Gerência e Segurança de Redes Wireless

Claudia Pereira

clpereir@cisco.com

Aplicações Interativas X Aplicações Transacionais

1950s-1990s

Cartas e memorandos definiam as comunicações entre as empresas e os clientes

1990s-2002

Voice Mail and Email passam para o cotidiano das empresas; expectativas the respostas no mesmo dia.

Hoje

Aplicações móveis em tempo real passam a existir, criaram um ambiente de negócios Interativos.

Os mundo de hoje requer Conectividade em qualquer lugar a qualquer hora.

Os usuários precisam de mobilidade de verdade …

Estudo NOP — Wireless LANs Aumentam a Produtividade

Baseada em pesquisa em mais de 300 organizações americanas, com mais de 100 funcionários:

- Usuários ficam em média 1¾ mais horas por dia conectados a sua rede corporativa
- Média de economia de tempo por dia: 70 minutos
- Produtividade: +22%

Source: NOP World-Technology, Sept. 2001

Barreiras para a Adoção de WLAN

- **Segurança**
- **Implantação e Gerenciamento**
- **Custo Total (TCO)**

WLAN TCO Estimates

Capital exp. (CapEx)	15%
Operational exp. (OpEx)	85%

Source: META Group, 2003

Para minimizar os custos de operação (OpEx), o sistema WLAN deve ser confiável, seguro e gerenciável.

Resumo dos Problemas Percebidos:
Falta de um sistema WLAN que minimize os custos de implementação e operação de uma solução WLAN segura, confiável e com alto desempenho, para empresas de diversos tamanhos.

Principais Ameaças

- Rogue AP: Funcionários criam uma porta de entrada para a rede corporativa
- Ad Hoc: Conexões cliente-cliente, não passam pelos mecanismos de segurança implementados
- Ataques DoS: Hackers maliciosos utilizam a WLAN para interromper serviços críticos
- APs externos: Funcionários se conectam em uma WLAN externa e abrem uma porta de entrada para a rede corporativa

Alguns Mitos sobre Segurança em WLAN

Se não implemento WLAN, tenho segurança na rede.

- Um único “rogue AP” na rede, é um enorme risco!
- As medidas de segurança tradicionais não são suficientes nesse caso.
- O risco pode ser criado pelos próprios funcionários.

Um site-survey periódico utilizando um laptop é suficiente.

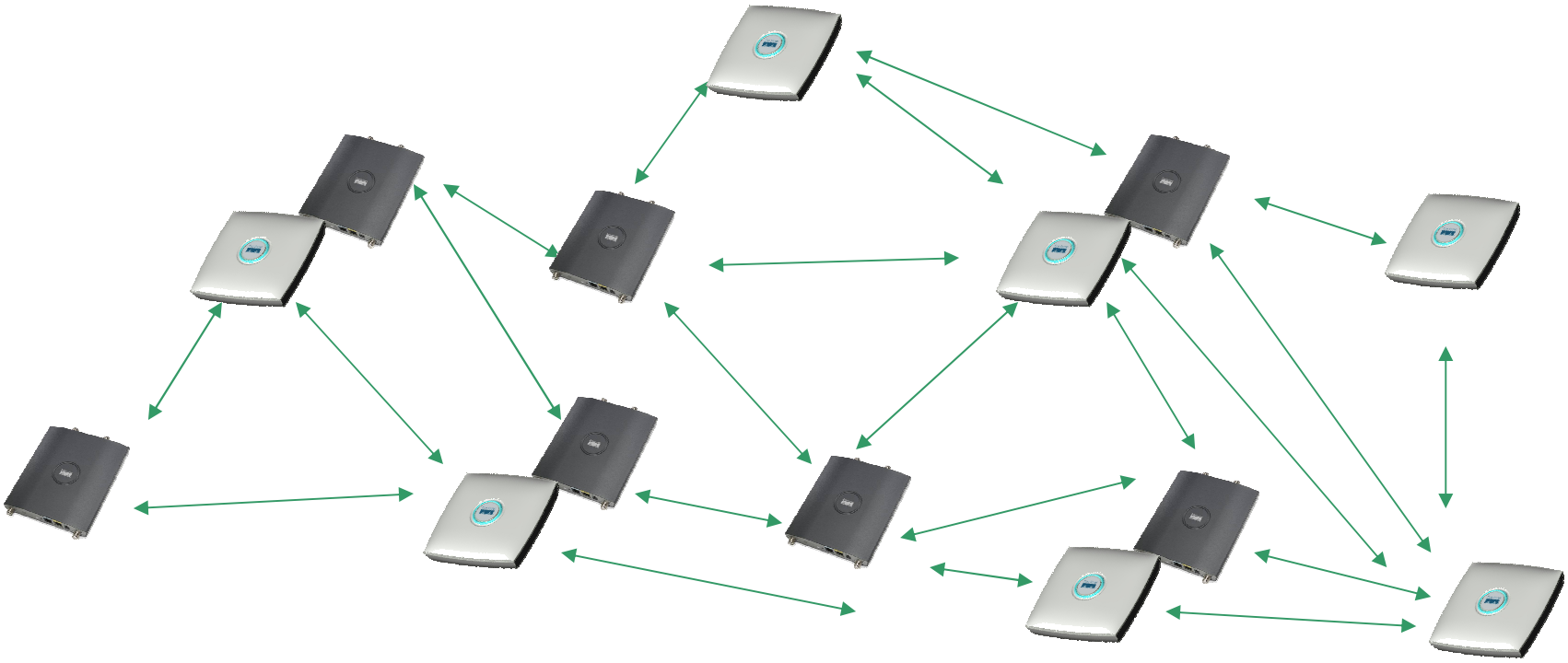
- Você liga seu firewall periodicamente?
- Não é prático para localidades remotas.
- Consome tempo, esforço e dinheiro.

Eu utilizo 802.11i, WPA ou VPN, logo minha WLAN é segura.

