UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMI PRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

BRUNO SILVA DE OLIVEIRA

GERENCIAMENTO DE REDES SEM FIO: UM CLIENTE SNMP PARA O OPENWRT

MONOGRAFIA

CURITIBA

2017

BRUNO SILVA DE OLIVEIRA

GERENCIAMENTO DE REDES SEM FIO: UM CLIENTE SNMP PARA O OPENWRT

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Christian Carlos Souza Mendes

CURITIBA

2017

TERMO DE APROVAÇÃO

Bruno Silva de Oliveira

GERENCIAMENTO DE REDES SEM FIO: UM CLIENTE SNMP PARA O OPENWRT

Esta Monografia foi apresentada em 01 de junho de 2017 como requisito parcial para a obtenção do título de Especialista em Gerenciamento de Servidores e Equipamentos de Rede. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Augusto Foronda
Prof. Coordenador do Curso

Christian Carlos de Souza Mendes
Prof. Orientador

Kleber Kendy Horikawa Nabas
Membro da Banca

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

Oliveira, B. S.. GERENCIAMENTO DE REDES SEM FIO: UM CLIENTE SNMP PARA O OPENWRT. 46 f. Monografia – Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Com a crescente utilização de redes sem fio, seu monitoramento e gerenciamento é indispensável para a manutenção da qualidade do serviço. O SNMP é um protocolo muito utilizado para este fim mas, sob o ponto de vista de uma rede sem fio, restringe-se aos equipamentos e serviços que constituem a infraestrutura da rede. O sistema operacional OpenWrt, por sua grande flexibilidade, pode ser utilizado nos pontos de acesso para a obtenção de informações customizadas sobre a rede e seus clientes e disponibilizá-los através do SNMP. Este trabalho propôs a criação de um software baseado no OpenWrt e no SNMP para coleta destas informações customizadas e sua validação foi realizada pela implantação de um servidor de monitoramento que permitiu acesso simplificado aos dados monitorados e visualização elaborada dos dados, possibilitando um melhor gerenciamento da rede como um todo.

Palavras-chave: SNMP, OpenWrt, 802.11, Wireless, Gerenciamento, Monitoramento.

ABSTRACT

Oliveira, B. S.. WIRELESS MANAGEMENT: A SNMP CLIENT FOR OPENWRT. 46 f. Monografia – Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

As the popularity of wireless networks grows, it's monitoring and management become essential to maintain quality of the provided wireless Internet service. The SNMP is the de facto standard used in order to achieve this goal but, from the wireless network perspective, it's use is limited to the network's infrastructure components and services. The OpenWrt, a flexible operating system, can be used on access points to collect arbitrary data regarding the network and it's clients and provide it through SNMP. In this context, this work sought to write a software, based on OpenWrt and SNMP, to gather customized data and to deploy a monitoring service that allowed simplified access and elaborated view of data which led to a better network management.

Keywords: SNMP, OpenWrt, 802.11, Wireless, Management, Monitoring.

LISTA DE FIGURAS

LISTA DE SIGLAS

IEEE	*Institute of Electrical and Electronic Engineers*
SNMP	*Simple Network Management Protocol*
AP	*Access Point*
OSI	*Open System Interconnection*
ISO	*International Organization for Standardization*
IETF	*Internet Engineering Task Force*
CMIP	*Common Management Information Protocol*
TMN	*Telecommunication Management Network*
ITU	*International Telecommunication Union*
SGMP	*Simple Gateway Monitoring Protocol*
NMS	*Network Management System*
MIB	*Management Information Base*
IETF	*Internet Engineering Task Force*
SMI	*Structure of Management Information*
ASN.1	*Abstract Syntax Notation 1*
OID	*Object Identifier*
UDP	*User Datagram Protocol*
MAC	*Media Access Control*
PDU	*Protocol Data Unit*
RFCs	*Requests for Comments*
USM	*User Security Model*
SHA1	*Secure Hash Algorithm 1*
DES	*Data Encryption Standard*
VACM	*View-Based Access Control Model*
LAN	*Local Area Networks*
MIMO	*Multiple Input, Multiple Output*
MU-MIMO	*Multiuser, Multiple Input, Multiple Output*
ESS	*Extended Service Set*
SSID	*Service Set Identifier*
DoS	*Denial of Service*
WEP	*Wired Equivalent Privacy*
WPA	*Wi-Fi Protected Access*
TKIP	*Temporary Key Integrity Protocol*
AES	*Advanced Encryption System*
EAP	*Extensible Authentication Protocol*
PSK	*Pre Shared Key*
RADIUS	*Remote Authentication Dial In User Service*
DNS	*Domain Name System*
TTL	*Time to live*
RTS	*Request-To-Send*
CTS	*Clear-To-Send*

ACL	*Access Control Lists*
DHCP	*Dynamic Host Configuration Protocol*
SO	Sistema Operacional
UCI	*Unified Configuration Interface*
BSSID	*Basic Service Set Identifier*
FCS	*Frame Check Sequence*
WMM	*Wi-Fi Multimedia*
WME	*Wireless Multimedia Extensions*
MFP	*Management Frame Protection*
TDLS	*Tunneled Direct Link Setup*
LLD	*Low-level discovery*
JSON	*JavaScript Object Notation*

SUMÁRIO

1 INTRODUÇÃO

Com a onipresença das redes sem fio baseadas no padrão IEEE 802.11, o gerenciamento e monitoramento dos elementos destas redes, bem como dos clientes conectados a elas, torna-se muito importante. Muitas empresas e entidades oferecem o serviço de internet sem fio a seus clientes ou usuários e o monitoramento e gerenciamento destas redes é essencial.

O *Simple Network Management Protocol* (SNMP) é o principal protocolo utilizado para monitoramento e gerenciamento de elementos de rede. No ponto de vista de uma rede sem fio, este protocolo é normalmente utilizado na porção controlada da rede: em seus ativos de rede, pontos de acesso (*Access Point* ou AP), servidores e afins. Uma vez que os clientes da rede sem fio podem ser dos mais diversos tipos, torna-se inviável contar com a obtenção de dados sobre eles através do SNMP.

O OpenWrt é um sistema operacional baseado no Linux indicado para utilização em dispositivos com recursos limitados e aplicações específicas, tais como pontos de acesso e pequenos roteadores, altamente configurável e customizável. Sua flexibilidade pode ser utilizada para obter informações extras sobre as redes 802.11 tanto do ponto de vista dos pontos de acesso quanto, de forma não invasiva, dos clientes conectados a ela.

1.1 JUSTIFICATIVA

A obtenção de informações sobre redes 802.11, principalmente sobre os clientes conectados a ela, comumente se dá através de técnicas de *sniffing* da rede (JOHNSON, 2009). Isto precisa ser feito ativamente e, pela natureza decentralizada dos pontos de acesso, dificulta o monitoramento e gerenciamento de redes sem fio. Além disso, no OpenWrt a porção referente às redes 802.11 possui apenas uma implementação parcial, como apresentado neste trabalho e em (MORREALE; TERPLAN, 2009).

Diante deste contexto, este trabalho visa disponibilizar informações pertinentes aos clientes conectados à rede e aos pontos de acesso OpenWrt de forma a complementar as in-

formações relativas ao monitoramento e gerenciamento. Pretende-se também demonstrar que a implementação pode ser visualizada e acessada de forma simples e centralizada através de um serviço de monitoramento.

1.2 OBJETIVOS GERAIS E ESPECÍFICOS

Os objetivos gerais deste trabalho foram ampliar a capacidade de gerenciamento de redes sem fio num ambiente composto por pontos de acesso baseados em OpenWrt utilizando o SNMP.

Especificamente, os objetivos deste trabalho foram, inicialmente, desenvolver um *software* para os pontos de acesso baseados em OpenWrt para a disponibilização de informações customizadas sobre a rede sem fio e seus clientes através do SNMP. Alterando minimamente os APs e de forma transparente aos clientes. Além da implementação do *software*, sua validação foi realizada pela implantação de um servidor de monitoramento que permitisse acesso simplificado aos dados monitorados, visualização elaborada dos dados que permite melhor gerenciamento da rede como um todo.

Para atingir os objetivos propostos, este texto estrutura-se como a seguir. O capítulo 2 detalha o protocolo SNMP, seu relacionamento com o gerenciamento de dispositivos e, mais especificamente, em dispositivos OpenWrt. O capítulo 3 descreve o tipo e a metodologia de pesquisa utilizada neste trabalho. O capítulo 4 descreve como o cliente SNMP foi criado no OpenWrt bem como a instalação de um serviço de monitoramento para o cliente. Por fim, o capítulo 5 faz uma análise de resultados obtidos e apresenta as considerações finais.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os conceitos básicos sobre gerenciamento de redes de computadores, o Protocolo de Gerenciamento Simples de Redes, o *Simple Network Management Protocol* (SNMP). Neste contexto são descritas características das redes sem fio 802.11 e suas peculiaridades quanto ao gerenciamento de dispositivos de rede, mais especificamente, dispositivos compatíveis com o OpenWrt.

2.1 GERENCIAMENTO DE REDES DE COMPUTADORES

O gerenciamento de uma rede é uma tarefa onde várias sistemas, técnicas e dispositivos são utilizados por um administrador no monitoramento e manutenção de redes (MAURO; SCHMIDT, 2005). Pode variar em escala, profundidade e complexidade de acordo com a infraestrutura da rede e recursos destinados a ela mas é extremamente importante em qualquer cenário.

Uma implantação mal preparada e um crescimento desordenado pode causar graves transtornos. Por isso, a primeira etapa em um processo contínuo de gerenciamento é o projeto da rede, incluindo um planejamento operacional e de crescimento da rede. A seguir, na etapa operacional, o gerenciamento em si é essencial para assegurar a entrada em funcionamento da rede e mantê-la em operação (PRAS, 1995). Ainda segundo este autor, um bom planejamento irá atender os requisitos do maior número de usuários potenciais e permitirá alterações na estrutura e o crescimento da rede sem problemas de gerência. Ao iniciar o gerenciamento de uma rede, para cada serviço ou dispositivo, é importante decidir qual o seu nível de atividade:

Inativo: sem nenhum monitoramento;

Reativo: sem monitoramento, apenas reagindo aos problemas quando surgem;

Interativo: monitoramento ativo com atuação para descobrir a origem do problema e tratar possíveis efeitos colaterais;

Proativo: monitoramento ativo e o sistema fornece a origem do problema e realiza processos predefinidos de restauração da rede automaticamente.

Na segunda fase, operacional, a definição de funcões de gerenciamento que permitam monitorar o que acontece na rede, definir alarmes e alterar informações nos sistemas remotos auxiliarão no tratamento de erros, reduzindo seu efeito, a monitorar o comportamento da rede, permitindo a criação de perfís (*baselines*) a fim de conhecer o comportamento normal da rede e poder definir limites aceitáveis de performance.

As principais entidades de padronização criaram modelos de gerenciamento de redes que definem uma arquitetura de gerenciamento de todos os nós que se comunicam na rede (MARTIN et al., 2013). Os modelos mais importantes são o modelo de Gerenciamento OSI (*Open System Interconnection*), desenvolvido pela Organização Internacional para Padronização (*International Organization for Standardization* - ISO)[1]. E o Modelo da Internet, desenvolvido pela Força Tarefa de Engenharia na Internet (*Internet Engineering Task Force* - IETF).

O modelo OSI é fortemente acoplado ao modelo de referência OSI de arquitetura de rede e utiliza o protocolo *Common Management Information Protocol* (CMIP)[2] para gerenciar os nós da rede (PRAS, 1995). Ele divide o gerenciamento em 5 "áreas funcionais" didaticamente muito utilizadas no entendimento do gerenciamento de redes e sob as quais deve-se basear qualquer processo de gerenciamento. São elas (MAURO; SCHMIDT, 2005; CISCO, 2004):

Gerência de falhas: detecta, registra, notifica, isola e corrige falhas no funcionamento dos recursos de rede;

Gerência de configuração: responsável pelo monitoramento dos parâmetros de configuração dos serviços da rede e implementação de funções para alteração dos recursos de rede, tais como versões de sistema operacional ou número de interfaces de rede;

Gerência de contabilização: mede a utilização dos recursos de rede para determinar os padrões de uso e regular quotas para otimizar o acesso aos usuários;

Gerência de desempenho: responsável pela medição e disponibilização das informações de desempenho da rede ou serviços de rede. Estes dados são usados para para análise de tendência e garantir que a rede opere como esperado;

[1] Muito similar, e até mesmo desenvolvido em conjunto, com o modelo *Telecommunication Management Network* (TMN), criado pela *International Telecommunication Union* (ITU) (PRAS, 1995)

[2] Protocolo concorrente do SNMP também fortemente acoplado ao modelo OSI.

Gerência de segurança: limita o acesso à rede ou recursos da rede e ajuda a detectar e prevenir seu uso indevido.

O modelo da Internet, entretanto, tornou-se o modelo de gerenciamento mais difundido basicamente por sua simplicidade e robustez. Ele opera no modelo de referência TCP/IP e é descrito pelo protocolo *Simple Network Management Protocol* (SNMP) (MAURO; SCHMIDT, 2005; PRAS, 1995), detalhado na sessão 2.2 a seguir.

2.2 SNMP

O SNMP é um protocolo de gerenciamento e monitoramento de redes de computadores. Com o aumento do tamanho e, consequentemente, da complexidade destas redes estas tarefas tornaram-se também mais complexas. O objetivo do SNMP então é facilitá-las e permitir visualizar o status atual da rede, manter um histórico de atividades, bem como receber avisos de forma imediata, para auxiliar a resolução e prevenção de problemas.

Publicado em 1988, este protocolo tornou-se muito popular e é considerado o protocolo padrão para gerenciar dispositivos em uma rede TCP/IP (STALLINGS, 1998b; NIC.BR, 2014). Ele opera na camada de aplicação transportando informações entre os dispositivos gerenciados e os sistemas de gestão de redes, possibilitando monitorar e alterar, por exemplo, interfaces, processadores, memórias, *softwares* de equipamentos como roteadores, *switches*, dispositivos *wireless*, servidores e *no-breaks*[3].

