mesmo AP: reduz o desempenho global da rede**
    - **puro compartilhamento da banda**
    - **contenção pelo acesso**

Diferentes materiais e características de atenuação do sinal

- **Baixa atenuação:**
  - madeira, gesso, materiais sintéticos, amianto, vidro
- **Média atenuação:**
  - vidros com malha de metal, corpo humano, água, tijolos, mármore
- **Alta atenuação:**
  - cerâmica, papel, concreto, vidro blindado
- **Atenuação muito alta:**
  - metal

Qualificação do ambiente

- Escopo e tamanho da rede a ser instalada
- Número de nós a serem instalados/suportados
- Capacidade de suportar a largura de banda da rede sem fio
- Tipo de tráfego
  - **grande número de pacotes pequenos em rajada**
    - **e-mail, web**
  - **transferência de arquivos grandes**
  - **fluxo de dados contínuo**
    - **aplicações multimídia**
- Existência de espaços abertos, sem obstáculos, para colocação dos pontos de acesso
- Considerar a alternativa cabeada

Cobertura e Capacidade

- **Cobertura:** Prover o mesmo nível de sinal para todos os nós da rede

- **Capacidade:** Número de nós e quantidade de largura de banda compartilhada disponível para cada nó

Considerar a relação entre estes dois parâmetros

Cobertura da WLAN

- **Colocar o AP no centro da área a ser coberta**
- **Em grandes áreas:**
  - múltiplos APs com sobreposição do sinal (em canais diferentes)
  - evitar muita sobreposição do sinal para que *handoffs* não sejam tão freqüentes (tempo de *handoff)*
- **Vantagens de múltiplos APs**
  - um nível adicional de redundância (na falha de um AP, estações podem migrar para outro AP)
  - balanceamento da carga (capacidade utilizada) entre os APs

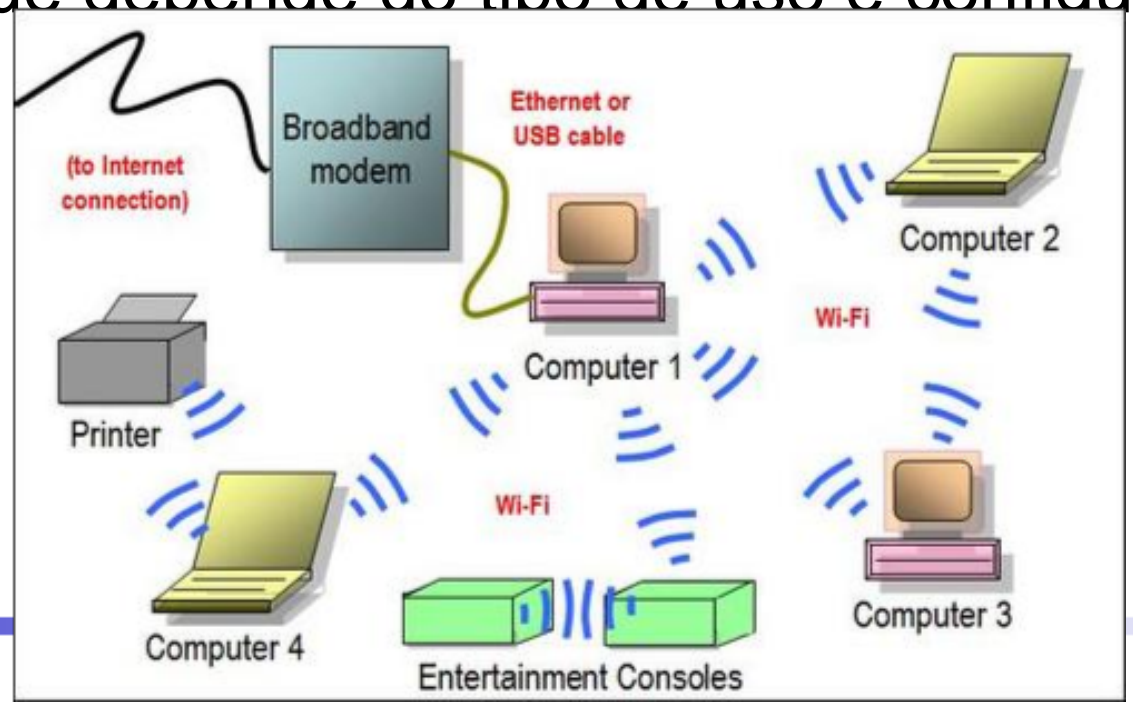
Capacidade da WLAN

- **Regra geral: 20 estações por AP**
  - capacidade do AP de suportar a quantidade de tráfego em um dado instante
  - depende do tipo de tráfego gerado pelos usuários
- **Exemplo: 802.11b, a 10 metros do AP**
  - 50 usuários ociosos na maior parte do tempo
  - 25 nós fazendo acesso a e-mail e arquivos pequenos
  - 10 a 15 nós ativos, transmitindo e recebendo arquivos de médio e grande porte
  - 20 nós: tráfego misto
- **Aumento da capacidade**
  - mais APs
  - uso de tecnologias com maior capacidade (ex.: 802.11 n)

