



## **SciFi – Sistema de Controle Inteligente para Redes sem Fio**

### **Manual do Controlador V2**

Autores: Helga Dolorico Balbi, Felipe Rolim e Souza, Ricardo Campanha Carrano, Luiz Claudio Schara Magalhães, Célio Vinicius Neves de Albuquerque, Débora Christina Muchaluat Saade, Luiza Ribas do Nascimento, Caio Gagliano.

Outubro/2013

## Índice

1.	Controlador SciFi .....	6
1.1.	Arquitetura de software.....	7
1.1.1.	Subsistema do Controlador Central .....	8
1.1.1.1.	Núcleo de Processamento Central .....	8
1.1.1.2.	Banco de Dados.....	10
1.1.1.3.	Interface Web.....	11
1.1.2.	Subsistema dos pontos de acesso.....	12
1.2.	Algoritmos utilizados pelo Núcleo de Processamento central .....	13
1.2.1.	Algoritmo de Seleção de canal .....	13
1.2.2.	Algoritmo de Controle de Potência.....	14
2.	Instalando e configurando o sistema operacional .....	15
2.1.	Configurando o dnsmasq .....	17
2.2.	Configurando o syslog para receber logs dos APs.....	19
2.3.	Configurando o ntpd .....	20
2.4.	Configurando o servidor SSH.....	22
2.5.	Configurando o Firewall .....	24
3.	Instalando OpenWrt nos Pontos de Acesso .....	28
3.1.	Fazendo <i>Download</i> da imagem OpenWrt .....	29
3.2.	Instalação do OpenWrt .....	30
3.2.1.	Exemplos de instalação de imagem OpenWrt via interface Web.....	30
3.2.2.	Exemplos de instalação de imagem OpenWrt via <i>tftp</i> .....	32
3.3.	Configuração do OpenWrt .....	33
3.3.1.	Configuração utilizando pacote de configuração automática .....	34
3.3.1.1.	Instalando programas sshpass e expect.....	35
3.3.1.2.	Gerando par de chaves pública e privada .....	35
3.3.1.3.	Configurando o script config.sh .....	37
3.3.1.4.	Executando o script config.sh.....	38
3.3.2.	Configuração sem utilização do pacote de configuração automática .....	40
3.3.2.1.	Configuração da rede sem fio (wireless).....	40
3.3.2.2.	Configuração Network .....	41
3.3.2.3.	Instalação dos pacotes necessários.....	42
3.3.2.4.	Instalação dos scripts SciFi .....	44
3.3.2.5.	Instalação da chave SSH pública .....	44
3.3.2.6.	Configuração do SNMMP .....	44
3.3.2.7.	Configuração do system .....	46
3.3.2.8.	Configuração do rc.local.....	47
3.3.2.9.	Configuração do dropbear .....	47
4.	Instalando e configurando o Controlador SciFi .....	47

4.1.	Banco de dados PostgreSQL.....	48
4.1.1.	Instalando o banco de dados PostgreSQL.....	48
4.1.2.	Configurando o banco de dados PostgreSQL.....	49
4.2.	Servidor de aplicações JBoss .....	57
4.2.1.	Instalando o JDK .....	57
4.2.2.	Instalando o JBoss AS .....	57
4.2.3.	Criação de usuário para inicialização do JBossAS.....	57
4.2.4.	Testando a inicialização do JBoss AS .....	59
4.3.	Interface web do SciFi .....	61
4.3.1.	Instalando o driver JDBC para acesso ao banco de dados .....	61
4.3.2.	Configurando a conexão do JBoss com o banco de dados Postgresql.....	62
4.3.3.	Configurando o HTTPS no JBoss AS utilizando keytool .....	64
4.3.4.	Instalando a interface Web do SciFi.....	65
4.4.	Instalando o Núcleo de Processamento Central do SciFi.....	68
5.	Utilizando a Interface Web de gerência do SciFi.....	70
5.1.	Acessando a interface Web do controlador.....	71
5.2.	Adicionando/Removendo regiões de controle .....	72
5.3.	Adicionando um novo ponto de Acesso controlado .....	73
5.4.	Visualizando informações e removendo pontos de acesso controlados .....	77
5.5.	Editando informações dos pontos de acesso controlados.....	81
5.6.	Executando comandos do controlador .....	83
5.7.	Editando parâmetros de execução do controlador .....	84
5.8.	Acessando a página de monitoramento .....	87
5.9.	Alterando a senha de acesso à interface Web.....	88
5.10.	Criando/alterando usuário de acesso à interface Web.....	89

## Índice de Figuras

Figura 1 - Exemplo de rede sem fio controlada pelo SciFi .....	6
Figura 2 - Arquitetura do Controlador.....	7
Figura 3 - Estrutura do banco de dados .....	10
Figura 4 - Estrutura da Interface Web do Controlador .....	12
Figura 5 - Firewall Builder: Alterando IPs das interfaces.....	24
Figura 6 - Firewall Builder: Configurando a subrede dos APs e WIFI .....	25
Figura 7 - Firewall Builder: Alterando a porta que será liberada para o SSH.....	26
Figura 8 - Firewall Builder: Compilando o firewall .....	27
Figura 9 - Firewall Builder: Firewall compilado com sucesso.....	27
Figura 10 - Atualização de firmware do ponto de acesso TP-Link WR841N v8.....	31
Figura 11 - Atualização de firmware do ponto de acesso NanoStation Loco M2. ....	32
Figura 12 - PgAdmin III – Adicionando conexão com o banco de dados.....	50
Figura 13 - PgAdmin III - Preenchendo as propriedades da conexão.....	51
Figura 14 - PgAdmin III - Criando um Login Role .....	52
Figura 15 - PgAdmin III - Criando usuário controlador.....	52
Figura 16 - PgAdmin III - Alterando definições do usuário controlador.....	53
Figura 17 - PgAdmin III - Configurando privilégios do usuário controlador.....	53
Figura 18 - PgAdmin III - Criando novo banco de dados. ....	54
Figura 19 - PgAdmin III - Definindo dono do novo banco de dados.....	54
Figura 20 - PgAdmin III - Definições do novo banco de dados.....	55
Figura 21 - PgAdmin III - Restaurando o banco de dados. ....	55
Figura 22 - PgAdmin III - Restaurando o banco de dados (2) .....	56
Figura 23 - PgAdmin III - Banco restaurado com sucesso.....	56
Figura 24 - Bem Vindo ao JBoss AS 7.....	61
Figura 25 - JBoss: Interface de administração do JBoss .....	66
Figura 26 - JBoss: Instalando a interface web do SciFi .....	67
Figura 27 - JBoss: Selecionar arquivo .....	67
Figura 28 - JBoss: Salvar configurações .....	67
Figura 29 - JBoss: Habilitar interface web do SciFi .....	68
Figura 30 - JBoss: Confirmar habilitação da interface web .....	68
Figura 31 - Acesso à interface Web do controlador SciFi.....	71
Figura 32 - Página inicial da seção de administração .....	72
Figura 33 - Adicionando região de controle .....	72
Figura 34 - Adicionando região de controle (2).....	73
Figura 35 - Removendo Região de Controle.....	73
Figura 36 - Marcando posição no mapa como <i>default</i> .....	73
Figura 37 - Cadastrando novo AP para controle utilizando o mapa.....	74
Figura 38 - Cadastrando novo AP para controle utilizando o mapa (2) .....	74
Figura 39 - Acessando a subseção para adição de novos APs controlados.....	74
Figura 40 - Página para adição de um novo ponto de acesso controlado .....	75
Figura 41 - Acesso às informações do AP via mapa .....	77
Figura 42 - Lista de APs visualizada a partir do mapa .....	78
Figura 43 - Acessando a subseção para visualização dos pontos de acesso.....	78
Figura 44 - Página para visualização dos pontos de acesso controlados .....	79

Figura 45 - Confirmando a exclusão de um ponto de acesso. ....	79
Figura 46 - Pontos de acesso desabilitado .....	80
Figura 47 - Ponto de acesso sem conexão com o controlador .....	80
Figura 48 - Acessando a subseção para edição das informações dos APs. ....	81
Figura 49 - Página de edição das informações dos pontos de acesso controlados .....	82
Figura 50 - Acessando página de edição do AP via mapa .....	82
Figura 51 - Página de edição individual das configurações de um AP .....	83
Figura 52 - Executando comandos do controlador .....	83
Figura 53 - Acessando a subseção para edição de parâmetros do controlador. ....	84
Figura 54 - Página de edição dos parâmetros de execução do controlador .....	85
Figura 55 - Acesso à página de monitoramento dos APs .....	87
Figura 56 - Exemplo de ferramenta para monitoramento.....	88

## 1. Controlador SciFi

O controlador SciFi é um sistema capaz de operar em redes de comunicação sem fio 802.11 b, g e n infra-estruturadas, compostas por dispositivos de diversas marcas e de baixo custo. Sua principal função é minimizar a interferência entre pontos de acesso (APs, do inglês *Access Points*) vizinhos. Para realizar essa tarefa, o controlador utiliza duas técnicas, que são: (1) seleção do canal de operação dos APs pertencentes à rede; (2) controle de potência de transmissão dos APs. Estas duas técnicas serão abordadas com mais detalhes nas seções 1.2.1 e 1.2.2, respectivamente.

A Figura 1 mostra a arquitetura de rede utilizada pelo sistema SciFi, que se assemelha a uma rede infraestruturada. Os quatro dispositivos básicos que compõe esta rede são:

- (1) pontos de acesso de baixo custo, capazes de operar com o sistema operacional embarcado de código aberto OpenWrt;
- (2) um controlador central (PC), que possuirá a visão da rede como um todo e definirá quais os melhores canais e potências de transmissão a serem utilizados pelos pontos de acesso;
- (3) um switch (ou uma rede de camada 2) que interliga os pontos de acesso e o controlador central através da rede cabeadas, possibilitando a comunicação entre eles;
- (4) clientes sem fio que acessam a rede através dos pontos de acesso;

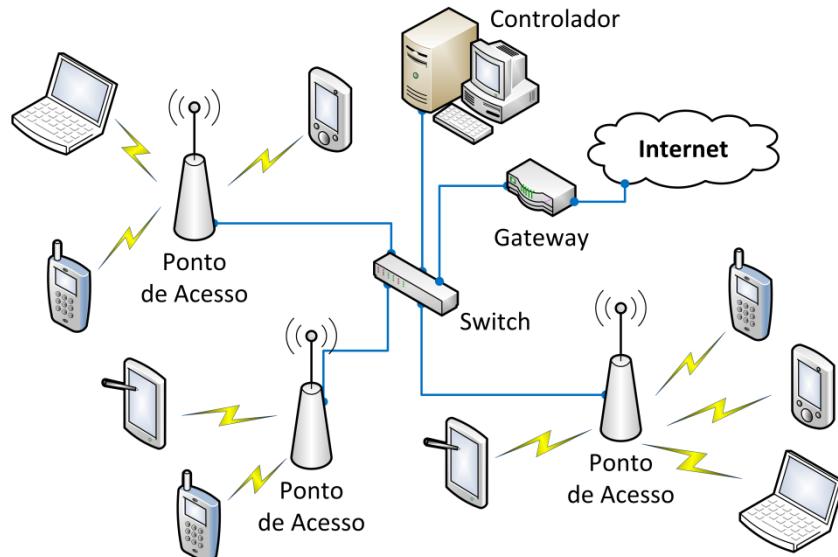


Figura 1 - Exemplo de rede sem fio controlada pelo SciFi

Nesta arquitetura, se for desejado, o controlador central também poderá atuar como Gateway da rede sem fio, oferecendo serviços de DHCP e NAT. Para fornecer estas duas funcionalidades, o controlador necessitará de duas interfaces de rede, uma interligada à rede interna (rede dos APs) e outra à rede externa (representada pela Internet na Figura 1). Retirar o serviço de DHCP do AP e impletá-lo no gateway possibilita que o usuário (estaçõa

associada) mantenha seu IP no momento em que realizar *roaming* entre os APs da rede. Para que o *roaming* ocorra, também é necessário que os APs possuam o mesmo SSID.

A próxima Seção (1.1) apresenta com detalhes a arquitetura de *software* do controlador SciFi.

### 1.1. Arquitetura de software

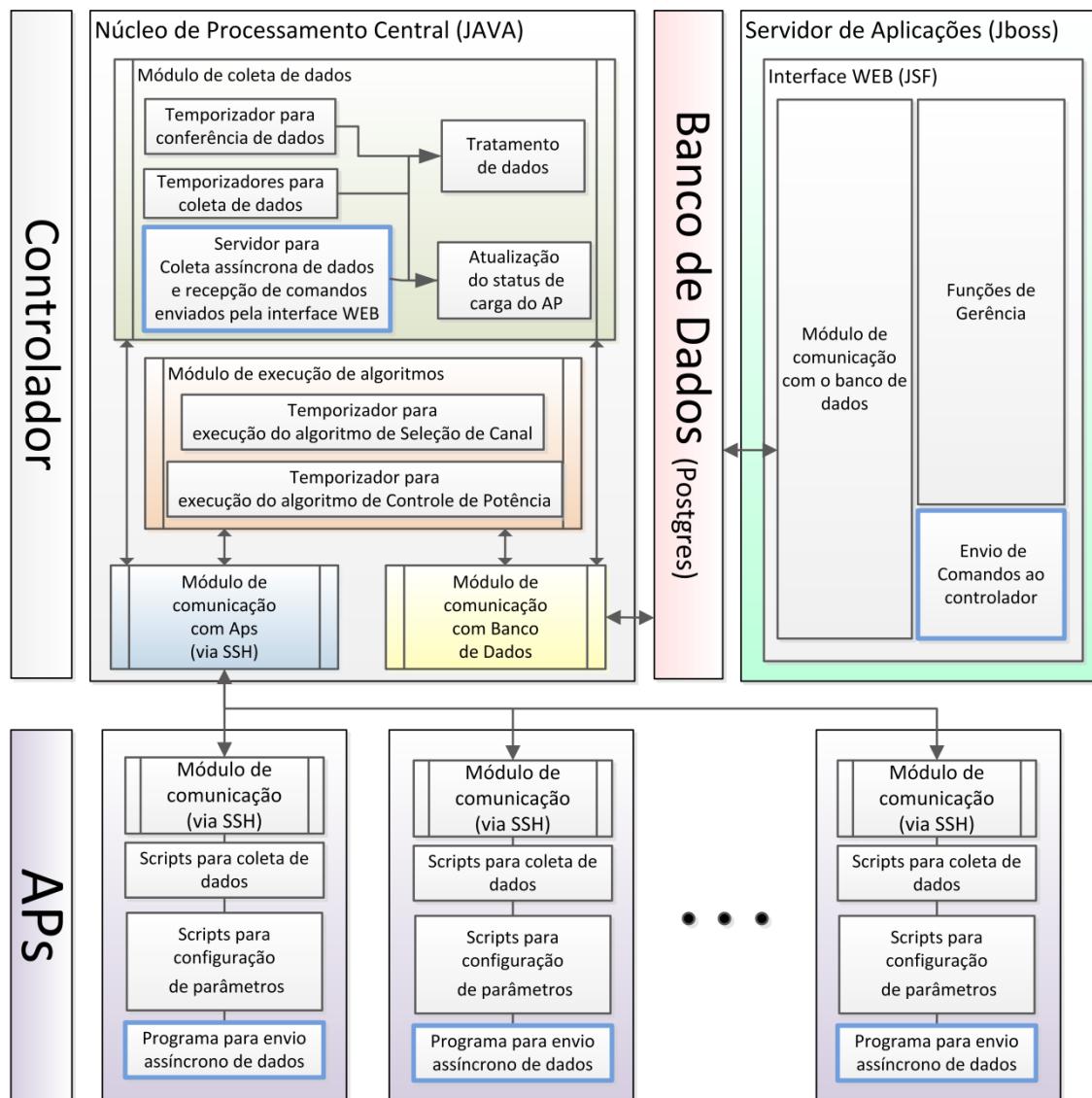


Figura 2 - Arquitetura do Controlador

A arquitetura do *software* do controlador SciFi, é apresentada na Figura 2. Nesta figura, pode-se observar que parte do sistema opera no controlador central (parte superior da figura), e outra parte opera nos pontos de acesso (parte inferior da figura). Esses subsistemas serão apresentados nas seções a seguir.

### **1.1.1. Subsistema do Controlador Central**

O subsistema que opera no Controlador Central se subdivide em três partes principais: Núcleo de Processamento Central, Banco de Dados e Interface Web. Cada uma delas será detalhada nas próximas seções.

#### **1.1.1.1. Núcleo de Processamento Central**

O Núcleo de Processamento Central é responsável pela definição dos parâmetros de canal e potência utilizados pelos pontos de acesso e se subdivide em quatro módulos: Módulo de Coleta de Dados, Módulo de Execução de Algoritmos, Módulo de Comunicação com o Banco de Dados e Módulo de Comunicação com APs.

O Módulo de Coleta de Dados contém os Temporizadores para Coleta de Dados, que agendam a execução dos *scripts* de coleta de dados instalados em cada ponto de acesso controlado. Os intervalos de tempo entre execuções das coletas podem ser definidos pelo administrador da rede através da interface web do controlador, como mostra a Seção 5.6. Basicamente, três tipos de dados são coletados: informações de *scan*, informações de *station dump*, e informações sobre as configurações de canal e potência dos pontos de acesso.

O processo de *scan* é a execução da varredura espectral no ponto de acesso. Através desta varredura, quadros de *beacon*, contendo informações relativas ao sinal proveniente de pontos de acessos vizinhos, são coletados. Estas informações são utilizadas pelos algoritmos de seleção de canal e controle de potência para a realização do cálculo da interferência entre os pontos de acesso. O processo de varredura espectral é realizado de forma sequencial em cada ponto de acesso, permitindo que, enquanto um ponto de acesso execute o *scan*, os outros operem normalmente e enviem quadros de *beacon* em seu canal de operação. Após a realização da coleta, os dados são tratados pelo controlador e inseridos no banco de dados.

Tendo em vista que os dados reportados pelo *scan* podem sofrer alterações abruptas devido a certas alterações no ambiente, para amenizar a influência de fatos isolados, o controlador realiza a ponderação dos valores de potência de sinal e qualidade antes de armazená-los no banco de dados. O valor armazenado é resultado de uma média ponderada, na qual os valores mais antigos de potência de sinal e qualidade possuem um peso na definição do novo valor. Esse peso pode ser definido pelo administrador da rede através da interface web do controlador, como mostra a Seção 5.6.

Outro tipo de informação coletada pelo controlador central é a obtida através do processo conhecido por *station dump*. Esta informação revela o número de usuários associados a cada ponto de acesso controlado e é utilizada pelo algoritmo de seleção de canal. Sua coleta é realizada paralelamente em cada ponto de acesso e, após sua realização, os dados são tratados pelo controlador e as informações sobre o status de carga do AP e clientes associados são atualizadas no banco de dados.

Buscando a coleta de informações assíncronas que poderiam ser enviadas por um AP, foi criado o submódulo de Coleta Assíncrona de Dados. Este submódulo é dividido em duas aplicações, uma que opera no controlador (servidor), e outra que opera no ponto de acesso

(cliente). O *software* cliente pode ser programado para enviar mensagens assíncronas para o servidor, como por exemplo, informação sobre uma nova estação associada, ou outra informação desejada. O servidor deve ser programado para fazer o tratamento dos dados e armazenar as informações obtidas no banco de dados. Atualmente, este módulo está em fase de testes e será disponibilizado em breve.

O mesmo servidor implementado no submódulo de Coleta Assíncrona de Dados também é utilizado para receber mensagens enviadas a partir da interface Web de gerência do controlador SciFi. Estas mensagens podem ordenar que o controlador execute determinada rotina, como a coleta de dados ou a execução de algoritmos.

Para conferir se as informações contidas no banco de dados sobre canal de operação e potência de transmissão dos pontos de acesso estão corretas, o controlador realiza um processo denominado “*check de sanidade*”. Neste processo, informações sobre o canal de operação e potência de transmissão de cada AP são coletadas e comparadas com as guardadas no banco de dados. Caso alguma delas esteja incorreta, o controlador ordena reconfiguração do ponto de acesso com a informação contida no banco de dados. A conferência de dados é executada paralelamente nos pontos de acesso com intervalo de tempo definido através da Interface Web.

O segundo módulo do Núcleo de Processamento Central é o Módulo de Execução de Algoritmos. Este módulo contém os Temporizadores para Execução de Algoritmos, que agenda a execução dos algoritmos de seleção de canal e controle de potência de cada ponto de acesso controlado. Os intervalos de tempo entre execuções desses algoritmos podem ser definidos pelo administrador da rede através da interface web do controlador, como mostra a Seção 5.6. Mais detalhes sobre eles serão apresentados nas seções 1.2.1 e 1.2.2, respectivamente.

As informações necessárias para a execução dos algoritmos, como a lista de APs controlados, dados de *scan* e *station dump*, são buscadas no banco de dados através do Módulo de Comunicação com o Banco de Dados. Após a configuração dos canais de operação e potência dos pontos de acesso, o banco de dados é atualizado com as novas informações.

A comunicação entre o controlador e os pontos de acesso é realizada através do Módulo de Comunicação, que utiliza o protocolo SSH (*Secure Shell*) para a criação de um canal seguro para troca de dados entre os dispositivos. Para estabelecer o canal seguro, o controlador deve se conectar ao ponto de acesso e, a seguir, poderá copiar arquivos de dados dos pontos de acesso ou ordenar que executem *scripts* de coleta de dados ou configuração de parâmetros.

Para prover maior escalabilidade do sistema, os pontos de acesso controlados podem ser divididos em regiões de controle. Para cada região, o controlador irá iniciar uma instância de controle que executará os temporizadores de coleta de dados e execução dos algoritmos de forma independente. Os pontos de acesso devem ser distribuídos entre as regiões de acordo com suas posições geográficas de forma que, aqueles que tenham proximidade física e que possam vir a se interferir, devem ser cadastrados na mesma região de controle.

### 1.1.1.2. Banco de Dados

O banco de dados utilizado pelo controlador SciFi, cuja estrutura é apresentada na Figura 3, armazena informações sobre os pontos de acesso controlados, regiões de controle, dados coletados dos APs e parâmetros de execução do controlador. Nesta figura, cada bloco representa uma tabela que armazena determinado tipo de informação. O banco de dados contém sete tabelas ao total, que são:

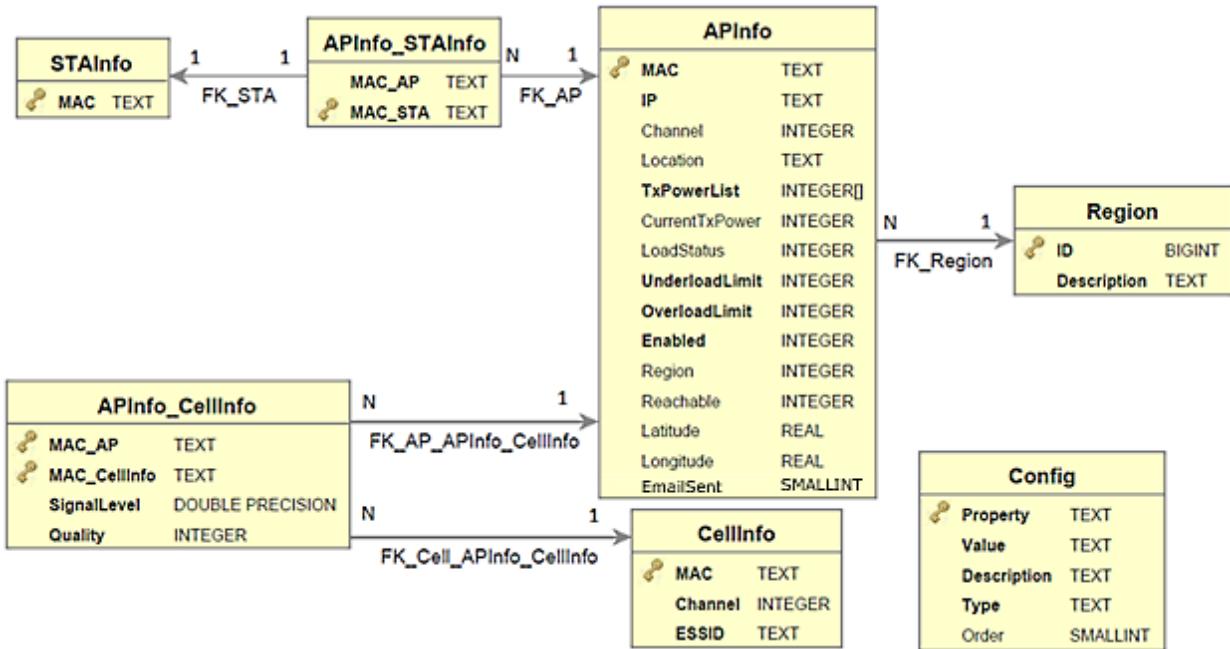


Figura 3 - Estrutura do banco de dados

- 1) APInfo – Tabela que armazena informações dos pontos de acesso. Cada linha desta tabela representa um AP e suas colunas armazenam, respectivamente, endereço MAC do AP, endereço IP, canal (Channel), localização (Location), lista de possíveis potências de transmissão (TxPowerList), potência de transmissão atual (CurrentTxPower), status de carga (LoadStatus), limiar de carga baixa (UnderloadLimit), limiar de sobrecarga (OverloadLimit), indicador de habilitação do AP para controle (Enabled), identificação da região de controle do AP (Region), indicador de conectividade via cabo entre AP e controlador (Reachable), latitude, longitude e indicador de envio de email (EmailSent). Os limiares de carga são utilizados na determinação do status de carga do ponto de acesso e o indicador de envio de email é utilizado para indicar se um email já foi enviado ao administrador do sistema informando problemas que possam estar ocorrendo com o AP.
- 2) CellInfo – Tabela que armazena, em cada linha, informações sobre os pontos de acesso vizinhos aos APs da rede controlada, ou seja, pontos de acesso que possam vir a causar interferência. Suas colunas armazenam, respectivamente, endereço MAC, Canal (Channel) e ESSID de um AP vizinho. Estas informações são obtidas através da execução da varredura espectral nos APs controlados.

- 3) APIInfo\_CellInfo – Tabela que armazena a relação entre um ponto de acesso controlado e outro ponto de acesso, controlado ou não, que esteja armazenado na tabela CellInfo. Cada linha desta tabela indica qual AP (inserido na tabela APIInfo) é capaz de receber sinal de outro AP (inserido na tabela CellInfo). Suas colunas armazenam, respectivamente, o endereço MAC do AP controlado (MAC\_AP), o endereço MAC do AP interferente (MAC\_CellInfo), o nível de sinal recebido (SignalLevel) e sua qualidade (Quality).
  
- 4) STAInfo – Tabela que armazena informações sobre os clientes associados aos pontos de acesso controlados. Cada linha desta tabela contém um endereço MAC de uma estação associada.
  
- 5) APIInfo\_STAInfo - Tabela que armazena a relação entre um ponto de acesso controlado e um cliente associado. Cada linha desta tabela indica qual estação (STAInfo) está associada a qual AP (APIInfo). Suas colunas armazenam, respectivamente, o endereço MAC do AP (MAC\_AP) e da estação (MAC\_STA).
  
- 6) Config – Tabela que armazena parâmetros de execução do controlador. Cada linha desta tabela representa um parâmetro. Suas colunas armazenam, respectivamente, o nome do parâmetro (Property), seu valor (Value), sua descrição (Description), o tipo do dado (Type) e sua ordem de exibição na página web (Order).
  
- 7) Region – Tabela que armazena informações sobre as regiões de controle. Cada linha desta tabela representa uma região. Suas colunas armazenam, respectivamente, o número de identificação da região (ID) e o nome da região (Description).