O SNMP constitui-se basicamente de:

- Um protocolo para a troca de informações de gerência;
- Um formato para a representação destas informações e;
- Um modelo arquitetural para organizar os sistemas distribuídos em termos de sistemas gerenciadores e agentes gerenciados ou gerentes e agentes.

A figura 9 mostra um sistema distribuído sob o ponto de vista do gerenciamento SNMP. Nela vários agentes, incluindo *firewall*, roteadores, impressoras, servidores de bancos de dados, etc, são monitorados por um gerente central que permite ao administrador gerenciá-los e receber alertas sobre seu funcionamento.

[3]Diferentemente de seu predecessor o *Simple Gateway Monitoring Protocol* (SGMP) mais voltado para o monitoramento de roteadores (MAURO; SCHMIDT, 2005). Apesar de apresentado pelos mesmos autores apenas um ano antes, os dois protocolos não possuem compatibilidade (CASE et al., 1988)

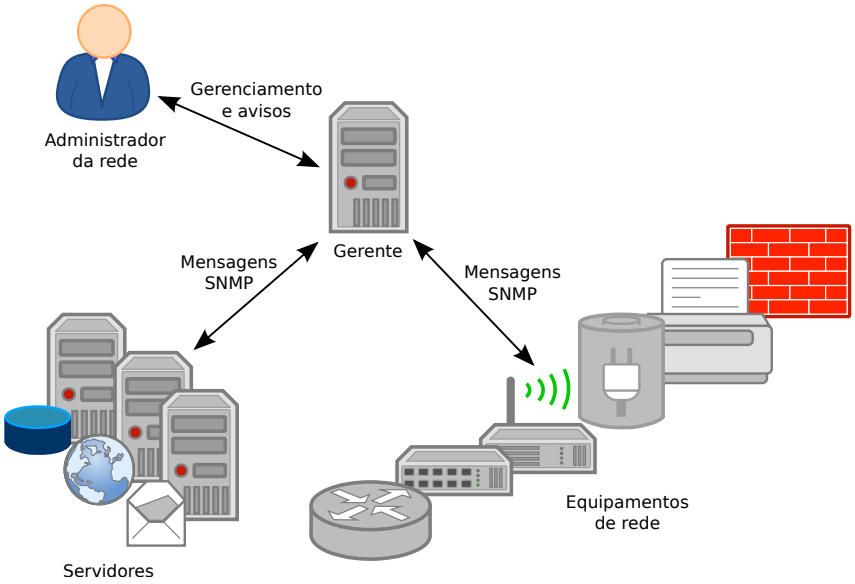


Figura 9: Um exemplo de arquitetura de um sistema SNMP contendo vários tipos de agentes. Adaptado de (LESKIW, 2017).

2.2.1 GERENTES E AGENTES

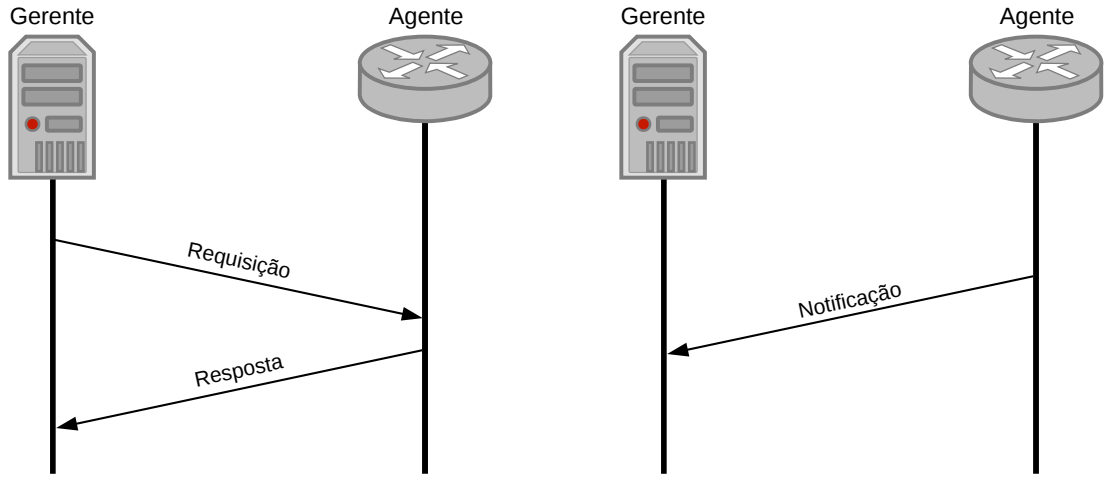
No modelo gerente/agente, um ou mais servidores com a função de gerente de rede, possuindo um conjunto de *softwares* ou Sistemas de Gestão de Redes (*Network Management System* - NMS), comunica-se com o agente de gerência de rede, instalado no dispositivo a ser gerenciado, através do protocolo de gerência.

O agente é um *software* em execução nos dispositivos que se deseja gerenciar. Nele, as informações relativas aos recursos gerenciados são mantidas em uma base de informações independente da arquitetura de *hardware* e *software* do agente, a MIB (*Management Information Base*) (MAURO; SCHMIDT, 2005). As MIBs serão descritas em detalhes na sessão 2.2.2 a seguir.

O gerente, no centro do sistema, recebe informações de todos os dispositivos/agentes da rede e, através do processamento destas informações, permite gerenciar toda a rede atuando como a interface o administrador da rede e o sistema gerenciado. É dele a tarefa de solicitar informações utilizando um modelo de requisições e respostas (*polling*). Através deste mecanismo as informações podem ser coletadas dos agentes periodicamente ou sob demanda e, além disso, permite enviar comandos aos agentes para alterar configurações ou o estado do dispositivo gerenciado. Por exemplo, o status das interfaces de rede, o tráfego de pacotes e o número de clientes associados a um *Access Point* gerenciado podem ser monitorados continuamente (mas não em tempo real) e, em face de algum erro, alguma ação pode ser tomada pelo gerente. Mais especificamente, um exemplo de objeto que pode ser recuperado seria um contador que

mantém registro do número de pacotes transmitidos e recebidos em um *link* e acompanhar sua carga. Ou o agente poderia ainda alterar o status de uma interface de rede, desabilitando-a.

Além de realizar solicitações, também é papel do gerente receber notificações (*traps*) dos agentes. As notificações são enviadas pelo agente quando determinados eventos ocorrem em um dispositivo e não dependem de uma solicitação. A figura 10 demonstra os mecanismos de comunicação do SNMP. Maiores detalhes sobre a troca de mensagens serão descritos na sessão 2.2.3.



(a) *Polling* (b) *Trap*

Figura 10: Modelos de comunicação do SNMP.
Elaborada pelo autor.

Estas funcionalidades básicas, a despeito de sua simplicidade, podem apresentar problemas na eficiência, segurança, flexibilidade e escalabilidade do protocolo (PEIXOTO, 2003). A fim de melhorá-las, uma nova versão do SNMP foi formulada. A versão 2 do protocolo, tecnicamente denominada SNMPv2c, foi apresentada em 1993 e revisada em 1996. Ela adicionou algumas funcionalidades e estruturas de dados apesar de ainda não possuir meios de autenticar o remetente das mensagens ou criptografar seus dados (STALLINGS, 1998a). Para uma listagem das RFCs que compuseram cada versão do SNMP, vide (JOHNSON, 2009).

2.2.2 MIBS

O SNMP em si não define os dados acessíveis em um dispositivo (JOHNSON, 2009). Estes dados são definidos por MIBs e é através delas que os agentes disponibiliza-os para os NMSs. Um agente pode conter várias MIBs e estas são criadas basicamente de duas maneiras, por padronizações do *Internet Engineering Task Force* (IETF) e outros órgãos de padronização

ou por terceiros (MAURO; SCHMIDT, 2005). Estes últimos normalmente são fabricantes de equipamentos de rede.

As MIBs são definidas através de um mecanismo, denominado SMI, que descreve e nomeia os objetos que serão gerenciados. Uma vez modelada, a MIB é escrita na notação *Abstract Syntax Notation 1* (ASN.1) – um padrão de sintaxe da ISO para tipos de dados e seus valores – uma linguagem muito utilizada para descrever informações estruturadas (MARTIN et al., 2013). Uma vez escritas, as MIBs devem ser publicadas de forma a permitir que agentes e gerentes as implementem.

No SMI os objetos gerenciados são representados por três atributos, seu nome, tipo e codificação (MAURO; SCHMIDT, 2005):

Nome ou identificador de objeto (*Object Identifier* - OID), define de forma global e única um objeto através de uma estrutura hierárquica, como uma árvore e de maneira similar a utilizada por servidores de nome (DNS). Ele pode ser representado por números ou de forma mais legível, porém verbosa. Ambos separados por pontos. Uma MIB pode incorporar OIDs de outras MIBs.

Tipo ou sintaxe, especifica como o dado é representado no *hardware*. Um dado pode, por exemplo, ser do tipo `INTEGER`, `STRING`, `COUNTER`, ou `SEQUENCE` dentre vários outros. Equipara-se aos tipos de dados em qualquer linguagem de programação. Uma MIB pode incorporar tipos de dados de outras MIBs. A implementação deste atributo é independente de arquitetura.

Codificação determina como um objeto é codificado e decodificado para que possam ser transmitidos entre NMSs e agentes em um meio físico qualquer.

Com base nestas definições, o objeto representando pelo OID `iso.org.dod.internet.mgmt.mib-2.interfaces`, ou 1.3.6.1.2.1.2, presente na MIB-II, uma MIB mandatória em qualquer nó da rede que implemente o SNMPv2 ou maior, disponibiliza o status de cada interface de rede da entidade gerenciada. Ela é representada como a subárvore da figura 11. Note entretanto que o nó raiz, `root-node`, apesar de representado na árvore, não deve aparecer no nome final e que algumas ramificações foram intencionalmente removidas da representação apenas por questão de simplicidade. As interfaces nesta OID são definidas como no trecho da MIB-II (MCCLOGHRIE; ROSE, 1991) apresentado a seguir:

```
ifTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF IfEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
            "A list of interface entries.  The number of
            entries is given by the value of ifNumber."
    ::= { interfaces 2 }
```

O tipo `SEQUENCE OF` é similar ao tipo `SEQUENCE` porém próprio para sequência de sequências (uma lista de listas). O que indica que cada entrada na tabela `ifTable` contém as colunas definidas em `IfEntry`. Este último, por sua vez, possui os dados mais relevantes sobre cada interface tais como MTU (unidade máxima de transmissão), velocidade, endereço físico, status administrativo, status operacional e número de octetos de entrada e saída. Note ainda que o objeto `ifTable` não pode ser acessado diretamente, apenas suas entradas estão acessíveis, e que ele é de implementação obrigatória.

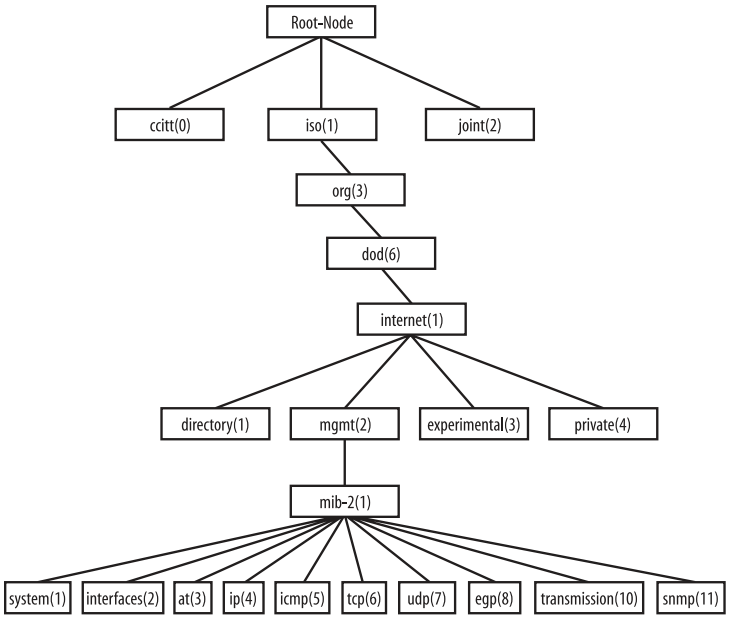


Figura 11: Subárvore da MIB-II contendo, dentre outros, o ramo `interfaces`. Adaptado de (MAURO; SCHMIDT, 2005).

A SMIv2, apresentada com o SNMPv2, estende a árvore do SNMP adicionando um novo ramo à subárvore `internet`, cuja OID é 1.3.6.1.6.3.1.1 ou `iso.org.dod.internet.-`

`snmpV2.snmpModules.snmp-MIB.snmpMIBObjects`. Isto resulta em alguns novos tipos dados na versão 2 do SNMP.

Abaixo da subárvore `private` (4), OID 1.3.6.1.4 na figura 11, existe um ramo denominado `enterprise` onde são adicionadas as MIBs de terceiros ou MIBs empresariais. A *Internet Assigned Numbers Authority* (IANA) é o órgão responsável pela distribuição, gratuita, de OIDs de forma a garantir sua universalidade. Uma lista de todos os números de empresas podem ser obtidos em sua página na internet. Por exemplo, o número privado da Universidade Tecnológica Federal do Paraná é 27165 (IANA, 2015), o que permite à instituição definir MIBs livremente abaixo da subárvore 1.3.6.1.4.1.27165 ou `iso.org.dod.internet.private.enterprise.utfpr`.

2.2.3 COMUNICAÇÃO

O protocolo SNMP utiliza segmentos UDP (*User Datagram Protocol*) no envio de mensagens entre gerentes e agentes. Com um grande número de nós sob monitoramento constante, uma quantidade considerável de tráfego pode se gerada. Apesar de não haver garantia na comunicação, o UDP foi escolhido por seu reduzido *overhead* minimiza o impacto na performance da rede. A figura 12 ilustra as formas de comunicação entre as entidades no modelo TCP/IP.

