Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Tecnologia da Informação – Segurança da Informação

UNIFIED WIRELESS NETWORK

ARTHUR SANTHIAGO FRANCO

Americana, SP
2013

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Tecnologia da Informação – Segurança da Informação

UNIFIED WIRELESS NETWORK

ARTHUR SANTHIAGO FRANCO

arthursfranco@gmail.com

Trabalho de conclusão de curso apresentada a Faculdade de Tecnologia de Americana como partes das exigências do Curso de Tecnologia em Segurança da Informação para obtenção de título de Tecnólogo em Segurança da Informação.

Americana, SP
2013

ARTHUR SANTHIAGO FRANCO

UNIFIED WIRELESS NETWORK

Trabalho de Conclusão de Curso aprovada como requisito para obtenção do título de Tecnólogo em Segurança da Informação no curso de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Prof. Carlos Henrique Rodrigues Sarro. – FATEC

Convidado: _____
Prof. Alexandre Garcia Aguado. – FATEC

Convidado: _____
Prof. Michel Brites dos Santos. – FATEC

Agradecimentos

Agradeço a Deus por estar presente a cada dia.

Agradeço aos meus pais, por ensinarem a mim os valores de um homem de bem e me ajudar durante os momentos difíceis.

Agradeço por meu irmão, pois sem ele, não saberia o que é compartilhar alegrias.

Agradeço aos meus avós, maternos e paternos, por me mostrar que família é a base da minha história e a base das minhas morais.

Agradeço pelo relógio de bolso, que representa as minhas raízes.

Agradeço meus amigos, por me suportarem, me animarem, me aconselharem e por compartilhar risadas, comemorações, tristezas e apreensões.

Agradeço aos meus professores de curso, especialmente meu orientador, Carlos H. R. Sarro, pelo apoio e pelo conhecimento dividido.

Resumo

Este trabalho visa avaliar e mostrar as vantagens da implementação e administração de uma solução *Wireless Unified Network* em corporações e outros ambientes organizacionais. O modelo avaliado abrange as soluções de administração para WLAN oferecido pela empresa Cisco Systems, comprovada pela sua excelência para soluções em redes, que possibilitou um controle centralizado da solução de infra-estrutura *wireless*, além de disponibilizar documentações técnicas sobre o processo de funcionamento. Desenvolvendo desde conceitos básicos de WLAN e radiofreqüência e focando nos benefícios e na Segurança da Informação da solução, o trabalho aborda os componentes físicos e lógicos do modelo até questões de *Rogue Management* e *Roaming*, explicando detalhadamente o funcionamento de uma solução tão transparente para o cliente final, e igualmente única no meio operacional. Ao final, será apresentado um estudo de caso onde será exemplificado uma situação-problema onde a *Unified Wireless Network* pode ser implementada para a resolução de problemas em WLANs corporativas, visando a melhor operação do usuário final, comprovando o objetivo do trabalho em mostrar as vantagens da *Unified Wireless Network*.

Palavras Chave: Redes Wireless, Unified Wireless Network, WLAN, Cisco Systems.

Abstract

This study aims to evaluate and demonstrate the advantages of the implementation and administration of an Unified Wireless Network solution in corporate and other organizational environments. The model evaluated covers administration solutions for WLAN offered by Cisco Systems, the proven excellence for solutions in networks that enabled centralized control of wireless infrastructure, besides providing technical documentation about your working process. Developing since basics of WLAN and radio and focusing on the benefits and Information Security of the solution, the work addresses the physical and logical components of the model to issues of Rogue Management and Roaming, explaining in detail the operation of a solution as transparent to the client end, and also unique in the operating way. At the end, will be presented a case study which will be exemplified by a situation where Unified Wireless Network can be implemented for solving problems in enterprise WLANs, targeting the best end-user operation, proving the purpose of the work to show the advantages of Unified Wireless Network.

Keywords: Wireless Networks, Unified Wireless Network, WLAN, Cisco Systems.

Lista de Figuras

Sumário

1. INTRODUÇÃO

A rede *wireless* é uma das tecnologias de mais rápida evolução atualmente, onde mais e mais companhias conseguem ver como um recurso de grandes possibilidades. Um dos requisitos atuais dos profissionais de TI (Tecnologia da Informação) é entender os últimos produtos e recursos *wireless* para implantar propriamente uma solução sem fio em uma empresa.

Nos últimos anos começaram a ser propagadas e implantadas as soluções de redes *wireless* unificadas, desenvolvidas para a gestão de redes *wireless* organizacionais de forma centralizada e totalmente integrada entre seus equipamentos e o meio cabeado, facilitando a implementação, configuração e suporte de dispositivos sem fio, para que no final, uma rede segura e de qualidade seja utilizada pelo cliente e o usuário final.

Dentre as várias soluções propostas por diferentes empresas, este trabalho adotou a solução Cisco *Unified Wireless Network* (CUWN) desenvolvida pela Cisco Systems com modelo para seus estudos, examinando todas suas características e benefícios para que uma visão geral das soluções *wireless* unificadas atinja o público alvo deste projeto. A Cisco Systems foi a empresa escolhida, pois ao longo dos últimos anos vem sediando uma posição de destaque no mercado mundial, sendo referência na área de soluções em redes com o desenvolvimento de produtos de alta capacidade.

Este projeto esta organizado de forma a abordar a Cisco *Unified Wireless Network* de maneira linear e sistemática, com foco na Segurança da Informação. Seu início se dá com a inserção de conceitos *wireless*, como WLAN (o objeto raiz em estudo), protocolos de segurança sem fio, topologias e ativos básicos de um cenário *wireless*. Em seguida, será apresentado o funcionamento básico da nova solução, destrinchando em frações referentes aos equipamentos, protocolos e aplicações utilizadas. Por último, serão expostas algumas características importantes, como seus recursos de segurança, suas novas propriedades de *roaming* e suas possíveis aplicabilidades.

Ao longo do projeto, ou seja, ao longo dos capítulos será desenvolvido através de textos, screenshots e imagens, o funcionamento da solução em questão. Ao final será apresentado um capitulo dedicado ao estudo de caso, abordando uma situação-problema num cenário WLAN corporacional com destaque para a Segurança da Informação, onde serão utilizados ferramentas e recursos da UWN para solucionar este incidente, comprovando a eficácia da UWN.

Com a análise desta nova solução é possível perceber que se pode estar diante de um novo paradigma para a administração de WLANs corporacionais, contando com recursos de segurança e gestão avançadas, podendo ser mais um passo para a evolução desta tecnologia que não para.

2. WLAN

O conceito WLAN (*Wireless Local Area Network*) é utilizado para definir uma rede local sem fio, que utilizando sinais de radiofreqüência (RF) e seguindo o padrão IEEE 802.11, conecta aparelhos *wireless* através de uma área de grande cobertura e boas taxas de transmissão (IEEE, 2012).

A distância de operação do padrão pode variar dentre 50 metros para ambientes fechados até 400 metros para ambientes abertos. Porém, sinais de rádio são utilizados para os mais variados serviços e finalidades, sendo necessário que estes operem dentro das exigências governamentais para que o controle seja eficaz e não gere problemas, especialmente interferências. As regras de administração dos sinais podem variar de país para país.

No entanto, algumas freqüências podem ser utilizadas sem aprovação do governo, como a faixa ISM (*Industrial, Scientific and Medical*) que podem operar nos seguintes intervalos: 902 MHz - 928 MHz; 2,4 GHz - 2,485 GHz e 5,15 GHz - 5,825 GHz (VAZZI, 2012).

Criado em 1997 por um grupo de trabalho do IEEE (*Institute of Electrical and Electronics Engineers*) para definição do conceito WLAN, o padrão 802.11 vem estabelecendo normas para a criação e uso das redes sem fio pelos últimos anos, sendo referência em todos os setores, desde a produção de equipamentos até o desenvolvimento de novas tecnologias (AMARAL; MAESTRELLI, 2004).

A seguir será desenvolvido algumas informações referentes ao padrão IEEE 802.11 de WLANs, oferecendo uma base de conhecimento sobre seu funcionamento básico e para o futuro entendimento da *Unified Wireless Network* e sua nova proposta.

2.1. Meios de Transmissão

O padrão 802.11 define uma relação de padrões de transmissão e codificação para comunicações sem fio na camada física. As principais funções da camada física para redes sem fios são:

- Codificação e decodificação de sinais;
- Geração/remoção de parâmetros para sincronização;
- Recepção e transmissão de bits;
- Incluí especificação do meio de transmissão.

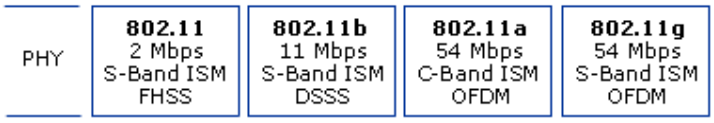


Figura 1 - Camada Física de uma rede 802.11 (TELECO, 2006).

As mais comuns técnicas de codificação são: FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*), ver Figura 1. Os principais padrões de rede sem fio para essa camada são (BULHMAN; CABIANCA, 2006):

2.1.1. 802.11

A taxa de transmissão original desse padrão era de 2 Mbit/s usando-se FHSS e 2,4 GHz (freqüência de operação). Entretanto, sob condições não ideais, uma taxa de transmissão de 1 Mbit/s era utilizada.

2.1.2. 802.11ª

Operando a taxas de 54 Mbit/s na freqüência de 5 GHz e utilizando o OFDM, o padrão 802.11ª foi o primeiro padrão a ser padronizado, porém, apenas atualmente esta sendo fortemente utilizado. O OFDM possibilita que dados sejam transmitidos por sub-frequências e grande taxa de transmissão. Este padrão

também possibilita a transmissão de voz e vídeo via rede sem fio, além de não sofrer interferências de outros tipos de padrões e equipamentos já que opera em uma faixa de freqüência diferente.

2.1.3. 802.11b

Usando a mesma faixa de freqüência de aparelhos microondas, telefones sem fio, câmeras de vídeo e equipamentos *Bluetooth*, o padrão 802.11b suporta taxas de 5,5 á 11 Mbit/s. O DSSS foi a técnica de codificação escolhida para taxas de transmissões maiores.

2.1.4. 802.11g

Fornecendo velocidades semelhantes ao 802.11ª e tendo a possibilidade de interoperabilidade com dispositivos 802.11b, este padrão opera a uma taxa de 54 Mbit/s, utilizando-se da freqüência de 2,4 GHz e modulação OFDM.

2.2. Topologias

Existem três principais tipos de topologias do padrão 802.11 (BULHMAN; CABIANCA, 2006). Podem-se observar graficamente estas topologias através da Figura 2.

2.2.1. *Basic Service Set* (BSS)

Consiste na topologia mais básica, que utiliza um Access Point (AP) conectado á rede cabeada, suportando um ou mais clientes sem fio. Também conhecida como Rede Infra-estrutura ou *Infrastructure Wireless Network*, a BSS tem o inconveniente de consumir o dobro da banda, mas um dos seus grandes benefícios é o armazenamento dos dados enquanto as estações estão em modo de economia de energia (*Power Save*). O AP providencia conectividade entre estações e a rede cabeada, além de possibilitar a comunicação de uma estação com outra estação ou nó do sistema de distribuição (DS).

2.2.2. *Extended Service Set* (ESS)

Uma rede ESS é composta por dois ou mais APs conectados na mesma rede cabeada, geralmente *ethernet*, que pertencem ao mesmo segmento lógico (*subnet*) separado por um roteador. Os clientes podem se mover entre os vários APs através da técnica chamada *Roaming*.