#### **1.1.1.3. Interface Web**

A interface WEB do controlador, cuja estrutura é apresentada na Figura 4, permite que o administrador da rede obtenha e modifique informações relacionadas ao controlador. Como apresentado na figura, a página inicial da interface Web dá acesso à área de administração do controlador, que requer o fornecimento de *login* e senha. Quando devidamente autenticado, o administrador ganha acesso às páginas de visualização e edição de APs, páginas de edição das regiões de controle, página de configuração dos parâmetros de execução do controlador, página de execução de comandos do controlador, e página de monitoramento (estatísticas) dos APs e servidor. Mais detalhes sobre utilização da interface Web serão apresentados na seção 5.

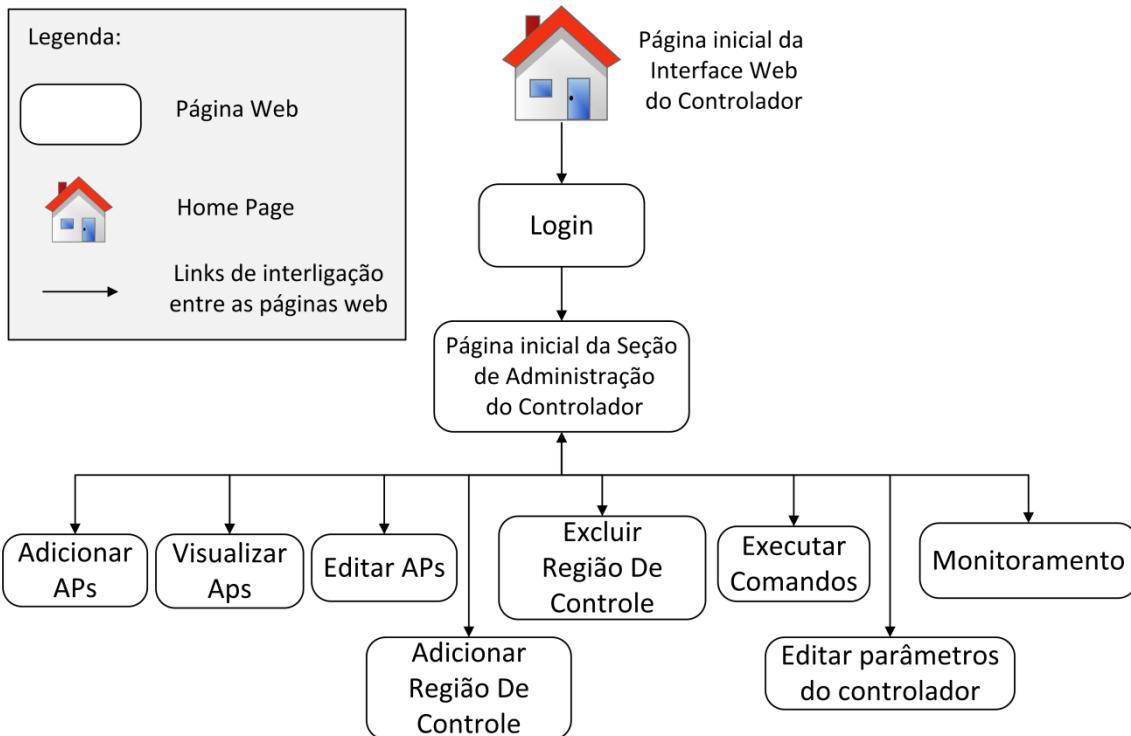


Figura 4 - Estrutura da Interface Web do Controlador

O servidor de aplicações possibilita o funcionamento da interface Web do controlador. Este servidor suporta a tecnologia JavaServer Faces (JSF), com a qual a interface foi desenvolvida. Na implementação atual, o controlador SciFi utiliza o JBoss AS como seu servidor de aplicações.

Os dados relativos à rede apresentados pela interface Web, como lista de APs, parâmetros de configuração, entre outros, são obtidos a partir do banco de dados. A comunicação entre esta interface e o *backend* do controlador é feita através do envio de mensagens ao servidor implementado no Núcleo de Processamento Central, que também é responsável por receber mensagens assíncronas enviadas pelos APs.

### 1.1.2. Subsistema dos pontos de acesso

A parte do sistema SciFi que opera nos pontos de acesso é composta pelo Módulo de Comunicação, *Scripts* de Coleta de Dados, *Scripts* de Configuração de Parâmetros, e programa para envio assíncrono de dados, como mostra a Figura 2.

Os *scripts* de coleta de dados possibilitam a obtenção de informações sobre clientes associados ao AP, obtenção da qualidade do sinal recebido dos pontos de acesso vizinhos, e obtenção dos parâmetros de funcionamento do AP, como canal e potência de transmissão. Já os *scripts* para configuração de parâmetros, possibilitam definir o canal e a potência de transmissão utilizada pelo AP. Esses *scripts* são acionados pelo controlador e os dados obtidos são armazenados no AP para posteriormente serem copiados pelo controlador. A recepção de comandos e a cópia de dados são realizadas através do módulo de comunicação, que utiliza SSH (*Secure Shell*) para estabelecer uma conexão segura entre o controlador e o AP.

Atualmente os scripts utilizados são:

- 1) scan.sh - utilizado para coleta de dados de *scan*;
- 2) set\_channel.sh - utilizado pelo algoritmo de seleção de canal para configurar o canal do AP;
- 3) set\_power.sh – utilizado pelo algoritmo de controle de potência para configurar a potência de transmissão do AP.
- 4) sta.sh – utilizado para coleta do número de estações associadas ao AP.
- 5) reboot.sh - utilizado para reiniciar o ponto de acesso. Este script possibilita que a reinicialização do AP possa ser realizada através da interface Web.
- 6) get\_channel.sh - utilizado para verificar o canal de operação atual do AP. Com esta informação, o controlador verifica se as informações no AP e no banco de dados coincidem (*check de sanidade*).
- 7) get\_power.sh - utilizado para verificar a potência de transmissão atual do AP. Com esta informação, o controlador verifica se as informações no AP e no banco de dados coincidem (*check de sanidade*).
- 8) ap\_type.sh – script utilizado pelo SNMPd para informar o modelo do ponto de acesso.
- 9) SCIFI.sh – script utilizado pelo SNMPd para informar que o AP faz parte do sistema SciFi e qual a versão suportada.
- 10) nsta.sh – script utilizado pelo SNMPd para informar o número de estações sem fio que estão associadas ao AP no momento da consulta.
- 11) init\_snmpd.sh – script utilizado para inicializar o SNMPd após o boot com determinado atraso. Este script evita que o AP responda SNMP sem antes obter informações de data e hora via NTP.

A utilização de *scripts* possui a vantagem de permitir que o controlador trabalhe com vários modelos de ponto de acesso, necessitando apenas que cada um deles possua os *scripts* compatíveis.

O ponto de acesso também possui uma aplicação (cliente) para envio assíncrono de dados, que é capaz de informar ao controlador a ocorrência de eventos assíncronos. Entretanto este módulo ainda está em fase de testes e será disponibilizado em breve.

## **1.2. Algoritmos utilizados pelo Núcleo de Processamento central**

### **1.2.1. Algoritmo de Seleção de canal**

O primeiro algoritmo a ser executado pelo controlador SciFi é o de seleção de canal. Sua função é definir o melhor canal de operação para um ponto de acesso da rede controlada, levando em consideração a interferência causada por APs vizinhos. Na versão atual do

controlador, a escolha se restringe a um dos três canais não sobrepostos do espectro de 2.4GHz utilizado pelos padrões 802.11b,g e n, ou seja, os canais 1, 6 e 11.

Para a escolha da melhor alocação de canais, inicialmente o controlador calcula o Grau de Saturação de cada ponto de acesso da rede, responsável por indicar qual deles terá prioridade na escolha de canal. Este grau é calculado com base nas informações de varredura espectral coletada dos pontos de acesso e indica a quantidade de canais diferentes utilizados pelos vizinhos, pertencentes ou não à rede controlada. Caso mais de um AP possua o mesmo grau, aquele que possuir maior número de clientes terá preferência na escolha de canal.

A interferência gerada por vizinhos em canais diferentes de 1,6 ou 11 é aproximada para o canal mais próximo. Por exemplo, um vizinho no canal 2 ou 3 é considerado como se estivesse no canal 1; um vizinho no canal 4 ou 5 é considerado como se estivesse no 6. Tendo em vista que isto pode inserir um pequeno erro, futuramente pretende-se implementar um mecanismo mais aprimorado de utilização de canais sobrepostos.

A princípio, os pontos de acesso da rede controlada não são considerados no cálculo do grau de saturação, já que seu canal será ainda determinado. Mas, a partir do momento em que um AP da rede ganha um canal, ele passa a influenciar o cálculo do grau de saturação de seus vizinhos.

Após a definição da lista de prioridade para a escolha do canal, o controlador escolhe o primeiro canal disponível para o AP com maior prioridade. No caso de não existirem canais disponíveis, será escolhido o canal com menor interferência. Esta interferência é calculada a partir da informação de qualidade com que um AP vizinho é “escutado”. É considerado que, quanto menor a qualidade do sinal interferente recebido, menor é a área de interferência daquele ponto de acesso, pois a relação sinal ruído do canal é pior, indicando maior distância entre os APs. Sendo assim, o controlador deve escolher o canal com menor qualidade do sinal recebido para reduzir a área de interferência e, no caso de existirem mais de um ponto de acesso vizinho em um mesmo canal, a soma das qualidades dos sinais recebidos no canal deve ser considerada.

Após escolhido o canal para um ponto de acesso, o processo descrito acima é repetido para os outros, até que todos tenham seus canais definidos pelo controlador. O algoritmo é executado com intervalo de tempo definido pelo administrador da rede através da interface web do controlador (vide Seção 5.6).

### **1.2.2. Algoritmo de Controle de Potência**

Após a execução do algoritmo de Seleção de Canal, o controlador executa o algoritmo de Controle de potência com o objetivo de reduzir a área de interferência entre pontos de acesso da rede que estejam operando no mesmo canal. Esta interferência pode ser detectada a partir de informações de varredura espectral coletadas nos pontos de acesso controlados. Para reduzi-la, o controlador ordena que os APs interferentes reduzam suas potências de transmissão até que deixem de ser “escutados” pelos outros da rede, ou até que a potência mínima determinada para o AP via interface web seja alcançada. Essa redução é feita

gradualmente a cada execução do algoritmo, e as potências utilizadas em cada passo são escolhidas pelo administrador da rede através da interface web do controlador, no campo “Lista de Potências”, nas páginas de adição ou edição dos pontos de acesso (ver Seção 5.5).

O fato de o ponto de acesso deixar de ser “escutado” pode representar a diminuição excessiva de sua potência ou mau funcionamento do AP. Por exemplo, caso a interface sem fio de um AP deixe de funcionar, ele deixará de “escutar” seus vizinhos e também não será mais “escutado”. Caso um vizinho não seja mais “escutado”, poderá aumentar sua potência buscando evitar o surgimento de áreas descobertas. Desta forma, o algoritmo determina que os APs que deixam de ser “escutados” têm suas potências aumentadas gradativamente, e, caso um AP seja o único em um canal, sua potência é aumentada ao máximo.

O algoritmo de Controle de potência, assim como o de Seleção de canal, é executado com intervalo de tempo definido pelo administrador da rede através da interface Web do controlador (ver Seção 5.6).

## 2. Instalando e configurando o sistema operacional

Neste tutorial de instalação do SciFi, optamos por utilizar o sistema operacional CentOS, embora o sistema possa ser instalado em outras distribuições Linux, como Debian e Ubuntu. Na época da escrita, a última versão disponível do CentOS era a 6.3. Neste tutorial, utilizamos a imagem Live CD 64 bits disponível em:

[http://vault.centos.org/6.3/isos/x86\\_64/CentOS-6.3-x86\\_64-LiveCD.iso](http://vault.centos.org/6.3/isos/x86_64/CentOS-6.3-x86_64-LiveCD.iso)

, cujo md5sum é:

9953ff1cc2ef31da89a0e1f993ee6335 CentOS-6.3-x86\_64-LiveCD.iso

Recomendamos que a máquina utilizada possua memória RAM mínima de 2GB.

A instalação é simples, apenas é necessário seguir o passo a passo do próprio CD.

- Insira o cd do CentOS

- Escolha *Create Custom Layout* para fazer o particionamento recomendado:

/boot - 512 MB

/swap - igual a memória real

/tmp - 20 GB

/ - espaço que restar

- Durante a instalação crie seu usuário e defina a senha de root. Guarde estas informações.

Ao terminar a instalação reinicie a máquina e faça *login* utilizando o usuário criado.

A partir desse ponto, acesse o terminal com privilégio root.

```
su -  
// digite a senha de root
```

Faça o redirecionamento do *log* para *tty6*, para facilitar sua visualização. Para isso, edite o arquivo **/etc/rsyslog.conf** e insira no final a seguinte linha

```
*.*          /dev/tty6
```

Reinic peace o rsyslog executando o comando:

```
service rsyslog restart
```

Configure as interfaces de rede utilizando a interface gráfica do Network-Manager.

Reinic peace o network manager para que as configurações sejam atualizadas:

```
/etc/init.d/Network-Manager restart  
/etc/init.d/network restart
```

Para configurar o hostname da máquina digite o comando:

```
system-config-network
```

Na tela que surgir, insira o novo "hostname" no campo "nome da máquina".

Para instalar o repositório EPEL digite:

```
wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-  
6-8.noarch.rpm  
rpm -Uvh epel-release-6*.rpm  
yum update  
yum install yumex
```

Para instalar o *firewall builder*, que será utilizado para criação do firewall, configure o repositório criando o arquivo:

```
/etc/yum.repos.d/fwbuilder.repo
```

A seguir, Insira o seguinte conteúdo neste arquivo:

```
[fwbuilder]  
name=Firewall Builder  
failovermethod=priority  
baseurl=http://packages/fwbuilder.org/rpm/stable/rhel-$releasever-$basearch  
enabled=1  
priority=14
```

Instale a chave do repositório:

```
rpm --import http://www/fwbuilder.org/PACKAGE-GPG-KEY-fwbuilder.asc
```

Agora instale o programa:

```
yum install fwbuilder rcs
```

Instalar programas adicionais:

```
yum install htop tree file-roller gnome-utils  
yum install perl-CPAN lynx ftp ncft  
yum install netsnmp netsnmp-utils mrtg nagios nagios-plugins  
yum install nagios-plugins-ifoperstatus  
yum install nagios-plugins-ifstatus snmpcheck  
yum install denyhosts
```

## 2.1. Configurando o dnsmasq

No caso em que o servidor seja utilizado para fornecer o serviço de DHCP, o dnsmasq deverá ser utilizado. O dnsmasq vem instalado por padrão no centos 6.3. Para habilitar sua inicialização do boot, digite o comando:

```
chkconfig dnsmasq on
```

Para inicializar o dnsmasq, digite:

```
service dnsmasq start
```

Para reiniciar:

```
service dnsmasq restart
```

Para parar:

```
service dnsmasq stop
```

O arquivo de configuração do dnsmasq é:

**/etc/dnsmasq.conf**

Antes de editar o arquivo de configuração do dnsmasq, faça um backup dele:

```
su -
```

```
cp /etc/dnsmasq.conf /etc/dnsmasq.conf_ori
```

As seguintes configurações devem ser utilizadas no arquivo **/etc/dnsmasq.conf** :

Obs.: ALTERE OU INSIRA APENAS AS LINHAS DESCOMENTADAS ABAIXO (i.e, não apague as demais linhas do arquivo):

```
# Never forward plain names (without a dot or domain part)
```

```
domain-needed
```

```
# Never forward addresses in the non-routed address spaces.
```

```
bogus-priv
```

```
# Or you can specify which interface _not_ to listen on
```

```

except-interface=eth0

#no-dhcp-interface= eth1
no-dhcp-interface= eth0

# Set this (and domain: see below) if you want to have a domain
# automatically added to simple names in a hosts-file.
expand-hosts

# Set the domain for dnsmasq. this is optional, but if it is set, it
# does the following things.
# 1) Allows DHCP hosts to have fully qualified domain names, as long
#     as the domain part matches this setting.
# 2) Sets the "domain" DHCP option thereby potentially setting the
#     domain of all systems configured by DHCP
# 3) Provides the domain part for "expand-hosts"
#domain=thekelleys.org.uk
domain=<INSIRA AQUI O NOME DE SEU DOMÍNIO CONFORME O EXEMPLO>

# Uncomment this to enable the integrated DHCP server, you need
# to supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
dhcp-range=10.0.16.0,10.255.255.254,255.0.0.0,12h

#dhcp-option=3

dhcp-option=2,4294956496

# Set the NTP time server address to be the same machine as
# is running dnsmasq
dhcp-option=42,0.0.0.0

#dhcp-option=19,0          # option ip-forwarding off
dhcp-option=44,0.0.0.0    # set netbios-over-TCP/IP nameserver(s) aka WINS server(s)
dhcp-option=45,0.0.0.0    # netbios datagram distribution server
dhcp-option=46,8          # netbios node type

# Send microsoft-specific option to tell windows to release the DHCP lease
# when it shuts down. Note the "i" flag, to tell dnsmasq to send the
# value as a four-byte integer - that's what microsoft wants. See
#   http://technet2.microsoft.com/WindowsServer/en/library/a70f1bb7-d2d4-49f0-96d6-4b7414ecfaae1033.mspx?mfr=true
dhcp-option=vendor:MSFT,2,1i

```

```

# Set the limit on DHCP leases, the default is 150
#dhcp-lease-max=150
dhcp-lease-max=4098

# Log lots of extra information about DHCP transactions.
log-dhcp

# Include another lot of configuration options.
#conf-file=/etc/dnsmasq.more.conf
conf-dir=/etc/dnsmasq.d

```

Para que os APs obtenham sempre o mesmo IP provido por DHCP, crie o arquivo **/etc/dnsmasq.d/hosts** e insira dentro dele, a seguinte linha para cada AP desejado:

```
dhcp-host=A0:F2:C1:DE:DA:B7,A0:F2:C1:DE:DA:B8,A0:F2:C1:DE:DA:B9,ap0010,10.0.0.10,240h
```

Neste exemplo, o AP ,cujo *hostname* é ap0010, pode requisitar IP utilizando qualquer um dos três endereços MACs especificados obtendo com sucesso o IP 10.0.0.10. A duração da reserva do IP (*lease*) é de 240h.

## 2.2. Configurando o syslog para receber logs dos APs

O CentOs utiliza por padrão o programa **rsyslog** para a realizar log das mensagens do sistema. Para que o controlador possa receber logs remotos provenientes dos pontos de acesso, as seguintes linhas devem ser descomentadas no arquivo **/etc/rsyslog.conf**:

```

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

```

Insira a linha para definir o IP do servidor:

```
$UDPServerAddress 10.0.0.1
```

A seguir o **rsyslog** deve ser reinicializado:

```
/etc/init.d/rsyslog restart
```

Para ler o syslog:

```
tail -f /var/log/messages
```

No firewall, uma regra deve ser inserida para liberar esta porta para o acesso dos APs. Esta regra será melhor documentada na seção 2.5 , que trata sobre o firewall do controlador.

Para verificar se o servidor está escutando na porta 514 (UDP), digite o comando:

```
netstat -plnu
```

Uma linha semelhante a esta deve surgir:

```
udp      0      0 10.0.0.1:514          0.0.0.0:*      8150/rsyslogd
```

O **rsyslog** também permite que o log de diferentes programas, ou que possuem determinada expressão, sejam redirecionados para diferentes arquivos de log.

Um exemplo é o log gerado pelo *firewall*, que pode ocasionar rápido crescimento do arquivo de log **/var/log/messages**.

Para evitar isto, iremos salvar o log do firewall em um arquivo próprio, o **/var/log/iptables.log**.

O redirecionamento do log pode ser configurado no arquivo **/etc/rsyslogd.conf**.

**Duas linhas** devem ser inseridas, conforme a seguir:

```
# Log all kernel messages to the console.  
# Logging much else clutters up the screen.  
# kern.* /dev/console  
:msg, startswith, "RULE "           /var/log/iptables.log  
:msg, startswith, "RULE "           ~
```

A primeira linha determina que todas as mensagens iniciadas com "RULE " (padrão do prefixo do log do firewall gerado pelo programa fwbuilder) são enviadas para o arquivo **/var/log/iptables.log**.

Na segunda linha, o "~" é utilizado para descartar as linhas que começam com RULE. Desta forma, elas não serão reescritas no **/var/log/messages**.

Após salvar as alterações, **reinicie o rsyslogd**:

```
/etc/init.d/rsyslogd restart
```

Para ler o log do firewall:

```
tail -f /var/log/iptables.log
```

### 2.3. Configurando o ntpd

O ntpd é o serviço responsável por obter data e hora do servidor. As informações são obtidas pela internet com a utilização do protocolo NTP (*Network Time Protocol*). Para configurar qual será o servidor que fornecerá a data/hora para o CentOs, devemos alterar o arquivo **/etc/ntp.conf** inserindo o seguinte bloco:

```
# servidores públicos do projeto ntp.br  
server a.st1.ntp.br iburst  
server b.st1.ntp.br iburst  
server c.st1.ntp.br iburst
```

```
server d.st1.ntp.br iburst
server gps.ntp.br iburst
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

Comente o bloco de servidores que já vem configurado por padrão no ntp.conf:

```
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
```

```
#server 127.127.1.0 iburst
```

Para que o servidor mantenha o tempo local quando a conexão com a internet não existir, descomente as linhas *server* e *fudge* conforme abaixo:

```
# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
server 127.127.1.0      # local clock
fudge  127.127.1.0 stratum 10
```

A linha **driftfile /var/lib/ntp/drift** deve permanecer descomentada. Neste arquivo é armazenado o erro de freqüência do clock do servidor (*clock drift*). As linhas que permitem que outros hosts sincronizem tempo com nosso servidor, mas sem modificar o serviço ou obter informações sobre o sistema são:

```
# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

Para saber mais sobre estas opções acesse:

<http://www.eecis.udel.edu/~mills/ntp/html/accept.html>

As linhas **restrict 127.0.0.1** e **restrict -6 ::1** liberam todo tipo de acesso ao servidor ntp para *localhost*.

Para outros guias de configuração, acesse:

<http://support.ntp.org/bin/view/Support/>

<http://ubuntuforums.org/showthread.php?t=862620>

<http://linux.die.net/man/5/ntp.conf>

<http://www.ntp.br/NTP/MenuNTPLinuxBSD>

## 2.4. Configurando o servidor SSH

Por padrão, o servidor SSH no CentOs já vem instalado,porém desabilitado. A configuração do servidor pode ser realizada no arquivo **/etc/ssh/sshd\_config**. Abra o arquivo de configuração do servidor SSH:

```
/etc/ssh/sshd_config
```

Descomente a linha `PermitRootLogin yes`, substituindo "yes" por "no". A linha ficará assim:

```
PermitRootLogin no
```

Logo a seguir, insira a linha:

```
AllowUsers nx joao maria
```

No lugar dos nomes “joao” e “maria”, insira o nome dos usuários que terão permissão para fazer SSH, separados por espaço.

Caso deseje alterar a porta do servidor SSH, comente linha "Port 22" e Insira, abaixo dela, a linha:

```
Port 2220
```

, substituindo 2220 pelo número da porta desejada. Também é possível que o servidor receba conexões em mais de uma porta, bastando repetir a linha alterando o número da porta para o desejado. Uma regra no firewall deverá ser inserida para que esta porta seja liberada, conforme documentado na seção 2.5.

Para configurar a inicialização do servidor de SSH no boot, execute o comando como root:

```
chkconfig sshd on
```

Para inicializar o servidor SSH, execute o comando como root:

```
/etc/init.d/sshd start
```

Para prover maior segurança contra invasões no acesso SSH, o programa denyhosts poderá ser utilizado. O denyhosts é um programa utilizado para evitar ataques de força bruta via SSH. Com o denyhosts, caso um determinado *host* tente se conectar e erre o *login* ou senha por mais de um determinado número de vezes, o IP deste host é bloqueado.

O denyhosts pode ser instalado como root através do comando:

```
su -
```

```
yum install denyhosts
```

Habilite a execução do denyhosts no boot através do comando:

```
chkconfig denyhosts on
```

Inicie o denyhosts:

```
/etc/init.d/denyhosts start
```

Faça um backup do arquivo de configuração do denyhosts se encontra em /etc/denyhosts.conf:

```
cp /etc/denyhosts.conf /etc/denyhosts.conf_ori
```

Abra arquivo de configuração do denyhosts se encontra em /etc/denyhosts.conf:

```
vim /etc/denyhosts.conf
```

Altere a linha PURGE\_DENY = 4w para:

```
PURGE_DENY = 4h
```

Este é o tempo que um IP ficará bloqueado. Após 4 horas ele será liberado.

Altere a linha DENY\_THRESHOLD\_VALID = 10 para:

```
DENY_THRESHOLD_VALID = 3
```

Esta linha informa quantas vezes a senha informada poderá estar errada, dado que o login era válido.

Para verificar os hosts que estão bloqueado, acesse o arquivo /etc/hosts.deny. Uma entrada como a seguir será encontrada, contendo o IP bloqueado:

```
sshd: 192.168.0.4
```

Diversas informações sobre o denyhosts podem ser encontradas no diretório **/var/lib/denyhosts**. O arquivo `purge-history`, por exemplo, mostra o histórico de bloqueios. O arquivo `users-valid` mostra tentativas com usuários válidos; `users-invalid` mostra tentativas com usuários inválidos.

Para remover um IP bloqueado, siga o passo a passo:

1) Pare o denyhosts:

```
/etc/init.d/denyhosts stop
```

2) Remova a entrada para o IP bloqueado no arquivo /etc/hosts.deny

3) Remova as linhas que contém o IP bloqueado dos seguintes arquivos contidos na pasta `/var/lib/denyhosts`:

- a. Hosts
- b. Hosts-restricted
- c. Hosts-root
- d. Hosts-valid
- e. User-hosts

4) Caso queira que o IP nunca mais seja bloqueado, inclua ele no arquivo `/var/lib/denyhosts/allowed-hosts`.