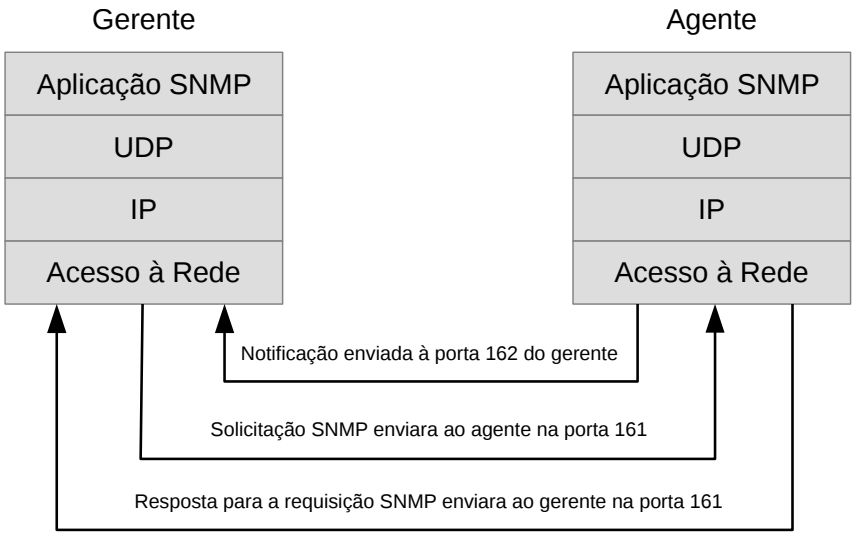


Figura 12: Troca de mensagens entre agente e gerente.
Adaptado de (MAURO; SCHMIDT, 2005).

Na camada de aplicação o agente ou gerente trata uma requisição ou notificação e provê serviços para os usuários. A camada UDP faz a comunicação entre as entidades nas portas definidas, o SNMP normalmente usa a porta UDP 161 para enviar e receber requisições e

a porta 162 para receber *traps*. A seguir, a camada IP encaminha os pacotes para seus endereços IP. E por fim, a camada de rede escreve os *bits* no meio físico, cabo metálico ou *wireless* por exemplo, endereçando-os ao endereço MAC da entidade.

SNMPv1 e SNMPv2 utilizam uma *string* denominada comunidade (*community*), que nada mais é do que uma senha, para o estabelecimento de comunicação confiável entre NMS e agente. O agente pode ser configurado com três tipos de *community*: somente-leitura, escrita e leitura e *trap*. A *community* somente-leitura permite apenas leitura de dados no agente, a leitura e escrita permite ler e modificar dados e valores no agente, e a *trap* permite envio de informações do agente para o NMS de forma assíncrona. É comum que os fabricantes utilizem a palavra *public* como padrão para a *community string* somente-leitura e *private* para leitura e escrita.

O mecanismo de comunidades é, entretanto, apenas uma tentativa|aproximação|versão simplista de segurança. Visto que a *community string* é enviada em texto pleno pela rede e pode ser facilmente interceptada e obtida, na prática o uso do SNMP torna-se limitado para fins de monitoração (STALLINGS, 1998a; PEIXOTO, 2003). A sessão 2.2.4 descreve como estes problemas foram solucionados.

Para realizar todas as tarefas de comunicação, o SNMP utiliza-se de um conjunto de operações. Cada uma delas pode possuir um formato especifico de *Protocol Data Unit* (PDU). Estas operações são sumarizadas a seguir.

get: é a requisição do gerente para o agente. Em sua execução devem ser fornecidos o dispositivo a ser consultado, uma lista de MIBs definidas por suas OIDs e a *community string* de acesso aos dados. Uma peculiaridade no formato do OID requisitado é que deve ser adicionado um número inteiro no final da OID, se o objeto for escalar termina-se a OID com um `.0`, se o objeto for uma tabela pode-se utilizar o índice da linha da tabela desejada, com `.1` para o primeiro registro.

getnext: permite obter mais de um valor de uma MIB. Nesta operação, após cada resposta com dados do agente, o NMS deve emitir um novo *getnext* até receber um erro indicando o fim dos dados.

getbulk: na operação *get*, se uma quantidade de dados superior à suportada pelo agente for solicitada, nenhum dado é retornado. Nesta operação, por outro lado, o agente retorna a informação solicitada ou o máximo que ele puder reunir para responder a solicitação, podendo inclusive truncar o resultado. Disponível a partir da versão 2.

set: usado para alterar o valor de um objeto gerenciado, criar uma nova entrada em uma tabela e alterar ou criar o atributo de um objeto (somente leitura ou leitura e escrita). Também é possível definir mais de um objeto por operação, mas se alguma delas falhar, nenhum objeto será alterado.

getresponse: em resposta a qualquer requisição ou atribuição (*set*) o agente, após reunir toda informação solicitada, envia ao NMS esta PDU.

trap: como descrito anteriormente, as *traps* são usadas no envio de informações não solicitadas. Nesta operação não é esperada do NMS uma confirmação de recebimento. As informações a serem enviadas e eventos que irão gerá-las são configurados no próprio agente. Podem ser úteis em reportar, por exemplo, alterações no status de interfaces de rede, a ventoinha de um *switch* ou roteador pára de funcionar ou ainda um serviço importante em um servidor pára.

A MIB enviada por uma *trap* contém um número de identificação que serve para determinar prontamente o tipo de problema ocorrido. Esta identificação assume valores de 0 a 6 indicando, por exemplo, `linkDown`, `authenticationFailure` ou `coldStart` que indica que o agente foi reiniciado. O valor 6 é reservado para *traps* customizadas definidas por terceiros. De fato, o OID das *traps* é composto pelo identificador da empresa (aquele fornecido pelo IANA) mais o número específico da *trap*. Tome, por exemplo, a *trap* customizada de OID 1.3.6.1.4.1.9.9.13.3.0.1, ela identifica o objeto `ciscoEnvMonShutdownNotification` e é enviada quando o dispositivo passar por um desligamento (CISCO, 2015).

notification: O SNMPv1 possui dois formatos diferentes, um para as *traps* e outro para as demais operações. No SNMPv2 o formato PDU é o mesmo para todas as operações (exceto a *getbulk*). Para padronizar o formato das traps do SNMPv1, o SNMPv2 introduziu o conceito de Notificação. Desta forma, o evento assíncrono enviado aos gerentes é chamado de *trap* no SNMPv1 e de *notification* no SNMPv2 e 3 (MAURO; SCHMIDT, 2005).

inform: também prevista a partir da versão 2 do SNMP, uma notificação de informe, diferentemente das notificações do tipo *trap* ou *notification*, espera uma confirmação de que foi recebida no destino. Caso não receba, deve ser retransmitida (PEIXOTO, 2003).

report: apesar de introduzida no SNMPv2, nunca foi implementada. Esta PDU é utilizada na versão 3 (ZELTSERMAN, 1999), conforme discutido na sessão 2.2.4 a seguir.

2.2.4 EVOLUÇÃO DO SNMP

Sua popularidade trouxe à tona seu principal problema, a segurança. O SNMPv3 foi criado então para complementar as funcionalidades do SNMPv1 e 2, fornecendo acesso seguro às informações através de autenticação e criptografia de pacotes.

Publicado como um conjunto de *Requests for Comments* (RFCs) em 1998, este conjunto de documentos apresentaram, mais especificamente, três importantes serviços: autenticação, privacidade e controle de acesso (STALLINGS, 1998a). Além disso, uma nova arquitetura para o protocolo é definida onde a ideia de agentes e gerentes é substituída, ambos são agora considerados entidades SNMP. O objetivo desta nova arquitetura é modularizar o sistema SNMP permitindo com que o protocolo seja facilmente estendido e que diferentes implementações dos módulos possam ser feitas (ZELTSERMAN, 1999; STALLINGS, 1998b).

A modularização permite, por exemplo, com que novos ou diferentes protocolos de segurança sejam portados para o SNMPv3 apenas definindo-os como novos módulos. Permite também implementações mais simples e enxutas para dispositivos com recursos limitados. Com isto, espera-se evitar com que "precisemos comprar livros SNMPv4 no futuro" (ZELTSERMAN, 1999).

As entidades são compostas de um motor (*engine*) e uma ou mais aplicações (*applications*) (MAURO; SCHMIDT, 2005), conforme pode ser visto na figura 13, primeiramente apresentada na RFC 2271. O motor é responsável pelo tratamento de mensagens (seu processamento e entrada e saída), controle de acesso e segurança. Ele é identificado pelo objeto `snmpEngineID`, definido na nova MIB 1.3.6.1.6.3.10.2.1, deve ser único no sistema distribuído em que estiver inserido. Um motor possui relação de um para um com sua entidade e portanto também a identifica de forma única no sistema (ZELTSERMAN, 1999). Os módulos do motor são disponibilizados como serviços para as aplicações configuradas na entidade efetivando sua comunicação.

O módulo *Dispatcher* realiza as seguintes três tarefas principais (STALLINGS, 1998a). Primeiramente ele é o controlador de tráfego, fazendo o envio e o recebimento das mensagens SNMP pela rede. Segundo, encaminha as mensagens para o Processador de Mensagens de modo a obter a PDU das que chegam e preparar a PDU de saída para envio na rede. Por fim, faz a entrega de PDUs vindas da rede para as aplicações e o encaminhamento de PDUs destas para a rede.

O Processador de Mensagens (*Message Processing Subsystem*) prepara as mensagens de saída para envio e extrai dados das provindas da rede. Pode conter submódulos para tratar

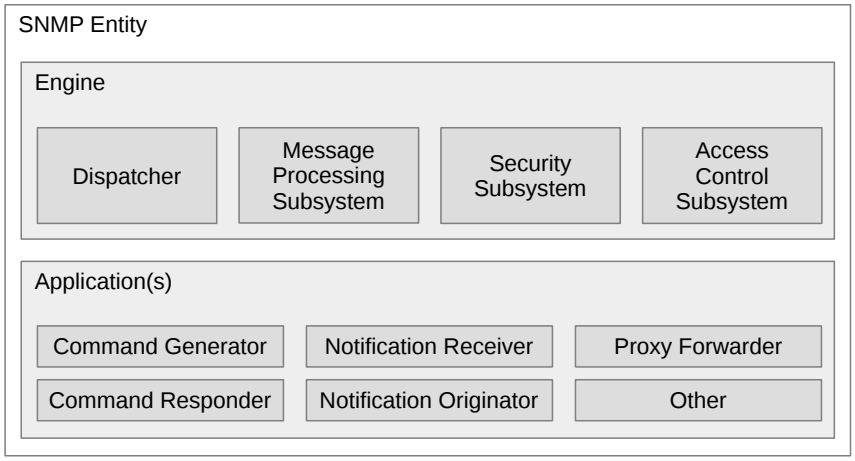


Figura 13: Entidade SNMP dividida em motor e aplicações, subdivididos em módulos. Adaptado de (HARRINGTON et al., 1998).

mensagens no formato SNMP 1, 2 e/ou 3 além de quaisquer outros formatos que se façam necessários (ZELTSERMAN, 1999).

O Subsistema de Segurança implementa o Modelo de Segurança do Usuário (*User Security Model* - USM) criado no SNMPv3 e provê autenticação e a criptografia e descriptografia de mensagens. Ele pode tratar tanto as *community strings* das versões 1 e 2 quanto autenticação de usuários da versão 3. A autenticação de usuários utiliza MD5 ou SHA1 nas senhas para que não sejam enviadas em texto aberto enquanto o algoritmo de criptografia padrão para garantir privacidade no envio de mensagens é o DES (MAURO; SCHMIDT, 2005). Mas é possível, claro, a implementação de diferentes módulos de segurança. Deve-se notar, por fim, que é possível configurar a comunicação com três tipos de segurança: nenhuma autenticação ou privacidade, apenas autenticação sem privacidade, ou autenticação e privacidade (MAURO; SCHMIDT, 2005).

Tanto para a autenticação quanto para a privacidade, o par a se comunicar deve ser configurado com uma senha compartilhada. Pode-se, apesar de menos seguro, usar apenas uma senha para configurar as duas funcionalidades. Para simplificar o gerenciamento destas senhas, foi proposto também um esquema de chaves localizadas (*localized keys*) onde o usuário compartilha a senha com um gerente central e este tem o papel de distribuí-la entre as *engines* remotas (STALLINGS, 1998b). Isto ocorre de forma independente para cada usuário de modo que ele precisará manter uma única senha (ou duas se estas forem configuradas para autenticação e privacidade).

O Controle de Acesso (*Access Control Subsystem*) implementa o Modelo de Controle de Acesso Baseado em Vistas (*View-Based Access Control Model* - VACM) proposto no SNMPv3 a fim de restringir o acesso às MIBs. Através de um conjunto de serviços de autori-

zação o acesso ao objeto gerenciado para o usuário autenticado será permitido ou negado. Este módulo é utilizado tanto para verificar autorizações quanto para modificar o acesso de usuários.

O controle no modelo VACM se dá através de grupos, níveis de segurança e contextos (STALLINGS, 1998b). Os grupos servem para categorizar os usuários e permitir diferentes direitos de acesso. Os níveis de segurança irá restringir ou permitir acesso a informações baseado no nível de segurança da mensagem, por exemplo, permitindo acesso somente-leitura para uma requisição sem autenticação. Um contexto refere-se a um subconjunto nomeado de MIBs em um agente determinando se o subconjunto de informações será acessível para uma SNMP *engine* ou não.

No SNMPv3 existem 5 tipos predefinidos de aplicações internas na entidade SNMP e novas aplicações podem ser criadas conforme necessário. Os 5 tipos básicos são listados a seguir:

Command Generator: emite as operações *get*, *getnext*, *getbulk* e *set* e processa suas respostas.

