UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

UERIC COSTA LEODORO

Monitoramento de Dispositivos Power Over Ethernet (PoE)

MONOGRAFIA

CURITIBA
2015

UERIC COSTA LEODORO

Monitoramento de Dispositivos Power Over Ethernet (PoE)

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2015

RESUMO

LEODORO, Ueric C. **Monitoramento de Dispositivos *Power Over Ethernet* (PoE)**. 2015. 64 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Este estudo tem por objetivo principal, o monitoramento de dispositivos PoE (*Power Over Ethernet*), através do protocolo SNMP utilizando a ferramenta de monitoramento *What's Up Gold*. Porém os dispositivos que devem ser monitorados não possuem um endereço de IP. Este trabalho contém uma abordagem de um estudo caso com base em um cenário muito próximo da realidade de armazéns, supermercados e demais estabelecimentos que necessitem de uma infraestrutura sem fio com o mínimo de indisponibilidade. Há a possibilidade, através da ferramenta, da construção de um mapa com estes dispositivos utilizando uma planta de um armazém para um melhor gerenciamento destes dispositivos.

Palavras-chave: PoE, SNMP, Redes, What's Up Gold, Monitoramento

ABSTRACT

LEODORO, Ueric C. ***Power Over Ethernet Port Monitoring*** **(PoE)**. 2015. 64 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2015.

The main goal of this work is the PoE (Power Over Ethernet) devices monitoring through the SNMP protocol by using the What's Up Gold monitoring tool. However, the devices that should be monitored do not have an IP address. This work is based on a topology very close to the reality of department stores, Supermarkets and other companies that require a wireless infrastructure with minimal downtime. The tool provides a building map with these devices using a plant of the warehouse for better management of these devices.

Keywords: PoE, SNMP, Networks, What’s Up Gold, Monitoring

LISTA DE SIGLAS

ACL – Access Control List

AP – Access Point

CLI – Command-Line Interface

CPU – Central Processing Unit

DHCP – Dynamic Host Configuration Protocol

GHz – Gigahertz

HTTP – Hypertext Transfer Protocol

HTTPS – Hyper Text Transfer Protocol Secure

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IGMP – Internet Group Management Protocol

IIS – Internet Information Services

IP – Internet Protocol

ISO – International Organization for Standardization

IPSec – Internet Protocol Security

Mbps – Megabit por Segundo

MIB – Management Information Base

NAT – Network Address Translation

NMS – Network Management Station

RAM – Random Access Memory

RFC – Request for Comments

RMON – Remote Monitoring

SNMP – Simple Network Management Protocol

SMI – Structured of Management Information

SSH – Secure Shell

TCP – Transmission Control Protocol

TI – Tecnologia da Informação

PoE – Power Over Ethernet

UDP – User Datagram Protocol

VLAN – Virtual Lan Area Network

VPN – Virtual Private Network

WMI – Windows Management Instrumentation

WMS – Warehouse Management System

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

SUMÀRIO

1 INTRODUÇÃO

Nesta presente seção será informado ao leitor os principais tópicos referentes a esta monografia com relação ao tema sobre o Monitoramento de dispositivos *Power Over Ethernet* (PoE) através do Protocolo *Simple Network Management Protocol* (SNMP), apresentando a ferramenta *What's Up Gold* juntamente com uma apresentação de um estudo de caso, bem com a construção e implantação deste monitoramento no cenário proposto.

1.1 Justificativa

Atualmente existe uma gama de dispositivos que utilizam a tecnologia PoE, desde *access-points*, câmeras IP e dispositivos VoIP. Alguns destes dispositivos, são considerados críticos, onde a imediata falta de comunicação, poderá acarretar em grandes prejuízos ao negócio.

O propósito deste trabalho está em estudar como monitorar estes dispositivos, principalmente os que não possuem um endereço de IP. Outro ponto a ser abordado é sobre a construção de mapas de rede, onde tais dispositivos estejam cadastrados e de forma haja monitoramento em tempo real do funcionamento dos mesmos, resultando em rápido tratamento de indisponibilidades destes ativos.

1.2 Objetivo Geral

Este estudo tem como finalidade, estudar e implantar um monitoramento de dispositivos PoE através do protocolo SNMP, utilizando a ferramenta *What's Up*.

1.3 Objetivos Específicos

- Apresentar a necessidade de monitoramento de dispositivos PoE, com base em um cenário baseado em fatos reais;
- Explorar recursos e funcionalidades da ferramenta de monitoramento *What's Up Gold*;
- Mostrar o processo de construção do ambiente e da solução da situação apresentada;
- Servir como base onde se identifique outras situações similares e complexas.

1.4 Metodologia de Pesquisa

O problema apresentado, bem como sua solução, terá como base, estudo de caso elaborado a partir de situações reais encontradas no dia-a-dia das organizações.

Serão utilizados livros de referência na área, sobre monitoramento de dispositivos, sites de fabricantes que utilizam a tecnologia PoE e artigos diversos.

2 Tecnologia Power Over Ethernet (PoE)

2.1 Conceitos Históricos (PoE)

Segundo Morimoto (2007), a tecnologia PoE surgiu da necessidade de se levar corrente elétrica para dispositivos de rede remotos, onde a implantação de uma rede elétrica a parte era considerada difícil execução, além da geração de custos de instalação e manutenção.

Como estes dispositivos utilizavam a conexão RJ-45, o mesmo cabo de comunicação pode ser utilizado para o envio de dados juntamente com a corrente elétrica. A fabricante *Cisco Systems* desenvolveu o primeiro dispositivo neste formato em 2000. Esta tecnologia foi chamada de *Cisco Inline Power*, com potência de 7 *Watts*. Em 2003 o IEEE (*Institute of Electrical and Electronics Engineers*) publicou o padrão IEEE 802.3af que descreve a tecnologia PoE, bem como o seu funcionamento e especificações. (Cisco Systems, 2015)

2.2 PoE+

O padrão PoE, proposto pela IEEE tem uma especificação de 15.4 *Watts* por porta PoE. Porém alguns dispositivos necessitavam de uma maior quantidade de potência. Neste contexto, o IEEE desenvolveu em 2009, um novo padrão chamado de IEEE 802.3at que especifica uma potência máxima de 30 *Watts* por porta PoE Este padrão possui retro compatibilidade com o padrão 802.3af. (Sheldon, 2010).

2.3 UPoE

Este padrão foi desenvolvido pela fabricante *Cisco Systems* em 2011. A única diferença em relação aos padrões anteriores, está novamente na potência máxima por porta PoE, que é de 60 *Watts*. (Cisco Systems, 2015)

2.4 Estrutura para dispositivos PoE

Existem duas formas para implantação de uma estrutura para dispositivos PoE. (De Oliveira, 2015)

2.4.1 Estrutura com fonte PoE individual

A figura 1 é uma descrição de uma topologia simples, onde temos a conexão da rede elétrica com a fonte PoE.

A fonte PoE dispõe de duas portas RJ-45, sendo uma normalmente marcada com inscrição *IN*, que significa a entrada de dados da rede local que vindo de um switch ou um ponto de rede qualquer.

Já a outra porta tem uma inscrição com o nome *OUT*, que significa saída. Isto é, a junção da conexão de dados com a corrente elétrica para serem disponibilizadas para o dispositivo remoto, como um *access-point*.

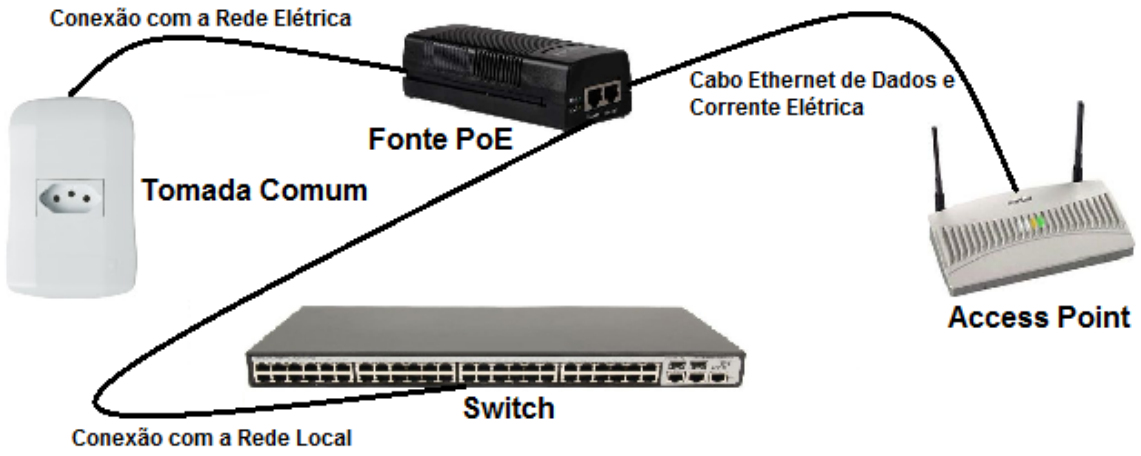

Figura 1 - Estrutura com fonte PoE individual
Fonte: Autoria Própria

2.4.2 Estrutura com *Switch* PoE

A segunda forma para implantação de uma estrutura PoE é mais simplificada que a primeira, já que há a unificação da fonte PoE com um *switch*, transformando este em um *switch* PoE. Desta forma elimina-se a necessidade de várias fontes PoE individuais para cada dispositivo, além da adição de um melhor gerenciamento dos dispositivos conectados, como mostrado na figura 2.

Figura 2 - Estrutura com *Switch* PoE
Fonte: Adaptado de Morimoto (2007)

2.5 Protocolo *Simple Network Management Protocol* (SNMP)

O protocolo SNMP foi desenvolvido a partir de 1988, com o propósito para o gerenciamento de dispositivos remotos, sendo uma das suas funções mais conhecidas, o monitoramento de diversos dispositivos.
A *Internet Engineering Task Force* (IETF), publicou várias RFCs, que são documentos para a padronização dos protocolos e que descrevem as diferentes versões do SNMP (MAURO; SCHIMIDT, 2001).

2.5.1 Versões SNMP

- SNMPv1 – É o padrão atual do protocolo, sendo definido na RFC 1157;
- SNMPv2 – É considerado um padrão experimental, sendo definido nas RFCs 1905, 1906 e 1907;
- SNMPv3 – É considerado o padrão a ser utilizado nos ambientes. Esta versão suporta uma autenticação mais forte e uma comunicação privada entre os dispositivos que são gerenciados. Este padrão está definido nas seguintes RFCs: 1905, 1906, 1907, 2571, 2572, 2573, 2574 e 2575. (MAURO; SCHIMIDT, 2001).

Uma informação a ser ressaltada com relação as versões do SNMP, é que em caso de uma atualização do *software* de monitoramento, para alguma versão com suporte a SNMPv2 ou a SNMPv3, não significa a obtenção de mais informações, comparado a uma versão de *software* apenas com suporte a versão SNMPv1.
A grande diferença entre as 3 versões do SNMP é a adição de recursos ao protocolo, incluindo mais segurança e mais opções de recuperação e definição de valores dentro do protocolo.
As informações que estão acessíveis nos dispositivos são determinadas através das MIBs – *Management Information Base* (assunto a ser apresentado

logo adiante) presentes no agente independentemente do protocolo em questão. (MAURO; SCHIMIDT, 2001).

2.5.2 Estrutura SNMP

O protocolo SNMP possui dois personagens principais: Gerenciadores e Agentes.

Os gerenciadores podem ser descritos como servidores para sistemas de *software*, tendo como principal função executar as tarefas de gerenciamento de rede. Eles também são conhecidos como NMSs (*Network Management Stations*). A operação básica dos NMSs está no recebimento dos chamados *polls*, que é uma operação para busca de informações sobre o estado do agente monitorado.

Já os agentes, são os clientes do *software* de gerenciamento implantados nos dispositivos. O agente utiliza as *traps*, que é a resposta do agente para o NMS, sobre qualquer situação ocorrida. (MAURO; SCHIMIDT, 2001).

A figura 3, apresenta a relação entre uma NMS e um agente.

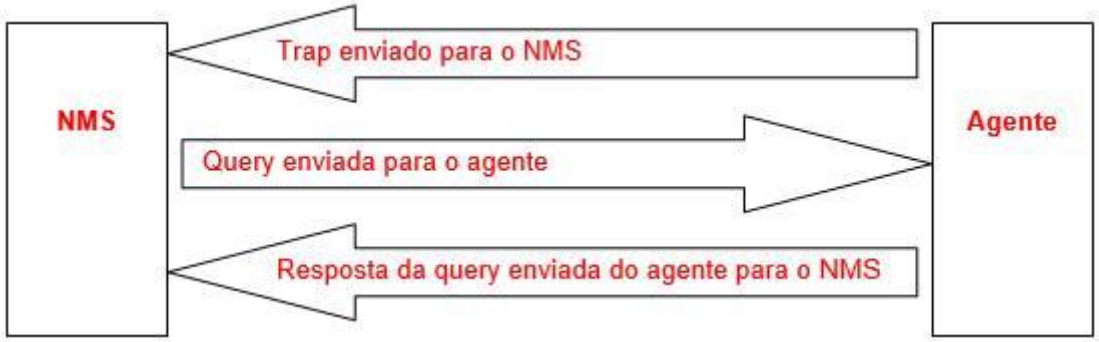

Figura 3 – Relação entre uma NMS e um agente
Fonte: Teleco (2015)

2.5.2.1 SMI (*Structured of Management Information* – Estrutura de Informações de Gerenciamento)

É uma forma para definição dos objetos a serem gerenciados e os seus comportamentos esperados. Cada agente possui uma série de objetos que são rastreados através do próprio agente.

Uma interface de *switch*, por exemplo, é um tipo de objeto e o seu comportamento esperado pode ser: funcional, em teste ou parada.

Esta série de objetos são consideradas pela NMS para a detecção do status do dispositivo, onde o agente está inserido. (MAURO; SCHIMIDT, 2001).

2.5.2.2 MIB (*Management Information Base* – Base de Informações de Gerenciamento)

É um tipo de banco de dados dos objetos administrados, onde o agente fez a identificação. Qualquer tipo de informação sobre o funcionamento do dispositivo que a NMS receberá, será de acordo com o especificado pela MIB.

Uma variedade de MIBs podem ser adicionadas por um agente. Porém, existe uma MIB obrigatória, onde todo o agente deve implantar, chamada de MIB-II (RFC-1213).

A MIB-II contém as instruções para o gerenciamento da plataforma TCP/IP, além das variáveis para certos tipos de dados, por exemplo, dados estatísticos como bits enviados e recebidos. (MAURO; SCHIMIDT, 2001).

2.5.2.3 RMON (*Remote Monitoring* – Monitoramento Remoto)

É um tipo de MIB. Existem duas versões: RMONV1 (RFC 2819) e RMONv2 (RFC 2021). A versão RMONV1 fornece estatísticas de uma determinada rede LAN ou WAN, a nível de pacotes.

Já a versão RMONv2, expande a versão RMONV1, incluindo as estatísticas à nível de rede e aplicações. (MAURO; SCHIMIDT, 2001).

2.5.3 Operação SNMP

Por padrão, o protocolo SNMP usa o protocolo UDP (*User Datagram Protocol*), através da porta 161 para o transporte de dados na relação entre gerenciadores e agentes. Já para receber os *traps* dos dispositivos monitorados, é usada a porta UDP 162. Por não haver conexão entre os mesmos, o UDP foi escolhido. Outro motivo da escolha do UDP, é o baixo *overhead* (consumo de recursos) na rede, já que se elimina o tráfego de confirmação de recebimento de pacotes.

Não há necessidade de orientação de conexão, visto que própria aplicação SNMP pode detectar a perda de pacotes e reenvia as informações.
Este processo funciona como base no *timeout* (tempo de espera). A NMS transmite uma solicitação UDP com destino ao agente e fica no aguardo de uma resposta. Em caso de não recebimento, o pacote enviado será considerado como perdido e assim a NMS, reenvia a solicitação. (MAURO; SCHIMIDT, 2001).

2.5.4 Operação SNMP no modelo TCP/IP

Tomando como base a pilha de protocolos no modelo de TCP/IP com quatro camadas, será apresentado a seguir quais eventos são causados pelas funções SMNP. Isto é, quando uma NMS ou um agente geram algum *trap* ou uma solicitação, por exemplo. (MAURO; SCHIMIDT, 2001).

2.5.4.1 Camada de Aplicação

Num primeiro momento, a aplicação SNMP, podendo ser uma NMS ou agente deve definir o que será realizado. Por exemplo, o envio de uma solicitação SNMP para um agente ou um envio de *trap* para a NMS.

