

Wireless LAN

DESAFIO

Disponibilidade

“Quando a rede cai, perdemos dinheiro”
- Financeiro

“Nossa rede wireless pode suportar e-mail, mas não a usáramos para aplicações críticas”
- Hospital

Segurança

“Acho que nossa rede wireless não pode suportar a adição de voz”
- Fábrica

“Não confio na minha rede wireless porque não tenho idéia do que está acontecendo nela”
- Instituição Financeira

“Tenho 30 prédios com WLAN's e não consigo fazer um mínimo de determinação de problemas”
- Companhia de Software

Gerência

“Não podemos contratar mais gente só para administrar a rede wireless” – Centro de Eventos



DESAFIO

Se lembra dos velhos tempos dos hubs? antes dos switches?

Era uma tecnologia que compartilhava o meio

Se lembram que a rede degradava quando muitos usuários acessavam?



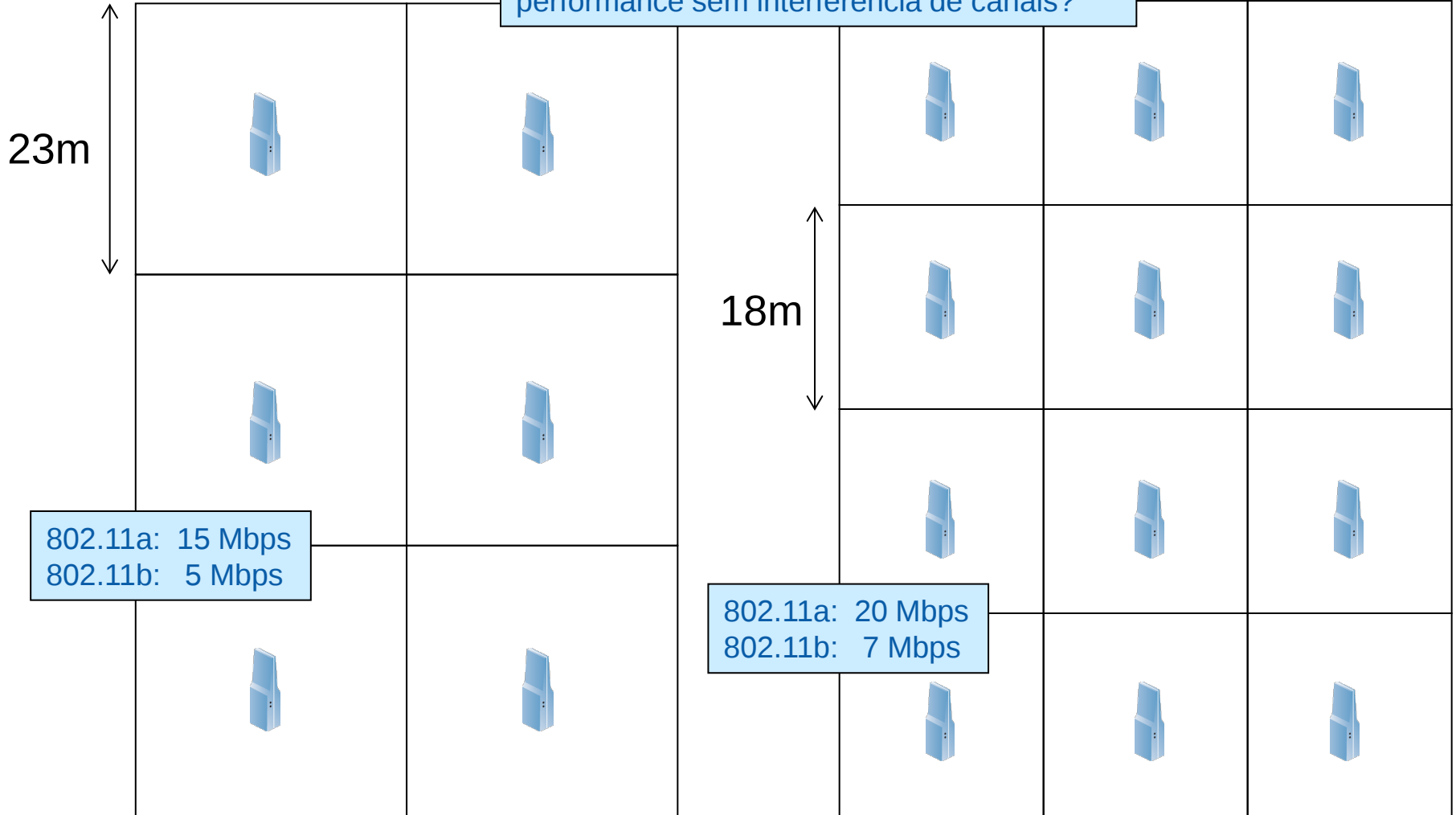
Wireless é exatamente assim

- A transmissão é semi-duplex
- A taxa máxima do 802.11b é 11 Mbps, o que significa que a melhor taxa de transmissão possível é cerca de 6 Mbps
- O meio é compartilhado
- Adicionar mais usuários significa contenção pelo meio de acesso, reduzindo a performance de todos

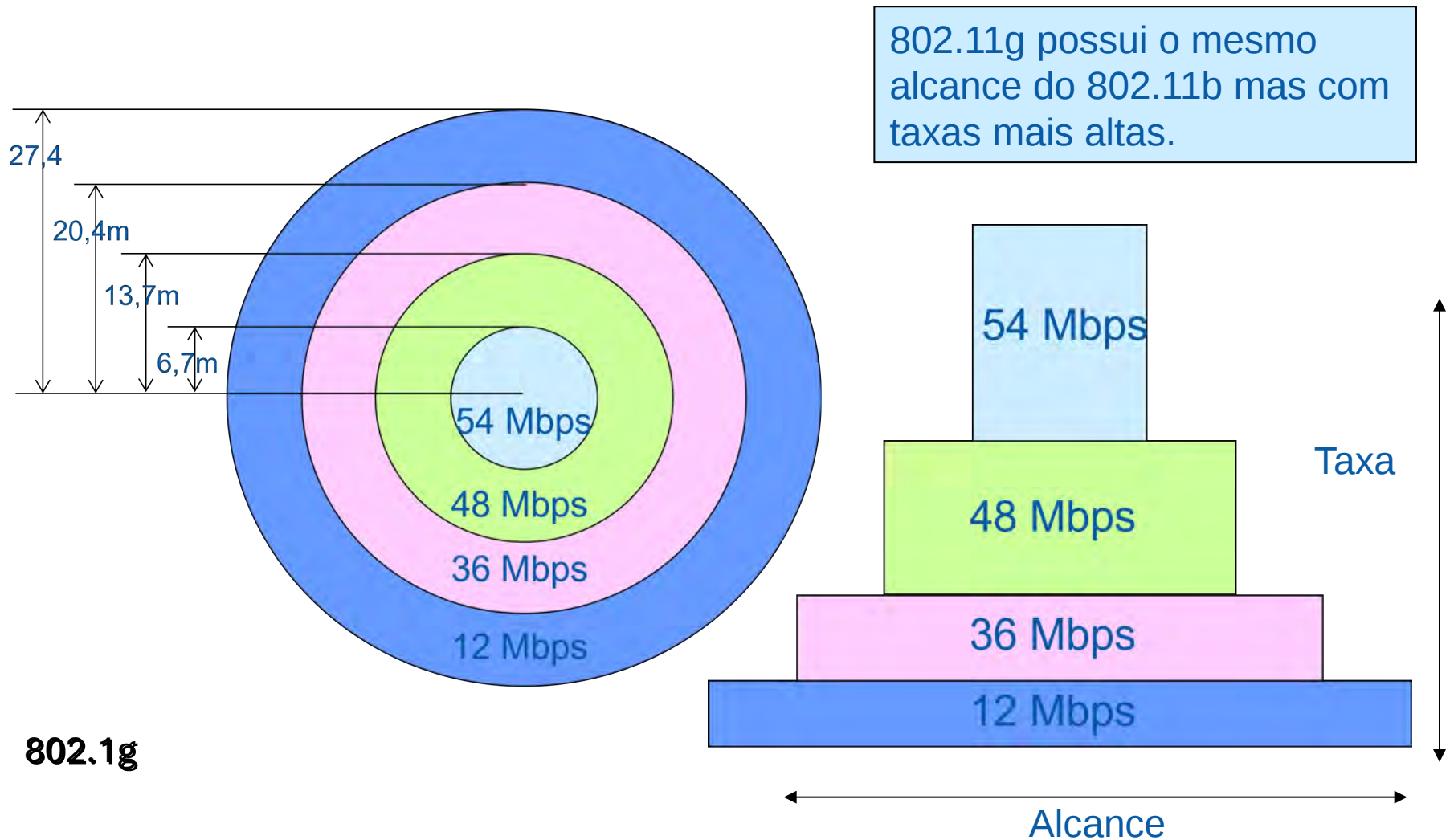
O padrão 802.11 automaticamente reduz sua taxa de transmissão para manter a comunicação com todos. Um cliente mal configurado, com recepção ruim, usará a menor velocidade possível, trazendo lentidão a todos os usuários