Command Responder: emite uma resposta para as requisições *get*, *getnext*, *getbulk* e *set* levando em consideração o controle de acesso.

Notification Originator: monitora o sistema e gera mensagens de notificação ou informe para eventos pré-configurados.

Notification Receiver: recebe notificações e informes processando-as e gerando uma resposta se a PDU recebida for um informe.

Proxy Forwarder: provê o encaminhamento de mensagens entre entidades. Sua implementação em uma entidade não é obrigatória.

De acordo com os módulos do motor e aplicações apresentadas, pode-se notar que o gerente das versões 1 e 2 é agora composto por um motor e as aplicações para gerar e receber notificações e um gerador de comandos. Um agente tradicional, por sua vez, além do motor conta com aplicações tais como um gerador de notificações e um componente responsável por responder comandos. Em ambos os casos, claro, o módulo de segurança utilizado seria o de *community strings*. Isto apenas torna evidente a compatibilidade da versão 3 com as versões anteriores.

Deve-se notar, porém, que o formato da mensagem SNMPv3 possui novos campos para suportar as funcionalidades de segurança. As mensagens são divididas em duas partes, o cabeçalho, que, dentre outras, contém informações a serem processadas para garantir segurança,

e a porção de dados (*payload*). O cabeçalho SNMPv3 apenas empacota uma PDU tradicional SNMP, ou seja, o *payload* de uma mensagem desta versão do protocolo equivale a uma PDU das versões 1 ou 2 (STALLINGS, 1998b; MAURO; SCHMIDT, 2005).

No SNMPv3 não há alteração nas operações definidas nas versões anteriores, entretanto, os *reports* passam a ser utilizados nesta versão. Eles permitem a comunicação entre motores de entidades para, por exemplo, informar um motor SNMP que um erro foi encontrado ao processar uma mensagem enviada por ele. *Reports* são gerados para basicamente dois tipos de problemas: uma mensagem de resposta não pôde ser gerada ou quando ocorrer um erro ao processar a criptografia de autenticação e privacidade de mensagens de entrada (ZELTSERMAN, 1999).

2.3 REDES SEM FIO 802.11

As redes sem fio apresentam uma série de vantagens sobre as redes cabeadas tradicionais, elas permitem mobilidade, são de implantação rápida e muito flexível além de ser financeiramente atraentes em manutenção e, pelo menos a longo prazo, implantação. Impulsionada principalmente pelo grande apelo em termos de mobilidade para usuários finais, é uma tecnologia em constante crescimento e desenvolvimento. A tecnologia de redes de dados sem fio de maior sucesso é o padrão 802.11 (GAST, 2005) do *Institute of Electrical and Electronic Engineers* (IEEE).

O 802.11 utiliza basicamente ondas eletromagnéticas como mídia de transporte de dados e, sendo um recurso limitado, é cuidadosamente regulamentado (WNDW; BUTLER, 2013; GAST, 2005). Tendo em mente que uma das formas de aumentar a banda de transmissões sem fio é alocando uma faixa maior do espectro eletromagnético, normalmente novos padrões de conexão são definidos com o avanço da tecnologia. A tabela 9 mostra alguns detalhes dos principais padrões sem fio.

Redes sem fio (*wireless* LANs ou WLANs) podem apresentar dois tipos de arquitetura, *ad-hoc*, onde os dispositivos estão conectados ponto-a-ponto entre si (não muito popular), e de infraestrutura onde os dispositivos estão associados a um ponto de acesso (AP) e deste tem acesso ao sistema de distribuição de uma LAN (TANENBAUM; WETHERALL, 2010; GAST, 2005). A figura 14 exibe um exemplo de arquitetura sem fio.

Um AP é responsável por converter os quadros da rede 802.11, vindos dos clientes *wireless*, para quadros compatíveis com a LAN cabeada em que estiver conectado. Vários APs podem estar conectados criando um conjunto de serviços estendido (*Extended Service Set* -

Tabela 9: Principais camadas físicas do padrão 802.11.

Padrão IEEE	Frequência (GHz)	Banda (MHz)	Velocidade por fluxo (Mbps)	Alcance aproximado (m)
802.11b	2,4	20	11 Mbps	35/140
802.11a	5	20	54 Mbps	35/120
802.11g	2,4	20	54 Mbps	38/140
802.11n	2,4/5	20/40	72,2/150[a]	70/250
802.11ac	5	20/40/80/160	87,6/200/433,3/866,7[b]	

[a] Utiliza multiplos fluxos de entrada e saída (MIMO) e permite utilização de até 4 antenas para transmissão.
[b] Utiliza MU-MIMO (uma antena pode transmitir multiplos fluxos para múltiplos usuários) e permite utilização de até 8 antenas para transmissão.

Adaptado de (WNDW; BUTLER, 2013).

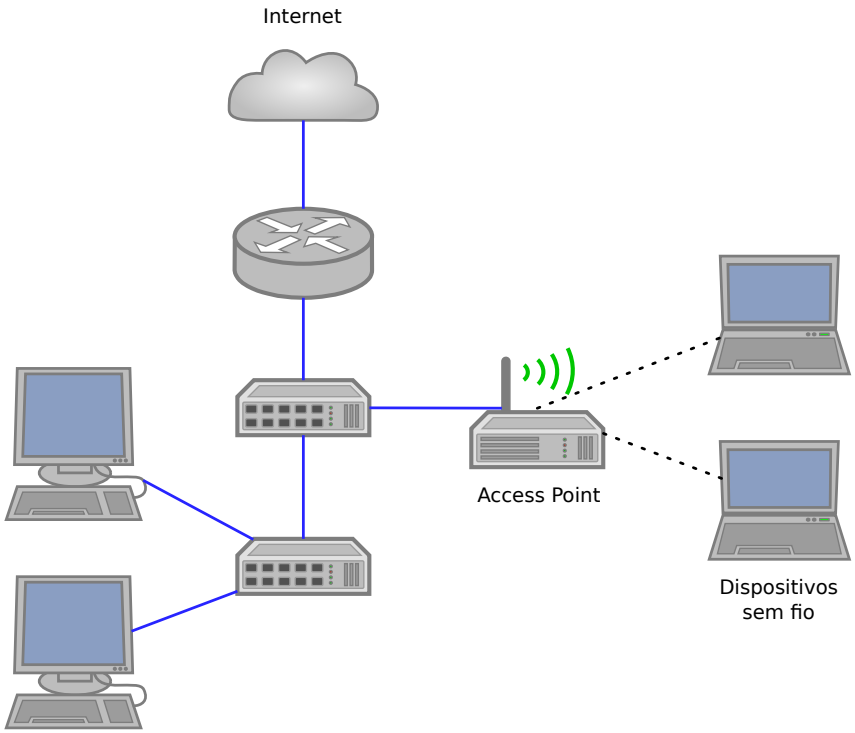


Figura 14: Arquitetura de uma LAN com suporte a 802.11.
Elaborada pelo autor.

ESS) permitindo que clientes conectados a diferentes APs possam se comunicar. Em um ESS, se a área de cobertura de um AP, denominada célula, possuir uma porcentagem mínima de sobreposição, variável de acordo com o equipamento e frequência utilizada (CISCO, 2010), com outra célula é possível criar o recurso de *roaming* (GAST, 2005).

Cada AP é identificado por um *Service Set Identifier* (SSID). Em uma ESS todos os APs devem possuir o mesmo SSID que irá funcionar como o "nome da rede" para o usuário (GAST, 2005).

Roteadores sem fio podem atuar como AP, switch e roteador (Cisco CCNA 4.0).

A natureza aberta da transmissão sem fio, entretanto, torna as questões de segurança ainda mais sensíveis. Tráfego não protegido pode ser facilmente interceptado (*eavesdropping*) e usuários não autorizados podem se conectar à rede livremente se não houver controle de acesso. Ou ainda, um ataque de negação de serviço, *denial of service* (DoS), pode ser gerado por aparelhos operando na mesma faixa de frequência da rede sem fio pode gerar interferência bem como por um invasor com um dispositivo *wireless* atuando como um AP pode gerando tráfego ou embaralhando comandos na rede. Para protegê-la, alguns protocolos de controle de acesso à rede sem fio foram definidos (GAST, 2005; WNDW; BUTLER, 2013):

WEP: elaborado em conjunto com o padrão 802.11, o *Wired Equivalent Privacy* realiza criptografia dos dados mas é facilmente quebrado e utiliza uma chave compartilhada única entre todos os usuários.

WPA: criado como um padrão interino para substituir o WEP, o *Wi-Fi Protected Access* provê melhor autenticação e privacidade através do protocolo *Temporary Key Integrity Protocol* (TKIP) mas, por ser compatível com o WEP, sua segurança pode ser questionada (WNDW; BUTLER, 2013).

WPA2: é padrão terminado, denominado IEEE 802.11i, que deprecia o TKIP. Utiliza o *Advanced Encryption System* (AES) e é o padrão indicado para a maioria das redes.

WPA e WPA2 podem operar em dois modelos de autenticação através do padrão IEEE 802.1X. Este padrão é baseado no *Extensible Authentication Protocol* (EAP) que permite implementar diferentes métodos para gerenciar o *login* na rede, tais como, LEAP, PEAP e EAP-TLS (GAST, 2005). No primeiro modelo, o *Personal*, chamado ainda Pessoal ou *Pre Shared Key* (PSK), uma chave é compartilhada entre todos os clientes e o AP, similar ao WEP. Já no modelo Empresarial (*Enterprise*), cada usuário tem um nome de usuário e senha e sua autenticação será feita em um servidor *Remote Authentication Dial In User Service* (RADIUS), responsável pela autenticação, autorização e contabilidade (GAST, 2005; WNDW; BUTLER, 2013).

Esta é apenas uma apresentação de alguns itens importantes relacionados à segurança nas redes 802.11 que podem ser objeto de monitoramento e gerenciamento. Este é um tema muito extenso e, para maior aprofundamento, recomenda-se, por exemplo, os trabalhos:

- 802.11 Security (POTTER, 2002);
- 802.11 Wireless Networks: The Definitive Guide (GAST, 2005) e;

- Building Secure Wireless Networks with 802.11 (KHAN, 2003).

2.4 OPENWRT

O OpenWrt, criado em 2004, é uma distribuição Linux, um *software* livre e gratuito sob a licença GPL, baseada em uma versão livre do código fonte do roteador sem fio WRT54G disponibilizado publicamente por sua fabricante, Linksys (OPENWRT, 2016b). Primariamente destinado para uso em sistemas embarcados, basicamente roteadores sem fio, para roteamento de tráfego de rede.

O projeto utiliza os códigos fonte oficiais do *kernel* GNU/Linux e adiciona código para dar suporte a mais *drivers* e dispositivos. Provendo, apesar de seu minimalismo, um ambiente altamente extensível e configurável, incluindo gerenciamento de pacotes e um *framework* para desenvolvimento (OPENWRT, 2016b).

Por estas características, vários projetos utilizam o OpenWrt, tais como, DD-WRT e Gargoyle. A Oi Telecomunicações, por exemplo, utiliza em seus *hotspots WiFi*[4] equipamentos da empresa Fon, cujo *software* é baseado no OpenWrt (FON, 2015).

Em sua página na *internet* está disponível uma lista de equipamentos compatíveis com o OpenWrt (OPENWRT, 2016b). Dentre eles encontra-se o *access point* PicoStation M2HP da empresa Ubiquiti, utilizado neste trabalho como descrito no capítulo 4.

2.5 GERENCIAMENTO

O gerenciamento em uma rede sem fio, apesar de similar ao das redes cabeadas, possui algumas peculiaridades. Segundo (LI; CHEN, 2004), estas redes possuem uma topologia hierárquica de dispositivos móveis associadas à pontos de acesso. Estes dispositivos estão em *roaming* entre os APs, muitas vezes não possuem agentes de gerenciamento e podem não apresentar um padrão de persistência na rede, entrando ou deixando a rede de maneira imprevisível. Além disso, as WLANs possuem esquemas mais delicados de segurança. Por outro lado, as tecnologias envolvidas em dispositivos e pontos de acesso fornecem uma nova gama de informações a serem gerenciadas.

Na fase de planejamento de uma WLAN, os quesitos mobilidade, segurança e transmissão devem ser considerados. A localização dos APs deve ser calculada para evitar desperdício

[4]Os termos *WiFi* e *hotspot* são os nomes comerciais para, respectivamente, rede sem fio e pontos de acesso (MORREALE; TERPLAN, 2009).

e pontos cegos, a performance deve ser otimizada no canal de rádio a ser usado e garantir a comunicação entre as redes cabeada e sem fio (GAST, 2005; WNDW; BUTLER, 2013). Durante a operação, a configuração e otimização de performance (qualidade e potencia de sinal) dos equipamentos, por exemplo, são essenciais no gerenciamento (LI; CHEN, 2004).

Os pontos de acesso são componentes complexos e fundamentais nas redes sem fio. Algumas de suas características dignas de gerenciamento e monitoramento podem ser:

- Endereço IP e rede da LAN conectada;
- Endereço IP do *gateway* padrão;
- SSID para identificar a rede;
- Nome e endereço MAC;
- Parâmetros de sinal, tais como, canal em uso, potência de transmissão, taxa de quadros *beacon*;
- Parâmetros da interface de rede: velocidade de conexão e modo duplex, endereços de DNS;
- Parâmetros de tráfego: *overhead* do protocolo de mensagens a serem filtradas, TTL de pacotes (*packet life limits*), tamanho do preâmbulo, limites de taxa máxima de mensagens (*maximum message rate thresholds*), limite dos tamanhos de *frames Request-To-Send*/*Clear-To-Send* (RTS/CTS);
- Parâmetros de segurança: listas de controle de acesso (*Access Control Lists* - ACL), método de criptografia de acesso, processo de autenticação, identificação do servidor RADIUS, chaves de criptografia, filtros de endereços MAC, limites de fragmentação;
- Clientes: lista de clientes conectados ao *access point*, seus sistemas operacionais, tempo de *lease* do DHCP.