Modo e Topologia da Rede

Modo ad hoc

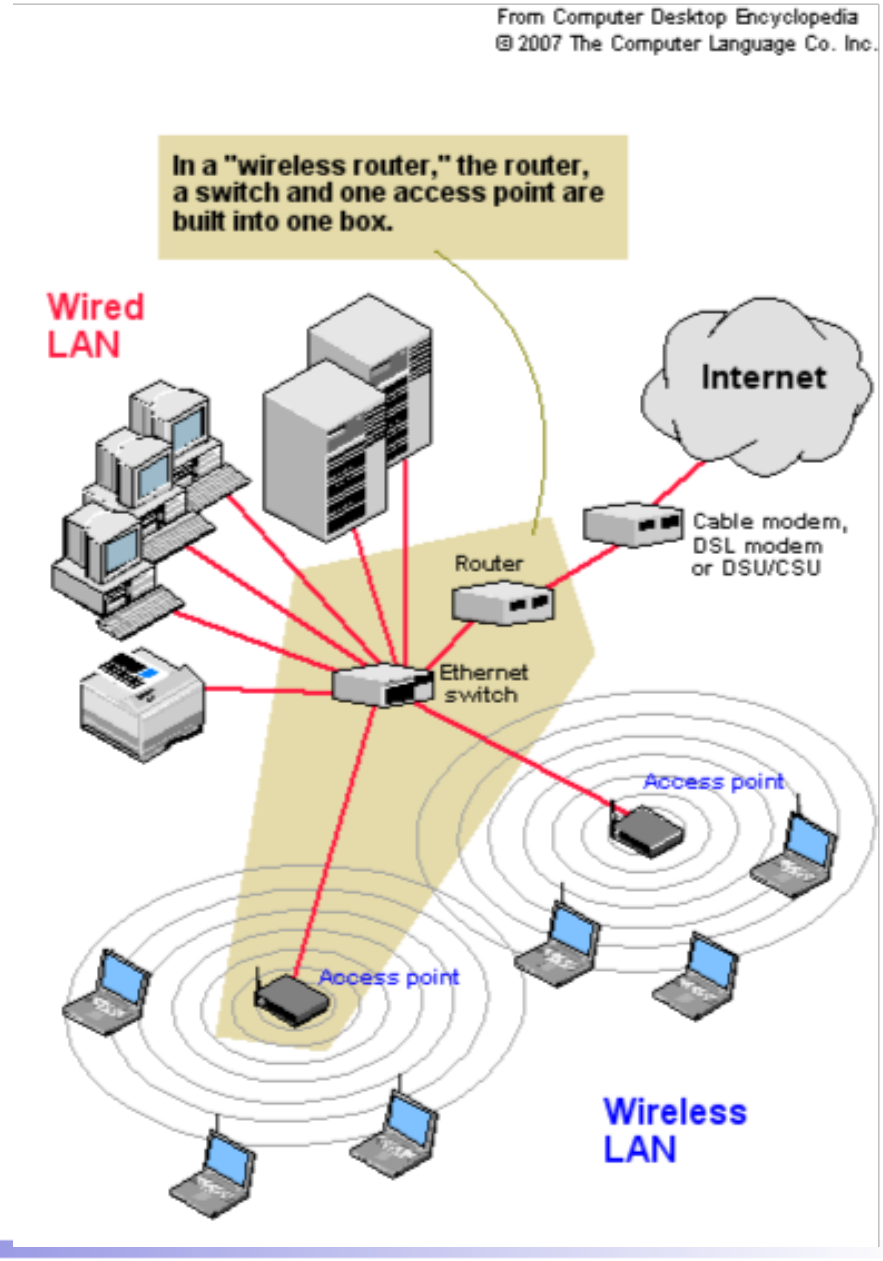
- estações se conectam entre si diretamente, formando um IBSS
- um dos nós da rede ad hoc pode se conectar a uma rede externa, podendo encaminhar tráfego da WLAN para a rede externa
- aplicabilidade depende do tipo de uso e configuração da WLAN



Modo e Topologia da Rede

Modo com Infra-estrutura

- default
- um ou mais APs inter-ligados (com ou sem fio)
- cada AP define um BSS
- o cojunto: ESS



Características da rede existente

Rede cabeada

- uso do servidor de DHCP já existente – uniformidade
- todos os APs dentro da mesma sub-rede IP
- vazão de dados suficiente para acomodar a WLAN

Rede sem fio

- a cobertura pode ser afetada com a adição de novos APs (sobreposição de sinal no mesmo canal de freqüência)
- capacidade: adição de novos nós pode necessitar novos APs
- compatibilidade: uso de padrões distintos
- topologia: adição de um AP pode forçar o modo com infra-estrutura (em uma rede originalmente ad hoc)
- expansibilidade: projetar a rede de forma a permitir seu crescimento incremental (nós e APs)

Site Survey

Objetivo:

- Obtenção de informação suficiente para planejar o número e localização dos pontos de acesso para fornecer a cobertura e capacidade desejadas

Levantamento dos níveis de ruído e interferência

- sinais gerados por outras fontes
- ex.: sinal de outra rede sem fio é considerado ruído

Levantamento sobre propagação e força do sinal

- testar as possíveis localizações dos APs
- evitar:
  - áreas de sombra (sem sinal ou com sinal fraco)
  - uso de mais recursos (APs) do que o necessário

Site Survey: Ruído e Interferência

Objetivo

- Identificar a distribuição da energia dentro da faixa de freqüência

Equipamento utilizado

- Analisador de espectro de RF ou laptop com cartão de rede sem fio e software de análise de espectro

Técnica

- Andar pelo local fazendo as medições de sinal nos pontos de interesse
- Durante um período de tempo estendido
- Registrar os resultados para análise (de preferência, com georreferenciamento)
- Antes da instalação dos APs

Uso dos resultados

- Planejar o uso eficiente dos recursos (orçamento)
- Determinar melhores canais ou mesmo entre 2.4 e 5GHz

Site Survey: Propagação e força do sinal

Objetivo

- Identificar o padrão de cobertura do sinal, a força do sinal e as taxas de dados alcançáveis em cada local onde uma estação móvel poderá ser utilizada