CUSTO x BOA COBERTURA

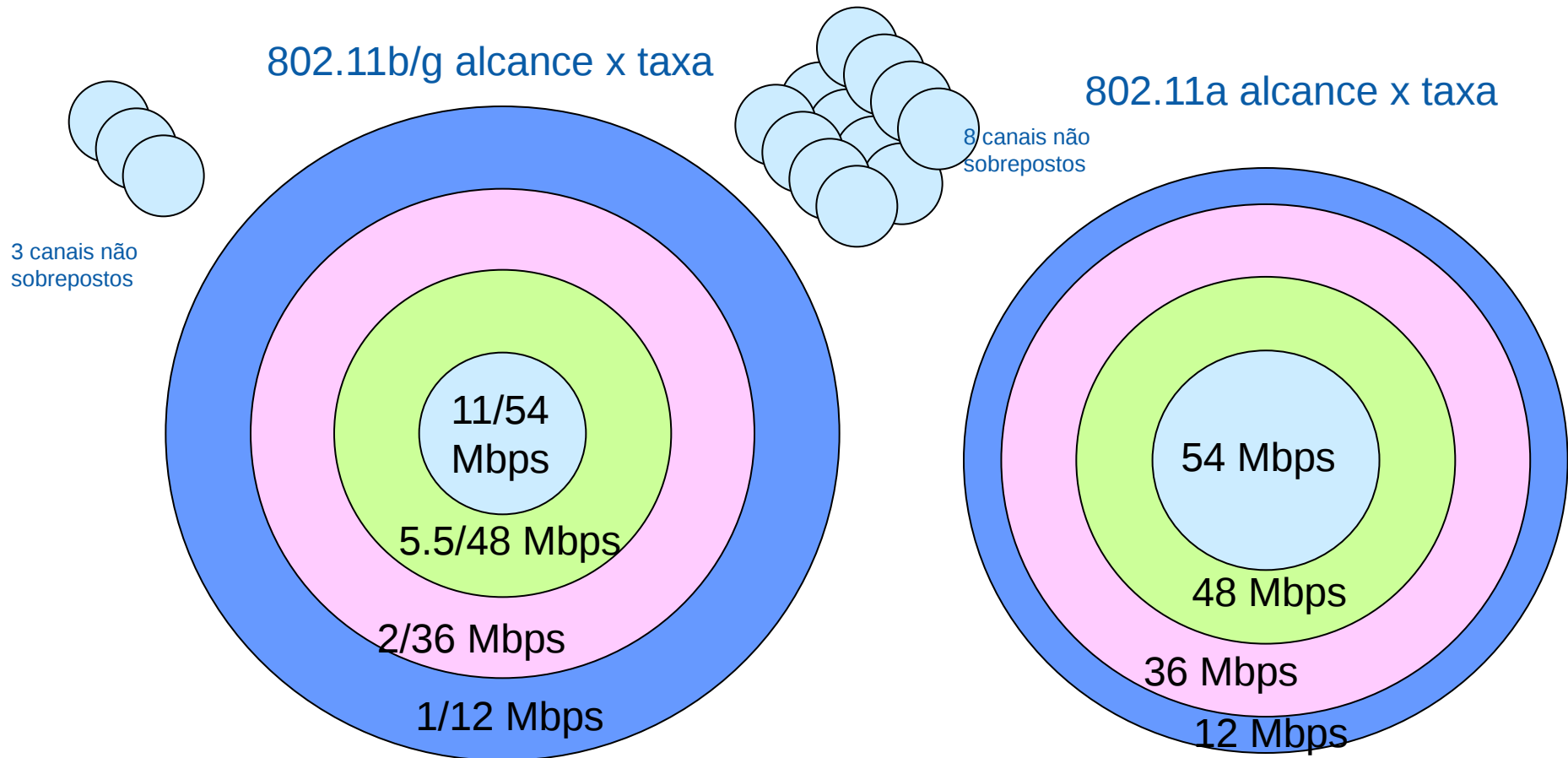
Qual a distância mínima para obter alta performance sem interferência de canais?



TAXA versus DISTÂNCIA



TAXA versus DISTÂNCIA



Teoricamente, 802.11a deveria cobrir ~75% da área de um rádio 802.11b/g. Estudos de campo da Alcatel mostram ~85-90% da cobertura de b/g.

OBSTÁCULOS

Construções normais
contém vários
obstáculos ao wireless

Cantos de alcance difícil

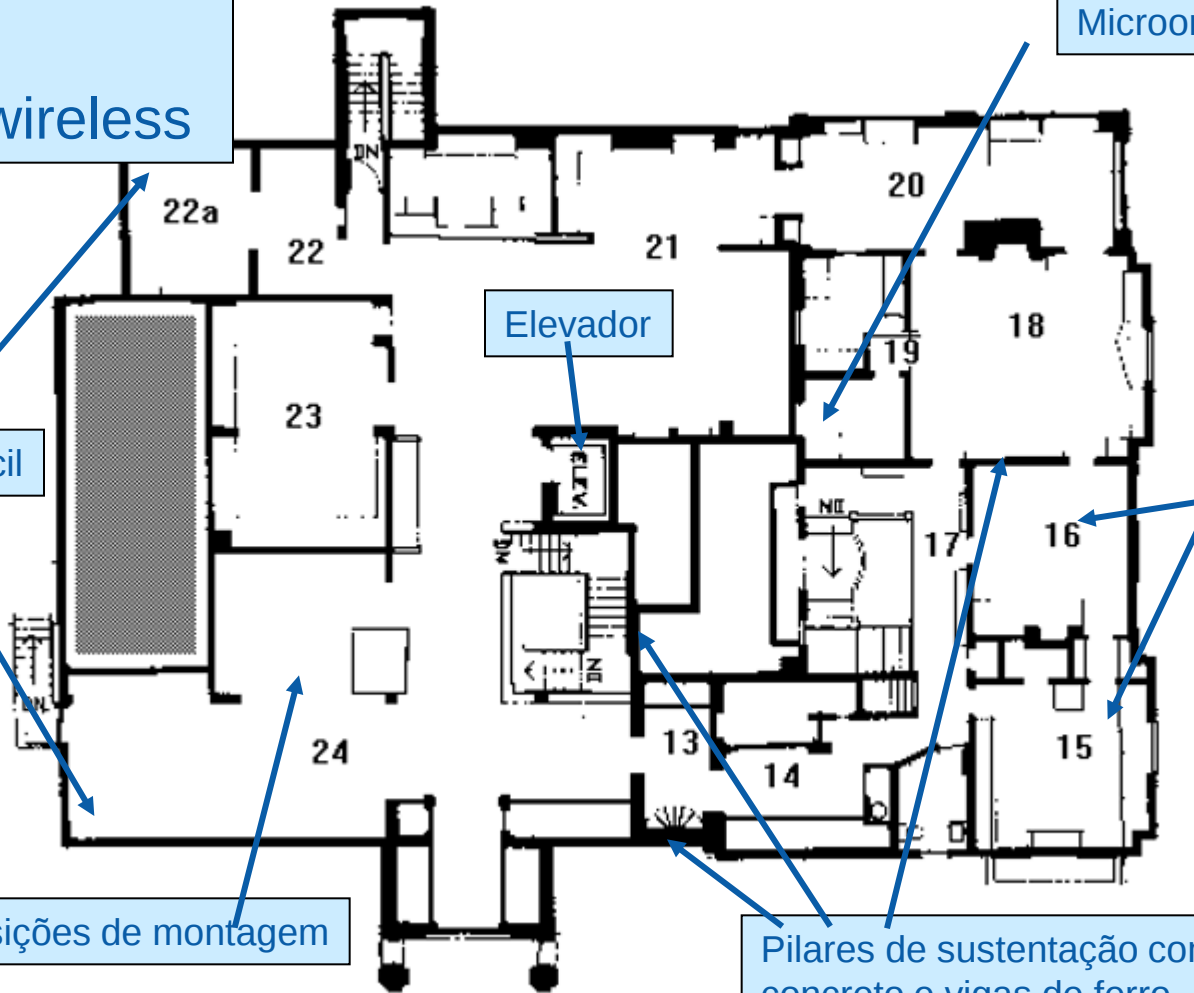
Falta de boas posições de montagem

Elevador

Microondas

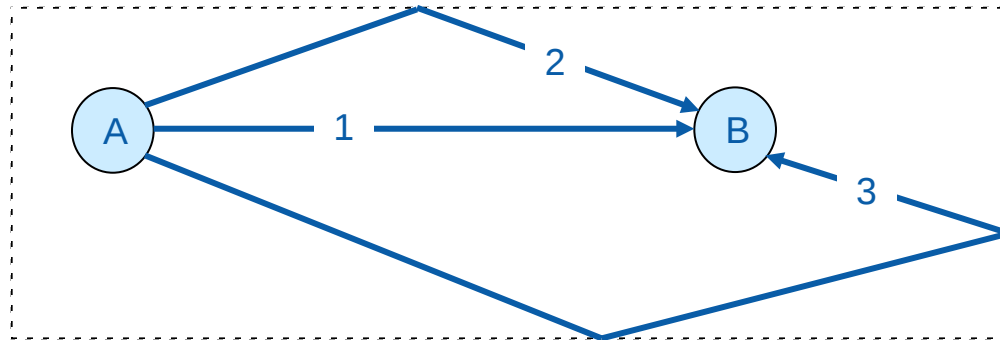
Paredes

Pilares de sustentação com
concreto e vigas de ferro

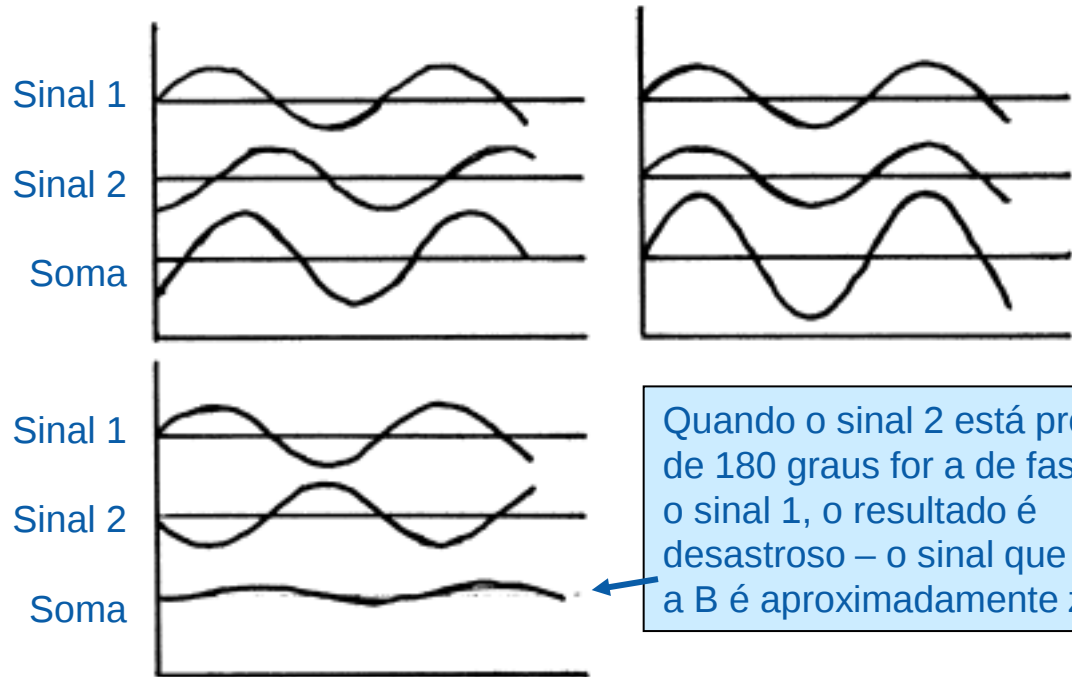


INTERFERÊNCIA MULTI-ROTAS

O sinal transmitido por A reflete em paredes e objetos, chegando em B com ligeiro atraso, ou *phase shifted*.