A camada de aplicação tem a função de oferecer serviços para o usuário final. Isso pode ser comparado, a um operador enviando solicitações sobre o *status* da porta de um roteador, por exemplo. (MAURO; SCHIMIDT, 2001).

2.5.4.2 Camada de Transporte – UDP

A próxima camada é a de transporte. Como informado anteriormente, o SNMP utiliza o protocolo UDP para a comunicação. Dentro do cabeçalho do UDP, estão contidas informações importantes, como a porta de destino do dispositivo. Ou seja, para onde estará sendo enviando a *trap* ou a solicitação gerada. As portas UDP 161 (consulta) ou UDP 162 (*trap*) são utilizadas como porta de destino. (MAURO; SCHIMIDT, 2001).

2.5.4.3 Camada de Internet – IP

Nesta camada, existe a tentativa de fornecimento do destino requerido do pacote SNMP, definido de acordo com o endereço IP. (MAURO; SCHIMIDT, 2001).

2.5.4.4 Camada de Acesso à Rede – *Medium Access Control* (MAC)

Na última camada, ocorre o controle do pacote SNMP na rede física, onde pode ser enviado para o seu destino final. (MAURO; SCHIMIDT, 2001).

2.5.4.5 Exemplificação da Operação SNMP

Na figura 4, é apresentada a relação da NMS e do Agente, quanto as suas atividades no modelo TCP/IP.

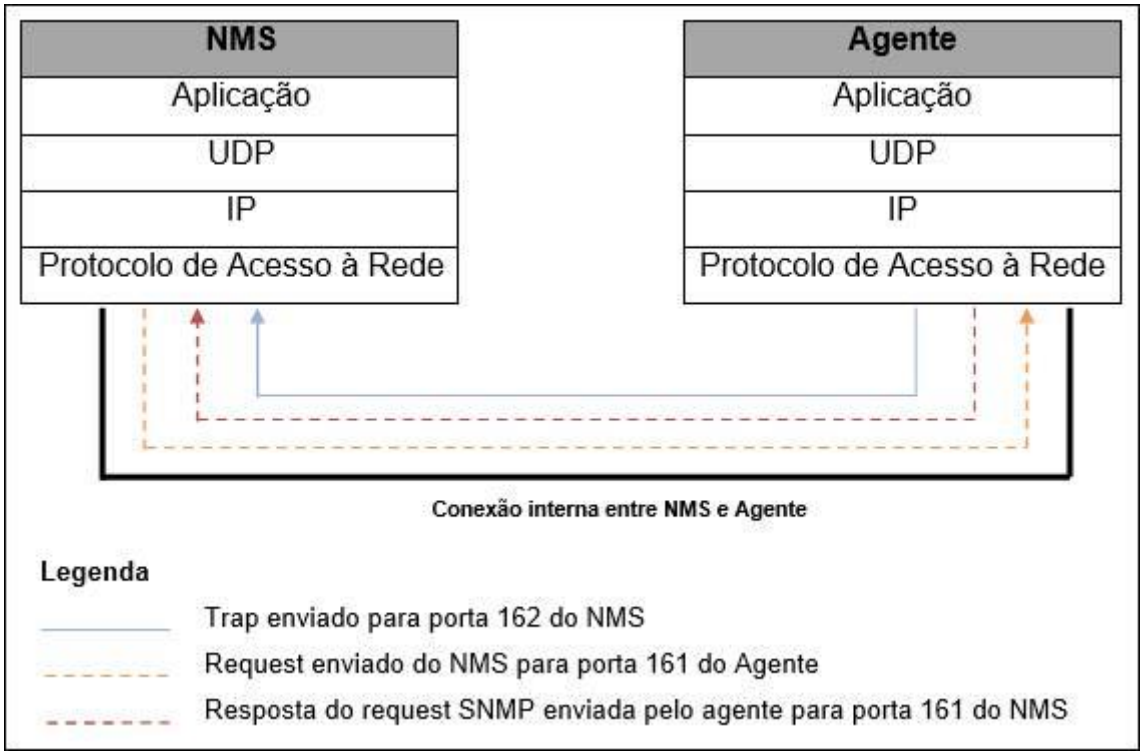

Figura 4 – Comunicação SNMP no modelo TCP/IP
Fonte: Teleco (2015)

2.5.5 Comunidades de SNMP

As versões SNMPv1 e SNMPv2 utilizam a classificação de comunidades para a determinação da confiança entre agentes e gerenciadores. Um agente deve a configuração de três nomes de comunidade: *read-only*, *read-write* e *trap*. Estas comunidades podem ser consideradas como senhas e coordenam

diferentes tipos de atividades. A comunidade *read-only* apenas permite a leitura de valores de dados, como o número de pacotes provenientes das portas de um roteador.

A comunidade *read-write* tem permissão para leitura e modificação de valores de dados, como alteração da configuração de um roteador, por exemplo.

A comunidade *trap* tem permissão para o recebimento de *traps* do agente. (MAURO; SCHIMIDT, 2001).

2.6 Ferramenta de Monitoramento de Rede: *What's Up Gold*

2.6.1 Visão Geral

A ferramenta de monitoramento *What's Up Gold* é um *software* proprietário da empresa *IPSwitch* e até o presente momento está na versão V16.3.

Está estruturado em 3 versões: *WhatsUp Gold Standard Edition*; *WhatsUp Gold Premium Edition* e *Distributed Edition*.

Há suporte para até 20 mil dispositivos que podem ser monitorados. Identificação de dispositivos nas camadas de rede 2 e 3. Ou seja, qualquer dispositivo que disponha de um endereço IP e que é acessível através dos protocolos de monitoramento padrão, tais como ICMP (*Ping*), SNMP, WMI e SSH.

2.6.2 Requisitos Mínimos

2.6.2.1 Requisitos para *hardware*

- Processador: 2 núcleos, 2.4 GHz;
- Memória: 4 GB de RAM;
- Espaço em Disco: 15 GB de espaço livre;

2.6.2.2 Requisitos para *software*

O *WhatsUp Gold* é compatível com a plataforma *Microsoft Windows Server*, nas seguintes versões.

- *Windows Server* 2012/R2;
- *Windows Server* 2008/R2 (64 bits);
- *Windows Server* 2008 (32/64 bits);
- *Windows Server* 2003/R2 (32/64 bits);

Existe a possibilidade de instalação da ferramenta nas versões do *Windows* 7. Porém, dada a criticidade da ferramenta, bem como sua função, é altamente recomendável realizar a instalação em um sistema operacional para uso em servidores (IP*Switch*, 2015):

- *Windows* 7 *Ultimate*/*Enterprise*/*Professional* (32/64 bits);

Software Gerenciador de Banco de Dados (SGBD).

- *Microsoft* SQL *Server* 2012 *Standard*/*Enterprise (*32/64 bits), local/remoto;

- *Microsoft* SQL Server 2008 R2 *Standard*/*Enterprise* (32/64 bits), local/remoto;
- *Microsoft* SQL *Server* 2008/R2 *Express Edition* (32/64 bits), somente local/remoto;
- *Microsoft* SQL *Server* 2005 *Standard*/*Enterprise* (32/64 bits), local/remoto;

Servidor *Web*.

- *Microsoft Internet Information Services* (IIS) 6/7/8.

Serviços de Função de Servidor *Web* IIS 7/8:

- ASP .NET;
- Conteúdo Estático;
- Redirecionamento *Hypertext Transfer Protocol* (HTTP);
- Documento Padrão;

Plataformas de Virtualização:

- *VMware vCenter Server* 4 e 5;
- *VMWare* ESXi 3.5, 4 e 5;
- *VMware* ESX 3.5 e 4;
- *Microsoft Windows Server* 2008 R2 *Hyper-V*;
- *Microsoft Windows Server* 2012 *Hyper-V*;

Navegadores *Web*

- *Google Chrome* (recomendado)
- *Microsoft Internet Explorer* 9/10
- *Mozilla Firefox* versão 36.0.1

3 Diagnóstico do Ambiente e Estudo de Caso

3.1 Introdução

Em diversos armazéns, como mercados e centros de logística, onde há grande quantidade de materiais à serem controlados, são utilizados computadores portáteis mais conhecidos como coletores de dados. Estes por sua vez, contém uma conexão com o *software* de gerenciamento destes armazéns, que são conhecidos como um exemplo de WMS – *Warehouse Management System*. A maioria dos coletores modernos, possui várias ferramentas para analisar a condição da rede sem fio em que estão conectados, de forma que, trocam de antena dinamicamente caso encontrem uma antena com um sinal mais forte. A figura 5 mostra um exemplo de um coletor de dados da fabricante Motorola.

Figura 5 – Coletor de Dados Motorola MC9190-G
Fonte: Zebra Technologies Corporation (2015)

Porém, para o operador do equipamento não deve haver preocupação com o estado da rede. Esta tarefa pertence ao administrador de rede. Por se tratar de um processo de alto impacto para o negócio da organização que dispõe de um armazém, o tempo de resposta para o atendimento às ocorrências é de vital importância. Neste conceito, pode-se aplicar a maturidade do departamento de TI (Tecnologia da Informação) da organização.

Se os usuários precisam informar ao departamento de TI, sobre às ocorrências detectadas, pode-se classificar este setor como reativo.
Mas qualquer setor de TI, pode se transformar dentro do conceito proativo. Um exemplo clássico, seria se este departamento realizasse a implantação de um sistema de monitoramento na rede.

3.2 Situação

Baseando nas informações acima, é possível simular um ambiente tendo como plataforma, uma organização que tenha como área de atuação, o ramo da logística e o armazenamento seja de produtos para exportação ou importação.

Como dito anteriormente, para o controle dos produtos no armazém, é necessário o uso dos coletores de dados, garantindo assim a mobilidade e a flexibilidade da operação. Como estes dispositivos são portáteis, é um requisito obrigatório a disposição de uma infraestrutura de rede sem fio.

Normalmente uma estrutura deste tipo é composta pelos seguintes equipamentos: *Access Points*, Fontes PoE ou *Switchs* PoE. Algumas infraestruturas mais modernas, possuem uma controladora, que fornece funções de gerenciamento à rede. Um exemplo deste tipo de equipamento é o Motorola RFS7000. A quantidade destes equipamentos será definida de acordo com a definição da área de abrangência da rede sem fio.

Um departamento de TI reativo, espera que os problemas serão apresentados pelos usuários da rede, o que gera um desperdício considerável de tempo, além do impacto na operação que pode ficar parada à espera da solução do problema. Por exemplo, um determinado local do armazém, está sem sinal da rede. Para identificar o problema, é necessário percorrer toda área afetada, em busca da antena responsável pela distribuição do sinal, já que provavelmente não deve haver nenhum tipo de mapa dos dispositivos que compõem esta rede.

Na figura 6, apresenta uma visão geral de um armazém com uma topologia de rede sem fio para uso dos coletores de dados.

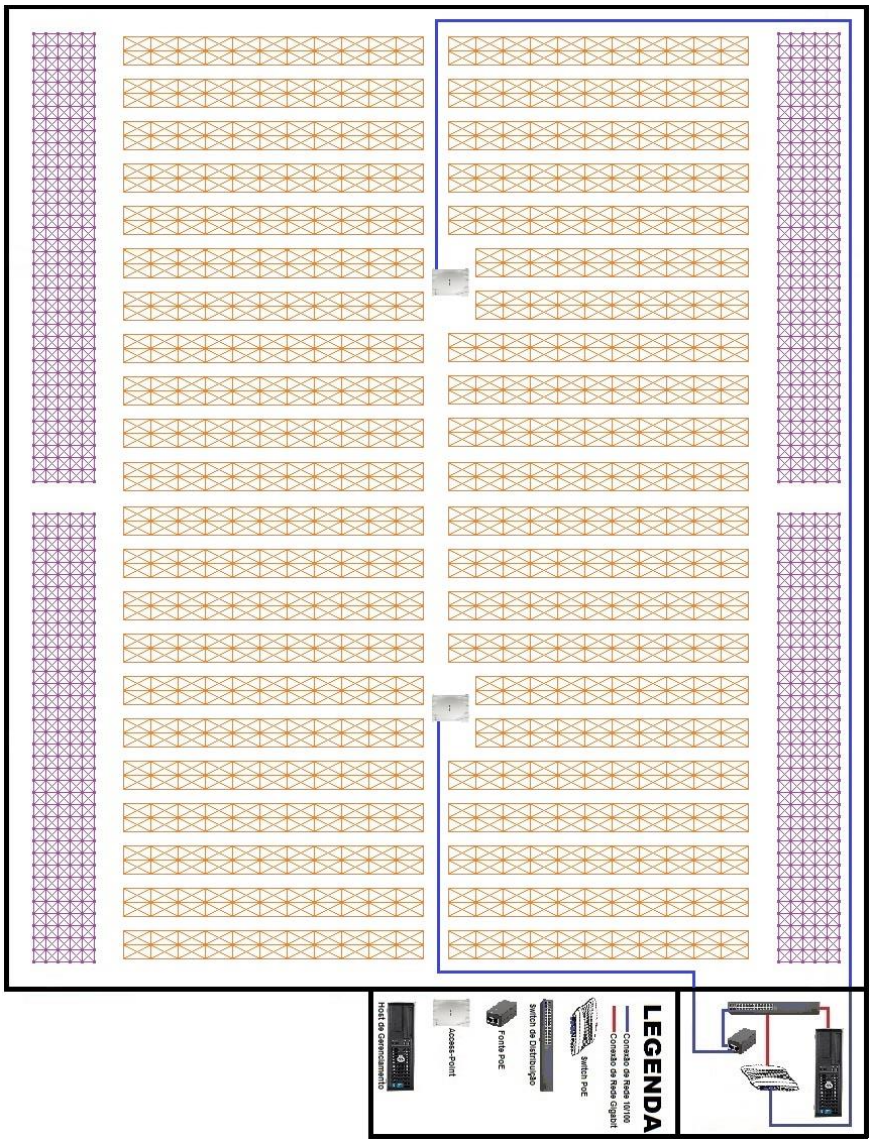

Figura 6 – Planta de um Armazém para Estudo de Caso
Fonte: Autoria Própria (2015)

Este estudo pretende atuar no problema apresentado acima, apresentando uma solução eficaz no gerenciamento desta infraestrutura de rede, seguindo o propósito de transformar o departamento de TI de reativo em proativo.

3.3 Definição de Equipamentos

Neste tópico serão apresentados, os equipamentos à serem usados no estudo de caso visando simular o ambiente descrito acima.

3.3.1 *Access Point Symbol* AP300

Na figura 7, está representado o modelo de *Access Point Symbol* AP300. Este dispositivo trabalha nos seguintes padrões de conectividade IEEE 802.11 para WLAN: 802.11a, 802.11b, 802.11g. Atua na faixa de 2.4 GHz à 5.2 GHz. Utiliza a conexão RJ-45 PoE. (Motorola Inc, 2015)

Figura 7 – Access Point Symbol AP300
Fonte: PenMobile (2015)

3.3.2 *Wireless Switch Symbol* WS 2000

Na figura 8, está representado o dispositivo *Wireless Switch Symbol* WS 2000. Este equipamento pode suportar até quatro conexões PoE para *access-points*. Opera nos seguintes padrões de conectividade IEEE 802.11 para WLAN: 802.11a, 802.11b, 802.11g. Oferece suporte à SSH, SNMP v1/v2 /v3, Roteamento, DHCP, NAT, *Firewall*, IPSec, VPN, ACL, Java *Applet* (HTTP, HTTPS) e Syslog. (Motorola Inc, 2015)

Figura 8 – Wireless Switch Symbol WS 2000
Fonte: BarcodesInc (2015)

3.3.3 Fonte PoE Motorola *Power Injector*

Na figura 9, está representada uma típica fonte PoE. Em alguns casos, pode ser necessária a instalação de uma fonte separada para a alimentação de um *access-point*. Essas situações ocorrem quando é esgotada a capacidade máxima de conexões em um *Switch* PoE ou quando apenas é necessário o uso de uma conexão PoE, dispensando o uso de um *Switch*. Este dispositivo opera na conexão *Ethernet* 10/100 Mbps e é compatível com os *access-points* AP300 e AP-5131. (Motorola Inc, 2015)

Figura 9 – Fonte PoE Motorola Power Injector
Fonte: Notebook Center (2015)

3.3.4 Computador Dell Optiplex 380

Na figura 10, está representado um típico computador de mesa pessoal. Como se trata de um ambiente de testes, este equipamento serve para o propósito. As especificações deste dispositivo são: Processador Intel Core 2 Duo E7500 2.93 GHz, Memória 4 GB, Disco Rígido de 160 GB, Conexão *Ethernet* 10/100/1000 Mbps, Sistema Operacional *Windows* 7 Profissional. (Dell Inc 2015).