Uma MIB unificada do padrão 802.11 foi criada, IEEE802dot11-MIB, mas apenas os maiores fabricantes tem suporte completo a ela, outros apenas parcialmente ou nenhum suporte. Além disso ela já está defasada, faltando algumas funcionalidades de tecnologias mais novas (MORREALE; TERPLAN, 2009).

3 METODOLOGIA

Este capítulo descreve a metodologia de pesquisa utilizada neste trabalho, sua classificação e os critérios em que se basearam.

Inicialmente, uma breve revisão de literatura, baseada em pesquisa bibliográfica (GIL, 2002), foi realizada com o objetivo de aprofundar-nos no protocolo SNMP, gerenciamento e seus relacionamentos com as redes 802.11. Isto permitiu que a hipótese da obtenção de informações customizadas via SNMP pudesse ser elaborada. Este cenário caracteriza as pesquisas exploratórias (GIL, 2002).

Esta é uma pesquisa qualitativa. Mais especificamente, o método qualitativo empregado foi o estudo de caso, no sentido de descrever o método de pesquisa deste trabalho (DIAS; SILVA, 2009).

Esta pesquisa enfoca a utilização de uma tecnologia bem difundida para expandir a capacidade de monitoramento de dispositivos sem fio. Mais especificamente empregando o protocolo SNMP e dispositivos compatíveis com o sistema operacional OpenWrt.

Inicialmente, os recursos disponibilizados pelo protocolo SNMP para fornecer informações customizadas foram avaliados. A seguir, analisou-se o protocolo 802.11 e dispositivos sem fio para listar os dados a serem monitorados.

Uma prova de conceito foi elaborada, implementando-se uma extensão ao SNMP e utilizando a aplicação de monitoramento Zabbix para visualizar os dados obtidos.

O universo desta pesquisa é formado por usuários tradicionais de redes sem fio que utilizam, de maneira transparente, pontos de acesso baseados no OpenWrt para navegar pela internet.

4 CLIENTE SNMP PARA OPENWRT

Este capítulo descreve o projeto e implementação do cliente SNMP para dispositivos OpenWrt, a definição das informações a serem gerenciadas e sua obtenção dos dispositivos.

4.1 OPENWRT

O OpenWrt utiliza o código oficial do GNU/Linux, conforme descrito na sessão 2.4. Isto permite que vários pacotes sejam portados para o OpenWrt mais facilmente. O Net-SNMP (NET-SNMP, 2016), por exemplo, é um *software* de código aberto e livre que possui uma versão portada para o OpenWrt. O *download* de seu código e executável podem ser feitos da página do OpenWrt na internet e de seus repositórios (OPENWRT, 2016b), respectivamente. Até a elaboração do presente trabalho, outubro de 2016, a versão disponibilizada no *site* e utilizada neste trabalho era a 5.4.2.1.

Como a maioria das distribuições Linux, o OpenWrt fornece um gerenciador de pacotes, denominado `opkg`, que permite a instalação descomplicada, dentre outros, do Net-SNMP (OPENWRT, 2016b). Uma vez instalado o *software* é possível habilitar o agente SNMP que fica em execução na forma do serviço `snmpd`.

O Sistema Operacional (SO) utiliza um sistema centralizado de configuração denominada Interface de Configuração Unificada (*Unified Configuration Interface* - UCI[1]) que uniformiza a localização e a formatação dos arquivos de configuração dos programas de terceiros instalados (OPENWRT, 2016b). O Net-SNMP utiliza este sistema e seu arquivo de configuração está localizado em `/etc/config/snmpd`[2].

Este arquivo é mantido pelos desenvolvedores do OpenWrt e está disponível em seu repositórios de pacotes. Ele permite configurar, por exemplo:

- Informações de rede como protocolo e porta;

[1] Vide `https://wiki.openwrt.org/doc/uci`.
[2] Vide `https://wiki.openwrt.org/doc/uci/snmpd`.

- Informações do dispositivo tais como nome, localização e responsável;
- As *community strings* públicas e privadas;
- Regras de acesso aos dados do dispositivo e;
- Definição de comandos arbitrários que permitem estender a funcionalidade do agente.

O último ponto listado permite que um dado programa, ou um conjunto de programas, seja executado a fim de obter informações que o agente não esteja programado para obter (de MIBs que ele não implemente) ou qualquer tipo de informação que se deseje. Esta informação é obtida através de uma requisição simples do gerente a uma determinada OID. Mais especificamente, a OID `UCD-SNMP-MIB::extTable`, ou 1.3.6.1.4.1.2021.8, denota uma tabela contendo o nome do comando, o comando em si e o resultado do mesmo, dentre outras informações.

Por exemplo, o seguinte trecho do arquivo de configuração `/etc/config/snmpd`, figura 17, define dois comandos customizados arbitrários, um para obter a carga do sistema (*load*) e outro para obter o tempo de funcionamento (*uptime*) do dispositivo.

```
# Comando para obter a carga
config exec
option name load
option prog /usr/local/bin/myload

# Comando para obter o uptime
config exec
option name uptime
option prog /usr/local/bin/myuptime
# option args /caminho/para/arquivo
```

Figura 17: Exemplo de configuração do snmpd.

Como de costume, as linhas começadas com cerquilha são consideradas comentários e não interferem nas configurações. No segundo bloco do exemplo, a opção comentada `args` permite que o valor fornecido ali seja passado como parâmetro para o comando definido. Isto permite, por exemplo, que um único programa seja utilizado para retornar diferentes tipos de dados de acordo com o parâmetro informado. O snmpd permite inclusive implementar OIDs indisponíveis através destes comandos customizados, vide 4.1.1.

No computador gerente, um comando *get* em um dispositivo com esta configuração irá obter como resposta uma tabela similar à 12:

Tabela 12: Exemplo do resultado obtido de um comando customizado configurado em um dispositivo OpenWrt.

OID	Dado
UCD-SNMP-MIB::extIndex.1	1
UCD-SNMP-MIB::extIndex.2	2
UCD-SNMP-MIB::extNames.1	load
UCD-SNMP-MIB::extNames.2	uptime
UCD-SNMP-MIB::extCommand.1	/usr/local/bin/myload
UCD-SNMP-MIB::extCommand.2	/usr/local/bin/myuptime
UCD-SNMP-MIB::extResult.1	1
UCD-SNMP-MIB::extResult.2	1
UCD-SNMP-MIB::extOutput.1	0.8
UCD-SNMP-MIB::extOutput.2	11:48

4.1.1 A MIB 802.11

Traduzindo livremente (JOHNSON, 2009):

> Existe uma MIB padrão para redes sem fio IEEE 802.11, `IEEE802dot11-MIB`. Algumas de suas OIDs incluem configurações do AP tais como o tempo limite de autenticação e o intervalo com o qual os *beacons* são transmitidos. Também estão incluídas várias métricas que estão diretamente relacionadas ao desempenho geral de uma rede sem fio, como contagens de quadros transmitidos e recebidos e quadros RTS bem-sucedidos e com falha para um AP específico.

O OpenWrt depende do projeto, e subsequente implementação, dos drivers para disponibilizar maiores informações sobre a placa e as conexões sem fio bem como sobre os clientes conectados (OPENWRT, 2014). Considerando os pontos de acesso utilizados nesta prova de conceito, baseado no *driver* `ath9k`, os dados relativos à MIB 802.11 suportados são exemplificados na figura 18 a seguir.

Como pode ser notado, a MIB é implementada apenas parcialmente. Algumas informações adicionais sobre o ponto de acesso podem ser obtidas através de comandos no OpenWrt, arquivos de configuração ou variáveis. Comandos como o `iw` pode fornecer, por exemplo, o BSSID, canal (frequência) em uso, tipo, interface em uso. Os arquivos de configuração podem conter tipo de segurança utilizada, dispositivo, rede em utilizada e força do sinal (TX Power) para cada SSID configurado. Por fim, algumas variáveis do *kernel* linux, disponíveis no sistema de arquivos proc, podem ser úteis. Contadores de RTS bem e mau sucedidos, ACKs e *Frame Check Sequence* (FCS) falhos podem ser obtidos desta forma.

```
IEEE802dot11-MIB::dot11StationID.9 = STRING: AA:AA:AA:11:11:11
IEEE802dot11-MIB::dot11StationID.10 = STRING: BB:BB:BB:22:22:22
IEEE802dot11-MIB::dot11PrivacyOptionImplemented.9 = INTEGER: true(1)
IEEE802dot11-MIB::dot11PrivacyOptionImplemented.10 = INTEGER: true(1)
IEEE802dot11-MIB::dot11PowerManagementMode.9 = INTEGER: active(1)
IEEE802dot11-MIB::dot11PowerManagementMode.10 = INTEGER: active(1)
IEEE802dot11-MIB::dot11DesiredBSSType.9 = INTEGER: any(3)
IEEE802dot11-MIB::dot11DesiredBSSType.10 = INTEGER: any(3)
IEEE802dot11-MIB::dot11AuthenticationAlgorithm.9.1 = INTEGER: openSystem(1)
IEEE802dot11-MIB::dot11AuthenticationAlgorithm.9.2 = INTEGER: sharedKey(2)
IEEE802dot11-MIB::dot11AuthenticationAlgorithm.10.1 = INTEGER: openSystem(1)
IEEE802dot11-MIB::dot11AuthenticationAlgorithm.10.2 = INTEGER: sharedKey(2)
IEEE802dot11-MIB::dot11AuthenticationAlgorithmsActivated.9.1 = INTEGER: true(1)
IEEE802dot11-MIB::dot11AuthenticationAlgorithmsActivated.9.2 = INTEGER: false(2)
IEEE802dot11-MIB::dot11AuthenticationAlgorithmsActivated.10.1 = INTEGER: true(1)
IEEE802dot11-MIB::dot11AuthenticationAlgorithmsActivated.10.2 = INTEGER: false(2)
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.9.1 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.9.2 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.9.3 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.9.4 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.10.1 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.10.2 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.10.3 = ""
IEEE802dot11-MIB::dot11WEPDefaultKeyValue.10.4 = ""
IEEE802dot11-MIB::dot11PrivacyInvoked.9 = INTEGER: false(2)
IEEE802dot11-MIB::dot11PrivacyInvoked.10 = INTEGER: false(2)
IEEE802dot11-MIB::dot11WEPDefaultKeyID.9 = Wrong Type (should be Gauge32 or
Unsigned32): INTEGER: 0
IEEE802dot11-MIB::dot11WEPDefaultKeyID.10 = Wrong Type (should be Gauge32 or
Unsigned32): INTEGER: 0
IEEE802dot11-MIB::dot11ExcludeUnencrypted.9 = INTEGER: false(2)
IEEE802dot11-MIB::dot11ExcludeUnencrypted.10 = INTEGER: false(2)
IEEE802dot11-MIB::dot11MACAddress.9 = STRING: AA:AA:AA:11:11:11
IEEE802dot11-MIB::dot11MACAddress.10 = STRING: BB:BB:BB:22:22:22
IEEE802dot11-MIB::dot11RTSThreshold.9 = Wrong Type (should be Gauge32 or
Unsigned32): INTEGER: 2347
IEEE802dot11-MIB::dot11RTSThreshold.10 = Wrong Type (should be Gauge32
or Unsigned32): INTEGER: 2347
IEEE802dot11-MIB::dot11FragmentationThreshold.9 = Wrong Type (should be Gauge32 or
Unsigned32): INTEGER: -1
IEEE802dot11-MIB::dot11FragmentationThreshold.10 = Wrong Type (should be Gauge32 or
Unsigned32): INTEGER: -1
IEEE802dot11-MIB::dot11ResourceTypeIDName.0 = STRING: RTID
IEEE802dot11-MIB::dot11manufacturerOUI.9 = STRING: "AA:AA:AA"
IEEE802dot11-MIB::dot11manufacturerOUI.10 = STRING: "BB:BB:BB"
```

Figura 18: Implementação parcial da MIB 802.11 no OpenWrt.

4.1.2 CLIENTES

Como citado na sessão 4.1.1, as ferramentas disponíveis no sistema operacional dependem do *driver* em uso. Com relação aos clientes conectados aos *access points* PicoStation

M2HP, sem intervir nos dispositivos clientes, através do comando `iw` (OPENWRT, 2017b), as informações a seguir podem ser obtidas:

- Endereço MAC;
- Número de *bytes* e pacotes transmitidos e recebidos (TX e RX);
- Número de transmissões falhas e re-tentadas;
- Nível imediato e médio de sinal;
- Taxa de *bits* por segundo transmitidos e recebidos;
- Autenticação e autorização;
- Tipo de preâmbulo;
- WMM/WME, MFP e TDLS.

4.2 INDO ALÉM DA MIB 802.11

Utilizando as ferramentas disponibilizadas pelo OpenWrt e os recursos do pacote snmpd, é possível estender o agente SNMP. A partir da lista de novos itens a serem monitorados, pôde-se escrever um código para obtê-los e utilizá-lo no agente SNMP.

Nesta prova de conceito optou-se por utilizar uma entrada de configuração `config exec` nas configurações do snmpd para cada tipo de informação a ser monitorada. A figura 19 apresenta um trecho do arquivo de configuração, `/etc/config/snmpd`, contendo os comandos customizados.

Como pode-se notar, um *script* único, `geser.sh`, foi desenvolvido para atender todas as solicitações de informação em um AP. O *script* apresenta um conjunto de funções independentes implementando cada tipo de requisição e foi escrito para o interpretador de linha de comando BusyBox[3] utilizado pelo OpenWrt. Mais especificamente, os recursos utilizados em cada função foram:

- O número de clientes conectados pode ser obtido pelo comando:
  `$ iw dev <interface sem fio> station dump`

[3] O BusyBox é um *fork* do interpretador `ash`, um projeto do Debian (OPENWRT, 2016a).

```
config exec
        option name     clients
        option prog     /etc/snmp/scripts/geser.sh
        option args     --clients
#       option miboid   1.2.3.4

config exec
        option name     wifi
        option prog     /etc/snmp/scripts/geser.sh
        option args     --wifi

config exec
        option name     numclients
        option prog     /etc/snmp/scripts/geser.sh
        option args     --numclients

config exec
        option name     BSSID
        option prog     /etc/snmp/scripts/geser.sh
        option args     --bssid

config exec
        option name     frequency
        option prog     /etc/snmp/scripts/geser.sh
        option args     --frequency
```

Figura 19: Configuração com comandos customizados.