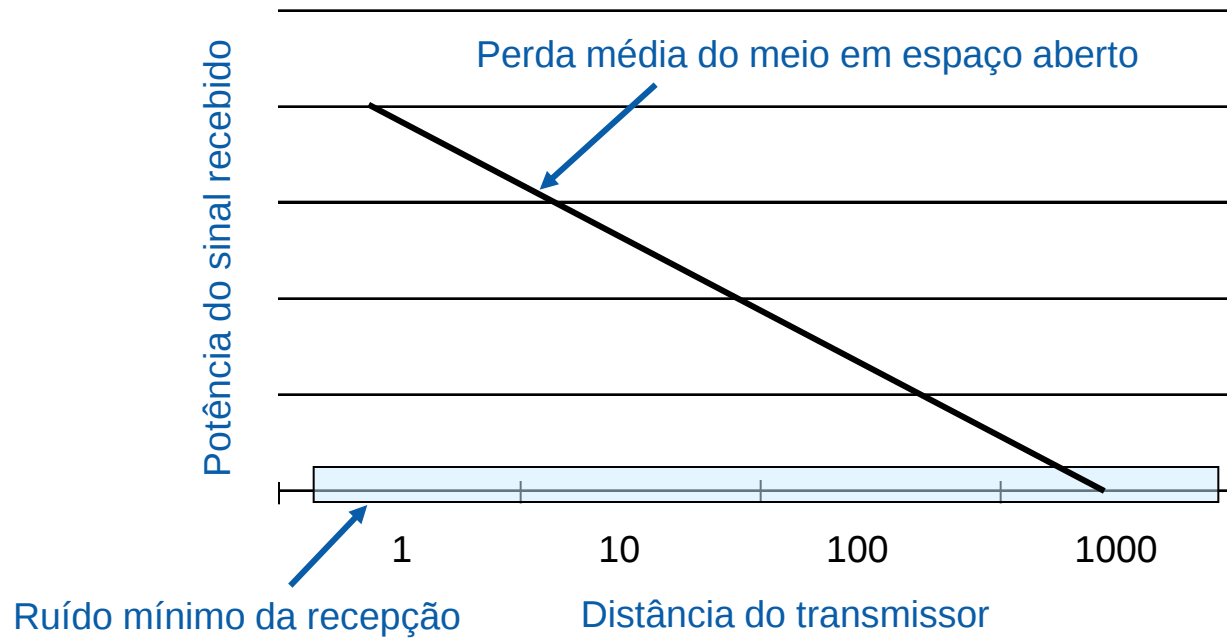


Para determinar o sinal final que B recebe, cada onda é somada (valores positivos acima da linha central, valores negativos abaixo.)



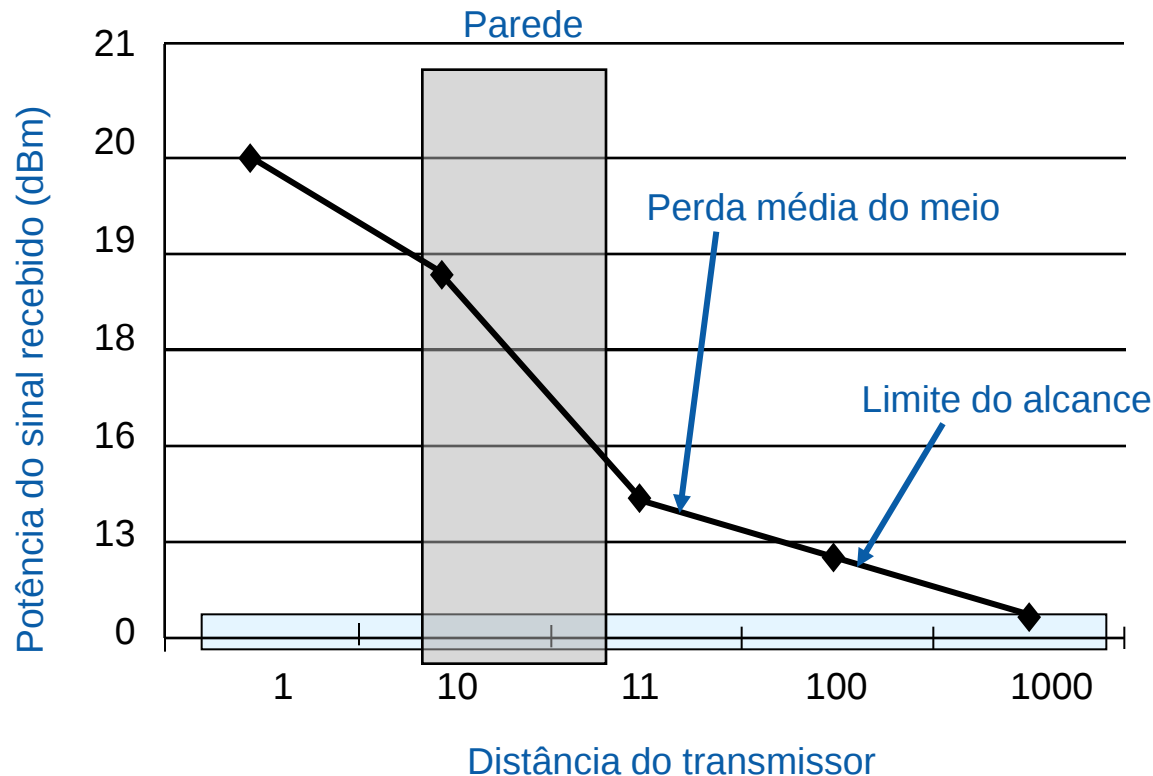
Quando o sinal 2 está próximo de 180 graus fora de fase com o sinal 1, o resultado é desastroso – o sinal que chega a B é aproximadamente zero!

EM ESPAÇO ABERTO



Cortesia de Gary Singh

OBSTÁCULOS



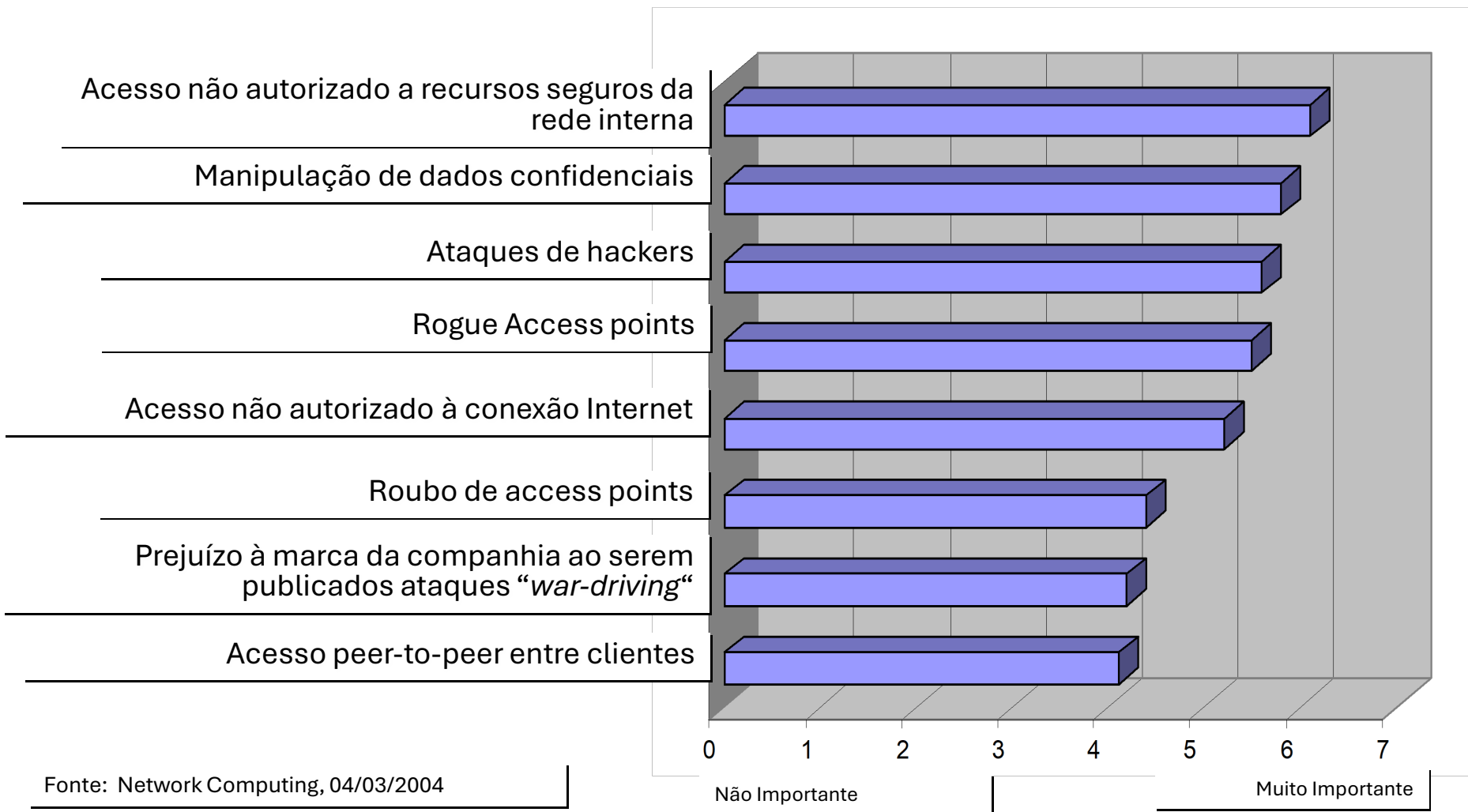
Partição	Perda (dB)
Parede fixa	3.0
Divisória	1.4
Porta	2.0
Partição metálica	5.0
Janela	2.0
Parede exterior	10.0
Parede de subsolo	20.0

Uma perda de 3 dB significa que *metade* da potência de transmissão foi perdida

Cortesia de Gary Singh

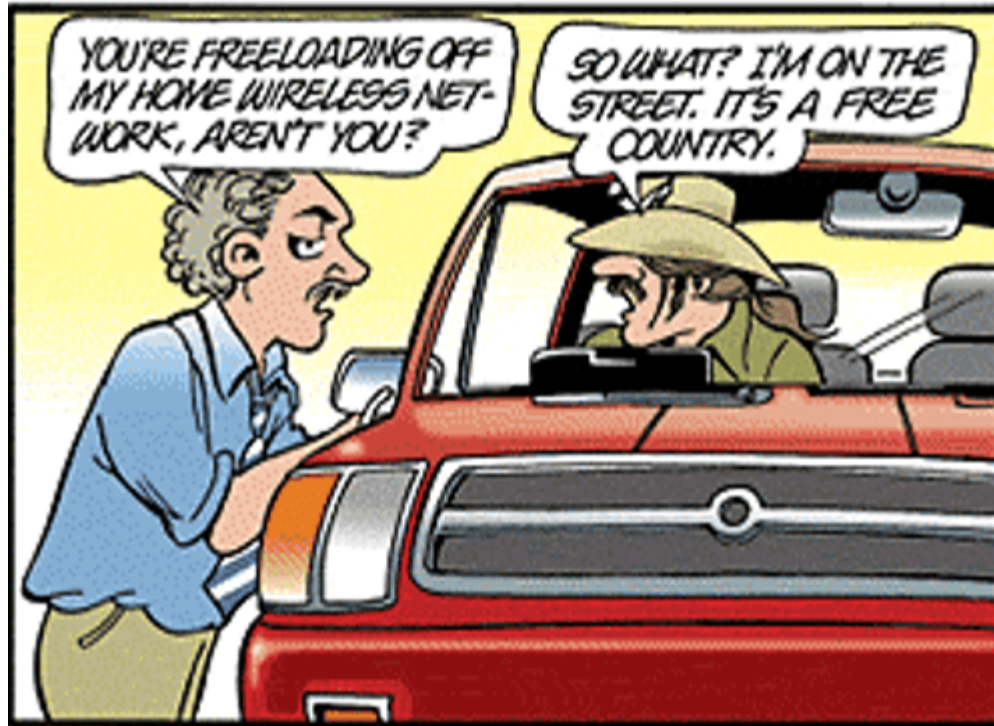
Potência de Transmissão (dBm) = $10 * \log[\text{Potência de Transmissão (mW)}]$

SEGURANÇA DO WIRELESS



SEGURANÇA DO WIRELESS

Você está usando a minha rede wireless doméstica, não está?



