CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

GERÊNCIA, MONITORAMENTO E PROVISIONAMENTO DE CPE TR-069

IVAN DAUN SAKAI

Marília, 2012

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

GERÊNCIA, MONITORAMENTO E PROVISIONAMENTO DE CPE TR-069

Monografia apresentada ao Centro Universitário Eurípides de Marília como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciência da Computação.
Orientador: Ms. Cairo Gomide Jr

Marília, 2012

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Ivan Daun Sakai

AUTOMATIZAÇÃO DE GERÊNCIA, MONITORAMENTO E PROVISIONAMENO DE CPEs TR-069

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Ciência da Computação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Ciência da Computação.

Nota: 8,0 (oito)

Orientador: Cairo Gomide Júnior

1°. Examinador: Paulo Rogerio de Mello Cardoso

2°. Examinador: Ricardo José Sabatine

Marília, 30 de novembro de 2012.

SAKAI, Ivan Daun. **Gerência, Monitoramento e Provisionamento de CPE – TR-069.** 2012. f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2012.

RESUMO

Um protocolo é um padrão que controla e possibilita uma conexão, comunicação e transferência de dados entre dois sistemas computacionais. Pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação. Os protocolos podem ser implementados por hardware, software ou por uma combinação dos dois. A expansão desses protocolos contribui para o poder e sucesso da internet. O projeto consiste no estudo e teste físico do protocolo CWMP (CPE WAN Management Protocol ou Protocolo de Gerenciamento de CPE WAN), assim como apresentar as vantagens do seu uso. Formulado a partir da especificação técnica TR-069 (Technical Report 069), tem a finalidade de gerenciar redes, controlar CPE, gerenciar QoS (políticas, monitoramento e performance de QoS), autoconfigurar e provisionar dinamicamente serviços, padronizar fabricantes, gerenciar softwares/firmwares, monitorar status e performance, notificar dinamicamente e gerar arquivos de logs e diagnósticos.

Palavras-chave: Protocolo. CWMP. TR-069. BroadBand Forum. CPE. ACS

SAKAI, Ivan Daun. **Gerência, Monitoramento e Provisionamento de CPE – TR-069.** 2012. f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2012.

ABSTRACT

A protocol is a standard that controls and enables a connection, communication and data transfer between two computer systems. It can be defined as "the rules that govern" the syntax, semantics, and synchronization of the communication. The protocols can be implemented by hardware, software or a combination of both. The expansion of such protocols contributes to the strength and success of the internet. The project consists in the study and physics tests of the protocol CWMP (CPE WAN Management Protocol or Protocol CPE WAN Management), as well as present the advantages of its use. Formulated from the technical specification TR-069 (Technical Report 069), has the purpose of managing networks, controlling CPE, managing QoS (policies (policies, monitoring performance of QoS), dynamically self-setting and providing services, standardizing manufacturers, managing software/firmware, monitoring status and performance, dynamically reporting and generating log files and diagnoses.

Keywords: Protocol. CWMP. TR-069. BroadBand Forum. CPE. ACS

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACS – Auto-Configuration Server, servidor de auto configuração de CPE.

API – Application Programming Interface, é de um conjunto de rotinas e padrões estabelecidos por um software.

CLI – Command-line Interface, mecanismo que permite um dispositivo físico interagir com um software para realizar determinadas tarefas.

CPE – Customer-Premises Equipment ou Customer-Provided Equipment, equipamento localizado nas instalações do cliente e conectado a um canal de uma operadora de telecomunicações.

CWMP – CPE WAN Management Protocol, também bem conhecido por TR-069, trata-se de um protocolo da camada de aplicação que permite gestão remota de CPE.

HTTP – HyperText Transfer Protocol, protocolo da camada de aplicação utilizado para transferir dados por intranets e pela World Wide Web.

HTTPS – HyperText Transfer Protocol Secure, implementação do protocolo HTTP sobre uma camada SSL ou TLS.

IETF – Internet Engineering Task Force, grupo internacional cuja função é estruturar corretamente a evolução da arquitetura da internet e garantir o seu correto funcionamento.

IP – Internet Protocol, protocolo no qual envolve toda a infraestrutura da Internet.

IPTV – IPTV ou TVIP, é um método de transmissão de sinais televisivos através do protocolo IP.

ISP – Internet Service Provider, são os fornecedores de acesso a internet.

JDK – Java Development Kit, é um conjunto de utilitários que permitem criar sistemas de software para a plataforma java. É composto por compilador e bibliotecas.

LAN – Local Area Network, rede de computadores de pequena dimensão, como por exemplo, uma área residencial, escritório ou mesmo de um pequeno grupo de edifícios.

MIB – Management Information Base, tipo de base de dados usada para gerir dispositivos em redes de comunicações.

NAT – Network Address Translation, é uma técnica que consiste em alterar o endereço IP de origem de um pacote que passa por um roteador ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública).

NETCONF – Network Configuration, é um protocolo de gestão de redes desenvolvido pelo IETF.

OSI – Open Systems Interconnection, arquitetura que define uma forma comum de conectar computadores.

QoS – Quality of Service, refere-se a capacidade de fornecer um serviço conforme as exigências.

RPC – Remote Procedure Call, trata-se de um processo de comunicação que permite que um programa local invoque remotamente a execução de outro programa.

SNMP – Simple Network Management Protocol, é um protocolo da camada de aplicação utilizado para gestão de redes TCP/IP.

SOAP – Simple Object Access Protocol, é um protocolo utilizado para troca de informações utilizando tecnologias baseadas em XML.

SSL – Secure Sockets Layer, protocolo utilizado para transmitir documentos de forma segura através da internet.

SSH – Secure Shell, trata-se de um protocolo de rede que permite a conexão com outro computador na rede de forma a executar comandos remotamente.

TCP – Transmission Control Protocol, é um dos protocolos sob os quais assenta o núcleo da Internet. Ele verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros, pela rede.

TCP/IP – Corresponde a um conjunto de protocolos utilizados para comunicação entre computadores em rede.

TLS – Transport Layer Security, tal como o seu predecessor trata-se de um protocolo criptografado que promove uma comunicação segura através da Internet.

TR-064 – Technical Report 64, desenvolvido pelo atual BroadBand Forum, corresponde a norma que especifica como deverá ser feita a comunicação entre o Residential Gateway e os hosts da LAN.

TR-069 – Technical Report 69, desenvolvido pelo atual BroadBand Forum, corresponde a norma de especificação do protocolo CWMP.

UPnP – Universal Plug and Play, é um conjunto de protocolos de redes de computadores que permite conexões directas e simplificadas para implementação de redes em casas e escritórios.

VoIP – Voice over Internet Protocol, tecnologia que permite transmissão de comunicações de voz sobre redes IP.

WAN – Wide Area Network, rede de computadores que cobre uma grande área.

xDSL – Família de tecnologias que fornecem um meio de transmissão digital de dados (ex: ADSL, HDSL, VDSL, SDSL, UDSL), aproveitando a própria rede de telefonia que chega na maioria das residências.

XML – Extensible Markup Language, é uma linguagem utilizada para facilitar o transporte e armazenamento de informação.

URL - Uniform Resource Locator, é o endereço de um recurso (um arquivo, uma impressora, etc.), disponível em uma rede.

URI - Uniform Resource Identifier, é uma cadeia de caracteres compacta usada para identificar ou denominar um recurso na Internet.

UDDI - Universal Description, Discovery and Integration, é um serviço de diretório onde empresas podem registrar e buscar por serviços Web Services.

WSDL - Web Services Description Language, é um documento escrito em XML que além de descrever o Web Service, especifica como acessá-lo e quais as operações ou métodos disponíveis.

Capítulo 1

1.1. Introdução

Quando as redes de computadores surgiram, as soluções eram de forma proprietária, ou seja, uma determinada tecnologia só era suportada por seu fabricante. Não havia possibilidade de se mesclar soluções de fabricantes diferentes. Dessa forma, um mesmo fabricante era responsável por toda construção de uma rede.

O OSI (Open Systems Interconnection) é um modelo de referência criado pela ISO (International Standards Organization) para entender como os protocolos de rede funcionam. Foi desenvolvido para que os fabricantes pudessem criar protocolos a partir deste modelo.

Protocolo é uma "linguagem" usada para transmitir dados pela rede. Para que dois computadores possam se comunicar, eles devem usar o mesmo protocolo (ou seja, a mesma linguagem).

Devido a grande demanda dos serviços de banda larga, o número de acesso a Internet cresce assim como equipamentos modens, roteadores, VoIP, IPTV e outros. Paralelamente, a configuração destes equipamentos torna-se uma difícil tarefa para usuários finais e administradores de rede. No entanto, foi desenvolvido o padrão TR-069, que oferece a possibilidade de configuração automática desses tipos de acesso.

Os ISP têm considerado que a gestão e segurança da rede do cliente estão fora da sua esfera de influência, devendo ser administrada autonomamente pelo cliente. Normalmente, os operadores consideram que a sua esfera de influência acaba no seu equipamento de fronteira, sendo responsabilidade do cliente a gestão dos seus próprios equipamentos de home gateway e de tudo o que esteja para lá desses equipamentos. (Silva, 2009)

Porém nem sempre é assim que funciona. Para manter a fidelidade do seu cliente, os ISP se sentem na obrigação de assumirem problemas técnicos de seus equipamentos.

A entrada dos operadores nas redes domésticas tem influenciado que entidades tais como BroadBand Forum e Home Gateway Initiative apostem na normalização das tecnologias que permitem administrar e monitorizar remotamente não só os equipamentos

gateways mas também outros equipamentos CPE (Customer Premise Equipment) localizados na rede do cliente. (Silva, 2009)

O TR-069 é uma especificação técnica padrão, intitulada como CWMP (CPE WAN Management Protocol), ela define uma camada de aplicação para gerenciamento de dispositivos de usuários finais.

Ele inclui uma configuração automática segura e o controle de outras funções de gerenciamento CPE dentro de um framework integrado.

Um ACS usando as especificações TR-069, proporciona a conectividade necessária entre CPE e servidor, automatizando sua gestão.

Neste contexto, o estudo e desenvolvimento do TR-069 são de grande importância para a formação e o conhecimento acadêmico, bem como sua contribuição tecnológica.

Baseado em SOAP/HTTP, protocolos bidirecionais, o CWMP fornece a comunicação entre Equipamentos de Premissas de Cliente (CPE) e Servidores de Configuração Automática (ACS).