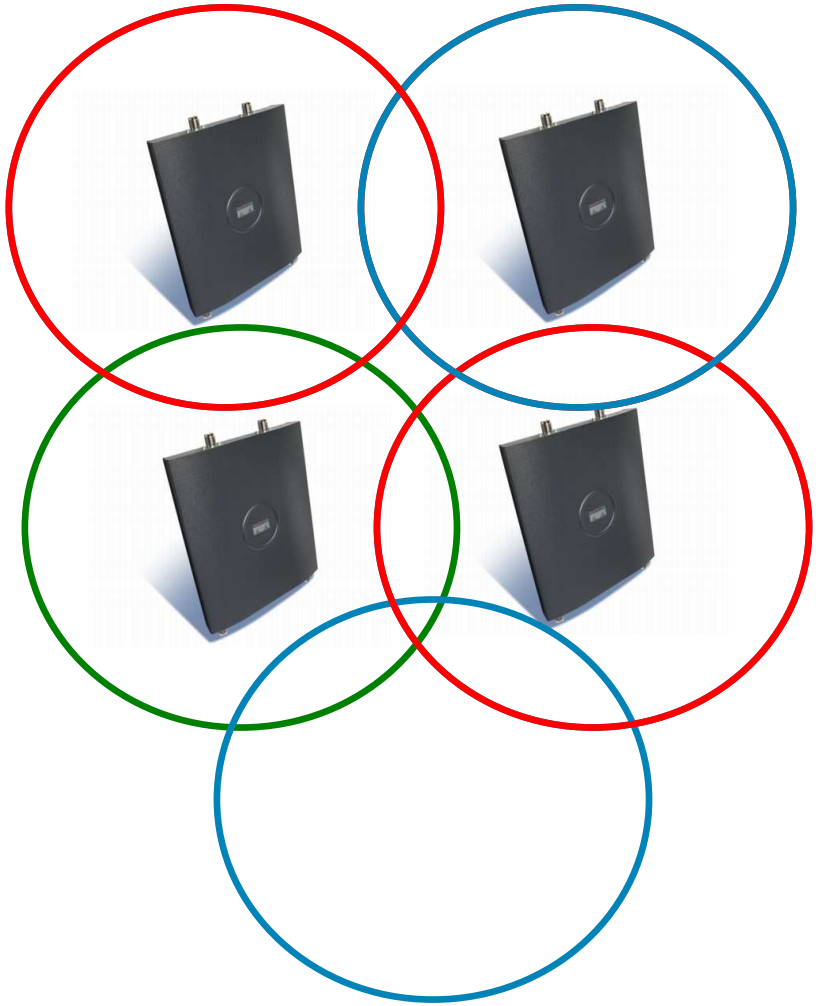
- Somente protege os clientes autorizados
- Não tem impacto sobre uma infra-estrutura ou conexões não autorizadas.

Soluções Autônomas Oferecem Pouca Coordenação

- Cada AP tem sua própria visão da rede
- Não existe uma visão hierárquica da rede RF



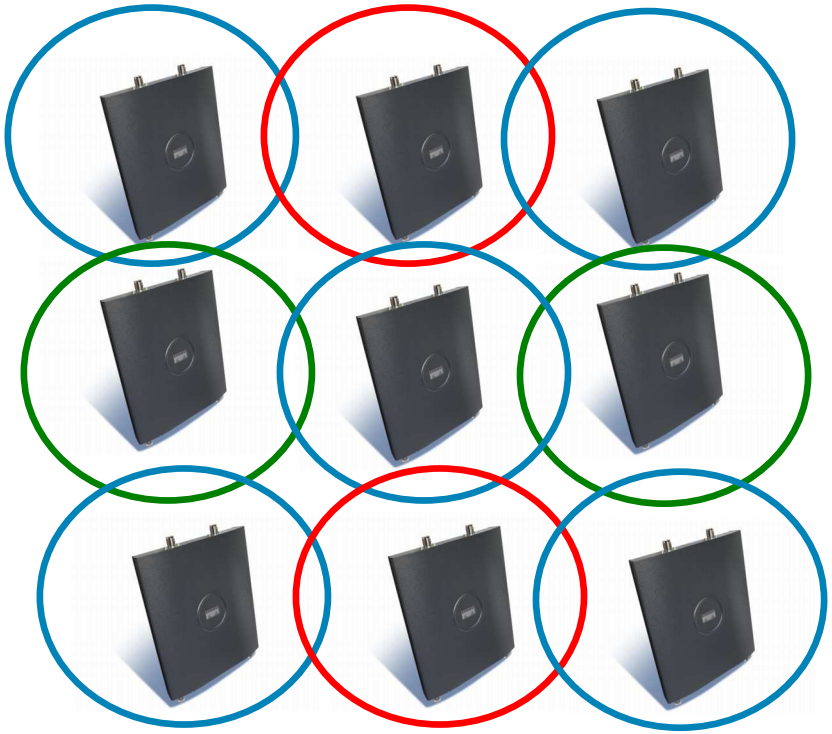
Interferência entre Canais RF



Mais um AP para suportar um maior número de clientes.

Ou alguma interferência.