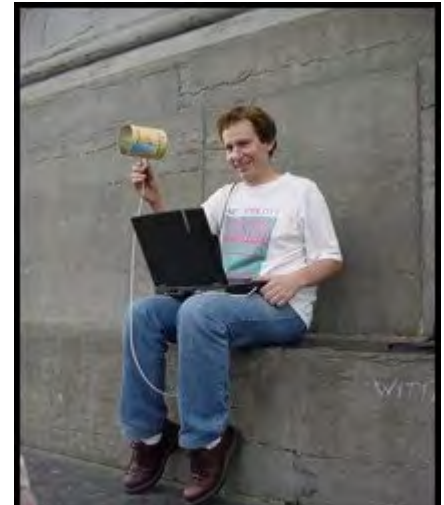
E daí? Estou na rua. Este é um país livre.

“Wireless usa um meio é praticamente impossível de controlar fisicamente.”

SEGURANÇA DO WIRELESS

- Roubo de banda
- Escuta
 - O sinal RF se propaga muito mais longe que um cliente comum pode ouvir – até 40km
 - Coleta de dados e informações
 - Senhas, configurações, SSID, AP MAC addr, etc.
- Acesso através de uma “Cantenna” ou “Antenas de alto ganho”
 - Fáceis de fazer ou comprar
 - Muito mais potentes que as normais das placas de rede wireless
 - Sem traço de alguém escutando
 - Há utilitários shareware para coletar dados, quebrar chaves WEP, etc.

Can = Lata



ROGUE AP, acesso peer-to-peer

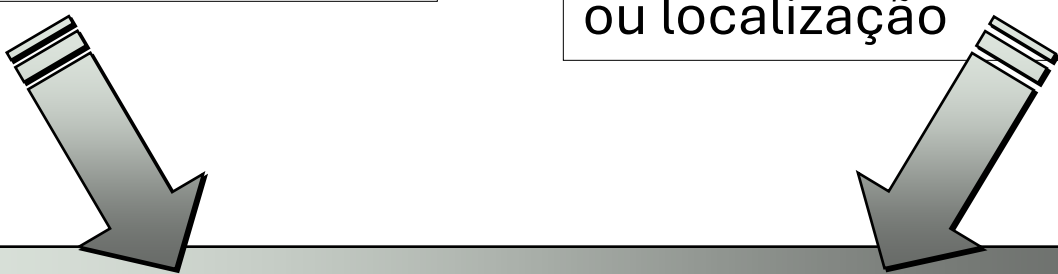
- Rogue Access Points (APs “clandestinos”)
 - Portas abertas para acesso à rede interna
 - Nem sempre maliciosos
 - Bypass nas políticas de segurança de IT
 - Encontrá-los e removê-los é caro e consome tempo
 - Potencial para ataque “Man in the middle”
 - Exemplo: Cavalo de Tróia coletando senhas
- Acesso “ad hoc” ou “peer-to-peer”
 - Configuração default do Windows XP se não encontrar um access point
 - Bypass nas políticas de segurança de IT

MOBILIDADE

- A mobilidade é impactada por:

Convergência: para uma empresa é a consolidação do serviço em menos plataformas e infraestrutura.

Novos requisitos de mobilidade: para o usuário é a capacidade de aumentar a eficiência, permanecendo conectado independente da aplicação ou localização



A resposta certa para suportar esta evolução é a mobilidade convergente

VISÃO INTEGRADA OSD

“Desenhar um projeto pensando em toda a infraestrutura da edificação, além de pensar em soluções de alta disponibilidade, seguras e fáceis de gerenciar”

Gerência

GERENCIABILIDADE

- Consistência entre as redes com e sem fio
- Soluções de gerência unificada
- Gerência inteligente de RF

Disponibilidade

DISPONIBILIDADE

- Redes com e sem fio projetadas para a mais alta disponibilidade
- QoS poderoso nas redes com e sem fio para aplicações de missão crítica
- Mobilidade transparente

SEGURANÇA

- Framework multi-camadas para as redes com e sem fio
- Autenticação de usuários e detecção e controle de não autorizados de forma incomparável no mercado

Segurança

INFRAESTRUTURA DE ATIVOS



- OmniAccess 4000 Series WLAN Switches



- OmniAccess 4100 Series WLAN Appliances



- OmniAccess 1200 Access Point

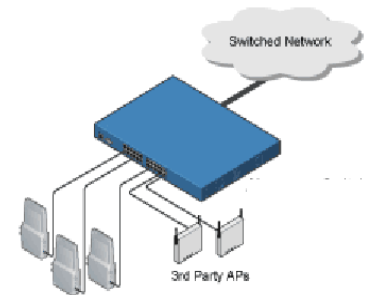
ARQUITETURA WLAN ALCATEL

- Baseada em um Access Point “Light”
 - **Escalável**: o Access Point não é uma entidade gerenciada
 - **Robusto**: A complexidade do SW do Access Point é minimizada
 - **Avançado**: Gerência de RF incomparável, serviços avançados
 - Suporte a 802.11b/g/a – Wi-Fi Alliance Certified
 - Segue as **Propostas de Valores** da linha fixa
OmniSwitch de Gerenciabilidade, Alta Disponibilidade e Segurança

ARQUITETURA WLAN ALCATEL

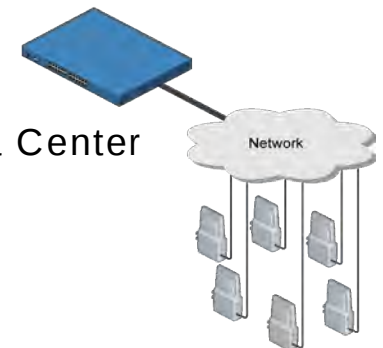
OmniAccess 4012 e 4024 Wireless Switches

- Aplicação distribuída, normalmente no wiring closet
- Controle do Wireless e funcionalidades Wired
- AP conectados a portas 10/100 do Wireless Switch
- 12 ou 24 portas 10/100 com PoE
- 1 ou 2 portas Gigabit de uplink



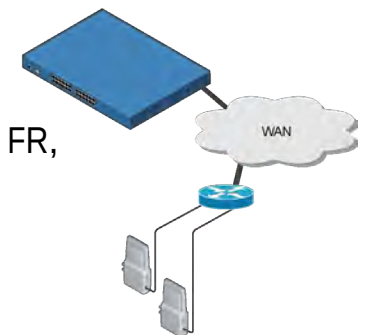
OmniAccess 4102 Wireless Appliance

- Aplicação centralizada, normalmente no Data Center
- Controle do Wireless conectado fisicamente ao switch do Data Center
- Não recebe clientes diretamente: sem portas 10/100 ou PoE
- Tráfego em túnel do AP ao Appliance
- Dois uplinks Gigabit Ethernet para conexão ao backbone
- Suporta até 36 APs



OmniAccess 1200 Access Points

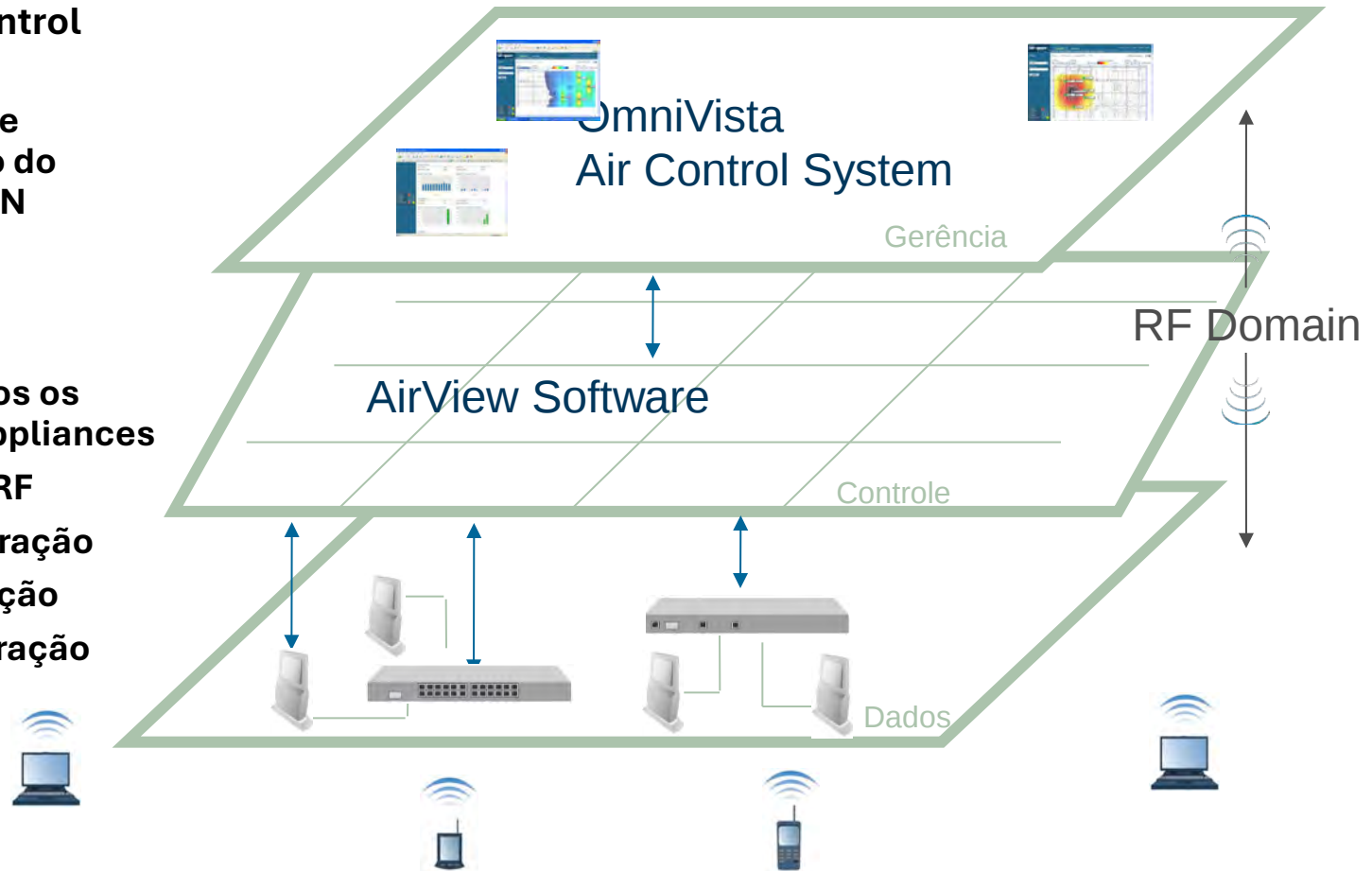
- 802.11b&g ou 802.11a/b&g (multimodo)
- 1200R estende os serviços WLAN por links WAN (E1, cable modem, FR, etc)
- Antena omni-direcional, direcional setorizada ou externa
- Alimentação inline 802.3af (fonte externa opcional)
- Monitoração do ar e tráfego de dados no mesmo dispositivo
- Lightweight Access Point Protocol (LWAPP)