Figura 10 – Computador Dell Optiplex 380
Fonte: Dell Inc (2015)

3.3.5 Switch 3Com 2928 SFP PLUS

Na figura 11, está representado um *switch* da marca 3*Com* como o modelo 2928 SFP *PLUS*. Possui 28 portas 10/100/1000 Mbps. Suporte a SNMP, *snooping* e *query* IGMP. Priorização de tráfego (802.1p). Configuração

Web-based, CLI limitado usando porta de console. ACLs. IEEE802.1d-*SpanningTree*; IEEE802.1p-*PriorityTags*; IEEE802.1Q-VLANs; IEEE802.1X-*PortSecurity*; IEEE802.1w-*RapidSpanningTree*; IEEE802.3-*Ethernet*; IEEE802.3ab-*GigabitEthernet*; IEEE802.3ad-*LinkAggregation*; IEEE802.3u-*FastEthernet*; IEEE802.3x-*FlowControl*; IEEE802.3z-*GigabitEthernet*; ISO8802-3. (Atera Informática, 2015).

Figura 11 – Switch 3Com 2928 SFP PLUS
Fonte: Plameni, Mikrotik Forúm (2015)

3.4 Diagrama de Topologia de Rede

Na figura 12, apresenta uma topologia de rede simples para o estudo de caso proposto. Nesta topologia, há um *host* de gerenciamento com a ferramenta de monitoramento implantada. Logo abaixo, um *switch* central para acesso à rede. Já a esquerda abaixo do *switch*, uma fonte PoE conectando um *access-point* e a direita, um *switch* PoE conectando outro access-point.

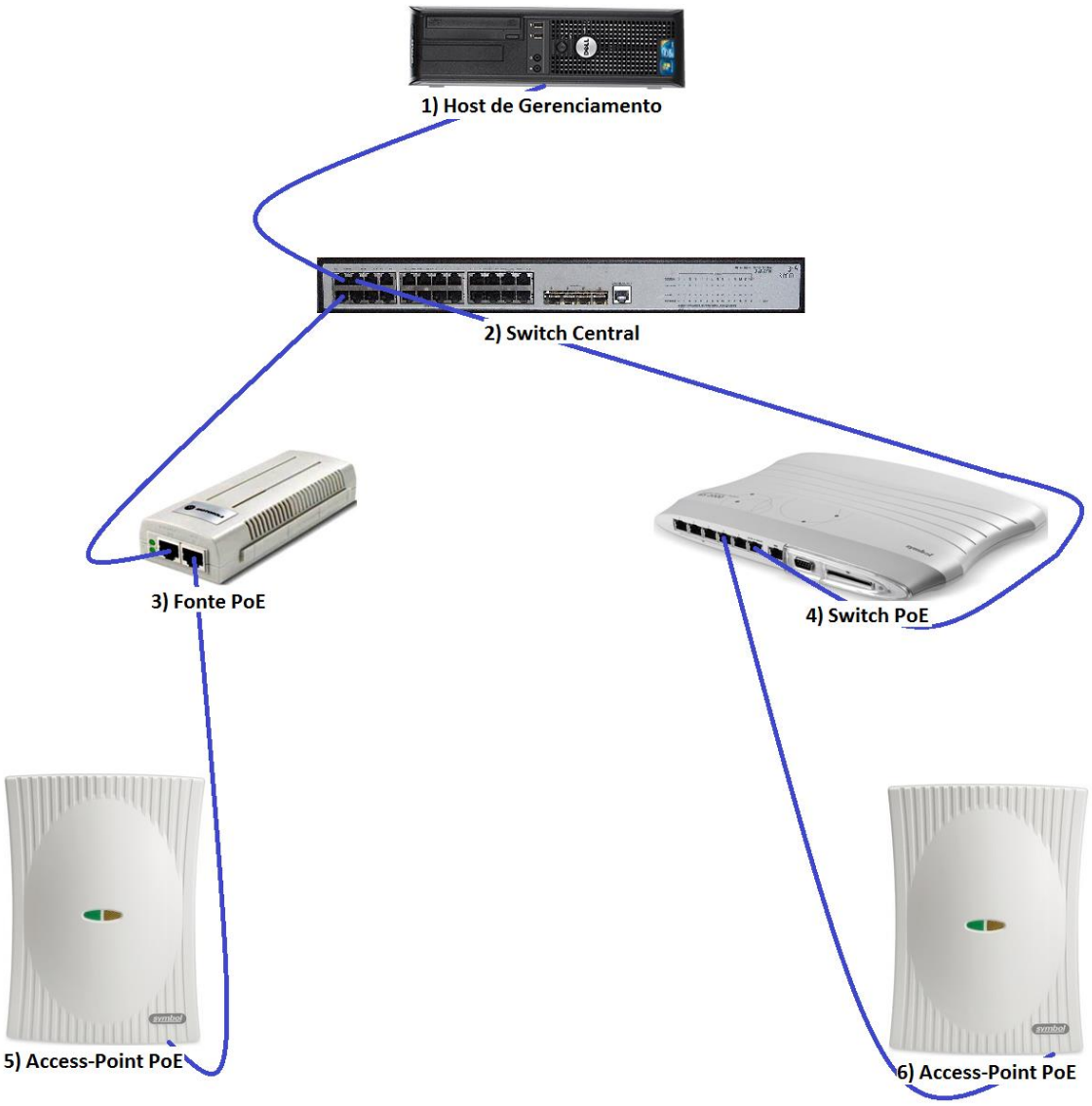

Figura 12 – Diagrama de Topologia de Rede
Fonte: Autoria Própria

3.5 Configuração Básica Windows Server 2008 R2

Antes de ser realizada a instalação da ferramenta, é necessário configurar o serviço SNMP do *Windows Server*. Isto é necessário para garantir que a ferramenta poderá enviar os pacotes SNMP aos dispositivos.

Após a instalação do serviço, devemos editar os parâmetros do agente SNMP conforme figura 13, por exemplo. Neste caso, selecionamos todos os serviços disponíveis.

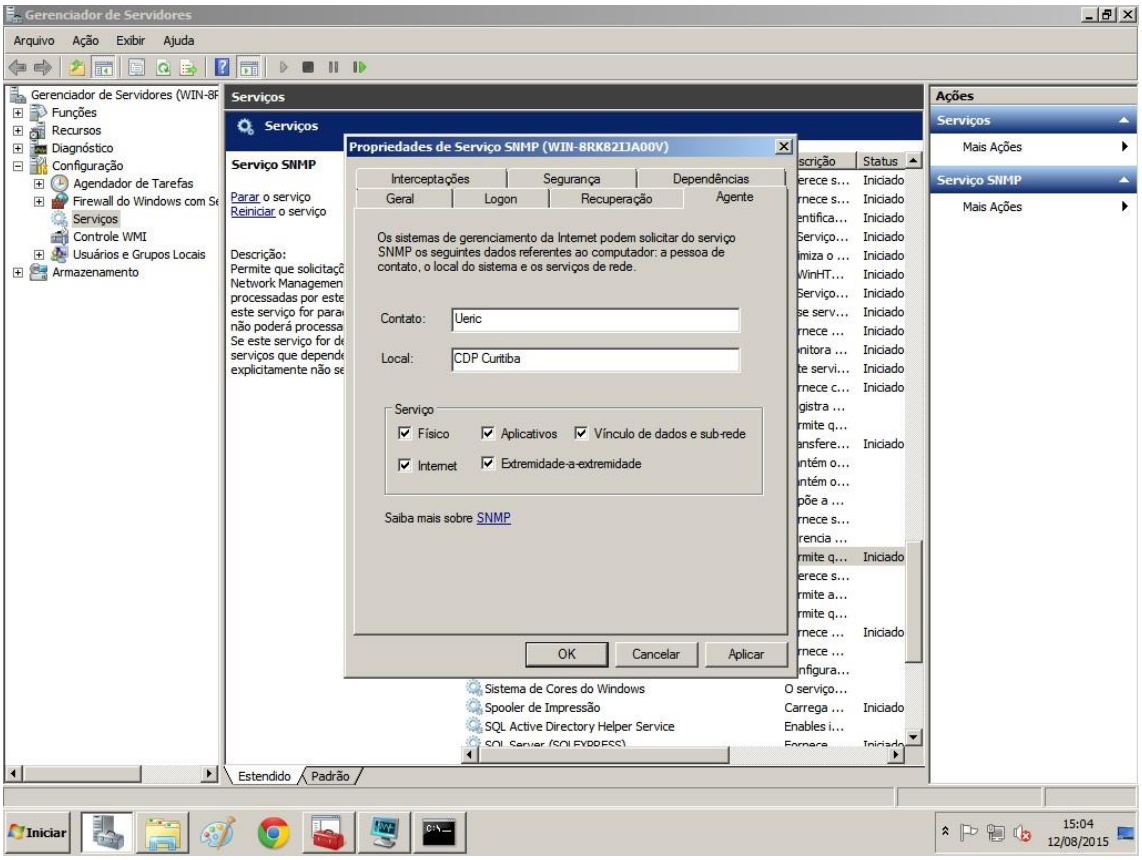

Figura 13 – Configuração Agente SNMP
Fonte: Autoria Própria

Na guia segurança, é obrigatório configurar o IP do *host* onde a ferramenta de monitoramento está instalada. Por questões de segurança, apenas uma será definida conforme figura 14.

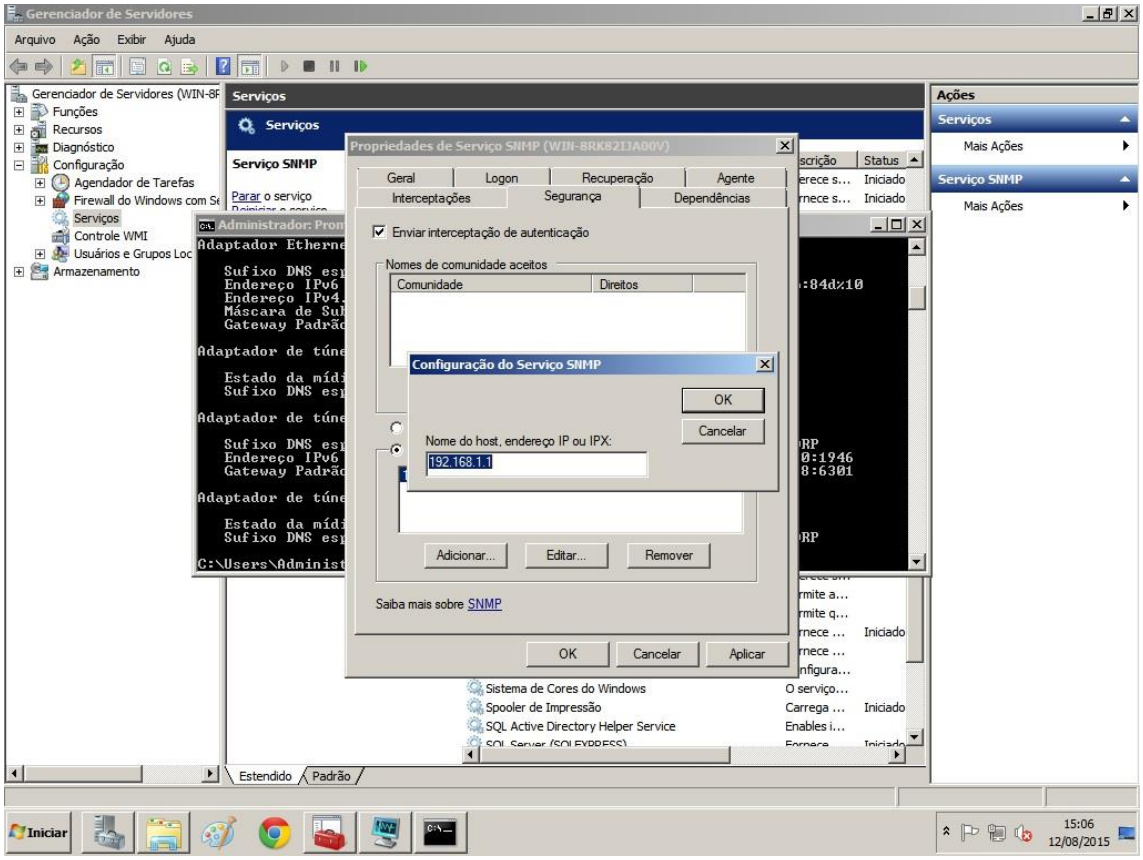

Figura 14 – Definição de IP de host de gerenciamento SNMP
Fonte: Autoria Própria

Continuando na guia segurança, onde é definido o nome da comunidade que os hosts SNMP dos membros que estão dentro da comunidade e tem a autenticação necessária para o envio das solicitações SNMP para *host* de gerenciamento. A definição deste nome de comunidade é como uma senha compartilhada pelos *hosts* SNMP. Caso seja enviada uma mensagem ao agente SNMP de uma comunidade não conhecida ou por algum host não aceitável, haverá uma falha na autenticação SNMP. Estes nomes de comunidade somente são utilizados para a autenticação das mensagens recebidas.

No campo direito da comunidade, definimos a opção “somente leitura” não que há necessidade para qualquer modificação pelo host SNMP dos objetos gerenciados pelo agente SNMP. (*Microsoft Corporation*, 2015)

A figura 15 apresenta o procedimento de criação da comunidade.

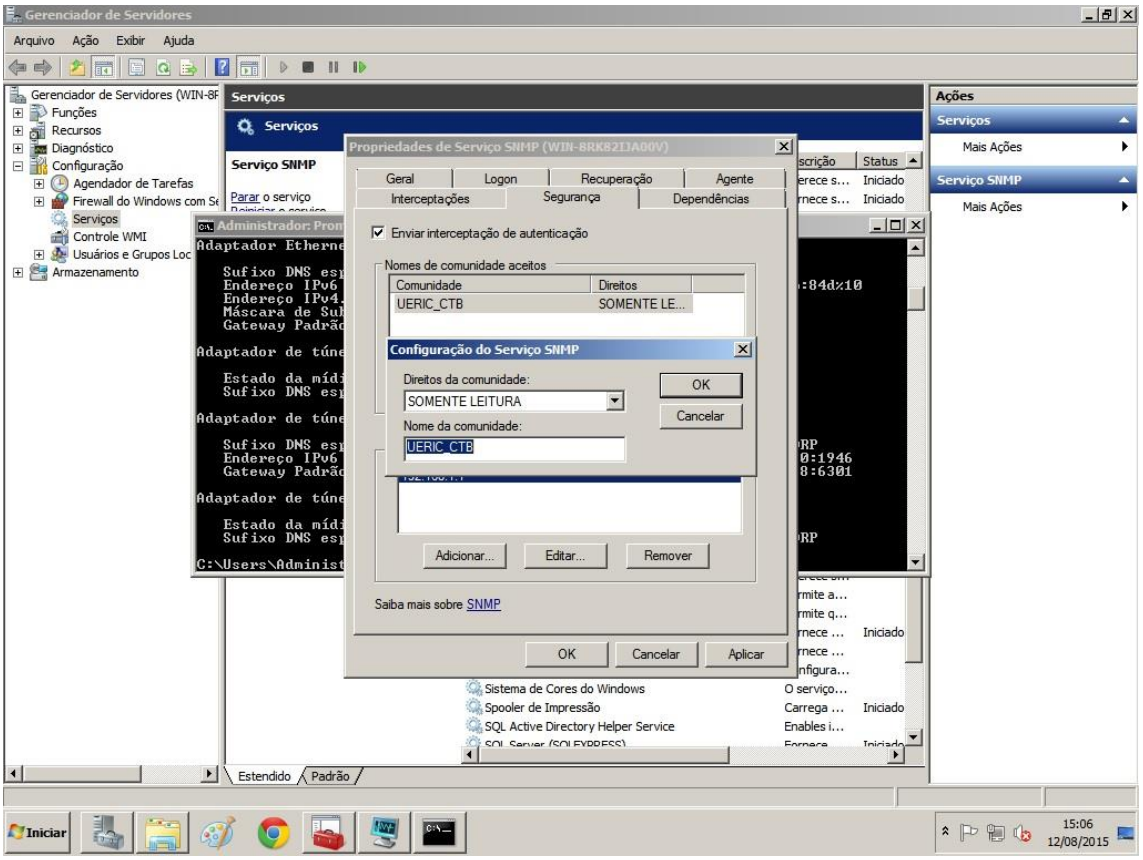

Figura 15 – Definição do nome de comunidade SNMP
Fonte: Autoria Própria

3.6 Instalação e Configuração Básica WhatsUp Gold

Nesta seção, será demonstrada as configurações básicas da ferramenta de monitoramento *WhatsUp Gold*. Alguns processos como o licenciamento da ferramenta não serão abordados.