Configuração de Canais RF



Situação com 9 APs

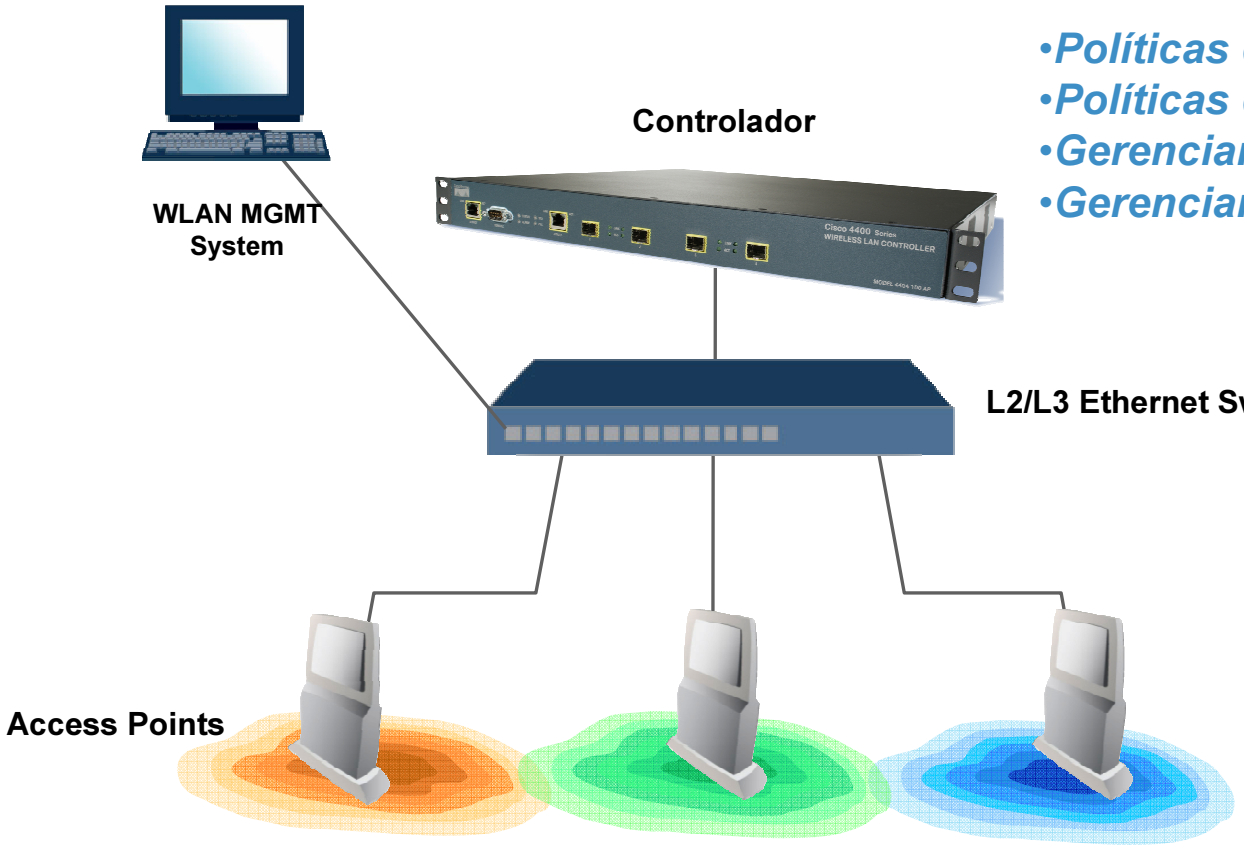
Princípios Básicos da Centralização

- **Visão holística da rede sem fio**

  Os APs enviam informações para um dispositivo central, que tem uma visão completa da rede

- **Os níveis de sinais de cada AP são conhecidos (SNR – Signal- to-Noise Ratio)**
- **Todos os dispositivos de clientes são conhecidos**
- **Dispositivos distribuídos só podem ser controlados por um dispositivo central**

Conceito Básico



- *Políticas de Segurança*
- *Políticas de QoS*
- *Gerenciamento RF*
- *Gerenciamento Móvel*

- *Interface Remota RF*
- *Encriptação camada MAC*
- *Monitoramento Aéreo*

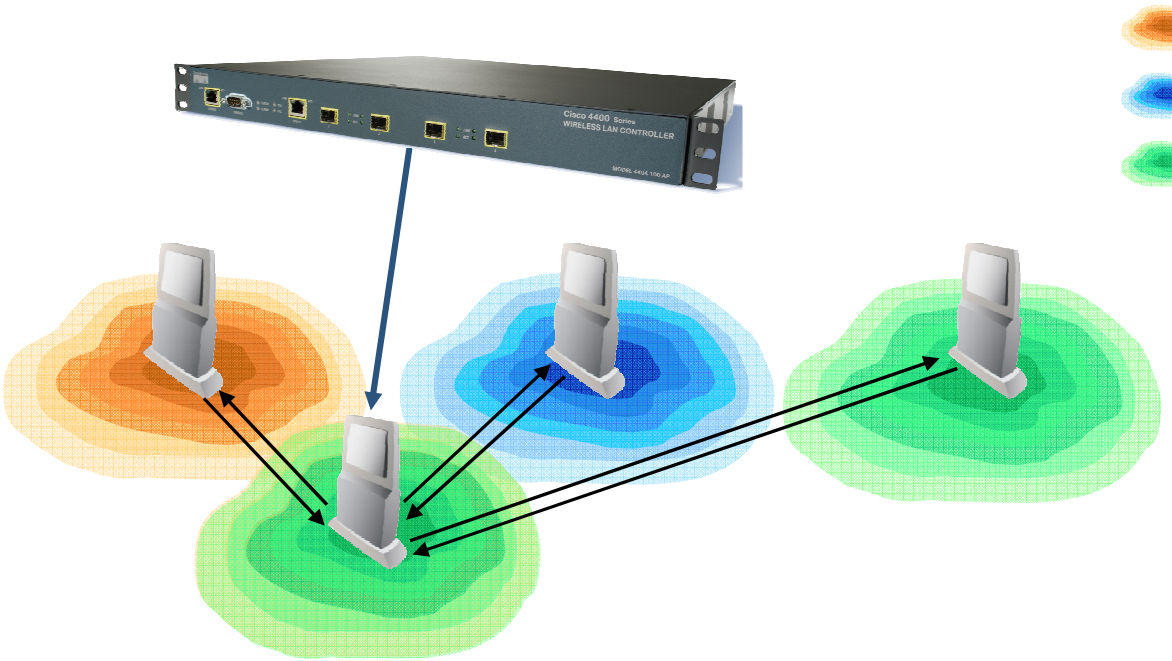
Arquitetura Centralizada
Benefícios em Segurança

- A configuração não é mantida no AP
  - A configuração é automaticamente carregada do controlador para o AP usando criptografia.
- APs autenticados pelo controlador por certificado X.509
- O controlador pode fazer autenticação por MAC dos APs
- O controlador é autenticado pelo AP por certificado
- Os APs não tem gerência remota
  - Não tem SNMP
  - Não tem Telnet, SSH X.509

Configuração Centralizada e Gerência de RF (Canal e Potência)