ARQUITETURA WLAN ALCATEL

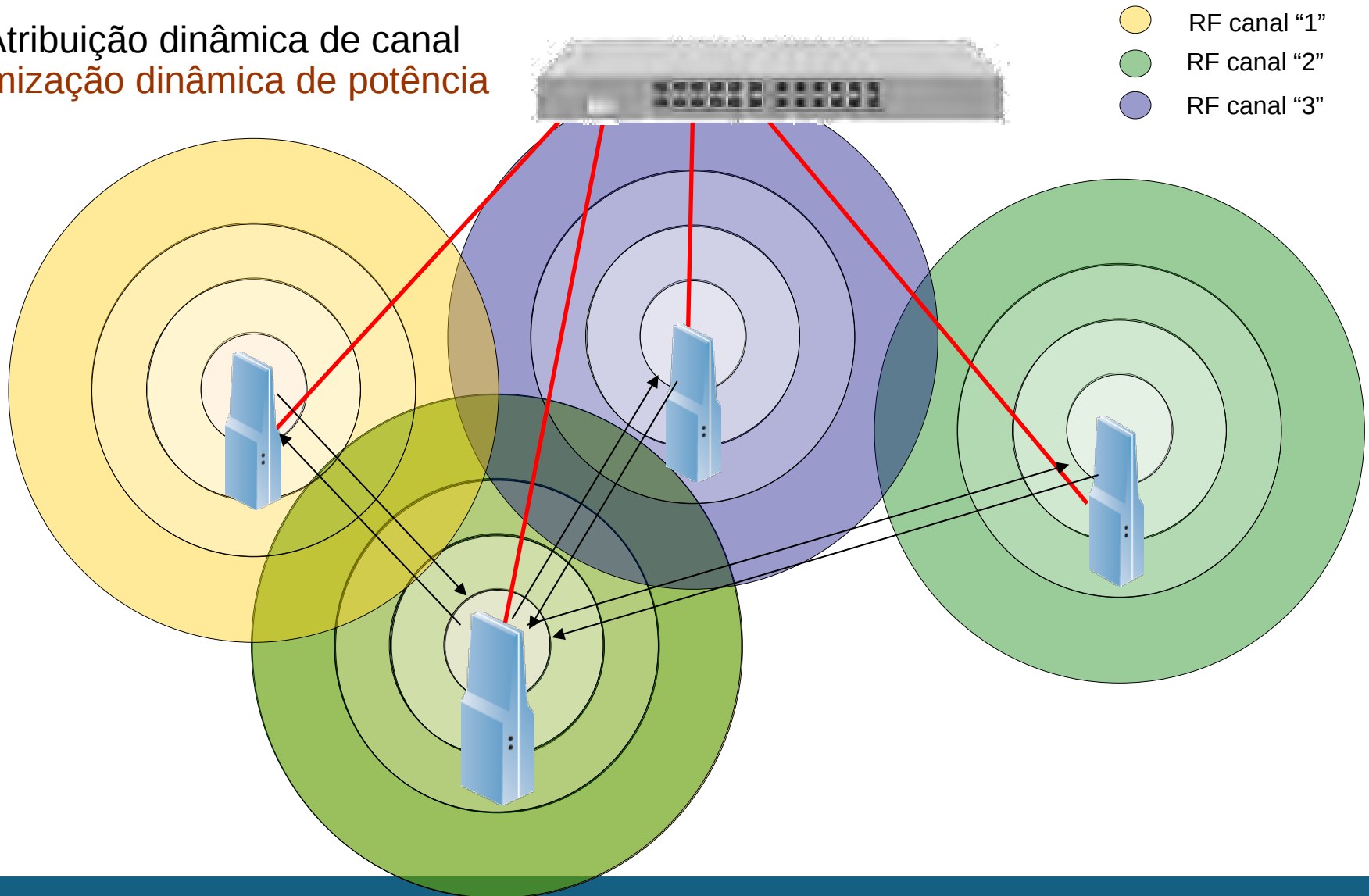
SOFTWARE

- **OmniVista Air Control System (ACS)**
 - **Monitoração e Configuração do sistema WLAN**
- **AirView**
 - **Roda em todos os switches e appliances**
 - **Gerência de RF**
 - **Auto Configuração**
 - **Auto Otimização**
 - **Auto Recuperação**



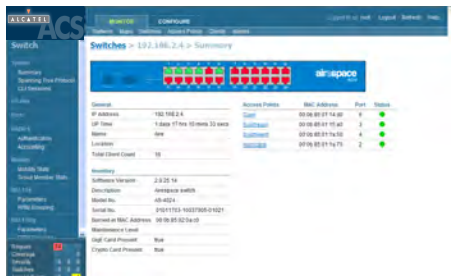
GESTÃO

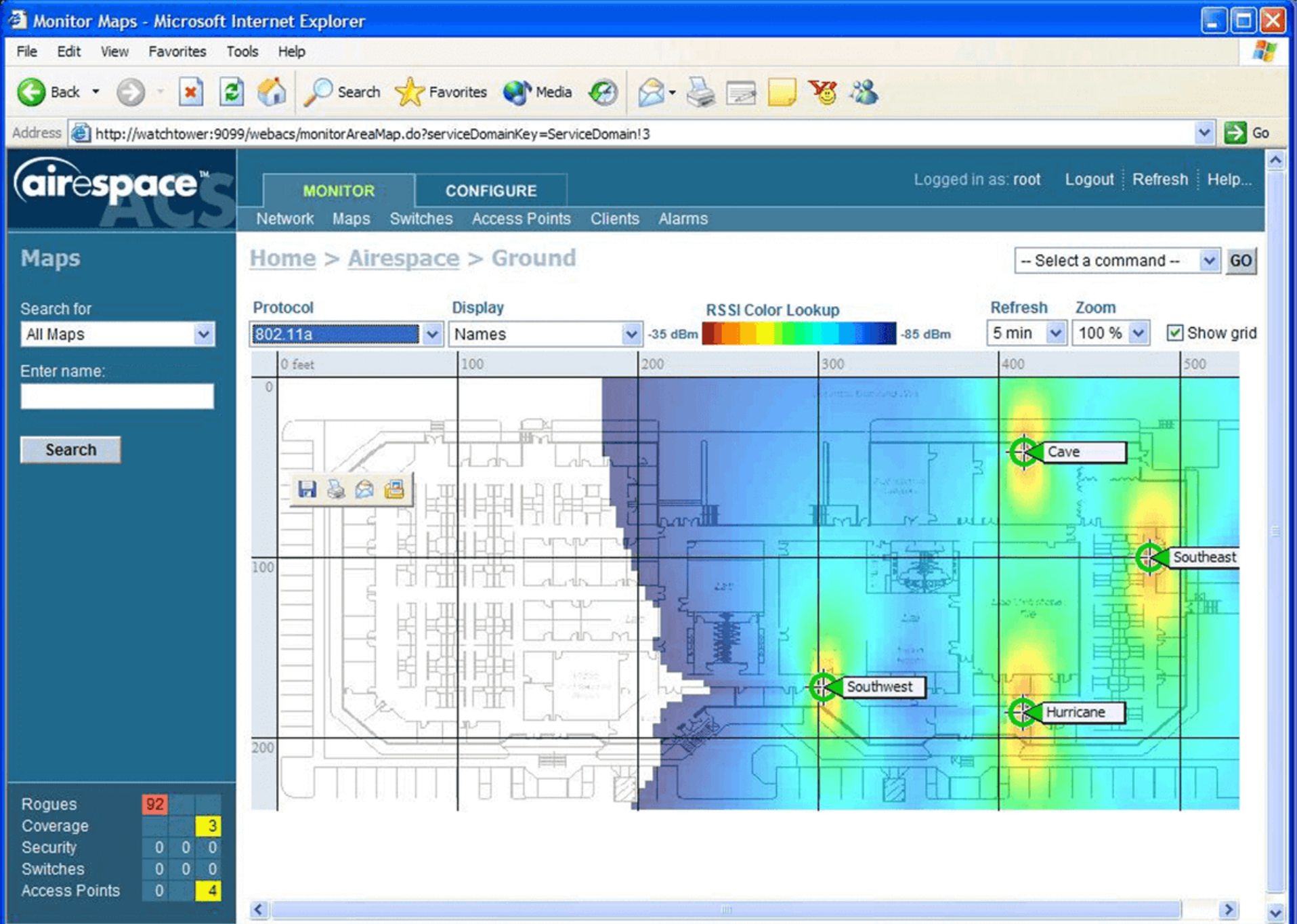
Atribuição dinâmica de canal
Otimização dinâmica de potência