Na figura 16, está representada a tela inicial de configuração. Escolhemos a opção *Standard*, pois a aplicação será instalada em um ambiente construído apenas tendo como objetivo, o suporte para a operação da ferramenta. Além do uso de configurações padrão dos sistemas *Microsoft*.

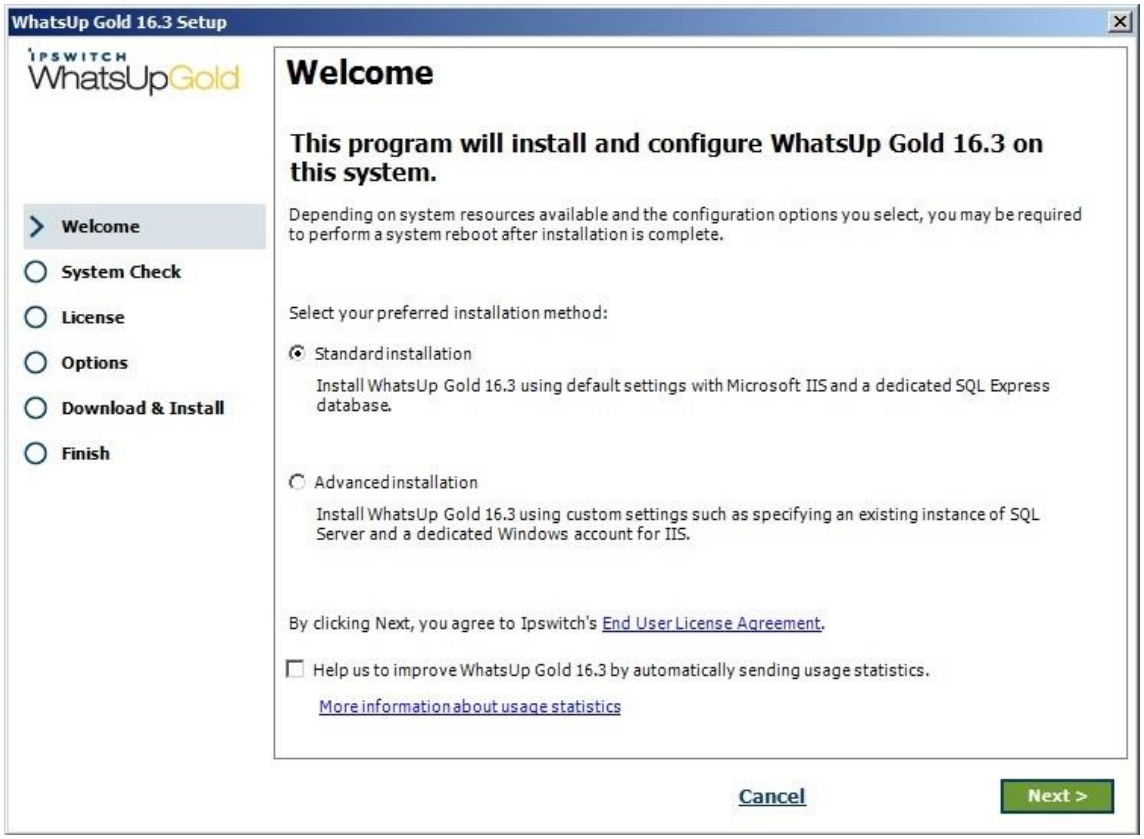

Figura 16 – Tela Inicial de Configuração - WhatsUp Gold
Fonte: Autoria Própria

A figura 17, apresenta o passo seguinte da instalação, onde a ferramenta fez uma varredura do sistema em que foi implantada e detectou os itens que necessitam ser instalados. Todo este processo necessita de conexão com a *internet*.

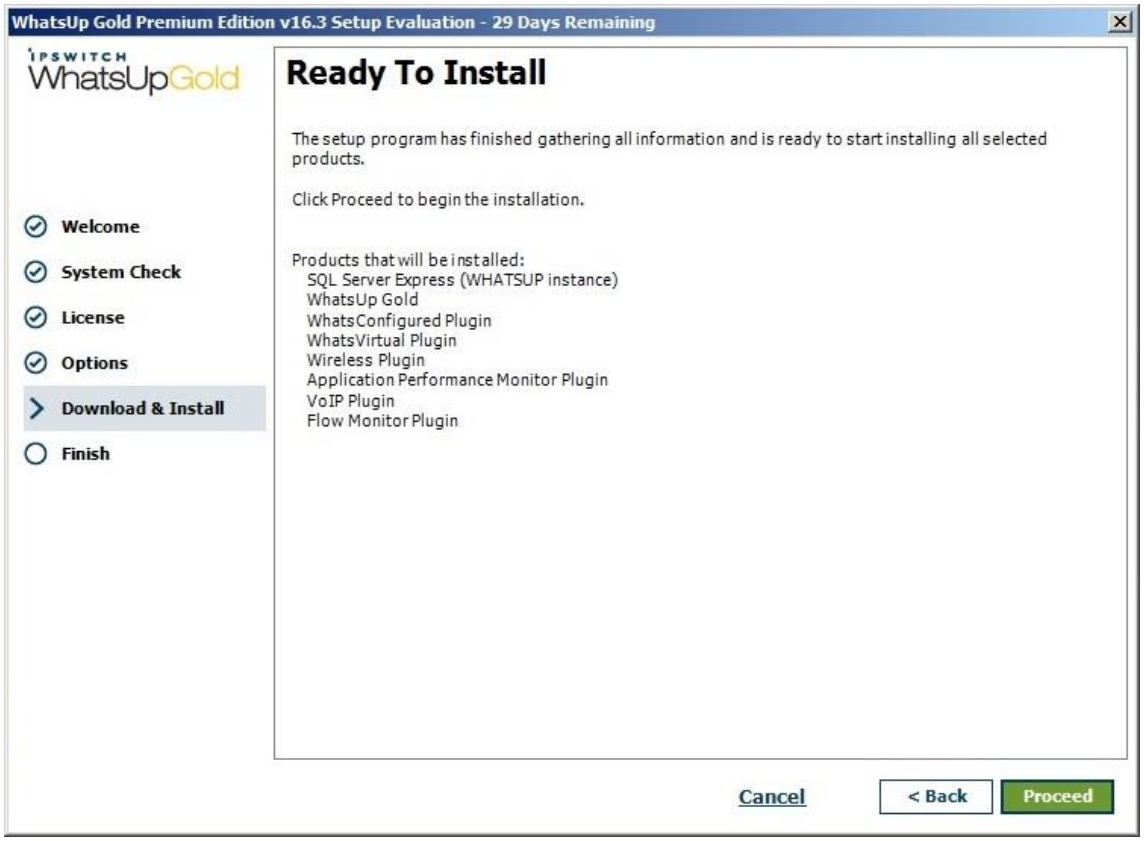

Figura 17 – Identificação dos Requisitos de Instalação
Fonte: Autoria Própria

Após a instalação, o próximo procedimento é a configuração de uma senha de acesso ao console de gerenciamento da aplicação. A figura 18, apresenta a interface para definição da senha de acesso. É notório que o acesso é realizado via *web browser*. Isso garante uma grande flexibilidade da aplicação, visto que não é necessário acessar o *host* onde a ferramenta se encontra instalada.

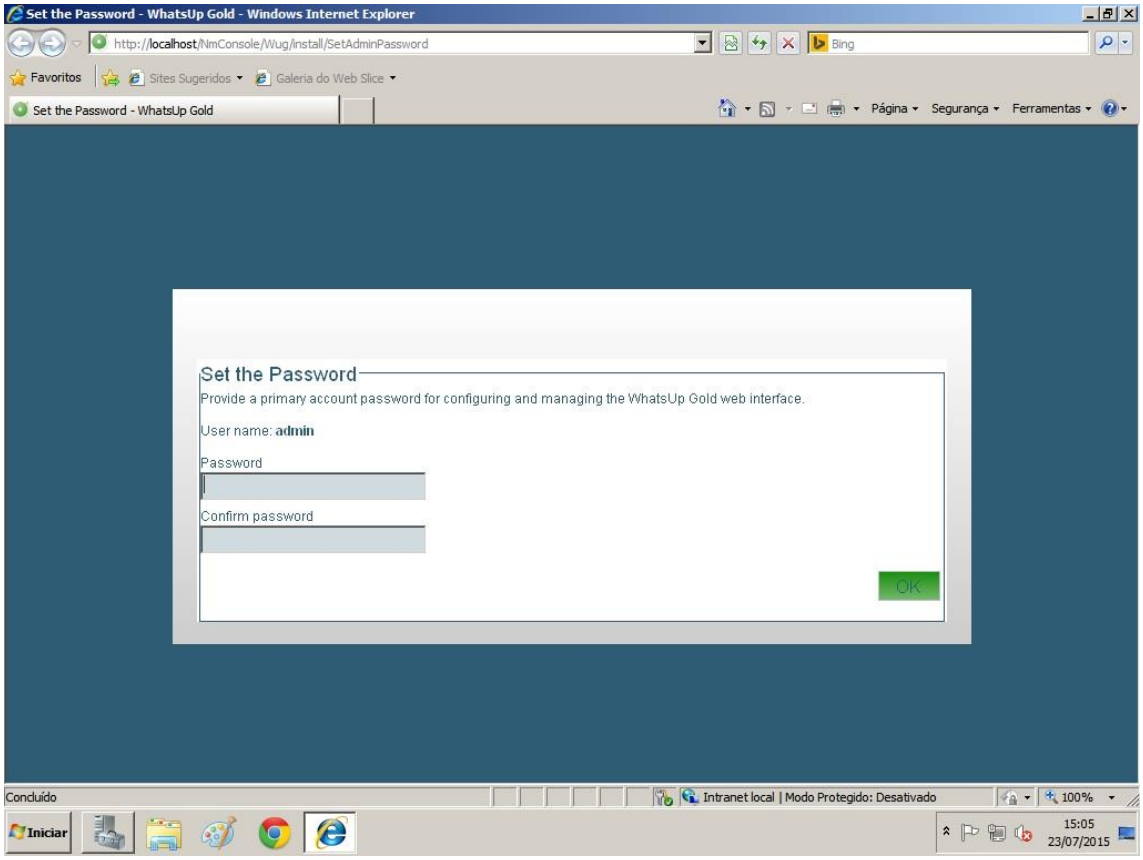

Figura 18 – Interface de Definição de Senha de Acesso
Fonte: Autoria Própria

Na figura 19, é o momento que ocorre a definição do escopo de DHCP a ser monitorado pela ferramenta. Como se trata de um ambiente de testes tendo como base uma rede de pequeno porte, o escopo escolhido foi um range de IP's na classe C.

Com base neste parâmetro utiliza-se a opção IP *Range Scan*, para definição do escopo. Porém, no estudo de caso, como são ip's fixos, foi definido que adição dos dispositivos será feita manualmente a qualquer momento, após a instalação.

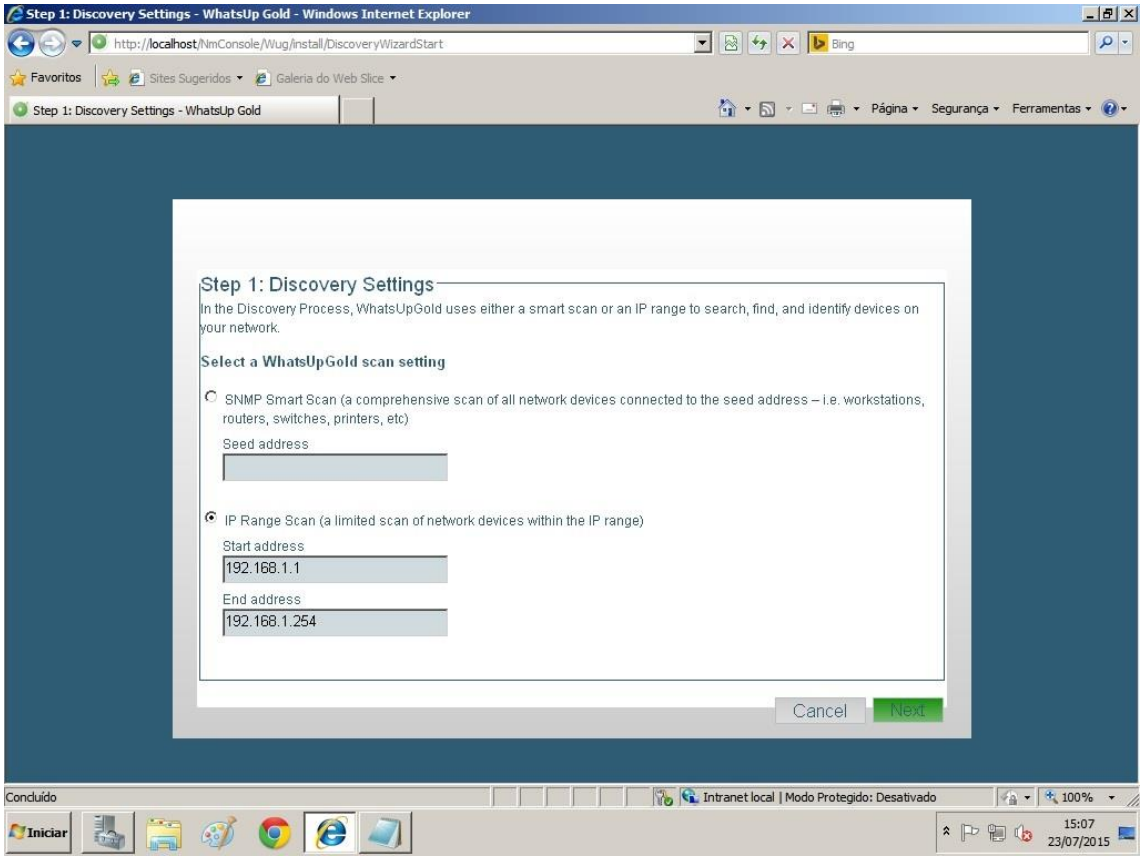

Figura 19 – Definição do Escopo de DHCP
Fonte: Autoria Própria

Na figura 20, é o momento onde há definição da credencial SNMP, onde utiliza-se o nome de comunidade que foi criado conforme a figura 15.

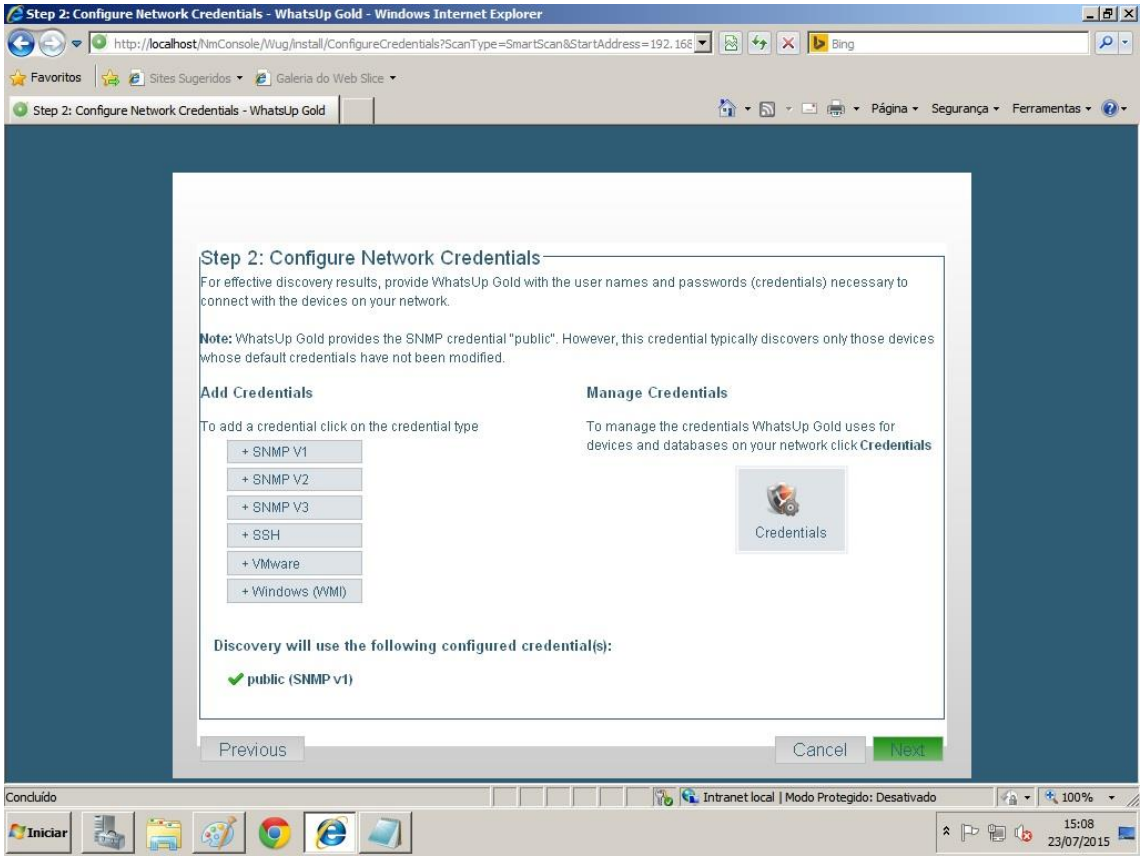

Figura 20 – Definição de Credenciais SNMP
Fonte: Autoria Própria

Na figura 21, está representado o console de administração da ferramenta *What's Up Gold*. Nesta tela, é selecionada a opção "*New Group*" para definir o nome do conjunto dos dispositivos monitorados.