- Uma vez que o número de clientes conectados varia no tempo, uma função que retorna uma lista de informações de cada cliente conectado foi criada. Ela trata (faz o *parse* e organiza) as informações obtidas do mesmo comando do item anterior.
- Considerando que o número de interfaces sem fio pode ser diferente em diferentes APs, uma lista de informações sobre cada interface é necessária. A lista é construída a partir do arquivo de configuração:
  `/etc/config/wireless`
- O BSSID pode ser obtido do comando:
  `$ iw dev <interface sem fio> info`
- A frequência de operação pode ser obtido do mesmo comando do item anterior.

Conforme descrito na sessão 4.1, estes dados podem ser obtidos, por exemplo, através

de um comando `snnpget`:

```
$ snmpget -v 2c -c <community string> <IP do ponto de acesso> \
UCD-SNMP-MIB::extOutput.1
```

A seguir são listados detalhadamente os dados fornecidos por esta implementação:

- Número de clientes conectados no AP;
- Lista de clientes conectados onde cada entrada contém as seguinte informações:
  - Índice do cliente;
  - Número de *bytes* transmitidos pelo cliente (TX);
  - Número de *bytes* recebidos pelo cliente (RX);
  - Potência do sinal, medido em dBm, recebido pelo cliente.
- Lista de interfaces sem fio onde cada entrada contém:
  - Índice da interface;
  - Dispositivo associado à interface;
  - SSID da rede;
  - Tipo de segurança utilizada na rede.
- O BSSID do ponto de acesso;
- Frequência de operação do ponto de acesso.

4.3 MONITORAMENTO

A fim de obter uma melhor visualização dos dados disponibilizados por esta implementação e completar este caso de uso, um servidor de monitoramento foi preparado para coletar informações dos *access points* de uma rede sem fio.

Existem vários *softwares* de monitoramento disponíveis, alguns deles em código aberto e gratuitos tais como o Cacti, Icinga (inicialmente um *fork* do Nagios) e o Zabbix. Neste trabalho optou-se por utilizar o Zabbix principalmente por alguns fatores:

- Quantidade de recursos oferecidos *out-of-the-box*;

- Flexibilidade, permitindo facilmente mapear as informações customizadas implementadas neste estudo;
- Documentação bem detalhada e comunidade de usuários ativa[4] e;
- Simplicidade de implantação, possuindo pacotes binários e repositórios disponíveis para as principais distribuições Linux.

A estrutura implantada, ilustrada na figura 20, contou com seis pontos de acesso PicoStation M2HP da Ubiquiti (tomados por amostragem), conectados a (e alimentados por) *switches* PoE que se conectam ao *gateway* da rede, um servidor Debian que possui conexão com a Internet e atua provendo serviços de DHCP, 802.1X (RADIUS) e cache de nomes e navegação.

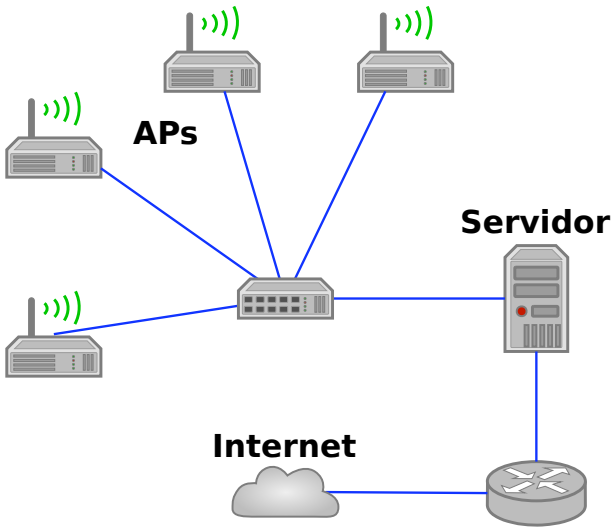


Figura 20: Estrutura física utilizada neste estudo. Elaborada pelo autor.

Os usuários recebem um nome de usuário e uma senha, cadastrados no RADIUS, e ao se associarem aos pontos de acesso podem se autenticar utilizando o modelo de segurança pré-configurado no servidor RADIUS.

Com a infraestrutura de redes e serviços em operação, o serviço de monitoramento Zabbix foi instalado e os 6 clientes (*hosts*), APs, foram configurados. O Zabbix conta com *templates* pré configurados inclusive para dispositivos SNMP-*ready*. Com isto, ao habilitar o serviço SNMP nos APs e aplicar o *templates*[5] no cliente Zabbix, as informações mais básicas já passam a ser monitoradas pelo *software*: informações gerais sobre o cliente e uso de disco, pro-

[4]Uma consulta rápida em `https://www.zabbix.com/forum/` indicou 38173 usuários registrados nos fóruns. Consulta realizada em 15/02/2017.

[5]Maiores informações disponíveis na documentação. Na versão 3.2, vide: `https://www.zabbix.com/documentation/3.2/manual/config/templates`.

cessador e interfaces de rede. Ainda há a vantagem do OpenWrt, como um sistema operacional Linux, permitir monitoramento via *template* Linux disponível "de fábrica" no Zabbix.

Os recursos básicos do Zabbix incluem a definição de itens a serem monitorados, gatilhos (*triggers*) para avaliar os dados de um item e definir o status do cliente e representações gráficas para vários itens em um cliente. A figura 21 mostra a visualização de um gráfico de uso de disco em um ponto de acesso no Zabbix enquanto a figura 22 mostra o gráfico de utilização da interface `wlan0`.

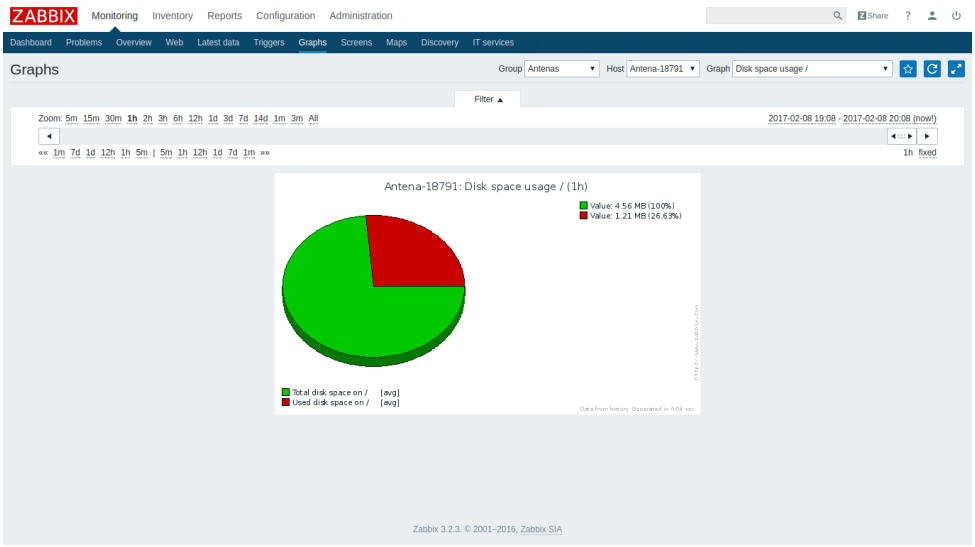


Figura 21: Visualização da utilização do espaço em disco no *access point*.

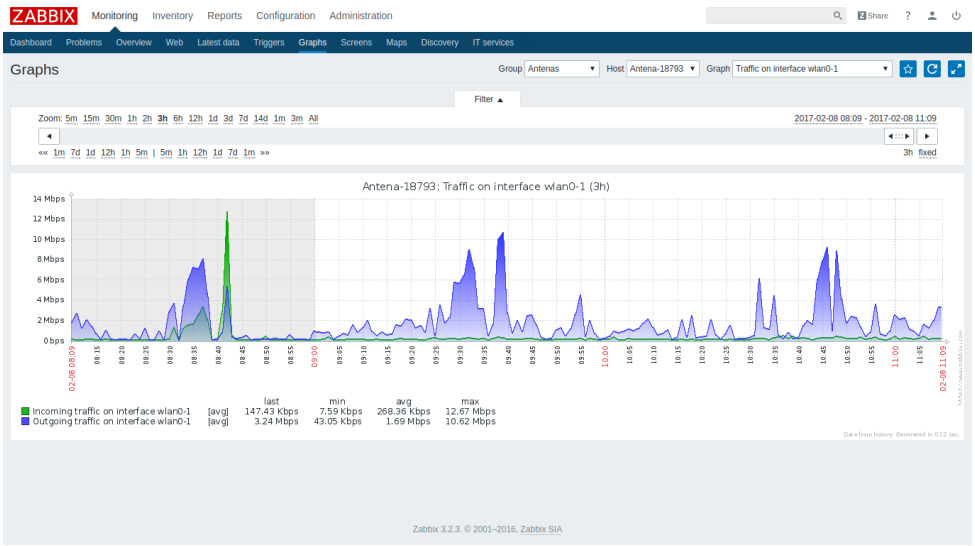


Figura 22: Visualização da utilização da interface de rede `wlan0` no *access point*.

O Zabbix permite obter informações customizadas através de alguns tipos de ferramentas. O mapeamento via Descoberta de baixo nível (*Low-level discovery* - LLD)[6] permite

[6]Vide: `https://www.zabbix.com/documentation/3.2/manual/discovery/low_level_discovery`.

criar automaticamente itens, gatilhos e gráficos para um cliente. A descoberta pode ser feita de diferentes maneiras, por exemplo, através de um agente zabbix instalado no cliente ou, como utilizado neste estudo, através do SNMP. Os dados são enviados do cliente para o servidor Zabbix no formato JSON e as regras de como interpretar estes dados são configuradas no servidor. A figura 23 a seguir mostra os dados customizados obtidos de um cliente OpenWrt.

```
{
"data":[
{"{#CLIIDX}":"1",  "{#CLIRX}":"26338",   "{#CLITX}":"56409",     "{#CLISIG}":"-83"},
{"{#CLIIDX}":"2",  "{#CLIRX}":"1456",    "{#CLITX}":"4073",      "{#CLISIG}":"-58"},
{"{#CLIIDX}":"3",  "{#CLIRX}":"36386",   "{#CLITX}":"82601",     "{#CLISIG}":"-78"},
{"{#CLIIDX}":"4",  "{#CLIRX}":"254628",  "{#CLITX}":"21605",     "{#CLISIG}":"-84"},
{"{#CLIIDX}":"5",  "{#CLIRX}":"81124",   "{#CLITX}":"1976093",   "{#CLISIG}":"-49"},
{"{#CLIIDX}":"6",  "{#CLIRX}":"53932",   "{#CLITX}":"46477",     "{#CLISIG}":"-74"},
{"{#CLIIDX}":"7",  "{#CLIRX}":"70553",   "{#CLITX}":"72170",     "{#CLISIG}":"-66"},
{"{#CLIIDX}":"8",  "{#CLIRX}":"173311",  "{#CLITX}":"296819",    "{#CLISIG}":"-38"},
{"{#CLIIDX}":"9",  "{#CLIRX}":"302547",  "{#CLITX}":"409732",    "{#CLISIG}":"-72"},
{"{#CLIIDX}":"10", "{#CLIRX}":"110249",  "{#CLITX}":"116864",    "{#CLISIG}":"-38"},
{"{#CLIIDX}":"11", "{#CLIRX}":"9006652", "{#CLITX}":"1518155",   "{#CLISIG}":"-74"},
{"{#CLIIDX}":"12", "{#CLIRX}":"2171232", "{#CLITX}":"11740895",  "{#CLISIG}":"-54"},
{"{#CLIIDX}":"13", "{#CLIRX}":"52856",   "{#CLITX}":"57511",     "{#CLISIG}":"-67"},
{"{#CLIIDX}":"14", "{#CLIRX}":"200166",  "{#CLITX}":"272985",    "{#CLISIG}":"-64"},
{"{#CLIIDX}":"15", "{#CLIRX}":"249581",  "{#CLITX}":"352524",    "{#CLISIG}":"-67"},
{"{#CLIIDX}":"16", "{#CLIRX}":"766924",  "{#CLITX}":"2161390",   "{#CLISIG}":"-79"},
{"{#CLIIDX}":"17", "{#CLIRX}":"3754927", "{#CLITX}":"108513525", "{#CLISIG}":"-55"},
{"{#CLIIDX}":"18", "{#CLIRX}":"1014936", "{#CLITX}":"1208160",   "{#CLISIG}":"-47"},
{"{#CLIIDX}":"19", "{#CLIRX}":"253980",  "{#CLITX}":"891468",    "{#CLISIG}":"-51"},
{"{#CLIIDX}":"20", "{#CLIRX}":"693554",  "{#CLITX}":"1645290",   "{#CLISIG}":"-47"}
]
}
```

Figura 23: Dados customizados enviados de um cliente OpenWrt em formato JSON.

As figuras 24 a 31 exibem capturas de tela contendo gráficos de monitoramento obtidos através do *script* implementado nos APs OpenWrt.

Os valores não numéricos monitorados pelo Zabbix podem ser visualizados por histórico ao invés de gráficos. A figura 28 mostra que duas interfaces sem fio, arbitrariamente denominadas “Wifi 1” e “Wifi 2”, estão atribuídas à mesma antena `radio0`.

A figura 29 mostra o SSID das duas redes associadas às interfaces Wifi 1 e 2.