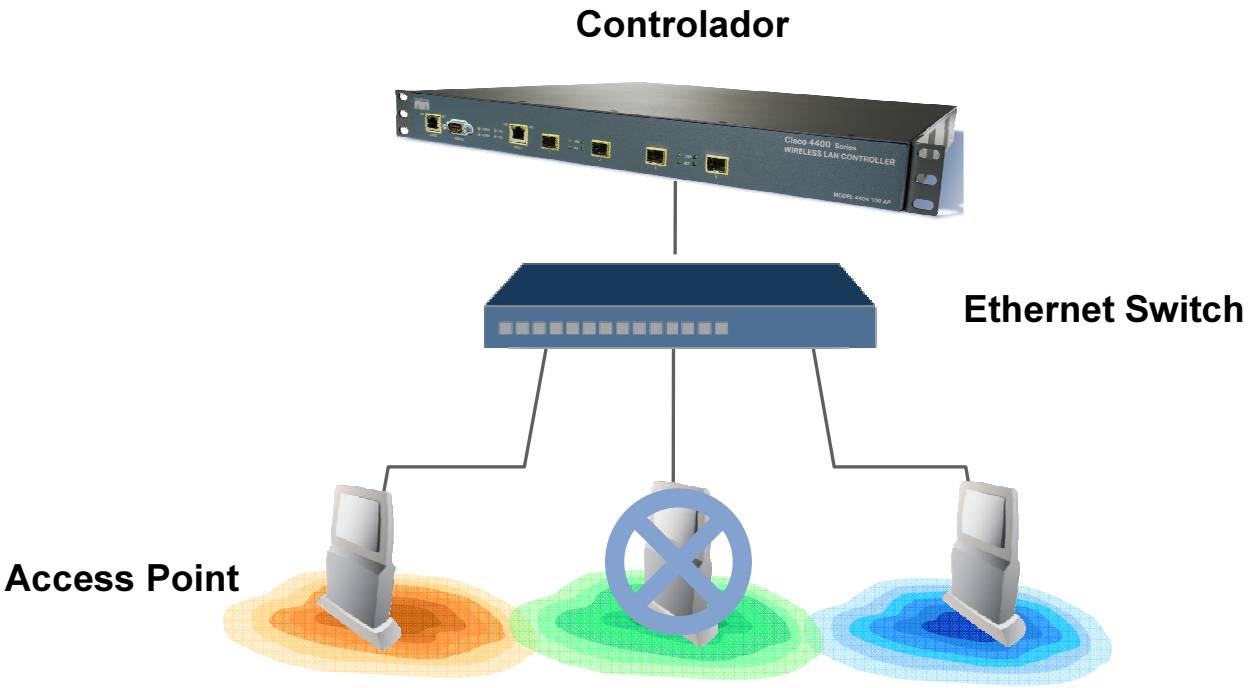
Alocação dinâmica do canal

Otimização dinâmica da potência



- Elimina buracos na cobertura
- Otimiza a área de cobertura
- Evita interferência / Melhora o desempenho
- Reduz a intervenção manual na administração da rede

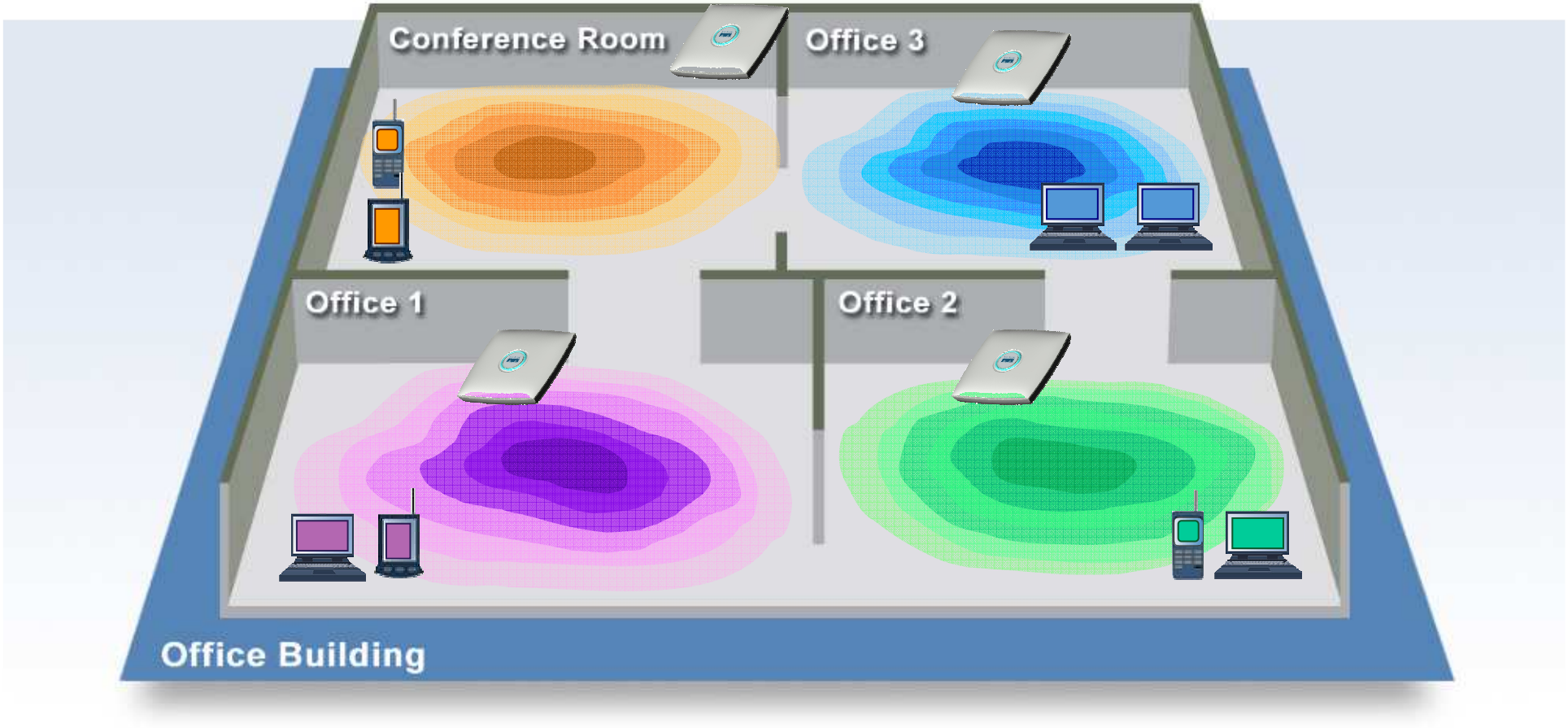
Redundância Embutida na Solução
Redundância de AP