2.2.3. *Independent Basic Service Set* (IBSS)

Conhecidas como topologias *Ad-hoc*, são similares as redes *peer-2-peer* internas. Constituída de pelo menos duas estações, onde não há ponto de acesso que conecte a rede a um sistema de distribuição (DS)

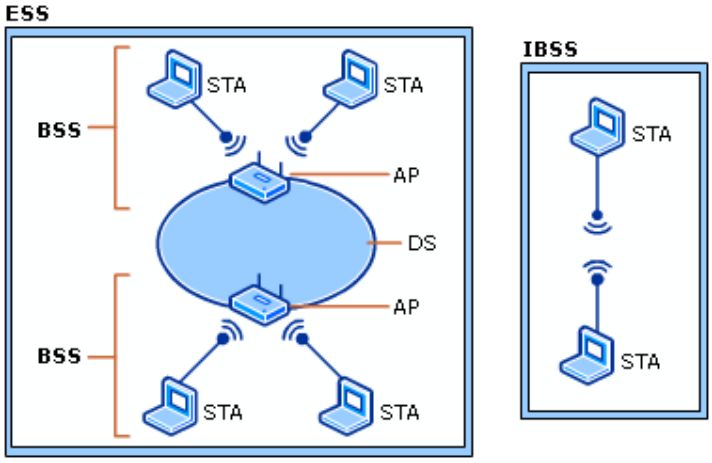


Figura 2 - Arquitetura Lógica de uma rede 802.11 (TELECO, 2006).

2.3. Localização de WLANs

Com um ambiente *wireless* instalado e configurado, os clientes sem fio irão em modo automático começar a procurar WLANs existentes dentro de seu alcance. Este *scanning* é o primeiro processo realizado, já que é onde o cliente tenta se conectar á rede. O cliente utiliza de certas informações para rastrear uma trilha *wireless* deixada por um AP. Esta trilha é composta por dois elementos: o *Service Set Identifier* e os *beacons* (ALVES; GONÇALVES; BARCELOS, 2003).

- ***Service Set Identifier*** **(SSID)** - Valor alfanumérico de 2 a 32 caracteres que define o nome da WLAN. Utilizado como

segmentador de redes e no processo de associação á rede, o SSID é recomendado a não ser divulgado em redes privadas e de acesso restrito. Apenas com a configuração correta do SSID do AP no cliente se poderá dar a conexão entre eles;

- ***Beacon*** - Pacotes enviados do AP para os clientes com a finalidade de sincronizar a comunicação sem fio numa WLAN.

2.4. Protocolos de Segurança

A utilização de protocolos de segurança não se restringe apenas ao meio cabeado, sendo possível e necessária a sua implantação também no meio sem fio. A seguir, serão apresentados alguns destes protocolos (AMARAL; MAESTRELLI, 2004).

2.4.1. *Wire Equivalency Privacy* (WEP)

Fornecendo um meio de criptografia entre o cliente e o AP, este protocolo foi o primeiro a ser utilizado para esta função criptográfica no meio *wireless*. Trabalhando na camada de Enlace, o WEP utiliza o algoritmo RC4 da RSA para criptografar os pacotes que serão trocados dentro de uma rede *wireless*. O RC4 usa um vetor de inicialização de 24 bits e uma chave secreta compartilhada k de 40 ou 104 bits, gerando uma seqüência criptografada RC4 (k,v) de 64 ou 128 bits (AMARAL; MAESTRELLI, 2004).

2.4.2. *Wi-fi Protected Access* (WPA)

Criado para substituir o WEP e suas vulnerabilidades, este protocolo usa a concepção de chave temporária. A compatibilidade com o protocolo WEP, a fácil migração para o padrão WPA (requer apenas atualizar *software*) e a integração com novos e velhos padrões 802.11 faz com que a utilização do WPA cresça nestes últimos anos. Apesar de formalmente não ser um padrão IEEE, o WPA é largamente utilizado (AMARAL; MAESTRELLI, 2004).

2.4.3. IEEE 802.1x e protocolo EAP

Um dos grandes responsáveis pela segurança das redes *wireless* atuais é o padrão IEEE 802.1x que desenvolveu um mecanismo de segurança de acesso otimizado, baseado em autenticação prévia dos usuários antes do usufruto dos recursos e serviços da rede. Utilizando serviços de autenticação para a identificação do usuário, este padrão geralmente utiliza servidores autenticadores RADIUS para ajudá-lo neste processo (AMARAL; MAESTRELLI, 2004).

Atuando junto com o *Extensible Authentication Protocol* (EAP), o 802.1x pode prover um ambiente seguro baseado em várias técnicas de autenticação para as redes sem fio atuais. Definido pela RFC 2284, o EAP fornece métodos de autenticação e credenciais de usuários (*passwords*, cerificações, etc.). Apesar de muito difundido, o EAP não é um padrão IEEE já que várias versões são propagadas e nenhum padrão simples foi identificado para se formalizar. Outra vantagem é a sua capacidade de suportar múltiplos métodos de autenticação (*smart cards*, *transport layer security*, TLS, Kerberos Microsoft, etc.).

3. CISCO *UNIFIED WIRELESS NETWORK*

Criada pela Cisco Systems, a solução *Unified Wireless Network* visa a implementação e administração de um ambiente sem fio de alto desempenho, proporcionando segurança e mobilidade para todos seus clientes. A seguir, será desenvolvido temas relacionados á solução, seus equipamentos, protocolos e plataformas de gerenciamento, além de recursos de segurança, características de *roaming*/mobilidade e possíveis aplicações do modelo em diversos ambientes, sejam eles corporativos ou públicos. Ao decorrer dos capítulos também será possível identificar as diferenças da UWN, desenvolvida pela Cisco, e as redes sem fio atuais, que atuam através dos APs *standalones* e sem um equipamento de gerenciamento central como os *Wireless Controllers*, além de muitas outras funcionalidades ausentes.

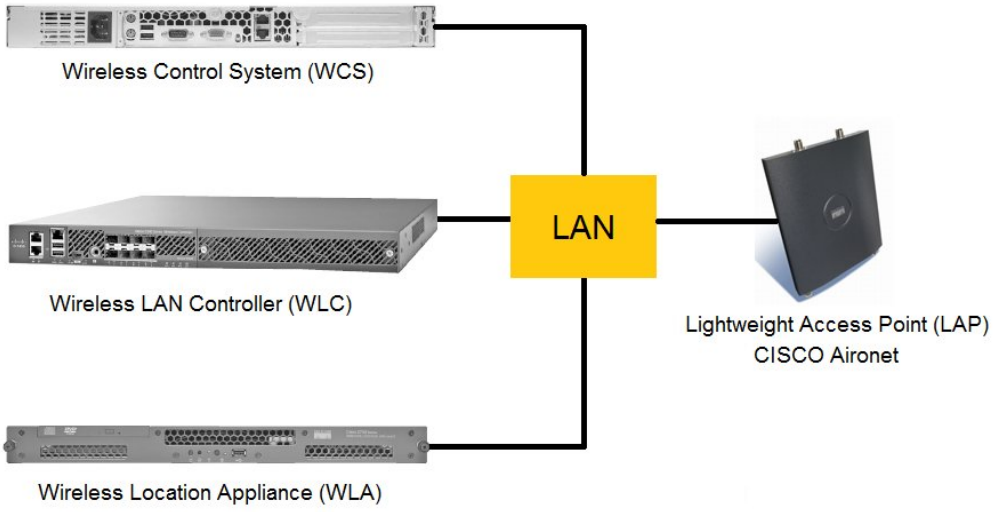


Figura 3 - Topologia física básica da Unified Wireless Network (AUTORIA PRÓPRIA).

3.1. A solução

A implementação de um projeto unificado da rede *wireless* ocorre primeiramente com a implantação do *Wireless LAN Controller* (WLC), equipamento principal da solução que tem função de gerenciar todos os pontos de acesso conectados a rede local, podendo automatizar as operações da WLAN,

pois toda a administração inteligente da rede *wireless* fica presente neste equipamento e não mais nos pontos de acesso como nas estruturas descentralizadas antigamente utilizadas (ver Figura 3), também conhecidas como estrutura standalone (autônoma). Apesar de variar por modelo, o WLC consegue suportar de 50 á 6000 APs (*Access Points*), mas dependendo do ambiente e das necessidades da organização, os mesmos podem ser configurados para trabalhar em *Load Balancing* e redundância, gerenciando apenas metade dos APs, mas aumentando a disponibilidade e qualidade da WLAN. Os modelos de APs necessários para se integrar aos WLCs na infra-estrutura da solução são os chamados LAPs ou *Lightweight Access Points* (ODORIZZI, 2010).

A seguir, é necessária a implantação do *Wireless Location Appliance* (WLA), um aplicativo opcional da solução que recolhe, computa e armazena a localização física dos clientes da rede local *wireless*, realizando estas operações através das informações recebidas dos WLCs. Todo esse processo se inicia através das informações de força de sinal (RSSI) coletadas pelos LAPs conectados á WLAN, e futuramente encaminhados para os WLCs através do protocolo LWAPP. Os *controllers* então agregam informações RSSI e as enviam para o WLA pelo protocolo SNMP. Pelo mesmo protocolo SNMP os dados do *Location Appliance* são comunicados ao *Wireless Control System* (WCS) para que este gere a localização física dos clientes de forma gráfica nos mapas da organização. Todos os equipamentos devem estar integrados entre si, seja diretamente ou através da LAN, para que as informações cheguem precisas para a administração da rede sem fio. Apesar de ser um aplicativo opcional, a utilização do WLA contribui para a formação de uma rede *wireless* baseada em localização, um recurso muito importante e que pode ser amplamente utilizado nos dias de hoje (ODORIZZI, 2010).

Por fim, com a instalação do WCS (através de uma maquina virtual) será criada uma plataforma de gerenciamento central de toda WLAN, desde os WLCs e LAPs até a construção e manutenção dos mapas do WLA, criando assim uma rede unificada sem fio de máxima qualidade e alta disponibilidade (ODORIZZI, 2010).

3.2. Requisitos e Serviços Corporacionais

Com a implantação de redes sem fio nas empresas, criou-se ao decorrer do tempo uma maior necessidade de depender dela para fins corporacionais, e consequentemente, desenvolvê-la e adaptá-la aos objetivos da empresa.

Assim, certos requisitos se mostraram importantes com o crescimento das WLAN's, para que a necessidade corporacional seja atendida. A *Unified Wireless Network* da Cisco foi desenvolvida pensando em atender este requisitos (ODORIZZI, 2010). Segue abaixo, alguns dos requisitos para as redes w*ireless* atuais:

- A cobertura total da área da empresa;
- A centralização de administração dos pontos de acesso e clientes;
- Ferramenta que permitisse a disponibilização de internet *Wi-Fi* para terceiros através de uma rede isolada;
- Recurso de localização através de mapas, ou plantas baixas da organização;
- Compatibilidade, unificação e integração do sistema WLAN e dos equipamentos envolvidos (*switches*, telefones IP *Wireless*, AP's).

A UWN também oferece variados tipos de serviços através da sua rede, os principais são: Segurança, conformidade e monitoração 24x7 contra violações através do meio *Wireless*; Controle de acesso à rede com base na localização do usuário; Redes de hóspedes para clientes, parceiros e auditores; Redes públicas de acesso; Voz em tempo real para comunicações movéis; Melhor colaboração via comunicações unificadas movéis; Resposta rápida ao serviço do cliente; Gestão de ativos e fluxo de trabalho simplificado usando localização histórica de dados. Ao longo do trabalho serão apresentadas as vantagens mencionadas anteriormente, além de novos recursos operacionais e de segurança.

3.3. Equipamentos

Nos tópicos a seguir serão abordadas características dos principais equipamentos que integram a *Unified Wireless Network*.

3.3.1. *Lightweight Access Point* (LAP)

Pontos de acesso (APs) fornecem uma maneira de estender redes cabeadas ou instalar componentes de rede onde a fiação física normal não pode ser instalada. APs também proporcionam alternativas de conectividade por uma fração do custo normal. APs vêm em dois tipos ou grupos atualmente:

- Um dispositivo autônomo (*standalone*) que interage diretamente com a rede cabeada;
- Um sistema de duas partes que se baseia em um controlador (*controller*). APs se comunicam diretamente com um *controller* ou equipamento central e este dispositivo interage diretamente com a rede cabeada.