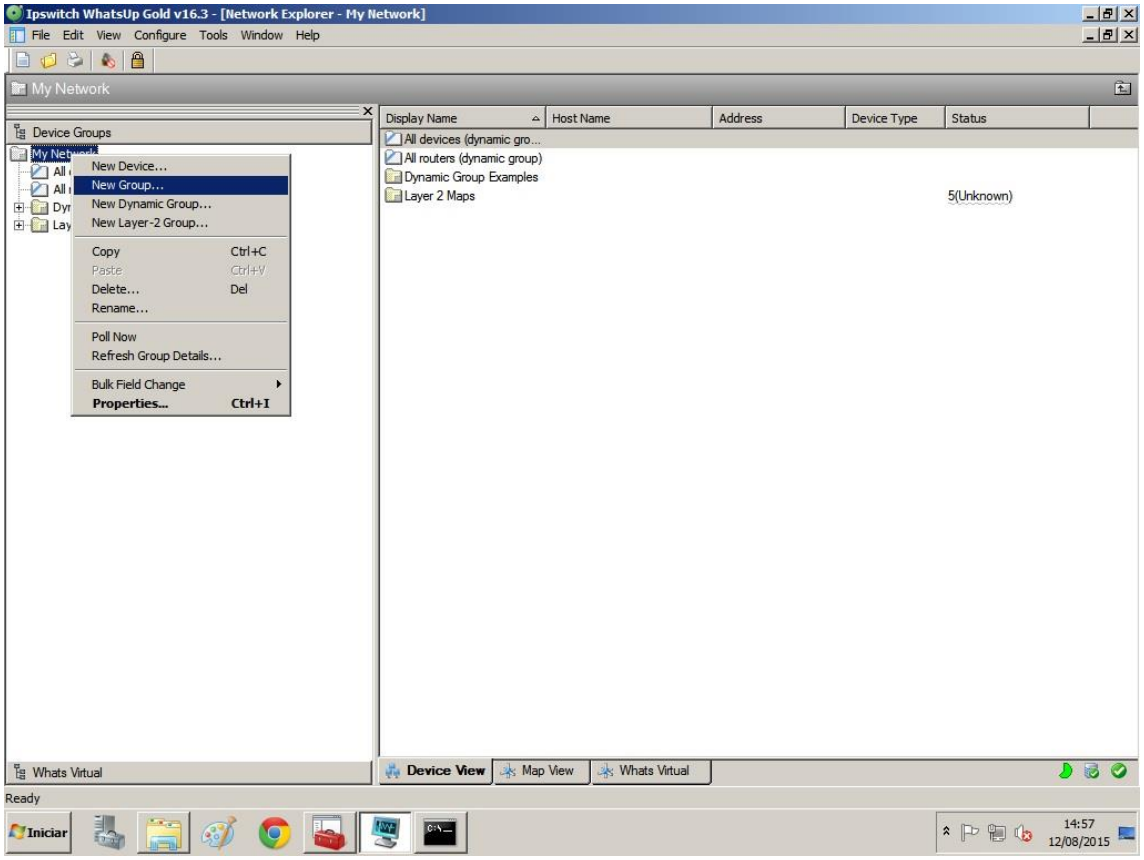

Figura 21 – Console de Administração
Fonte: Autoria Própria

Na figura 22, é adicionado quais são os dispositivos serão monitorados dentro do grupo criado anteriormente, utilizando a opção “*New Device*”.

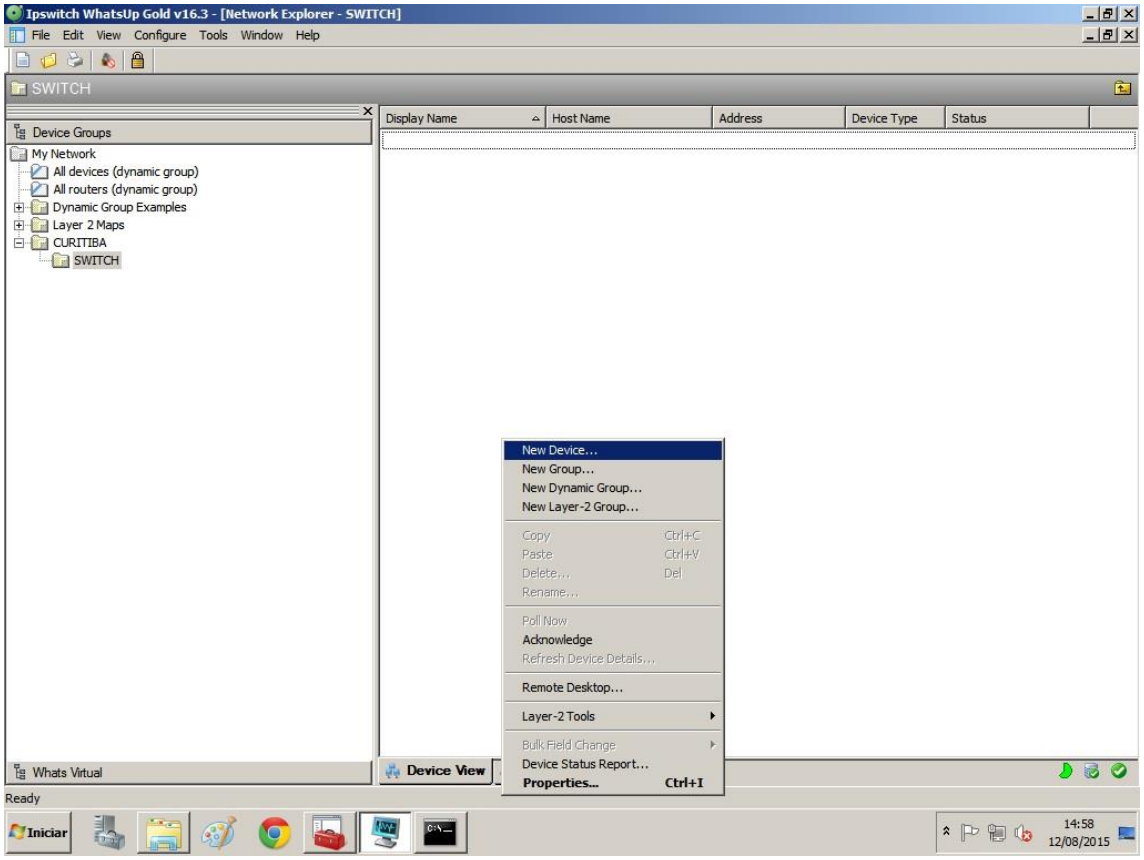

Figura 22 – Cadastro de Dispositivos
Fonte: Autoria Própria

Na figura 23, é definido o IP do dispositivo. Neste caso o IP definido é o 192.168.1.1, que é o IP do host de gerenciamento da figura 12.

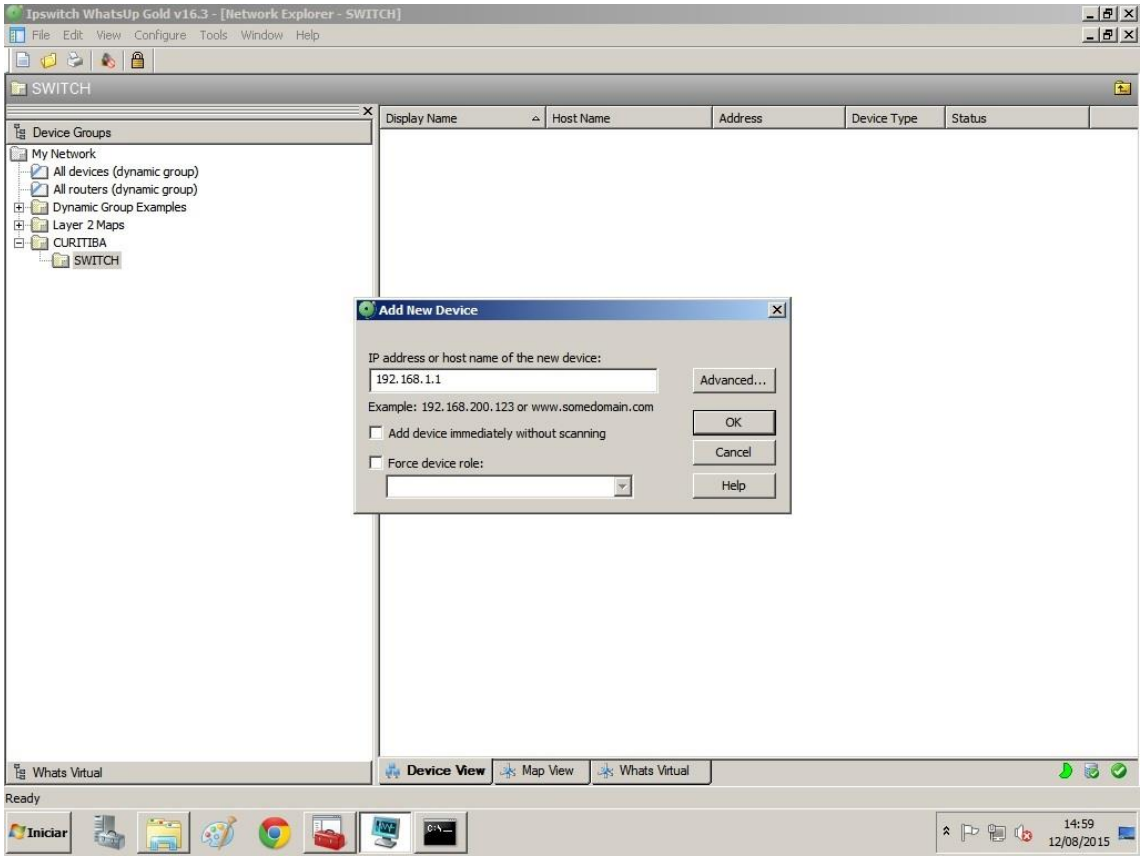

Figura 23 – Cadastro de IP Dispositivos
Fonte: Autoria Própria

Na figura 24, após o dispositivo ser descoberto, a ferramenta de monitoramento What's Up Gold, apresenta todas as informações reunidas do dispositivo.

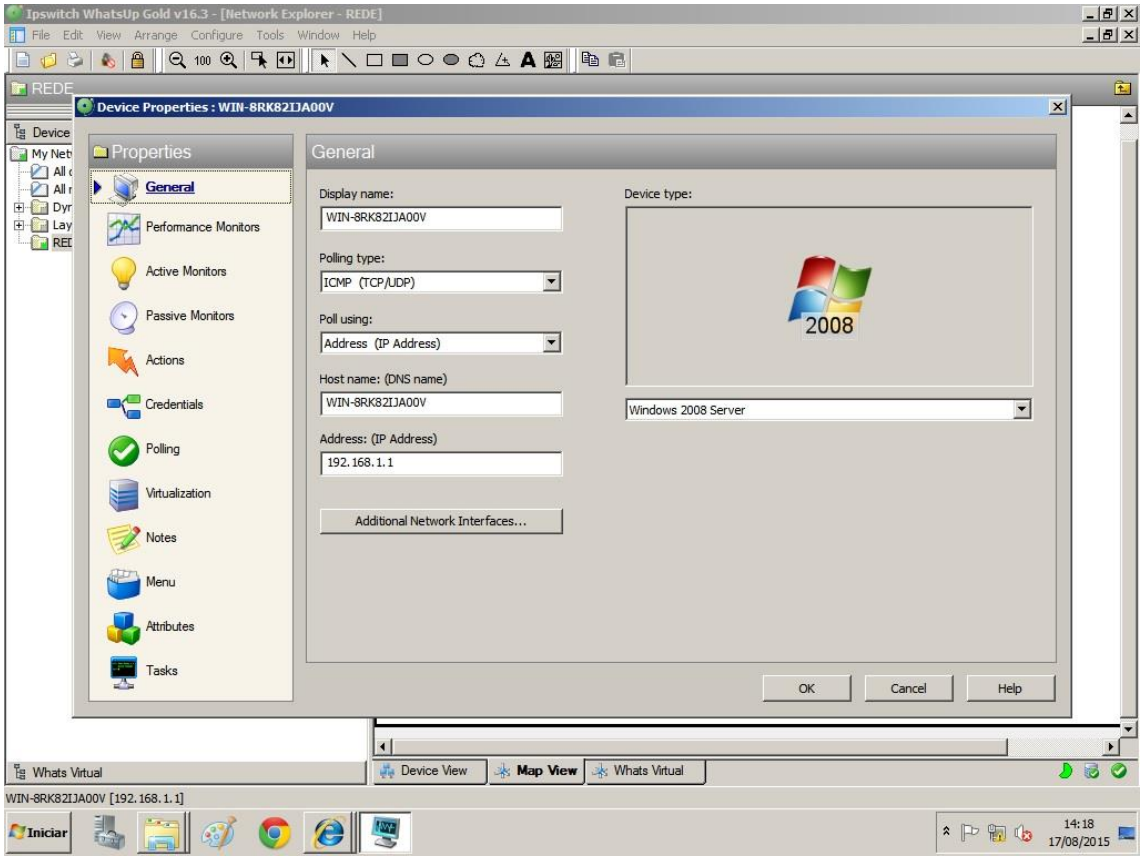

Figura 24 – Identificação de Dispositivo
Fonte: Autoria Própria

Na figura 25, a ferramenta identificou os principais recursos de *hardware* do *host* de gerenciamento que podem ser monitorados na guia "*Performance Monitors*".

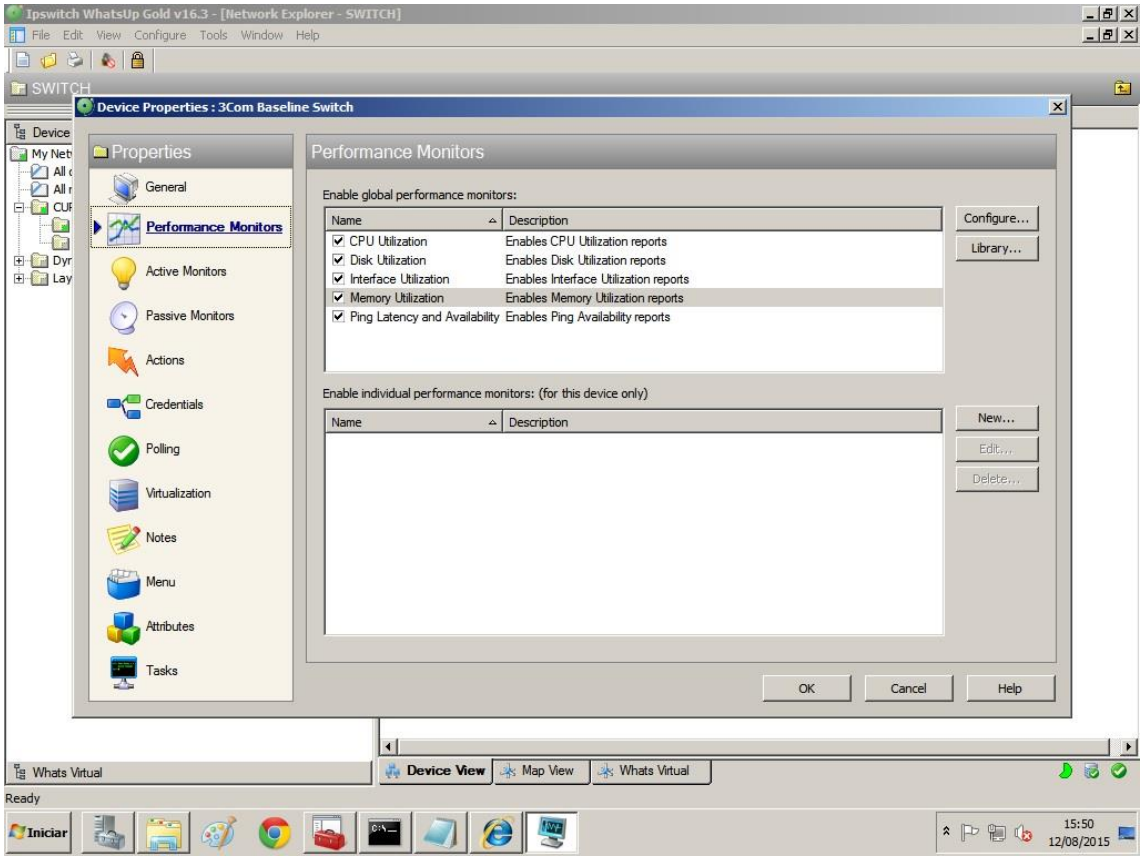

Figura 25 – Recursos do Dispositivo
Fonte: Autoria Própria

Na figura 26, na guia "*Active Monitors*" é o momento onde há a possibilidade da criação dos monitoramentos críticos aqui propostos neste estudo de caso. Num primeiro momento, é definido o monitoramento do recurso de "*ping*" do *host* de gerenciamento para verificar se o mesmo está se comunicando normalmente na rede.