Melhor Desempenho para a Rede WLAN

Balanceamento Dinâmico da Carga

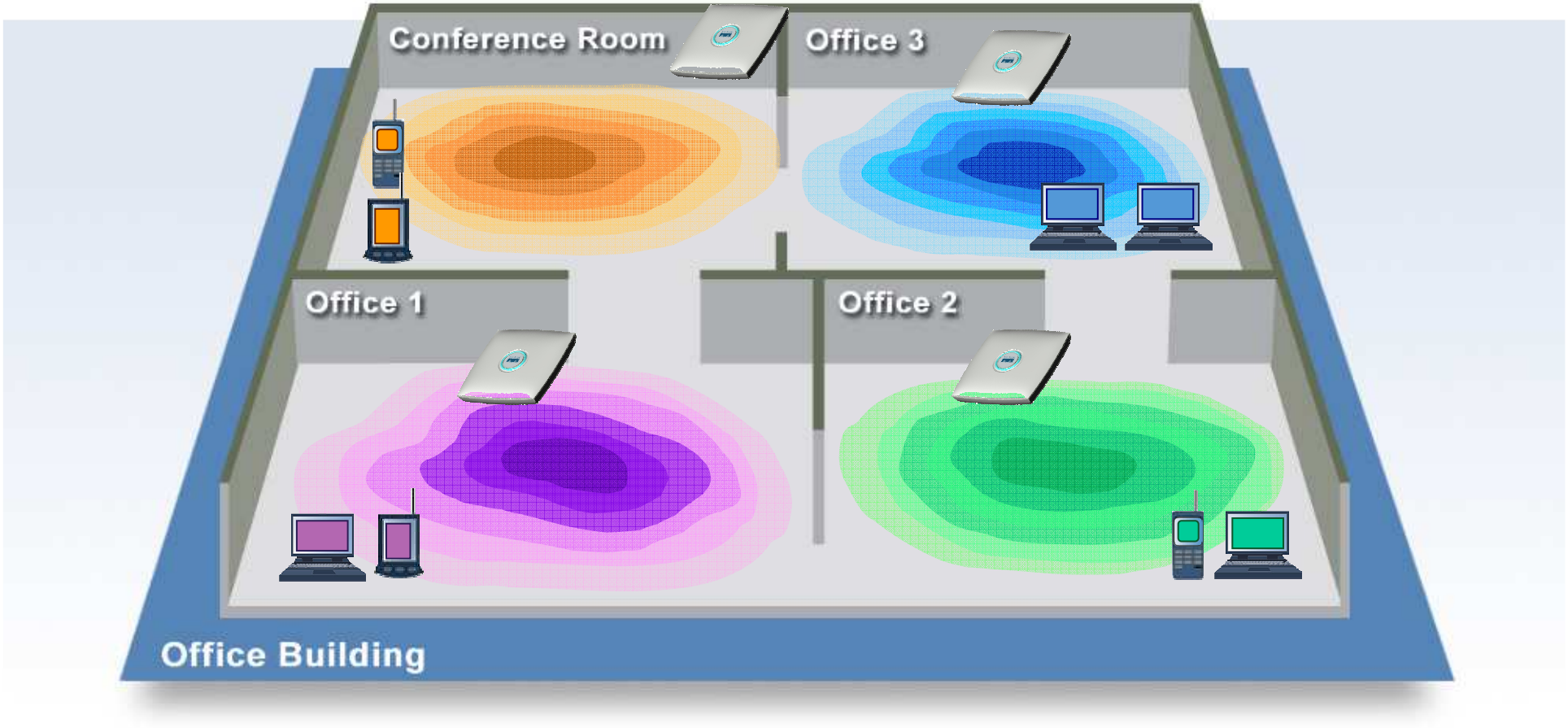
Resolvendo problemas de desempenho e capacidade em áreas de alta densidade (exemplo: salas de reunião)



Melhor Desempenho para a Rede WLAN

Balanceamento Dinâmico da Carga

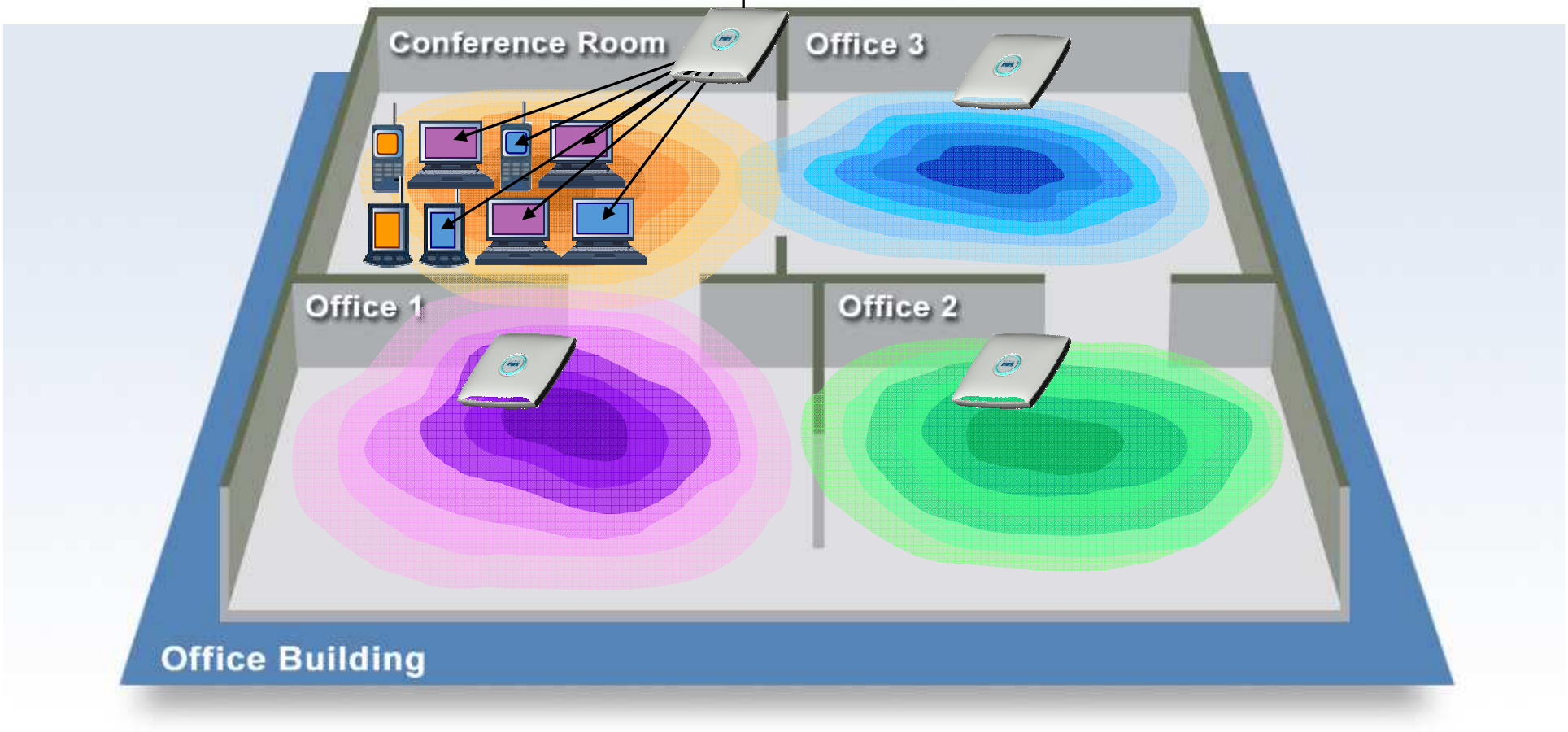
Resolvendo problemas de desempenho e capacidade em áreas de alta densidade (exemplo: salas de reunião)