O CPE WAN Management Protocol é destinado para suportar uma variedade de funcionalidades para gerenciar uma coleção de CPE, incluindo os seguintes recursos principais: Auto-configuração e provisionamento de serviços dinâmicos; Gerenciamento de imagens software/firmware; Monitoramento de status e desempenho; Diagnósticos. (Broadband Forum, 2011)

O CPE WAN Management Protocol faz uso de vários protocolos padrões. A pilha de protocolos, definida pelo CPE WAN Management Protocol, é mostrada na Figura 1. Observe que o CPE e o ACS devem aderir às exigências dos protocolos, a menos que o CPE não utilize o padrão TR-069. (Broadband Forum, 2011)

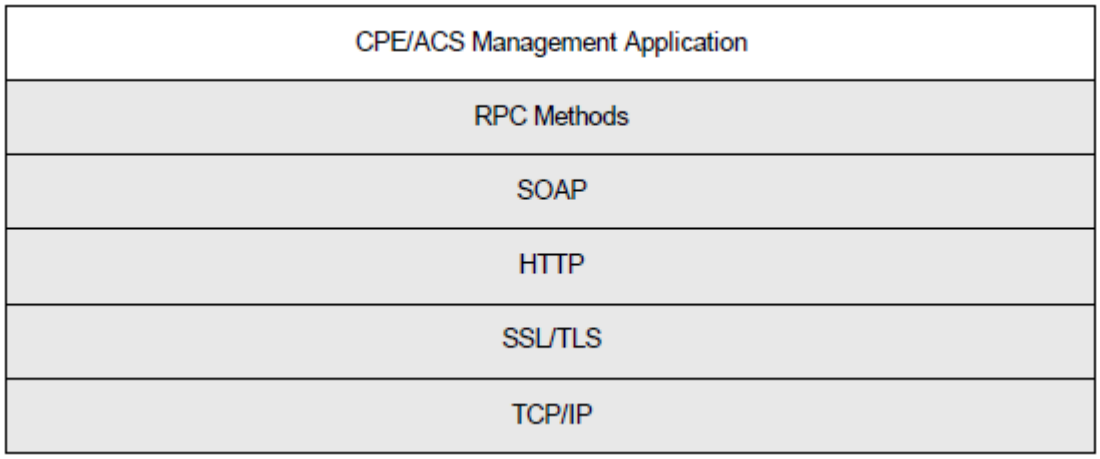

Figura 1 - Pilha de Protocolos

A comunicação estabelecida pelo protocolo TR-069 corresponde a uma troca bidirecional de pedidos e respostas RPC. Esta transação é concluída quando ambos os terminais não tem mais mensagens para enviar. O CPE é responsável por estabelecer e terminar as sessões TR-069.

De modo a possibilitar uma troca sequencial de operações numa única sessão, o CPE deverá manter a conexão TCP durante toda sessão.

Como objetivo geral, o projeto como todo propõe o estudo detalhado do protocolo CWMP bem como testes reais com uma ferramenta ACS, com o propósito de obter resultados sobre seu funcionamento e sua aplicação no gerenciamento de redes.

Segundo a especificação técnica TR-069, descrita pela BroadBand Forum: (BroadBand Forum, 2011)

O protocolo deve proporcionar flexibilidade no modelo de conectividade:

- Permitir que CPE e ACS inicie o estabelecimento da conexão, evitando a necessidade de uma conexão persistente entre cada CPE e um ACS.
- Permitir uma ou mais ACS servir uma população de CPE, o qual pode ser associado com um ou vários prestadores de serviços.

O protocolo visa apoiar a descoberta e a associação dos ACS e CPE:

- Fornecer mecanismos para um CPE descobrir os ACS adequados para um determinado provedor de serviços.

- Fornecer mecanismos para permitir que um ACS identifique com segurança um CPE e associá-lo com um usuário/cliente.

O protocolo permite que um ACS controle e monitore vários parâmetros associados a um CPE.

- CPE diferentes podem ter diferentes níveis de capacidade, como também a implementação de diferentes subconjuntos de funcionalidades. Além disso, um ACS pode gerenciar uma variedade de dispositivos oferecendo uma gama variada de serviços. Como resultado, um ACS deve ser capaz de descobrir as capacidades de um CPE particular.
- Um ACS deve ser capaz de controlar e monitorar a configuração atual de um CPE.

1.2. Motivação para realização do trabalho

A cada dia o TR-069 vem sendo um padrão mais aceito pelas empresas que realizam gestão e configuração de CPE. Para os ISP, resolver um problema técnico de forma mais eficiente, traz benefícios para a empresa e para o cliente.

As principais motivações para a realização deste trabalho, será sua construção e utilização pela empresa Interfocus, que, atualmente, presta serviços de gerência para ISP, como também, o estudo deste padrão é de grande importância para a formação e o conhecimento acadêmico, bem como sua contribuição tecnológica.

1.3. Objetivos

Como objetivo geral, o projeto propõe o estudo e teste do protocolo CWMP, com o propósito de aplicação no gerenciamento de redes de diferentes arquiteturas bem como realizar controle de CPE como também implementar em ambientes físicos que serão definidos no decorrer do projeto, com o propósito de obter resultados relevantes para a área acadêmica. Por fim, publicar resultados no formato de artigos científicos.

O projeto completo será dividido em quatro principais fases que abordam (I) estudo bibliográfico, (II) levantamento e estudo detalhado da TR-069, (III) elaboração e concepção do ambiente para aplicação e (IV) apuração de resultados.

I. Estudo bibliográfico

Levantamento de livros e artigos científicos publicados na área, para a obtenção de informações confiáveis e relevantes para o estudo e desenvolvimento.

II. Levantamento e estudo detalhado da TR-069

Realizar o estudo detalhado da especificação TR-069, utilizando versão 1.3, mais atual, lançada em julho de 2011, pela Broadband Fórum, para a construção adequada desta arquitetura.

III. Elaboração e concepção do ambiente para aplicação

A arquitetura será baseada no estudo realizado no item II, que será definida no decorrer do projeto, incluindo a escolha de softwares e dispositivos para testes.

IV. Apuração de resultados

Após o sucesso da realização dos passos anteriores, será elaborada a apuração dos resultados no formato de textos, gráficos e tabelas, ressaltando a importância do TR-069.

1.4. Organização da monografia

A dissertação é composta por cinco capítulos, “Introdução”, “Protocolos de Gestão”, “Concepção”, “Testes” e “Conclusões e Trabalhos Futuros”.

Desenvolveu-se um capítulo introdutório, para que brevemente seja demonstrada a ideia principal do projeto.

No capítulo dois, Protocolos de Gestão, foram ressaltados os principais protocolos de gestão e a importância de gerenciar equipamentos nas redes atuais e futuras.

O capítulo três, Concepção, consiste no estudo e descrição detalhada da API_TR-069, demonstrando o funcionamento dos componentes principais do ACS.

O quarto capítulo, Testes, em parceria com a empresa iK1, representante nacional Daytrek, seguindo Anexo A, demonstra o funcionamento prático da TR-069 utilizando o software Vigor ACS SI da empresa Daytrek Corp. e o CPE modelo Daytrek Vigor 2110 series básico, mostrando resultados do uso deste padrão.

Por último, o capítulo cinco, Vantagens, Conclusões e Trabalhos Futuros, concluirá as vantagens do uso deste padrão, bem como demonstrar a continuação deste projeto.

Capítulo 2

2.1. Protocolos de Gestão

Apesar do alto crescimento tecnológico geral, duas áreas que vem se destacando são redes de telecomunicações e redes de computadores.

Os novos avanços tecnológicos das redes, fez com que essas duas áreas convergissem numa mesma dimensão, que é a disponibilização de múltiplos serviços numa mesma infraestrutura.

Esta convergência, que conecta redes individuais, forma redes com maiores dimensões. Estas redes são formadas pelo emprego de computadores e seus recursos, junto às técnicas de comunicação e transmissão de pacotes.

A Internet é a grande chave desta convergência.

A criação do modelo de referência OSI (Gouveia, 1997) (Wikipedia, 2012) corresponde a um dos maiores passos dados na gestão de redes. Este modelo promoveu a coordenação e estruturação das comunicações de dados, permitindo redução da complexidade de desenvolvimento de normas; maior flexibilidade e simplicidade de implementação de alterações e funcionalidades nas camadas; incorporação de novas tecnologias e compatibilidade entre fabricantes. (W3schools, 2012)

Atualmente, as tecnologias de gestão de equipamentos mais utilizadas são o protocolo padronizado SNMP e as interfaces CLI integradas nos equipamentos. Porém, o SNMP nunca foi uma solução fiel e segura para configurações e as linhas de comando (CLI), demonstraram pouca flexibilidade. (Silva, 2009)

Se analisarmos todos esses fatores, nas redes modernas atuais, mostra-se que essas ferramentas não atendem de forma eficiente. Com isso surge a necessidade de criar soluções de gestão automáticas a partir de protocolos padronizados e extensíveis. (Silva, 2009)

Dentre as razões que tornaram o TR-069 uma tecnologia padrão para a gestão de equipamentos de clientes finais dos ISP, a criação do protocolo CWMP (TR-069), possibilita:

- Que ISP sejam capazes de gerenciar remotamente equipamentos CPE de diferentes fabricantes através de uma mesma infraestrutura; (Silva, 2009)

- Permite a aplicação deste protocolo dentro de rede WAN e LAN, por incorporar tecnologias como UPnP, tornando-se assim extensível; (Silva, 2009)
- Considera-se flexível por basear-se em protocolos normalizados e de utilização aberta (SOAP, XML, HTTP/HTTPS, TCP), permitindo que seus próprios utilizadores (ISP) desenvolvam ferramentas próprias; (Silva, 2009)
- Disponibiliza mecanismos que facilita a instalação de novos serviços e software nos equipamentos e garanta uma comunicação segura e fiel entre cliente e servidor. (Silva, 2009)

Relevando as limitações de configuração do SNMP, o IETF criou o protocolo Network Configuration (NetConf), tratando-se também de configuração e gestão remota baseado em tecnologias abertas e padronizadas. O TR-069 em comparação com o NetConf, tem como diferença, ser encapsulado e transportado através de diferentes tecnologias (SOAP, BEEP, SSH) e é igualmente seguro. (Silva, 2009)

Este capítulo mostrará as soluções SNMP, CLI, UPnP, NetConf, porém será focado no TR-069, a fim de compreender as diferenças entre eles.