5) Ligue o denyhosts:

```
/etc/init.d/denyhosts start
```

Para mais informações, acesse:

<http://denyhosts.sourceforge.net/>

## 2.5. Configurando o Firewall

Para a criação e manutenção do firewall, optamos por utilizar o programa *firewall builder* (<http://www.fwbuilder.org/>), que permite que as regras de firewall sejam criadas através do uso de interface gráfica de forma prática. Um modelo de firewall preparado para o SciFi pode ser obtido no site:

<http://www.midiacom.uff.br/br/downloads-sciFi/FW-SCIFI.fwb>

Faça o *download* do arquivo e abra-o com o programa *firewall builder*:

fwbuilder FW-SCIFI.fwb &

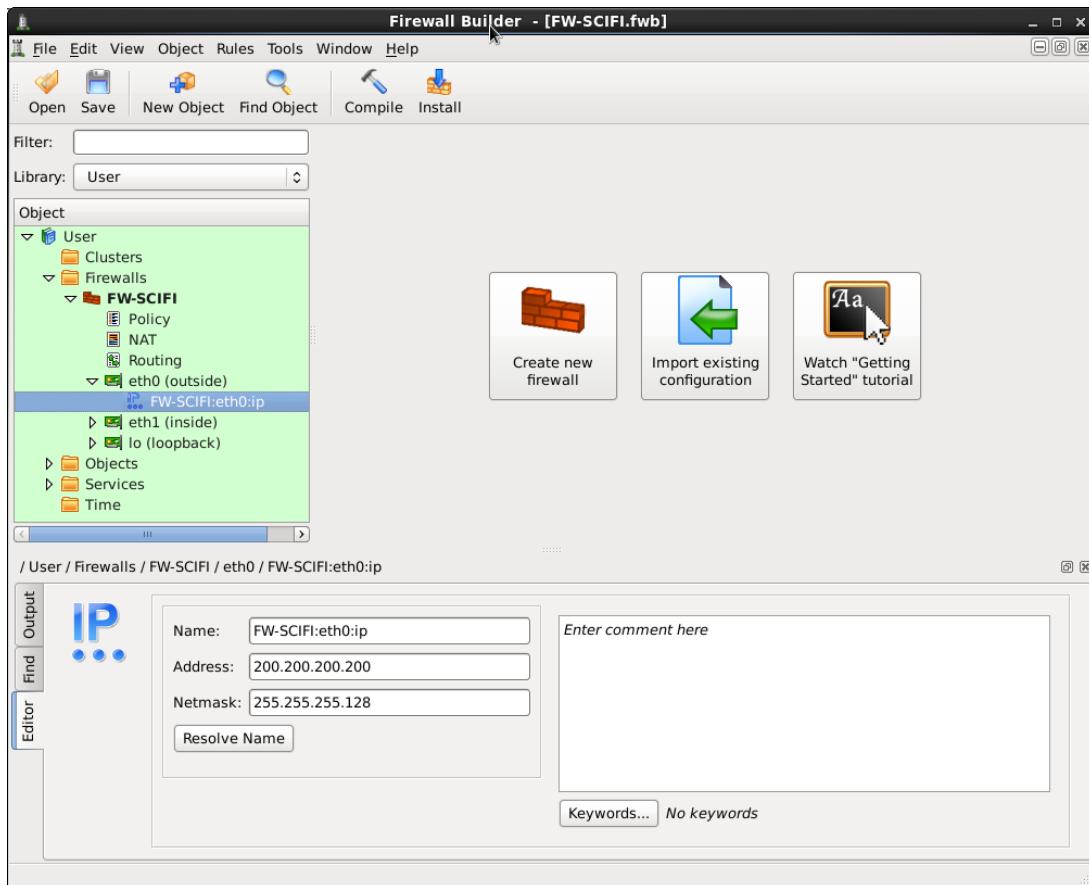


Figura 5 - Firewall Builder: Alterando IPs das interfaces

O primeiro passo para configuração do firewall é a configuração das interfaces e sub-redes. Para configurar as interfaces eth0 e eth1, no menu esquerdo, clique em **Firewalls > FW-SCIFI > eth0 (ou eth1)**, conforme mostra a Figura 5.

No SciFi utilizamos o padrão:

eth0 - interface externa (que faz conexão com a internet)

eth1 - interface interna (que faz conexão com os APs)

Para configurar a eth0 clique em eth0 e dê um duplo clique em **FW-SCIIFI:eth0:ip**. Digite em "Address" o IP da interface e em "Netmask", a máscara da rede. A seguir, faça o mesmo para eth1.

A seguir, configure qual será a subrede dos APs clicando em **Objects > Networks > APs**, conforme mostra a Figura 6. No campo "Address" digite o endereço IP da subrede dos APs. No campo "Netmask", digite a máscara da subrede dos APs. Esta subrede deverá conter apenas pontos de acesso. Faça o mesmo para a definir a subrede da Rede WiFi. Esta subrede deverá abranger todos os APs e clientes da rede sem fio.

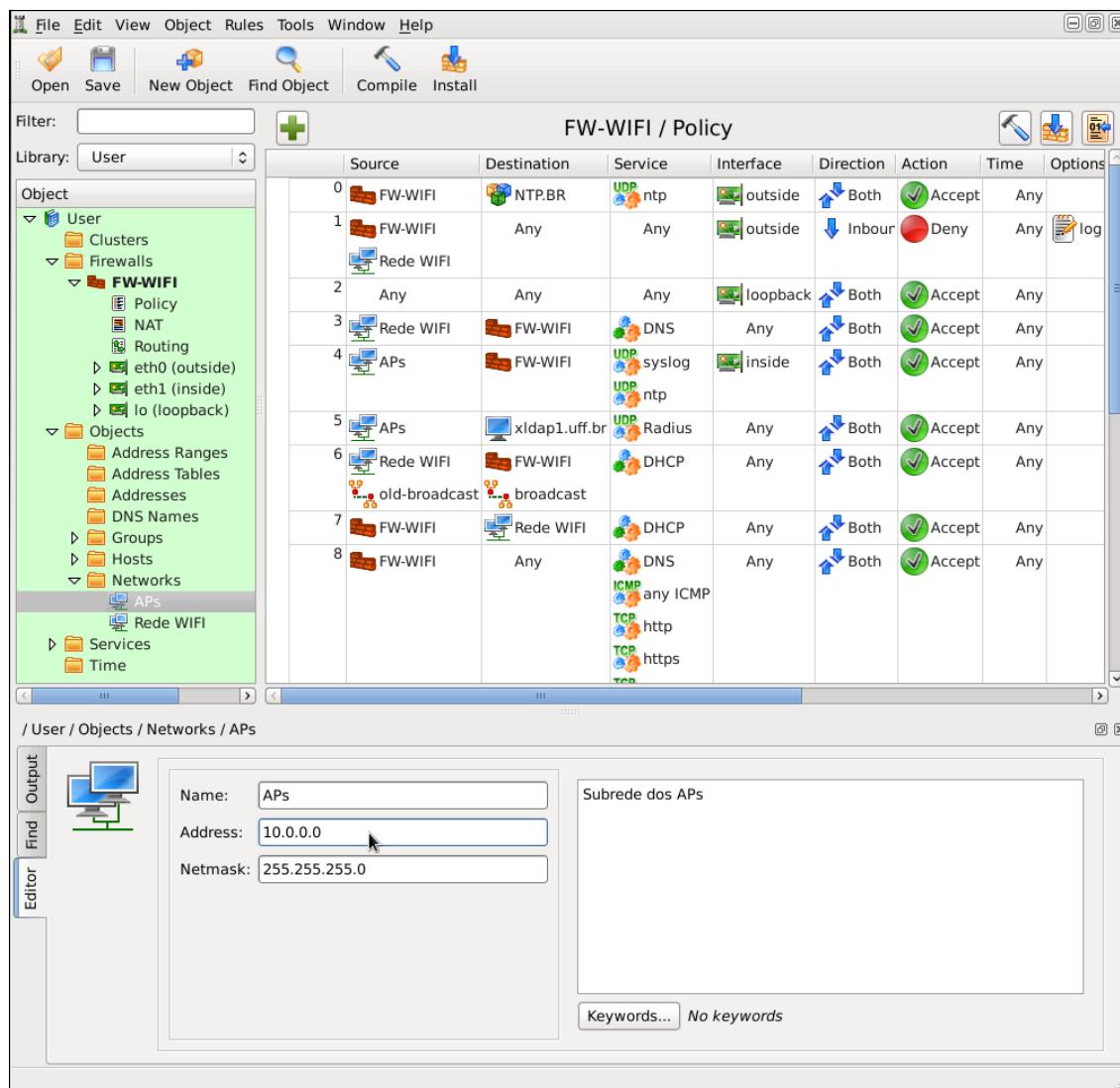


Figura 6 - Firewall Builder: Configurando a subrede dos APs e WIFI

Para visualizar as regras gerais do firewall, clique em **Firewalls > FW-SCIIFI > Policy**. As regras serão mostradas na parte direita da janela do programa, conforme mostra a Figura 6.

Por fim, altere a porta alternativa que será liberada para o SSH. Para isso, no menu esquerdo, clique em **Services > TCP > ssh-alt** e insira nos campos "Destination Port Range" a porta desejada, conforme mostra a Figura 7.

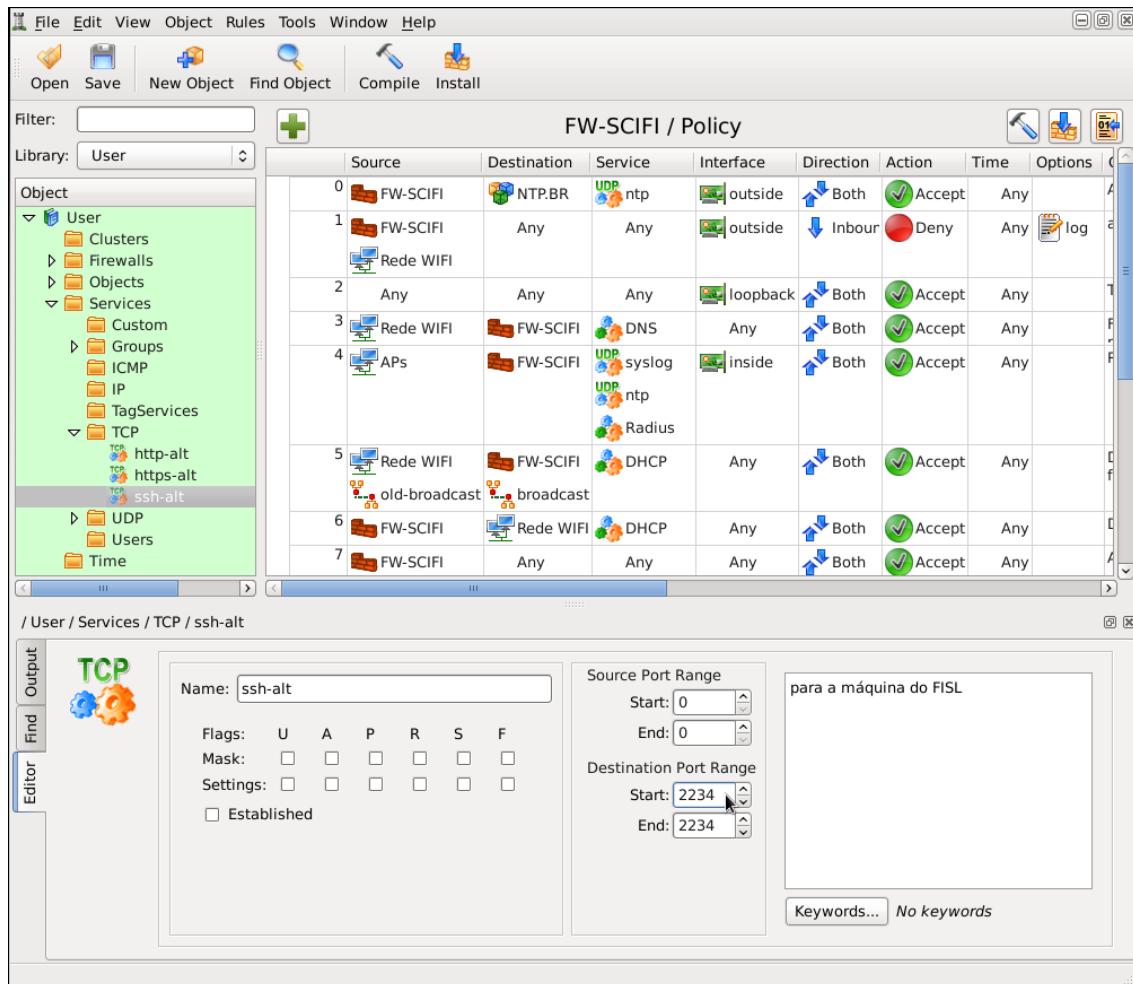


Figura 7 - Firewall Builder: Alterando a porta que será liberada para o SSH

Após terminar as configurações compile o firewall clicando no botão "Compile" do menu superior (botão com ícone de um martelo). Uma tela semelhante a mostrada na Figura 8 surgirá. Clique em "Next".

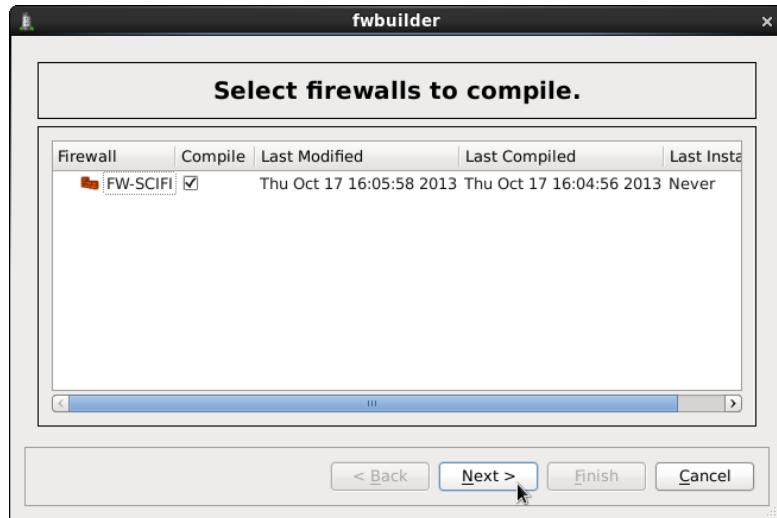


Figura 8 - Firewall Builder: Compilando o firewall

Após compilado, uma tela semelhante a da Figura 9 surgirá caso o firewall tenha sido compilado com sucesso. Caso a compilação indique erro, corrija o firewall conforme o próprio programa indicará e tente novamente. Ao final, clique em “Finish”.

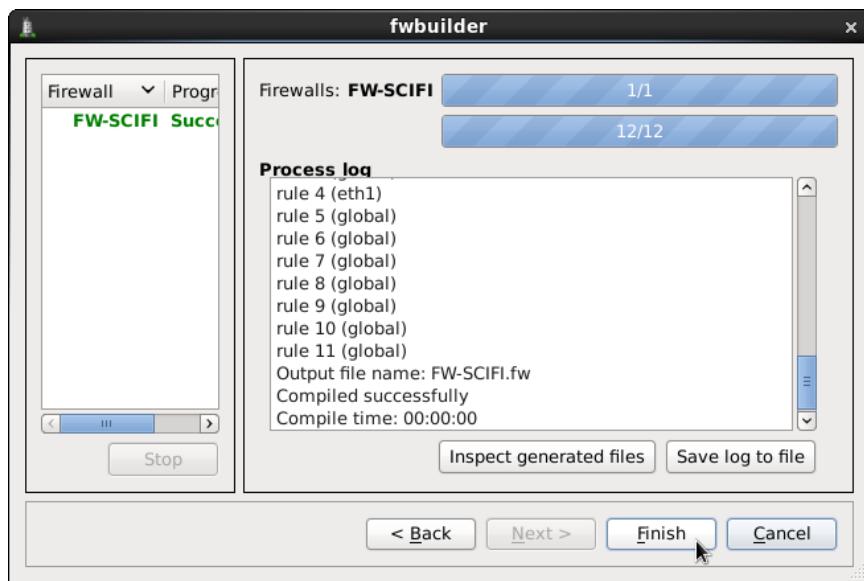


Figura 9 - Firewall Builder: Firewall compilado com sucesso

Após compilar o firewall, o arquivo FW-WIFI/fw será gerado na mesma pasta em que o arquivo “.fwb” está localizado. Para executar o firewall, vá até a pasta no qual ele foi compilado e execute o comando:

```
./FW-SCIFI.fw start
```

Para desligar o firewall, execute o comando:

```
./FW-SCIFI.fw stop
```

Para que o firewall seja inicializado no boot, o script de inicialização deve ser obtido no link:

<http://www.midiacom.uff.br/br/downloads-scifi/firewall>

Após fazer o *download* copie os arquivos **firewall** e **FW-SCIFI/fw** na pasta **/etc/init.d**, com permissão de root. A seguir, altere o proprietário dos scripts e execute o comando para inicialização do serviço no boot:

```
su - root  
cd /etc/init.d  
chown root:root FW-SCIFI/fw  
chown root:root firewall  
chmod 755 firewall  
chkconfig firewall on
```

Além de ser executado no boot, este script pode ser utilizado da seguinte forma:

```
service firewall opção
```

, onde a "opção" deve ser substituída por uma das opções:

- start: Ativa o firewall
- stop: Desativa o firewall
- restart: Reativa o firewall
- clear: Limpa os contadores
- status: Mostra as regras estabelecidas

### 3. Instalando OpenWrt nos Pontos de Acesso

Para instalar o OpenWrt no ponto de acesso, os seguintes passos devem ser realizados:

- Fazer *Download* da imagem
- Instalação da imagem
- Configuração

A seguir, será apresentado um passo a passo para a instalação do OpenWrt nos modelos Linksys WRT54G, Ubiquiti Bullet, Ubiquiti Nanostation e Ubiquiti Picostation. Para a instalação de outros modelos de ponto de acesso, consulte o site do OpenWrt (<https://openwrt.org/>).

### **3.1. Fazendo Download da imagem OpenWrt**

Observação: A imagem do OpenWrt está incluída no pacote disponibilizado para configuração automática do AP. Caso você tenha o pacote para o modelo do AP específico, não é necessário seguir as etapas abaixo. A imagem pode ser encontrada na pasta “arquivos/imagens” do pacote. Após encontrar a imagem, pule para a seção 3.2.1 . Caso você não tenha o pacote siga o passo a passo listado:

- 1) Procurar o ponto de acesso na lista de hardware suportados
  - \* <http://wiki.openwrt.org/toh/start>
- 2) Verificar o valor inserido em sua coluna "target" de seu ponto de acesso. Por exemplo, Picostation M2 possui "target" "ar71XX". Este valor corresponde à arquitetura do OpenWrt compatível com o dispositivo.
- 3) Verificar na coluna "Status" qual é a primeira versão do OpenWrt que suporta seu ponto de acesso. Provavelmente versões subsequentes irão suportá-lo também. Por exemplo, o *Picostation M2* possui "Status" "10.03.1".
- 4) Clicar no link de seu ponto de acesso e verificar as observações dos desenvolvedores do OpenWrt. Nesta página podem ser encontrados o guia de instalação e o nome da imagem que deve ser utilizada.
- 5) Ir ao site de download do OpenWrt
  - \* <http://downloads.openwrt.org/>
- 4) Escolher a pasta com a versão do firmware de interesse (por exemplo, *attitude adjustment*, *backfire*, *kamikaze*, etc.). As últimas versões que ainda não foram lançadas (versões "trunk") estão na pasta "snapshots". Alguns modelos novos de APs e algumas novas funcionalidades são suportadas apenas pela versão "trunk" do OpenWrt.
- 5) A seguir, escolher a pasta que contém o "target" do AP em questão. Por exemplo, a do *Picostation M2* seria a "ar71XX".
- 6) Procurar o link para o .bin que contém o nome de seu AP, seguindo as observações dos desenvolvedores, e fazer o *download*. Por exemplo, o link do *Picostation M2* seria "openwrt-ar71xx-ubnt-bullet-m-squashfs-factory.bin" . A versão do firmware que termina com a palavra "factory" deve ser utilizada para a primeira instalação no AP. No caso de *upgrade do firmware*, a versão que termina com a palavra "sysupgrade" poderá ser utilizada. Para saber mais sobre o upgrade de firmware, leia a documentação que se encontra no site: <http://wiki.openwrt.org/doc/howto/generic.sysupgrade>
- 7) Obtenha o arquivo com o md5sum das imagens do OpenWrt. Este arquivo chama-se *md5sums* e encontra-se na mesma pasta da imagem para *download*.
- 8) Cheque o md5sum da imagem obtida, comparando o resultado com o registrado no arquivo md5sum. Este processo ajuda a verificar se a imagem foi corrompida durante o *download*.

Caso os resultados sejam diferentes, faça novamente o *download* da imagem e repita a verificação.

### **3.2. Instalação do OpenWrt**

Os pontos de acesso que serão controlados pelo SciFi devem ser compatíveis com OpenWrt, que é um *firmware* de código aberto baseado em Linux. Uma lista de compatibilidade pode ser encontrada no endereço:

[http://wiki.openwrt.org/toh/start?s\[\]=compatibility](http://wiki.openwrt.org/toh/start?s[]=compatibility)

Nesta página, clicando-se no modelo desejado, informações e instruções de instalação do *firmware* são apresentadas.

As imagens são instaláveis através da interface Web de administração original do AP, ou via *tftp*. Os processos, no entanto, são ligeiramente diferentes para cada modelo de ponto de acesso. A seguir serão apresentados exemplos de instalação em alguns modelos através de destes mecanismos.

#### **3.2.1. Exemplos de instalação de imagem OpenWrt via interface Web**

O processo de instalação do OpenWrt via interface Web original de administração do ponto de acesso é semelhante ao processo de atualização de firmware padrão do dispositivo. Normalmente, o fabricante oferece instruções para a realização deste processo. A diferença será a utilização do *firmware* obtido a partir do site do OpenWrt, e não o disponibilizado pelo fabricante. A seguir serão listadas as instruções básicas:

- 1) Ligue o roteador ou ponto de acesso na energia elétrica.
- 2) Interligue o PC ao roteador ou ponto de acesso utilizando um cabo ethernet. Caso o dispositivo tenha mais de uma porta, utilize a porta nº 1.
- 3) Caso o PC tenha interface sem fio, desligue-a para evitar problemas.
- 4) Configure a interface ethernet do PC para obter IP automaticamente por DHCP.  
Aguarde até que o endereço seja obtido.
- 5) No PC, abra o navegador web e digite o endereço IP da interface administrativa do roteador. Este é endereço normalmente é 192.168.0.1, 192.168.1.1 ou 192.168.1.20. Procure esta informação no manual do seu roteador ou verifique o IP do *gateway* obtido por DHCP.
- 6) Digite o *login* e senha para acesso à interface web administrativa do roteador.  
Normalmente, as credenciais são *admin* para o login e *admin* para a senha. Procure esta informação no manual do seu roteador.
- 7) Entre na seção relativa ao sistema e a seguir, procure a seção de atualização de *firmware* do dispositivo. Escolha o *firmware* do OpenWrt e a seguir execute a atualização.  
Aguarde até que o dispositivo reinicie automaticamente. Isto pode levar alguns minutos.

As figuras a seguir mostram exemplos da página de atualização de *firmwares* de alguns modelos de pontos de acesso. A Figura 10 mostra a página de atualização de *firmware* do ponto de acesso TP-Link WR841N v8. Esta página é semelhante para os modelos WR743ND e WR740N, entre outros. Após acessar o menu “System Tools > Firmware Upgrade”, escolha o *firmware* do OpenWrt clicando em “Choose File” e a seguir, clique em “Upgrade”. Aguarde até que o ponto de acesso reinicie. Isto pode levar alguns minutos.

A Figura 11 mostra a página de atualização de *firmware* do ponto de acesso Ubiquiti NanoStation Loco M2. Esta página é semelhante para os modelos Picostation M2, Rocket M2 e Bullet M2. Após acessar a aba “System”, escolha o *firmware* do OpenWrt clicando em “Choose File”, aguarde até que ele seja transferido para o AP. A seguir, clique em “Update” e aguarde até que o ponto de acesso reinicie. Isto pode levar alguns minutos.

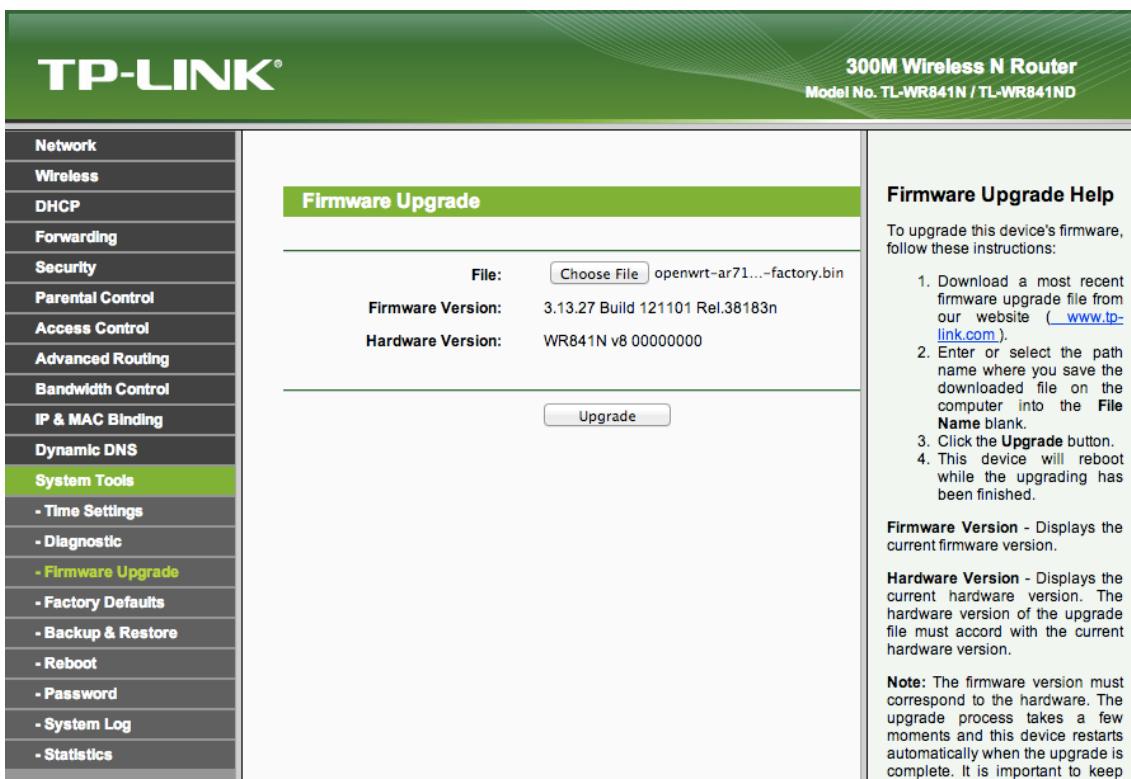


Figura 10 - Atualização de firmware do ponto de acesso TP-Link WR841N v8.

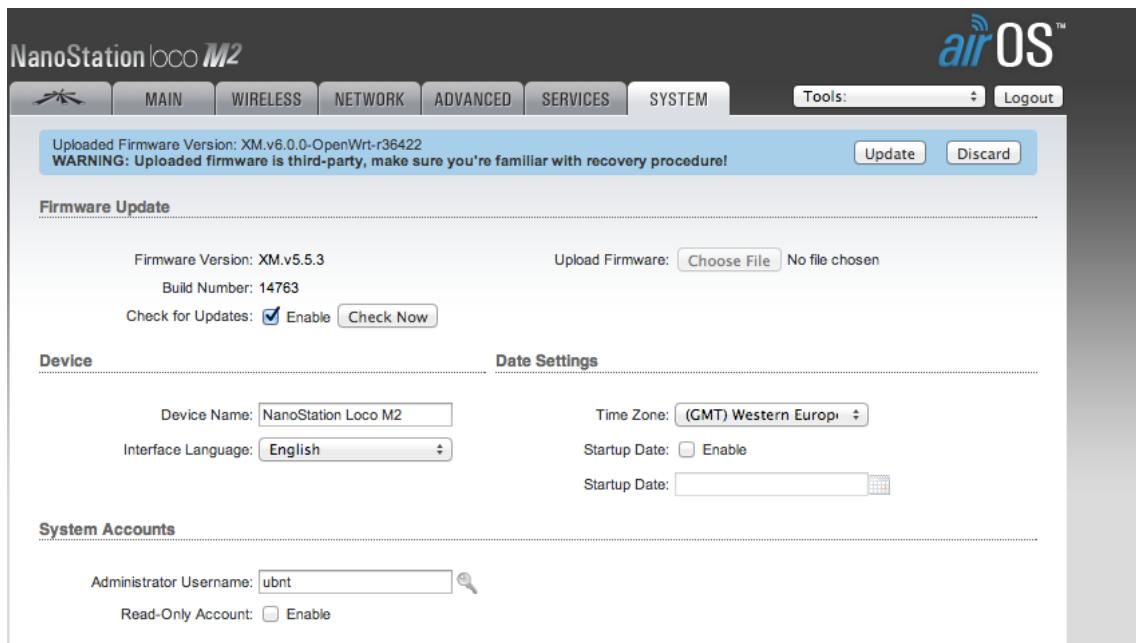


Figura 11 - Atualização de firmware do ponto de acesso NanoStation Loco M2.