Equipamento utilizado

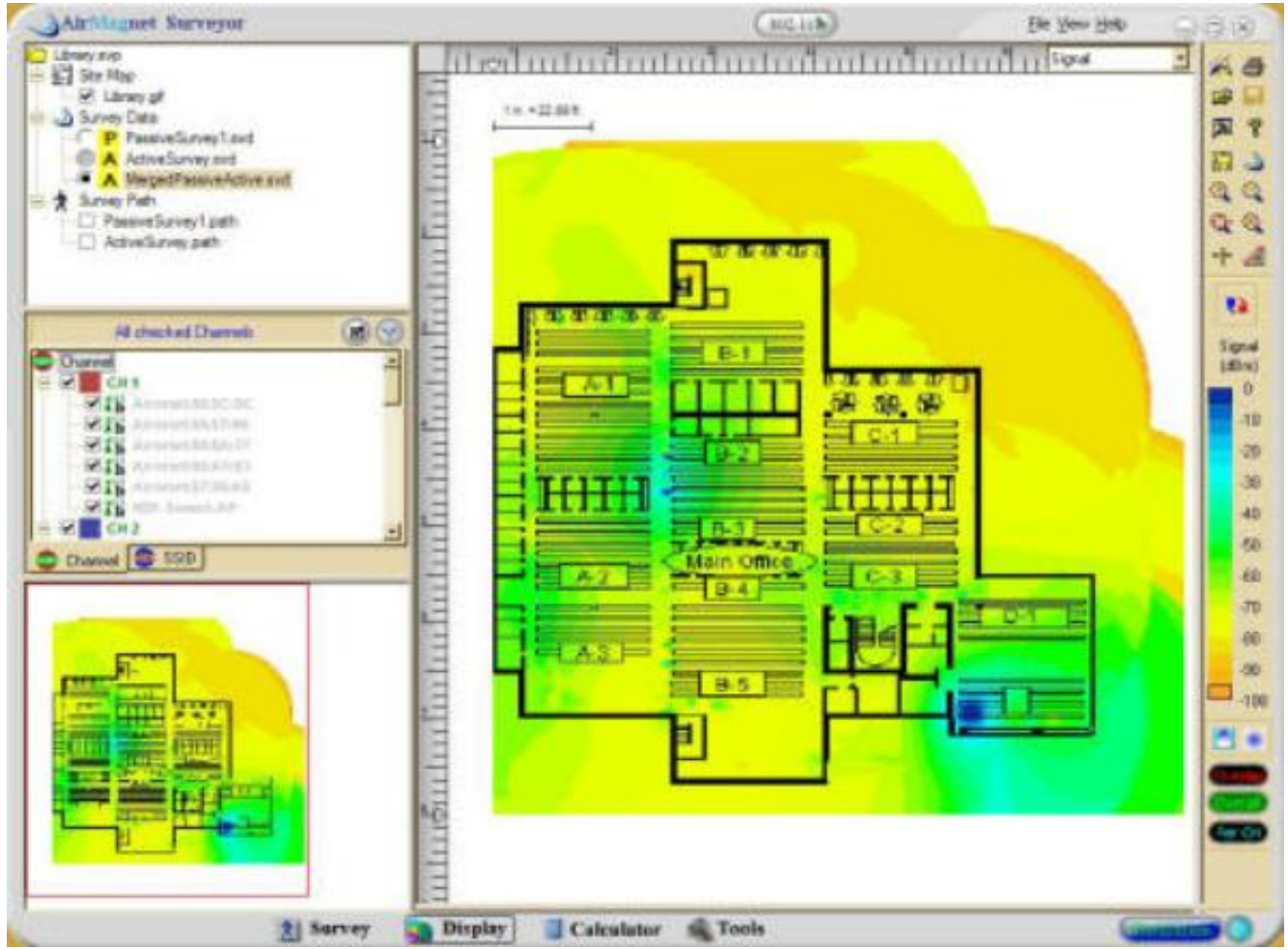
- Laptop ou handheld com cartão de rede sem fio e software de site survey
- Hardware idêntico ao que será utilizado em produção
- Georeferenciar os dados (GPS)

Técnica

- Alocação preliminar dos APs
- Andar pelo local medindo a força do sinal recebido e a taxa de dados

Resultados: planejamento do layout físico da rede

Site Survey: Software



Arquitetura Física da Rede

Número de APs

- considerando a área a ser coberta e o raio de distância dos APs dentro da taxa de dados desejada
- não ignorar o efeito de obstáculos (info do site survey)

Localização ótima das antenas/APs

- omnidirecional: próximo ao centro da área a ser coberta
- próximo ao teto, livre de obstáculos
- posicionamento específico se antena unidirecional

Canal de operação

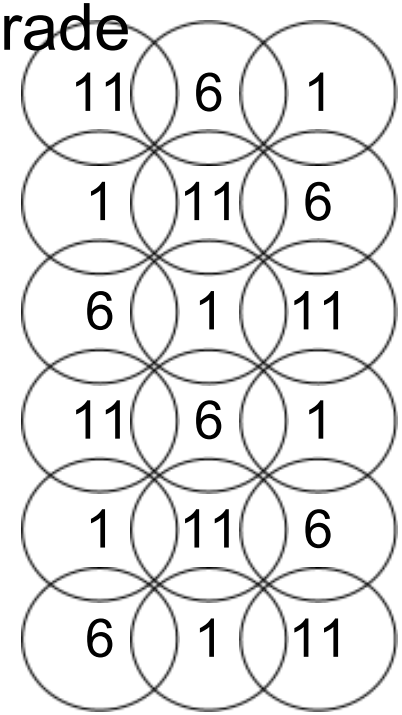
- evitar canais que tenham ruído de fundo ou esporádico significativo