Melhor Desempenho para a Rede WLAN

Balanceamento Dinâmico da Carga

Resolvendo problemas de desempenho e capacidade em áreas de alta densidade (exemplo: salas de reunião)



Gerenciamento da Rede Wireless

Gerenciamento de toda a rede WLAN

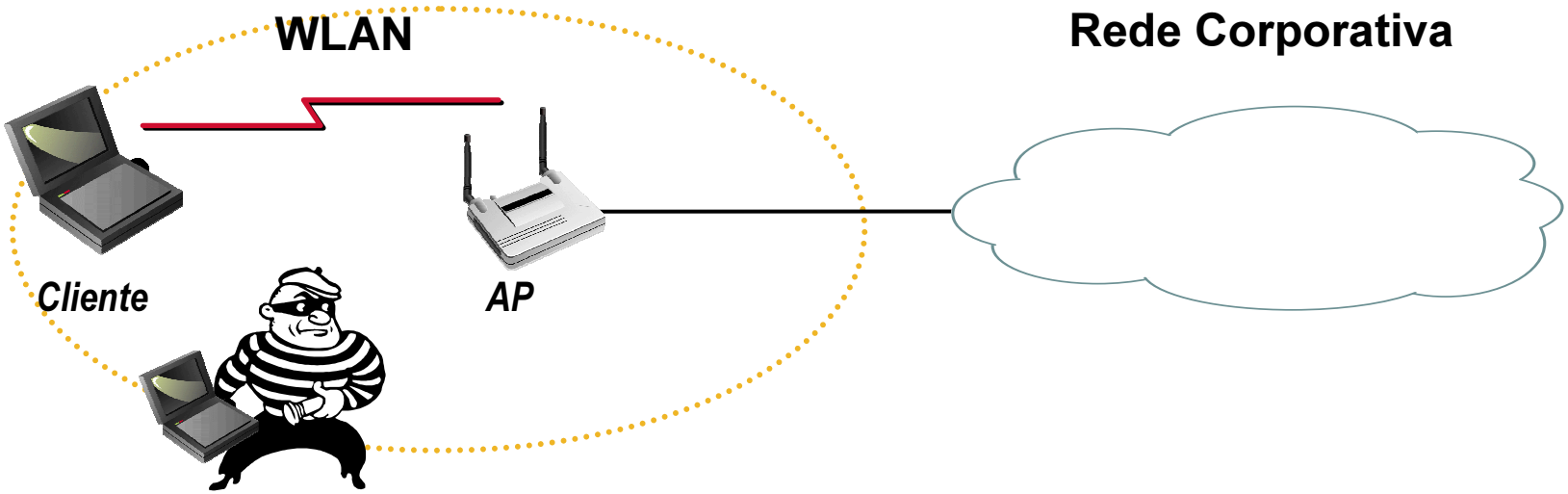
Características

- Planejamento, Configuração, Monitoração, Localização, IDS, depuração de problemas
- Mapas hierárquicos
- Interface GUI amigável; templates
- Aplicação de políticas de rede (QoS, segurança, RRM, etc.)

Benefícios

- OPEX e CAPEX menores
- Melhor visibilidade e contole da área coberta
- Funcionalidade comum a todo o sistema wireless

Segurança na WLAN



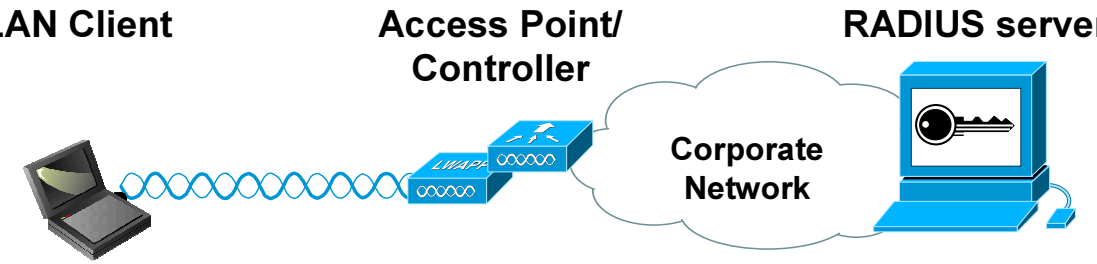
Preocupações:

- **Privacidade – Sniffer Wireless pode ver todos os pacotes que trafegam na WLAN**
- **Autenticação – Qualquer pessoa na área de cobertura do AP pode ter acesso à WLAN**

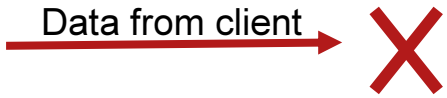
Objetivo: A segurança da WLAN deve ser equivalente à da rede cabeada