2.2. Simple Network Management Protocol (SNMP)

O protocolo SNMP, pertencente a camada de aplicação do modelo OSI, foi desenvolvido no início da década de 80, pelo Internet Engineering Task Force (IETF), com o objetivo de gerenciar equipamentos numa rede de computadores. (Silva, 2009)

Com o SNMP, tanto pode ser obtido informações de equipamentos SNMP pertencentes a uma rede baseada nos protocolos TCP/IP, quanto alterar suas configurações.

Os equipamentos são chamados de agentes SNMP, e a entidade que os gerencia, é chamada de gestor SNMP.

Os agentes possuem informações de gestão que são conhecidas através do repositório Management Information Base (MIB).

Seu funcionamento baseia-se numa troca de informações entre o gestor e a MIB do agente. A gestão é realizada através do protocolo de transporte UDP (User Datagram Protocol), onde o gerente envia pedidos a um ou mais agentes. (Silva, 2009)

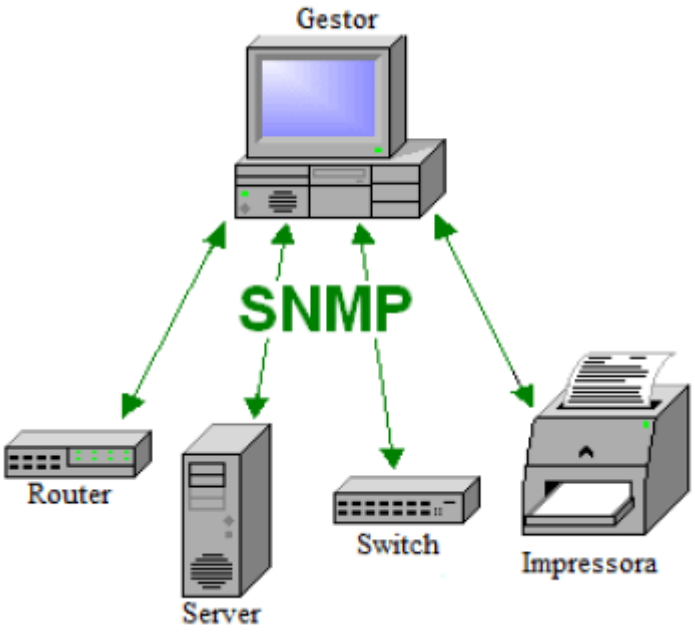

Figura 2 - Ambiente de gestão SNMP (Wikimedia, 2006)

O SNMP trabalha através de duas operações básicas (SET e GET), e duas derivações (GET-NEXT e TRAP). (Silva, 2009)

O SET é utilizado pelo gestor para alterar valores de variáveis dos agentes.

O GET é utilizado pelo gestor para ler valores de determinadas variáveis dos agentes.

A operação GET-NEXT é utilizada para obter valor da próxima variável, ou seja, o gestor fornece o nome de uma variável, e ao executar o GET-NEXT é apresentado o nome e valor da próxima variável. Também é utilizada para obter variáveis e valores de uma tabela desconhecida. (Silva, 2009)

O TRAP, a partir de determinado evento ocorrido, é utilizado para informar o gestor.

O SNMP, apesar de demonstrar um excelente protocolo de monitorização, o mesmo não traz confiabilidade e segurança nas ações de configuração, devido ao fato de utilizar datagramas UDP para transporte de suas informações. Por esta deficiência, o IETF vem desenvolvendo novas versões do protocolo (SNMPv2 e SNMPv3). (Silva, 2009)

Uma especificação completa e detalhada desde protocolo pode ser entrada no RFC 1157. (Case J., 1990)

2.3. Command Line Interface (CLI)

Uma interface de linha de comando é um mecanismo que permite o envio de comandos para realizar tarefas em determinado computador ou sistema, possibilitando assim uma interação com o mesmo. (Wikipedia, 2012)

A Interface de linha de comando (CLI) é um utilitário de configuração baseado em texto que suporta um conjunto de comandos de teclado e parâmetros para configurar e gerenciar um AP. (DELL, 2012)

Os usuários digitam Instruções de comando, compostas de Comandos CLI e seus parâmetros associados. As instruções podem ser emitidas de um teclado para controle em tempo real ou de scripts que automatizam a configuração. (DELL, 2012)

Por exemplo, ao fazer download de um arquivo, os administradores digitam o Comando CLI **download** juntamente com os parâmetros de Endereço IP, nome do arquivo e tipo do arquivo. (DELL, 2012)

Você acessa a CLI por meio de uma conexão serial de HyperTerminal ou via Telnet. Durante a configuração inicial, você pode usar a CLI por meio de uma conexão de porta serial para configurar o endereço IP de um Ponto de acesso. Ao acessar a CLI via Telnet, você pode comunicar-se com o Ponto de acesso por meio da LAN (switch, hub, etc.), pela Internet, ou com um cabo de Ethernet "invertido" conectado diretamente à porta Ethernet de seu computador. (DELL, 2012)

Os fabricantes de equipamentos de rede incluem em seus dispositivos, mecanismos para configurá-los através de CLI, facilitando aos administradores, técnicas simples de configuração. O seu uso representa elevados custos operacionais, associado ao desenvolvimento dos seus scripts e da sua manutenção. Ainda vale salientar, que o seu uso, exige um alto nível de conhecimento do equipamento por parte dos administradores.


```
************************************************************
*       Net Optics Command Line Interface (CLI)            *
*                  for xBalancer                           *
*                                                          *
*       Copyright (c) 2010 by Net Optics, Inc.             *
*                                                          *
*            Restricted Rights Legend                      *
*                                                          *
* Use,  duplication,  or disclosure by the Government is   *
* subject  to  restrictions as set forth in subparagraph   *
* (c)  of  the Commercial Computer Software - Restricted   *
* Rights  clause at FAR  sec. 52.227-19 and subparagraph   *
* (c)(1)(ii) of the Rights in Technical Data and Computer  *
* Software clause at DFARS sec. 252.227-7013.              *
*                                                          *
*       Net Optics, Inc.                                   *
*       5303 Betsy Ross Drive                              *
*       Santa Clara, California 95054                      *
*       (408) 737-7777                                     *
*       e-mail: cs-support@netoptics.com                   *
*                                                          *
************************************************************
user login: admin
password:
Net Optics>
```

Figura 3 - Net Optics Interface Linha de Comando (CLI, 2012)

2.4. Universal Plug And Play (UPnP)

A tecnologia Universal Plug and Play (UPnP) estende do Plug and Play; é constituída por protocolos abertos (TCP/IP) direcionados para a comunicação na Internet e por tecnologias Web; é promulgada pelo UPnP Fórum; define uma arquitetura capaz de estabelecer conexão ponto a ponto em redes de dispositivos inteligentes e é projetada para proporcionar fácil utilização e flexibilidade, dado basear-se em padrões de conectividade ad-hoc. (UPnP Forum, 2012)

Essas redes são pequenas, podem ser caracterizados como redes presentes em nossas casas, escritórios ou em pequenos espaços públicos, onde poderá existir ou não conexão à internet. Esta tecnologia vem para facilitar a implementação e instalação destas redes, o compartilhamento de dados e a comunicação entre os dispositivos.

Figura 4 - Ambiente UPnP (Intel, 2008)

A existência desta tecnologia faz com que o conceito futurista "All-IP" (tudo possuirá endereço IP) se torne possível num futuro não muito distante. Podemos imaginar um despertador ativado pela rede que sabe das suas reuniões, verifica o trânsito e a previsão do tempo, calcula quando você precisa acordar e, pela manhã, o informa do horário do seu voo, a previsão do local de destino, e quando você precisa sair. Em direção ao aeroporto, o seu assistente pessoal digital (PDA) ativado pelo UPnP encontra o melhor lugar para estacionar o carro e solicita um jornal para você se informar sobre a atualidade. Enquanto viaja, o seu PDA verifica as suas reuniões, faz as reservas dos restaurantes e hotéis e pede alguns petiscos para quando você chegar a casa. Atualmente estas extravagâncias ainda não existem, mas serão possíveis com a existência do UPnP. (UPnP Forum, 2012)

Ao conectar dispositivos à rede, que incorporam a tecnologia UPnP, automaticamente conectam-se uns aos outros, sem a necessidade de configurar ou centralizar serviços.

A especificação UPnP é baseada nos protocolos IP, TCP, UDP, HTTP e XML, permitindo que dispositivos se conectem e comuniquem entre si, negociando portas e permitindo que aplicações UPnP trabalhem sem a necessidade de configuração. Daí vem o nome universal, por não necessitar de nenhum driver de dispositivo. (UPnP Forum, 2012)

Os dispositivos UPnP, automaticamente, configuram seus endereços de rede, anunciam sua presença na sub-rede e permitem troca de serviços.

Basicamente, dispositivos UPnP transmitem as suas capacidades a todos os pontos na rede, permitindo que clientes UPnP ajam como pontos de controle.

Em comparação com a tecnologia Plug and Play, que facilitou a integração de novos periféricos a um único computador, o UPnP não destaca-se como uma novidade tão revolucionária, mas mostra-se como um importante passo para a evolução de nossas redes. (UPnP Forum, 2012)

2.5. Network Configuration (NetConf)

O Network Configuration (NetConf) trata-se de uma tecnologia de gestão e configuração de rede. A sua implementação foi iniciada em Maio de 2003 e foi publicado em Dezembro de 2006 pelo Internet Engineering Task Force (IETF). (Enns R., 2006)

O NetConf disponibiliza recursos que possibilitam instalar, manipular, apagar e recuperar configurações de dispositivos de rede. A sua funcionalidade é semelhante à CLI e às interfaces WEB, quando esta última é utilizada para a configuração de equipamentos de rede. Geralmente, CLI e Interfaces WEB, são direcionadas à interação direta entre humano e equipamento. Já o NetConf pode ser utilizado para gerenciar equipamentos remotamente, disponibilizando uma interface flexível e programável, fomentando a criação de aplicações de autoconfiguração e monitorização.

Numa sessão NetConf é possível realizar várias configurações simultâneas, e somente depois aplicá-las, diminuindo erros de operação.

As principais características do NetConf são: (Silva, 2009)

- Capaz de fornecer mecanismos que diferenciem dados configuráveis de dados não configuráveis;
- Seja suficientemente extensível para que fabricantes proporcionem acesso a todos os dados de configuração dos dispositivos usando um protocolo único;
- Interface aberta e programável;
- Utilize uma representação textual dos dados, de forma a serem facilmente editados, não havendo assim necessidade da utilização de ferramentas complexas de manipulação;

- Permita integração com os atuais métodos de autenticação do utilizador;
- Independência a nível de transporte;
- Suporte um conjunto de operações de configuração;
- Promova suporte a notificações assíncronas.