A figura 30 mostra o protocolo de criptografia utilizado nas redes configuradas no ponto de acesso. `wpa2` indica “WPA2 Enterprise” e `psk-mixed` indica “WPA/WPA2 Personal (PSK) mixed mode” (OPENWRT, 2017a).

De maneira similar às interfaces, SSIDs e segurança, o monitoramento do BSSID tam-

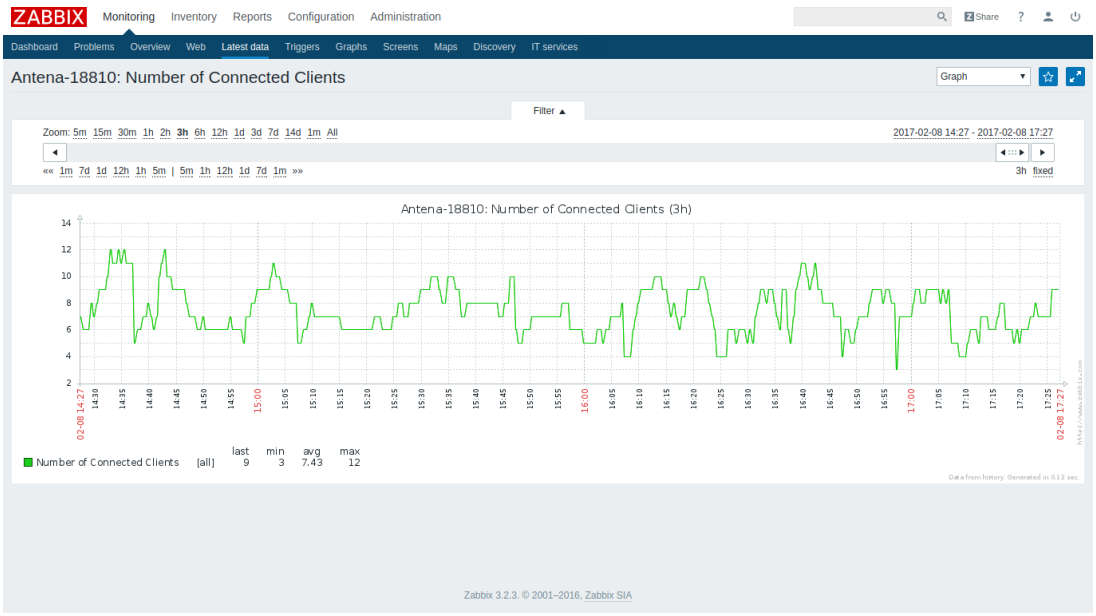


Figura 24: Número de clientes conectados no AP.

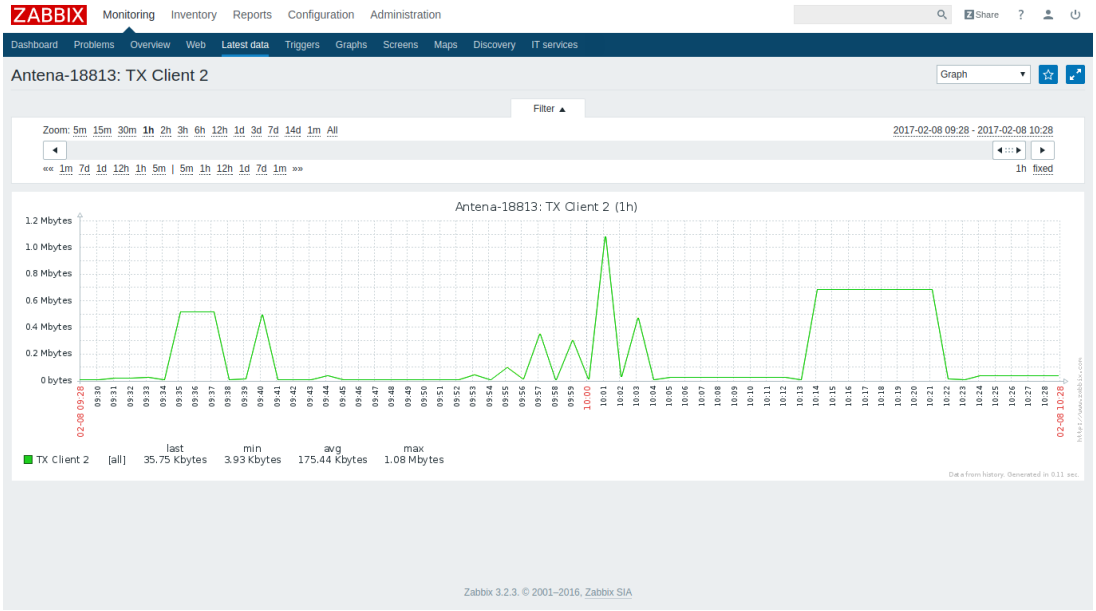


Figura 25: Número de *bytes* transmitidos por um cliente arbitrário conectado ao AP.

bém foi habilitado no Zabbix.

Por fim, a figura 31 mostra a frequência de operação do ponto de acesso. O dado é estático mas, como o valor é numérico, o Zabbix exibe seu histórico através de um gráfico onde a frequência assume um valor constante no tempo.

Este monitoramento ajuda a alcançar os principais objetivos do gerenciamento (PRAS, 1995):

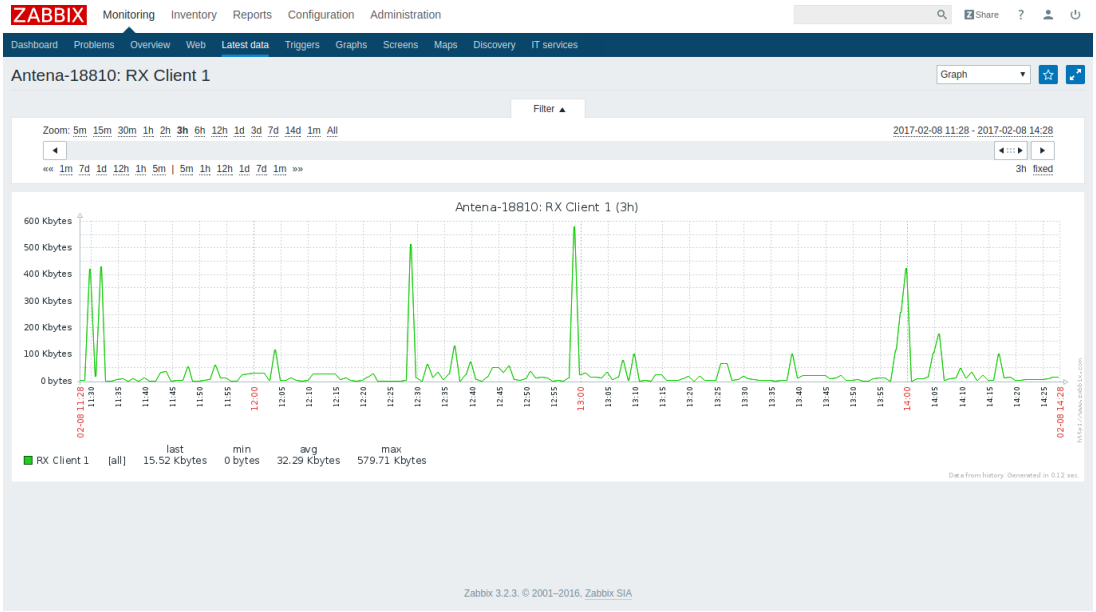


Figura 26: Número de *bytes* recebidos por um cliente arbitrário conectado ao AP.

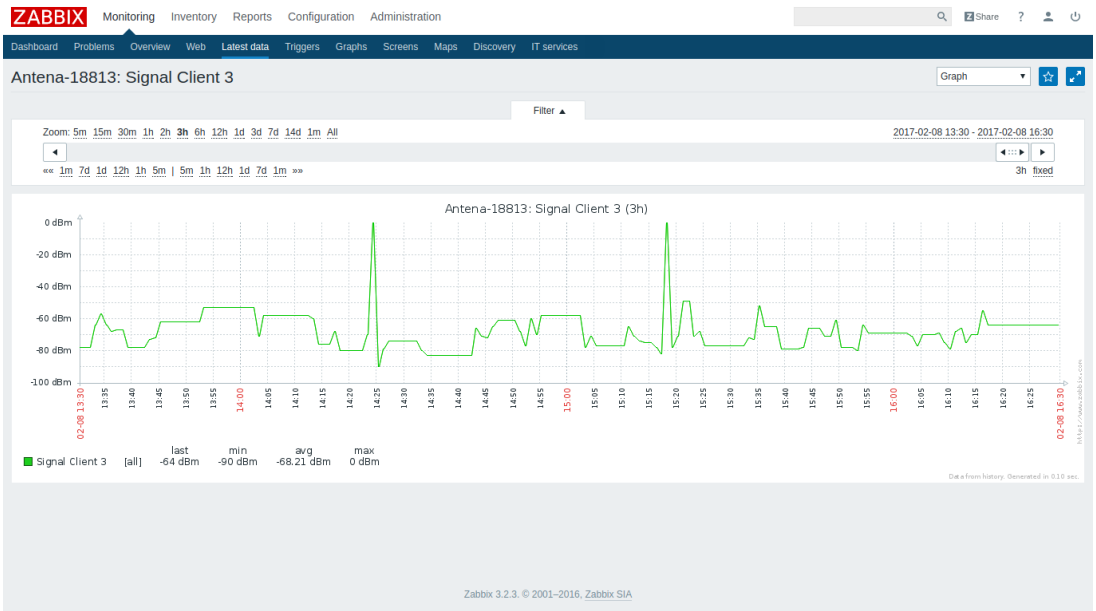


Figura 27: Potência do sinal medido em um cliente arbitrário conectado ao AP.

- Dimensionar a rede para atender o maior número de usuários potenciais, permitir estimar crescimento e projetar alterações. Isto pode ser realizado, por exemplo, acompanhando-se o número de usuários conectados, banda utilizada, estatísticas de uso e navegação. Sendo uteis para detectar gargalos e dimensionar a infraestrutura necessária.

- Tratamento de erros, para reduzir seus efeitos e permitir sua correção, por exemplo, através de alarmes e respostas automáticas.

- Monitorar o que acontece na rede, acompanhar o comportamento atual, compará-lo com

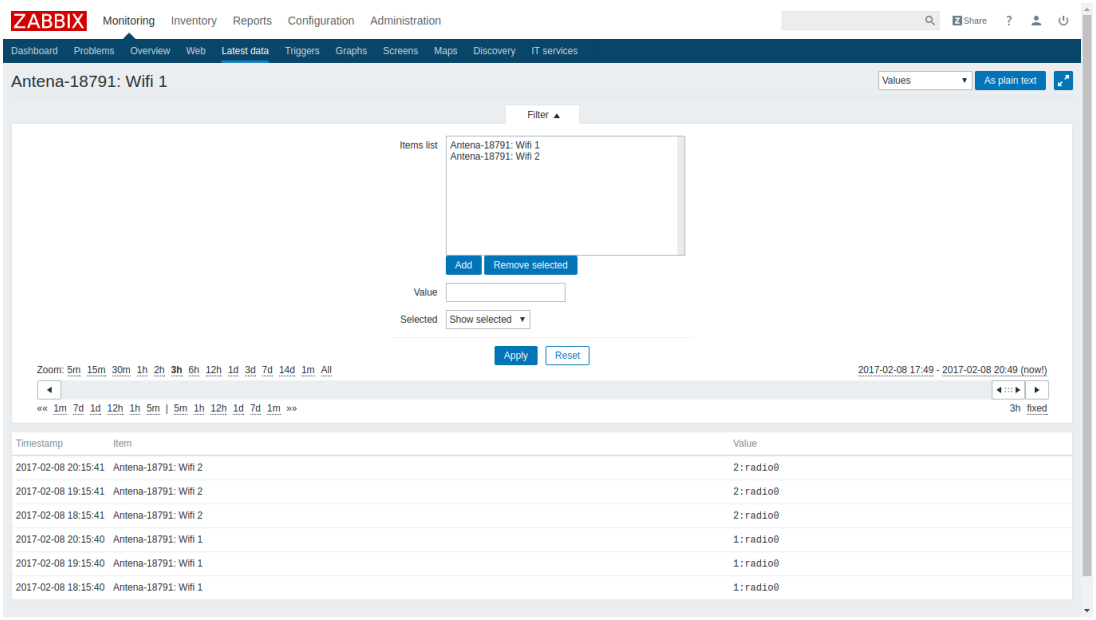


Figura 28: Antena associada às interfaces sem fio do AP.

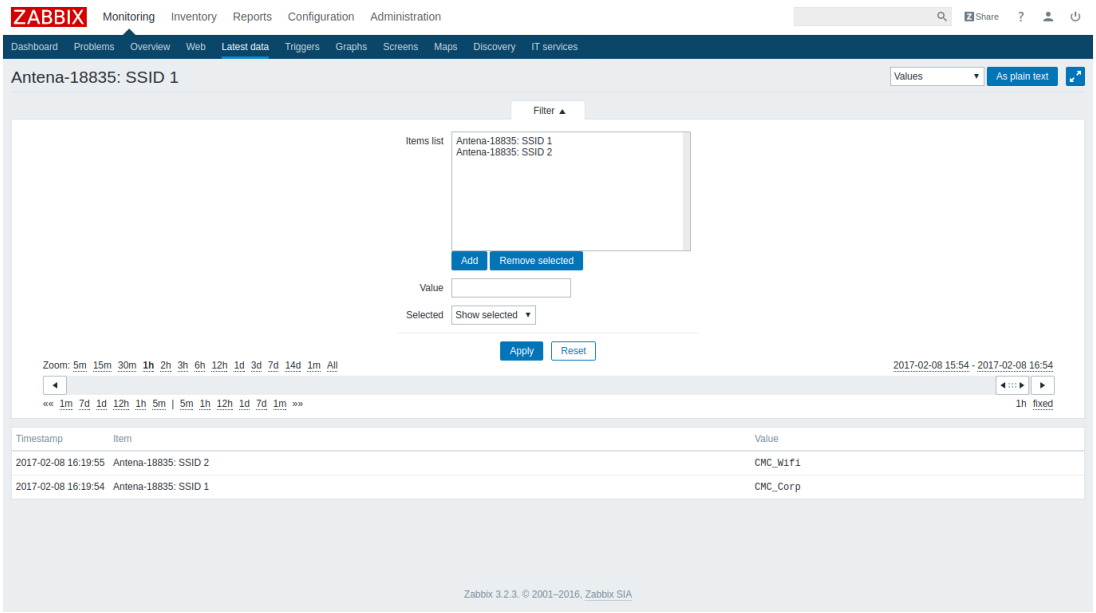


Figura 29: SSID das redes disponibilizadas pelo AP.

o comportamento no decorrer do tempo e com o esperado a fim de indicar anomalias. Os padrões de comportamento da rede e dos clientes podem ser excelentes indicativos.