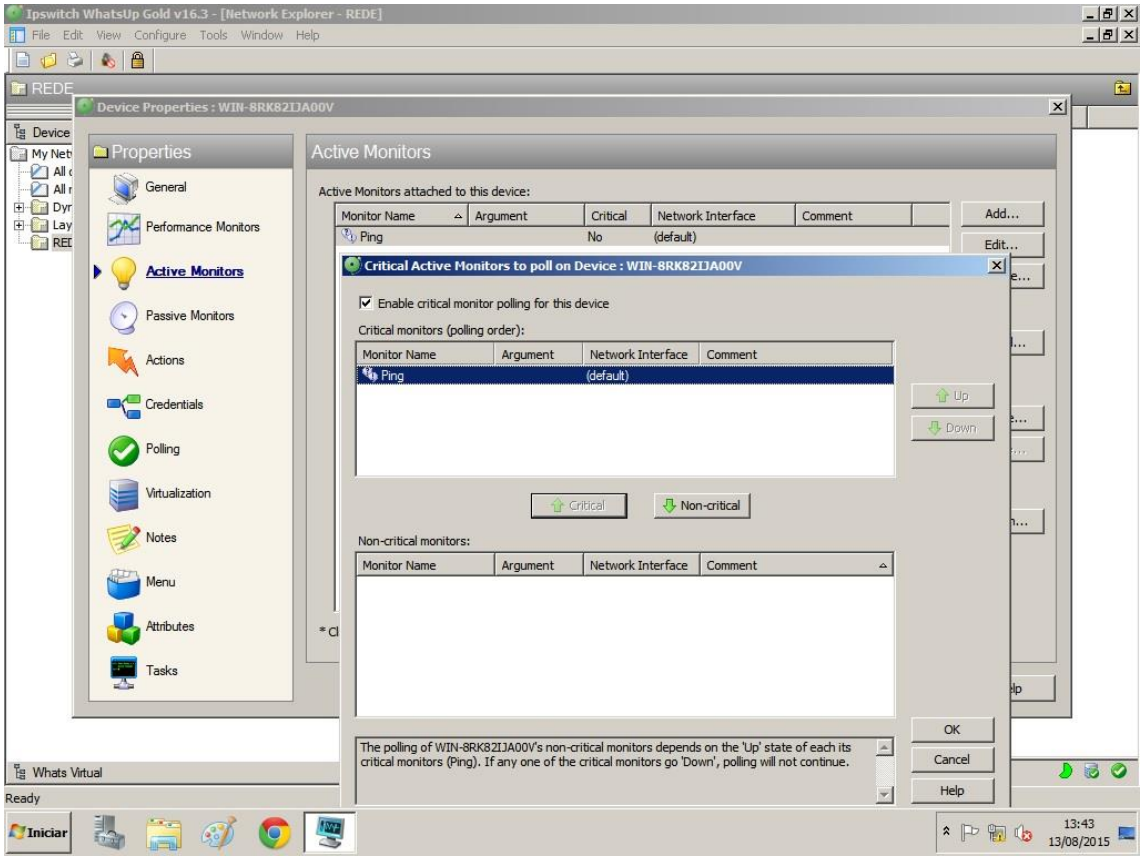

Figura 26 – Definição de Criticidade do Dispositivo
Fonte: Autoria Própria

Na figura 27, é selecionada qual será a ação tomada em caso do dispositivo monitorado apresente falha de comunicação na rede.

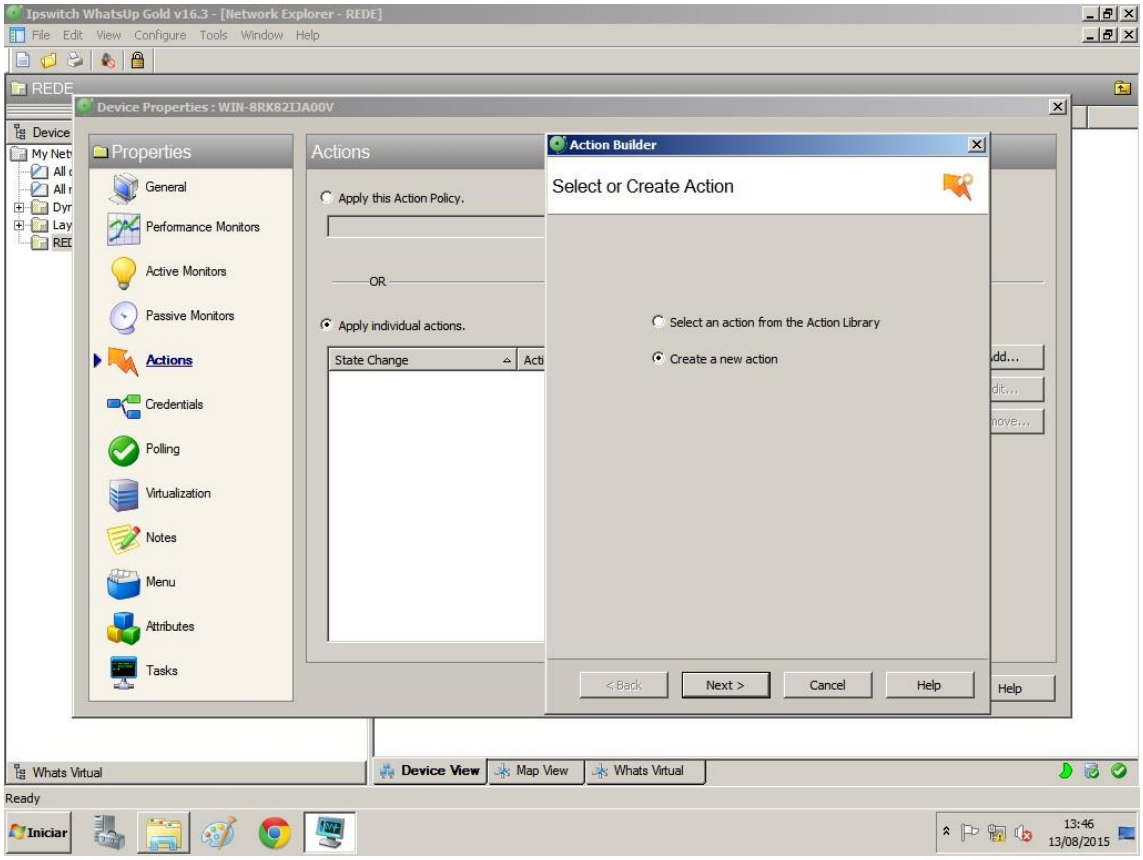

Figura 27 – Criação de ação para identificação de falha no dispositivo.
Fonte: Autoria Própria

Na figura 28, é definido que será disparado um alarme no portal de administração da ferramenta.

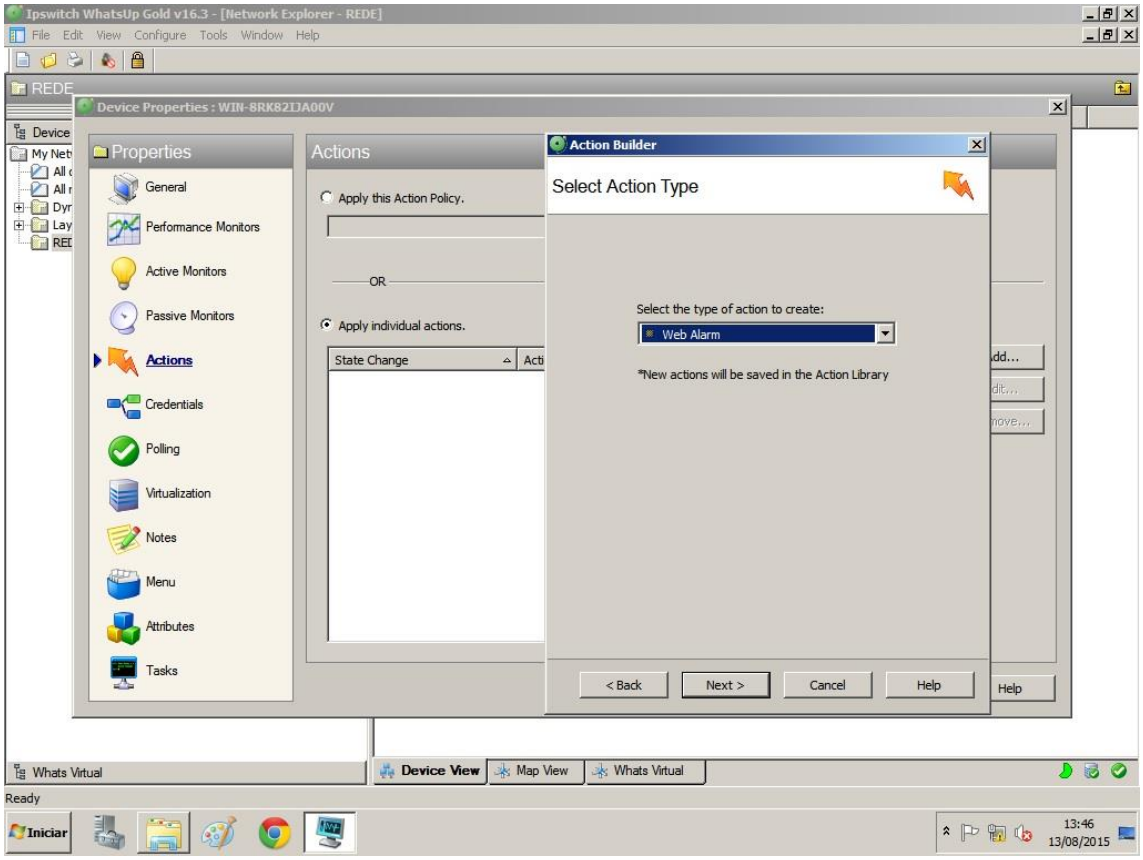

Figura 28 – Definição de ação em caso de falha no dispositivo.
Fonte: Autoria Própria

Na figura 29, é definido de quanto em quanto tempo, a ferramenta verificará a comunicação do dispositivo.

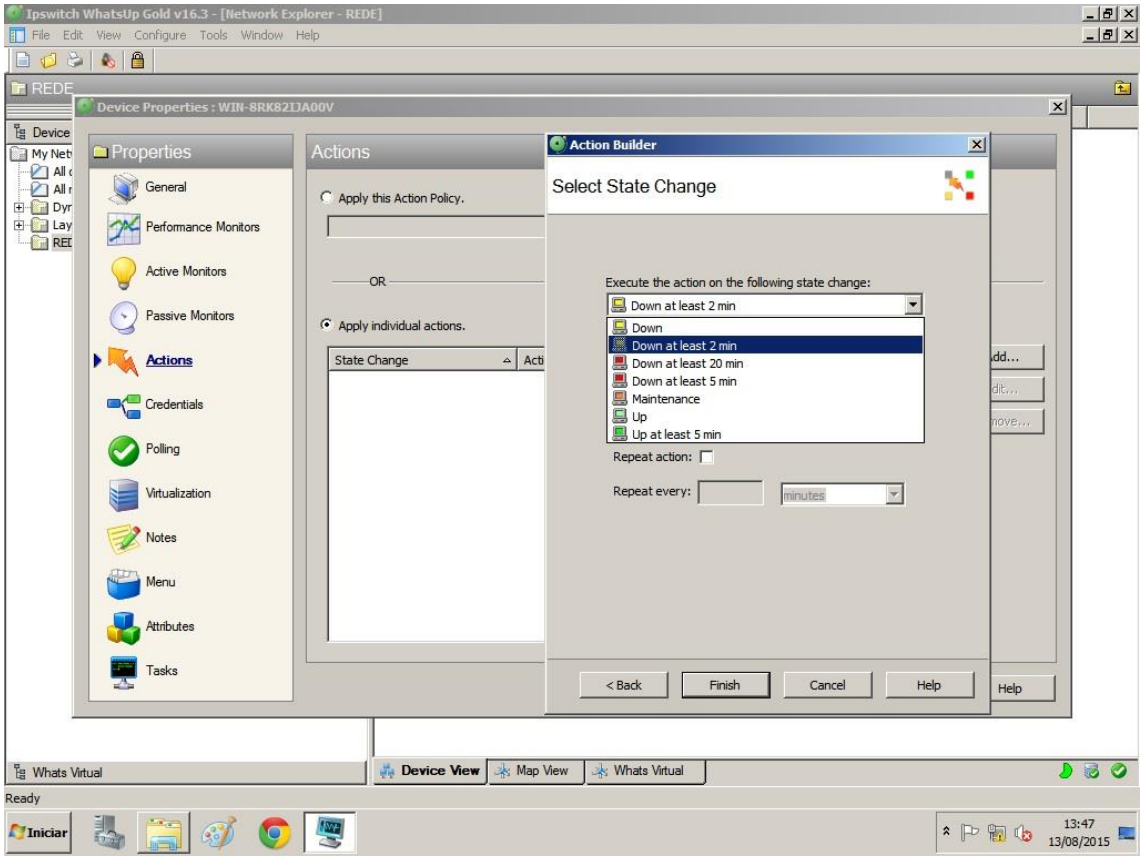

Figura 29 – Tempo de Monitoramento.
Fonte: Autoria Própria

Na figura 30, é definido o período de tempo que o monitoramento será realizado. Dada a criticidade do dispositivo, optou-se por um monitoramento 7 dias por semana e 24 horas por dia.

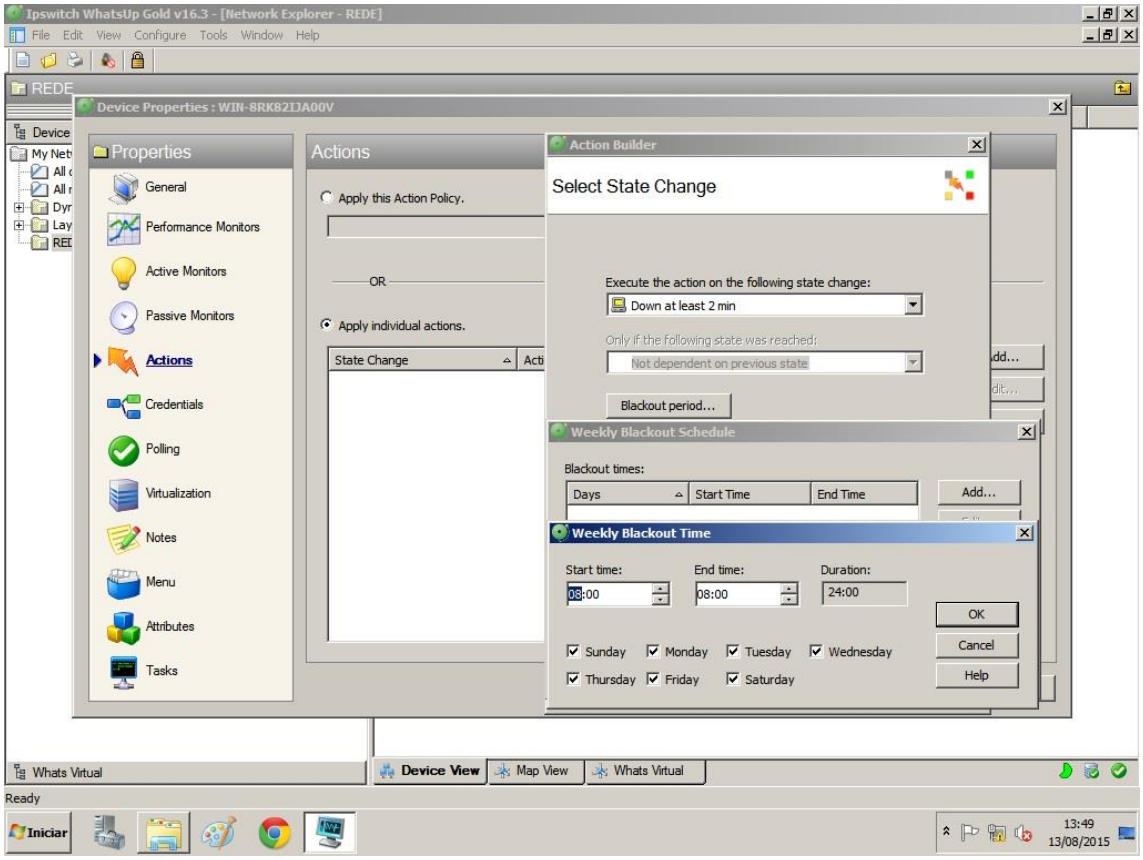

Figura 30 – Definição de Intervalo de Monitoramento.
Fonte: Autoria Própria

Na figura 31, é definido qual a mensagem que será informada em caso de falha do dispositivo.