Antes do NetConf, a resolução atual para configuração de dispositivos era o SNMP. O SNMP foi altamente difundido entre fabricantes e frequentemente encontrado em dispositivos comerciais. Porém, as carências do protocolo, confiabilidade e segurança, a nível de configuração, deixa a desejar. Como já foi dito, o SNMP mostra-se como um excelente protocolo de monitorização.

O IETF, com a criação do NetConf, mostrou um protocolo de configuração sem as limitações encontradas no SNMP, como também, baseado nas novas tecnologias de Web Services (WS), que tem sido muito estudado no contexto de gestão de redes. (W3schools, 2009)

Os objetivos principais do NetConf, são unificar e propor um padrão suficientemente genérico para configurar diversos tipos de dispositivos.

Basicamente, o NetConf é um conjunto de definições para a confecção de arquivos Extensible Markup Language (XML) de configurações. (Wikipedia, 2012)

Dentre as características dos Web Services, pode-se citar sua simplicidade e padronização. O protocolo Simple Object Access Protocol (SOAP), baseado em XML e, geralmente, transportado via HTTP, é utilizado para troca de mensagens entre Web Services.

O IETF propõe as seguintes formas de transportar o protocolo NetConf:

- NetConf encapsulado em mensagens SOAP sobre HTTP; (Iijima T., 2008)
- NetConf encapsulado em mensagens SOAP sobre HTTPS (via SSL-TLS); (Paiossin, 2012)
- NetConf encapsulado em mensagens SOAP sobre BEEP; (Goddard T., 2006)
- NetConf diretamente sobre BEEP (Blocks Extensible Exchange Protocol); (Lear E., 2006)
- NetConf diretamente sobre SSH (Secure Shell); (Wikipedia, 2012)

O princípio de funcionamento do NETCONF é baseado no paradigma RPC (Remote Procedure Call), através do qual é definido um conjunto de operações do protocolo (Netconf, 2008). Basicamente o gerente NETCONF (cliente) codifica uma requisição RPC em XML e a envia ao agente NETCONF (servidor). O agente, ao receber uma mensagem

NETCONF, processa a requisição e envia uma resposta RPC de volta ao gerente. Tanto mensagem de pedido como resposta é enviada em formato XML, e têm as suas estruturas totalmente descritas em schema XML (W3schools, 2012), permitindo ao gerente e agente NETCONF validarem as mensagens recebidas. (Silva, 2009)

2.6. CPE WAN Management Protocol (CWMP)

O CPE WAN Management Protocol foi publicado em Maio de 2004 no relatório técnico 69 do DSL Fórum (atual BroadBand Forum), daí o protocolo ser também conhecido por TR-069. Trata-se de um protocolo de gestão remota de dispositivos e já encontrou ampla aceitação por grandes fabricantes, tais como a Thomson, Alcatel e Cisco, que implementam clientes TR-069 em seus dispositivos. (BroadBand Forum, 2011)

2.6.1. BroadBand Forum

O BroadBand Forum corresponde a um consórcio, sem fins lucrativos, dedicado ao desenvolvimento de especificações de redes de banda larga. É constituído por cerca de 200 líderes da indústria das telecomunicações, computação, redes e empresas provedoras de serviços. Foi fundado em 1994, inicialmente com o nome de DSL Forum, com cerca de 200 empresas associadas em divisões diferentes dos setores de telecomunicações e tecnologia da informação. Esta cooperação tem desenvolvido diferentes padronizações para ADSL, SHDSL, VDSL, ADSL2+ e VDSL2. Em 1999 tornou-se DSL Forum, nome da tecnologia Digital Subscriber Line (Linha de Assinante Digital, DSL). (BroadBand Forum, 2011)

Além de trabalhos desenvolvidos associados a este conjunto de tecnologias DSL, tem surgido outros trabalhos associados a outras tecnologias tais como: PON, EPON e desenvolvimento de normas Ethernet ponto a ponto. (Silva, 2009)

A partir de 2004, expandiu seu trabalho em outras tecnologias, incluindo fibra óptica. A partir de 17 de junho de 2008, mudou seu nome para BroadBand Forum. Sua especificação para Servidor de Autoconfiguração (ACS) de TR-069, originalmente publicado em 2004, foi adaptado para uso com set-top box e unidades de Network Attached Storage (Armazenamento Dedicado a Rede, NAS). Em 18 de maio de 2009, conseguiu uma forte união com o IP/MPLS Forum. (Silva, 2009)

O IP/MPLS Forum trata-se de uma organização internacional cujos seus membros são entidades tais como: provedores de serviço, fabricantes de equipamentos, centros de teste e utilizadores empresariais. Seu objetivo é encontrar soluções e aplicações direcionadas à correta utilização de diversas tecnologias de rede. (Silva, 2009)

Resultado desta união, o BroadBand Forum, tornou-se o órgão principal para criação de novas soluções ou padrões da próxima geração de redes IP.

O BroadBand Forum age em benefício dos seus membros, reconhecendo a competitividade entre eles, com isso gerando leis globais. Com estas leis o BroadBand Forum pretende ainda garantir uma correta utilização das técnicas especificadas, partilhar as melhores práticas de implementação, promover o mercado da banda larga e facilitar o desenvolvimento interoperacional da banda larga com base em componentes de rede. (Silva, 2009)

Além destes trabalhos, o BroadBand Forum, tem se preocupado com a eficiência energética, propondo medidas que proporcionam aderência de indústrias aos compromissos globais de redução de energia.

O desenvolvimento do protocolo de gestão remota da rede digital doméstica (TR-069) corresponde a um marco importante na história do BroadBand Forum, tornando-se mesmo como protocolo padrão para gestão remota. A capacidade de facilmente adicionar modelos de objetos a novos equipamentos tem contribuído para que provedores de serviço sejam capazes de manter sempre atualizados serviços e aplicações nos dispositivos. (Silva, 2009)

2.6.2. Descrição CWMP (TR-069)

Basicamente, a finalidade deste protocolo foi gerar uma padronização de gestão de equipamentos em ambiente WAN. Com base neste padrão, provedores de serviços podem, através da internet, gerenciar todos os seus equipamentos independentemente do dispositivo ou fabricante. Até o momento, não havia uma solução comum de gerenciamento de equipamentos, pelo fato de seus fabricantes criarem seus próprios mecanismos de gerência e não partilharem com seus concorrentes. (BroadBand, 2011)

O padrão TR-069 trata-se de um protocolo da camada de aplicação que proporciona comunicação bidirecional entre determinado equipamento que se pretenda

configurar e a respectiva entidade configuradora. Essa comunicação é baseada em mensagens SOAP sobre HTTP e garante uma configuração segura.

O TR-069 trata-se de uma resposta à complexidade de gerir equipamentos do usuário comum. É usado para a gestão ou configuração remota de equipamentos TR-069 domésticos (roteadores, modems, set-top box, telefones VoIP). (Silva, 2009)

Sendo sua grande maioria, equipamentos residenciais, poderá também gerenciar dispositivos não TR-069, visto ser possível a sua integração com a tecnologia UPnP, tornando-o capaz de alcançar uma vasta quantidade de equipamentos nas nossas redes.

> "[...] Num ambiente TR-069, o elemento responsável pela gestão dos equipamentos CPE (Customer Premises Equipment) é o ACS (Auto Configuration Server) que terá duas interfaces de comunicação distintas como se pode observar na figura 5. Uma diz respeito à informação trocada com fornecedores de serviço, sistemas de controle de acesso e operadores que utilizarão este servidor (esta interface está fora do âmbito de aplicação do TR-069). A outra interface corresponde à comunicação deste servidor com os dispositivos TR-069. [...]" (Silva, 2009)

> "[...] Cada CPE só pode ser gerido por um único ACS, num ambiente multi-provedor. Poderá ser limitativo, dado que toda a configuração de gestão de determinado CPE terá que ser mantida num único ACS que será responsável por resolver todos os conflitos relacionados com a configuração dos dados de configuração e distribuir a configuração para os respectivos dispositivos. [...]" (BroadBand Forum, 2011)

A Figura 5 representa um ambiente TR-069 contendo as entidades CPE e ACS.

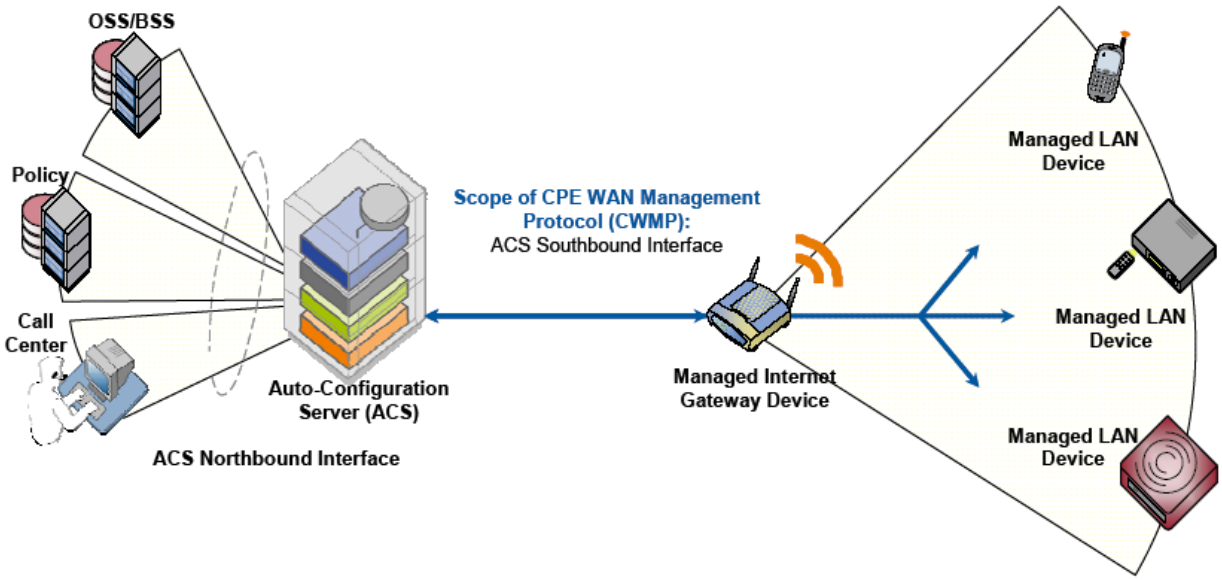

Figura 5 - Ambiente de gestão utilizando o protocolo CWMP (BroadBand Forum, 2011)

2.6.3. Funcionalidades

O TR-069 oferece as seguintes ferramentas e funcionalidades de gestão:

Autoconfiguração e provisionamento dinâmico de serviço.