Controle da potência do sinal

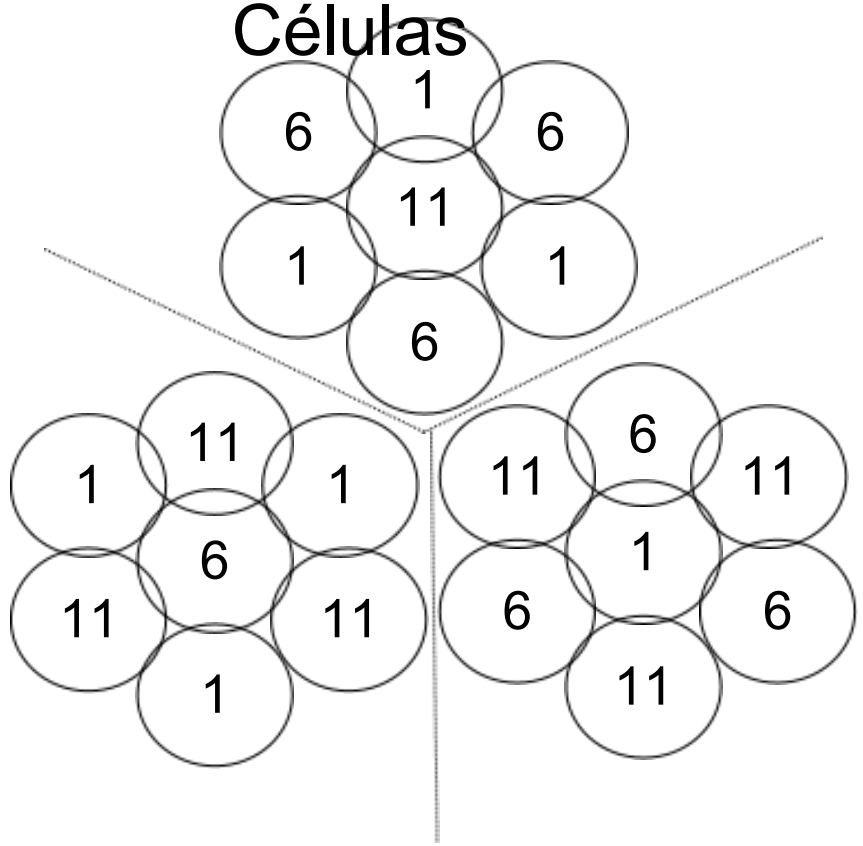
- se necessário restringir a área de cobertura (discutir a necessidade)

Padrões de alocação de canais

Padrão em Grade



Padrão em Células



802.11 b/g

Teste Piloto

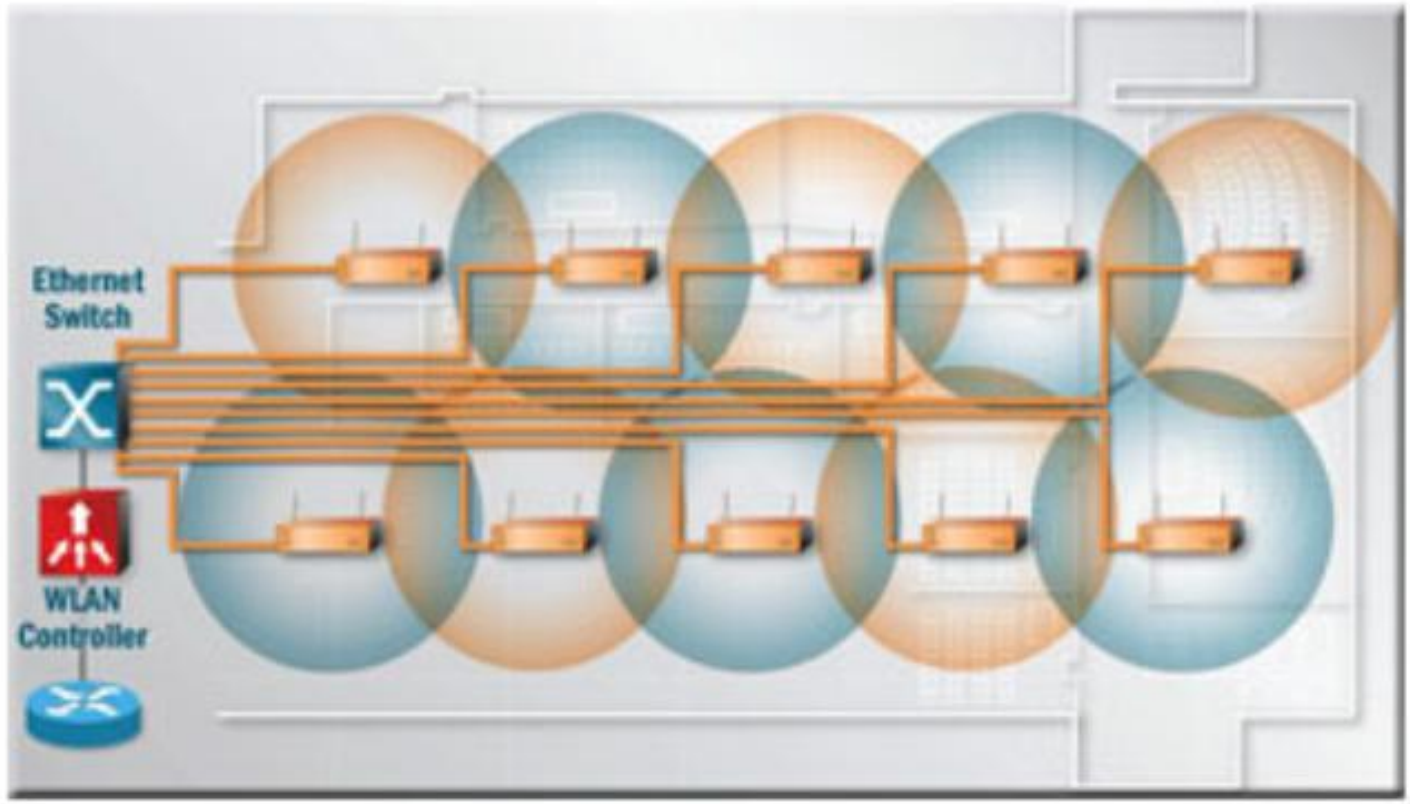
Implementar e avaliar o design proposto em local/situação de uso real