GESTÃO

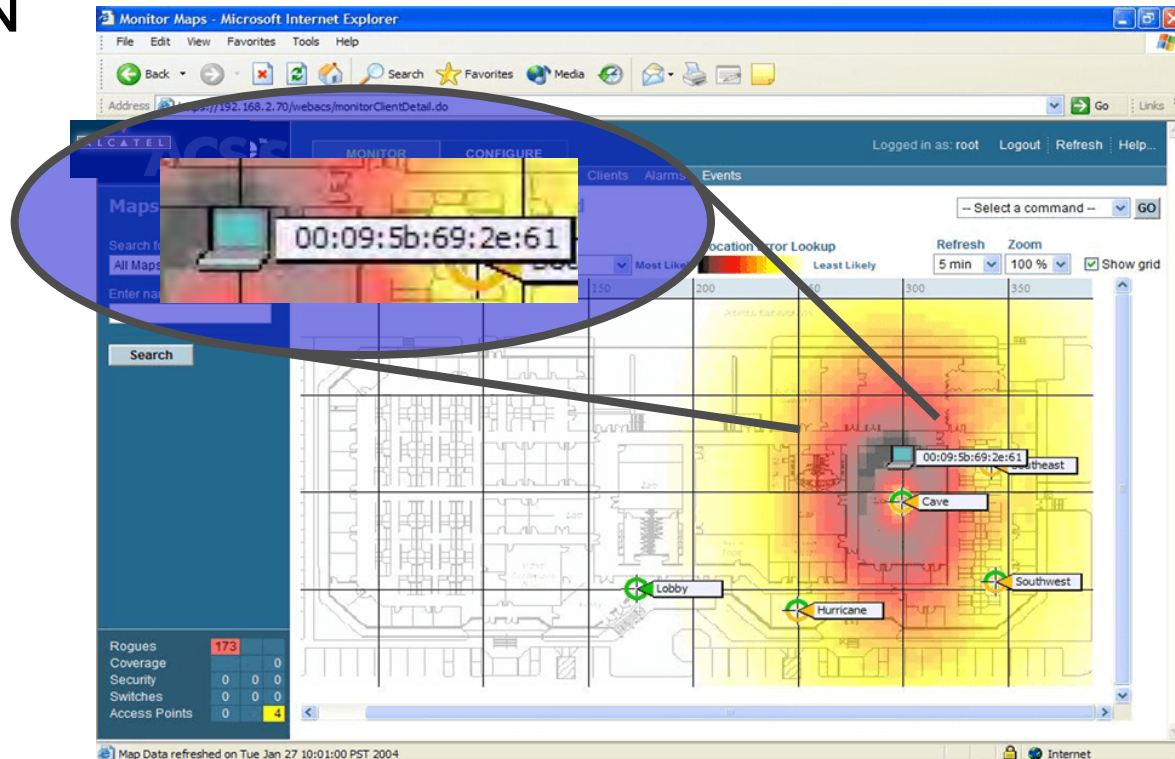
- **Gerência dos sistemas WLAN**
 - Planejamento WLAN (Site survey)
 - Gerência inteligente de RF - portal no AirView
 - Wireless Protection System (WPS)
 - Location Tracking
 - **Gerência de Elementos completa**
 - FCAPS
 - Visibilidade centralizada dos clientes
 - Determinação de problemas, alarmes, upgrades, etc.
 - **Políticas avançadas**
 - Atribuição de políticas “Point and click” (layers 1-3)
 - Visibilidade de rede
- > **Opções de acesso flexíveis**
 - CLI, HTTP, HTTPS, SNMP
 - GUI detalhada, incluindo heat maps
 - Integração com ferramentas externas
 - HP OpenView e outros via SNMP
 - > **OmniVista Network Management**
 - Ferramenta unificada para redes com e sem fio
 - Segurança, VLAN, Políticas de QoS





LOCATION TRACKING

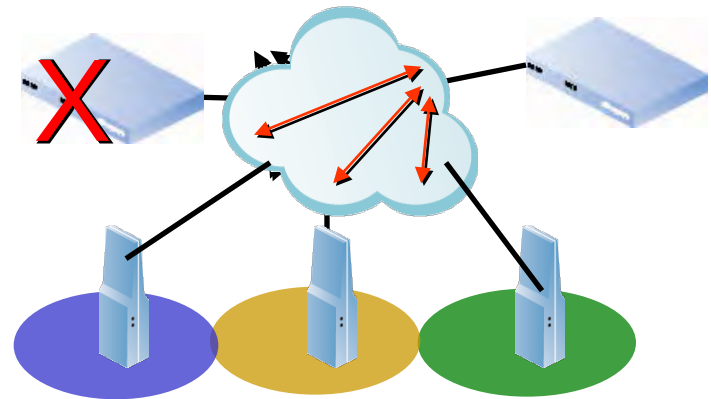
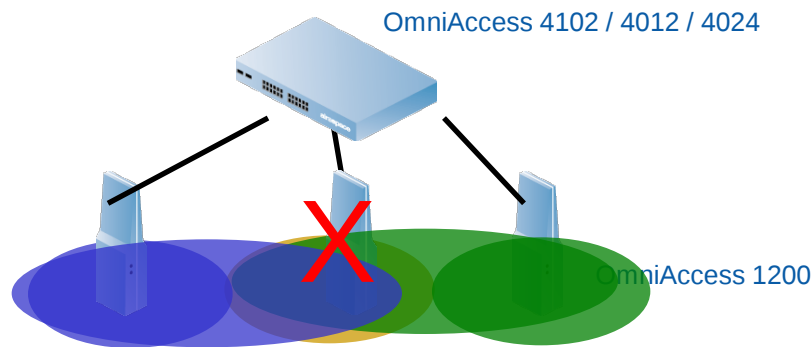
- ACS usa um avançado sistema de localização com precisão de menos de 10 metros
- Melhor visibilidade sobre o que está acontecendo na WLAN



DISPONIBILIDADE

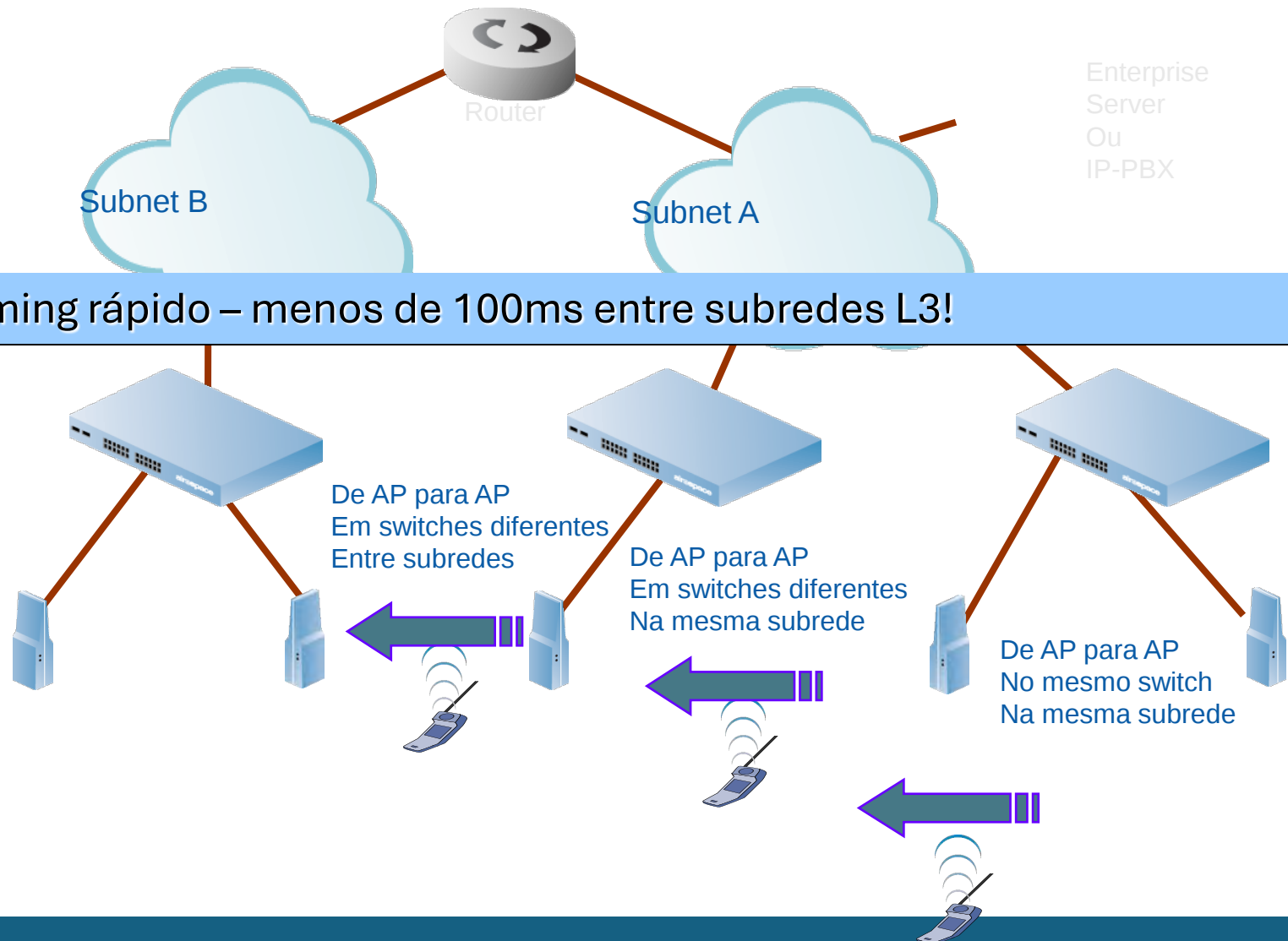
- Alta Disponibilidade

- Cobertura automática de buracos em caso de falha do AP
- Proteção 1:N do appliance WLAN



- QoS forte: por VLAN para dados, SVP (Spectralink Voice Protocol) para voz, futuro 802.11e
- QoS uniforme nas redes com e sem fio