Cada grupo possui características únicas, podendo ser tanto benéficas quanto maléficas. Ambos os mecanismos suportam conectividade 802.11a/b/g/n para ambientes internos e externos (GRESS; JOHNSON, 2010).

Figura 4 - Lightweight Access Point (CISCO, 2013).

Os *Lightweight APs Aironet* da Cisco (ver Figura 4) são APs que foram convertidos para rodar o protocolo LWAPP e operar com WLCs. Eles fornecem segurança e facilitam a implantação e gestão de itens de controle direcionados para WLANs corporacionais de larga escala. Como elementos-chave da Cisco *Unified Wireless Network* - um sistema integrado, de ponta a ponta – Os Cisco Aironet APs oferecem recursos abrangentes, incluindo o seguinte:

- Voz sobre IP sem fio;
- Acesso para convidados;
- Prevenção e detecção de intrusão via *Wireless;*
- Serviços baseados em localização.

Os preços de um LAP Aironet da Cisco pode variar de R$500 á R$26500 dependendo da tecnologia empregada no dispositivo (CISCO, 2013).

3.3.2. *Wireless Location Appliance* (WLA)

O *Location Appliance Cisco Wireless* (ver Figura 5) é a primeira solução da indústria de redes que simultaneamente rastreia milhares de dispositivos de dentro da infra-estrutura WLAN. Trazendo uma aplicação baseada em localização de alta resolução para aplicações críticas como o rastreamento de ativos de grande valor. Além disso, oferece opções de implantação de gestão de TI, segurança e política de negócios. Essas características tornam o *Wireless Location Appliance* um recurso crítico para toda a classe empresarial de WLANs hoje em dia.

Figura 5 - Wireless Location Appliance (CISCO, 2013).

O WLA é uma solução inovadora, fácil de implantar, que usa tecnologia digital avançada de radiofreqüência (RF) para monitorar simultaneamente milhares de dispositivos sem fio 802.11 diretamente de dentro de uma infra-estrutura WLAN, aumentando a visibilidade dos ativos e o controle do espaço sem fio. Além disso, o aparelho fornece alertas baseados em localização para uma aplicação de política de negócios, além de ricos registros históricos que podem ser usados para a localização de tendências, resolução de problemas e gerenciamento de capacidade de RF. Ao permitir a implantação de poderosos aplicativos baseados em localização, o aparelho torna-se uma solução crítica para clientes de grande porte (CISCO, 2006).

Pelo projeto, o WLA está diretamente integrado na infra-estrutura WLAN para reduzir o custo total da propriedade do cliente e ampliar o valor e segurança da infra-estrutura WLAN existente, tornando-a "*location aware*". Como um componente da Cisco *Unified Wireless Network*, a *Location Appliance* usa *Wireless LAN Controllers* e *Aironet Lightweight Access Points* para rastrear a localização física de dispositivos sem fio por metros, como pode ser observado na Figura 6. O preço do WLA pode variar de R$4000 á R$7000 (CISCO, 2013)

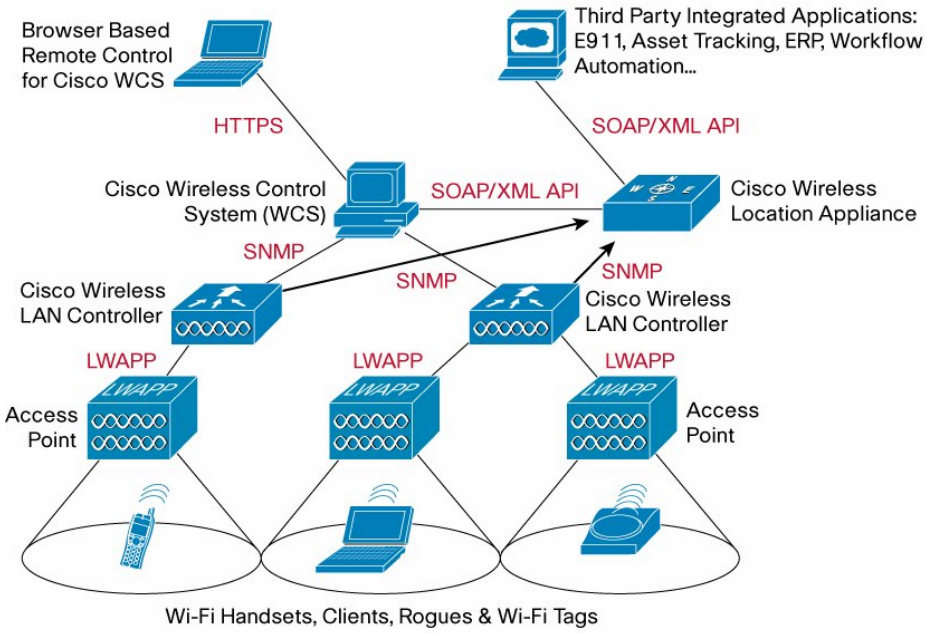


Figura 6 - Visão Geral da Arquitetura dos Serviços Integrados de Localização da UWN (CISCO, 2006).

A Cisco *Location Appliance* sem fio usa os mesmos *Lightweight* APs que proporcionam tráfego como "leitores" de localização para clientes sem fio 802.11 e *Wi-Fi tags*. Esses pontos de acesso coletam e recebem indicações de força de sinal (RSSI) de todos os dispositivos Wi-Fi, incluindo laptops Wi-Fi, aparelhos de voz, *Wi-Fi tags*, dispositivos não autorizados (*rogue devices*) e pontos de acesso não autorizados. As informações RSSI coletadas são então enviadas através do *Lightweight Access Point Protocol* (LWAPP) para os *Wireless LAN Controllers* integrados á rede *wireless*. Os *controllers*, em seguida, agregam as informação RSSIs e enviam para o *Wireless Location Appliance* através do *Simple Network Management Protocol* (SNMP). O *Location Appliance* executa cálculos de localização com base nas informações RSSI recebidas dos WLCs, estas as quais devem estar associadas *ao Wireless Location Appliance*.(CISCO, 2006).

O WLA incluí uma variedade de ferramentas de pré e pós implantação que simplificam a implementação e gestão dos serviços. Abaixo segue algumas dessas principais ferramentas que ajudam a implementar e monitorar uma WLAN de qualidade.

- ***Planning Mode Tool*** - Este modo de ferramenta fornece recomendações para a implementação de APs numa WLAN (ver Figura 7);

Figura 7 - Planning Mode Tool (CISCO, 2006).

- ***Location Readiness Assessment Tool*** - Esta ferramenta ajuda os clientes a determinar se a WLAN atual é suficiente para suportar as especificações dos aparelhos sem fio (ver Figura 8);

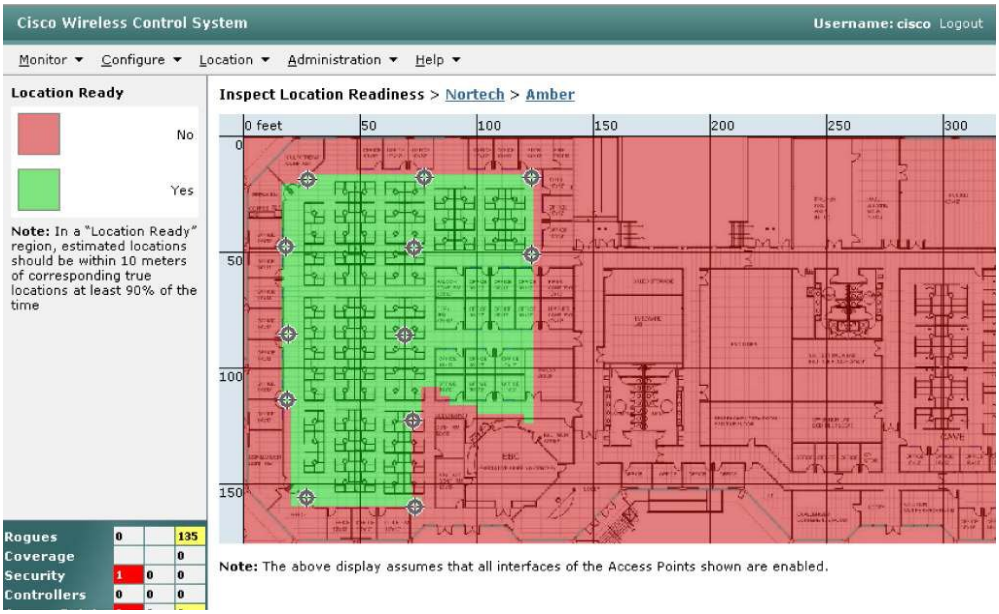


Figura 8 - Location Readiness Assessment Tool (CISCO, 2006).

- ***Calibration Tool*** — Clientes podem optar por realizar uma calibração pós-implantação de sua rede se esta se torna fora de especificação. Durante esta calibração, um dispositivo cliente 802,11 sem fio é usado para fazer medições de RSSI no meio do ambiente *wireless*. O RSSI medido é então utilizado pelo sistema de localização para afinar a precisão da localização do dispositivo. Melhorias na precisão de localização dos aparelhos podem ser visualizadas usando a ferramenta *Location Inspector Tool*;

- ***Location Inspector Tool*** — Esta ferramenta é usada pós-implantação para determinar a precisão de localização através de toda WLAN. Fornece uma representação visual da qualidade da precisão de localização dos dispositivos. Também pode ser utilizado para ajuste de desempenho da rede enquanto esta esteja sendo desenvolvida ou implementada (CISCO, 2006).

3.3.3. *Wireless LAN Controller* (WLC)

O *Wireless LAN Controller* (equipamento visto na Figura 9) é um dispositivo que assume um papel central dentro da *Unified Wireless Network* (UWN) proposta pela Cisco. Tarefas consideradas tradicionais dos *Access Points*, como a associação e a autenticação de clientes *wireless*, são realizadas agora pelo WLC. Os *Access Points*, chamados de *Lightweight Access Points* (LAPs) neste sistema unificado, se registram com um WLC e enviam todos os pacotes de dados e gerenciamento para os WLCs, que depois mandam os pacotes dos clientes até a porção cabeada da rede. Todas as configurações são realizadas através do WLC, equipamento que pode chegar ao preço de R$120000, dependendo da quantidade de APs suportados. LAPs baixam toda sua configuração dos WLCs e agem como uma interface sem fio para os clientes.

Figura 9 - Wireless LAN Controller (CISCO, 2013).

Com a introdução do WLC na arquitetura *wireless* pode-se estar diante de uma nova topologia sem fio, onde o *controller* atua como o cérebro e os LAPs como apenas uma interface de acesso á usuários, diferente das topologias já existentes (ver capitulo 2.2. Topologias).

Como mencionado em capítulos anteriores, os APs *standalones* eram conectados diretamente no meio cabeado e cada um necessitava de uma configuração especifica, tornando lento e cansativo o processo de implantação e configuração do sistema sem fio. Com o WLC, as configurações podem ser implantadas nos LAPs no momento em que estes se tornam operantes, além de oferecer uma vasta seleção de recursos de segurança, como será visto ao

decorrer deste trabalho. Abaixo segue duas figuras exemplificando a diferença de gerações da tecnologia *wireless* antes e depois do WLC.