### 3.2.2. Exemplos de instalação de imagem OpenWrt via *tftp*

O site que documenta a instalação do OpenWrt via TFTP pode ser encontrado no endereço:

<http://wiki.openwrt.org/doc/howto/generic.flashing.tftp>

A seguir será apresentado o passo a passo básico para diferentes modelos.

#### - Linksys WRT54G

- 1) Ligar o roteador a uma máquina (PC Linux) através de um cabo ethernet conectado na porta 1 do roteador.
- 2) Configurar a interface de rede da máquina para o endereço 192.168.1.10/24 (ou qualquer endereço nesta sub-rede, exceto por 192.168.1.1).
- 3) Iniciar o *tftp* para o endereço 192.168.1.1, através do comando #tftp 192.168.1.1
- 4) No terminal do *tftp*, executar os seguintes comandos (substitua "nomelimagem.bin" pelo nome da imagem adequada):

```
> trace
> binary
> rexmt 1
> timeout 60
> put nomeImagem.bin
```

5) Ligar o roteador enquanto o *tftp* tenta realizar o envio.

A imagem será enviada para o roteador, que será reiniciado. Não interrompa este processo, que pode demorar alguns minutos. A atualização de firmware estará completa quando o *led power* estiver ligado (sem piscar) e o *led DMZ* estiver apagado.

#### - Ubiquiti Bullet, Nanostation e Picostation

- 1) Ligar o ponto de acesso a uma máquina (PC Linux) através de um cabo ethernet.
- 2) Configurar a interface de rede da máquina para o endereço 192.168.1.10/24 (ou qualquer endereço nesta sub-rede, exceto por 192.168.1.20).
- 3) Iniciar o *tftp* para o endereço 192.168.1.20.
- 4) Ligar o ponto de acesso e, imediatamente, segurar o botão reset por cerca de 10 segundos. Se feito de modo correto, os *leds* vermelho e laranja irão piscar alternadamente.
- 5) No terminal do *tftp*, executar os seguintes comandos (substitua "nomeImagem.bin" pelo nome do arquivo adequado):

```
> trace  
> binary  
> rexmt 1  
> put nomeImagen.bin
```

A imagem será enviada para o ponto de acesso, que será reiniciado. Não interrompa este processo. A atualização de *firmware* estará completa quando os *leds* vermelho e laranja ficarem apagados.

### 3.3. Configuração do OpenWrt

Após a instalação do *firmware*, acesse o roteador através do endereço 192.168.1.1 via *telnet*. Inicialmente, o roteador estará disponível apenas via *telnet*. No primeiro acesso, deve-se executar o comando *passwd* para definir uma senha de *root*. Após esta definição, é possível acessar o roteador através de *ssh*.

Após instalar o *firmware* correto para o modelo de AP escolhido, é necessário preparar o ponto de acesso para trabalhar com o controlador SciFi. Para tanto *scripts* necessitam ser copiados para o AP e a configuração das interfaces de rede devem ser realizadas. Ao final, a chave SSH de comunicação do AP com o controlador deve ser instalada. Para realizar esta etapa, é necessário conhecimento básico de comandos em Linux.

A seguir, o ponto de acesso deverá ser configurado. Esta configuração pode ser realizada manualmente ou através da utilização de um pacote preparado para automatizar o processo. A seguir, as duas formas serão apresentadas.

### 3.3.1. Configuração utilizando pacote de configuração automática

Após obter o arquivo “.zip” contendo o pacote para configuração automática de determinado ponto de acesso para o sistema SciFi, descompacte-o. Os seguintes arquivos serão obtidos:

- config.sh : script principal que deve ser executado para a realização da configuração do AP. A configuração das variáveis que serão configuradas no AP devem ser inseridas neste *script* antes de sua execução.

- edit\_wireless.sh : este script é executado automaticamente para configuração da rede sem fio do AP.

- only\_wireless\_config.sh : este script é similar ao config.sh, porém configura apenas parâmetros da rede sem fio do AP.

- expect.sh : este script é executado automaticamente e sua função é inserir, na lista de *hosts* conhecidos do servidor, a Impressão digital da chave RSA do AP. O script apenas escreve a palavra “yes” automaticamente, evitando a necessidade de que isto seja feito pelo usuário, conforme mostra a figura abaixo:

```
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.  
RSA key fingerprint is d1:93:ab:ea:3d:bb:0f:22:1a:7d:0f:8c:ad:a2:73:ae.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
```

- Pasta “arquivos”: contém alguns arquivos já prontos para configuração do AP. Além disso, a chave pública SSH que será utilizada para comunicação do controlador com o AP (*authorized\_keys*) deve ser criada e inserida nesta pasta.

- Pasta “arquivos/imagens”: possui as imagens *sysupgrade* e *factory* para o modelo do AP. A versão do firmware que termina com a palavra “factory” deve ser utilizada para a primeira instalação no AP. No caso de *upgrade do firmware*, a versão que termina com a palavra “*sysupgrade*” poderá ser utilizada. Antes de realizar a configuração do AP, a imagem deve ser instalada no AP conforme indicado na seção 3.2.

- Pasta “arquivos/scripts”: contém os scripts do sistema SciFi para coleta de dados e configuração de parâmetros do AP, entre outros.

- Pasta “arquivos/ipk”: contém os pacotes que serão instalados no OpenWrt para compatibilidade com o SciFi. Basicamente, são 3 pacotes e suas dependências: Wireless Tools (ferramentas para configuração e consulta de parâmetros da rede sem fio); Hostapd (programa com funcionalidade de AP que suporta autenticação wpa2-enterprise) e Snmpd-static (servidor Snmp).

O pacote de instalação automática deve ser executado em sistemas Linux. Antes de utilizá-lo, algumas configurações devem ser realizadas:

- 1) Intalar no linux os programas *sshpass* e *expect* necessários para a execução do script de configuração automática do AP.

- 2) Gerar par de chaves pública e privada para comunicação SSH entre controlador e AP. A chave pública deve ser inserida na pasta “arquivos”.
- 3) Configurar o script *config.sh* com as seguintes informações:
  - a. senha de acesso SSH ao ponto de acesso;
  - b. SSID e configuração da segurança da rede sem fio
  - c. IP do servidor de *log* para o qual o AP enviará seu *log*
  - d. email de contato do administrador da rede que será inserido na configuração do servidor SNMP do AP.
- 4) Executar o script *config.sh*;

Cada passo listado será visto nas próximas seções.

### **3.3.1.1. Instalando programas sshpass e expect**

Instale os programas sshpass e expect através dos comandos:

- Caso seu sistema seja Centos, Red-Hat, Fedora, ou outro baseado em um destes:  

```
yum install sshpass
yum install expect
```
- Caso seu sistema seja baseado em Debian, Ubuntu:  

```
apt-get install sshpass
apt-get install expect
```

### **3.3.1.2. Gerando par de chaves pública e privada**

Gere o par de chaves SSH pública e privada que serão utilizadas para a comunicação entre o controlador e o ponto de acesso através dos comandos:

```
su -
Password: // digite a senha de root
cd /root
ssh-keygen -t rsa -f controller_key_nova
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase): // Deixe este campo vazio
Enter same passphrase again: // Deixe este campo vazio
Your identification has been saved in controller_key_nova.
Your public key has been saved in controller_key_nova.pub.
The key fingerprint is:
1e:22:3e:28:66:ae:0c:56:67:7f:52:d9:d8:db:e1:98
root@controlador-SciFi
The key's randomart image is:
```

```
+--[ RSA 2048]----+
|                   |
|                   |
|                   |
|       =          |
|   ..o. S+ o .   |
|   .oo...o... * . |
|o+. o o.. E o   |
|B. . o          |
|oo              |
+-----+
```

Neste comando, *-t* representa o tipo da chave e *-f* representa o nome do arquivo. O comando irá gerar dois arquivos:

- *controller\_key\_nova* - chave privada que deve ser instalada no controlador;
- *controller\_key\_nova.pub* - chave pública que deve ser instalada em todos os pontos de acesso da rede.

O conteúdo do arquivo *controller\_key\_nova* será parecido com este:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQE Ary3e0k4K6SKZgJKA+Nzh1U2tTjoLgp2RxAiAIPG2Usq+VWaI
VUCsqcrmuXWWqyMj2dRHieR1a2wJUk0XzwuegGgo3J/NP8J5VbMHG9L2Ddz8YW59
sZUqeLDrzZqqB2z+W/c/erfZJhVkJDUUz62N5PENalhKjVBCd2gK5ZPAjCqDVjfWI
L89711kKz8Fs/hmfp8jSXQkDLr7dkc3Y7PWYvo6NtnOqqj+8XQI+71SWkMCMYIHE
DZChvBXCKijGm6SZCWlbZieIX+Zggh+2FdTpSLV15Z/Ijo0NEkAXi4YiDL29q+uX
4Lp6dmnKIgo6lB5mwfII6s9ubTJ1whexjoG1/QIBIwKCAQBFGoasrgXsRfuO8HHm
Ls0876c5GDIiVYmk7qv0oHjrHZqGIcd3b8fJ4yzLE/K0rK0P2aMtmUcObdksrYH0
DZ8vw4Ple1Ip7TqNm7Nm4Dxt7P4JAXdvB9U6NCg9S7tjHeqjnCnGRovS2GmDi/ed
Ch09+K2Eqwg08xPcv6Z4n53+c6sVk8PungoxOkGlqczaK/EkESPT0S39OUDRyBgG
n7Yg8zWjBS2wyCoStGKvMCnZESe5C1z158y4cUM7dq54N6yXccy0cd9HVGTmEsDk
87rnTqhP+GHXXrElOesXza3KhvZQ1uh6Jego2LSQRrs+/SwZ28s8ERvLoi7kJfx1
9AHLAoGBANxf2Q5rkUOGVm5T2Ubzs14Wb0gI5nxI6HiMffDvsx0AihTlf12AlYZQ
07nq5nz3RIDJAWE23Svf2Q7RRwWPvMMQ/+226vwgnjAB55kp0To7iO+vb85/vb1
nO09sg9XOYZKF0EFSF66ZpTzSlmrQaJ2NPx0z7Ik8+nxzAWBmxsxAoGBAMt/oHyg
5TMCzTEHXpA74Hxp26alhj+n1Vln7Mk0bR7EsD5uw1dPzbKmW35izjhM/iC75Le1
7YNnWe+O0yXC5CSwP8DpnB6ANDtdpLRcRD8CvRmTkcdIxLT0EA1y0nRAckeJi9MH
601V01Ra30SdQEqi11K2ged1Vvf2ILEvaHyNAoGBAKoAzAPPUs2wx1UcHKRy2g4R
TogG3bBVgCJ7AhGi9+MsTUNR88R5IuP1NZ4M+vKwHucBdhfLPOdkEdD6hcU1u4hL
```

```

SmYt+esJ/j/kmCm7XHb81PcA24TjmM0Xh6+zQDe4UPeUlZiPC/FN91z2Mgqorvmr
pTfH02wrIo/majAiJzI7AoGBAL/eu+M4nZZ++/sG8sKBmSTY1mnshQ+6+aVL7Zk
oWYnKdR3D/M8nV9MZOTgbwHiMW9SEimORldS0SOyjJFRWsOBmzI7WK8LKe7Uopts
7+OjfxgdbCrkcFLMLGRzkzpopLUXoRdt25osWJitc2yUQ+6ZiTC6tP6+oqIFUgYl
YoQPAoGBAMzjG1G3Y2Oca94jgtXmVteDXudsM74AHzaHdjtoVYtDFHCrxJCvkSlJ
Hi8qLT3FOKOL0D4eV5xicc14GRtxp/1y7BI2EUJ1DcsmxZePI5RRwFHhNtb7I1NH
6VPC0muYbmH76JjS17yzxH3pDaxpL4g7+JTIqnjyVYbucbFERmpO
-----END RSA PRIVATE KEY-----

```

E o conteúdo do arquivo *controller\_key\_nova.pub* será parecido com este:

```

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAry3e0k4K6SKZgJKA+Nzh1U2tTjoLgp2RxAiAIPG2Us
q+VWalVUcsqcrmuXWWqyMj2dRHieR1a2wJUk0XzwuegGgo3J/NP8J5VbMHG9L2Ddz8YW59
sZUqeLDrzZqqB2z+W/c/erfZJhVkJDUUz62N5PENalhKjVBCd2gK5ZPAjCqDVjfWIL89711
kKz8Fs/hmxp8jSXQkDLr7dkc3Y7PWYvo6Ntn0qqj+8XQI+71SwkMCMyIHEDZChvBXCKijG
m6SZCWlbZiEiX+Zggh+2FdTpSLV15Z/IjoONEkAXi4YiDL29q+uX4Lp6dmnKIgo61B5mwf
II6s9ubTJ1whexjoG1/Q== root@controlador-SciFi

```

Agora renomeie as chaves para o padrão através dos comandos:

```

mv controller_key_nova controller_key
mv controller_key_nova.pub authorized_keys

```

Por fim, copie a chave pública para a pasta “arquivos” do pacote de instalação autotático do AP: (obs: Substitua **CAMINHO\_DO\_PACOTE**, pelo caminho da pasta em que o pacote de configuração automática do AP foi *deszipado*.)

```
cp authorized_keys CAMINHO_DO_PACOTE/arquivos
```

### 3.3.1.3. Configurando o script config.sh

Este *script* realiza a instalação de pacotes e altera arquivos de configuração do AP. Antes de utilizá-lo é necessário passar ao *script* algumas informações. Abra o *script* e preencha a “seção de configuração do *script*”, conforme os textos explicativos acima de cada variável. Insira os valores entre as aspas ‘’. As variáveis a configurar são:

- SYS\_CONTACT** : contato (email) do administrador da rede que será inserido na configuração do servidor SNMP do AP.
- SENHA** : senha de acesso SSH ao ponto de acesso;
- LOG\_SERVER** : IP do servidor de *log* para o qual o AP enviará seu *log*
- SSID** : SSID da rede sem fio
- ENCRYPTION** : tipo da segurança sem fio (none, psk2 ou wpa2)
- KEY** : chave compartilhada da rede sem fio ou chave para acesso do AP ao Radius
- SERVER** : IP do servidor Radius, caso a ENCRYPTION seja wpa2
- PORT** : Porta do servidor Radius, caso a ENCRYPTION seja wpa2

A seguir, veja o formato da seção de configuração do *script*:

```
#####
# Seção de configuração do script          #
#####

# Antes de iniciar, gere a chave SSH para comunicação entre o servidor e o AP e
# coloque-a na pasta "arquivos". Esta chave será configurada no AP por este script
# O script necessita que os programas "sshpass" e "expect" estejam instalados.
# Instale-os através dos comandos "yum install sshpass" e "yum install expect"
# A seguir, preencha as variáveis abaixo com os valores desejados:

# Email do administrador (usado no arquivo de configuração do snmpd do AP)
SYS_CONTACT=''

# Senha de acesso SSH ao AP (usada por este script para acessar o AP)
SENHA=''

# Ip do servidor de log para o qual AP enviará seu syslog
LOG_SERVER=''

# SSID da rede sem fio do AP
SSID=''

# Tipo de segurança da rede sem fio do AP:
# none - rede aberta;
# psk2 - wpa2 com chave compartilhada
# wpa2 - wpa2 enterprise com autenticação via Radius;
# ENCRYPTION=''

# Chave de segurança
# Caso a segurança seja none, esta opção não deve ser preenchida
# Caso a segurança seja psk2, esta será a chave compartilhada para acesso à rede sem
# fio. A chave necessita ter entre 8 e 63 caracteres.
# Caso a segurança seja wpa2, esta será a chave compatilhada para acesso do AP ao
# Radius.
KEY=''

# IP do servidor Radius
# Caso a segurança seja none ou psk2, esta opção não deve ser preenchida
# Caso a segurança seja wpa2, este será o endereço IP do servidor Radius.
SERVER=''

# Porta do servidor Radius
# Caso a segurança seja none ou psk2, esta opção não deve ser preenchida
# Caso a segurança seja wpa2, este será a porta do servidor Radius.
PORT=''

#####

```

### 3.3.1.4. Executando o script config.sh

O script *config.sh* necessita dos seguintes parâmetros para execução:

- a. IP atual do AP (EX.: 192.168.1.1)
- b. *Hostname* que será configurado no AP (EX.: ap0001)
- c. Localização do AP. Este parâmetro será utilizado pelo SNMP do AP. (EX.: "Lab de Redes") Obs.: Caso os parâmetros possuam mais de uma palavra, utilize aspas "" para agrupá-las.

Após definidos os parâmetros, entre na pasta em que se encontra o script *config.sh* e execute o script através dos comandos:

```
su -
Password: // digite a senha de root
./config.sh 192.168.1.1 ap0001 "Lab de Redes"
```

O resultado deve ser parecido com este:

```
adicionando estação ao known_hosts
spawn ssh root@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA key fingerprint is d1:93:ab:ea:3d:bb:0f:22:1a:7d:0f:8c:ad:a2:73:ae.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
root@192.168.1.1's password: copiando authorized_keys
copiando pacotes para /tmp
desinstalando dnsmasq e wpad-mini, criando pasta /etc/scripts e instalando pacotes
Removing package dnsmasq from root...
Removing package wpad-mini from root...
Installing hostapd (20120910-1) to root...
Configuring hostapd.
Installing libelf (0.8.13-1) to root...
Configuring libelf.
Installing snmpd-static (5.4.2.1-5) to root...
Configuring snmpd-static.
Installing wireless-tools (29-5) to root...
Configuring wireless-tools.
Connection to 192.168.1.1 closed.
  copiando scripts para pasta /etc/scripts
  copiando rc.local /etc/
  copiar dropbear para /etc/config
  criando arquivo snmpd
  atualizando /etc/config/snmpd
  removendo arquivo snmpd intermediário criado
  criando arquivo network
  copiando network para a pasta /etc/config
  removendo arquivo network intermediário criado
  copiando root para pasta /etc/crontabs/
  copiando script de configuração do wireless para /tmp
  criando arquivo system
  copiando system para /etc/config/
alterando permissões dos scripts, authorized_keys, network , crontabs, rc.local,
dropbear, desabilitando snmpd; habilitando cron; criando arquivo
/etc/config/wireless; alterando arquivo /etc/config/wireless; rebootando AP;
Connection to 192.168.1.1 closed.
```

Neste ponto, seu AP já estará configurado.

Caso o resultado a seguir seja obtido, aperte “ctrl+c” para parar a execução do script e apague a linha especificada do arquivo “/root/.ssh/known\_hosts”: (obs.: Neste exemplo a linha era 16)

```
@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack) !
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d1:93:ab:ea:3d:bb:0f:22:1a:7d:0f:8c:ad:a2:73:ae.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:16
RSA host key for 192.168.1.1 has changed and you have requested strict
checking.
Host key verification failed.
```

### **3.3.2. Configuração sem utilização do pacote de configuração automática**

#### **3.3.2.1. Configuração da rede sem fio (wireless)**

Através do arquivo *wireless*, que se encontra no diretório */etc/config/* do ponto de acesso, as configurações da interface sem fio podem ser realizadas. Neste *link* encontra-se a documentação de configuração disponibilizada pelo OpenWrt:

\* <http://wiki.openwrt.org/doc/uci/wireless>

Caso o arquivo não exista, para gerá-lo automaticamente (ou voltar às configurações originais), execute o comando dentro do AP:

```
wifi detect > /etc/config/wireless
```

Basicamente, o que deve ser configurado neste arquivo é:

- SSID do AP (option SSID)
- Segurança do AP (option encryption). Dependendo do tipo de segurança a ser utilizado, novas opções deverão ser inseridas.

Algumas possibilidades de valores para “option encryption” são:

none: rede sem fio aberta.

psk2: rede com autenticação WPA2 e chave compartilhada.

wpa2: rede com autenticação WPA2-enterprise.

Ao utilizar autenticação psk2 é necessário definir a senha compartilhada através da linha:

```
option key chavecompartilhada
```

A chave deve conter entre 8 e 63 caracteres.

Ao utilizar a autenticação wpa2, é necessário inserir as seguintes opções:

```
option key chave_de_acesso_ao_radius
option server IP_do_servidor_radius
option port porta_do_servidor_radius
```

A seguir é mostrado um exemplo de arquivo *wireless* retirado de um *Nanostation M2 Loco*:

```
config wifi-device radio0
    option type      mac80211
    option channel   1
    option macaddr   00:15:6d:3a:34:50
    option hwmode    11ng
    option htmode    HT20
    option beacon_int 170
```

```

        list ht_capab      SHORT-GI-20
        list ht_capab      SHORT-GI-40
        list ht_capab      TX-STBC
        list ht_capab      RX-STBC1
        list ht_capab      DSSS_CCK-40

config wifi-iface
    option device    radio0
    option network   lan
    option mode      ap
    option ssid      GTSciFi
    option encryption none

```

### **3.3.2.2. Configuração Network**

Através do arquivo *network*, que se encontra no diretório */etc/config/* do ponto de acesso, configurações da interface cabeada do ponto de acesso podem ser realizadas. Neste link encontra-se o manual de configuração:

<http://wiki.openwrt.org/doc/uci/network>

Basicamente, o que deve ser configurado é o IP da interface lan.

Caso o IP seja estático, as seguintes opções devem ser inseridas:

- Tipo do IP (*option proto 'static'*)
- IP do AP (*option ipaddr 'IP\_DO\_AP'*)
- Máscara de subrede (*option netmask 'MASCARA\_DE\_SUBREDE'*)
- Gateway (*option gateway 'IP\_DO\_GATEWAY'*)

Caso o IP seja obtido por DHCP, as seguintes opções devem ser inseridas:

- Tipo do IP (*option proto 'dhcp'*)
- Hostname do AP (*option hostname 'HOSTNAME\_DO\_AP'*)
- O MAC que será utilizado pela interface *bridge* (*option macaddr 'MAC'*).

Nesta opção, insira o Mac da interface cabeada do AP.

A seguir é apresentado um exemplo de arquivo *network* retirado de um *Nanostation M2 Loco*:

```

config interface 'loopback'
    option ifname 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'

```

```

option netmask '255.0.0.0'

config interface 'lan'
    option ifname 'eth0'
    option type 'bridge'
    option proto 'dhcp'
    option hostname 'ap0010'
    option macaddr '00:15:6d:3a:34:51'

```

Caso seu AP possua mais de uma interface cabeada e você queira inserí-las na mesma *bridge*, insira o nome delas na “option ifname”, por exemplo:

```
option ifname 'eth0 eth1'
```

### 3.3.2.3. Instalação dos pacotes necessários

Algumas imagens do OpenWrt não possuem os pacotes necessários para o funcionamento do SciFi.

Por exemplo, a versão 12.09 do OpenWrt com arquitetura AR71XX necessita dos seguintes pacotes adicionais:

- Wireless-tools : ferramentas para verificar e configurar parâmetros da rede sem fio;
- Snmpd-static : SNMP *deamon*
- Hostapd : funcionalidades de AP com suporte a autenticação wpa2-enterprise.

Além de instalar os pacotes, é necessário instalar também suas dependências.

Por padrão, as imagens incluem o pacote *wpad-mini*, porém este não suporta a autenticação wpa2-enterprise. Portanto, optamos por substituí-lo pelo pacote *hostapd*. Optamos também por desinstalar o pacote *dnsmasq*, já que não iremos utilizar o AP como servidor DHCP.

Os pacotes podem ser instalados de dois modos:

- *online* : o AP possui conexão com a internet;
- *offline* : o AP não possui conexão com a internet;

O modo de instalação de pacotes mais simples é o *online*. Após conectar o AP à internet, acesse seu terminal via SSH e digite os seguintes comandos:

```

opkg update
opkg install wireless-tools
opkg remove wpad-mini

```

```
opkg install hostapd  
opkg install snmpd-static  
opkg remove dnsmasq
```

No modo *online*, as dependências são instaladas automaticamente pelo *opkg*. Caso deseje apenas desabilitar o pacote *dnsmasq*, sem removê-lo, execute o comando:

```
/etc/init.d/dnsmasq disable
```

Para realizar a instalação de pacotes no modo *offline*, é necessário primeiro obter, no site do OpenWrt, os pacotes e suas dependências e, a seguir, instalá-los. O passo a passo para a instalação *offline* é:

1) Procurar o ponto de acesso na lista de hardware suportados

\* <http://wiki.openwrt.org/toh/start>

2) Encontrar o seu ponto de acesso e verificar o valor inserido em sua coluna "target". Por exemplo, *Nanostation M2* possui *target* "ar71XX"

3) Ir ao site de download do OpenWrt

\* <http://downloads.openwrt.org/>

4) Escolher a pasta com a versão do firmware de interesse (por exemplo, backfire, kamikaze, etc.)

As últimas versões, mas que ainda não foram lançadas, estão na pasta "snapshots".

5) A seguir, escolher a pasta que contém o "target" do AP em questão. Por exemplo, a do *Picostation M2* seria a "ar71XX".

6) Entre na pasta "packages", procure o pacote desejado e faça o *download*.

7) Transfira (por *scp*) o pacote para a pasta */tmp* do ponto de acesso.

8) Utilize o comando *opkg install* no AP para instalar o pacote. Caso necessite de dependências, baixe-as e as instale primeiro. Uma lista completa dos pacotes, com descrição e dependências pode ser encontrada no arquivo "Packages", na mesma pasta dos pacotes.

Considerando a versão 12.09 do OpenWrt, arquitetura AR71XX, e que os pacotes necessários são *hostapd*, *wireless-tools* e *snmpd-static*, os comandos executados para instalação dos pacotes serão:

```
opkg install wireless-tools_29-5_ar71xx.ipk  
opkg remove wpad-mini  
opkg install hostapd_20120910-1_ar71xx.ipk  
opkg install libelf_0.8.13-1_ar71xx.ipk  
opkg install snmpd-static_5.4.2.1-5_ar71xx.ipk  
opkg remove dnsmasq
```

### **3.3.2.4. Instalação dos scripts SciFi**

Obtenha os scripts que serão instalados nos APs no site:

<http://www.midiacom.uff.br/br/downloads-scifi>

Para obter versões mais atuais, entre no grupo de discussões sobre o SciFi voltado para a comunidade e peça informações:

<https://groups.google.com/forum/?hl=pt-PT#!forum/gtscifi-community>

Após obter os scripts, conecte-se ao AP via SSH e crie a pasta /etc/scripts. A seguir, copie os scripts, via SCP, para esta pasta.

Abra o script *ap\_type.sh* para edição. Neste script, insira o modelo do AP na linha MODELO. Caso o modelo do AP fosse TL-WR740N, o resultado seria:

```
MODELO='TL-WR740N'
```

Por fim, configure a permissão dos *scripts* para 755 através do comando:

```
chmod 755 /etc/scripts/*
```

### **3.3.2.5. Instalação da chave SSH pública**

Execute os passos listados na seção 3.3.1.2 para gerar as chaves pública e privada.

Após gerar as chaves, copie a chave pública (*authorized\_keys*) para a pasta /etc/dropbear do AP via SCP.

A seguir, mude a permissão da chave para 0600 através do comando:

```
chmod 0600 /etc/dropbear/authorized_keys
```

### **3.3.2.6. Configuração do SNMpd**

O arquivo de configuração do SNMpd está localizado no diretório /etc/config/snmpd do AP. Abra este arquivo para edição e faça as seguintes alterações:

- 1) Comente o bloco “config exec”. O resultado será:

```
#config exec
#    option name filedescriptors
#    option prog /bin/cat
#    option args /proc/sys/fs/file-nr
#    option miboid      1.2.3.4
```

- 2) Preencha o bloco “config system”. O resultado será parecido com o a seguir, substituindo os valores de sysLocation, sysContact e sysName:

```
config system
    option sysLocation      'Localização do AP'
    option sysContact       'email do administrador do sistema'
```