- em locais onde mais problemas foram detectados no site survey
- monitoramento do uso diário da rede
- submeter a rede a condições extremas: grande quantidade de tráfego, vários usuários concorrentes
- logs para análise
- questionários/consultas aos usuários

Instalação da Rede

- **Cabeamento Ethernet para os APs**
- **Instalar, configurar e testar um AP de cada vez**
  - juntamente com as estações a ele associadas
- **Fat APs**
  - todas as funções de configuração em cada AP
- **Thin APs**
  - APs desempenham apenas a função de ponto de acesso
  - configuração feita através de um único controlador para toda a rede
  - APs obtêm configuração a partir do controlador

Thin APs e Controladores



Configuração dos APs

- Endereço IP (para administração via Web)
- SSID
- SSID broadcast
- Potência máxima de transmissão
- Canal de rádio
- Modo de operação (802.11b/g ou somente g)
- Segurança (WEP, WPA etc)
- Configuração de antena

Configuração das Estações

- Modo da rede (ad hoc ou infra-estrutura)
- SSID
- Canal de rádio
- Modo de operação (802.11b/g ou apenas g)
- Segurança

Segurança em Redes 802.11

- Principais ameaças
- WEP
- WPA e autenticação (RADIUS)
- IEEE 802.11i e WPA2
- Medidas de segurança típicas

A natureza do problema

- **O sinal pode se propagar além dos limites físicos desejáveis**
  - acessível a qualquer um que esteja dentro da cobertura do sinal
  - riscos:
    - captura de dados privativos
    - roubo de largura de banda da conexão com a Internet
- **Não se pode confiar na técnica de modulação e transmissão por espalhamento de sinal**
  - qualquer receptor padrão é capaz de decodificar
- **War Driving e War Walking**
  - mapear redes sem fio existentes
  - War Chalking: identificar redes para acesso público

Principais ameaças

Negação de Serviço (DoS)

- inundar os APs com pedidos de associação e autenticação

Jamming

- inundar a faixa de RF com interferência (DoS no nível físico)

Ataques de Inserção

- conectar estações não-autorizadas a um AP

Ataque de Replay

- interceptar tráfego de autorização (como chaves ou senhas) e depois usá-lo para ganhar acesso não autorizado

Monitoramento de Broadcast

- se AP conectado a HUB: acesso a tráfego da rede fixa

Principais ameaças

ARP Spoofing

- corromper as tabelas ARP para que tráfego seja direcionado para a estação intrusa

Seqüestro de Sessão (man-in-the-middle)

- faz-se passar por uma estação sem fio e requisita sua desassociação do AP
- faz-se passar pelo AP e reassocia a mesma estação consigo

Rogue Access Point (ataque do gêmeo mau)

- instala um AP não-autorizado com o mesmo SSID
- aumenta a potência do sinal desse AP para fazer com que os clientes se associem com ele

Ataque Criptoanalítico

- explora uma fraqueza do sistema para quebra de código

Ataques no Canal

- uso de informações do nível físico
  - consumo de energia, temporizações, emissões eletromagnéticas
- para obter informações sobre o sistema criptográfico
- permite obter a chave de criptografia diretamente ou uma mensagem em plain text a partir da qual a chave pode ser computada

Segurança em Redes Locais Sem Fio

Autenticação dos usuários

- confirmar que o usuário é quem diz ser

Controle de acesso

- permitir acesso à rede apenas a usuários autorizados

Privacidade dos dados

- criptografia dos dados transmitidos

Gerenciamento de chaves

- criação, proteção e distribuição das chaves usadas para encriptação de mensanges

Integridade das mensagens

- garantir que mensagens não sejam modificadas durante a transmissão

WEP

Uso de chave secreta

- configurada no AP
- distribuída (por meios externos, na maioria das vezes, manual) para estações autorizadas
- usada par encriptar os dados