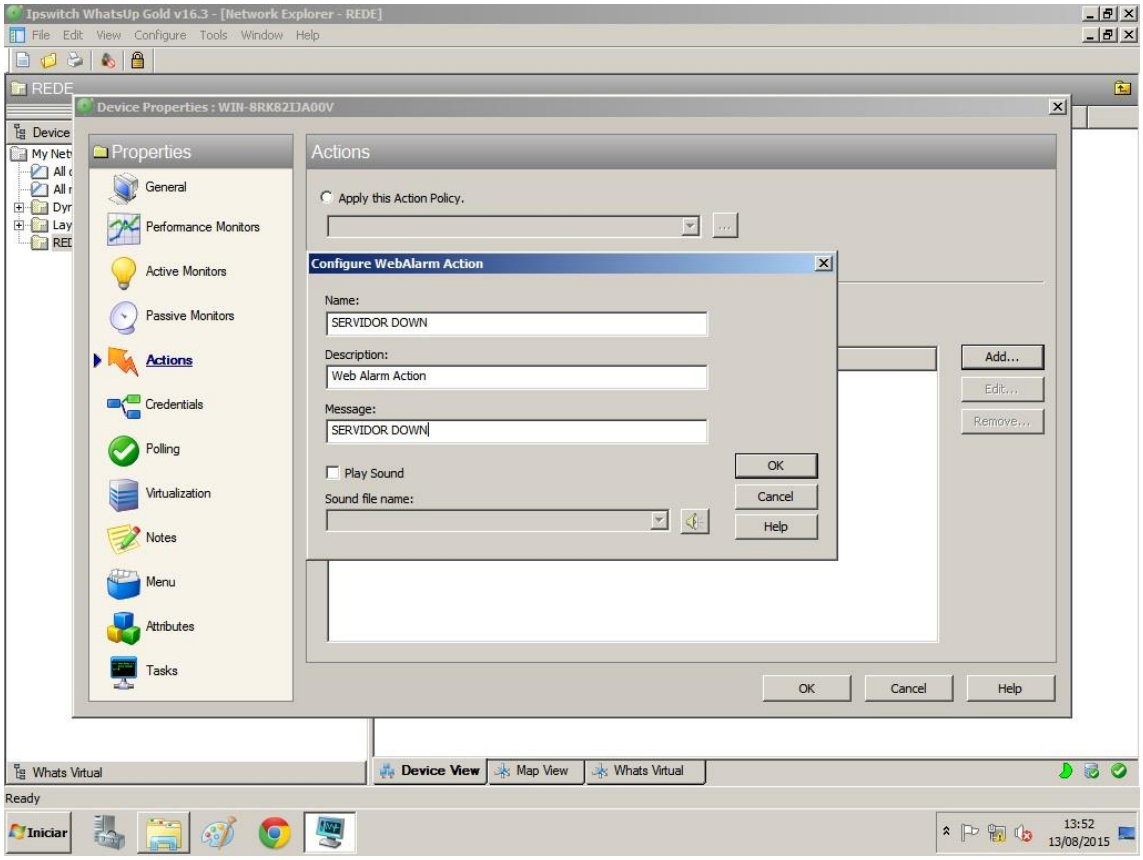

Figura 31 – Identificação de Alarme.
Fonte: Autoria Própria

Na figura 32, foi necessário adicionar uma credencial do *Windows* para a ferramenta de forma a ser realizado o monitoramento sem limitações de permissão de acesso.

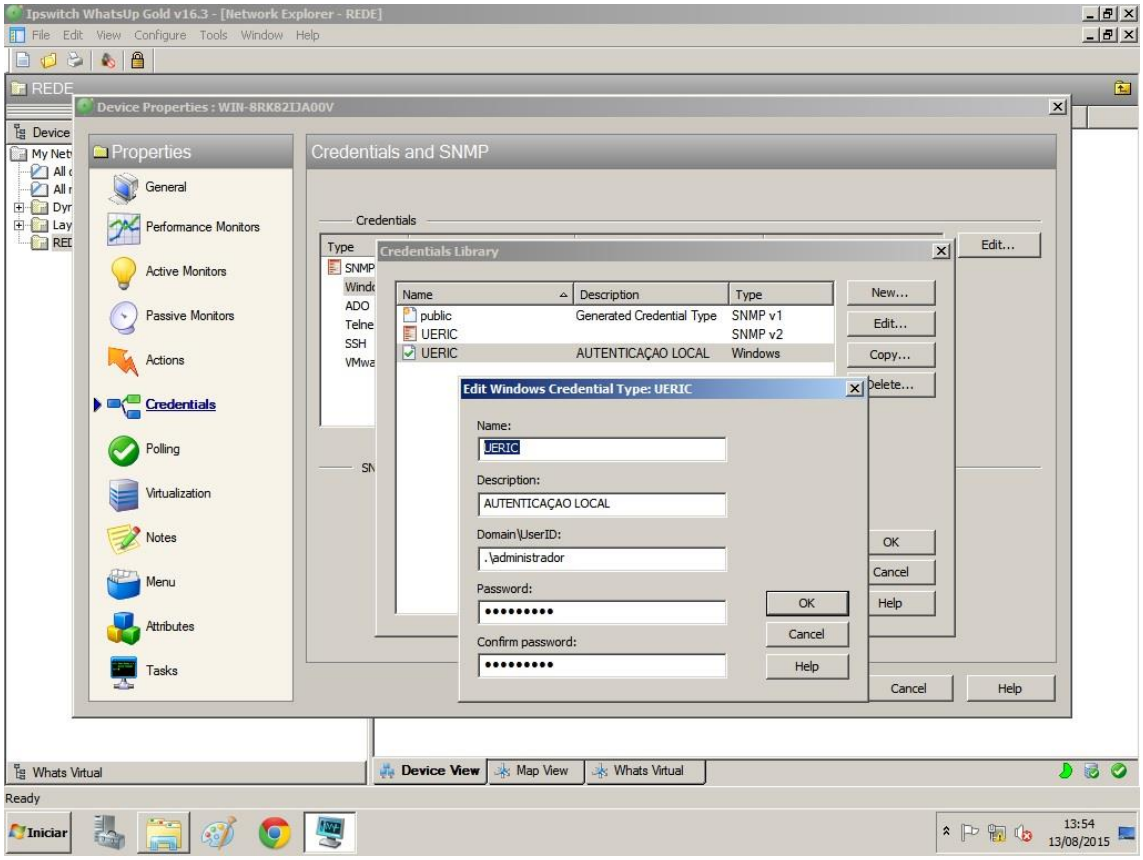

Figura 32 – Adição de Credencial do Windows Server.
Fonte: Autoria Própria

Esta referida configuração, foi realizada de forma similar em todos os dispositivos com IP, conforme figura 12.

Na figura 33, todos os dispositivos com IP foram adicionados. Porém as antenas PoE que não possuem IP ainda não foram identificadas.

Outra observação importante, é que estes dispositivos estão interdependentes um do outro, através de flechas indicativas. Esta configuração é necessária, pois caso o *switch* de gerenciamento deixe de responder, deverão aparecer vários alarmes de cada dispositivo, sendo que estes podem estar com o funcionamento normal. Este processo é explicado na figura 34 e 35.

É possível verificar linhas saindo do *switch* de distribuição e do *switch* PoE. Estas linhas são as interfaces ativas cadastradas no monitoramento.

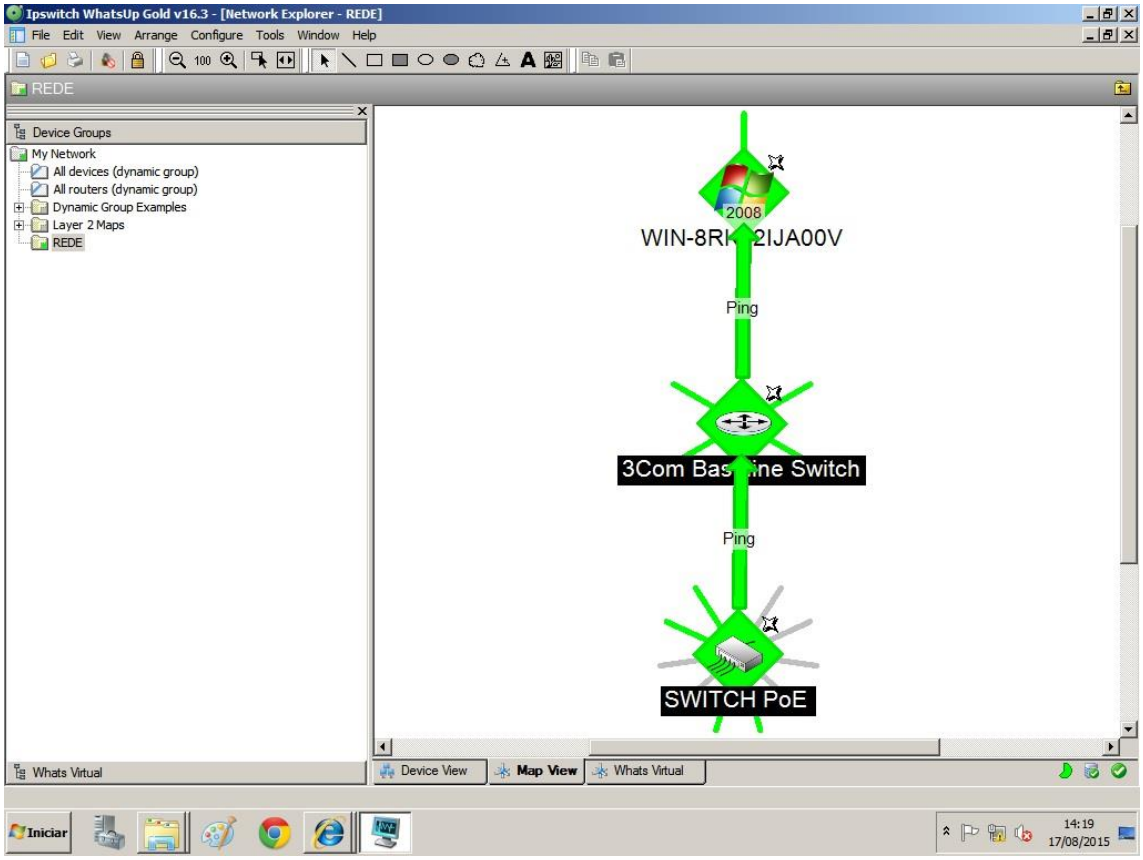

Figura 33 – Mapa dos Dispositivos.
Fonte: Autoria Própria

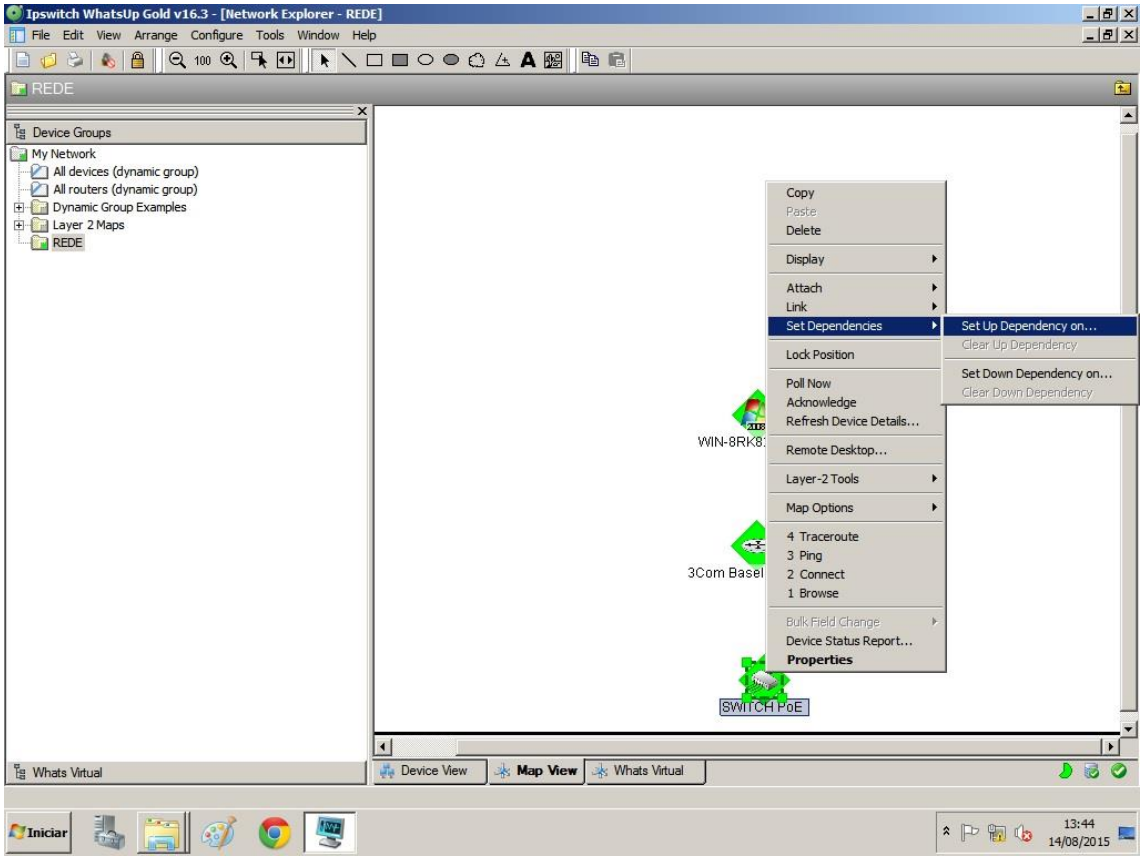

Figura 34 – Configuração de dependências entre dispositivos.
Fonte: Autoria Própria

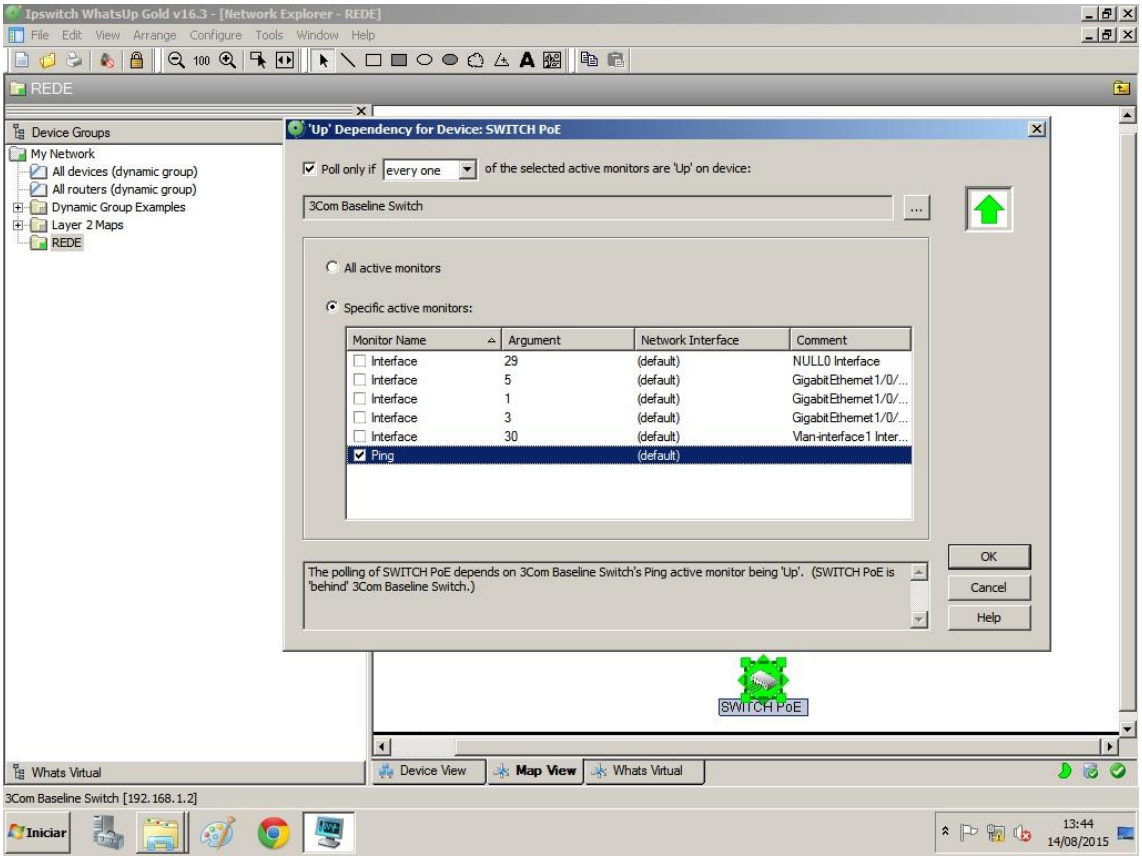

Figura 35 – Definição o IP do dispositivo dependente.
Fonte: Autoria Própria

3.7 Testes e Resultados

Como as antenas PoE, não possuem IP não é possível monitorar estes equipamentos diretamente. Mas isso pode ser contornado, monitorando as interfaces de rede onde estes equipamentos estão conectados. A ferramenta *What's Up Gold* é capaz de monitorar se está ocorrendo ou não atividade de rede em determinada interface conforme figura 33 e 36. Uma destas interfaces com tráfego é uma conexão da antena PoE com uma fonte individual, conforme figura 12, uma outra conexão é a do *switch* com o *host* de gerenciamento a terceira conexão é com o Switch PoE.