```

        option sysName      'hostname do AP, ex: AP0001'
#       option sysServices    72
#       option sysDescr       'adult playground'
#       option sysObjectID   '1.2.3.4'

```

3) Inclua no final do arquivo as seguintes configurações:

```

config exec
        option name      SCIFI
        option prog     /bin/sh
        option args    /etc/scripts/SCIFI.sh

config exec
        option name      n_StationNumber
        option prog     /bin/sh
        option args    /etc/scripts/nsta.sh

config exec
        option name      AP_Type
        option prog     /bin/sh
        option args    /etc/scripts/ap_type.sh

```

Estas configurações são responsáveis por disponibilizar em OIDs os resultados dos *scripts* listados em “option args”. Para verificar o resultado, execute no servidor o seguinte comando, substituindo IP\_DO\_AP pelo IP do AP:

```

[root@wifi ~]# snmpwalk -v 1 -c public IP_DO_AP .1.3.6.1.4.1.2021.8
UCD-SNMP-MIB::extIndex.1 = INTEGER: 1
UCD-SNMP-MIB::extIndex.2 = INTEGER: 2
UCD-SNMP-MIB::extIndex.3 = INTEGER: 3
UCD-SNMP-MIB::extNames.1 = STRING: SCIFI
UCD-SNMP-MIB::extNames.2 = STRING: n_StationNumber
UCD-SNMP-MIB::extNames.3 = STRING: AP_Type
UCD-SNMP-MIB::extCommand.1 = STRING: /bin/sh /etc/scripts/SCIFI.sh
UCD-SNMP-MIB::extCommand.2 = STRING: /bin/sh /etc/scripts/nsta.sh
UCD-SNMP-MIB::extCommand.3 = STRING: /bin/sh /etc/scripts/ap_type.sh
UCD-SNMP-MIB::extResult.1 = INTEGER: 11 // Versão do SciFi
UCD-SNMP-MIB::extResult.2 = INTEGER: 3 //Número de estações associadas
UCD-SNMP-MIB::extResult.3 = INTEGER: 0
UCD-SNMP-MIB::extOutput.1 = STRING: SCIFI //AP é compatível com SciFi

```

```

UCD-SNMP-MIB::extOutput.2 = STRING: 3
UCD-SNMP-MIB::extOutput.3 = STRING: TL-WR740N // Modelo do AP
UCD-SNMP-MIB::extErrFix.1 = INTEGER: noError(0)
UCD-SNMP-MIB::extErrFix.2 = INTEGER: noError(0)
UCD-SNMP-MIB::extErrFix.3 = INTEGER: noError(0)
UCD-SNMP-MIB::extErrFixCmd.1 = STRING:
UCD-SNMP-MIB::extErrFixCmd.2 = STRING:
UCD-SNMP-MIB::extErrFixCmd.3 = STRING:

```

Caso o snmpwalk não esteja instalado no servidor, instale-o através do comando:

```
yum install net-snmp-utils
```

### 3.3.2.7. Configuração do system

No arquivo /etc/config/system, configurações de servidor de tempo, envio de *log* para servidor remoto e leds do AP podem ser realizadas.

A documentação sobre o arquivo system pode ser encontrada em:

<http://wiki.openwrt.org/doc/uci/system>

No SciFi utilizamos as seguintes configurações:

```

config system

    option hostname 'HOSTNAME_DO_AP' //Inserir o hostname do AP
    option timezone 'BRT3BRST,M10.3.0/0,M2.3.0/0' //timezone do Brasil
    option log_port '514' //Inserir a porta do servidor de log
    option log_size '16'
    log_type      'circular'
    option log_ip   'IP_DO_SERVIDOR_DE_LOG' //Inserir o IP do servidor de log

config timeserver 'ntp'

    list server 'a.st1.ntp.br'//Inserir os endereços dos servidores de tempo
    list server 'b.st1.ntp.br'
    list server 'c.st1.ntp.br'
    list server 'd.st1.ntp.br'
    list server 'a.ntp.br'
    list server 'b.ntp.br'
    list server 'c.ntp.br'
    list server 'gps.ntp.br'
    option enable_server '0'
```

As configurações de led padrão de cada modelo de ponto de acesso são mantidas.

### 3.3.2.8. Configuração do rc.local

O arquivo /etc/rc.local pode ser configurado para executar tarefas após o processo de boot do AP. No SciFi, o rc.local é utilizado para retardar a inicialização do snmpd. Isto é feito para que o AP possa obter informações de tempo antes de responder requisições SNMP, de forma que dados de tempo sejam informados de forma correta. Para isto, a seguinte linha deve ser inserida no arquivo:

```
/etc/scripts/init_snmpd.sh &
```

O script *init\_snmpd.sh* é utilizado para aguardar um intervalo de 10 minutos e, a seguir, inicializar o *snmpd*.

### 3.3.2.9. Configuração do dropbear

No arquivo /etc/config/dropbear, configurações do servidor SSH do AP podem ser realizadas. A documentação detalhada de configuração do dropbear no OpenWrt pode ser encontrada no endereço:

<http://wiki.openwrt.org/doc/uci/dropbear>

No SciFi a autenticação SSH entre servidor e AP é realizada através de chaves pública e privada. Desta forma, a autenticação por senha pode ser desabilitada. Para desabilitar o SSH por senha, faça as seguintes configurações no arquivo /etc/config/dropbear:

```
config dropbear
    option PasswordAuth 'off' // desabilitar ssh por senha
    option RootPasswordAuth 'off' // desabilitar ssh por senha para o usuário root
    option Port          '22'
#    option BannerFile   '/etc/banner'
```

## 4. Instalando e configurando o Controlador SciFi

A instalação do SciFi pode ser dividida em quatro etapas:

- Instalação e configuração do banco de dados PostgreSQL
- Instalação e configuração do servidor de aplicações Jboss AS
- Instalação da interface web de gerência do SciFi
- Instalação do Núcleo de Processamento Central do SciFi

As próximas seções abordarão estas quadro etapas.

## 4.1. Banco de dados PostgreSQL

### 4.1.1. Instalando o banco de dados PostgreSQL

O PGDG (*PostgreSQL Global Development Group*), mantém um repositório RPM de pacotes do Postgresql para Centos, Fedora, Redhat e Scientific Linux. Este repositório está localizado em <http://yum.postgresql.org>. Para mais informações, acesse [https://wiki.postgresql.org/wiki/YUM\\_Installation](https://wiki.postgresql.org/wiki/YUM_Installation).

Para configurar o uso deste repositório pelo YUM, abra o arquivo /etc/yum.repos.d/CentOSBase.repo com permissão de root:

```
su -  
// digite sua senha  
vim /etc/yum.repos.d/CentOSBase.repo
```

No final das seções [base] e [updates], adicione a seguinte linha:

```
exclude=postgresql*
```

Obtenha em <http://yum.postgresql.org/repopackages.php> o arquivo RPM disponibilizado pelo PGDG para a distribuição CentOs. A arquitetura utilizada neste tutorial foi a de 64 bits. Neste exemplo, o arquivo será obtido através do seguinte comando:

```
curl -O http://yum.postgresql.org/9.2/redhat/rhel-6-x86_64/pgdg-centos92-9.2-6.noarch.rpm
```

Agora instale o pacote:

```
rpm -ivh pgdg-centos92-9.2-6.noarch.rpm
```

Para listar alguns dos pacotes disponíveis no repositório, use o comando:

```
yum list postgres* pgadmin*
```

Por fim, instale o postgresql através do comando:

```
yum install postgresql92-server.x86_64
```

Para conferir a versão instalada, digite o comando:

```
psql --version
```

Neste tutorial, a versão utilizada foi: **psql (PostgreSQL) 9.2.4**

Para instalar a interface gráfica de administração do postgresql (pgAdmin3), digite o comando:

```
yum install pgadmin3_92.x86_64
```

A versão do pgAdmin3 utilizada foi a **1.16.1**.

O pgAdmin pode ser inicializado através do menu *Aplicativos > Desenvolvimento > Pgadmin III*.

Caso ocorra o erro abaixo:

Falha ao executar processo filho "/usr/bin/pgadmin3\_92" (Arquivo ou diretório não encontrado)

, substitua no arquivo /usr/share/applications/fedora-pgadmin3\_92.desktop a linha:

```
Exec=/usr/bin/pgadmin3_92
```

pela linha:

```
Exec=/usr/bin/pgadmin3
```

O arquivo final ficará assim:

```
[Desktop Entry]
Encoding=UTF-8
Name=pgAdmin III Exec=/usr/bin/pgadmin3
Exec=/usr/bin/pgadmin3
Icon=/usr/share/pgadmin3_92/pgadmin3_92.xpm
Type=Application
Categories=Application;Development;X-Fedora;
MimeType=text/html;
DocPath=/usr/pgsql-9.2/share/pgadmin3/docs/en_US/index.html
Comment=PostgreSQL Tools
X-Desktop-File-Install-Version=0.15
```

#### 4.1.2. Configurando o banco de dados PostgreSQL

Após instalado o postgresql, o banco de dados necessita ser inicializado e configurado.

Para inicializar o banco de dados o seguinte comando deve ser executado somente uma vez com permissão de root:

```
service postgresql-9.2 initdb
```

Após a execução deste comando, os arquivos referentes ao banco de dados podem ser encontrados no diretório **/var/lib/pgsql/9.2/data**. Para que o postgresql seja inicializado automaticamente no boot do sistema, execute como root o comando:

```
chkconfig postgresql-9.2 on
```

Para inicializar o postgresql execute o comando:

```
service postgresql-9.2 start
```

Por padrão, o postgresql será executado pelo usuário postgres, criado automaticamente na instalação do programa. É interessante que a senha deste usuário seja alterada para maior segurança. Para alterar a senha, execute os seguintes comandos como root:

```
passwd postgres
```

A seguir digite e redigite uma senha para este usuário. Após alterar a senha do usuário Unix postgres, altere a senha do usuário de administração e acesso ao banco de dados, que também se chama postgres, substituindo **nova\_senha** pela senha desejada:

```
su - postgres psql postgres
```

```
ALTER USER postgres WITH PASSWORD 'nova_senha';
\q
```

Abra o arquivo **/var/lib/pgsql/9.2/data/pg\_hba.conf** e substitua nas seguintes linhas “ident” por “md5”:

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5 # IPv6 local connections: host all all ::1/128 md5
```

O *ident* deve ser substituído porque é uma forma de autenticação que depende do usuário que está logado no sistema. Por exemplo, se você está logado como *postgres* e tenta se conectar ao banco de dados com outro usuário, a autenticação irá falhar porque este outro usuário não está logado atualmente.

Reinicie o *postgresql* executando o comando:

```
service postgresql-9.2 restart
```

Saia do usuário *postgre* digitando “exit” e logue como root.

Abra o programa *pgAdmin* executando o comando:

```
pgadmin3 &
```

Clique no botão “**Add a connection to a server**”, como mostra a Figura 12:

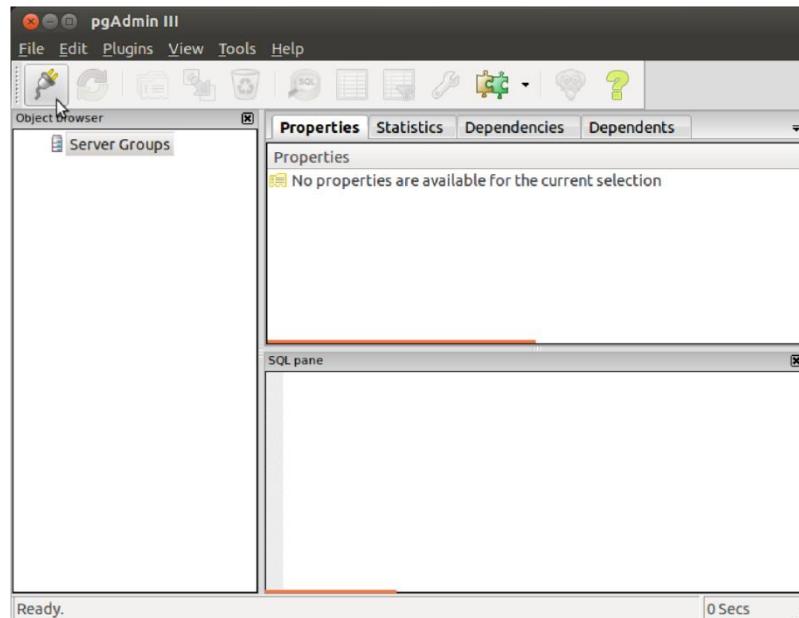


Figura 12 - PgAdmin III – Adicionando conexão com o banco de dados.

Insira as informações conforme mostra a Figura 13:

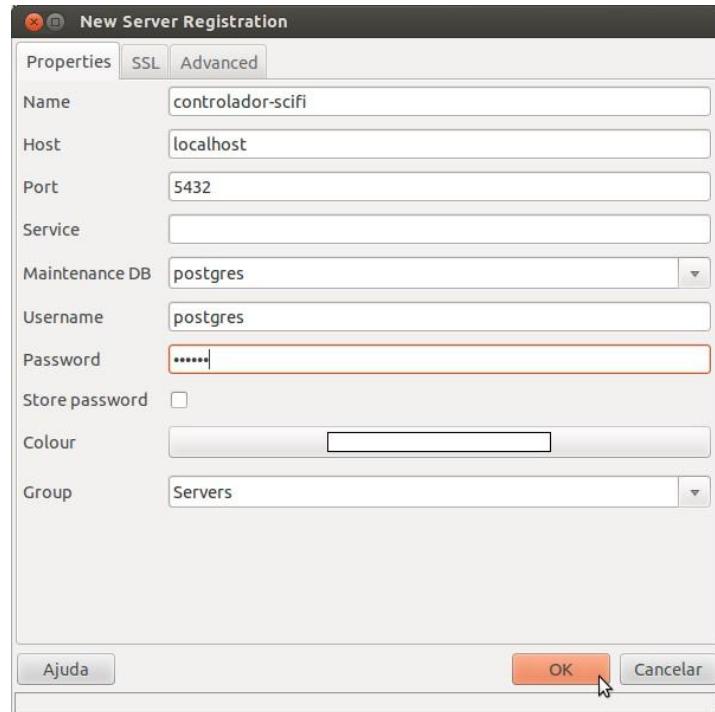
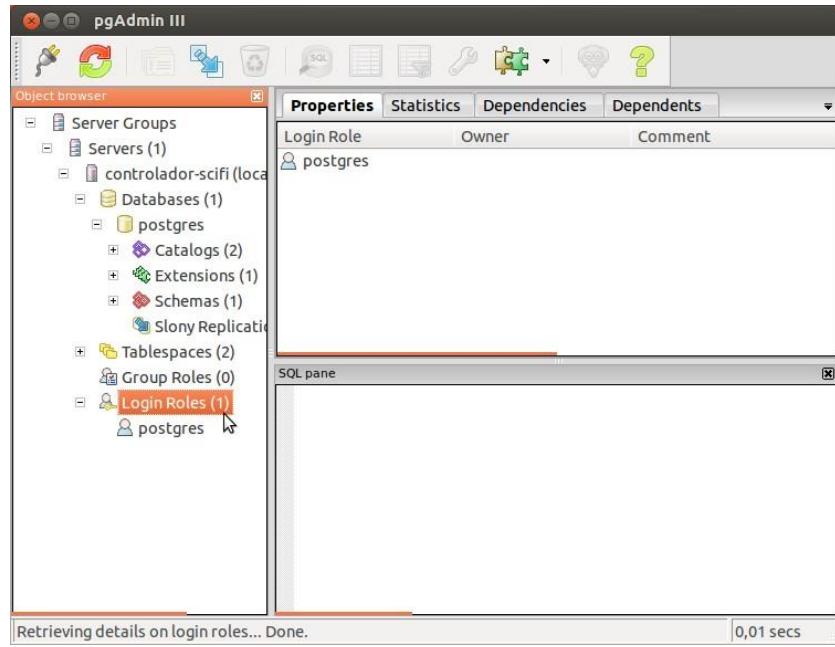


Figura 13 - PgAdmin III - Preenchendo as propriedades da conexão.

No campo “Name” insira um texto para identificar o servidor. O campo “Host” deve ser preenchido com o endereço IP do servidor ou seu nome de domínio. O campo “Maintenance DB” é utilizado para especificar o banco de dados inicial ao qual o pgAdmin irá se conectar. Ao marcar a opção “Store password” a senha será guardada em um arquivo sem nenhum tipo de criptografia. Caso não queria que isto ocorra, **desmarque esta opção**. Desta forma, o programa pedirá sua senha sempre que for reiniciado para se conectar ao banco de dados. Para mais informações:

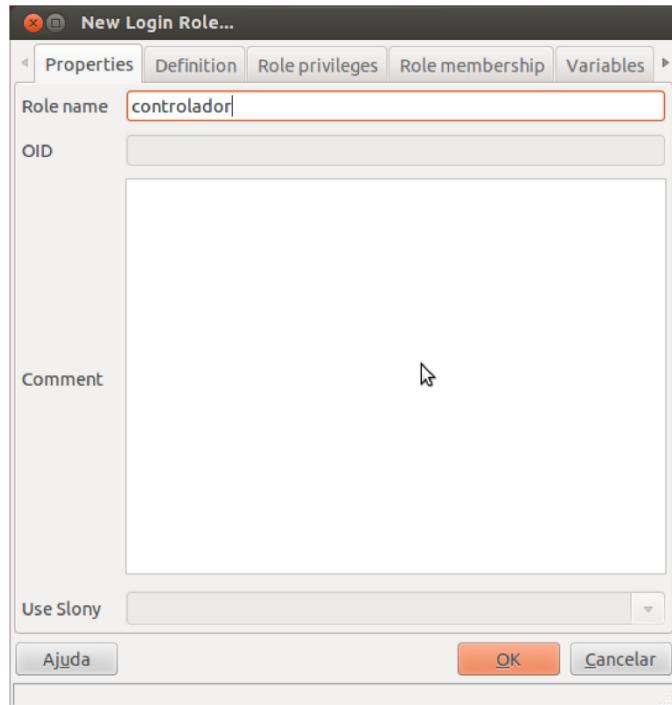
<http://www.pgadmin.org/docs/1.16/connect.html>

Crie um novo usuário clicando com o botão direito em “Login Roles” e a seguir em “New Login Role...” conforme mostra a Figura 14:



**Figura 14 - PgAdmin III - Criando um Login Role**

Na aba “Properties”, no campo “Role name” digite “controlador”, conforme mostra a Figura 15. Este será o usuário utilizado pelo controlador SciFi para acesso ao banco de dados.



**Figura 15 - PgAdmin III - Criando usuário controlador.**

Na aba “Definition”, insira nos campos “Password” e “Password (again)” uma senha para este usuário. A seguir, no campo “Account Expires”, insira a data na qual a senha irá expirar e no campo “Connection Limit” insira -1, conforme mostra a Figura 16:

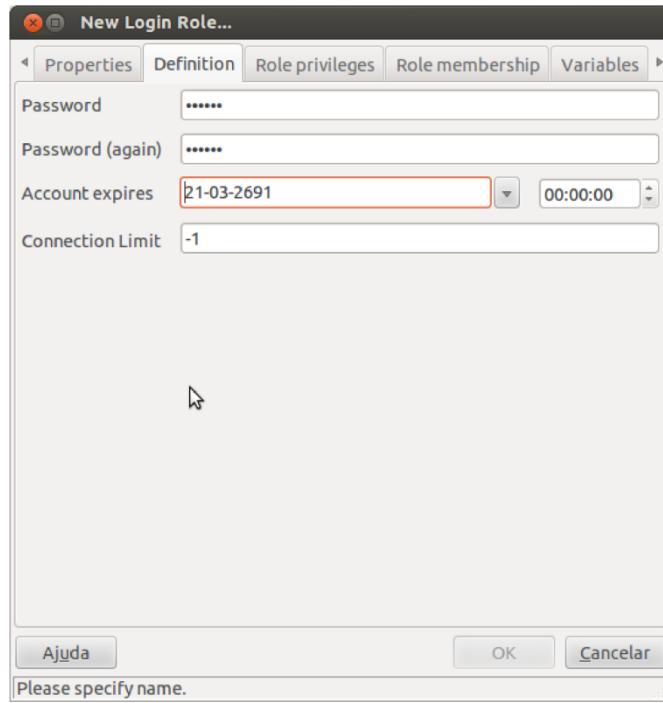


Figura 16 - PgAdmin III - Alterando definições do usuário controlador.

Na aba “Role Privileges”, marque a opção “Inherits rights from parent roles”, e após clique em “OK” conforme mostra a Figura 17:

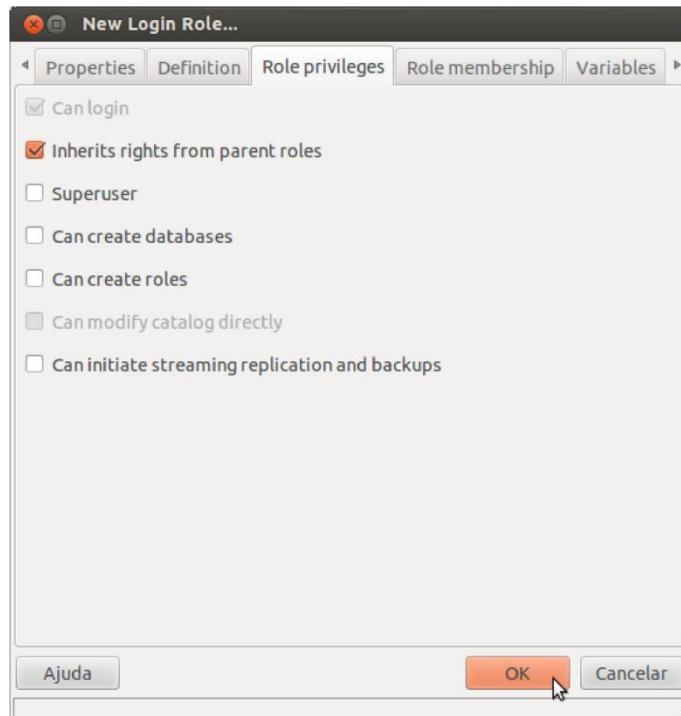


Figura 17 - PgAdmin III - Configurando privilégios do usuário controlador.

Clique com o botão direito sobre a opção “Databases”, e a seguir escolha a opção “New Database...”, conforme mostra a Figura 18:

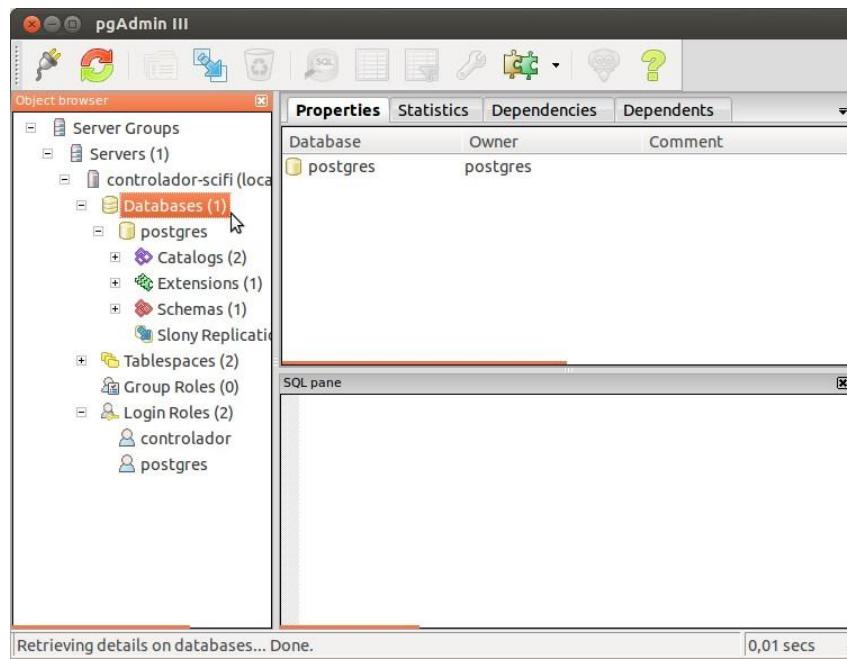


Figura 18 - PgAdmin III - Criando novo banco de dados.

Na aba “Properties”, insira no campo “Name” o nome do novo banco de dados, que será controladorbd. Na opção “Owner”, escolha controlador, conforme mostra a Figura 19:

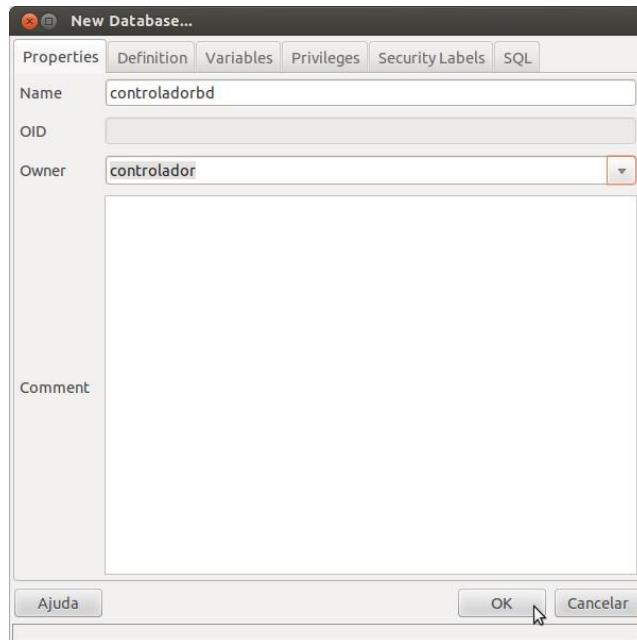


Figura 19 - PgAdmin III - Definindo dono do novo banco de dados.

Na aba “Definition” escolha no campo “Encoding” a opção UTF8, no campo “Template” a opção “template0”, no campo “Tablespace” escolha pg\_default, nos campos “Collation” e “Character Type” escolha pt\_BR.UTF-8, no campo “Connection Limit” escolha insira o valor -1. Por fim, clique em OK, conforme mostra a Figura 20:

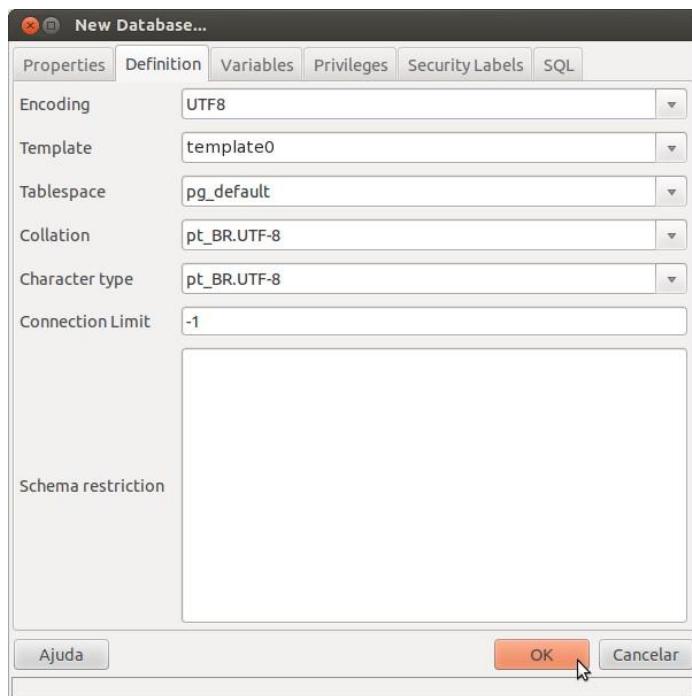


Figura 20 - PgAdmin III - Definições do novo banco de dados.