- Capacidade de reconfigurar e recolher informação de CPE TR-069. (Silva, 2009)

Download de Software / Firmware

- Oferece ferramentas de gestão de download do software CPE bem como a atualização de arquivos de firmware. Coloca ainda ao nosso dispor mecanismos para identificação da versão, inicialização do download, e notificação de sucesso ou falha de download. (Silva, 2009)
- Quando o Download é iniciado pelo ACS, o ACS fornece ao CPE a localização do arquivo que será transferido. O CPE, em seguida, efetua a transferência, e notifica o ACS.
- No entanto estas transferências podem ser opcionalmente iniciadas pelo próprio CPE. Nesse caso, o CPE envia um pedido de download de um determinado tipo de arquivo ao ACS. O ACS responde iniciando o download seguindo os mesmos passos como se fosse o ACS que fará download. (Silva, 2009)

Acompanhamento de Estado e Performance

- Proporciona suporte a CPE de forma a tornar disponível informação com a qual o ACS poderá usar para monitorar o estado e performance do CPE. Também define um conjunto de mecanismos que permite que o CPE notifique o ACS de alterações no seu estado. (Silva, 2009)

Diagnóstico

- Disponibiliza suporte a CPE de forma a tonar disponível informação com a qual o ACS usará para diagnosticar e resolver problemas de conectividade ou serviços, bem como executar testes de diagnósticos. (Silva, 2009)

2.6.4. Arquitetura

O CWMP (CPE WAN Management Protocol), apesar de conter mecanismos exclusivos, baseia-se no uso de diversos protocolos padrão.

A tabela 1 as camadas protocolares que definem o CWMP.

Tabela 1 - Camadas protocolares do protocolo CWMP (Silva, 2009)

Camada	Descrição
CPE/ACS Application	Aplicações CWMP usadas nas entidades CPE e ACS. A aplicação é localmente definida e não faz parte do CPE WAN Management Protocol
RPC Methods	Métodos RPC especificados na norma CPE WAN Management Protocol
SOAP	Uma norma baseada em sintaxe XML utilizada para codificar RPC Methods. Especificamente SOAP 1.1
HTTP	HTTP 1.1
SSL/TLS	Padrão do Internet Transport Layer Security Protocols. Especificamente, SSL 3.0 (Secure Socket Layer) ou TLS 1.0 (Transport Layer Security).

TCP/IP	Padrão TCP/IP

O uso de SSL / TLS para transporte do CWMP é recomendado pela BroadBand Forum, gerando confiabilidade e integridade dos dados, como também permitindo autenticação em ambos os terminais. O protocolo pode ser utilizado diretamente sobre uma conexão TCP, sendo sacrificadas características importantes do uso de SSL / TLS. (Silva, 2009)

O funcionamento básico deste protocolo de configuração baseia-se em troca de mensagens SOAP transacionadas entre CPE e ACS através de HTTP 1.1, onde o CPE comporta-se como cliente HTTP e ACS como servidor HTTP. No entanto o protocolo contém também um mecanismo de pedidos de conexão que permite ao ACS comportar-se como cliente e CPE por sua vez como servidor. (Silva, 2009)

As operações e informações CWMP transmitidas através das mensagens SOAP são emitidas no formato textual, codificadas e decodificadas na linguagem de transporte XML.

Para um ACS configurar e monitorar um CPE, é informado uma série de métodos RPC disponibilizados pelo protocolo (*Get, Set, Inform, Download, Upload, Reboot* e outros).

Este protocolo possibilita aos desenvolvedores, a criação de ferramentas de configuração seguras, dinâmicas e escaláveis.

2.6.4.1. SOAP

> "[...] SOAP (Simple Object Access Protocol), no português, Protocolo Simples de Acesso a Objeto, é um protocolo para troca de informações estruturadas em uma plataforma descentralizada e distribuída. Ele se baseia na Linguagem de Marcação Extensível (XML) para seu formato de mensagem, e normalmente baseia-se em outros protocolos da Camada de aplicação, mais notavelmente em Chamada Remota de Procedimento (RPC) e Protocolo de Transferência de Hipertexto (HTTP), para negociação e transmissão de mensagens. SOAP pode formar a camada base de uma pilha de protocolos de *web services*, fornecendo um *framework* de mensagens básico sob o qual os serviços web podem ser construídos. Este protocolo baseado em XML consiste de três partes: um envelope, que define o que está na mensagem e como processá-la, um conjunto de regras codificadas para expressar instâncias do tipo de dados definidos na aplicação e uma

convenção para representar chamadas de procedimentos e respostas [...]" (W3C SOAP, 2012), como mostra a figura 6.

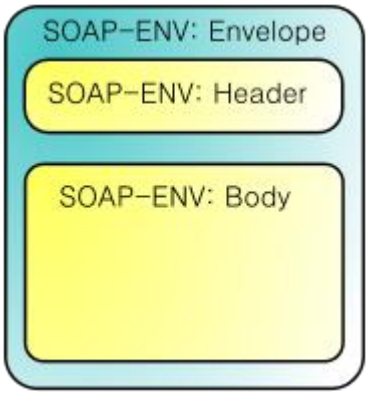

Figura 6 - Estrutura do SOAP (Wikipedia, 2012)

"[...] Sua especificação define um *framework* que provê maneiras para se construir mensagens que podem trafegar através de diversos protocolos e que foi especificado de forma a ser independente de qualquer modelo de programação ou outra implementação específica. Por não se tratar de um protocolo de acesso a objetos, o acrônimo não é mais utilizado. [...]" (W3C SOAP, 2012)

"[...] Geralmente servidores SOAP são implementados utilizando-se servidores HTTP, embora isto não seja uma restrição para funcionamento do protocolo. As mensagens SOAP são documentos XML que aderem a uma especificação fornecida pelo órgão W3C. [...]" (W3C SOAP, 2012)

"[...] O primeiro esforço do desenvolvimento do SOAP foi implementar RPC sobre XML. [...]" (Wikipedia, 2012)

2.6.4.2. HTTP

"[...] O **Hypertext Transfer Protocol ou** Protocolo de Transferência de Hipertexto **(HTTP**) é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) utilizado para sistemas de informação de hipermídia distribuídos e colaborativos. Seu uso para a obtenção de recursos interligados levou ao estabelecimento da World Wide Web. [...]" (T. Berners-Lee, 1996)

"[...] Para que o protocolo HTTP consiga transferir seus dados pela Web, é necessário que os protocolos TCP e IP (*Internet Protocol*, Protocolo de Internet) tornem

> possível a conexão entre clientes e servidores através de *sockets* TCP/IP. [...]" (Bastos, 1999)
>
> "[...] O HTTP utiliza o modelo cliente-servidor, como a maioria dos protocolos de rede, baseando-se no paradigma de requisição e resposta. Um programa requisitante (cliente) estabelece uma conexão com outro programa receptor (servidor) e envia-lhe uma requisição, contendo a URI, a versão do protocolo, uma mensagem MIME (padrão utilizado para codificar dados em formato de textos ASCII para serem transmitidos pela Internet) contendo os modificadores da requisição, informações sobre o cliente e, possivelmente, o conteúdo no corpo da mensagem. [...]" (Fielding, 1996)
>
> "[...] O protocolo HTTP faz a comunicação entre o cliente e o servidor por meio de mensagens. O cliente envia uma mensagem de requisição de um recurso e o servidor envia uma mensagem de resposta ao cliente com a solicitação. Segundo Foscarini, os dois tipos de mensagens existentes no protocolo utilizam um formato genérico, definido na RFC 822, para a transferência de entidades. [...]" (T. Berners-Lee, 1996)
>
> "[...] Uma mensagem, tanto de requisição quanto de resposta, é composta, conforme definido na RFC 2616, por uma linha inicial, nenhuma ou mais linhas de cabeçalhos, uma linha em branco obrigatória finalizando o cabeçalho e por fim o corpo da mensagem, opcional em determinados casos. [...]" (Herrmann, 1997)

Abaixo serão apresentados os campos que compõem uma mensagem mais detalhadamente.

Cabeçalho da mensagem

- O cabeçalho da mensagem (*header*) é utilizado para transmitir informações adicionais entre o cliente e o servidor. Ele é especificado imediatamente após a linha inicial da transação (método), tanto para a requisição do cliente quanto para a resposta do servidor, seguido de dois pontos (:) e um valor. Existem quatro tipos de cabeçalhos que poderão ser incluídos na mensagem os quais são: *general-header*, *requestheader*, *response-header* e *entity-header*. (Fielding, 1999)

Corpo da mensagem

- Uma mensagem HTTP pode conter um corpo de dados que são enviados abaixo das linhas de cabeçalho. Em uma mensagem de resposta, o corpo da mensagem é o recurso que foi requisitado pelo cliente, ou ainda uma mensagem de erro, caso este recurso não seja possível. Já em uma mensagem de requisição, o corpo pode conter dados que serão enviados diretamente pelo usuário ou um arquivo que será enviado para o servidor. Quando

uma mensagem HTTP tiver um corpo, poderão ser incluídos cabeçalhos de entidades que descrevem suas características, como por exemplo, o *Content-Type* que informa o tipo MIME dos dados no corpo da mensagem e o *Content-Length* que informa a quantidade de bytes que o corpo da mensagem contém. A tabela 2 apresenta alguns tipos MIME. (Fielding, 1999)

Tabela 2 - Tipos de MIME

Exemplo	**Descrição**
text/plain	Arquivo no formato texto (ASCII)
text/html	Arquivo no formato HTML, utilizado como padrão pra documentos Web
Image/gif	Imagem com formato GIF
Image/jpeg	Imagem com formato JPEG
application/zip	Arquivo compactado

Requisição

- Segundo Fielding, uma mensagem de requisição do cliente é composta pelos seguintes campos: uma linha inicial (*Request-Line*); linhas de cabeçalhos (*Request-header*); uma linha em branco obrigatória e um corpo de mensagem opcional. A linha inicial de uma requisição é composta por três partes separadas por espaços: o método (*Method*), a identificação do URI (*Request-URI*) e a versão do HTTP (*HTTP-Version*) utilizado.

- Segundo Bastos & Ladeira, *Request-URI* é um *identificador uniforme de recurso* (Uniform Resource Identifier) que identifica sobre qual recurso será aplicada a requisição. No protocolo HTTP, o tipo de URI utilizado é chamado de URL (Uniform Resource Locater), composto pela identificação do protocolo, pelo endereço do computador servidor e pelo documento requisitado.