Não Fale com Estranhos

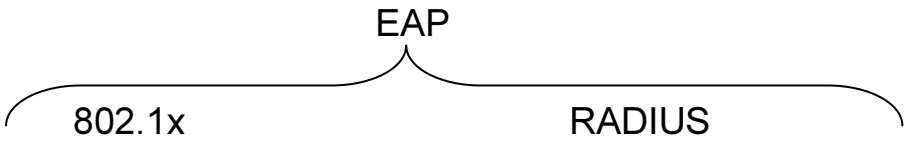
Cliente se associa,



mas não pode transmitir dados até que …



…a autenticação EAP seja concluída



Cliente transmite dados

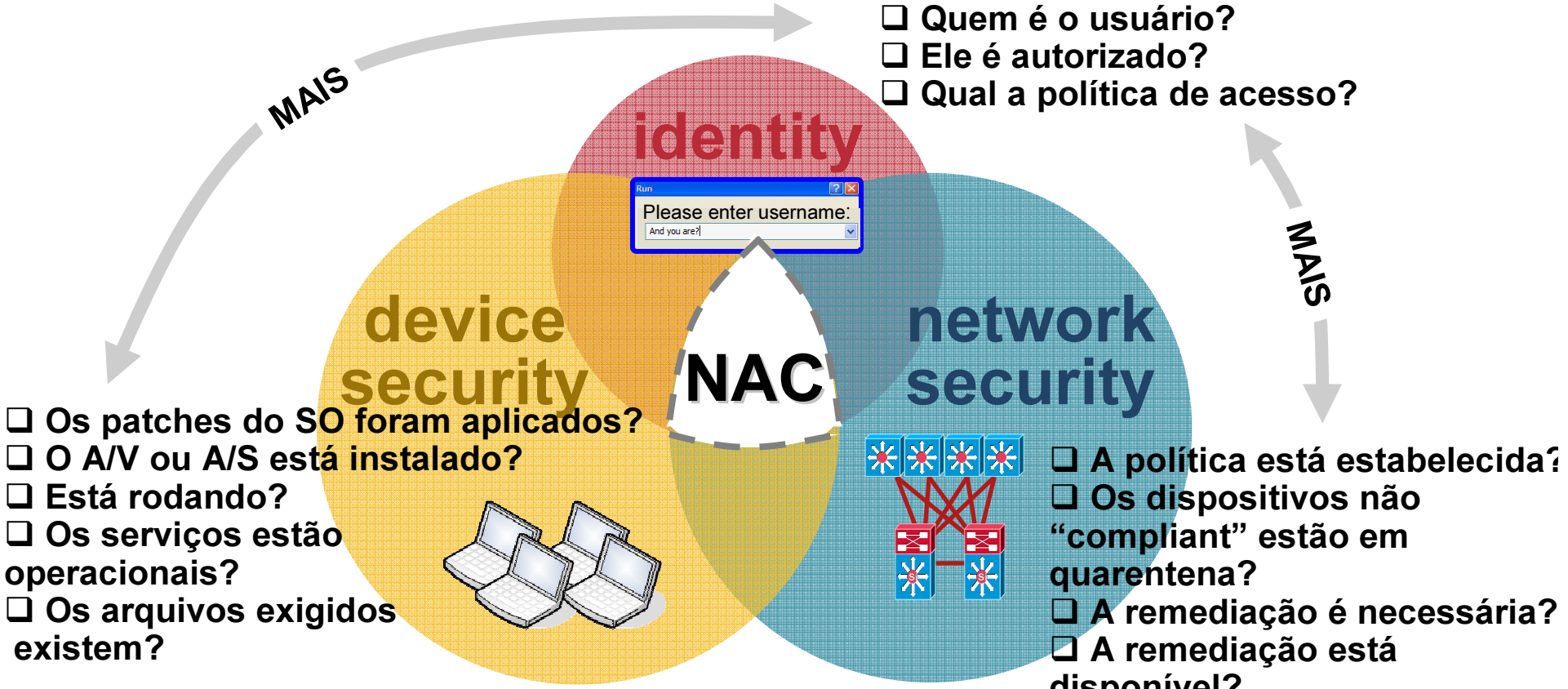
Criptografia Forte

- Temporal Key Integrity Protocol (TKIP) – Wi-Fi WPA
  - Evolução da criptografia WEP
  - Cada pacote é transmitido com sua própria chave de criptografia
  - Checagem da Integridade da Mensagem

- AES – 802.11i = Wi-Fi WPA2
  - Advanced Encryption Standard
  - Padrão “Gold”
  - 128,192 e 256 bit key support

Network Admission Control

Utiliza a rede para aplicar políticas que garantam que os dispositivos de acesso seguem as normas de segurança.



Host Intrusion Prevention System

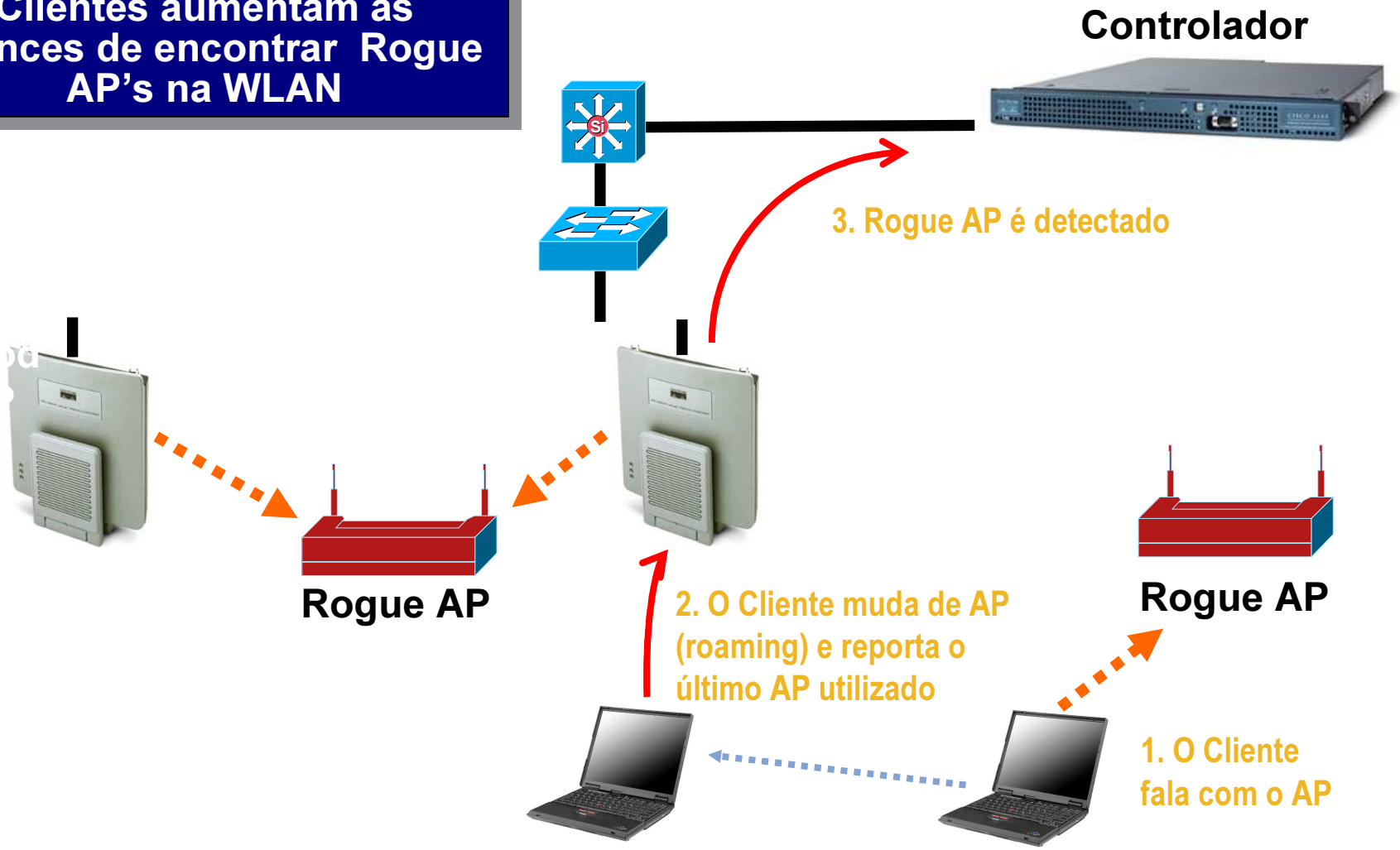
- Protege o cliente contra “day zero” ataques
- Intercepta todos os acessos do sistema para arquivos, rede, registry e recursos dinâmicos como memória e bibliotecas compartilhadas
- Utiliza regras que definem comportamentos inadequados para as aplicações
- Correlaciona as regras com o comportamento das aplicações para prevenir intrusões