Faça o download do arquivo que contém a estrutura do banco de dados utilizada pelo SciFi no link: <http://www.midiacom.uff.br/br/downloads-sciFi/controladorbd.backup>

A seguir, clique com o botão direito em “controladorbd” e escolha a opção “Restore...”, conforme mostra a figura Figura 21:

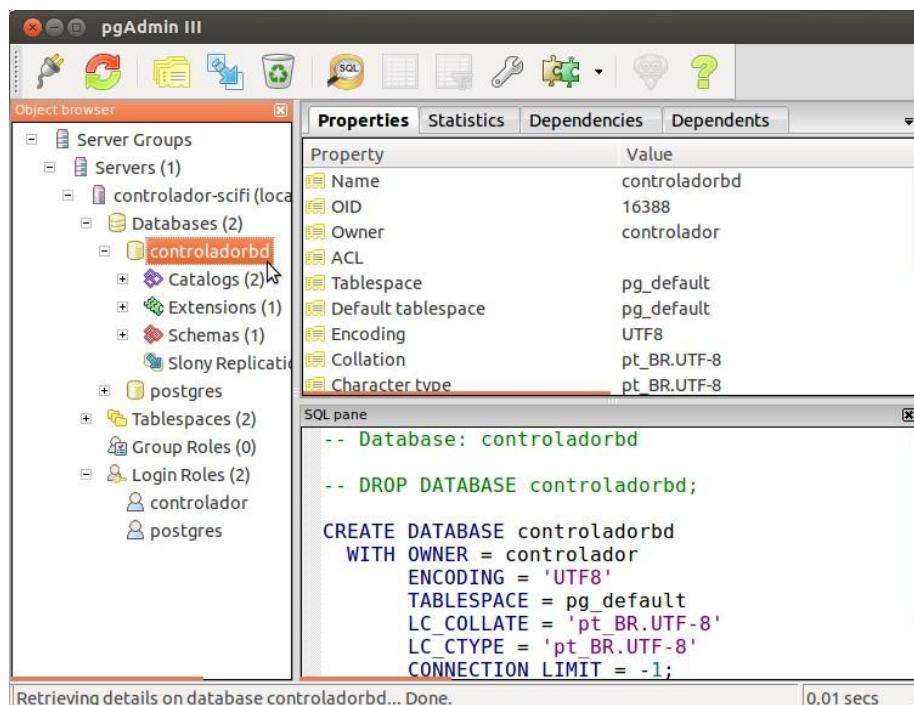


Figura 21 - PgAdmin III - Restaurando o banco de dados.

No campo “Format”, escolha a opção “Custom ou tar” e no campo “Filename”, aponte o local onde o arquivo do banco de dados do SciFi (controladorbd.backup) foi salvo. A seguir, clique em “Restore” conforme mostra a Figura 22:

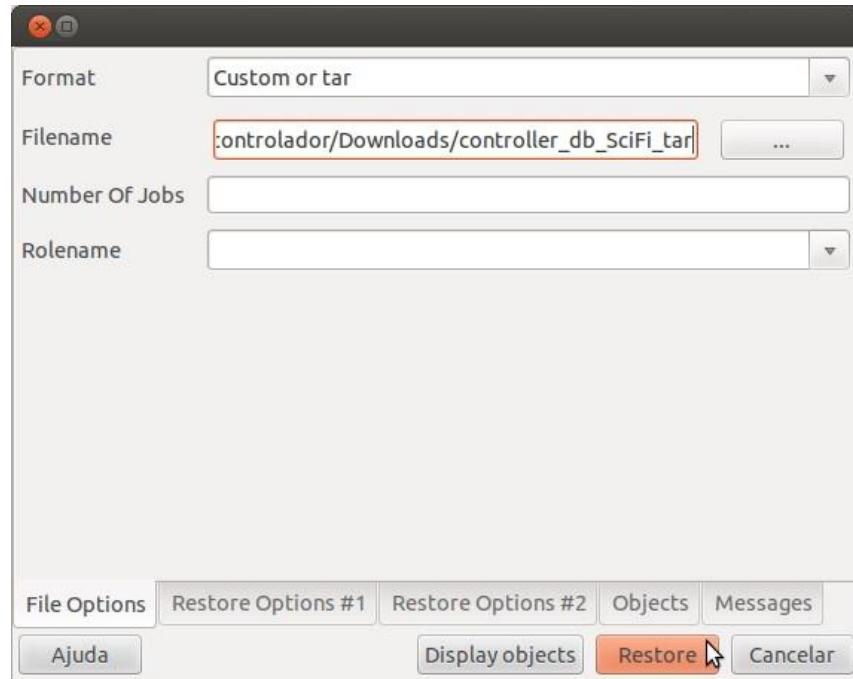


Figura 22 - PgAdmin III - Restaurando o banco de dados (2)

Uma mensagem semelhante à contida na Figura 23 surgirá. Clique em “Done” para finalizar o processo de configuração do banco de dados.

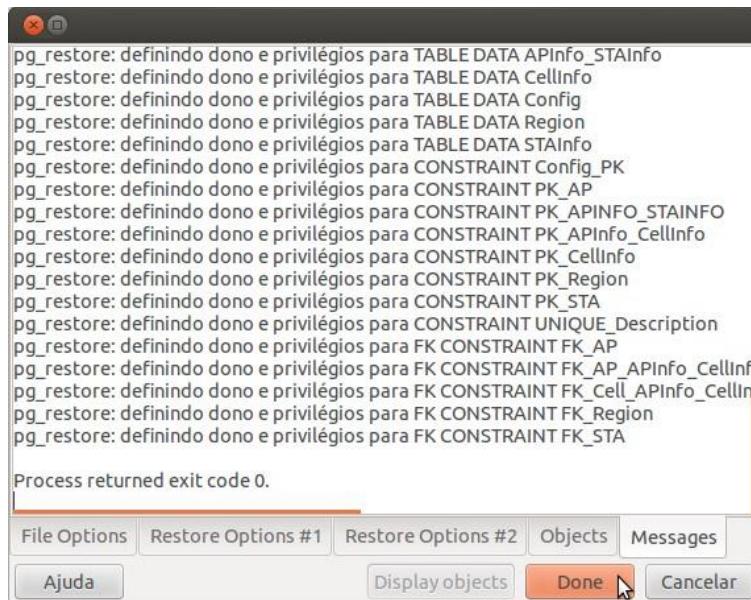


Figura 23 - PgAdmin III - Banco restaurado com sucesso.

## 4.2. Servidor de aplicações JBoss

### 4.2.1. Instalando o JDK

O primeiro passo para a instalação do JBoss no CentOS é a instalação do JDK (*Java Development Kit*). O JDK contém todas as bibliotecas, Máquina Virtual Java e outros componentes contidos na JRE (*Java Runtime Environment*), que permitem a execução de aplicações java. A vantagem do JDK em relação ao JRE é que o primeiro possui funcionalidades adicionais que podem ser necessárias para o funcionamento do JBoss.

Os pacotes java que serão utilizados neste tutorial são os fornecidos pelo OpenJDK:

<http://openjdk.java.net/>

No momento da escrita deste manual, a última versão disponível do JDK é a 7. Para instalar o pacote, execute o comando como root:

```
yum install java-1.7.0-openjdk-devel.x86_64
```

Para verificar a versão instalada execute o comando:

```
java -version
```

No caso deste tutorial, o resultado foi:

```
java version "1.7.0_09-icedtea"  
OpenJDK Runtime Environment (rhel-2.3.8.0.el6_4-x86_64)  
OpenJDK 64-Bit Server VM (build 23.7-b01, mixed mode) v
```

### 4.2.2. Instalando o JBoss AS

O segundo passo para a instalação do Jboss AS é o *download* e a instalação do servidor de aplicação.

Para realizar o download do JBoss AS execute o comando:

```
wget http://download.jboss.org/jbossas/7.1/jboss-as-7.1.1.Final/jboss-as-7.1.1.Final.zip
```

O arquivo também pode ser obtido no site <http://www.jboss.org/jbossas/downloads/>.

A versão 7.1.1 era a última disponível no momento da escrita deste manual.

A instalação do JBoss AS é realizada através da descompactação do arquivo, executando o comando:

```
unzip jboss-as-7.1.1.Final.zip -d /usr/share
```

### 4.2.3. Criação de usuário para inicialização do JBossAS

Como não é indicado que o JBoss seja executado pelo usuário root por questões de segurança, devemos criar um usuário com privilégios apropriados para a execução do programa. Para criar o usuário com nome “jboss”, execute o comando como root:

```
adduser jboss
```

Para definir a senha deste usuário execute o comando e a seguir insira a senha desejada:

```
passwd jboss
```

Agora é necessário configurar o direito de propriedade do diretório no qual o JBossAS foi instalado para o novo usuário:

```
chown -fR jboss.jboss /usr/share/jboss-as-7.1.1.Final/
```

A seguir, troque o usuário utilizado atualmente para o novo usuário jboss através do comando:

```
su jboss
```

Buscando prover maior segurança, as novas distribuições do JBoss AS (7.1.x) não possuem um usuário padrão para acesso ao console de gerência do servidor. Para acessá-lo é necessário que um novo usuário, interno ao JBoss, com permissões administrativas seja criado.

Para adicionar um usuário, o script add-user.sh, incluído na distribuição, pode ser utilizado, como é mostrado a seguir:

```
cd /usr/share/jboss-as-7.1.1.Final/bin/ ./add-user.sh
```

As seguintes mensagens surgirão:

What type of user do you wish to add?

a) Management User (mgmt-users.properties)

b) Application User (application-users.properties)

(a) : **a //Escolha a opção “a”**

Enter the details of the new user to add.

Realm (ManagementRealm) :

Username : jboss // **escreva o nome do usuário. Neste exemplo foi jboss.**

Password : **// digite a senha**

Re-enter Password : **// redigite a senha**

About to add user 'jboss' for realm 'ManagementRealm'

Is this correct yes/no? yes **//Digite sim para confirmar**

Digite “enter” na opção Realm. A seguir, insira o nome do usuário (no exemplo foi jboss) e a senha escolhida. Por fim, digite “yes” para confirmar as informações. Não é necessário reiniciar o servidor ao inserir um novo usuário.

Atualmente não existe um script para exclusão de usuários ou alteração de senha. Caso deseje excluir ou alterar a senha do usuário de gerência criado, acesse os arquivos:

```
/usr/share/jboss-as7.1.1.Final/standalone/configuration/mgmt-users.properties
```

/usr/share/jboss-as-7.1.1.Final/domain/configuration/mgmt-users.properties  
, e apague a linha que se inicia com o nome deste usuário. A seguir, crie o usuário novamente com a nova senha desejada. Para maiores informações acesse:

<https://docs.jboss.org/author/display/AS71/Admin+Guide>

#### 4.2.4. Testando a inicialização do JBoss AS

O JBoss AS 7 possui dois modos de execução, o “standalone” e o “domain”. O primeiro é utilizado quando se deseja executar apenas um servidor. Já o segundo é utilizado para se executar diversos servidores e gerenciá-los a partir de um mesmo ponto de controle. Como no nosso caso desejamos executar apenas um servidor, iremos utilizar o modo “standalone”.

Para inicializar o JBoss no modo “standalone” execute o seguinte comando dentro do diretório **/usr/share/jboss-as-7.1.1.Final/bin/**:

```
./standalone.sh -b 0.0.0.0 -bmanagement 0.0.0.0 &
```

Uma mensagem parecida com esta surgirá:

```
=====
JBoss Bootstrap Environment
JBoss_HOME: /usr/share/jboss-as-7.1.1.Final
JAVA: java
JAVA_OPTS: -server -XX:+UseCompressedOops -XX:+TieredCompilation -Xms64m -Xmx512m -
XX:MaxPermSize?=256m -Djava.net.preferIPv4Stack=true -Dorg.jboss.re
=====
16:44:17,175 INFO [org.jboss.modules] JBoss Modules version 1.1.1.GA
16:44:17,378 INFO [org.jboss.msc] JBoss MSC version 1.0.2.GA
16:44:17,436 INFO [org.jboss.as] JBAS015899: JBoss AS 7.1.1.Final "Brontes" starting
16:44:18,336 INFO [org.xnio] XNIO Version 3.0.3.GA
16:44:18,337 INFO [org.jboss.as.server] JBAS015888: Creating http management service using
socket-binding (management-http)
16:44:18,351 INFO [org.xnio.nio] XNIO NIO Implementation Version 3.0.3.GA
16:44:18,364 INFO [org.jboss.remoting] JBoss Remoting version 3.2.3.GA
16:44:18,387 INFO [org.jboss.as.logging] JBAS011502: Removing bootstrap log handlers
16:44:18,391 INFO [org.jboss.as.configadmin] (ServerService Thread Pool -- 26) JBAS016200:
Activating ConfigAdmin Subsystem
16:44:18,404 INFO [org.jboss.as.clustering.infinispan] (ServerService Thread Pool -- 31)
JBAS010280: Activating Infinispan subsystem.
16:44:18,419 INFO [org.jboss.as.osgi] (ServerService Thread Pool -- 39) JBAS011940:
Activating OSGi Subsystem
16:44:18,431 INFO [org.jboss.as.naming] (ServerService Thread Pool -- 38) JBAS011800:
Activating Naming Subsystem
16:44:18,449 INFO [org.jboss.as.security] (ServerService Thread Pool -- 44) JBAS013101:
Activating Security Subsystem
16:44:18,457 INFO [org.jboss.as.connector] (MSC service thread 1-9) JBAS010408: Starting
JCA Subsystem (JBoss IronJacamar 1.0.9.Final)
```

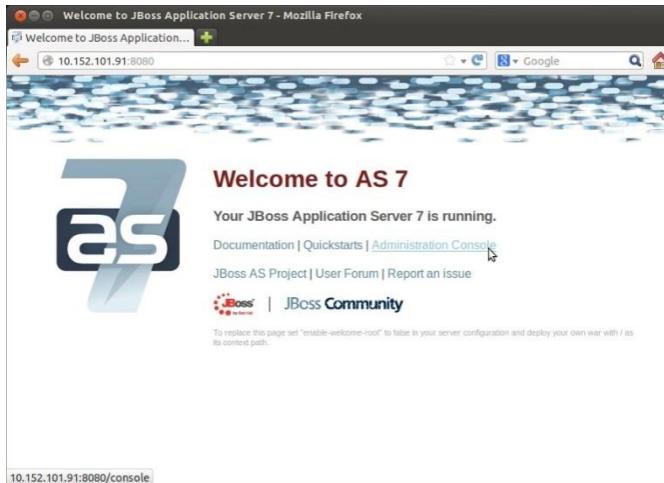
```
16:44:18,487 INFO  [org.jboss.as.security] (MSC service thread 1-1) JBAS013100: Current
PicketBox version=4.0.7.Final
16:44:18,502 INFO  [org.jboss.as.webservices] (ServerService Thread Pool -- 48) JBAS015537:
Activating WebServices Extension
16:44:18,540 INFO  [org.jboss.as.connector.subsystems.datasources] (ServerService Thread
Pool -- 27) JBAS010403: Deploying JDBC-compliant driver class o
16:44:18,555 INFO  [org.jboss.as.naming] (MSC service thread 1-4) JBAS011802: Starting
Naming Service
16:44:18,563 INFO  [org.jboss.as.mail.extension] (MSC service thread 1-4) JBAS015400: Bound
mail session [java:jboss/mail/Default]
16:44:18,670 INFO  [org.jboss.ws.common.management.AbstractServerConfig] (MSC service
thread 1-3) JBoss Web Services - Stack CXF Server 4.0.2.GA
16:44:18,744 INFO  [org.apache.coyote.http11.Http11Protocol] (MSC service thread 1-15)
Starting Coyote HTTP/1.1 on http--0.0.0.0-8080
16:44:19,032 INFO  [org.jboss.as.remoting] (MSC service thread 1-15) JBAS017100: Listening
on /0.0.0.0:4447
16:44:19,034 INFO  [org.jboss.as.remoting] (MSC service thread 1-13) JBAS017100: Listening
on /0.0.0.0:9999
16:44:19,036 INFO  [org.jboss.as.server.deployment.scanner] (MSC service thread 1-6)
JBAS015012: Started FileSystemDeploymentService for directory /usr
16:44:19,062 INFO  [org.jboss.as.connector.subsystems.datasources] (MSC service thread 1-9)
JBAS010400: Bound data source [java:jboss/datasources/ExAMPL
16:44:19,177 INFO  [org.jboss.as] (Controller Boot Thread) JBAS015951: Admin console
listening on http://0.0.0.0:9990
16:44:19,178 INFO  [org.jboss.as] (Controller Boot Thread) JBAS015874: JBoss AS 7.1.1.Final
"Brontes" started in 2309ms - Started 133 of 208 services (74 services are passive or on-
demand)
```

Por padrão, o JBoss aceita apenas conexões do servidor local (localhost). Ao definir os parâmetros -b e -bmanagement como 0.0.0.0, permitimos o acesso do servidor e de sua interface de configuração via internet, respectivamente.

Para testar se o JBoss inicializou corretamente, tente acessar o servidor através de seu navegador web digitando o endereço:

`http://seu_IP:8080`

Uma tela como a da figura abaixo surgirá:



**Figura 24 - Bem Vindo ao JBoss AS 7**

Clique em “Administration Console” para acessar o console de gerência do JBoss. A seguir insira o usuário (jboss) e senha criados anteriormente.

Caso deseje finalizar o servidor JBoss, execute o seguinte comando dentro do diretório **/usr/share/jboss-as-7.1.1.Final/bin/**:

```
./jboss-cli.sh --connect command=:shutdown
```

### 4.3. Interface web do SciFi

#### 4.3.1. Instalando o driver JDBC para acesso ao banco de dados

O driver JDBC é um componente que permite que a aplicação JAVA interaja com o banco de dados. No caso do SciFi, o banco de dados é o postgresql. Para instalar o JDBC do postgresql, mude o usuário para o usuário de gerência do JBoss:

```
su jboss
```

Crie dois novos diretórios relativos ao novo módulo que será instalado:

```
mkdir /usr/share/jboss-as-7.1.1.Final/modules/org/postgresql
mkdir /usr/share/jboss-as-7.1.1.Final/modules/org/postgresql/main
```

Crie um arquivo chamado “**module.xml**” no diretório “**main**” recém criado com o seguinte conteúdo:

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="org.postgresql">
<resources>
    <resource-root path="postgresql-9.2-1002.jdbc4.jar"/>
</resources>
<dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
```

```
<module name="javax.servlet.api" optional="true"/>
</dependencies>
</module>
```

O driver JDBC para o postgresql pode ser obtido no site <http://jdbc.postgresql.org/download.html>. A última versão disponível no momento da escrita deste manual era a postgresql-9.2-1002.jdbc4.jar.

Para fazer o download, utilize o navegador web ou digite o seguinte comando:

```
wget http://jdbc.postgresql.org/download/postgresql-9.2-1002.jdbc4.jar
```

Mova o driver para o diretório “**main**” recém criado:

```
mv postgresql-9.2-1002.jdbc4.jar /usr/share/jboss-as-7.1.1.Final/modules/org/postgresql/main
Altere as permissões dos arquivos:
```

```
cd /usr/share/jboss-as-7.1.1.Final/modules/org/postgresql/main
chmod 644 *
```

Verifique as permissões com o comando **ls -l**. O resultado deve ser:

```
-rw-r--r-- 1 jboss jboss 360 Mar 19 16:49 module.xml
-rw-r--r-- 1 jboss jboss 579785 Mar 19 16:50 postgresql-9.2-1002.jdbc4.jar
```

Caso o jboss não esteja rodando, digite dentro do diretório **/usr/share/jboss-as-**

### **7.1.1.Final/bin/:**

```
./standalone.sh -Djboss.bind.address=0.0.0.0 -Djboss.bind.address.management=0.0.0.0&
```

Abra o console do JBoss:

```
cd /usr/share/jboss-as-7.1.1.Final/bin
./jboss-cli.sh --connect
```

Execute o comando:

```
/subsystem=datasources/jdbc-driver=postgresql-driver:add(driver-name=postgresql-driver,
driver-class-name=org.postgresql.Driver, driver-module-name=org.postgresql)
```

O resultado deve ser:

```
{"outcome" => "success"}
```

Saia do console digitando “**exit**”.

Fonte:

<http://stackoverflow.com/questions/12403428/how-to-connect-jboss-as-7-1-1-with-postgresql>

### **4.3.2. Configurando a conexão do JBoss com o banco de dados Postgresql**

Digite os seguintes comandos para configurar a variável **CLASSPATH** de forma que aponte para os pacotes **.jar** que realizarão a criptografia da senha de acesso ao banco de dados:

```
export JBOSS_HOME=/usr/share/jboss-as-7.1.1.Final/
```

```
export      CLASSPATH=${JBOSS_HOME}/modules/org/picketbox/main/picketbox-
4.0.7.Final.jar:${JBOSS_HOME}/modules/org/jboss/logging/main/jboss-
logging-3.1.0.GA.jar:$CLASSPATH
```

Criptografe a senha de acesso ao banco de dados do usuário “**controlador**” através do seguinte comando:

```
java org.picketbox.datasource.security.SecureIdentityLoginModule <senha>
,substituindo <senha> pela senha real.
```

Insira no arquivo:

**/usr/share/jboss-as-7.1.1.Final/standalone/configuration/standalone.xml**

o seguinte bloco após a tag <**security-domains**>:

```
<security-domain name="EncryptDBPassword">
  <authentication>
    <login-module
      code="org.picketbox.datasource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username" value="controlador"/>
        <module-option name="password" value="senha_criptografada"/>
      </login-module>
    </authentication>
  </security-domain>
,substituindo "senha_criptografada" pela senha recém criptografada.
```

A seguir, insira o seguinte bloco após a tag <**datasources**> no arquivo **/usr/share/jboss-
as-7.1.1.Final/standalone/configuration/standalone.xml**:

```
<datasource jndi-name="java:/ControllerDB" enabled="true" pool-name="ControllerDB"
use-java-context="true" >
  <connection-url>jdbc:postgresql://localhost:5432/controladorbd</connection-url>
  <driver>postgresql-driver</driver>
  <pool>
    <min-pool-size>5</min-pool-size>
    <max-pool-size>20</max-pool-size>
    <prefill>true</prefill>
  </pool>
  <security>
    <security-domain>EncryptDBPassword</security-domain>
  </security>
</datasource>
```

Para testar se a configuração está correta, **reinicie o jboss** e execute o seguinte comando na interface CLI:

```
su jboss
cd /usr/share/jboss-as-7.1.1.Final/bin/
./jboss-cli.sh --connect command=:shutdown
./standalone.sh -b 0.0.0.0 -bmanagement 0.0.0.0
./jboss-cli.sh --connect
```

```
/subsystem=datasources/data-source=ControllerDB:test-connection-in-
pool
exit
```

O resultado deve ser:

```
{
  "outcome" => "success",
  "result" => [true]
}
```

Para mais informações leia:

<https://docs.jboss.org/author/display/AS71/Security+subsystem+configuration>  
<http://middlewaremagic.com/jboss/?p=1026>

#### 4.3.3. Configurando o HTTPS no JBoss AS utilizando keytool

O primeiro passo é gerar o certificado SSL através do uso da ferramenta “keytool”, que está incluído no JDK. Para isso, execute os seguintes comandos:

```
su jboss
cd /usr/share/jboss-as-7.1.1.Final/standalone/configuration
keytool -genkey -alias ControllerWebCert -keyalg RSA -keystore
ControllerWebCert.keystore -validity 10950
```

Neste comando, a validade do certificado é dada em dias.

A seguir, preencha os campos que surgirão:

Enter keystore password: **(escolha uma senha complexa e comprida para a área de armazenamento de chaves)**

Re-enter new password: **(repita a senha escolhida)**

What is your first and last name?

[Unknown] : **(digite seu nome e sobrenome)**

What is the name of your organizational unit?

[Unknown] : **(seu setor)**

What is the name of your organization?

[Unknown] : **(sua empresa)**

What is the name of your City or Locality?

[Unknown] : **(sua cidade)**

What is the name of your State or Province?

[Unknown] : **(seu estado)**

What is the two-letter country code for this unit?

[Unknown] : **BR**

Is CN=seu nome, OU=seu setor, O=sua empresa, L=sua cidade, ST=seu estado, C=BR correct?

[no] : **yes**

```

Enter key password for
(RETURN if same as keystore password) : (aperte Enter)

```

O segundo passo é a configuração do Jboss.

No arquivo **standalone.xml**, insira dentro da tag:

```

<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host"
native="false">

```

o seguinte bloco:

```

<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http" redirect-
port="8443" />
<connector name="https" scheme="https" protocol="HTTP/1.1" socket-binding="https" enable-
lookups="false" secure="true">
    <ssl name="ControllerWeb-ssl" password="<repita a senha escolhida>" protocol="TLSv1" key-
alias="ControllerWebCert" certificate-key-
file="${jboss.server.config.dir}/ControllerWebCert.keystore" />
</connector>
, substituindo <repita a senha escolhida> pela senha do keystore escolhida.

```

A seguir exclua a tag relativa ao HTTP, já que esta foi alterada no bloco acima:

```
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
```

Para mais informações leia:

<https://docs.jboss.org/author/display/AS71/SSL+setup+guide>

#### 4.3.4. Instalando a interface Web do SciFi

Para que a interface web do SciFi requisite *login* e senha no momento do acesso, insira o seguinte bloco no arquivo:

```

/usr/share/jboss-as-7.1.1.Final/standalone/configuration/standalone.xml
,entre as tags <security-domains> ... </security-domains>:
<security-domain name="Controller" cache-type="default">
    <authentication>
        <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule"
flag="required">
            <module-option name="usersProperties"
value="${jboss.server.config.dir}/controller-users.properties"/>
            <module-option name="rolesProperties"
value="${jboss.server.config.dir}/controller-roles.properties"/>
            <module-option name="hashAlgorithm" value="SHA-1"/>
            <module-option name="hashEncoding" value="base64"/>
        </login-module>
    </authentication>
</security-domain>

```

```
</authentication>  
</security-domain>
```

Os arquivos **controller-users.properties** e **controller-roles.properties** devem ser criados no diretório **/usr/share/jboss-as-7.1.1.Final/standalone/configuration/**.

Será necessária uma senha criptografada, para isso utilize o comando, substituindo <password> pela **senha do usuário**:

```
echo -n <password> | openssl dgst -sha1 -binary | openssl base64
```

Preencha o arquivo **controller-users.properties** com os seguintes campos:

```
<usuário>=<senha>
```

Substitua <usuário> para um nome de usuário do seu desejo, e <senha> pela senha criptografada.

No arquivo **controller-roles.properties** insira o papel de cada usuário, da seguinte forma:

```
<usuário>=Admin
```

Para instalar a aplicação web do SciFi, a forma indicada é através do console de gerência do JBoss AS 7.1.

Faça o download da interface web do controlador SciFi no endereço:

<http://www.midiacom.uff.br/br/downloads-scifi/ControllerWeb-svn-rev206.war>

Com o **servidor Jboss ligado**, abra o **navegador web** e digite o endereço:

<http://localhost:9990/console/>

Uma tela parecida com a mostrada na Figura 25 irá surgir. Insira o usuário e senha criados para administrar o jboss e clique em **OK**.

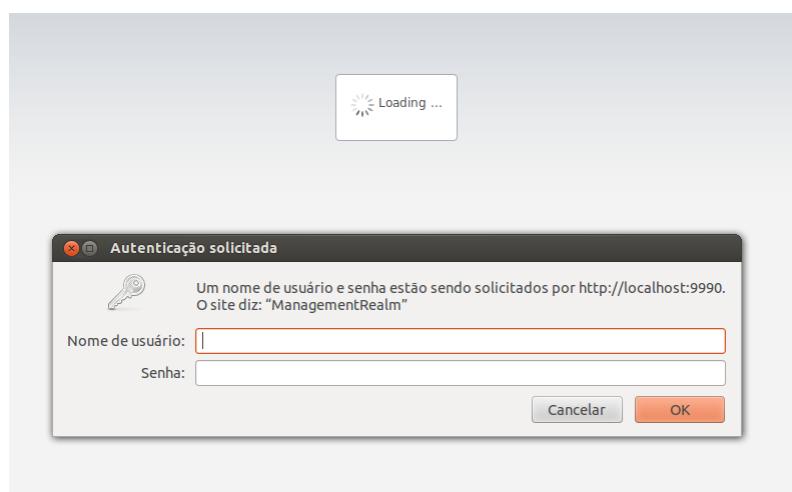
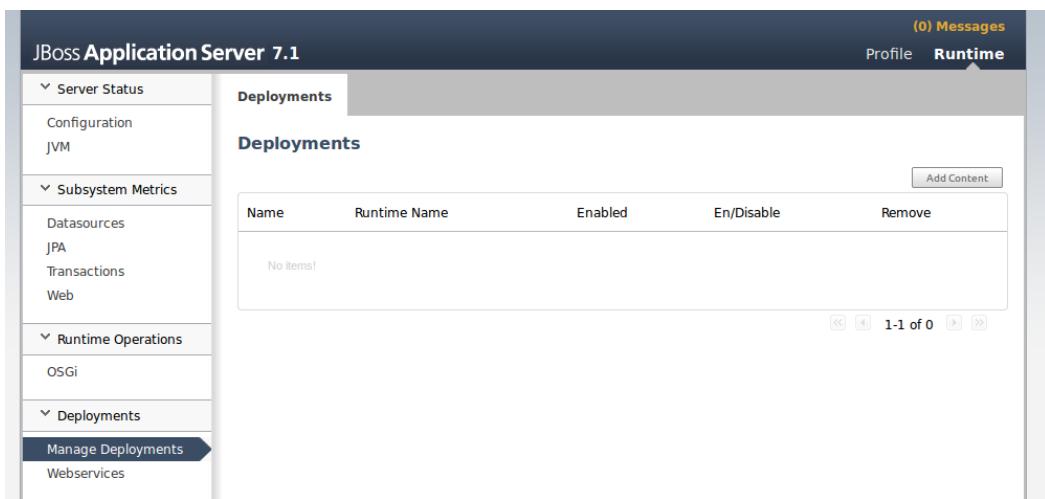


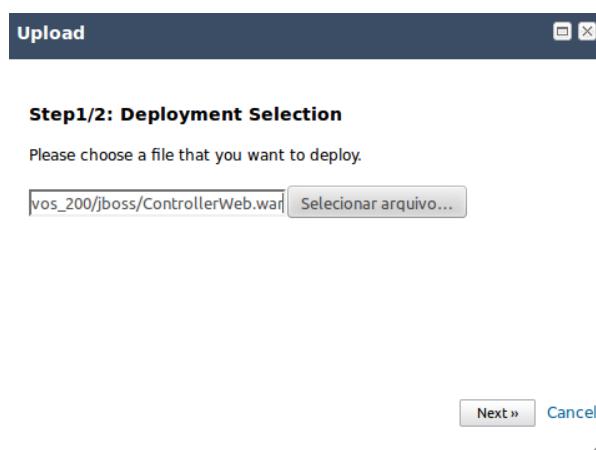
Figura 25 - JBoss: Interface de administração do JBoss

A seguir, na aba lateral “**Manage Deployments**”, clique em “**Add Content**”, conforme mostra a Figura 26.



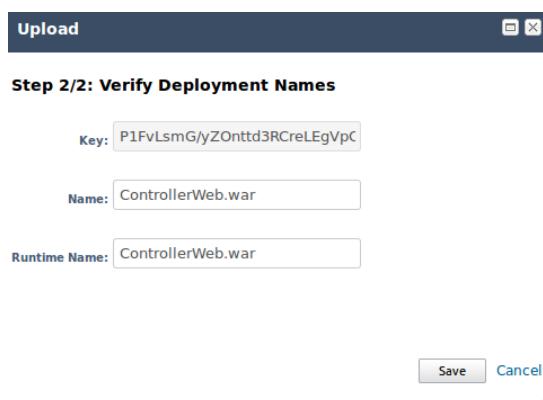
**Figura 26 - JBoss: Instalando a interface web do SciFi**

Uma janela como a mostrada na Figura 27 irá surgir. Clique em “**Escolher arquivo...**” e escolha o arquivo ControllerWeb-svn-rev206.war obtido previamente. A seguir clique em “**Next**”.



**Figura 27 - JBoss: Selecionar arquivo**

Na próxima janela, conforme mostra a Figura 28, clique em “Save”.



**Figura 28 - JBoss: Salvar configurações**

A seguir habilite a interface clicando em “Enable”, conforme mostra a Figura 31:

Figura 29 - JBoss: Habilitar interface web do SciFi

Na janela que surgir, clique em “Confirm”.



Figura 30 - JBoss: Confirmar habilitação da interface web

#### 4.4. Instalando o Núcleo de Processamento Central do SciFi

O Núcleo de Processamento Central (NPC) do SciFi é a parte do sistema responsável pela comunicação com os APs e execução dos algoritmos de controle.

O NPC do SciFi pode ser obtido através do link:

<http://www.midiacom.uff.br/br/downloads-scifi/scifi-svn-rev206.zip>

Após realizar o download, **desape** o arquivo e copie seu conteúdo para a pasta pasta **/usr/share/**.

```
unzip scifi-svn-rev206.zip -d /usr/share/
```

Entre na pasta copiada:

```
cd /usr/share/scifi
```

Altere a senha do usuário controlador para acesso ao banco de dados na segunda linha do arquivo **login\_config**:

```
controlador
```

```
insira a senha aqui
```

Caso ainda não tenha sido criado, crie no linux o **usuário** que será responsável por executar o controlador SciFi, chamado "**controlador**":

```
su - root
```

```
adduser controlador
```

Para definir a senha deste usuário execute o comando e a seguir insira a senha desejada:

```
passwd controlador
```

Com permissão de root, altere o dono do diretório e arquivos no qual o SciFi está instalado, da seguinte forma:

```
chown -R controlador:controlador /usr/share/scifi
```

Altere as permissões do arquivo **login\_config** para restringir sua leitura:

```
chmod 0600 /usr/share/scifi/login_config
```

Para que o controlador SciFi seja inicializado no boot, insira a seguinte linha no arquivo **/etc/rc.local**:

```
sh /usr/share/scifi/StartController.sh
```

O conteúdo final do arquivo ficará assim:

```
#!/bin/sh
#
# This script will be executed *after* all the other init
scripts.

# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
```

```
touch /var/lock/subsys/local
```

```
sh /usr/share/scifi/StartController.sh
```

A seguir, descomente no arquivo **/usr/share/scifi/StartController.sh** as linhas de inicialização do Jboss e APController. O script ficará assim:

```
# Inicializando o Nocat. Descomente a linha abaixo caso queira que o Captive Portal
(splash) seja ativado.
#/usr/share/nocat/bin/gateway

# Liberando os APs no Nocat. Insira uma linha para cada AP contendo MAC da interface
cabeadas e IP do AP.
#sh /usr/share/nocat/bin/access.fw permit 00:27:22:29:F1:E5 10.0.0.2 Public

# Inicialização do Jboss. A opção -b 0.0.0.0 libera acesso à interface administrativa
do scifi para qualquer IP.
```

```

# Por padrão, o acesso à interface de gerência do servidor de aplicações Jboss é
liberado apenas para localhost. Para liberar a acesso para outro ip, insira a opção -
bmanagement ip.

su - jboss -c "sh /usr/share/jboss-as-7.1.1.Final/bin/standalone.sh -b 0.0.0.0 &"

sleep 60

# Inicialização do Núcleo Central de Processamento do SCIFI. Um servidor tcp é criado
em localhost, porta 5000 para receber mensagens provenientes da interface web de
gerência.

su - controlador -c "cd /usr/share/scifi;java -cp APController.jar loader.JLoader
127.0.0.1 5000 &"

exit 0

```

Por fim, instale a chave privada para comunicação SSH entre o controlador e os pontos de acesso. Caso a chave ainda não tenha sido gerada, gere-a seguindo a documentação na seção 3.3.1.2. Ao final desta seção você obterá a chave pública e a privada na pasta /root. Altere o dono da chave privada e, a seguir, copie-a para a pasta /usr/share/scifi e mude a permissão para apenas leitura.

```

su -
//digite sua senha
cd /root
chown controlador:controlador controller_key
mv controller_key /usr/share/scifi
chmod 0600 /usr/share/scifi/controller_key

Para inicializar o SciFi, initialize antes o banco de dados e o Jboss. Por fim initialize o
SciFi:

```