Resposta

- Segundo Fielding, uma mensagem de resposta do servidor é composta pelos seguintes campos: uma linha inicial (*Status-Line*); linhas de cabeçalhos (*Responseheader*);

uma linha em branco obrigatória e um corpo de mensagem opcional. A linha inicial de uma resposta, chamada de linha de status, possui por sua vez três partes separadas por espaços: a versão do protocolo HTTP (*HTTP-Version*), um código de status (*Status-Code*) da resposta, que fornece o resultado da requisição, e uma frase de justificativa (*Reason-Phrase*) que descreve o código do status.

2.6.4.3. TLS e SSL

> "[...] O **Transport Layer Security** - TLS (Segurança da Camada de Transporte) e o seu predecessor, **Secure Sockets Layer** - SSL (Protocolo de Camada de Sockets Segura), são protocolos criptográficos que conferem segurança de comunicação na Internet para serviços como email (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados. [...]" (RFC 5246, 2008)
>
> "[...] O protocolo SSL provê a privacidade e a integridade de dados entre duas aplicações que comuniquem pela Internet. Isto ocorre através da autenticação das partes envolvidas e da cifra dos dados transmitidos entre as partes. Esse protocolo ajuda a prevenir que intermediários entre as duas pontas da comunicação tenham acesso indevido ou falsifiquem os dados transmitidos. [...]" (RFC 5246, 2008)
>
> "[...] O servidor do site que está sendo acessado envia uma chave pública ao browser, usada por este para enviar uma chamada secreta, criada aleatoriamente. Desta forma, fica estabelecida a trocas de dados criptografados entre dois computadores. [...]" (RFC 5246, 2008)

2.6.4.4. TCP/IP

> "[...] O **TCP/IP** é um conjunto de protocolos de comunicação entre computadores em rede (também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração. [...]" (Craig, 1998)

> "[...] O TCP, é um mecanismo de transporte confiável, orientado à conexão e que fornece um *stream de bytes* confiável, garantindo assim que os dados cheguem íntegros (não danificados e em ordem). O TCP tenta continuamente medir o quão carregada a rede está e desacelera sua taxa de envio para evitar sobrecarga. Além disso, o TCP irá tentar entregar todos os dados corretamente na seqüência especificada. Essas são as principais diferenças dele para com o UDP, e pode se tornar desvantajoso em *streaming*, em tempo real ou aplicações de *routing* com altas taxas de perda na camada internet. [...]" (Craig, 1998)

2.6.5. Parâmetros

O CWMP dispõe de mecanismos que possibilita um ACS ler, alterar ou apagar parâmetros internos dos CPE, ou seja, atribui a um ACS capacidades de configuração, monitorização e edição/adição de novos serviços aos CPE. Os parâmetros dos diferentes tipos de CPE, são definidos em normas separadas, tais como:

TR-106: Modelo de Dados para Equipamentos TR-069. (BroadBand Forum, 2011)

TR-098: Modelo de Dados para Internet Gateway Device TR-069. (Bernstein J., 2005)

TR-104: Modelo de Dados para VoIP CPE. (BroadBand Forum, 2011)

Cada parâmetro consiste num par nome/valor. O nome identifica um determinado parâmetro, e possui uma estrutura hierárquica semelhante de arquivos num diretório, com cada nível separados por um "." (ponto). O valor de um Parâmetro pode ser uma definição de diversos tipos de dados. (Silva, 2009)

Os parâmetros podem ser definidos como de leitura ou leitura e escrita. Os parâmetros só de leitura podem ser utilizados pelo ACS, apenas para reunir informações ou dados estatísticos do funcionamento do CPE.

Os parâmetros de leitura e escrita possibilitam ao ACS, gerenciar vários aspectos do funcionamento do CPE.

Apesar de certos parâmetros serem passíveis a alteração, contém informação confidencial (por exemplo, *passwords* de determinado utilizador); nessas situações, caso seja pretendida a leitura desses valores, será retornado um valor vazio. O valor de alguns parâmetros de escrita podem ser modificáveis por outros meios, por exemplo, via alguma

autoconfiguração existente na LAN. Daí a necessidade de precaução na implementação dos mecanismos de autoconfiguração tanto do lado WAN como LAN.

2.6.6. Estabelecimento de Sessões

O protocolo CWMP, define mecanismos permitindo que o CPE se conecte ao ACS em diversas condições, fazendo com que essa comunicação ocorra numa frequência mínima.

O CPE poderá a qualquer momento estabelecer uma comunicação com o ACS, desde que este conheça o endereço do ACS, e essa comunicação ocorrerá após o CPE enviar uma mensagem de *Inform* num POST HTTP.

Este *Inform* trata-se de um método RPC invocado pelo CPE e executado no ACS, e é utilizado para estabelecer as sessões de transação entre CPE e ACS. A invocação deste método contém informação relevante acerca do equipamento e informa o ACS das razões pela qual ele pretende estabelecer sessão. (Silva, 2009)

O CPE inicia comunicação com ACS em diversas situações tais como o momento em que é ligado à rede após a sua instalação inicial; sempre que seja ligado ou reiniciado ou mesmo quando ocorrem eventos que devam ser comunicados ao ACS (como por exemplo, quando o endereço IP do CPE é alterado). Além destas condições é ainda definido no CPE um período de tempo no qual estabelece comunicação periódica com o ACS sobre uma base de tempo contínua. Caso a mensagem de *Inform* se trate de uma invocação periódica deste método, a mensagem SOAP deverá indicar na estrutura de eventos a ocorrência do evento PERIODIC. (Silva, 2009)

Este protocolo contém, no entanto, um mecanismo que permite estabelecimento assíncrono de sessões. Cada CPE TR-069 possui um serviço HTTP suportando autenticação do tipo *digest* no qual o ACS poderá atuar como cliente HTTP, podendo assim informar o CPE de que se pretende comunicar com ele. Uma vez que o CPE receba um pedido de conexão enviado pelo ACS, irá responder nos próximos 30 segundos com a invocação do método *Inform*, indicando a ocorrência do evento de CONNECTION REQUEST. (Silva, 2009)

Quando a comunicação entre CPE e ACS é fechada, o CPE identifica-se através da informação de fábrica (número serial), de modo que faça com que o ACS conheça-o e possa responder de forma correta.

2.6.7. Modelo de Comunicação

A comunicação estabelecida pelo protocolo TR-069 corresponde a uma troca bidirecional de pedidos e respostas RPC. A transação é finalizada após ambos os terminais não estiverem mais transmitindo. O CPE tem a responsabilidade de iniciar ou finalizar sessões de comunicação entre terminais TR-069. (Silva, 2009)

Para manter uma troca de operações numa única sessão, o CPE deverá manter a conexão TCP durante toda sessão.

A figura 7 contém um exemplo de uma transação entre CPE e ACS e demonstra o fluxo da comunicação e como a mesma ocorre em ambos os sentidos. Neste exemplo o ACS invoca no CPE os métodos *GetParameterValues* e *SetParameterValues*, e recebe do CPE as respostas das invocações desses métodos. (Silva, 2009)

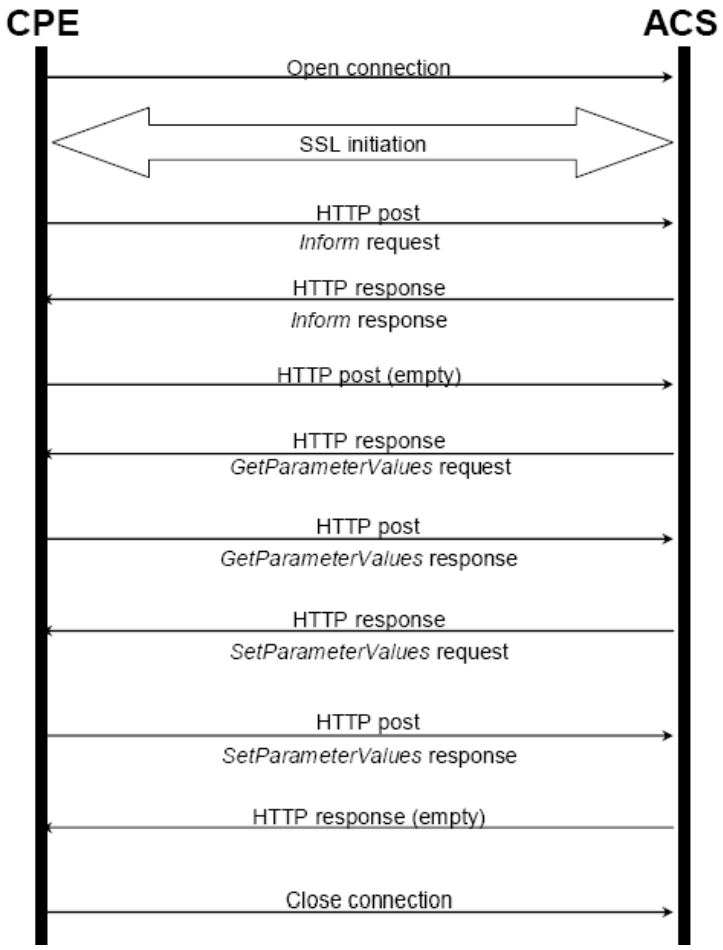

Figura 7 - Exemplo de uma transação de mensagens numa sessão TR-069 (BroadBand Forum, 2011)

- A sessão inicia com o estabelecimento da conexão TCP.

- Estabelecimento e ativação de SSL e respectiva ativação do mecanismo de segurança.
- Neste momento o CPE envia um POST HTTP invocando o método *Inform* para inicializar a transação de operações com o ACS.
- O ACS responde com *InformResponse*, indicando ao CPE de que o *Inform* enviado foi recebido com sucesso e que o CPE foi autenticado com sucesso.
- No seguimento da chegada do *InformResponse* o CPE entrega ao ACS um POST HTTP vazio indicando que a sessão foi estabelecida com sucesso e que está pronto a receber pedidos de invocação de métodos RPC.
- Em resposta ao POST vazio, o ACS responde invocando no CPE uma operação, sendo neste caso do exemplo apresentado na imagem, um *GetParameterValues*.
- O CPE responde num novo POST com o *GetParameterValuesResponse* retornando o resultado à invocação do referido método.
- O ACS opta por invocar nova operação, desta feita um *SetParameterValues*.
- O CPE retorna o resultado dessa operação no *SetParameterValuesResponse*.
- O ACS envia uma mensagem vazia ao equipamento informando que não pretende invocar mais operações.
- O CPE termina sessão e em seguida irá iniciar uma conexão do tipo "*standby*" podendo vir a ser aproveitada novamente pelo ACS posteriormente.