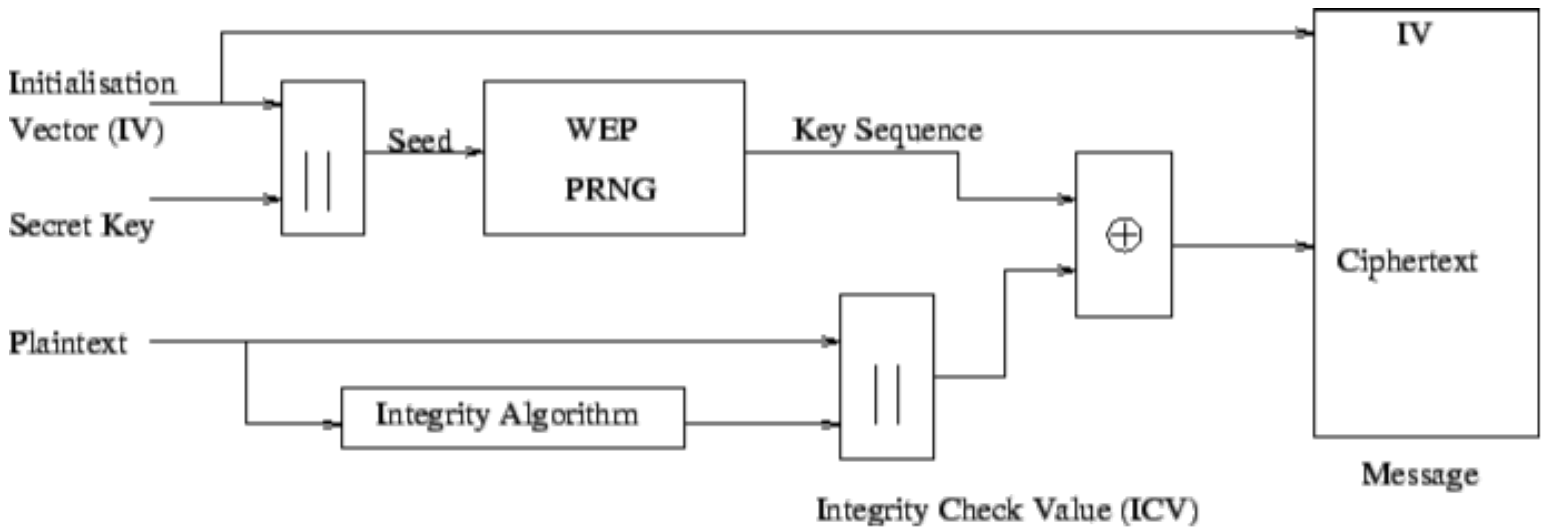
Chaves secretas de 40 ou 104 bits

- combinada com vetor de inicialização de 24 bits para gerar chaves de criptografia de 64 e 128 bits
- independente do tamanho da chave, pode-se derivar a chave a partir da análise de cerca de 4 milhões de quadros!

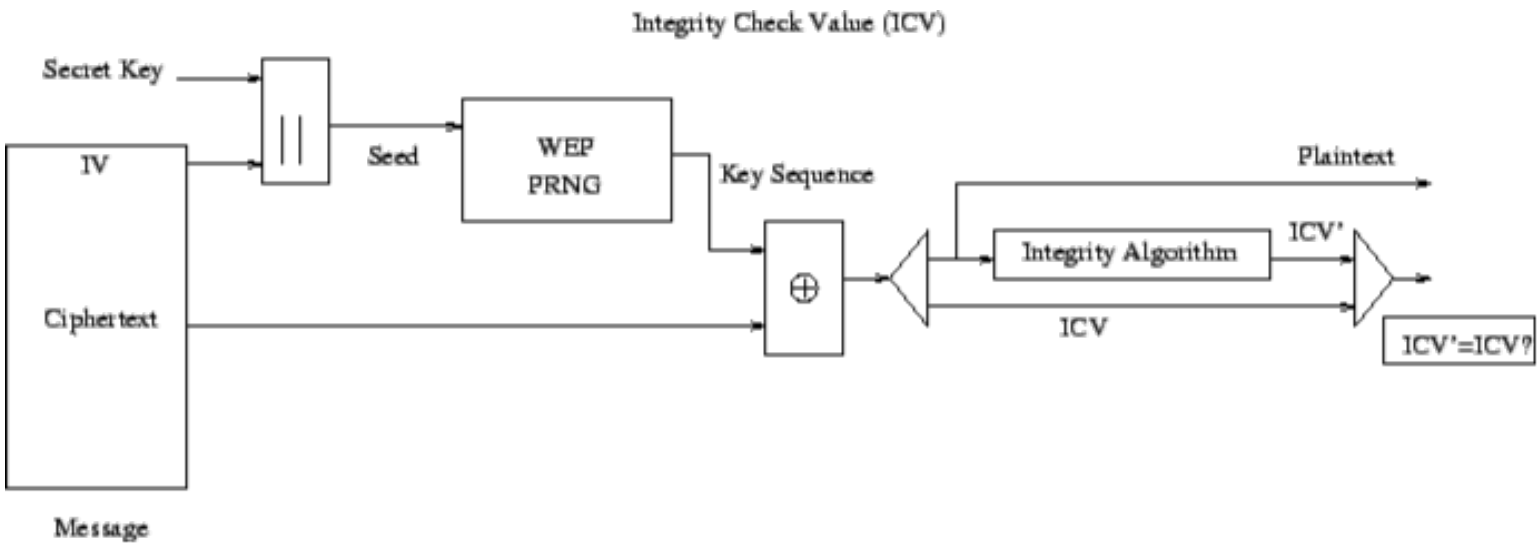
Encriptação

- seqüência de dados XOR seq. de bits pseudo-aleatória
  - *keystream* criada utilizando o algoritmo RC4

Encriptação



Decriptação



Crítica

- IV (vetor de inicialização) muito curto: 24 bits, independentemente do tamanho da chave: repetido com freqüência e incluso no ciphertext
  - pode ser utilizado para extrair a chave de criptografia após um número “não muito grande” de tentativas
- Não há um mecanismo para troca dinâmica da chave
  - a mesma chave permanece em uso por tempo suficiente para dar a oportunidade de quebrá-la (o que não demora mais do que alguns minutos!)

Solução intermediária

- Reforçar o uso de WEP
  - algum mecanismo para troca (distribuição) de chaves com freqüência (em 802.1X)
- Utilizar filtragem de endereços MAC