HIPS e Wireless

- Desabilita múltiplas interfaces de rede
- Desabilita modo Ad Hoc
- Conecta apenas aos SSIDs corporativos

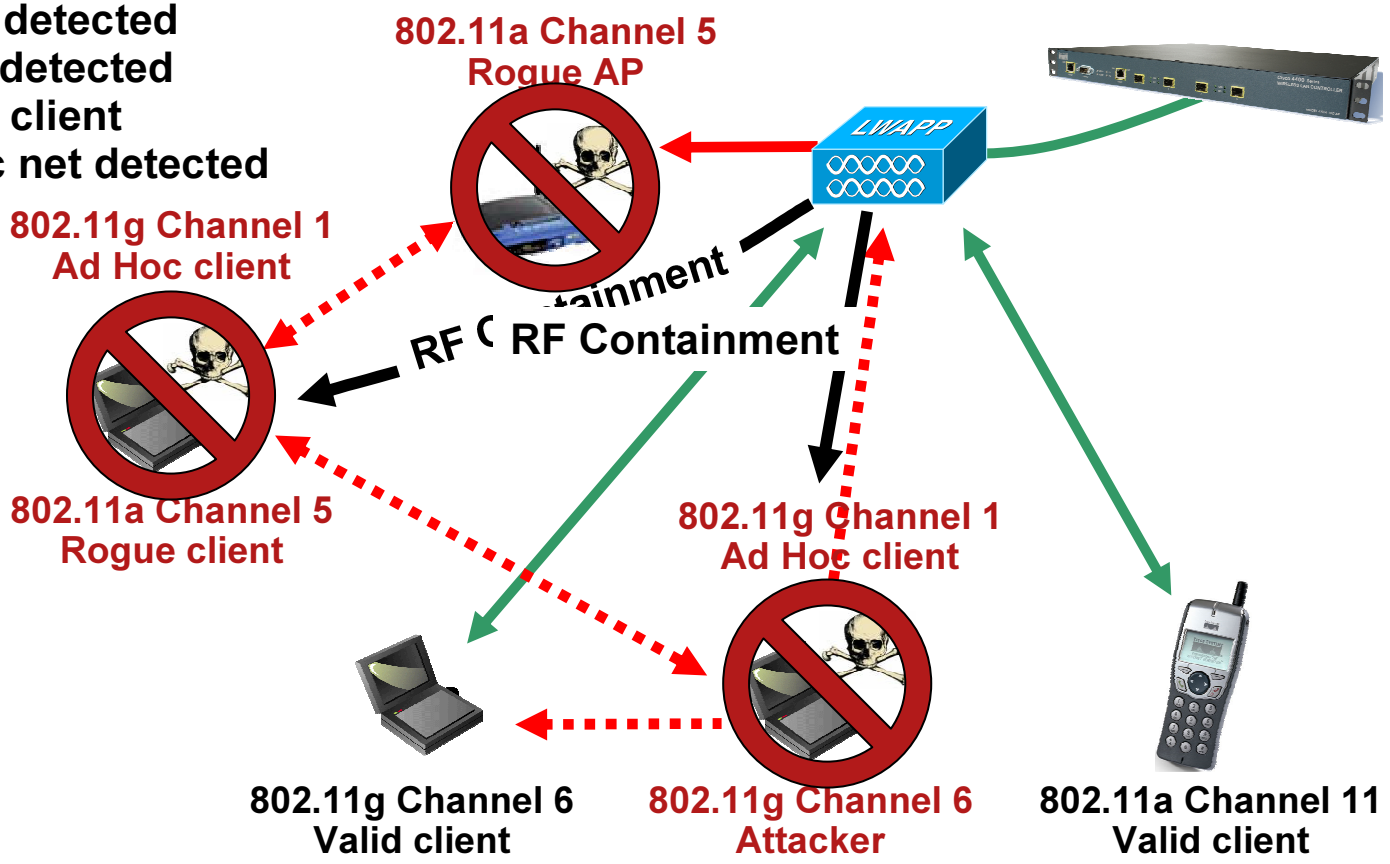
Detecção de Rogue APs

A utilização dos AP's e Clientes aumentam as chances de encontrar Rogue AP's na WLAN



IDS/IPS Wireless

- ✓On-channel attack detected
- ✓Off channel rogue detected
- ✓AP contains rogue client
- ✓Off channel ad hoc net detected
- ✓AP contains ad hoc net



Segurança de redes WLAN: Vulnerabilidades e Lições

Vulnerabilidades:


THE WALL STREET JOURNAL.

Hackers Can Penetrate Wireless Network

The weakness is another reminder of the difficulty in implementing effective network security.

Hackers

"War Driving"

Empregados

Lições:

- Não confie na criptografia WEP básica; sempre use senhas seguras
- Segurança precisa ser implementada no primeiro momento (faz parte do processo de instalação)
- Empregados vão instalar seus próprios equipamentos WLAN! (comprometimento da segurança de toda a sua rede)

Perguntas