2.6.8. Métodos RPC

O CPE WAN Management Protocol utiliza um mecanismo bidirecional de chamada de procedimentos remotos (RPC) que permite que uma aplicação chame um serviço de outra aplicação que será executado em uma máquina remota. A máquina que invoca a execução desses procedimentos remotos, envia mensagens contendo informações que indicam qual procedimento deve executar e quais parâmetros devem utilizar para a execução. Após a execução, os respectivos resultados são enviados à aplicação que fez a chamada. (BroadBand Forum, 2011)

O CPE deverá suportar uma série de métodos RPC, que poderão ser invocados pelo servidor de autoconfiguração ACS, como também, o CPE poderá invocar chamadas de procedimentos no ACS.

Na tabela 3, são apresentados os métodos requeridos e opcionais existentes em ambos os lados, conforme é especificado na norma TR-069. (BroadBand Forum, 2011)

Tabela 3 - Parâmetros TR-069 (BroadBand Forum, 2011)

Method name	CPE requirement	ACS requirement
CPE methods	Responding	Calling
GetRPCMethods	REQUIRED	OPTIONAL
SetParameterValues	REQUIRED	REQUIRED
GetParameterValues	REQUIRED	REQUIRED
GetParameterNames	REQUIRED	REQUIRED
SetParameterAttributes	REQUIRED	OPTIONAL
GetParameterAttributes	REQUIRED	OPTIONAL
AddObject	REQUIRED	OPTIONAL
DeleteObject	REQUIRED	OPTIONAL
Reboot	REQUIRED	OPTIONAL
Download	REQUIRED[5]	REQUIRED[5]
Upload	OPTIONAL	OPTIONAL
FactoryReset	OPTIONAL	OPTIONAL
GetQueuedTransfers	OPTIONAL[6]	OPTIONAL
GetAllQueuedTransfers	OPTIONAL	OPTIONAL
ScheduleInform	OPTIONAL	OPTIONAL
SetVouchers	OPTIONAL[7]	OPTIONAL[7]
GetOptions	OPTIONAL[7]	OPTIONAL[7]
ACS methods	Calling	Responding
GetRPCMethods	OPTIONAL	REQUIRED
Inform	REQUIRED	REQUIRED
TransferComplete	REQUIRED[8]	REQUIRED[9]
AutonomousTransferComplete	OPTIONAL	REQUIRED
RequestDownload	OPTIONAL	OPTIONAL
Kicked	OPTIONAL	OPTIONAL

2.6.8.1. Métodos CPE

Os métodos CPE são de total responsabilidade do ACS. Porém, o método Reboot, em situações específicas, pode ser executado pelo próprio CPE.

Abaixo, seguem os principais métodos que podem ser invocados em equipamentos TR-069. (Silva, 2009) (BroadBand Forum, 2011)

GetRPCMethods

- Invocando este método, o ACS receberá como resposta, uma lista de todos os métodos suportados pelo CPE.

SetParameterValues

- Este método é invocado pelo ACS para modificar o valor de um ou mais parâmetros do CPE. Deve ter como parâmetros de entrada uma lista de pares "nome – valor", onde "nome" corresponderá ao parâmetro e "valor" o que se pretende atribuir. A resposta a chamada *SetParameterValues*, informará se todos os métodos e seus respectivos valores, foram validados e aplicados ou se foram validados e não aplicados.

GetParameterValues

- Este método é chamado pelo ACS, quando se pretender obter o valor de um ou mais parâmetros do CPE. Deve ter como parâmetros de entrada uma lista dos parâmetros que pretendemos conhecer. A resposta será uma lista de pares "nome – valor", sendo nome e valor do parâmetro, respectivamente.

GetParameterNames

- Este método deverá ser chamado pelo ACS para obter os parâmetros possíveis de um determinado CPE. Deve ter como parâmetros de entrada um apontador e um booleano. O primeiro apontará para um nó da hierarquia de parâmetros, correspondendo assim ao diretório completo de um parâmetro ou uma parte parcial desse diretório. Caso o apontador seja vazio, apontará para o topo da hierarquia.
- Sendo o booleano falso, na resposta constarão todos os parâmetros cujo nome contenha o apontador passado. Caso contrário, na resposta constarão somente os nós filhos do apontador passado.
- Na resposta além de conter os nomes dos parâmetros que pretende visualizar, constará informações se o parâmetro é só de leitura ou de leitura e escrita.

Reboot

- Este método faz com que o CPE reinicie. A chamada desse método é mais realizada pelo lado do CPE do que do ACS. Sempre que no CPE realizar uma mudança em

suas configurações, o próprio deverá executar o método Reboot. Também, visto ser opcional, poderá também ser implementado do lado do ACS.

- Reboot é um método bastante simples. É usado um parâmetro vazio na sua invocação, sendo a resposta também vazia.

Factory Reset

- Este método invocado, faz com que as configurações do CPE voltem no estado definido pelo fabricante.

Download

- Este método é usado pelo ACS, fazendo com que o CPE inicie um download a partir de uma URL estabelecida. Comparando aos outros métodos até aqui falados, para a invocação deste método, são necessários vários parâmetros, fazendo dele, um dos métodos mais complexos do CWMP. É importante ressaltar os parâmetros mais utilizados, tais como: o tipo de download que o CPE efetuará (Firmware Upgrade Image, Web Content e Vendor Configuration File); a URL onde se encontra o arquivo; dados de usuário e senha, quando necessários, para autenticação no servidor onde se encontram os arquivos, caso contrário, esses dados deverão ser vazios; a especificação do nome e do tamanho do arquivo em bytes.
- Em resposta à invocação, o CPE indica se o Download foi completado e aplicado com sucesso e os momentos de início e fim desta ação.

2.6.8.2. Métodos ACS

A invocação destes métodos é de total responsabilidade dos CPE.

Abaixo, seguem as principais operações que podem ser invocadas num ACS. (Silva, 2009) (BroadBand Forum, 2011)

GetRPCMethods

- Invocando este método, o CPE receberá como resposta, uma lista de todos os métodos suportados pelo ACS.

Inform

- O CPE invocará este método sempre que necessitar estabelecer sessão com o ACS.
- A mensagem de *Inform* carregará diversas informações, tais como: Identificação do CPE (Organizationally Unique Identifier, Serial Number, Manufacturer, ProductClass); listagem dos eventos ocorridos no equipamento desde o último *inform*; a data e hora atual; e algumas informações de configuração do equipamento.

TransferComplete

- Esse método é invocado pelo CPE de forma a informar o ACS que foi concluído um download ou upload, iniciados pelo ACS, anteriormente, através da chamada do método de Download ou Upload.
- Na mensagem deste método, conterá a indicação de sucesso ou falha, como também os instantes de início e fim da ação.

2.6.9. Integração TR-069 e UPnP

Sendo um protocolo de escalabilidade local, os CPE que suportam UPnP mas não suportam TR-069, não possibilitarão sua configuração remota.

Há um componente intermediário entre os protocolos UPnP e TR-069 que permite ao ACS descobrir, controlar e receber eventos de dispositivos UPnP, mesmo que o servidor se encontre numa rede diferente.

Este componente intermédio atuará como proxy e terá como objetivo traduzir a comunicação utilizada por ambos os protocolos, a sua localização será dentro da rede local e terá conexão com o ACS. (Royon, 2007)

A arquitetura geral deste proxy pode ser analisada na figura 8.

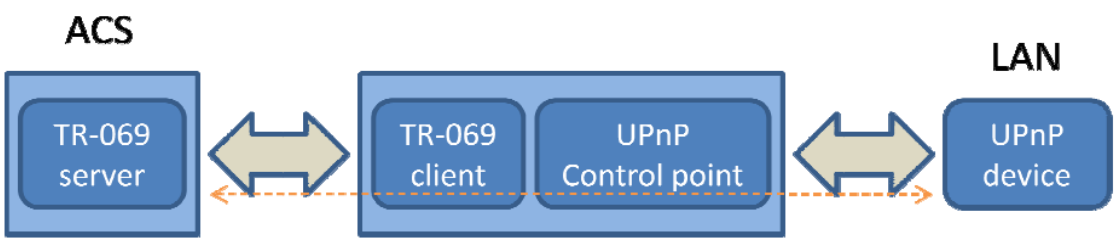

Figura 8 - Integração de TR-069 com UPnP

O desenvolvimento do protocolo TR-064 (LAN-side CPE Configuration Specification) é o grande responsável pela possibilidade de integração destas duas tecnologias. (Stark B., 2004)

O protocolo TR-064 é um complemento do protocolo TR-069, onde nele são tratadas especificações UPnP. Ele permite que um gateway TR-069 possa configurar e gerenciar equipamentos em nossas LAN, possibilitando assim, que um ACS TR-069, alcance e gerencie remotamente CPE TR-069.

O TR-064 é dividido em dois grandes componentes, a arquitetura do dispositivo UPnP, na qual define como o software do dispositivo consegue descobrir e aprender dinamicamente as capacidades de outros pontos UPnP e assim controlá-los e configurá-los; e um modelo que anuncia as suas próprias capacidades e funções. (Kirksey, 2005)

Dado ao fato do TR-064 tratar especificações UPnP, permite uma gestão padrão entre vários fabricantes, favorecendo os ISP. (Kirksey, 2005)

Os ISP têm geralmente optado por protocolos padrão para suporte e ativação de serviços em todos os seus CPE. No entanto, as ferramentas anteriormente existentes para este fim apresentavam lacunas e complexidade e nenhuma delas provou ser robusta, segura, bem definida e extensível o suficiente. (Silva, 2009)

A solução para encontrar uma tecnologia que permitisse aos ISP interagir ou gerenciar equipamentos CPE, e que fosse capaz de contornar as limitações impostas anteriormente, surgiu após uma combinação normalizada entre redes WAN e LAN.

Esta combinação, só foi possível após o aparecimento dos protocolos TR-069 e TR-064. (BroadBand Forum, 2011)

Os CPE podem ser manipulados por ambos os protocolos (TR-069 e TR-064). (BroadBand Forum, 2011)

Para um melhor entendimento dos protocolos TR-064 e TR-069, segue o exemplo: num serviço VoIP as configurações podem ser enviadas ao dispositivo através de um ACS TR-069 presente no ISP; já a aplicação TR-064, existente localmente no PC do usuário, é responsável pelo serviço.