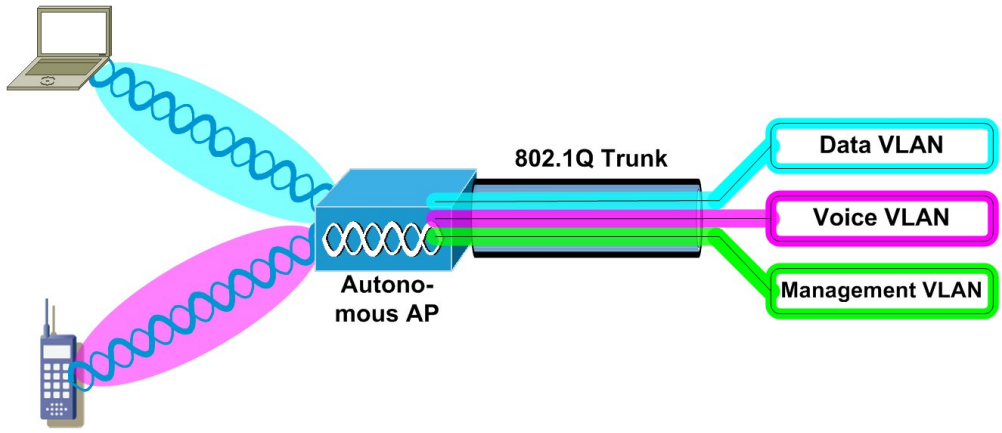


Figura 10 - 1ª e 2ª Geração – AP's atuando em modo bridge, colocando o tráfego de clientes em VLANs locais (CISCO, 2008).

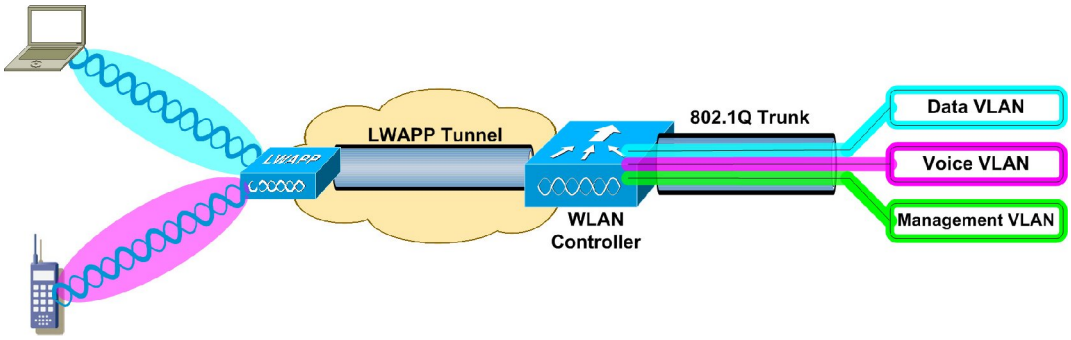


Figura 11 - 3ª Geração – Controller gerencia tráfego cliente centralmente (CISCO, 2008).

Com a responsabilidade de ser o equipamento "cérebro" da solução, o WLC oferece várias funcionalidades, como: o registro de novos perfis de WLAN; desabilitação de pontos de acesso; monitoramento da segurança da WLAN; identificação de pontos de acessos desconhecidos dentro (capitulo 3.7.7. Rogue Management) e próximos a empresa; geração de *logs* e alertas de segurança em diferentes categorias; verificação do histórico e detalhes de clientes e LAPs conectados.

3.4. Protocolos

Outra das grandes mudanças da solução *standlone* para a solução unificada foi a utilização de um novo protocolo para a gerencia de LAPs pelos WLCs. Este protocolo foi desenvolvido especialmente para a *Unified Wireless Network* e seus requisitos de qualidade e segurança. A seguir será apresentado o protocolo que faz com que todo sistema sem fio unificado funcione dentro das especificações da administração e do cliente final.

3.4.1. *Lightweight Access Point Protocol* (LWAPP)

Implantações de *Wireless* LANs (WLAN) tradicionais utilizavam um número X de pontos de acesso (AP) espalhadas por todo o local que precisavam de cobertura sem fio. Com o AP autônomo (*standalone*), cada AP era uma entidade individual, que precisava de configuração, provisionamento de monitoração, e assim por diante. Se essas tarefas fossem necessárias para apenas alguns dispositivos, eles seriam administráveis, no entanto, quando você está falando de uma empresa com uma WLAN completa, que pode estar oferecendo serviços avançados como Voz sobre *Wireless*, a gestão de cada AP torna-se assustadora (GRESS; JOHNSON, 2010).

Você pode adicionar complexidades adicionais a uma WLAN empresarial, tais como gestão de freqüência de rádio (se adaptar dinamicamente às mudanças no ambiente) e de segurança, o que é crítico no ambiente *wireless* por causa da natureza do meio de transmissão. A menos que algum tipo de coordenação seja implantada, mais cedo ou mais tarde, a empresa vai atingir limitações práticas e de escalabilidade. O *Lightweight Access Point Protocol* (LWAPP) foi projetado para superar essas limitações e expandir o conjunto de recursos e usos de WLANs, sem aumentar a carga de gerenciamento do ponto de vista da segurança da empresa. LWAPP não é uma solução geral. Em alguns cenários, um AP tradicional é melhor - por exemplo, com conexão ponto a ponto, onde nenhuma coordenação ou monitoramento de RF é necessário por causa das características do ambiente controlado para essa implantação (GRESS; JOHNSON, 2010).

Dado o crescimento das redes sem fio e a onipresença que estes serviços têm nas empresas atualmente, os fornecedores têm implementado várias abordagens para simplificar a operação e implantação de serviços sem fio. Proposto como uma forma potencial de simplificar a operação das redes sem fio, o LWAPP foi implementado em todo o conjunto de produtos da Cisco *Unified Wireless* (*Wireless LAN Controller*, APs e dispositivos relacionados) a partir de sua versão de software inicial. Mesmo que nunca tenha se tornado um padrão RFC, o LWAPP ainda é um protocolo relevante e amplamente utilizado. As idéias por trás do LWAPP são os seguintes (GRESS; JOHNSON, 2010):

- Encaminhamento de tráfego com funções de segurança, como autenticação e políticas de segurança a partir da borda (AP) em direção a um ponto centralizado (WLC);

- Simplificar o AP, porque funções de nível superior agora são feitas separadamente, o que reduz a complexidade e custo do AP;

- Fornecer um mecanismo de encapsulamento e transporte para o tráfego sem fio;

- Centralizar configuração e gerenciamento de APs.

LWAPP é um caminho de comunicação direto do AP para com uma entidade de gestão - o WLC. Esta nova abordagem para as redes sem fio foi projetada para ter nós ou pontos de presença em toda a rede. Estes dispositivos nós não exigem configuração e contam com um dispositivo mestre para suas configurações e instruções. Esses nós existem para fornecer um ponto na rede para que um usuário sem fio possa se conectar. Depois que um usuário se conecta, todo o tráfego indo para este nó seria enviado para o dispositivo mestre. O dispositivo mestre, então, determina aonde na rede ou sobre que Virtual LAN (VLAN) o pacote precisa ir. Esta abordagem oferece muitas vantagens sobre a configuração do dispositivo, mas exige um protocolo para fornecer conectividade constante e direção de operação para esses dispositivos. O LWAPP fornece a solução (GRESS; JOHNSON, 2010).

3.5. Plataforma de Gerenciamento

A UWN também conta com uma plataforma de gerenciamento chamada *Wireless Control System*, onde toda a administração da rede sem fio é feita de maneira fácil e intuitiva. A seguir serão apresentadas algumas das características da plataforma.

3.5.1. *Wireless Control System* (WCS)

O *Wireless Control System* é a ferramenta que gerencia os WLCs e o WLA. Com este aplicativo é possível gerenciar os ciclos de uma rede WLAN (ver Figura 12). Segundo a Cisco Systems, os benefícios e características da plataforma são:

- Possibilidade de gerenciamento centralizado de até 30000 APs com o WCS *Navigator*;
- Acompanhamento do ciclo de vida da WLAN, desde o planejamento até o monitoramento;
- Projetar a área de instalação e cobertura dos APs através de ferramentas de design e planejamento da WLAN;
- Verificação em tempo real da disponibilidade da WLAN, com possibilidade de auditorias;
- Segmentação da WLAN, criando vários SSID's, cada um com diferentes permissões de tráfego, seja para funcionários, clientes ou visitantes;
- Providencia segurança através de um modulo IPS (*Intrusion Prevention System*), além de também poder gerar alarmes e eventos para dispositivos e clientes não autorizados.

Figura 12 - Ciclos de Serviço do WCS (CISCO, 2010).

A seguir serão apresentadas as principais funcionalidades do WCS. É possível verificar na figura abaixo a interface principal do aplicativo, mostrando uma visão abrangente da rede sem fio através de gráficos (ver Figura 13 e 14) exibindo o número de equipamentos ativos, tais como *Wireless LAN Controllers*, Pontos de acesso por freqüência e quantidade de clientes por horário.

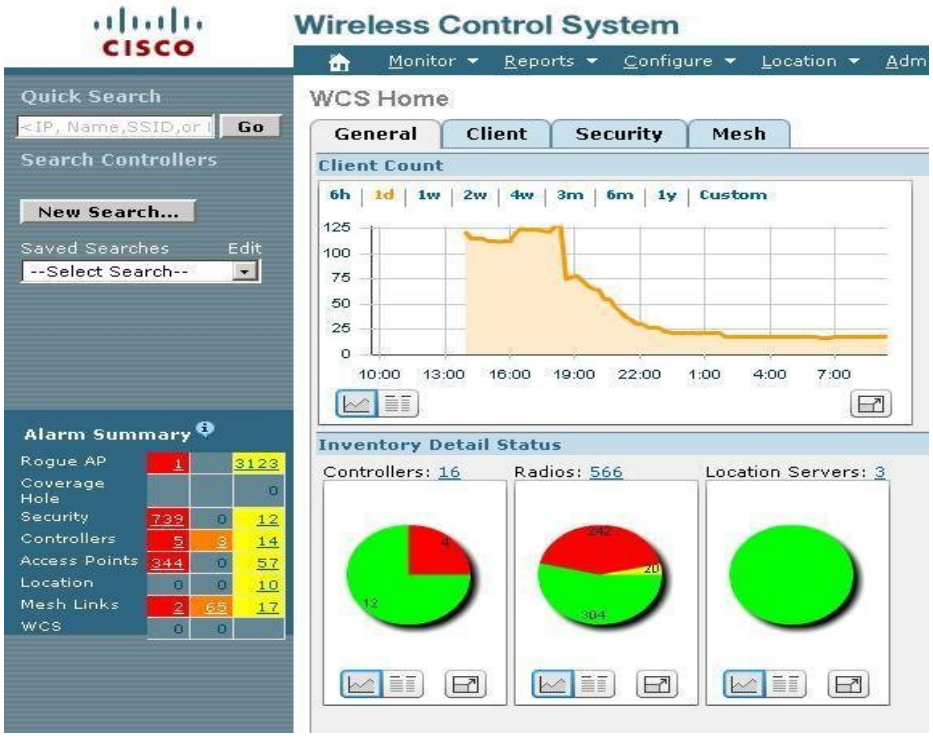


Figura 13 - WCS Home com contagem de clientes e detalhes de inventário (CISCO, 2010).

A visão gráfica facilita a visualização da quantidade de clientes por tipo de protocolo A/B/G, quantidade de clientes por AP e também a respectiva taxa de *downstream* (banda de *download*) e *upstream* (banda de *upload*) geral dos clientes. O aplicativo também disponibiliza a inserção de filtros, mostrando o histórico de clientes como quantos GHz estão sendo utilizados, como também os clientes associados, autenticados, detectados, excluídos e proibidos. O WCS exibe variadas visões de segurança e monitoramento, todas estas customizáveis de acordo com a necessidade do cliente e da infra-estrutura *wireless*.

Figura 14 - WCS Home com o tráfego do cliente e áreas de cobertura (CISCO, 2010).

O administrador do aplicativo WCS também consegue selecionar um cliente especifico autenticado em um Ponto de Acesso para verificar detalhes sobre este, como: Endereço IP e MAC do cliente, protocolo e perfil de WLAN que o usuário esta associado, taxa de pacotes enviados e recebidos, tipo de encriptação e histórico de associação e *roaming* na rede. Outras funções também

são disponibilizadas para facilitar o trabalho do administrador na resolução de problemas, como: visualização da localização atual do cliente, remoção de clientes, geração de relatórios da conexão do usuário e detecção dos APs que o cliente consegue captar.