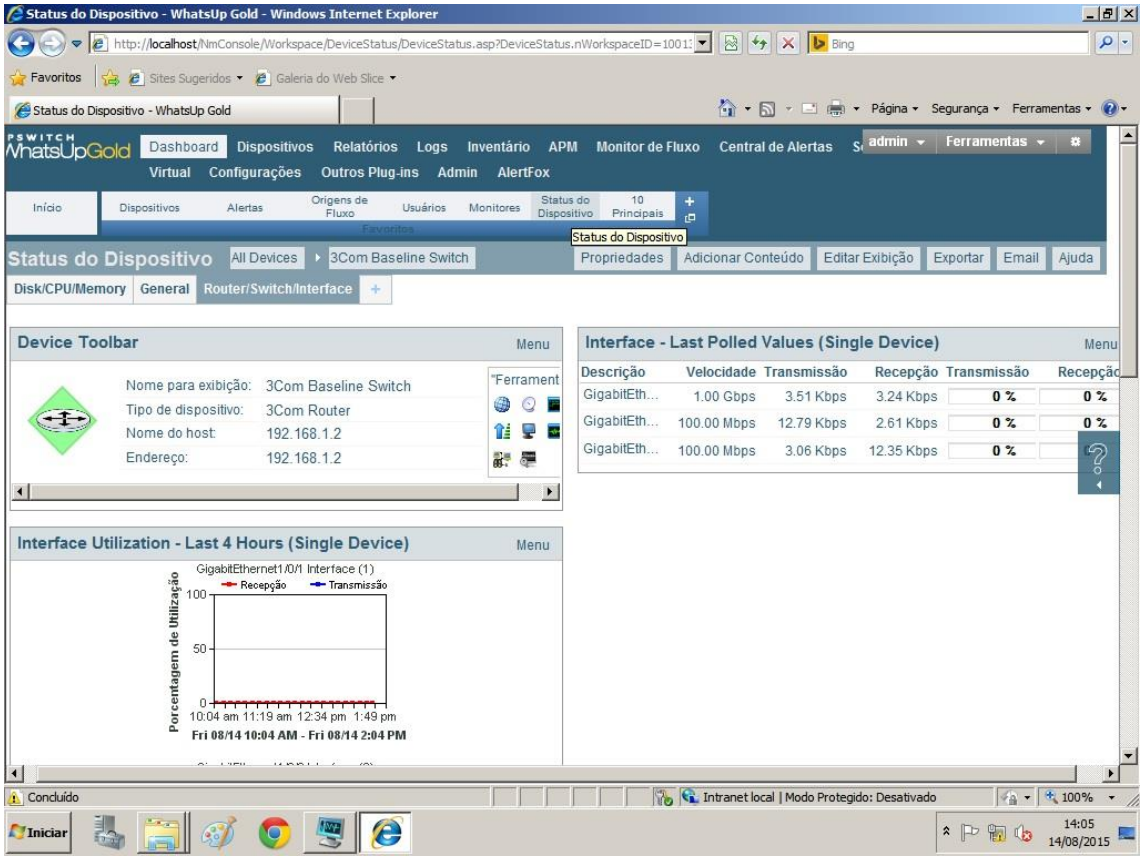

Figura 36 – Visão Geral de Tráfego de Rede do Dispositivo
Fonte: Autoria Própria

3.7.1 Teste de Desligamento de Antena

Neste teste foi avaliado qual o comportamento do *What's Up Gold*, caso uma antena seja desligada da rede com conexão proveniente de uma interface monitorada. A antena escolhida foi aquela com conexão indireta no *switch* através da fonte PoE, conforme topologia da figura 12. O objetivo será investigar se a fonte PoE interferirá no monitoramento deste dispositivo.

Foi realizado a desconexão da ponta da fonte PoE com a antena. O resultado é demonstrado na figura 37 e 38.

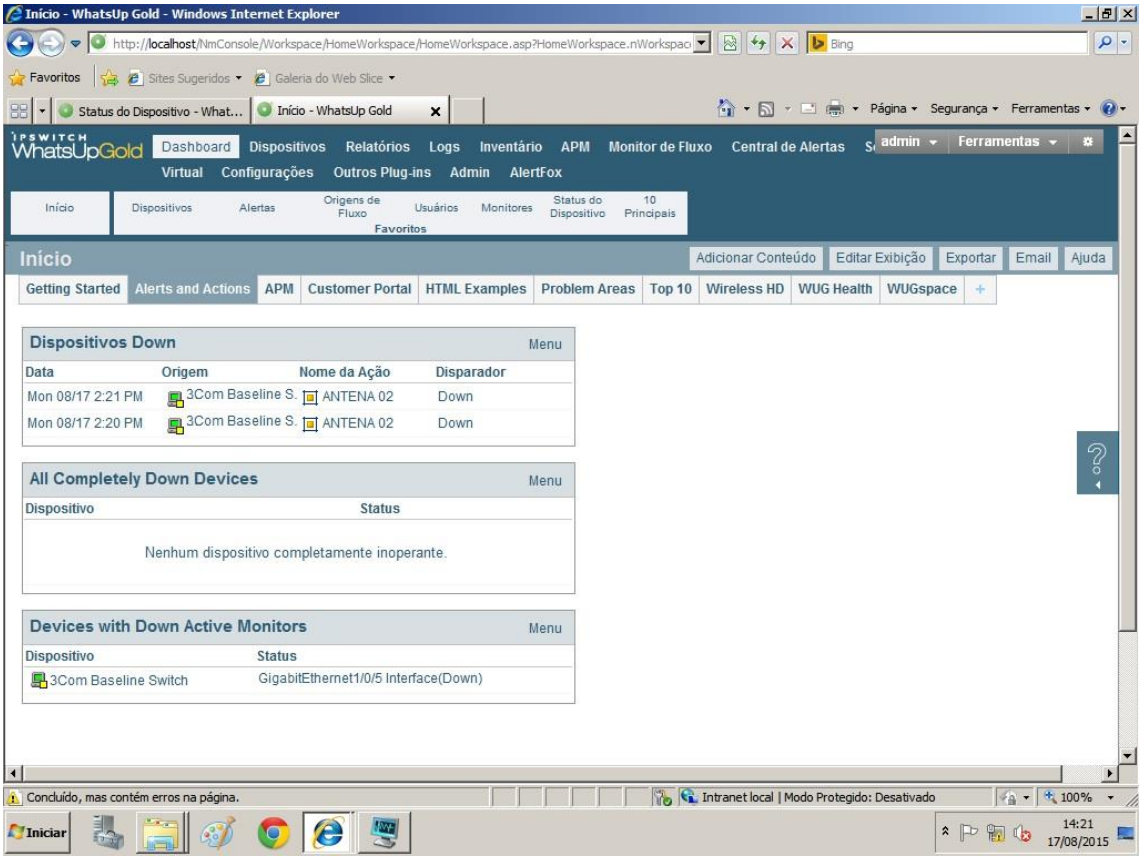

Figura 37 – Alerta de Antena sem Comunicação.
Fonte: Autoria Própria

Na figura 38, uma das interfaces aparece com sinal de alerta, destacada na cor amarela.

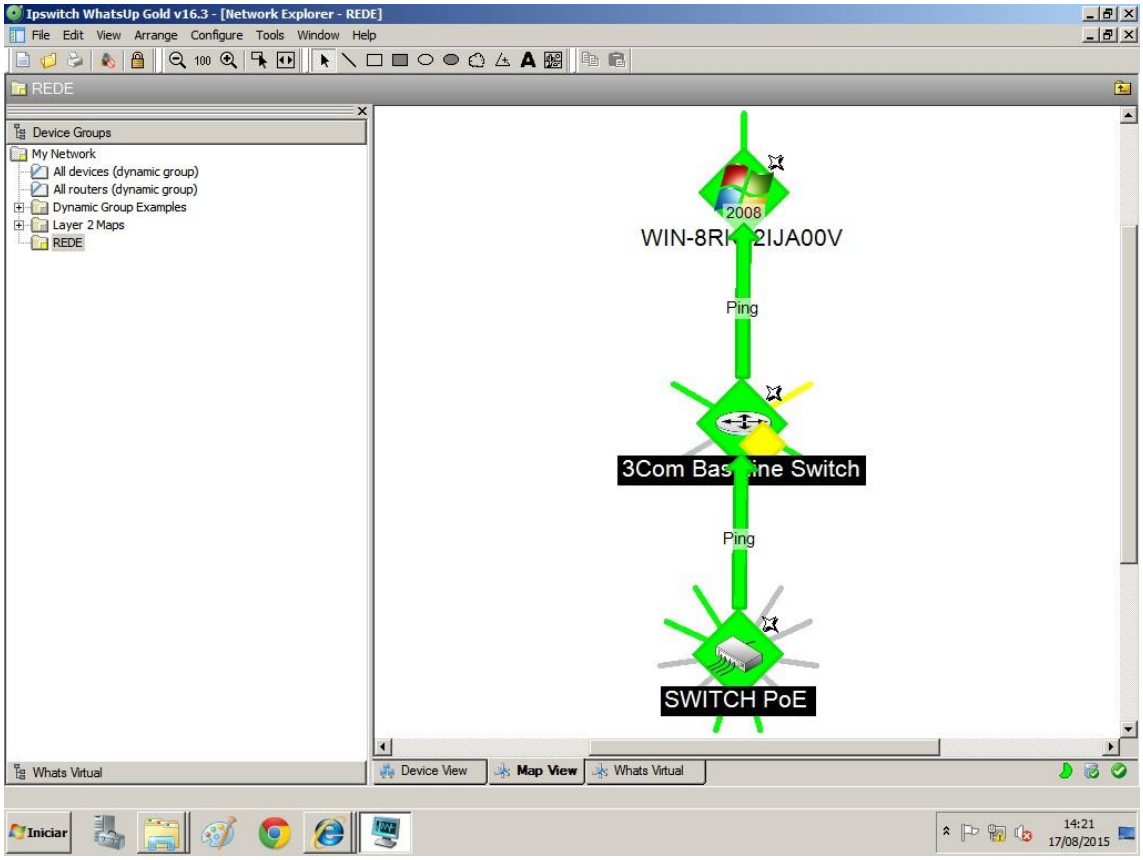

Figura 38 – Mapa da Rede indicando Alerta de Antena sem Comunicação.
Fonte: Autoria Própria

Apesar do monitoramento destes modelos de antenas sem IP ser possível, existe um problema na visualização do mapa. Não é possível saber de qual antena está conectada cada interface.

Este problema pode ser resolvido dependo do modelo de switch com uma função onde podemos definir cada IP em cada interface de rede com alguma antena. Assim podemos tratar cada interface como um dispositivo na rede com um IP, tornando o recurso do mapa, mais intuitivo quanto a resolução de problemas. Mas esta situação não será abordada neste estudo de caso.

Outro recurso que a ferramenta de monitoramento dispõe, é a alteração do plano de fundo do mapa apresentando na figura 36. Onde é possível redimensionar os dispositivos de forma a ser mais eficaz a solução do problema, já que está função permite atrelar o dispositivo à sua correspondente localização.

4 CONSIDERAÇÕES FINAIS

O grande desafio deste estudo era monitorar dispositivos PoE que estão conectados à rede, mas que não possuem IP, além da construção de um mapa para gerenciamento destes dispositivos.

A ferramenta de monitoramento What's Up Gold mostrou-se bem-sucedida nesta tarefa, mesmo não sendo capaz de monitorar as antenas diretamente, foi possível monitorar o tráfego de rede nas portas do *switch*. Neste caso a ferramenta de monitoramento identificou com exatidão quando as antenas estavam trafegando dados ou não.

Também foi possível a construção de um mapa flexível com interdependências entre os dispositivos, tornando mais eficaz o processo de identificação de problemas. Caso o switch possua a função de definição de IP para cada de suas portas é possível localizar com exatidão a localização da antena de acordo com a planta da edificação.

REFERÊNCIAS

Atera Informática. Switch 3Com Baseline 2928-SFP plus 24 portas e 4 SFP. Disponível em < http://atera.com.br/produto/3CRBSG2893/Switch+3Com+Baseline+2928-SFP+plus+24+portas+e+4+SFP> Acesso em 26/07/15, 17:07

Cisco Systems, Inc. Cisco Universal Power Over Ethernet - Unleash the Power of your Network White Paper. <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/white_paper_c11-670993.html> Acesso em 21/06/15, 14:07

De Oliveira, Carlos. Redes wireless: o que é Power over Ethernet? Disponível em <http://nfs.net.br/redes-wireless-o-que-e-power-over-ethernet-2/> Acesso em 07/06/15, 17:09

Dell Inc. Informações sobre configuração e recursos. Disponível em <http://downloads.dell.com/Manuals/all-products/esuprt_desktop/esuprt_optiplex_desktop/optiplex-380_setup%20guide_pt-br.pdf> Acesso em 06/07/15, 01:17

IPSwitch. Release Notes for Ipswitch WhatsUp Gold v16.2. Disponível em <http://docs.ipswitch.com/NM/69_WhatsUpGoldv16.2/01_ReleaseNotes/index.htm> Acesso em 28/06/15, 16:37

MAURO, D. R.; SCHIMIDT, K. J. SNMP Essencial. Rio de Janeiro: Campus, 2001.

Microsoft Corporation. Guia de Segurança SNMP. Disponível em < https://technet.microsoft.com/pt-br/library/Cc754924.aspx> Acesso em 12/08/15, 21:47

Morimoto, Carlos E. Power Over Ethernet. Disponível em < http://www.hardware.com.br/dicas/power-over-ethernet.html> Acesso em 07/06/15, 16:45

Motorola, Inc. 802.3af Single-Port Power Injector. Disponível em <http://www.motorolasolutions.com/content/dam/msi/docs/business/products/accessories/wireless_broadband_accessories/wlan_accessories/power_over_ethernet/802.3af_single_port_power_injector/_documents/_staticfiles/ds_sppi_0906_new.pdf> Acesso em 06/07/15, 00:56

Motorola, Inc. AP300 Wireless Access Port from Motorola. Disponível em <http://www.symbol.com/product.php?productid=256> Acesso em 05/07/15, 23:55

Motorola, Inc. WS2000 Wireless Switch from Motorola. Disponível em <http://www.symbol.com/product.php?productID=255&tab=Data Sheet> Acesso em 06/07/15, 00:15

Plameni, Mikrotik Forum. Switch 3Com 2928 SFP PLUS. Disponível em <http://www.mikrotik-bg.net/topic/7898-%D1%81%D1%83%D0%B8%D1%87-3com-2928-sfp-plus-3crbsg2893-hp-v1910-24g/> Acesso em 09/07/15, 16:46

Sheldon, Mike. Inline Power, POE or POE+ -- which do you need? Disponível em <http://www.networkworld.com/article/2230808/cisco-subnet/inline-power--poe-or-poe------which-do-you-need-.html> Acesso em 21/06/15, 13:56.

Teleco.SNMP I: Estudo do Protocolo. Disponível em < http://www.teleco.com.br/tutoriais/tutorialsnmpred1/pagina_4.asp> Acesso em 09/07/15, 21:23

Zebra Technologies Corporation. MC9190-G Mobile Computer. Disponível em <https://www.zebra.com/us/en/products/mobile-computers/handheld/mc9190-g.html> Acesso em 05/07/15, 22:44