```

service postgresql-9.2 start;
su - jboss -c "sh /usr/share/jboss-as-7.1.1.Final/bin/standalone.sh -b 0.0.0.0 &";
su - controlador -c "cd /usr/share/scifi;
java -cp APController.jar loader.JLoader 127.0.0.1 5000 &";

```

Os logs gerados pelo SciFi encontram-se na pasta de instalação: /usr/share/scifi.

O log \*Connection\* mostra as conexões SSH com os APs. O log \*Java\* mostra o log geral do java. O log \*Loader\* mostra o log do processo pai que inicializa novos processos para cada região de controle. Cada região de controle possuiá seus próprios *logs* de conexão e java. Os logs são criados quando o programa APController é iniciado.

## 5. Utilizando a Interface Web de gerência do SciFi

A Interface Web do controlador SciFi possibilita que o administrador da rede insira e modifique dados em relação aos pontos de acesso controlados e parâmetros de execução do controlador. A versão atual integra um mapa do google maps para inserir a localização dos pontos de acesso. As próximas seções deste manual apresentarão um guia de utilização desta interface.

### 5.1. Acessando a interface Web do controlador

Para acessar a interface Web do controlador SciFi, abra o navegador Web de sua escolha e digite o endereço:

<http://<IP do controlador>:8080/ControllerWeb>

, onde o texto <IP do controlador> deve ser substituído pelo endereço IP de uma das interfaces de rede do controlador. A Figura 31 mostra a página inicial da interface Web do controlador SciFi.



Figura 31 - Acesso à interface Web do controlador SciFi

A seguir, digite o nome de usuário e a senha de acesso criados durante o processo de instalação do SciFi (seção 4.3.4). Um passo a passo para a alteração da senha para acesso à interface web é apresentado na Seção 5.9. A seguir, clique no botão “Entrar”.

A página inicial da seção de administração do controlador será exibida, como mostra a Figura 32. Esta página apresenta as seguintes opções de navegação: adicionar e remover regiões de controle; adicionar, editar e visualizar pontos de acesso; executar comandos do controlador; e editar configurações do controlador; Monitoramento. Cada uma dessas subseções será abordada, respectivamente, nos itens 5.2, 5.3, 5.4, 5.6, 5.7 e 5.8 deste manual.



Figura 32 - Página inicial da seção de administração

## 5.2. Adicionando/Removendo regiões de controle

Antes de cadastrar os pontos de acesso para controle, o administrador deve criar regiões de controle. As regiões devem ser criadas de acordo com a posição geográfica dos pontos de acesso, de forma que pontos de acesso que possam vir a se interferir sejam adicionados a mesma região. Este mecanismo foi criado para possibilitar a utilização do controlador em redes de larga escala.

A criação de uma região de controle pode ser feita na subseção "Adicionar Região de Controle", como mostra a Figura 33.

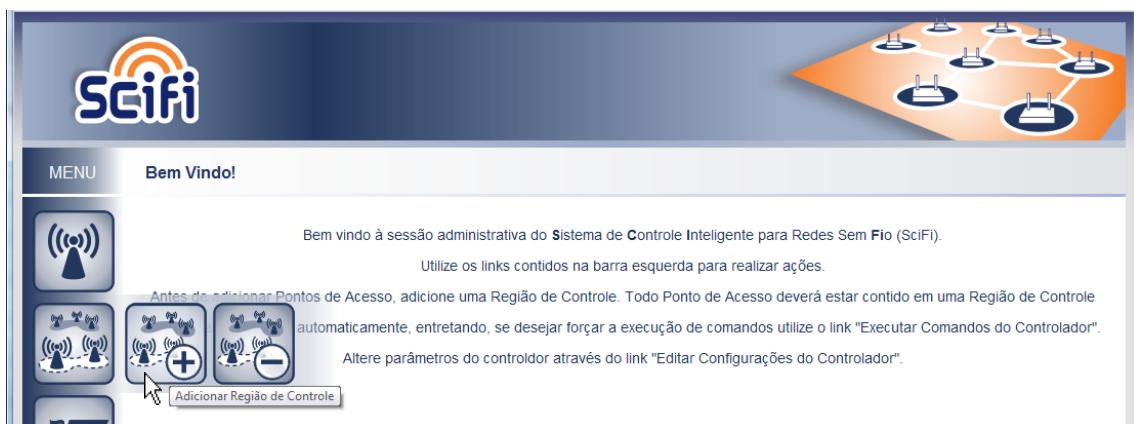


Figura 33 - Adicionando região de controle

Na página de adição de região, escreva o nome da região e clique em “adicionar”. Uma mensagem confirmará a criação da região.

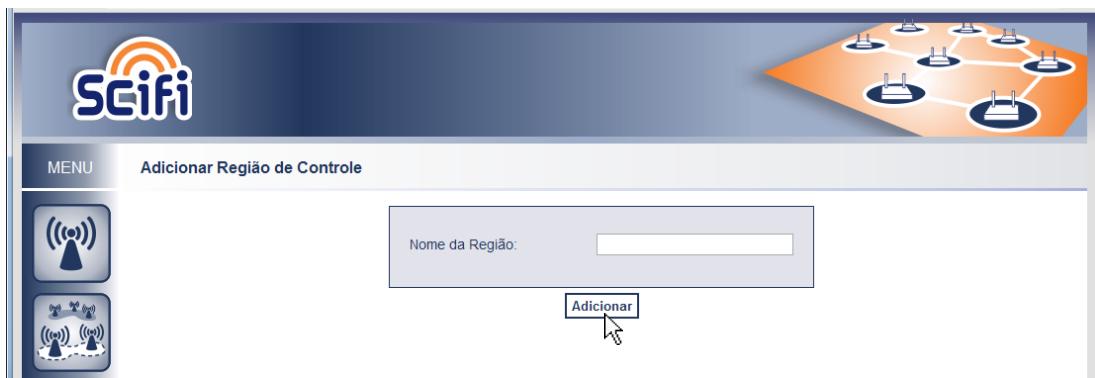


Figura 34 - Adicionando região de controle (2)

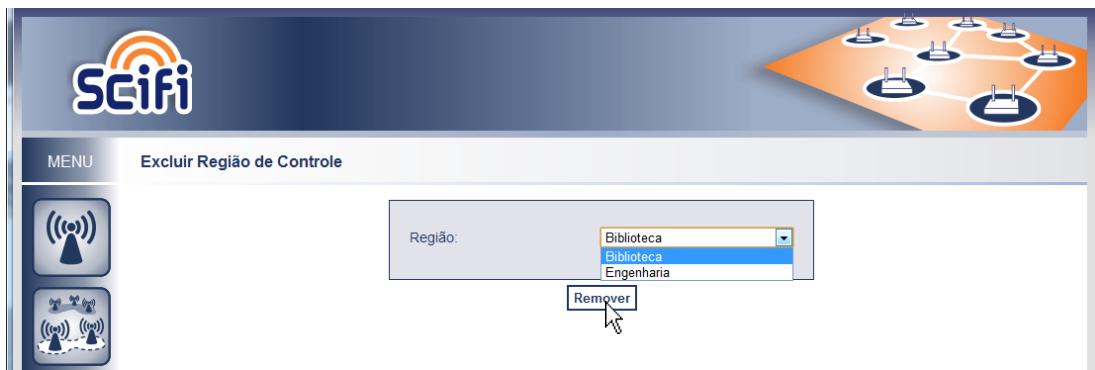


Figura 35 - Removendo Região de Controle

Para remover uma região existente, clique na subseção "Remover Região de Controle", escolha a região a ser excluída e clique em "Remover". Uma mensagem confirmará a exclusão da região.

### 5.3. Adicionando um novo ponto de Acesso controlado

Um novo ponto de acesso a ser controlado pode ser cadastrado a partir do mapa contido na tela inicial. Primeiro, encontre no mapa a localização de onde o(s) AP(s) serão instalados. Esta localização poderá ser marcada como *default*. Desta forma, toda vez que o mapa for acessado, esta localização será mostrada inicialmente. Para marcar uma posição como *default*, clique com o botão direito e a seguir escolha "Adicionar Posição como Default", conforme mostra a Figura 36.

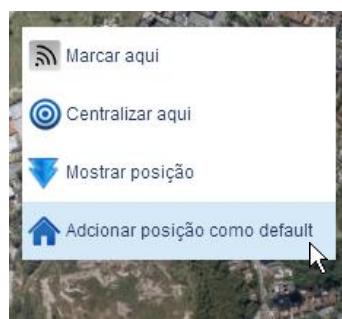


Figura 36 - Marcando posição no mapa como *default*

Para cadastrar um ponto de acesso, clique com o botão direito no mapa em sua posição e escolha "Marcar Aqui", conforme mostra a Figura 37. A seguir, surgirá um ícone cinza. Clique nele e escolha "Cadastrar", conforme mostra a Figura 38.

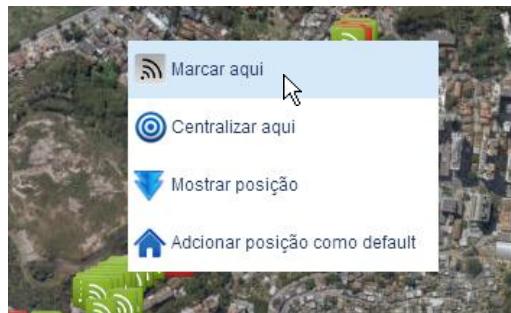


Figura 37 - Cadastrando novo AP para controle utilizando o mapa



Figura 38 - Cadastrando novo AP para controle utilizando o mapa (2)

Outra opção é o cadastro de APs através da subseção “Adicionar ponto de acesso”, acessada a partir do menu Pontos de Acesso na página inicial da seção de administração do controlador, como mostra a Figura 39.

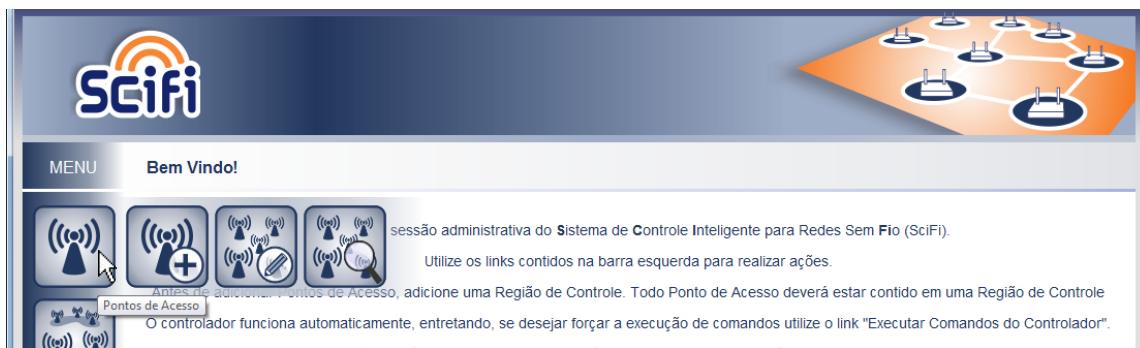


Figura 39 - Acessando a subseção para adição de novos APs controlados.

Ao clicar com o *mouse* no ícone “Adicionar ponto de acesso” (no menu) ou em “Cadastrar” (no mapa) uma página, como a mostrada na Figura 40, será apresentada. Esta página apresenta nove campos relativos ao novo ponto de acesso que se deseja adicionar.

The screenshot shows the SciFi web application interface. At the top left is the SciFi logo. On the right is a network diagram icon. The top navigation bar has links for 'MENU', 'Adicionar Ponto de Acesso', and 'Logout'. The main content area is titled 'Adicionar Ponto de Acesso'. It contains a form with the following fields:

- MAC da interface sem fio:
- IP:
- Localização:
- Lista de Potências:
- Limite de Carga Baixa:
- Limite de Sobre carga:
- Latitude:
- Longitude:
- Região:

At the bottom of the form is a blue button labeled 'Adicionar AP'.

At the bottom of the page, there is a dark footer bar with logos for UFF (Universidade Federal Fluminense), MÍDIACOM (Laboratório MÍDIACOM), Instituto de Computação, and RNP.

**Figura 40 - Página para adição de um novo ponto de acesso controlado**

O campo “MAC da interface sem fio” deve ser preenchido com o endereço MAC da interface sem fio do ponto de acesso. Este endereço deve seguir o padrão XX:XX:XX:XX:XX:XX, onde X representa um dígito hexadecimal entre 0 e F. Para descobrir o MAC desejado, o administrador deve executar o comando *ifconfig* no ponto de acesso e procurar pela interface sem fio e suas propriedades.

O campo “IP” deve ser preenchido com o endereço IP do ponto de acesso. Este endereço deve ser único e seguir o padrão XXX.XXX.XXX.XXX, onde XXX representa um número decimal entre 0 e 255. O administrador deve estar ciente de que o ponto de acesso deve estar na mesma sub-rede do controlador para que possam se comunicar diretamente sem a necessidade de roteamento entre sub-redes. Além disso, o primeiro e o último endereço da sub-rede não devem ser utilizados, já que representam o endereço da sub-rede e o endereço de broadcast.

O campo “Localização” deve ser preenchido com um texto descrevendo a localização física do ponto de acesso, como, por exemplo, “Sala de reuniões” ou “Biblioteca”.

O campo “Lista de Potências” deve ser preenchido com a lista das possíveis potências de transmissão que serão utilizadas pelo ponto de acesso. Esta lista deve seguir o padrão {X,X,X,...,X}, onde X representa valores de potência de transmissão em dBm. Notar que não há espaços entre os valores e as vírgulas. Estes valores não devem ser repetidos e devem estar em ordem crescente da esquerda para direita. Um exemplo de lista válida é: {5,8,11,14,17,20}. É importante que o administrador conheça as potências de transmissão mínima e máxima permitidas para utilização por cada ponto de acesso da rede. Para saber a potência máxima

suportada por seu ponto de acesso, entre outras funcionalidades suportadas, execute o comando "iw list" no terminal do AP.

Os campos “Limite de carga baixa” e “Limite de sobrecarga” representam os limiares para definição do status de carga de um ponto de acesso. Se o número de clientes associados ao AP está abaixo do “Limite de carga baixa”, o ponto de acesso é considerado com carga baixa. Se este número estiver acima do “Limite de sobrecarga”, o ponto de acesso é considerado sobrecarregado. Caso este número esteja entre os dois limites, o ponto de acesso é considerado com carga média. Os campos devem ser preenchidos com números inteiros, de forma que o “Limite de sobrecarga” seja maior do que o “Limite de carga baixa”.

O campo Latitude deve conter a latitude do ponto de acesso e o campo Longitude, a longitude do ponto de acesso. Os valores devem ser informados em graus decimais (mesmo padrão utilizado pelo *google maps*).

O campo região deve ser escolhido de acordo com a localização do ponto de acesso. Aqueles pontos que possam vir a se interferir devem estar na mesma região.

Para que um novo ponto de acesso seja adicionado, é necessário que os campos apresentados sejam preenchidos. Caso não sejam preenchidos de acordo com os padrões exigidos, ou os endereços MAC e IP já estejam em uso por outro ponto de acesso cadastrado, mensagens de erro serão apresentadas.

Após o preenchimento dos campos corretamente, o administrador deve clicar com o mouse no botão “Adicionar AP” para que o novo ponto de acesso seja adicionado na lista de pontos de acessos controlados. Após a adição, uma mensagem de confirmação é mostrada na tela.

#### 5.4. Visualizando informações e removendo pontos de acesso controlados

Após o cadastramento de um ponto de acesso para controle, um ícone verde será inserido no mapa. Ao clicar neste ícone, as informações do AP poderão ser acessadas, conforme mostra a Figura 41. Nesta figura, os ícones representam:

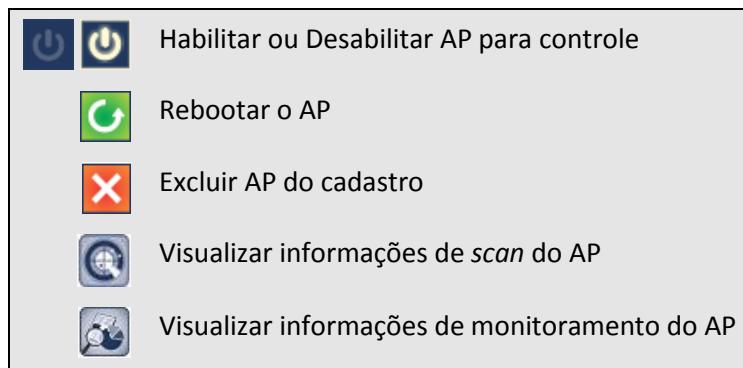


Figura 41 - Acesso às informações do AP via mapa

Clicando na seta localizada na lateral direita do mapa, uma lista completa das regiões e APs controlados pode ser visualizada, conforme mostra a Figura 42. No topo desta figura, vemos o filtro de MAC ou IP. Após digitar um MAC ou IP neste filtro, o AP referente será localizado no mapa. O AP também pode ser localizado clicando-se em "IR PARA" conforme mostra a tabela contida na figura. Na parte abaixo da figura, a legenda mostra as cores correspondentes aos estados dos APs:

- Cinza: ponto marcado no mapa para cadastro de AP

- Verde: AP habilitado para controle
- Vermelho: AP desabilitado para controle
- Laranja: AP sem comunicação cabeadas com o servidor (incomunicante).



Figura 42 - Lista de APs visualizada a partir do mapa

As informações detalhadas de todos os APs controlados podem ser visualizadas também em uma lista. Para acessá-la, clique no ícone “Visualizar pontos de acesso”, como mostra a Figura 43.

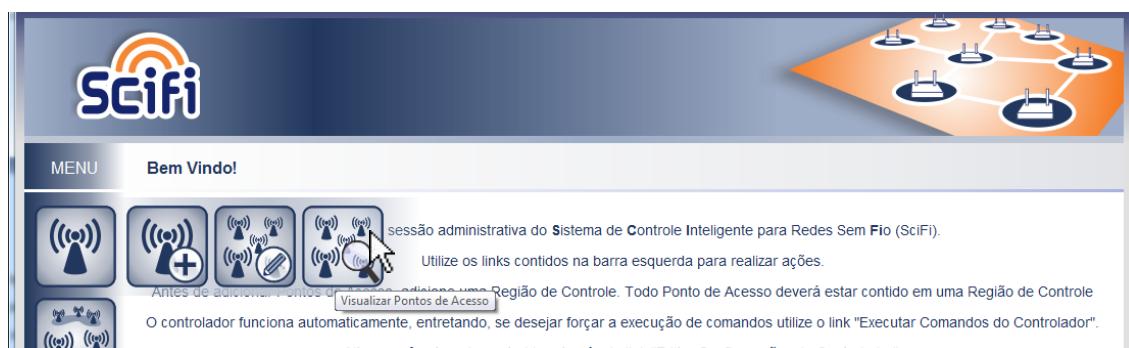
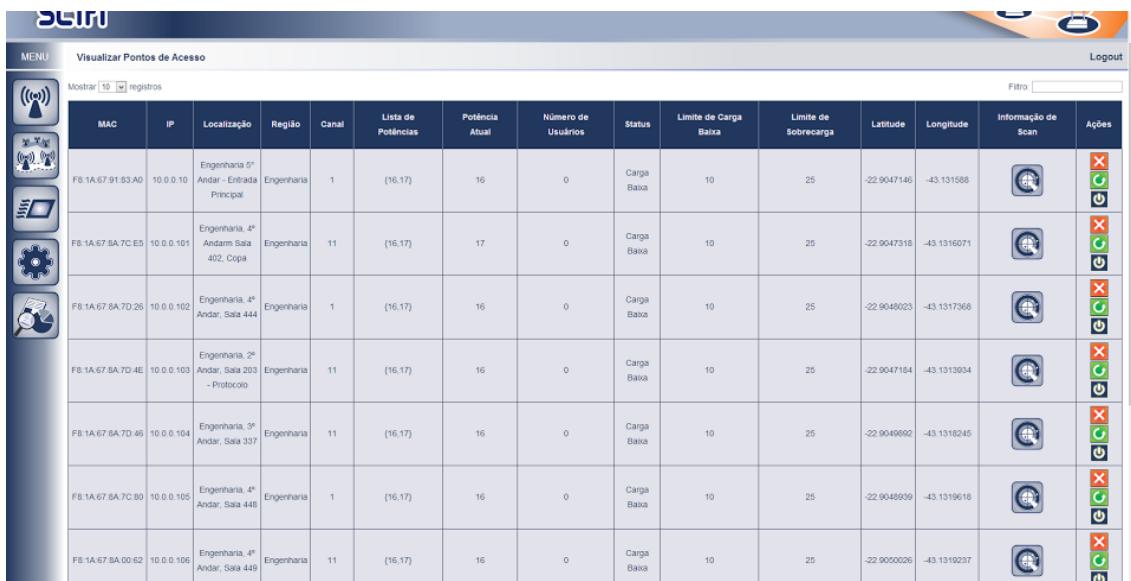


Figura 43 - Acessando a subseção para visualização dos pontos de acesso.

Ao clicar com o *mouse* no botão “Visualizar pontos de acesso”, uma página, como a mostrada na Figura 44, será apresentada.



The screenshot shows a web-based interface for managing network access points. On the left, there is a vertical sidebar with icons for different management functions. The main area has a header "Visualizar Pontos de Acesso" and a search/filter bar. Below is a table with the following columns: MAC, IP, Localização, Região, Canal, Lista de Potências, Potência Atual, Número de Usuários, Status, Limite de Carga Baixa, Limite de Sobrecarga, Latitude, Longitude, Informação de Scan, and Ações. The table lists seven access points with their respective details. Each row in the table includes a set of three buttons in the "Ações" column: a red X for removal, a green circle for restarting, and a blue power symbol for disabling.

MAC	IP	Localização	Região	Canal	Lista de Potências	Potência Atual	Número de Usuários	Status	Limite de Carga Baixa	Limite de Sobrecarga	Latitude	Longitude	Informação de Scan	Ações	
F8:1A:67:8A:7C:A0	10.0.0.10	Engenharia 5º Andar - Entrada Principal	Engenharia	1	(16,17)	16	0	Carga Baixa	10	25	-22.9047146	-43.131588			
F8:1A:67:8A:7C:E5	10.0.0.101	Engenharia, 4º Andar Sala 402, Copia	Engenharia	11	(16,17)	17	0	Carga Baixa	10	25	-22.9047318	-43.1316071			
F8:1A:67:8A:7D:26	10.0.0.102	Engenharia, 4º Andar, Sala 444	Engenharia	1	(16,17)	16	0	Carga Baixa	10	25	-22.9048023	-43.1317368			
F8:1A:67:8A:7D:4E	10.0.0.103	Engenharia, 2º Andar, Sala 203 - Protocolo	Engenharia	11	(16,17)	16	0	Carga Baixa	10	25	-22.9047184	-43.1313934			
F8:1A:67:8A:7D:46	10.0.0.104	Engenharia, 3º Andar, Sala 337	Engenharia	11	(16,17)	16	0	Carga Baixa	10	25	-22.9049692	-43.1318245			
F8:1A:67:8A:7C:80	10.0.0.105	Engenharia, 4º Andar, Sala 448	Engenharia	1	(16,17)	16	0	Carga Baixa	10	25	-22.9048939	-43.1319618			
F8:1A:67:8A:00:62	10.0.0.106	Engenharia, 4º Andar, Sala 449	Engenharia	11	(16,17)	16	0	Carga Baixa	10	25	-22.9000026	-43.1319237			

Figura 44 - Página para visualização dos pontos de acesso controlados

Esta página exibe uma tabela cujas linhas apresentam informações relativas a cada ponto de acesso controlado. As informações exibidas em cada coluna são, respectivamente: MAC do ponto de acesso, endereço IP, localização, região, canal atual de operação, lista de possíveis potências de transmissão, potência de transmissão atual, número de usuários conectados ao AP, status de carga, limite de carga baixa, limite de sobrecarga do ponto de acesso, latitude, longitude e informações de *scan*.

O status de carga pode assumir um dentre os três valores: Carga Baixa, Carga Média ou Sobrecarregado, que é definido pelo controlador. O canal do ponto de acesso e sua potência de transmissão atual, também definidos pelo controlador, são obtidos através dos algoritmos de seleção de canal e controle de potência (seções 1.2.1 e 1.2.2). As outras informações são definidas durante a inserção de um ponto de acesso na lista de controle (ver Seção 5.2).

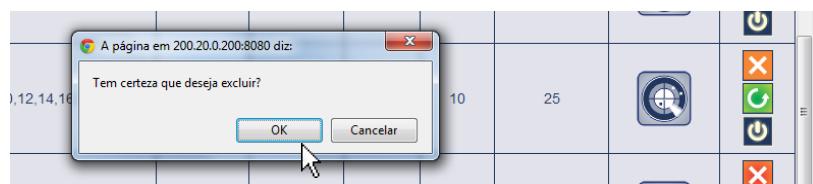


Figura 45 - Confirmando a exclusão de um ponto de acesso.

O número de APs mostrados por página pode ser configurado no topo esquerdo da janela. No padrão, 10 registros são mostrados por página.

A última coluna, denominada “Ações”, apresenta três botões: remover, reiniciar e desabilitar. O primeiro, quando acionado, remove da lista o ponto de acesso da linha determinada. Uma pergunta de confirmação é mostrada antes que a remoção seja realizada, como mostra a Figura 45. Ao remover o AP da lista, este continuará funcionando, porém o

controlador não terá mais acesso a ele. O segundo comando reinicia o AP. Atenção ao executar este comando, pois os clientes daquele ponto de acesso poderão ser desassociados. O terceiro botão, quando acionado, desabilitará o ponto de acesso. Quando desabilitado, o ponto de acesso não será mais controlado, ou seja, não sofrerá ação do controlador, seja para definição de parâmetros ou coleta de dados. Pontos de acesso desabilitados são mostrados em linhas cinza azuladas escuras, como mostra a Figura 46.

	MAC	IP	Localização	Região	Canal	Lista de Potências	Potência Atual	Número de Usuários	Status	Limite de Carga Baixa	Limite de Sobre carga	Informação de Scan	Ações
1	00:15:6D:3A:0F:A9	10.0.0.25	Chalé Arquitetura	Engenharia	11	(6,8,10,12,14,16,18,20,22,24,27)	27	0	Carga Baixa	10	25		
2	00:15:6D:3A:13:79	10.0.0.21	Bloco H - Add Labs	Biblioteca	1	(6,8,10,12,14,16,18,20)	20	0	Carga Baixa	10	25		
3	00:15:6D:3A:14:09	10.0.0.22	Casarão (Próximo à entrada da Engenharia)	Engenharia	1	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
4	00:15:6D:4C:EC:58	10.0.0.24	Física	Biblioteca	6	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
5	00:15:6D:E6:B0:57	10.0.0.19	Quiosque do Cláudio (Eng)	Engenharia	1	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
6	00:15:6D:F2:14:98	10.0.0.20	Bandejão	Biblioteca	11	(6,8,10,12,14,16,18,20)	10	0	Carga Baixa	10	25		
									Carga				

Figura 46 - Pontos de acesso desabilitado

Se o controlador perder conexão com o ponto de acesso, este ficará automaticamente destacado na cor laranja, como mostra a Figura 47.

	MAC	IP	Localização	Região	Canal	Lista de Potências	Potência Atual	Número de Usuários	Status	Limite de Carga Baixa	Limite de Sobre carga	Informação de Scan	Ações
1	00:27:22:28:F1:FB	10.0.0.10	Engenharia 5º Andar - Entrada Principal	Engenharia	11	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
2	00:27:22:28:F1:E8	10.0.0.11	Engenharia 2º Andar - Entrada Principal	Engenharia	1	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
3	00:27:22:28:F1:AC	10.0.0.12	Engenharia 2º Andar - Entrada Secundária	Engenharia	1	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
4	00:27:22:28:F2:6F	10.0.0.13	Laboratório MídiaCom	Engenharia	11	(6,8,10,12,14,16,18,20)	20	0	Carga Baixa	10	25		
5	00:27:22:28:F2:62	10.0.0.14	Engenharia 1º Andar - Entrada Secundária	Engenharia	11	(6,8,10,12,14,16,18,20)	16	0	Carga Baixa	10	25		
6	00:27:22:28:F1:D2	10.0.0.15	Auditório da Engenharia	Engenharia	11	(6,8,10,12,14,16,18,20)	6	0	Carga Baixa	10	25		
									Carga				

Figura 47 - Ponto de acesso sem conexão com o controlador

## 5.5. Editando informações dos pontos de acesso controlados

A alteração de informações dos pontos de acesso controlados pode ser realizada através da subseção “Editar pontos de acesso”, acessada a partir da página inicial da seção de administração do controlador, como mostra a Figura 48. Ao clicar com o *mouse* no botão “Editar pontos de acesso”, uma lista contendo todas as informações de todos os pontos de acesso será mostrada, como na Figura 49.

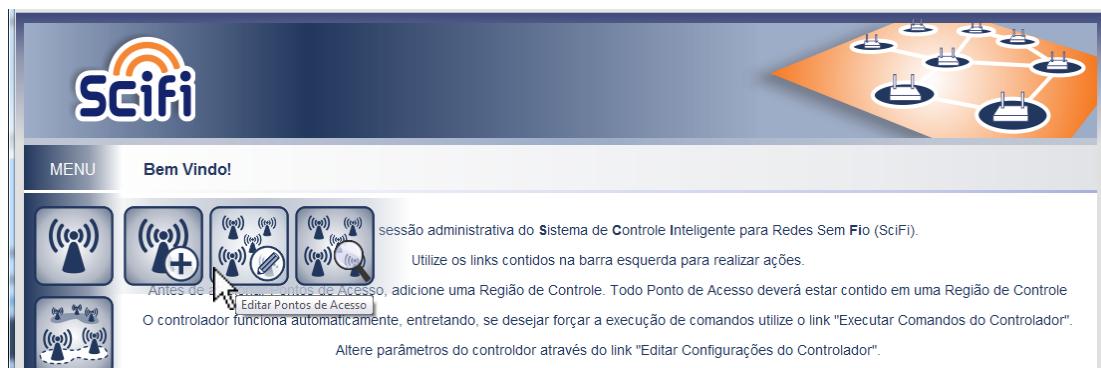


Figura 48 - Acessando a subseção para edição das informações dos APs.

Nesta tabela, as linhas apresentam informações relativas a cada ponto de acesso controlado. As informações exibidas em cada coluna são, respectivamente: MAC do ponto de acesso, endereço IP, localização, região, lista de possíveis potências de transmissão, Limite de carga baixa, Limite de sobrecarga, Latitude e Longitude do ponto de acesso.

Informações de MAC e IP não podem ser alteradas, já que identificam um ponto de acesso. Para “alterar” o endereço MAC ou IP do ponto de acesso é necessário excluí-lo (ver Seção 5.4) e posteriormente adicioná-lo com o endereço desejado (ver Seção 5.2).

Para que as modificações das informações sejam salvas, é necessário que os campos apresentados sejam preenchidos corretamente. Caso não sejam, mensagens de erro serão exibidas e as novas informações não serão salvas. Para mais informações sobre o preenchimento dos campos, consulte a seção 5.2. Após o preenchimento dos campos corretamente, o administrador deve clicar com o *mouse* no botão “Salvar Modificações” para que as informações sejam alteradas.




MENU

Logout

Editar Pontos de Acesso

MAC	IP	Localização	Região	Lista de Potências	Limite de Carga Baixa	Limite de Sobrecarga	Latitude	Longitude
F8:1A:67:91:83:A0	10.0.0.10	Engenharia, 5º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9047148	-43.131588
F8:1A:67:8A:7C:E5	10.0.0.101	Engenharia, 4º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9047318	-43.1316071
F8:1A:67:8A:7D:28	10.0.0.102	Engenharia, 4º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9048023	-43.1317368
F8:1A:67:8A:7D:4E	10.0.0.103	Engenharia, 2º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9047184	-43.1313934
F8:1A:67:8A:7D:4E	10.0.0.104	Engenharia, 3º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9049892	-43.1318245
F8:1A:67:8A:7C:8B	10.0.0.105	Engenharia, 4º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9048939	-43.1319618
F8:1A:67:8A:00:62	10.0.0.106	Engenharia, 3º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9050026	-43.1318237
F8:1A:67:8A:7C:F8	10.0.0.107	Engenharia, 3º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9049034	-43.1317329
F8:1A:67:8A:7C:78	10.0.0.108	Engenharia, 2º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9049435	-43.1318436
F8:1A:67:8A:7D:28	10.0.0.109	Engenharia, 2º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9048557	-43.1316605
F8:1A:67:91:8D:60	10.0.0.111	Engenharia 2º Andar	Engenharia	<input checked="" type="checkbox"/> (16,17)	10	25	-22.9047585	-43.1315002

Figura 49 - Página de edição das informações dos pontos de acesso controlados

A página de edição das configurações de um AP individual também pode ser acessada através do mapa. Após clicar no AP escolhido, clique em "Editar". A seguir, uma página individual de edição das configurações do AP será mostrada, conforme mostra a Figura 51. Os campos são semelhantes aos anteriores, porém somente um AP poderá ser editado. Ao final da edição, clique em "Salvar modificações". Caso algum campo esteja preenchido de forma incorreta, mensagens de erro serão mostradas.



Figura 50 - Acessando página de edição do AP via mapa

SciFi

MENU Adicionar Ponto de Acesso Logout

MAC da interface sem fio: 00:15:6D:3A:34:50

IP: 10.0.0.25

Localização: Chalé Arquitetura

Lista de Potências: {17.24.27}

Limite de Carga Baixa: 10

Limite de Sobre carga: 25

Latitude: -22.9045849

Longitude: -43.13077550000003

Região: Engenharia

uff Universidade Federal Fluminense LABORATÓRIO MÍDIACOM Instituto de Computação RNP

Figura 51 - Página de edição individual das configurações de um AP

### 5.6. Executando comandos do controlador

O controlador SciFi realiza suas funções de forma automática, porém é possível forçar a execução de alguns comandos quando necessário. Para executar comandos do controlador, clique com o *mouse* no botão “Executar comandos do Controlador” e, como mostra a Figura 52, uma página com diversos botões de comandos surgirá.



Figura 52 - Executando comandos do controlador

Os seguintes comandos são disponibilizados através da página de execução de comandos:

- **Reiniciar Controlador:** reinicia o núcleo de processamento central do controlador;
- **Forçar Reinício dos Temporizadores:** reinicia todos os temporizadores do controlador;
- **Forçar Seleção de Canal:** executa o algoritmo de seleção de canal;
- **Forçar Controle de Potência:** executa o algoritmo de controle de potência;
- **Forçar Escaneamento do Ambiente:** executa a varredura espectral em todos os APs;
- **Forçar Coleta de Dados dos Usuários:** coleta dados dos usuários associados aos APs;
- **Reiniciar todos os Pontos de Acesso:** reinicia todos os pontos de acesso;
- **Forçar Análise de Configurações dos Pontos de Acesso:** compara a configuração de potência e canal dos APs com as informações do banco de dados e corrige possíveis erros.

### 5.7. Editando parâmetros de execução do controlador

A alteração de parâmetros de execução do controlador pode ser realizada através da subseção “Editar parâmetros de execução do controlador”, acessada a partir da página inicial da seção de administração do controlador, como mostra a Figura 53.



Figura 53 - Acessando a subseção para edição de parâmetros do controlador.

Parâmetro	Valor	Tipo da Propriedade
Intervalo entre as execuções do algoritmo de seleção de canal	21600	Segundos
Intervalo entre as análises de configurações	900	Segundos
Intervalo entre as execuções do algoritmo de controle de potência	600	Segundos
Intervalo entre a execução de scans	540	Segundos
Porcentagem da qualidade do último scan a ser utilizada na média ponderada do próximo	0	Porcentagem
Intervalo entre a obtenção de dados sobre os usuários de cada AP	300	Segundos
IP através do qual a interface Web se comunica com o Controlador	127.0.0.1	IP
Porta do Controlador através da qual a Interface Web se comunicará	5000	Inteiro Positivo
Valor da latitude padrão do mapa de localização dos pontos de acesso	-22.90126096005722	Decimal
Valor da longitude padrão do mapa de localização dos pontos de acesso	-43.129719123244286	Decimal
Nível de zoom padrão do mapa de localização dos pontos de acesso	16	Inteiro Positivo
Endereço do Servidor de Email do remetente (formato: mail ENDEREÇO_DO_SERVIDOR_DE_EMAIL)	mail.midiacom.uff.br	Texto
Destinatário para envio de emails sobre status dos pontos de acesso	helado@midiacom.uff.br	Email
Remetente para envio de emails sobre status dos pontos de acesso	noreply-scifi@midiacom.uff.br	Email
Caminho da ferramenta de monitoramento MRTG (formato: "http://IP:PORTA/CAMINHO"). O IP deve ser acessível via internet.	http://200.20.0.201/mrtg	Texto

[Salvar modificações](#)

**Figura 54 - Página de edição dos parâmetros de execução do controlador**

Ao clicar com o *mouse* no botão “Editar parâmetros de execução do controlador”, uma página, como a mostrada na Figura 54, será apresentada.

Esta página exibe uma tabela cujas linhas apresentam informações relativas aos parâmetros de execução do controlador. A coluna “Parâmetro” exibe o nome do parâmetro e a coluna “Valor” exibe o valor atual do parâmetro.

- **Intervalo entre as execuções do algoritmo de seleção de canal:** Seu valor, dado em segundos, deve ser preenchido com um número inteiro.
- **Intervalo entre as análises de configurações:** Seu valor, dado em segundos, deve ser preenchido com um número inteiro. Na análise de configurações, o canal e a potencia dos pontos de acesso são comparados com as contidas no banco de dados. Se existir alguma diferença, o controlador altera o canal e/ou potência do ponto de acesso com a informação contida no banco de dados.
- **Intervalo entre as execuções do algoritmo de controle de potência:** Seu valor, dado em segundos, deve ser preenchido com um número inteiro.
- **Intervalo entre as execuções de scans:** Seu valor, dado em segundos, deve ser preenchido com um número inteiro. O *scan* é utilizado para obtenção de informações sobre a interferência entre os pontos de acesso. O administrador deve levar em consideração o fato de que, durante a realização do *scan*, a interface sem fio do ponto de acesso varre todos os canais de comunicação possíveis. Isto pode acarretar a perda da conexão entre o ponto de acesso e suas estações clientes momentaneamente.
- **Porcentagem da qualidade do último scan a ser utilizada na média ponderada do próximo:** esta porcentagem indica o quanto os *scans* antigos influenciarão na definição atual da interferência entre os pontos de acesso.
- **Intervalo entre a obtenção de dados sobre os usuários de cada AP:** parâmetro que representa o intervalo de tempo entre execuções da coleta do número de estações

associadas ao ponto de acesso. Seu valor, dado em segundos, deve ser preenchido com um número inteiro. O administrador deve levar em conta que, quanto menor este valor, mais atualizada a informação utilizada pelo controlador estará.

- **IP através do qual a Interface Web se comunica com o Controlador:** IP da interface na qual o servidor de SciFi aguarda conexões provenientes da interface web para envio de comandos, entre outros. Como normalmente a interface web e o núcleo de processamento central do SciFi rodam na mesma máquina, o valor padrão deste campo é 127.0.0.1.
- **Porta do Controlador:** número da porta do servidor que possibilita que o controlador receba comandos provenientes da interface web. A porta padrão no controlador é 5000.
- **Valor da latitude padrão do mapa de localização dos pontos de acesso:** O valor deve ser dado em graus decimais.
- **Valor da longitude padrão do mapa de localização dos pontos de acesso:** O valor deve ser dado em graus decimais.
- **Nível de zoom padrão do mapa de localização dos pontos de acesso:** número decimal. Valor padrão é 16.
- **Endereço do Servidor de Email do remetente:** o formato deve ser mail.ENDEREÇO\_DO\_SERVIDOR\_DE\_EMAIL. Através deste servidor de email, o SciFi enviará notificações quando um ponto de acesso se tornar incomunicante. Um email é enviado por dia por ponto de acesso. Ao final do dia, um relatório contendo os pontos de acesso incomunicantes para cada região de controle é enviado.
- **Destinatário para envio de emails sobre status dos pontos de acesso:** este ítem é relacionado ao anterior. Aqui deve ser inserido o endereço de email para o qual as mensagens de alerta do SciFi são enviadas.
- **Rementente para envio de emails sobre status dos pontos de acesso:** Aqui deve ser inserido o email que será preenchido no campo remetente dos emails de alerta do SciFi.
- **Caminho da ferramenta de monitoramento:** O formato deve ser "http://IP:PORTA/CAMINHO/". O IP deve ser acessível via internet. Neste campo pode ser inserido um link para a página de monitoramento dos pontos de acesso. Este link será acessível através do ícone "Monitoramento", conforme indica a seção 5.8.

Para que as modificações sejam realizadas, é necessário que campo “Valor” seja preenchido corretamente para todos os parâmetros. Caso não sejam, mensagens de erro serão exibidas e as novas informações não serão salvas. Após o preenchimento dos campos corretamente, o administrador deve clicar com o *mouse* no botão “Salvar Modificações” para que as informações sejam salvas.

## 5.8. Acessando a página de monitoramento

Para acessar a ferramenta de monitoramento dos APs, clique no ícone "Monitoramento" no menu direto, conforme mostra a Figura 55. Para configurar o endereço da página web da ferramenta de monitoramento, consulte a seção 5.7. No SciFi, optamos por utilizar a ferramenta MRTG. Ao clicar no ícone, a página web de monitoramento será mostrada. A Figura 56 mostra o exemplo no qual a ferramenta MRTG customizada é utilizada.



Figura 55 - Acesso à página de monitoramento dos APs

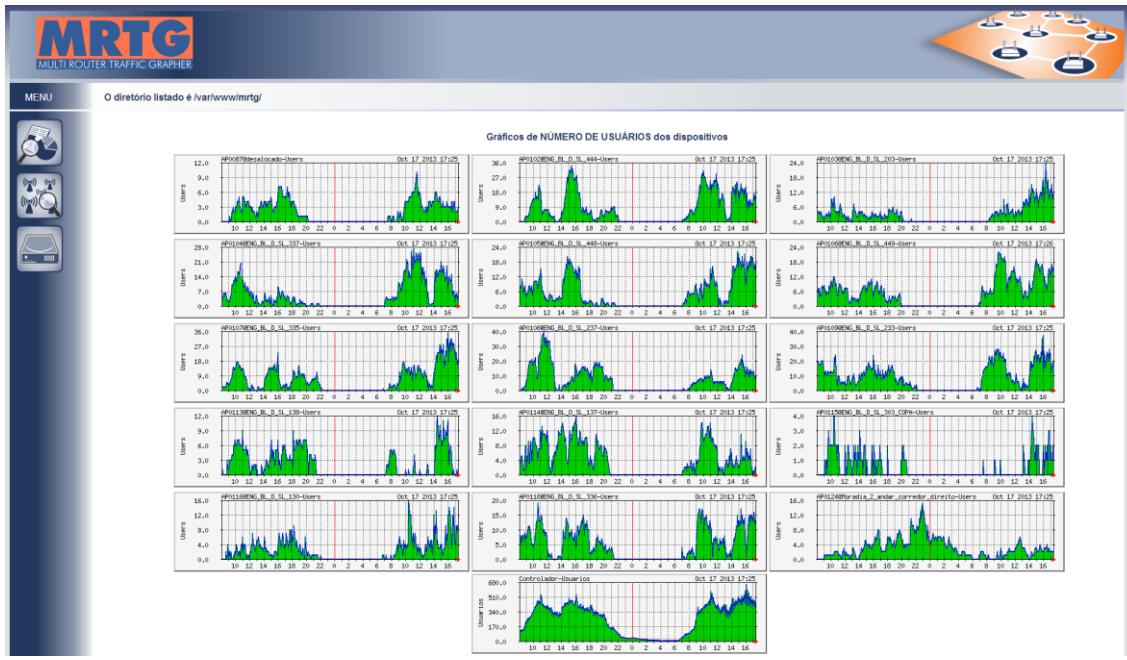


Figura 56 - Exemplo de ferramenta para monitoramento

## 5.9. Alterando a senha de acesso à interface Web

A alteração da senha de acesso à interface Web do controlador pode ser realizada através do arquivo **controller-users.properties**, localizado em **/usr/share/jboss-as-7.1.1.Final/standalone/configuration/**. Para modificar o arquivo, é necessária permissão de administrador (root).

Este arquivo possui o seguinte formato:

```
<usuário>=<senha>
```

onde o campo **<senha>** representa a senha criptografada com o algoritmo SHA1.

Portanto, a nova senha a ser utilizada deve estar criptografada com SHA1. Para realizar a criptografia da nova senha, digite o comando:

```
echo -n <password> | openssl dgst -sha1 -binary | openssl base64
```

onde **<password>** é a nova senha desejada.

A seguir, copie o resultado do comando e substitua o campo **<senha>** do arquivo **controller-users.properties** pela nova senha gerada.

Por exemplo, ao utilizar o **<password>** *midiacom*, o resultado obtido a partir do comando acima foi:

```
echo -n midiacom | openssl dgst -sha1 -binary | openssl base64
heRLQHWNxauAwbBei88InA/v8To=
```

Após substituir o campo **<senha>** pela nova senha criptografada, e supondo que o nome do usuário seja "admin" o arquivo **controller-users.properties** ficou da seguinte forma:

```
admin=heRLQHWNxauAwbBei88InA/v8To=
```

Salve o arquivo para finalizar o processo de alteração da senha de acesso à interface Web.

### 5.10. Criando/alterando usuário de acesso à interface Web

A criação/alteração de usuário de acesso à interface Web pode ser realizada através do arquivo **controller-roles.properties**, localizado em **/usr/share/jboss-as-7.1.1.Final/standalone/configuration/**. Para modificar o arquivo é necessária a permissão de administrador (root).

Este arquivo possui o seguinte formato "usuário=papel", por exemplo:

```
admin=Admin
```

Se for desejado apenas alterar o nome de usuário, insira o novo nome no lugar do nome do usuário antigo (admin). O nome antigo também deve ser substituído pelo novo nome no arquivo que guarda as senhas de acesso à interface web **/usr/share/jboss-as-7.1.1.Final/standalone/configuration/controller-users.properties** ).

Para adicionar um novo usuário, insira neste arquivo uma linha contendo o *login* do usuário e seu papel:

```
admin=Admin  
novousuario=Admin
```

A seguir, é necessário adicionar uma senha de acesso para o novo usuário no arquivo **controller-users.properties**, que está localizado no diretório **/usr/share/jboss-as-7.1.1.Final/standalone/configuration/**. Para isso, gere uma senha criptografada com SHA1 através do seguinte comando:

```
echo -n <password> | openssl dgst -sha1 -binary | openssl base64
```

Após criar a senha, insira uma nova linha no arquivo **controller-users.properties** contendo o nome do usuário e a senha gerada, da seguinte forma:

```
novousuario=senhaCriptografada
```

Para modificar este arquivo é necessária a permissão de administrador (root).

Por fim, salve os arquivos para concretizar o processo de criação de novo usuário para acesso à interface web. Não é necessária a reinicialização do sistema.