O WCS oferece também a opção de *troubleshooting* do cliente (como mostrado na Figura 15) que faz um pequeno teste de quatro etapas como: teste de associação, teste de autenticação, teste de atribuição de endereço IP e acaso o WCS identifique algum problema durante estas etapas, irá informar na interface o problema que pode esta ocorrendo com o cliente, sugerindo uma resolução para este determinado problema. Também é possível capturar log´s de um cliente especifico e também observar o histórico de eventos de um usuário. (ODORIZZI, 2010).

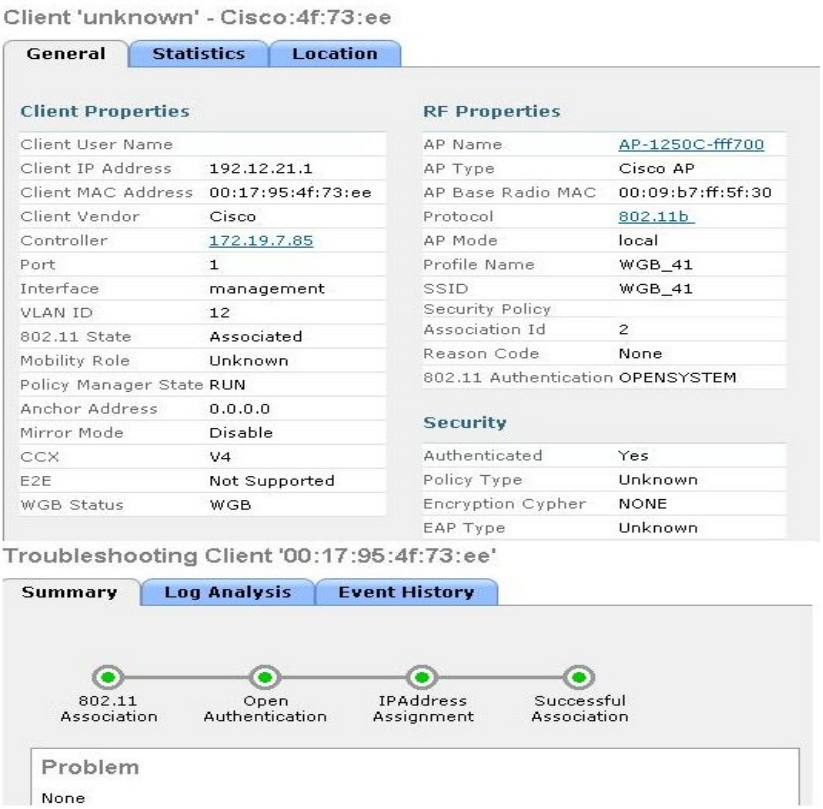


Figura 15 - Detalhes e Troubleshooting de Clientes (CISCO, 2010).

O WCS também provê um modulo onde o administrador visualiza a cobertura dos pontos de acesso dentro de um perímetro, conseguindo verificar a localização dos clientes, intensidade do sinal, além de poder identificar nos mapas a localização de *wireless* TAG's (sensores), pontos de acesso e clientes não autorizados, caso houvesse pontos de acesso que sobrepõe os canais ativos dos pontos de acesso controlado pelos controladores *wireless*, no mapa seria gerado um alerta especifico a esta situação (ODORIZZI, 2010).

Com a construção do mapa, a visão da necessidade de mais pontos de acesso se torna clara (ver Figura16), pois após o posicionamento dos pontos de acesso no mapa a ferramenta indica os pontos de sombra e a intensidade de sinal de cada área do setor através de cores que representam a força do sinal, como observado no exemplo da figura os pontos com melhor alcance de sinal estão em amarelo e os pontos mostrados com críticos pela ferramenta estão em azul, pois representa fraca intensidade de sinal (ODORIZZI, 2010).

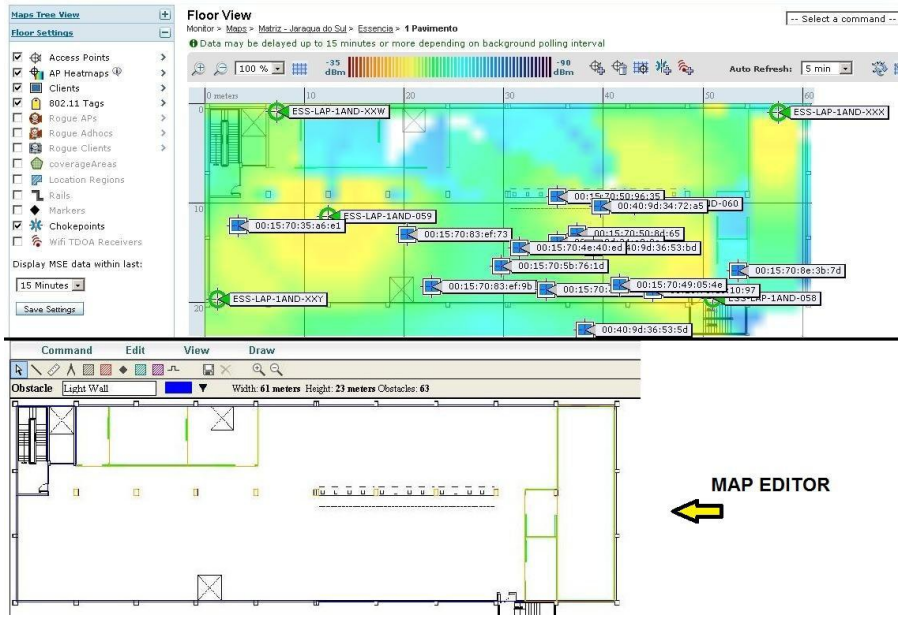


Figura 16 - Visão de cobertura e Editor de mapas (ODORIZZI, 2010).

Todo o mapa é construído através do WCS, uma planta baixa em formato CAD é importada para o WCS através de um editor próprio da ferramenta e todas as paredes ou obstáculos são colocados, selecionando os tipos de materiais como: parede fina, parede grossa, vidro ou madeira. Através destas informações e após a inclusão dos pontos de acesso no mapa, a ferramenta efetua os cálculos de propagação do sinal.

Figura 17 - Módulo de relatórios do WCS (CISCO, 2010).

O WCS possui o módulo de relatórios (como visto na Figura 17) que permite diversos tipos de relatórios sejam gerados sobre a WLAN, podendo ser divididos em: cliente, visão geral, equipamento, convidados, desempenho e segurança. O acompanhamento dos relatórios em tempo real também é possível, verificando detalhes do cliente através de gráficos que indicam o histórico de associação com APs e a intensidade de sinal captada por este cliente (ODORIZZI, 2010). O WCS pode custar de R$3500 á R$9000 (CISCO, 2013).

3.6. Mobilidade *& Roaming*

Um evento de mobilidade ocorre quando um cliente vaga entre APs ou entre *controllers*. Se a LAN sem fio (WLAN) é segura, 802.1x ou *Wi-Fi Protected Access* (WPA), o cliente deve se autenticar novamente para cumprir com o padrão IEEE 802.11i. É preferível que esse processo tenha baixa latência e seja transparente para o usuário o quanto possível enquanto se mantêm a segurança (GRESS; JOHNSON, 2010).

O WLC atua como autenticador central e trata todos os *frames* 802.1x. Após a autenticação ser concluída, o *controller* envia o material criptográfico necessário para o AP. Com base na arquitetura LWAPP, todo o tráfego do cliente é enviado centralmente pelo túnel até o *controller*. Esta característica fundamental permite que todos os APs registrados possam servir cada cliente VLAN, mesmo se os APs estão em diferentes sub-redes/VLAN (*intra-controller roaming*). Isto é algo que não é possível em uma solução *standalone*.

Além do tráfego de clientes "tunelados" entre a AP e o *controller*, a mobilidade permite o tráfego de tunelamento de clientes entre os *controllers*, isto é necessário se as interfaces de gerenciamento do *controller* acontecem de estar em uma sub-rede separada (*inter-controller de roaming*) uma da outra. Quando o cliente se associa á um AP, o WLC cria uma entrada de cliente em seu banco de dados. Essa entrada incluí a WLAN, contexto de segurança, qualidade de serviço (QoS), IP e MAC do cliente, o AP associado, e o túnel LWAPP onde o tráfego de clientes é originado e destinado (GRESS; JOHNSON, 2010).

3.6.1. Eventos de *Roaming*/Mobilidade de clientes

Como clientes sem fio se movem entre APs no mesmo WLC e APs se conectam aos diferentes WLC de dentro da rede, três tipos principais de eventos de *roaming* podem ocorrer, cada tipo gerando um comportamento diferente no ambiente *wireless*. As seções seguintes descrevem os diferentes tipos de *roaming* (GRESS; JOHNSON, 2010).

- ***Intra-Controller Roaming***

Se um cliente vaga entre APs de mesmo WLC, esta ação é chamada de evento de mobilidade *Intra-Controller* (Figura 18). *Intra-controller roaming* é o mais simples dos eventos, tudo o que o WLC precisa fazer é atualizar o banco de dados com o AP associado e estabelecer novos contextos de segurança se necessário. Basicamente, a mobilidade relacionada á camada 3 é tratada pelo AP. Como o cliente vaga, o *controller* atualiza o estado do cliente. O tráfego de cliente, em seguida, flui através do novo túnel LWAPP para o *controller* e para fora da rede.

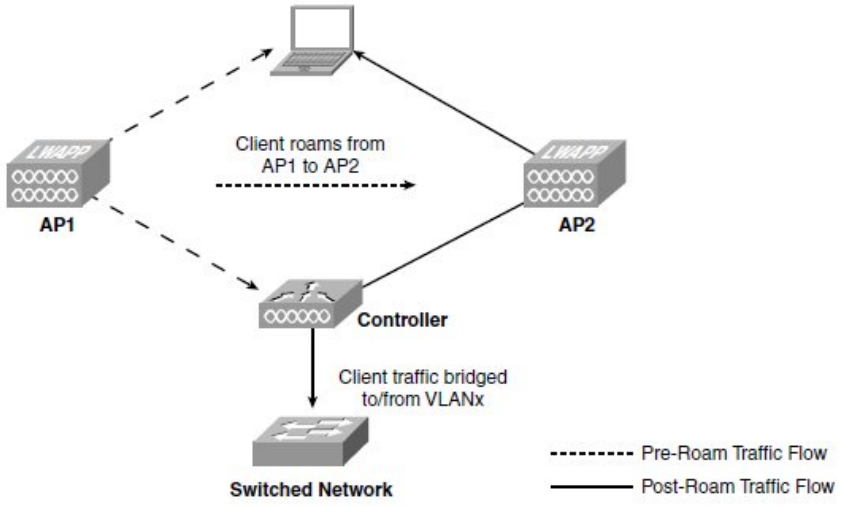


Figura 18 - Intra-Controller Roaming (GRESS; JOHNSON, 2010).

- ***Inter-Controller Roaming***

Inter-controller roaming ocorre quando um cliente anda entre dois APs registrados em dois *controllers* diferentes, onde cada *controller* tem uma interface na sub-rede do cliente (Figura 19). Quando um cliente vaga entre os *controllers* sobre a mesma sub-rede, os WLCs trocam mensagens de mobilidade, e a entrada do banco de dados do cliente é transferida do *controller* original para o novo *controller*. O tráfego de cliente, então, flui através do novo WLC na rede como o fez no WLC original.