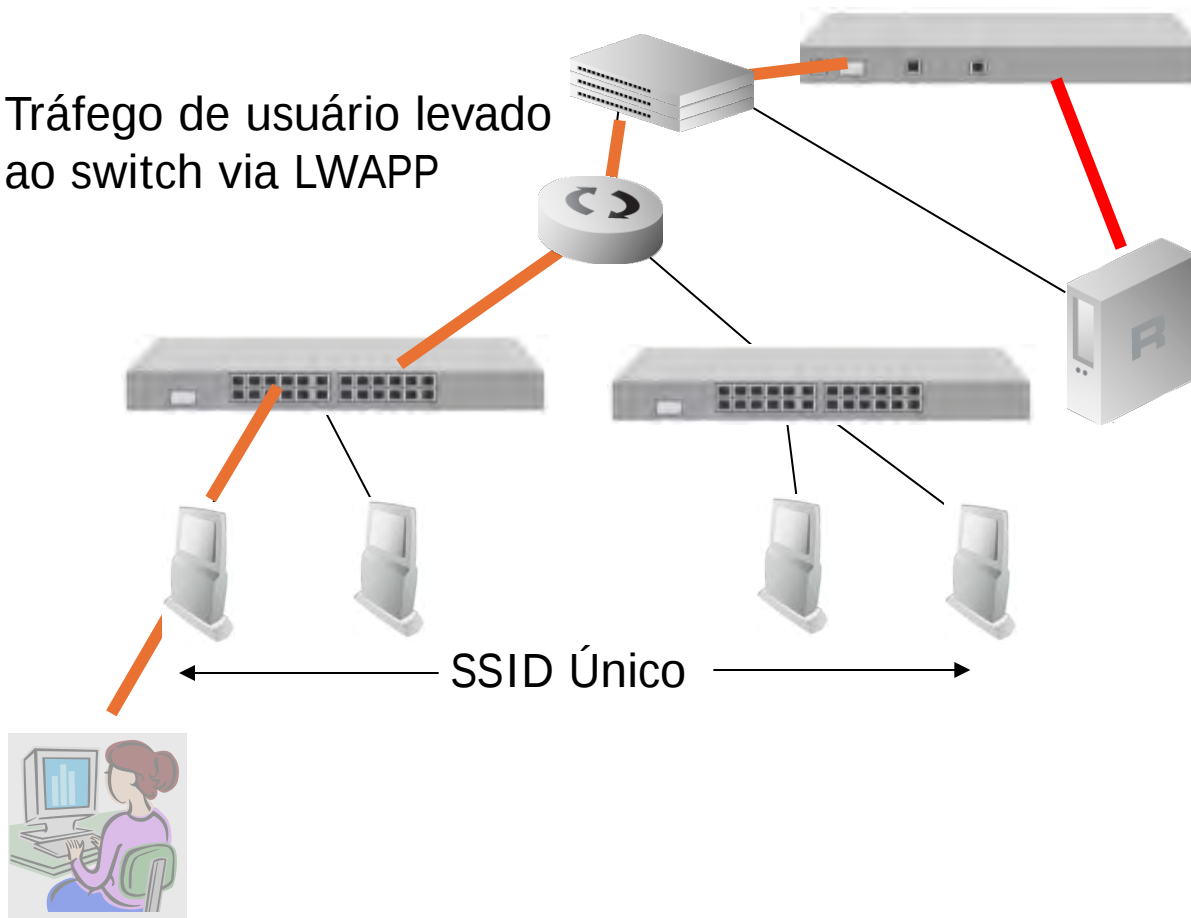
VOICE OVER WLAN



IDENTIFICAÇÃO EM REDE

MOBILIDADE SEGURA

Tráfego de usuário levado
ao switch via LWAPP



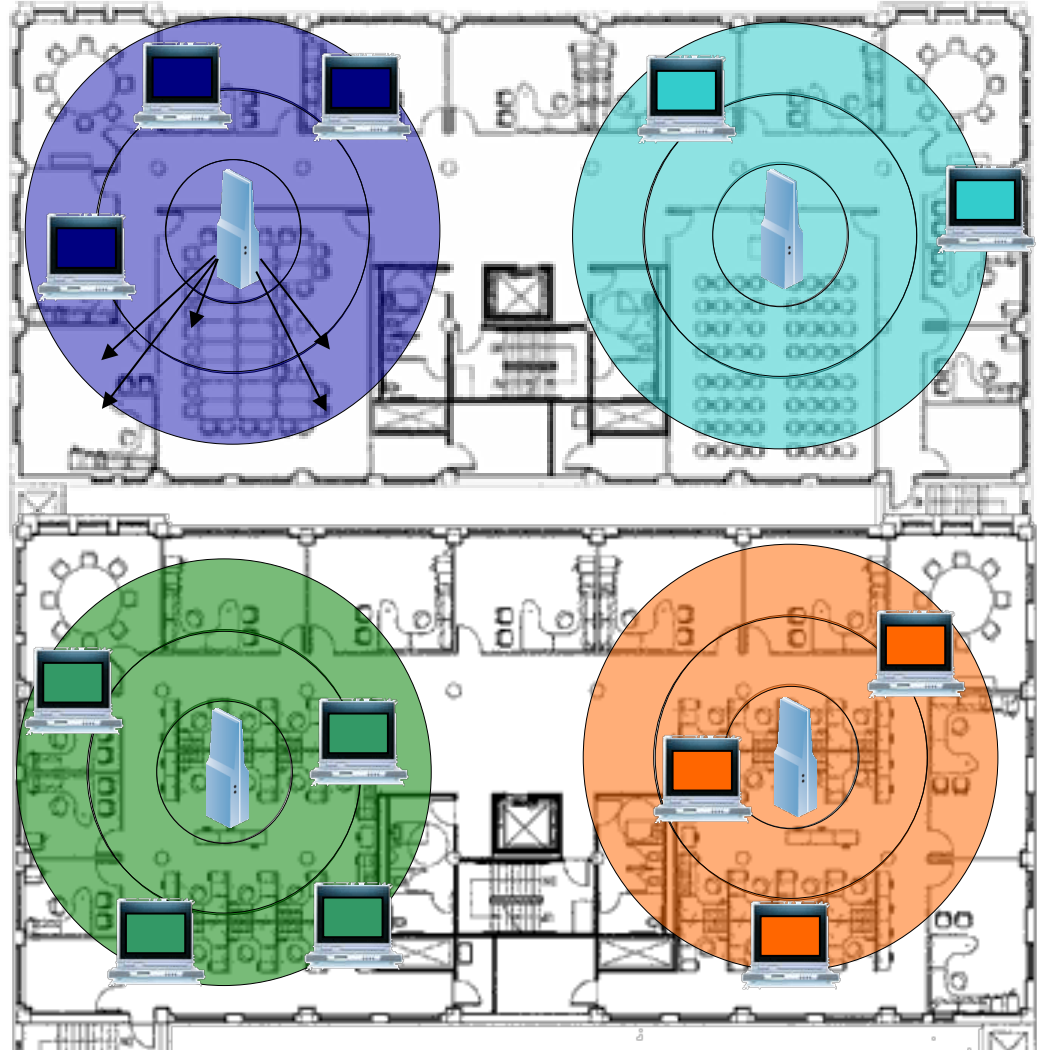
Switch usa servidor Radius
determinar identidade do
usuário
Esta informação é usada
para políticas de QoS e
Segurança

Usuário: maria
Grupo: Marketing
ACL: Corp_1
QoS: Silver

BALANCEAMENTO DE CARGA



Resolver problemas de Performance e Capacidade em áreas de alta densidade: salas de reunião, restaurante...



SEGURANÇA - COMO GARANTIR?

- **WLANs requerem segurança sofisticada e multicamadas**
 - Garantir o controle do acesso
 - Gerenciar o meio
 - Camadas mais altas de segurança como nas redes com fio
- **Autenticação e Privacidade**
 - WEP
 - Autenticação Web
 - IPSec
 - 802.1x
 - 802.11i e WPA
- **Acesso protegido à rede**
 - Prevenir acesso rogue ou intrusos
- **Segurança física dos dispositivos**



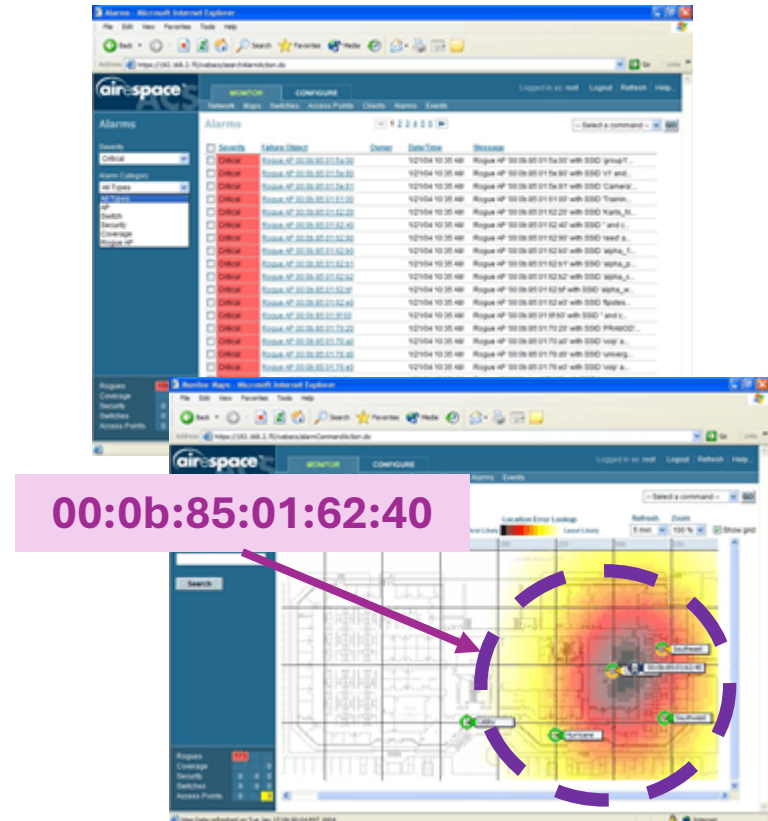
PROTEGENDO A WLAN

- “Defense Shield” – proteger completamente o RF
 - Rogue APs
 - Redes Ad-hoc (peer-to-peer)
 - Detecção e resposta a ataques Denial of Service
 - Listas de exclusão Global
 - Utilizar-se das vantagens das ferramentas de localização



PROTEGENDO DE ROGUE AP

- Rogue APs devem ser eliminados
 - Abrem acesso à rede na ausência de políticas de segurança de IT
- Detecção
 - Alerta ao administrador da rede da presença de rogue AP's na rede
- Localização
 - Descobrir a localização física dos rogue APs em um mapa
 - O OmniVista pode localizar a porta do switch que o rogue AP está conectado.
- Contenção
 - Evita que usuários se associem aos rogue APs



Alarms - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address <https://192.168.2.70/webacs/searchAlarmAction.do> Go Links

airespace™

MONITOR CONFIGURE

Logged in as: root Logout Refresh Help...

Network Maps Switches Access Points Clients Alarms Events

Alarms

Severity: Critical

Alarm Category: All Types

AP
Switch
Security
Coverage
Rogue AP

Rogues: 106
Coverage: 0
Security: 0
Switches: 0
Access Points: 4

Alarms

1 2 3 4 5 6

-- Select a command -- GO

☐	Severity	Failure Object	Owner	Date/Time	Message
☐	Critical	Rogue AP 00:0b:85:01:5a:00		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:5a:00' with SSID 'group1'...
☐	Critical	Rogue AP 00:0b:85:01:5e:80		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:5e:80' with SSID 'x1' and...
☐	Critical	Rogue AP 00:0b:85:01:5e:81		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:5e:81' with SSID 'Camera'...
☐	Critical	Rogue AP 00:0b:85:01:61:00		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:61:00' with SSID 'Trainin...
☐	Critical	Rogue AP 00:0b:85:01:62:20		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:20' with SSID 'Karls_N...
☐	Critical	Rogue AP 00:0b:85:01:62:40		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:40' with SSID " and c...
☐	Critical	Rogue AP 00:0b:85:01:62:90		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:90' with SSID 'reed' a...
☐	Critical	Rogue AP 00:0b:85:01:62:b0		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:b0' with SSID 'alpha_1...
☐	Critical	Rogue AP 00:0b:85:01:62:b1		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:b1' with SSID 'alpha_p...
☐	Critical	Rogue AP 00:0b:85:01:62:b2		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:b2' with SSID 'alpha_x...
☐	Critical	Rogue AP 00:0b:85:01:62:bf		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:bf' with SSID 'alpha_w...
☐	Critical	Rogue AP 00:0b:85:01:62:e0		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:62:e0' with SSID 'fipstes...
☐	Critical	Rogue AP 00:0b:85:01:6f:60		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:6f:60' with SSID " and c...
☐	Critical	Rogue AP 00:0b:85:01:70:20		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:70:20' with SSID 'PRAMOD'...
☐	Critical	Rogue AP 00:0b:85:01:70:a0		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:70:a0' with SSID 'voip' a...
☐	Critical	Rogue AP 00:0b:85:01:76:d0		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:76:d0' with SSID 'univerg...
☐	Critical	Rogue AP 00:0b:85:01:76:e0		1/21/04 10:35 AM	Rogue AP '00:0b:85:01:76:e0' with SSID 'voip' a...
☐	Critical	Rogue AP 00:0b:be:df:71:5f		1/21/04 10:35 AM	Rogue AP '00:0b:be:df:71:5f' with SSID 'tsunami...
☐	Critical	Rogue AP 00:40:96:40:d1:6a		1/21/04 10:35 AM	Rogue AP '00:40:96:40:d1:6a' with SSID 'Mitlan2...
☐	Critical	Rogue AP 00:40:96:45:76:eb		1/21/04 10:35 AM	Rogue AP '00:40:96:45:76:eb' with SSID 'tsunami...