WPA

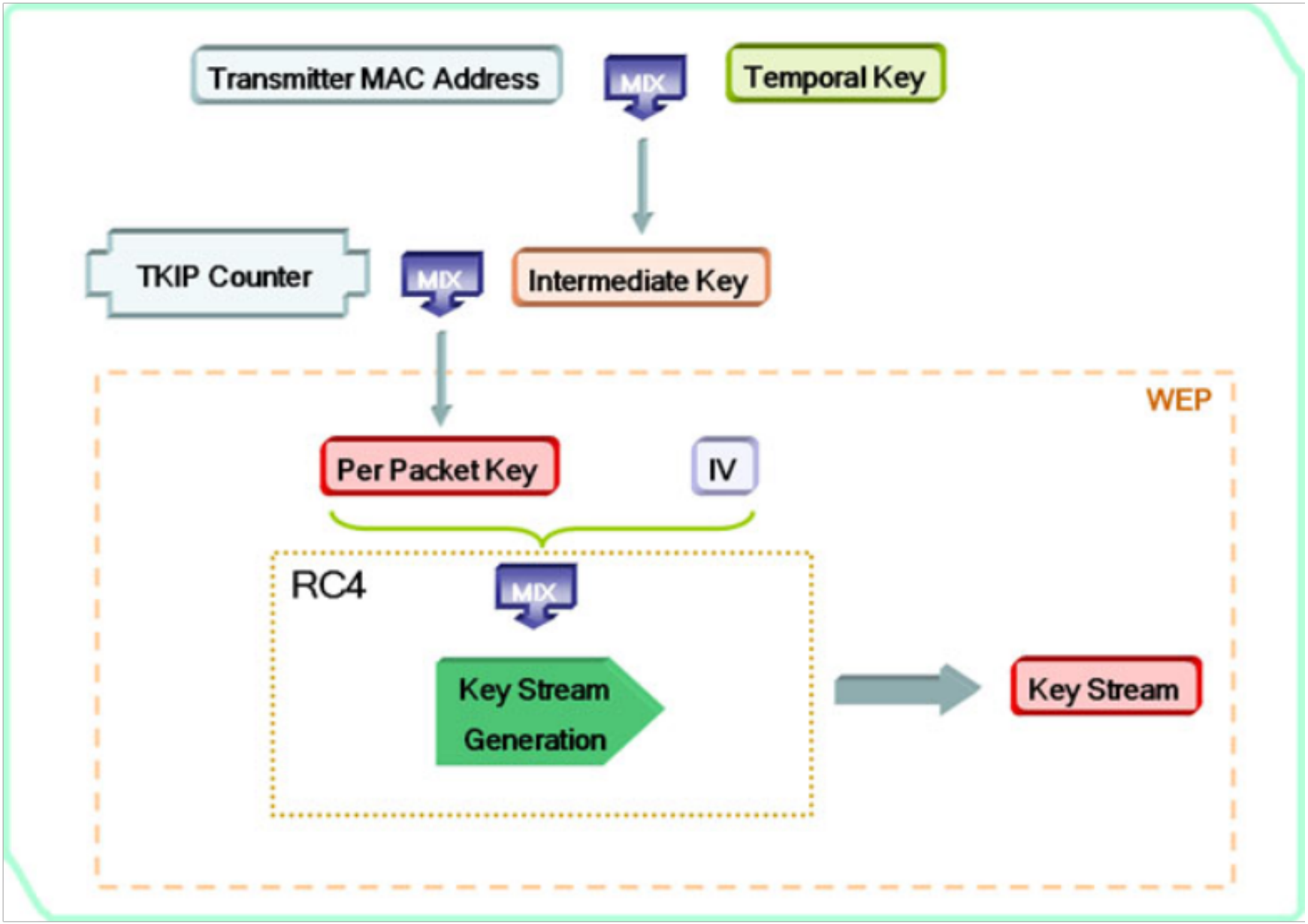
Procura eliminar a vulnerabilidade de WEP

- Chaves dinâmicas (de 128 bits)
  - Protocolo para criação e distribuição de chaves: TKIP
  - Chave
    - criada para cada sessão (estação-AP)
    - pelo protocolo de autenticação ou manualmente
- Vetor de inicialização maior (48 bits)
- Função de checagem da integridade das mensagens
- Pode ser considerado um WEP dinâmico (usa RC4)

TKIP (Temporal Key Integrity Protocol)

- cálculo da chave:
  - chave temporal + end. MAC + contador TKIP + IV de 48 bits
- distribui chaves periodicamente
  - intervalos de 1 a 10.000 pacotes
- MIC (message integrity code)

WPA = TKIP + WEP


Transmitter MAC Address
MIX
Temporal Key
TKIP Counter
MIX
Intermediate Key
WEP
Per Packet Key
IV
RC4
MIX
Key Stream Generation
Key Stream