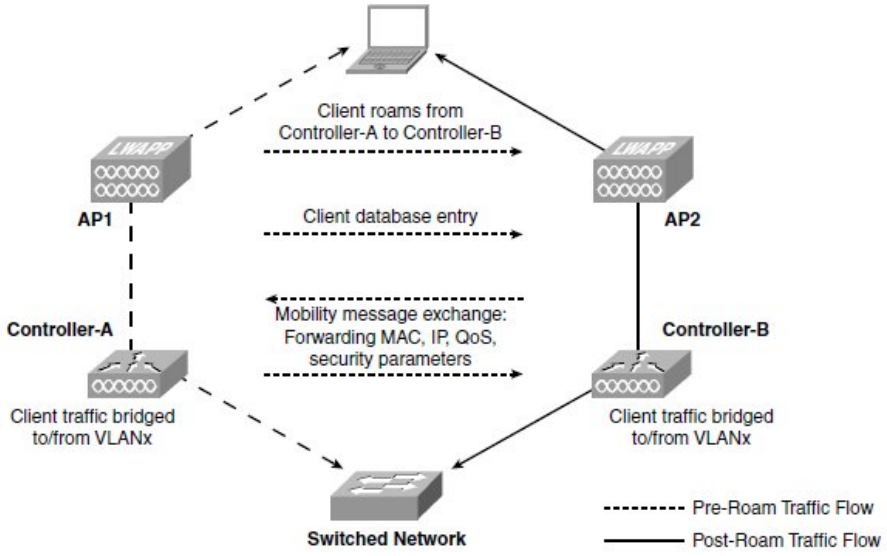


Figura 19 - Inter-Controller Roaming (GRESS; JOHNSON, 2010).

- ***Auto-Anchoring***

Auto-Anchoring é quando uma WLAN é "ancorada" para um *controller* em particular. Auto-ancoragem pode ser usada para balanceamento de carga (*load balancing*) e segurança. Você pode forçar os clientes a estar em um determinado WLC/sub-rede, independentemente do *controller* que estes acessem para se conectar á rede sem fio. O uso mais comum do *Auto-Anchor* é com a rede de convidados, possibilitando a conexão de visitantes e terceiros de maneira separada á de funcionários, evitando possíveis acessos indevidos.

3.7. Recursos de Segurança

As funcionalidades de segurança do modelo 802.11 combinada com a segurança física e facilidade de implementação da arquitetura LWAPP melhora a segurança geral das implementações WLAN. Além das vantagens de segurança inerentes oferecidas pelo protocolo LWAPP, a solução Cisco *Unified Wireless* também incluí as seguintes características adicionais de segurança (CISCO, 2012):

3.7.1. Opções simultâneas de segurança

A solução Cisco *Unified Wireless Network* suporta opções simultâneas de segurança WLAN. Por exemplo, múltiplas WLANs podem ser criadas em um WLC, cada uma com suas próprias definições de segurança WLAN que vão desde redes de hóspedes abertas até redes utilizando a plataforma WEP em combinação com configurações de segurança WPA e/ou WPA2 (CISCO, 2012).

3.7.2. *Access Control List* (ACL)

O WLC permite listas de controle de acesso (ACLs) a serem definidas para qualquer interface configurada no WLC, bem como ACLs para a CPU do próprio WLC. Essas ACLs podem ser usadas para aplicar políticas em determinadas WLANs para limitar o acesso a determinados endereços e protocolos, bem como para fornecer proteção adicional para o próprio WLC (CISCO, 2012).

3.7.3. Proteção através de DHCP e ARP

O WLC atua como um agente de retransmissão WLAN para pedidos DHCP dos clientes. Ao fazer isso, o WLC realiza uma série de verificações para proteger a infra-estrutura DHCP. A verificação principal é verificar se o endereço MAC incluído no pedido DHCP corresponde ao endereço MAC do cliente WLAN enviando a solicitação. Isso protege contra ataques de exaustão DHCP, porque um cliente WLAN pode solicitar apenas um endereço de IP para sua própria interface. O WLC por padrão, não encaminha mensagens *broadcast* de clientes WLAN de volta para a WLAN, o que impede um cliente WLAN de atuar como um servidor DHCP e falsificar informações DHCP incorretas.

O WLC também atua como um *proxy* ARP para clientes WLAN, mantendo as associações MAC-IP. Isso permite que o WLC bloqueie endereços IPs duplicados e ataques de *spoofing* ARP. O WLC não permite comunicação ARP direta entre clientes WLAN. Isso também impede ataques de *spoofing* ARP direcionadas a dispositivos clientes WLAN (CISCO, 2012).

3.7.4. Bloqueio *Peer-to-peer*

O WLC pode ser configurado para bloquear a comunicação entre os clientes na mesma WLAN. Isso evita que possíveis ataques entre os clientes na mesma sub-rede aconteçam, forçando a comunicação através do roteador (CISCO, 2012).

3.7.5. Sistema de detecção de intrusão sem fio (IDS)

O WLC realiza análise IDS na WLAN usando todos os APs conectados e reporta ataques detectados sobre o WLC, assim como para o WCS. A análise IDS *Wireless* é complementar a qualquer análise que pode de outra forma ser realizada por um sistema IDS na rede cabeada (CISCO, 2012).

3.7.6. Exclusão de clientes

Adicionalmente ao IDS *Wireless*, o WLC é capaz de tomar medidas adicionais para proteger a infra-estrutura WLAN e seus clientes. O *Controller* é capaz de programar políticas que excluem clientes WLAN cujo comportamento é considerado ameaçador ou inadequado (CISCO, 2012).

3.7.7. Rogue Management

Possibilitando estender o acesso á informações onde as redes cabeadas não podem chegar, as redes sem fio aumentam a disponibilidade da informação e consequentemente a produtividade dos usuários. No entanto, quando uma rede *wireless* não autorizada é detectada em um ambiente coporacional, uma camada adicional de preocupação em segurança é necessária (CISCO, 2010).

Assim, quando um funcionário traz e instala seu próprio ponto de acesso em uma rede *wireless* bem protegida e permite acesso de usuários não

autorizados a esta rede, toda a segurança previamente estabelecida no ambiente poderá ser comprometida.

A gerência de *rogue devices* (dispositivos não autorizados) permite que o administrador da rede monitore e elimine essa preocupação de segurança. A Cisco *Unified Wireless Network* fornece métodos para detecção de invasor que permite uma identificação completa do elemento e propõe uma solução de contenção, sem a necessidade de ferramentas complexas (CISCO, 2010).

Qualquer dispositivo que compartilhe o seu ambiente e não é administrado por você pode ser considerado um invasor. Um *Rogue Device* se torna perigoso nestes cenários:

- Quando configurado para usar o mesmo SSID que sua rede;
- Quando é detectado na rede com fio também;
- Configuração realizada por um estrangeiro/desconhecido, na maioria das vezes, com intenção maliciosa.

Há três fases principais de gerenciamento de rogue *devices* no UWN (ver Figura 20 para melhor visualização) :

- **Detecção** - Uma varredura através do *Radio Resource Management* (RRM) é usado para detectar a presença de dispositivos não autorizados;
- **Classificação** - Detectores de invasores e rastreadores de porta de *switch* são usados para identificar se o dispositivo não autorizado está conectado à rede cabeada. Regras de classificação também auxiliam na filtragem de *Rogue Devices* em categorias específicas com base em suas características. Além disso, o *Rogue Location Discovery Protocol* (RLDP) é utilizado para transmitir informações destes dispositivos de maneira rápida e coerente;

- **Mitigação** – *Shut* de portas de *Switch*, localização e contenção de *rogue devices* são usados para rastrear sua localização física e anular/diminuir a ameaça de o dispositivo invasor causar danos.

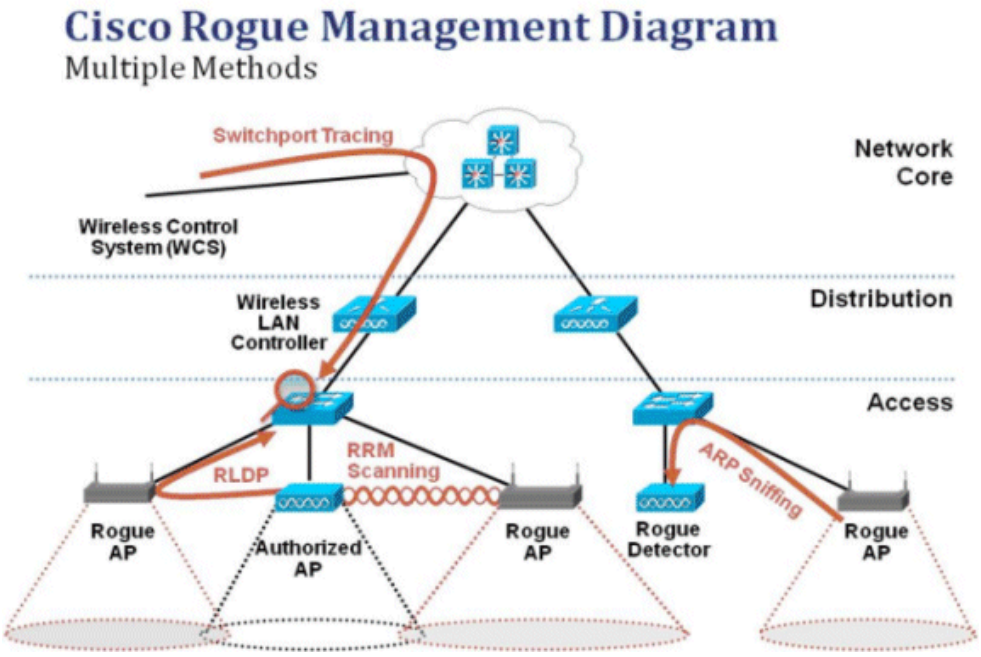


Figura 20 - Diagrama de Métodos de Rogue Management (CISCO, 2010).

Se as ondas de freqüência de um dispositivo *rogue* são ouvidos, a informação é então comunicada através de LWAPP à LAN *Wireless Controller* (WLC) para processamento. De forma a evitar falsos positivos, um certo número de métodos são usados para garantir que outros APs baseados em Cisco não são identificados como um dispositivo não autorizado. Estes métodos incluem atualizações de *mobility groups*, pacotes vizinhos de RF e controle de APs autônomos via *Wireless Control System* (CISCO, 2010).

Enquanto o banco de dados do *controller* contém apenas o conjunto atual de *rogue devices*, o WCS também incluí um histórico de eventos e *logs* de dispositivos *rogues* que não são mais vistos (CISCO, 2010).

Um AP LWAPP alcança até 50 metros fora de seu canal, a fim de ouvir clientes invasores, monitorando o ruído e interferência nos canais. Qualquer

cliente ou AP invasor detectado é enviado para o *controller*, que reúne as seguintes informações:

- O endereço MAC do AP invasor;
- Nome do AP detectado;
- O endereço MAC dos clientes conectados;
- Se os quadros são protegidos com WPA ou WEP;
- A relação sinal-ruído (SNR = *Signal-to-Noise Ratio*);
- O indicador de força de sinal recebido (RSSI = *Receiver Signal Strength Indicator*);
- Canal de detecção de *Rogue;*
- *Rogue* SSID (se o SSID rogue é transmitido);
- Endereço IP do equipamento invasor;
- Primeira e última vez que o invasor é reportado;
- Largura de banda do Canal.

Por padrão, todos os invasores que são detectados pela Cisco UWN (*Unified Wireless Network*) são considerados não classificados. Como mostrado neste gráfico, *rogue devices* podem ser classificados em uma série de critérios, incluindo RSSI, SSID, tipo de segurança e o número de clientes (Figura 21):

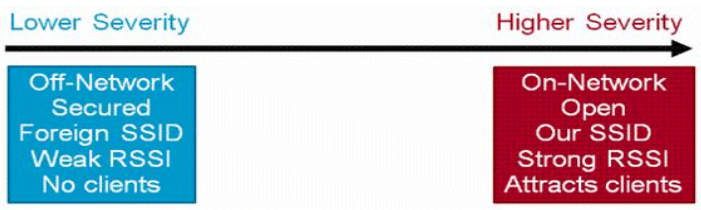


Figura 21 - Nível de Severidade e Critérios de classificação de Rogue Devices (CISCO, 2010).