Internet

Monitor Maps - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media Mail Print Send To Favorites

Address <https://192.168.2.70/webacs/alarmCommandAction.do> Go Links >>

airespace™

MONITOR CONFIGURE

Network Maps Switches Access Points Clients Alarms Events

Logged in as: root Logout Refresh Help...

Maps > AIRESpace > Ground

-- Select a command -- GO

Protocol: 802.11a and 802.11b/g Display: Names Location Error Lookup: Most Likely Least Likely Refresh: 5 min Zoom: 100 % Show grid: ☒

Search for: All Maps Enter name: Search

Rogues: 173 Coverage: 0 Security: 0 0 0 Switches: 0 0 0 Access Points: 0 3

Map Data refreshed on Tue Jan 27 09:50:04 PST 2004

Internet

Protocol	Display	Location Error Lookup	Refresh	Zoom	Show grid
802.11a and 802.11b/g	Names	Most Likely Least Likely	5 min	100 %	☒

Search for: All Maps Enter name: Search

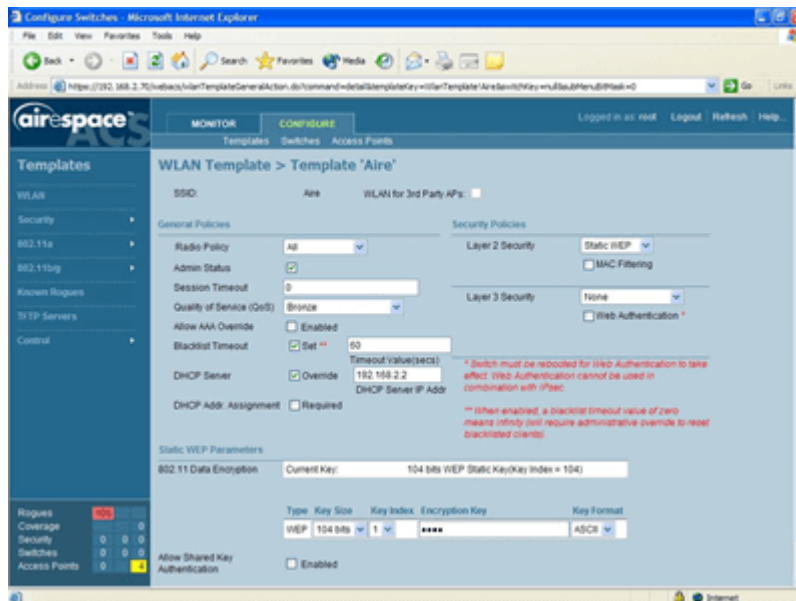
Rogues: 173 Coverage: 0 Security: 0 0 0 Switches: 0 0 0 Access Points: 0 3

Map Data refreshed on Tue Jan 27 09:50:04 PST 2004

Internet

OMNIACCESS WLAN

- > A linha Alcatel OmniAccess WLAN se alinha à arquitetura de segurança de dispositivos definida pela estratégia de segurança Alcatel CrystalSec.



- Segurança “out of the box”
- Gerência segura
 - SSHv2, SSL, TLS, SNMPv2/v3 e certificados X.509
- Todo o tráfego de controle é criptografado
- APs Lightweight: não há nada para ser roubado
- Templates de segurança para mapeamento rápido de políticas de segurança



MONITOR

CONFIGURE

Templates

Switches

Access Points

Logged in as: root

Logout

Refresh

Help...

Templates

WLAN

Security

802.11a

802.11b/g

Known Rogues

TFTP Servers

Control

WLAN Template > Template 'Aire'

SSID:

Aire

WLAN for 3rd Party APs: ☐

General Policies

Radio Policy

All

Admin Status



Session Timeout

0

Quality of Service (QoS)

Bronze

Allow AAA Override



Enabled

Blacklist Timeout



Set **

60

Timeout Value(secs)

DHCP Server



Override

192.168.2.2

DHCP Server IP Addr

DHCP Addr. Assignment



Required

Security Policies

Layer 2 Security

Static WEP

☐ MAC Filtering

Layer 3 Security

None

☐ Web Authentication *

* Switch must be rebooted for Web Authentication to take effect. Web Authentication cannot be used in combination with IPsec.

** When enabled, a blacklist timeout value of zero means infinity (will require administrative override to reset blacklisted clients).

Static WEP Parameters

802.11 Data Encryption

Current Key:

104 bits WEP Static Key(Key Index = 104)

Type

Key Size

Key Index

Encryption Key

Key Format

WEP

104 bits

1

....

ASCII

Allow Shared Key Authentication



Enabled

Rogues

106

Coverage

0

Security

0

Switches

0

Access Points

0

4

SEGURANÇA BASEADA EM PADRÕES

- **Várias camadas de proteção**

- **RF**

- Interferência às frequências 802.11
 - Defesa contra Denial of service
 - Vazamento da área de cobertura
 - Detecção de AP mal configurado

- **Rede**

- Dispositivos seguros
 - Detecção, localização e contenção de rogue APs
 - Prevenção de acessos ad-hoc (peer-to-peer)
 - Access control lists
 - Prevenção de address spoofing

- **Usuário**

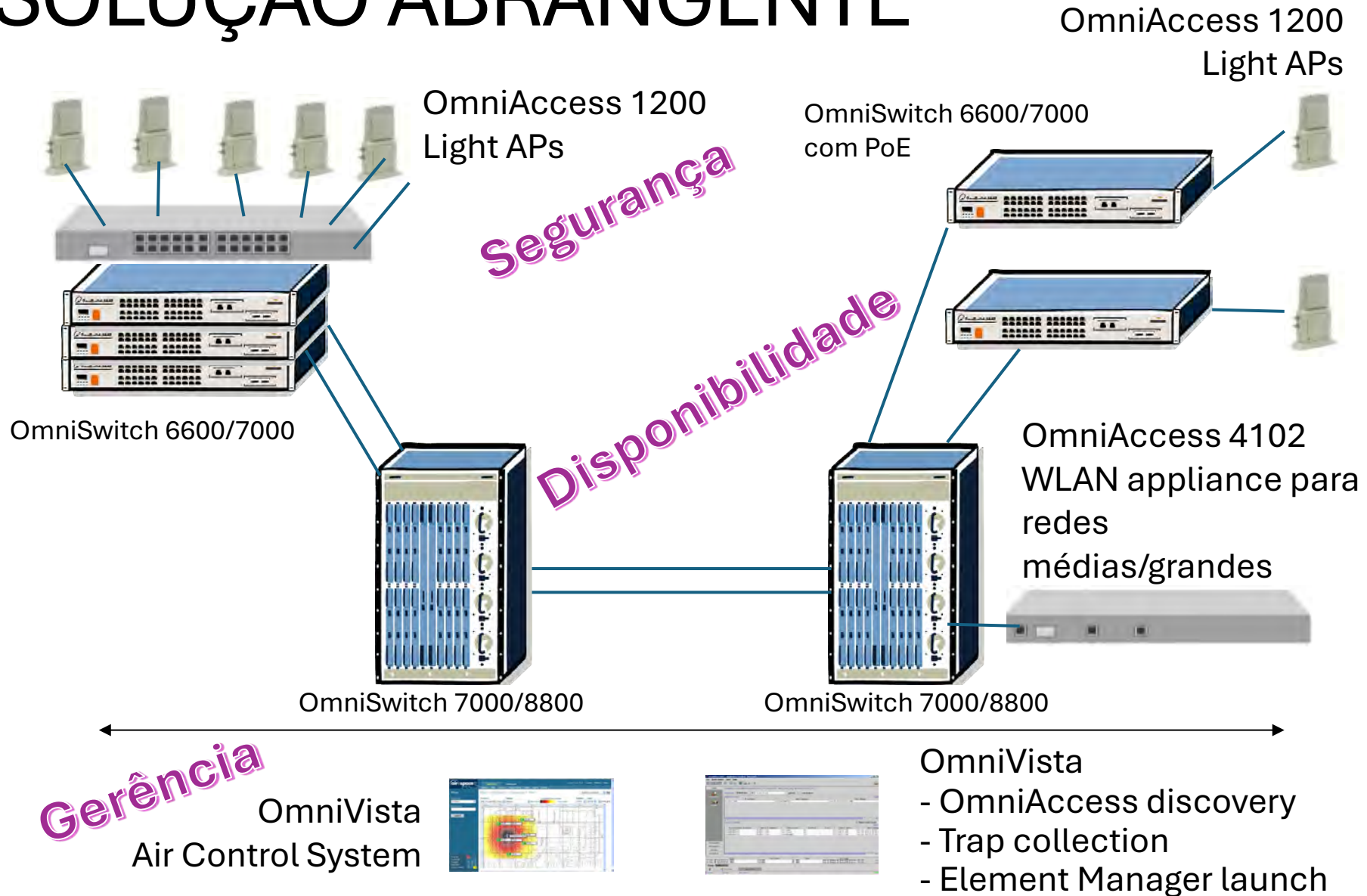
- Proteção contra ataques de dicionário e outros
 - Lista de usuários excluídos
 - Visibilidade de usuários conectados a redes não confiáveis ou de terceiros

- **Rede única para monitoração e encaminhamento de tráfego**

- Não é necessário nenhum hardware ou software adicional



SOLUÇÃO ABRANGENTE



DIFERENCIAIS

- **Gerenciabilidade: Melhor visibilidade e controle do ambiente RF**
 - OmniVista ACS oferece o mais completo sistema de gerência de WLAN
 - Ferramenta de location tracking integrada
 - Estabelecer políticas corporativas de forma centralizada
 - Visibilidade total do ambiente RF
- **Gerência de RF real-time**
 - Auto configuração, auto otimização, auto recuperação
 - Aumenta a performance, reduz custos operacionais do dia-a-dia
- **Proteção Wireless integrada**
 - Rede única para monitoração e encaminhamento de tráfego
 - Detecção, localização e contenção de intrusos na WLAN
- **Suporte para aplicações real-time**
 - Políticas de QoS fim-a-fim para garantir performance
 - Encaminhamento rápido entre APs e entre switches
 - Roaming rápido (<100ms) entre APs, entre switches, ou entre subredes (L2/L3)
 - VoWLAN 802.11e ready

ESTRATÉGIA DE WLAN ALCATEL

“é mais um marco na construção da oferta mais abrangente de redes corporativas convergentes da indústria. Nossa herança em tecnologias móveis, nossa liderança em infraestrutura convergente, e nossa estratégia de criar e suportar novas gerações de aplicações de negócios nos tornam o único fornecedor global equipado para concretizar uma oferta de redes corporativas WLAN verdadeiramente abrangente, baseada em padrões e convergente.”

OBRIGADO PESSOAL