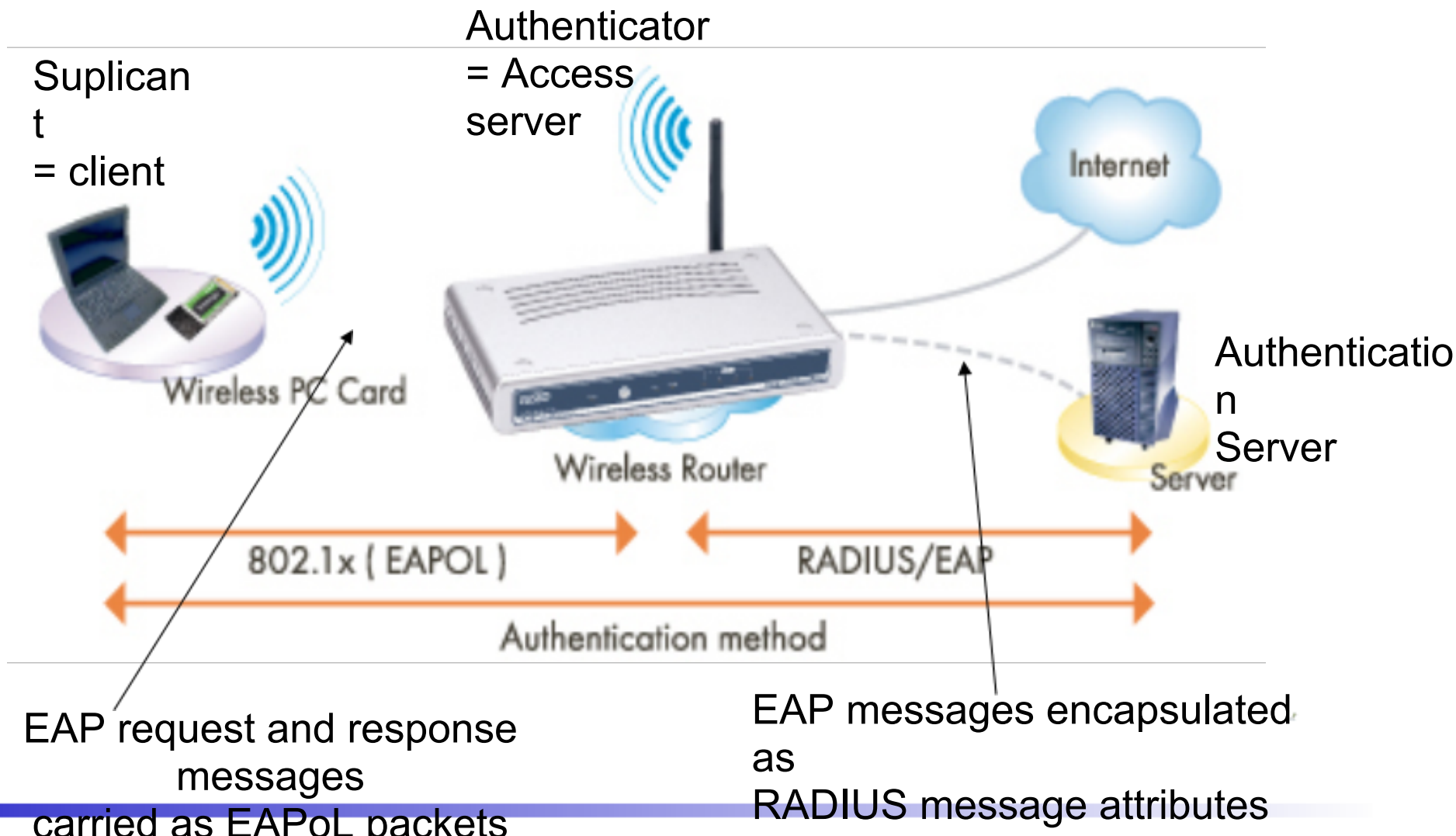
Medidas de segurança adicionais

- Se uma violação é detectada através do cálculo do MIC
  - o que pode significar que uma chave foi quebrada
- Todas as chaves são resetadas
- Aumenta-se a taxa de atualização de chaves
- Envia alerta para o administrador da rede
- Opcional:
  - desautentica todas as estações
  - shutdown do BSS por 1 minuto caso o AP receba uma sucessão de pacotes forjados

Autenticação

- Primeiro passo na associação: não associa se não autenticar
- 802.1X
- Configuração mais comum: servidor de autenticação

Autenticação com RADIUS



EAP (Extensible Authentication Protocol)

- usado na camada de enlace para passar informação de autenticação entre o suplicante e o servidor de autenticação
- tanto para redes cabeadas quanto para redes sem fio
- em redes sem fio, o AP funciona como um autenticador, mas desempenha esta função fazendo uso do servidor de autenticação propriamente dito
  - um intermediário entre o suplicante e o servidor de autenticação
- Vários tipos de EAP são permitidos
  - EAP-TLS: utiliza certificados de cliente e servidor
  - EAP-TTLS e PEAP: apenas certificado do servidor – dados de autenticação do cliente (ex.: usuário e senha) são passados para o servidor encriptados com sua chave pública
- Requer uma PKI (Public Key Infrastructure) para validar os certificados

802.11i e WPA2

802.11i

- criptografia mais forte (AES)
- autenticação
- gerenciamento de chaves
- conceito de RSNs (*Robust Security Network*)
  - negociação do protocolo de confidencialidade durante associação do dispositivo
  - sistema de chaves: chaves unicast e chaves de grupo
  - TKIP e AES
- cache de chaves e pré-autenticação: *roaming* mais rápido

WPA2

- implementação do padrão 802.11i pela Wi-Fi Alliance
- substituto para WPA a partir de 2004

WPA e WPA2: Modos de autenticação

Enterprise Mode

- autenticação automática via 802.1X / EAP

Personal Mode

- PSK – Private Shared Key
  - configuração manual de chaves
  - cliente autentica se possuir a chave correta
- apenas viável em redes de pequeno porte (SOHO)

Discutir a aplicabilidade de cada um

Medidas Gerais de Segurança I

Política de segurança

- requisitos de controle de acesso, uso de senhas, encriptação, controle da instalação de equipamentos etc

Avaliação dos riscos

- qual o valor dos dados/acesso e as potenciais conseqüências de acesso não-autorizado?

Inventariar todos os APs e dispositivos sem fio

- por varredura do espaço de RF e análise de logs

Colocação dos APs no interior do prédio

- reduzir “vazamento” de RF para fora

Colocar os APs em locais seguros

- e desabilitar gerenciamento a partir da própria rede sem fio

Medidas Gerais de Segurança II

Trocar o SSID default e desabilitar SSID broadcast

Desabilitar protocolos de gerenciamento não essenciais nos APs

Troca periódica de chaves compartilhadas

Listas de controle de acesso de endereços MAC

Na administração dos APs

- habilitar autenticação de usuário e usar senhas fortes

Implantar Autenticação de usuários

Detecção de Intrusão

Manter o firmware atualizado (APs e NICs)

Manter e examinar os logs com freqüência

Quando dispositivos são descartados

- resetar (zerar) a configuração

Segurança de Hot Spots

- Setup da conexão de rede para conectar-se apenas a APs preferenciais
- Utilizar VPN para conexão com rede da empresa
- Instalar uma firewall pessoal em estações móveis que utilizam hot spots
- Proteger os arquivos nas estações móveis utilizando criptografia no sistema de arquivos e desabilitar compartilhamento de arquivos
- Proteger dados transmitidos ao AP (usar SSL)
- Desabilitar a NIC sem fio quando não estiver em uso
- Manter o SO e software de segurança sempre