3.8. Aplicabilidades

A *Unified Wireless Network* pode ser implantada em uma grande variedade de ambientes e situações. BASF (Químicos e sintéticos), Mars Incorporated (produtos alimentícios), Procter & Gamble (bens de consumo) figuram entre as grandes empresas que já adotaram a solução desenvolvida pela Cisco . Alguns dos cenários primários de uso incluem:

3.8.1. Visibilidade e controle de dispositivos móveis

Despesas operacionais e de capital podem ser reduzidas, evitando a perda ou o roubo de valiosos bens móveis, como cadeiras de rodas e bombas de infusão em um ambiente hospitalar e retro projetores, computadores portáteis e aparelhos de voz em uma empresa. Indivíduos e ativos podem ser rapidamente localizadas em qualquer lugar dentro de um ambiente *wireless* (CISCO, 2010).

3.8.2. Automação de fluxo de trabalho e controle de pessoas

Uso de inventário e processos de despacho são otimizados. Em um ambiente de varejo, o layout de loja e gestão de fila podem ser otimizados com base no acompanhamento de "padrões" de clientes comerciais; em parques de diversões, as crianças podem ser controladas, permitindo que os pais saibam onde eles estão em todos os momentos; seguranças também podem ser rastreados em qualquer recinto. Nas unidades de saúde onde os médicos são severamente poucos, os hospitais podem acompanhar os médicos durante o funcionamento normal de suas operações ou em situações de emergência, onde o atendente/médico de plantão mais próximo é mais necessário. Outros recintos de saúde com instalações para necessidades especiais podem precisar acompanhar crianças ou os doentes idosos, tais como aqueles que sofrem de Alzheimer, que podem acidentalmente vaguear fora das instalações.

3.8.3. Telemetria

Wi-Fi tags com interfaces seriais podem ser conectados a um equipamento para transmitir informações importantes sobre o dispositivo diretamente para aplicações de negócios. Por exemplo, as empresas de aluguel de automóveis

muitas vezes querem informações de telemetria relacionadas com quilometragem e nível de combustível de carros devolvidos, enquanto que os clientes querem informações sobre o local que irá ajudá-los a encontrar veículos mais fáceis. Farmácias, fábricas e varejistas querem informações sobre os números de lote, data de validade, e informações sobre os componentes fora de especificação. Além disso, na área da saúde, saber a localização de uma bomba de infusão é valioso, mas saber se está ou não em uso (ligado ou desligado) é ainda mais valioso (CISCO, 2010).

3.8.4. Segurança WLAN e controle de rede

A equipe de TI pode localizar rapidamente as ameaças de segurança, tais como pontos de acesso não autorizados e dispositivos clientes mal intencionados. Os gerentes de TI também podem usar a aplicação para estabelecer um quadro para a segurança baseada em localização, em que a segurança física num edifício é utilizada para controlar o acesso à Internet sem fio - reforçando a segurança na WLAN (CISCO, 2010).

3.8.5. Gerência de Capacidade e Visibilidade de RF

Integrando o controle de localização na WLAN permite que a equipe de TI faça mais do que simplesmente rastrear usuários. Com esta solução eles conseguem gerar relatórios de padrões baseados em localização e investigar á fundo o comportamento de uso da rede para que consiga acomodar mudanças nos padrões de tráfego, ajudando a habilitar uma melhor gerência da capacidade de RF (CISCO, 2010).

3.8.6. Cisco Connected Stadium Wi-Fi

A demanda de acesso á rede através do meio *Wireless* tem como grande aliada a redução de custos e a sua comodidade para o usuário. A possibilidade de se movimentar e utilizar a internet ao mesmo tempo é um beneficio no panorama corporacional hoje em dia. Porém, estes benefícios vem se estendendo além das empresas e indústrias, sendo atualmente necessários em grande eventos sociais e culturais. Um dos ambientes mais utilizados pelos brasileiros é o estádio. Nele, grandes concertos são realizados e diferentes atividades esportivas são

exercidas. Público ou privado, o estádio é um símbolo de eventos sociais e culturais no Brasil. E essa cultura nos próximos anos terá sua força dobrada com a chegada de grandes eventos mundiais no país, como a Copa do Mundo FIFA 2014 e os Jogos Olímpicos 2016 no Rio de Janeiro (ver logotipos dos eventos na Figura 22).

Figura 22 - Eventos Mundiais sediados pelo Brasil que necessitam de infra-estrutura tecnológica especial (AUTORIA PRÓPRIA).

Para suprir a necessidade tanto dos espectadores quanto das empresas relacionadas, é necessária a presença de uma infra-estrutura tecnológica de topo. Assim sendo, a Cisco Systems elaborou uma solução *wireless* especifica para os estádios a fim de atender com qualidade qualquer usuário do ambiente. Desenvolvida a partir da arquitetura da *Unified Wireless Network*, a Cisco implantou o *Connected Stadium Wi-Fi* em alguns dos maiores estádios do mundo, desenvolvendo uma compreensão profunda de como superar os desafios da criação de redes *wireless* nesses ambientes. A solução cria um ambiente *wireless* de grande disponibilidade e mobilidade, além de contribuir (CISCO, 2011):

- Oferecendo suporte nas diferentes redes Wi-Fi utilizadas, atendendo os requisitos de acesso e segurança específicos para cada uma, como pontos de vendas, emissão de bilhetes, sistemas de gerenciamento, convidados e prestadores de serviços;

- Melhorando a capacidade dos dispositivos clientes e suprindo os requisitos estéticos de cada estádio em particular;

- Diminui a interferência de radiofreqüência e oferece recursos de gerenciamento para milhares de dispositivos e usuários com o WCS.

Um dos benefícios para os provedores de serviços é a rede de terceira ou quarta geração (3G/4G) que não é mais sobrecarregada com aplicativos de dados por largura de banda; as chamadas de voz e mensagens de texto funcionam novamente, eliminando as reclamações de clientes recebidas com freqüência pelos provedores de serviço em relação ao uso de celulares nesse tipo de ambiente exigente.

3.8.7. BYOD

BYOD (*Bring Your Own Device*) é uma das maiores tendências nos últimos tempos na área de mobilidade. Milhões de pessoas estão adquirindo dispositivos móveis de alta capacidade, como *smartphones* e *notebooks*, para ajudar a gerenciar seu cotidiano. Cada vez mais as pessoas estão levando esses dispositivos para o trabalho e os integrando no fluxo de trabalho diário, e é nisso que consiste o BYOD. A *Unified Wireless Network* conseguiu acompanhar essa nova moda, oferecendo uma maneira fácil e segura de monitorar os dispositivos pessoais no local de trabalho através de seus recursos e equipamentos, como o WLC e o WLA.

4. ESTUDO DE CASO

O estudo de caso deste trabalho visa o desenvolvimento de uma solução para uma situação-problema baseada em um caso real em um ambiente corporativo, utilizando os recursos e ferramentas da UWN completa (incluindo WLA) para o *troubleshooting* do incidente, com foco na Segurança da Informação. A situação problema proposta aborda alguns pontos importantes da Segurança da Informação, como a Disponibilidade, Confiabilidade e Integridade da Informação; a segurança da informação em camadas (Física, Lógica e Humana) e a importância de uma política de segurança da informação (PSI) e seu cumprimento. A seguir será apresentada a situação-problema e a respectiva solução através dos recursos da *Unified Wireless Network*, com foco na Segurança da Informação.

4.1. Situação-Problema

Numa empresa de médio-porte, possuindo políticas de Segurança da Informação e com infra-estrutura WLAN suportada pela UWN e gerenciada por uma administração de redes terceirizada, um dos usuários reporta um incidente de instabilidade da sua conexão *wireless*. Este mesmo problema esta afetando apenas o usuário e mais quatro funcionários que dividem a mesma área do escritório, enquanto que o resto das áreas não há reclamação de degradação de serviço. Após ser providenciado o IP e o MAC de dois usuários afetados para o administrador da rede da empresa terceirizada (atuando remotamente) em um breve momento de conectividade, o administrador consegue identificar pelo WLC (através de uma sessão HTTPS) o AP que suporta a área afetada (Figura 23).

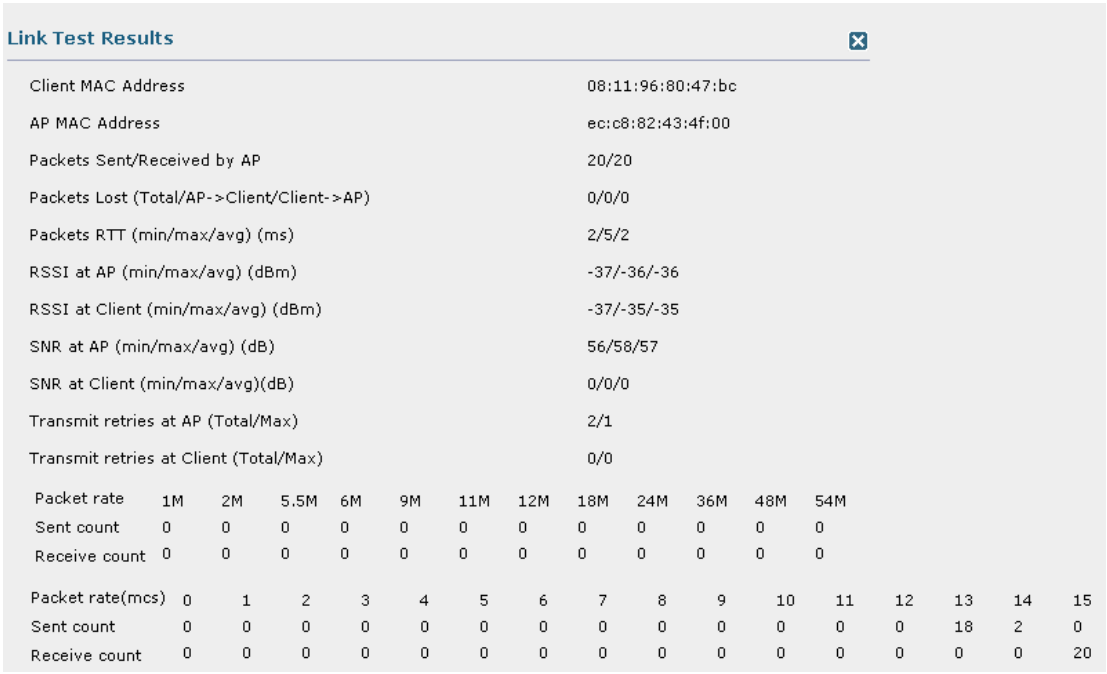
Clients

Current Filter MAC Address: 08:11:96:80:47:bc [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
08:11:96:80:47:bc	ap-01	Protected	Protected	802.11bn	Associated	Yes	13	No

Figura 23 - Identificação do cliente através do WLC (AUTORIA PRÓPRIA).

Assim, o administrador através da conexão HTTPS com o WLC da empresa, busca recolher detalhes e proceder com o *troubleshooting*. Através de um recurso de teste (ver Figura 24), o administrador testa e constata que a conexão entre o AP e o cliente afetado está sem problemas lógicos. Com uma investigação física através do cliente, também foi possível identificar que os LEDs e o cabeamento LAN do AP estavam operacionais.