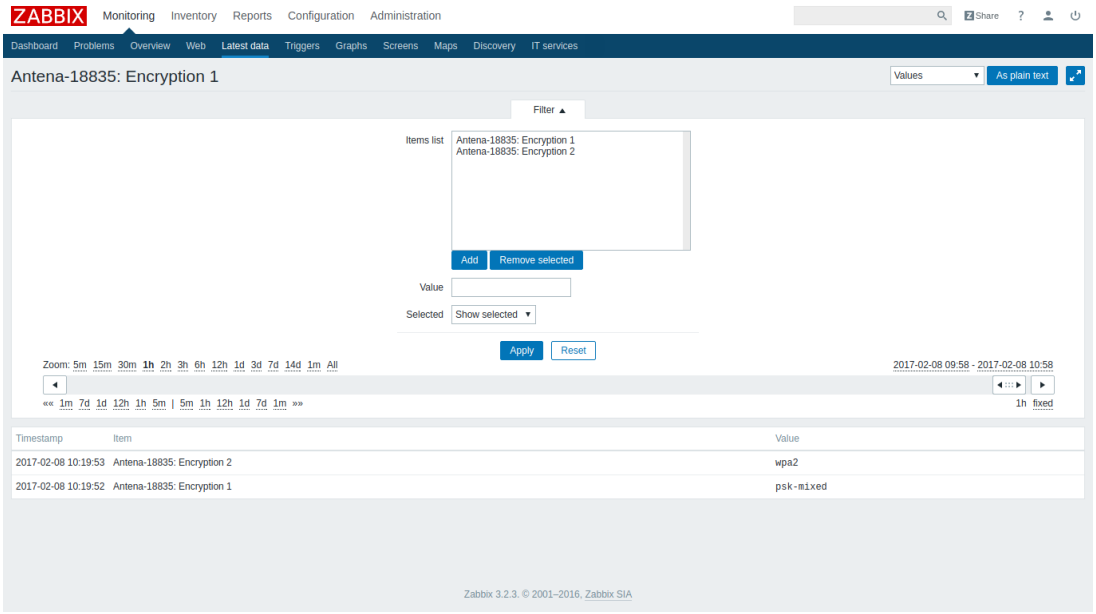


Figura 30: Tipo de segurança utilizada na rede.

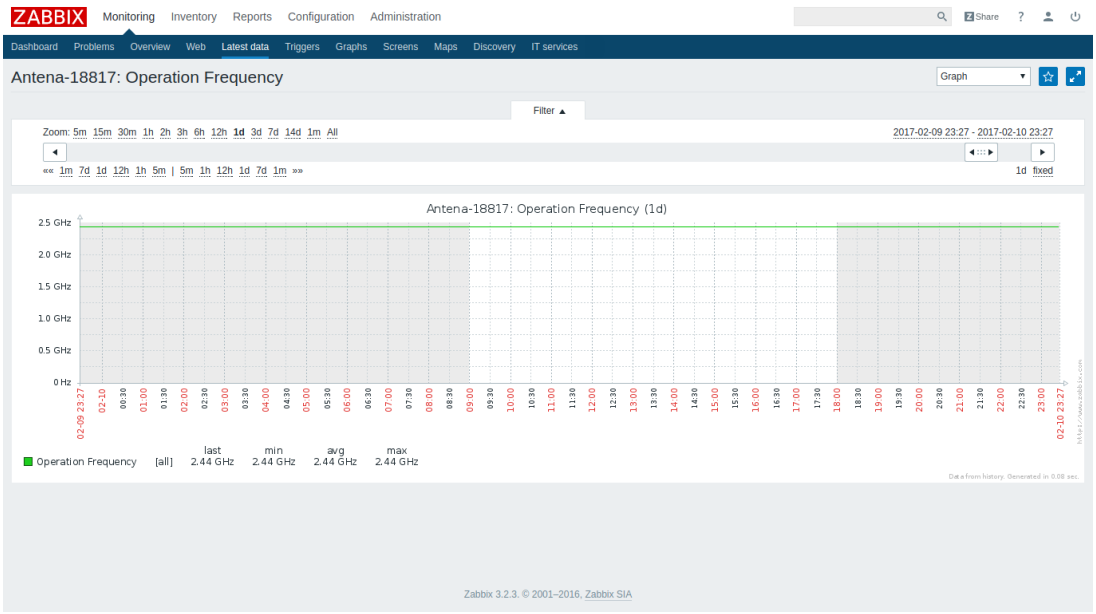


Figura 31: A frequência de operação, como esperado, não sofre alterações no tempo.

5 CONCLUSÃO

Conforme descrito na seção 4, a solução proposta neste trabalho foi implementada em um caso de uso real baseada na necessidade de uma empresa de gerenciamento e manutenção da qualidade do serviço de Internet sem fio oferecida a seus usuários/clientes. A utilização de pontos de acesso com o sistema operacional OpenWrt mostrou-se flexível tanto em termos de funcionalidades disponíveis para instalação, através dos pacotes da distribuição, quanto em recursos para coletar as informações customizadas almejadas.

Após a definição das informações a serem monitoradas, um *script* compatível com o *shell* do OpenWrt foi implementado para obtê-las. Para validar o caso de uso, o *software* Zabbix foi instalado e configurado para monitorar as informações customizadas dos pontos de acesso. A solução mostrou-se eficaz, de fácil implementação e gerenciamento, atendendo satisfatoriamente a proposta deste trabalho.

Para o administrador, a melhoria na qualidade do gerenciamento se deu pela possibilidade de obtenção de informações mais direcionadas e refinadas, tornada viável pela flexibilidade do OpenWrt. De maneira mais ampla, isto permite ao gestor melhor estimar as dimensões da rede, tratar e detectar erros e avaliar o comportamento da rede. Especificamente, o monitoramento dos clientes conectados aos pontos de acesso permite melhor dimensionamento dos APs, tanto em termos de capacidade de clientes conectados quanto em potência de sinal, acompanhamento do comportamento dos usuários e evitar gargalos. Um acompanhamento mais fino se dá também dos usuários em relação à rede em que estão associados, considerando mais de um BSSID disponível em um ponto de acesso. A partir destas análises, o administrador pode também definir métricas e *tresholds* e programar alarmes e respostas automáticas a eventos na rede.

A seguir são apresentados alguns possíveis futuros projetos baseados neste trabalho. Os dados customizados a serem gerenciados podem ser expandidos utilizando técnicas de monitoramento sem fio (JOHNSON, 2009), utilizando os APs como *sniffers* para captura e análise de pacotes. Baseadas no estudo realizado sobre a MIB 802.11 no OpenWrt, mais uma possível

linha de trabalho pode ser a implementação de alguns dos itens faltantes desta MIB. O que poderia vir a tornar-se uma importante contribuição ao projeto. Outra melhoria seria a criação de um *software* e a definição de interfaces, através do SNMP, em um dispositivo OpenWrt para recuperação de erros, tratamento de eventos ou execução de comandos. Isto permitiria por exemplo que, quando da detecção de problemas/eventos no monitoramento, um gatilho fosse disparado ativando a interface no dispositivo para tratar adequadamente o evento. Por fim, outra sugestão de melhoria seria o desenvolvimento de uma ferramenta de análise automática das informações obtidas no monitoramento, possivelmente permitindo a detecção de padrões, gargalos ou previsão de problemas. Nos moldes deste trabalho, isto permitiria, por exemplo, detectar abuso no uso da banda por parte de um dado usuário, constante aumento/queda no número de usuários conectados, crescente aumento no uso da banda indicando futuro gargalo, etc.

REFERÊNCIAS

CASE, J. et al. **A Simple Network Management Protocol**. [S.l.], 8 1988. RFC 1067. Disponível em: <http://tools.ietf.org/html/rfc1067>.

CISCO. **Voice over Wireless LAN 4.1 Design Guide**. Cisco Systems, Inc., 2010. Disponível em: <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg-/vowlan41dg-book.html>.

CISCO. **Cisco SNMP Object Navigator**. 2015. Disponível em: <http://tools.cisco.com-/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9-.9.13.3.0.1>.

CISCO, S. **Internetworking Technologies Handbook**. [S.l.]: Cisco Press, 2004. (Cisco Press networking technology series). ISBN 9781587051197.

DIAS, D. de S.; SILVA, M. F. da. **Como Escrever uma Monografia**. [S.l.]: COPPEAD, 2009. ISBN 9788575080719.

FON. **Fon Network**. Fon Wireless, Ltd., 2015. Disponível em: <http://corp.fon.com/>.

GAST, M. S. **802.11 Wireless Networks: The Definitive Guide**. 2nd. ed. [S.l.]: O'Reilly Media, 2005. ISBN 0596100523.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. [S.l.]: Editora Atlas, 2002. ISBN 8522431698.

HARRINGTON, D.; PRESUHN, R.; B., W. **An Architecture for Describing SNMP Management Frameworks**. [S.l.], 1 1998. RFC 2271. Disponível em: <http://tools.ietf.org/html-/rfc2271>.

IANA. **PRIVATE ENTERPRISE NUMBERS**. Internet Assigned Numbers Authority, 2015. Disponível em: <http://www.iana.org/assignments/enterprise-numbers>.

JOHNSON, R. B. **Evaluating the use of SNMP as a Wireless Network Monitoring Tool for IEEE 802.11 Wireless Networks**. Dissertação (Mestrado) — Clemson University, 5 2009.

KHAN, A. K. J. **Building Secure Wireless Networks with 802.11**. 1st. ed. [S.l.]: Wiley, 2003. ISBN 0471237159.

LESKIW, A. **SNMP Basics: What is SNMP & How Do I Use It?** 2017. Disponível em: <http://www.networkmanagementsoftware.com/snmp-tutorial/>.

LI, H.; CHEN, G. Wireless LAN network management system. In: **Industrial Electronics, 2004 IEEE International Symposium on**. [S.l.: s.n.], 2004. v. 1, p. 615–620.

MARTIN, A.; LEON, C.; LÓPEZ, A. An intelligent approach to an efficient internet network management. In: **ICN 2013: The Twelfth International Conference on Networks**. Seville, Spain: [s.n.], 2013. p. 101–106.

MAURO, D. R.; SCHMIDT, K. J. **Essential SNMP**. 2nd. ed. [S.l.]: O'Reilly Media, 2005. ISBN 0596008406.

MCCLOGHRIE, K.; ROSE, M. **Management Information Base for Network Management of TCP/IP-based internets: MIB-II**. [S.l.], 3 1991. RFC 1213. Disponível em: <http://tools-.ietf.org/html/rfc1213>.

MORREALE, P. A.; TERPLAN, K. **CRC Handbook of Modern Telecommunications**. 2nd. ed. [S.l.]: CRC Press, 2009. ISBN 1420078003.

NET-SNMP. **Net-SNMP**. 2016. Disponível em: <http://www.net-snmp.org/>.

NIC.BR. **Introdução ao Gerenciamento de Redes - parte 4 - SNMP**. 2014. Disponível em: <http://www.youtube.com/watch?v=PqgDoG4gLK0>.

OPENWRT. **Wireless overview**. 2014. Disponível em: <https://wiki.openwrt.org/doc/howto-/wireless.overview>.

OPENWRT. **Command-line interpreter**. 2016. Disponível em: <https://wiki.openwrt.org-/doc/howto/user.beginner.cli>.

OPENWRT. **OpenWrt Wireless Freedom**. 2016. Disponível em: <http://openwrt.org/>.

OPENWRT. **Wireless configuration**. 2017. Disponível em: <https://wiki.openwrt.org/doc/uci-/wireless>.

OPENWRT. **Wireless Utilities**. 2017. Disponível em: <https://wiki.openwrt.org/doc/howto-/wireless.utilities>.

PEIXOTO, J. C. **Implementação e Gerência de uma Arquitetura de Voz sobre IP**. 167 p. Dissertação (Mestrado) — Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil, 2003.

POTTER, B. F. B. **802.11 Security**. [S.l.]: O'Reilly Media, 2002. ISBN 0596002904.

PRAS, A. **Network Management Architectures**. Tese (Doutorado) — University of Twente, Enschede, The Netherlands, 1995.

STALLINGS, W. Security comes to SNMP: The new SNMPv3 proposed internet standards. **The Internet Protocol Journal**, Cisco News Publications Group, v. 1, n. 3, p. 2–12, 1998.

STALLINGS, W. SNMPv3: A security enhancement to SNMP. **IEEE Communications Surveys and Tutorials**, v. 1, n. 1, p. 2–17, 1998.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks**. 5th. ed. [S.l.]: Pearson, 2010. ISBN 0132126958.

WNDW; BUTLER, J. S. **Wireless Networking in the Developing World**. 3rd. ed. CreateSpace Independent Publishing Platform, 2013. ISBN 9781484039359. Disponível em: <http://wndw-.net>.

ZELTSERMAN, D. **Practical Guide to SNMPv3 and Network Management**. [S.l.]: Prentice Hall PTR (ECS Professional), 1999. 352 p. ISBN 0130214531.