Link Test Results

Client MAC Address	08:11:96:80:47:bc
AP MAC Address	ec:c8:82:43:4f:00
Packets Sent/Received by AP	20/20
Packets Lost (Total/AP->Client/Client->AP)	0/0/0
Packets RTT (min/max/avg) (ms)	2/5/2
RSSI at AP (min/max/avg) (dBm)	-37/-36/-36
RSSI at Client (min/max/avg) (dBm)	-37/-35/-35
SNR at AP (min/max/avg) (dB)	56/58/57
SNR at Client (min/max/avg)(dB)	0/0/0
Transmit retries at AP (Total/Max)	2/1
Transmit retries at Client (Total/Max)	0/0

Packet rate	1M	2M	5.5M	6M	9M	11M	12M	18M	24M	36M	48M	54M
Sent count	0	0	0	0	0	0	0	0	0	0	0	0
Receive count	0	0	0	0	0	0	0	0	0	0	0	0

Packet rate(mcs)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sent count	0	0	0	0	0	0	0	0	0	0	0	0	0	18	2	0
Receive count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20

Figura 24 - Teste entre o cliente e o AP através do WLC (AUTORIA PRÓPRIA).

Problemas com o servidor DHCP são descartados, pois caso o *range* (alcance) de IP dispostos pela rede fosse insuficiente para a quantidade de usuários, mais áreas da empresa estariam afetadas.

Como mencionado anteriormente, uma das grandes vantagens do UWN é a escalabilidade. Sem encontrar problemas entre o WLC, o AP e o cliente, o próximo passo do administrador seria a criação de uma conexão com o WCS para a análise de detalhes e eventos da rede, além da possibilidade de verificar problemas de cobertura do AP para os usuários, analisando os mapas gerados pelo WLA.

Porém, antes de passar para o próximo nível de escalabilidade, o administrador identificou um AP que não faz parte da infra-estrutura da empresa (Figura 25), ou seja, um *Rogue* AP. Através de um recurso presente no WLC, foi possível identificar este dispositivo, além de detalhar que o AP onde os clientes estavam conectados detectou este *Rogue* AP dentro de sua cobertura *wireless*.

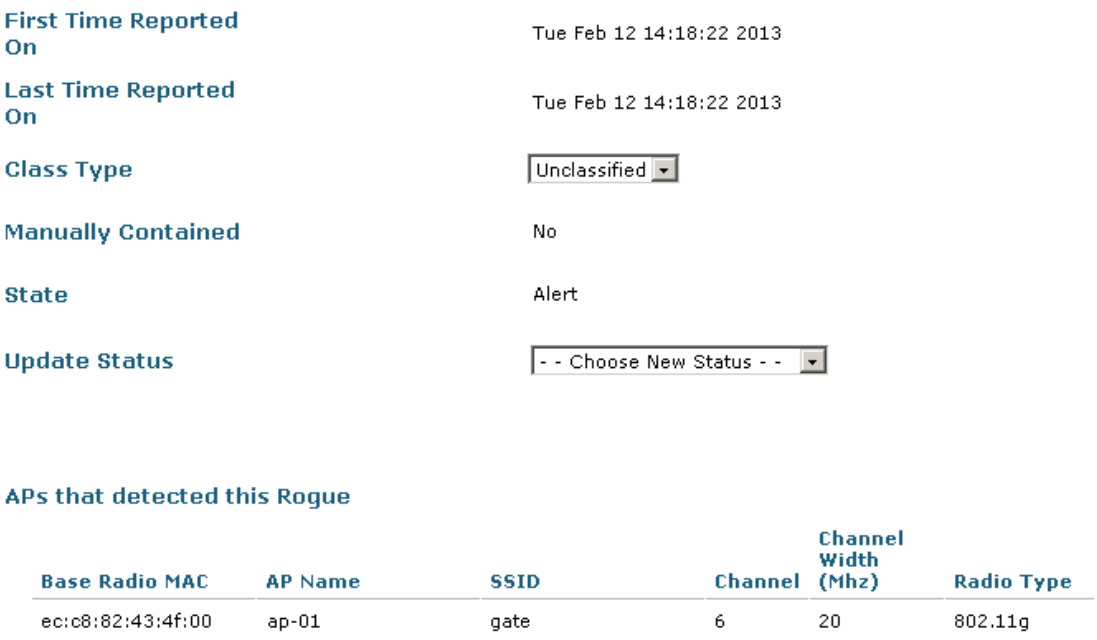


Figura 25 - Rogue AP detectado pelo AP autorizado através do WLC (AUTORIA PRÓPRIA).

Como dito em capítulos anteriores (3.7.7.*Rogue Management*), a presença de um dispositivo não autorizado na infra-estrutura de uma rede *wireless* pode gerar graves problemas de segurança, sendo sua implementação para propósitos maléficos ou apenas falha humana. Estes dispositivos podem estar sem medidas e protocolos de segurança, além de poder influenciar a estabilidade de conexão de outros aparelhos se presente próximo dos APs autorizados e no mesmo canal. Este tipo de interferência é chamada de co-canal. Este é um conceito fundamental para entender quando se trata de compreender o comportamento e o desempenho de WLANs 802,11. É um fenômeno em que as transmissões a partir de um dispositivo 802.11 atravessam a faixa de atuação de outros dispositivos

802,11 de mesmo canal, provocando interferências e redução do desempenho disponível.

Após seguir as instruções do administrador (com informações sobre o *switch* e a porta onde o dispositivo não autorizado estava conectado), o usuário identificou que o *Rogue* AP estava instalado próximo do AP pertencente a infra-estrutura da empresa.

Após retirá-lo da rede e monitorar a conexão dos usuários em algumas horas, foi possível confirmar que o AP não autorizado estava influenciando na conectividade do AP autorizado e consequentemente no acesso de usuários. Com a data de reporte da primeira incidência do *Rogue* AP na rede conjuntamente com a informação onde o AP não autorizado estava conectado, foi possível passar um reporte para a equipe de segurança da empresa, de forma a tentar identificar o funcionário que conectou o dispositivo na rede através de câmeras de segurança. A partir da identificação do usuário, será necessário aplicar as penalidades de acordo com a Política de Segurança vigente e a alta administração da empresa, já que a implantação de dispositivos não autorizados sem prévia comunicação com o departamento de TI ou gerência é uma quebra de procedimento da Segurança da Informação.

5. CONCLUSÃO

Com este trabalho, pode-se concluir que o desenvolvimento e implantação de um sistema centralizado de monitoração e gerenciamento de uma rede *wireless* é essencial para manter o nível de qualidade do serviço dos usuários e clientes, além de assegurar um maior poder de segurança na WLAN corporativa, um recurso que é e será cada vez mais utilizado para o auxilio de funções, sejam estratégicas, táticas ou operacionais. Com o aumento da funcionalidade do *wireless* numa empresa, o acréscimo da visibilidade e atenção deste recurso não se volta apenas para os funcionários de TI, mas também para possíveis atacantes em busca do lucro em cima de suas violações nas redes empresariais, tornando a necessidade de uma solução bem construída em volta de seus ativos de segurança algo essencial, e é exatamente isso que a Cisco *Unified Wireless Network*, solução abordada, aplica na sua operabilidade.

Ao longo do trabalho pode-se ver que a UWN se integra á rede do usuário/cliente de maneira a manter sempre a Confidencialidade, Integridade e Disponibilidade, seja por meio de opções de *Access List* (ACL), *Rogue Management* e IDS (*Intrusion Detection System*), ou por suas características de escalabilidade entre equipamentos, possibilidade de redundância, planejamento e monitoração de cobertura do sinal *wireless* através de plantas, e configuração de dezenas de dispositivos de maneira centralizada e fácil.

Ademais, a possibilidade de integração entre a solução e políticas de segurança e de BYOD é um fator animador para o desenvolvimento do gerenciamento da rede *wireless* e o ajustamento á normas de Governança de TI. Atender a características de uma política de BYOD também demonstra que a solução se mantém atualizada á tendências, sempre estando um passo adiante de redes sem fio com plataformas de administração ausentes.

Através do estudo de caso e sua situação-problema, constatou-se como um administrador de rede pode lidar com problemas na rede sem fio do usuário, utilizando técnicas de *troubleshooting* disponibilizadas pelos equipamentos e aplicativos da Cisco, comprovando o objetivo deste trabalho em mostrar as vantagens de um sistema de administração wireless como a UWN, e como *a*

Unified Wireless Network se ajusta também no suporte á falhas humanas (implantação de dispositivos não permitidos) e físicas (conexão de ativos *wireless* não permitidos na rede cabeada) com a área de segurança da empresa (verificação humana através de monitoração por câmeras).

Como mencionado nos capítulos, variadas são suas aplicabilidades e benefícios, fazendo com que grandes empresas adotem esta solução. Porém, uma de suas desvantagens é o custo dos equipamentos utilizados, fazendo com que a solução se limite em atender, na maioria dos casos, a empresas de médio-grande porte devido ao caro valor dos ativos e manutenção. Outro fator que pode ser considerado negativo é a falta de total integração com outras marcas, fazendo com que a solução seja completamente proprietária pela Cisco. Contudo, a utilização de apenas dispositivos Cisco em uma solução pode fornecer um melhor poder de comunicação e configuração entre equipamentos, além do maior suporte dado pela empresa.

O que antes era um trabalho longo, realizando a implementação e configuração de cada *Access Point* em uma empresa, se tornou algo fácil com a UWN e o surgimento do *Wireless LAN Controller*. A solução também possibilitou criar uma rede onde o usuário pode se deslocar ao longo de todo o local suportado sem perder sua conexão, isso devido as novas propriedades de *roaming* que os WLCs disponibilizam, além de possuir recursos específicos para a criação *de guest networks*, ou redes de visitantes.

A Cisco *Unified Wireless Network* representou um grande passo para o gerenciamento de uma WLAN corporacional, um assunto que cada vez mais será desenvolvido e comentado. A adoção de empresas por redes *wireless* já é uma constatação atual em suas infra-estruturas. O próximo passo será a adesão de plataformas de gerenciamento para este ambiente sem fio de forma a manter a qualidade e a segurança do serviço, algo que a UWN já esta um passo a frente e que servirá como base para futuras soluções *wireless*.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ACKER, S. **Enterprise WLAN Architecture**. 2012.

ACKER, S. **Troubleshooting WLANs with Centralized Controllers**. 2009.

ALVES, N.; SILVA, S. L. P.. **Introdução as Redes Wireless**. CBPF, 2003.

AMARAL, B. M.; MAESTRELLI, M.. **Segurança em Redes Wireless 802.11**. CBPF, 2004.

BARCELOS, J. P. M.; GONÇALVES, R. G.; ALVES; N.. **O Padrão 802.11**. CBPF, 2003.

CARPENTER, T.; BARRETT, J.. **CWNA Certified Wireless Network Administrator: Official Study Guide**. 4ª ed. McGraw-Hill, 2008.

CISCO IBSG HORIZONS. **BYOD: uma perspectiva global**. 2012.

CISCO SYSTEMS. **Cisco Wireless Location Appliance**. 2006.

CISCO SYSTEMS. **Enterprise Mobility 4.1 Design Guide**. 2012.

CISCO SYSTEMS. **Migrate to the Cisco Unified Wireless Network**. 2007.

CISCO SYSTEMS. **Rogue Management in a Unified Wireless Network**. 2010.

CISCO SYSTEMS. **Solução Cisco Connected Stadium Wi-Fi**. 2011.

CISCO SYSTEMS. **Wireless and Network Security Integration Design Guide**. 2008.

CISCO SYSTEMS. **Q&A: CISCO WIRELESS LAN CONTROLLER**. 2005.

CISCO SYSTEMS. **Wireless LAN Controller (WLC) FAQ**. 2009.

GEIER, J. **Special Report: The State of Wireless LANs**. Network World, 2004.

GRESS, M. L.; JOHNSON, L.. **Deploying and Troubleshooting Cisco Wireless LAN Controllers**. CiscoPress, 2010.

IEEE. **Std 802.11™-2012** (Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications). Março 2012.

ODORIZZI, J. **Estudo de caso da Solução Unified Wireless Cisco**. Curitiba: Pontifícia Universidade Católica do Paraná, 2010.

SILVA, M. W. R. **Alocação de canal em redes sem fio IEEE 802.11 independentes**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2006.

VAZZI, M. R. G. **Tópicos em REDES de COMPUTADORES**. Centro Paula Souza: Monte Alto, 2012.