Caso o usuário registre algum problema com o serviço, o protocolo TR-064, sendo executado através de uma aplicação local, possibilita diagnosticar e restaurar, facilmente o dispositivo. Junto, a aplicação de gestão TR-069 possibilitará monitorar o desempenho e a disponibilidade do serviço. (Silva, 2009)

Capítulo 3

Neste capítulo, será realizado uma análise teórica da respectiva API_TR-069, focando em apresentar as respectivas necessidades e precauções que se devem ter durante sua utilização; sua forma correta de implementação; e seu resultado final.

Serão descritos os requisitos; casos de uso e a arquitetura de um ACS utilizando um diagrama de classe da API_TR-069.

3.1. Requisitos da API_TR-069 (Silva, 2009)

A API_TR-069, foi desenvolvida para apresentar os seguintes requisitos e funcionalidades:

BroadBand Forum Compliant

API_TR-069 implementando os métodos obrigatórios e procedimentos estabelecidos pela TR-069.

Comunicação entre ACS e CPE

Obrigatoriamente, deverá:

- Suportar sessões SSL/TLS de HTTPS ou HTTP.
- Suportar autenticação Básica e *Digest*.
- Suportar simultaneamente múltiplas sessões TR-069 com diferentes fabricantes de CPE.
- Aproveitar sessões já criadas para novos pedidos de configuração.
- Ser capaz de invocar todos os métodos, dentre esses, *Reboot, FactoryReset e GetRPCMethods.*

Configuração

- Ser capaz de configurar serviços, aplicar reconfiguração e instalar novo firmware nos CPE.
- Permitir buscar informações de Configuração, Falhas e Desempenho do CPE.

3.2. Casos de Uso

Nesta sessão, será demonstrada a forma de interação entre a aplicação de gestão e o usuário, através de alguns dos principais métodos desta API: *Reboot*; Atualização de firmware (*Donwload*), Configuração de serviço no CPE (*SetParameterValues*) e Detecção de falha de energia (*Inform*). (Silva, 2009)

Reboot

- Usuário pede à API um CPE passando o ID do CPE;
- Usuário invoca método *Reboot*;
- Por fim, CPE envia ao ACS resposta do método invocado;
- Se API recebe resposta de sucesso
    - Usuário recebe a mensagem de sucesso, então pode invocar novos métodos ou terminar sessão.
- Se API recebe falha
    - Usuário recebe a mensagem de erro e a sessão é terminada.

Atualização de firmware (Download)

- Usuário pede à API um CPE passando o ID do CPE;
- Usuário invoca método *Download*, parametrizado com a URL onde se localiza o arquivo;
- Por fim, o CPE envia ao ACS a resposta do método invocado;
- Se o método *Download* foi executado com sucesso;
    - Usuário recebe a mensagem de sucesso, então pode invocar novos métodos ou terminar sessão.
- Se método falha;
    - Usuário recebe a mensagem de erro, é esperado que nas próximas sessões o CPE envie uma mensagem *TransferComplete* informando o sucesso ou erro da execução e aplicação do Download, e então o usuário pode invocar novos métodos ou finalizar a sessão.

Configuração de serviço (SetParameterValues)

- Usuário pede à API um CPE passando o ID do CPE;
- Usuário invoca método *SetParameterValues*, parametrizando as alterações nas configurações que pretende realizar no CPE;
- Por fim, o CPE envia ao ACS a resposta do método invocado;
- Se o método *SetParameterValues* tenha sido executado e aplicado com sucesso;
    - Usuário recebe a resposta mostrando a alteração dos parâmetros da configuração e a ativação/desativação do serviço, então pode invocar novos métodos ou finalizar a sessão;
- Se o método foi executado, porém não aplicado;
    - Usuário recebe a resposta informando as alterações e a necessidade de invocar o método *Reboot*;
    - Então, usuário invoca método *Reboot*;
    - Usuário pode invocar novos métodos ou terminar sessão.

Detecção de falha de energia (Inform)

- O CPE sendo reiniciado, invocará automaticamente o método *Inform*;
- Se houve ocorrência do evento BOOT;
    - Usuário recebe mensagem da ocorrência de falha de energia.

3.3. Arquitetura – Diagrama de Classe API_TR-069

A figura 9 mostra a arquitetura representada pelo diagrama de classe da API_TR-069. Serão descritos os funcionamentos dos componentes. (Silva, 2009)

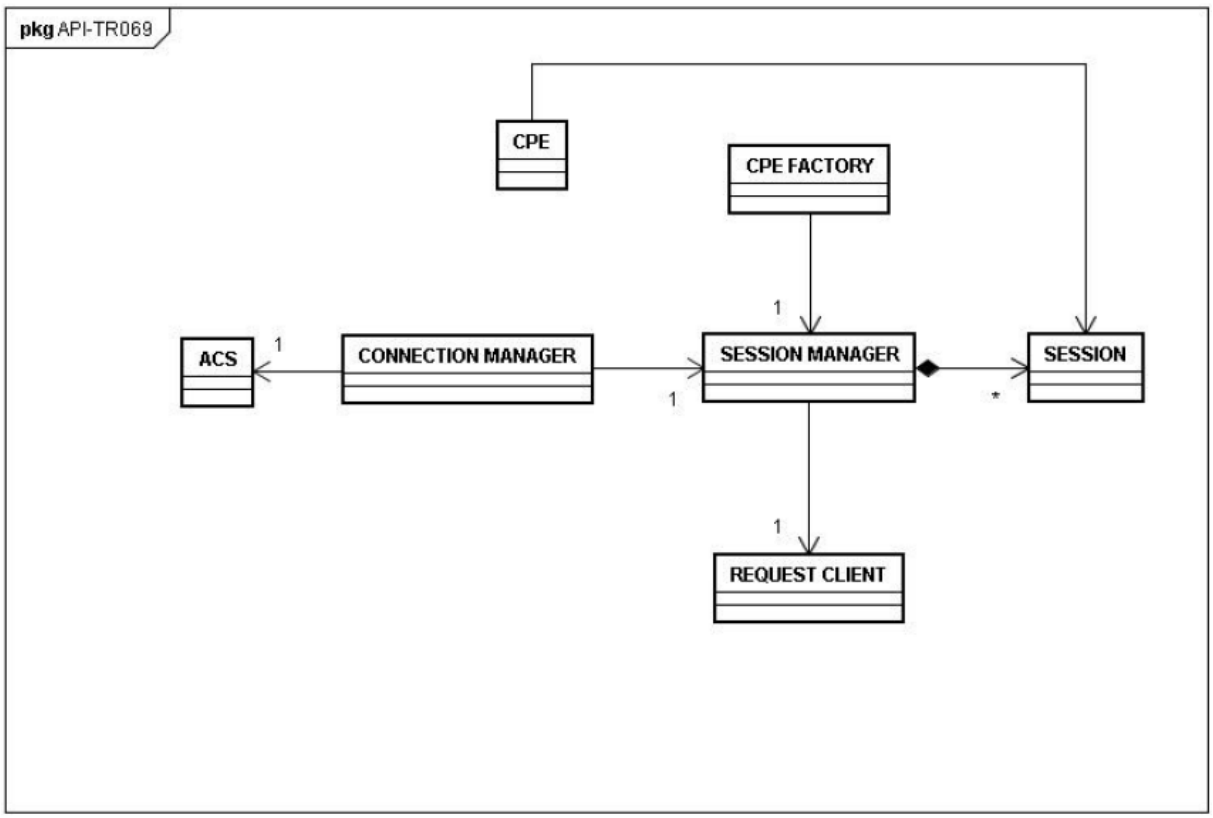

Figura 9 - Diagrama de Classe da API_TR-069 (Silva, 2009)

O bloco CPE FACTORY é responsável por criar entidades CPE. E para isso, necessita de informações de identificação do dispositivo CPE de uma sessão TR-069. Mais tarde a sessão será retornada pelo bloco SESSION MANAGER.

O bloco CPE FACTORY está ligado diretamente ao bloco SESSION MANAGER, que este último registrará o pedido e fechará sessão com determinado dispositivo.

SESSION MANAGER deverá ser capaz de gerenciar múltiplas sessões TR-069, conforme pedidos de configuração e diagnóstico. Este bloco não só gerencia os pedidos de sessão, como também, as sessões ativas. Este bloco está associado ao REQUEST CLIENT, que é o responsável por enviar pedidos de conexão aos CPE e funcionará como um cliente HTTP. Os CPE TR-069 incorporam um servidor HTTP, no qual será utilizado para comunicação com o ACS. Este servidor mantem-se à escuta e para utilizá-lo, é necessária autenticação.

Conforme é registrado o interesse de sessão de um equipamento no SESSION MANAGER, é passada a informação necessária ao REQUEST CLIENT, para que possa informar ao CPE, a necessidade de se comunicar com ele.

Como resposta ao pedido HTTP, enviado ao CPE pelo REQUEST CLIENT, o

dispositivo deverá responder permitindo estabelecer uma sessão TR-069 com o ACS.

O bloco CONNECTION MANAGER é responsável por receber, via HTTP, e processar as mensagens enviadas pelo dispositivo.

O bloco ACS incorpora as operações TR-069, que podem ser invocadas pelos dispositivos CPE no ACS.

Caso o pedido HTTP seja para execução de um método ACS, logo o CONNECTION MANAGER recorre ao ACS para que seja executada a respectiva operação e envie a mensagem de resposta.

Em seguida, o CONNECTION MANAGER recorre ao SESSION MANAGER informando que há conexão com determinado dispositivo. Com esta informação, o bloco SESSION MANAGER cria uma sessão ativa com o dispositivo, simbolizado na figura 9 pelo bloco SESSION.

Todo o diagrama é concluído quando a sessão criada é retornada ao CPE FACTORY que utilizará para criar a entidade CPE.

O CPE incorpora todas as operações que poderão ser executadas pelo protocolo de gestão remota TR-069.

O bloco SESSION MANAGER é o responsável por criar, conhecer, entregar e terminar sessões.

Portanto, toda a comunicação entre um CPE e um ACS passará pelo bloco CONNECTION MANAGER que assim será entregue ao SESSION MANAGER que saberá encaminhar essa informação à respectiva sessão.

Capítulo 4

Neste capítulo, será demonstrado o funcionamento real do protocolo, utilizando a ferramenta VigorACS SI da empresa chinesa DrayTek Corp. junto ao CPE Vigor 2110 series, adquiridos através de parceria com seu representante comercial nacional iK1 Tecnologia Ltda, residente na cidade de São Paulo. Nos itens 4.1 e 4.2, verá uma breve descrição das empresas parceiras citadas anteriormente. Todas as informação contidas neste capítulo, foram analisadas e autorizadas para divulgação pela empresa iK1 Tecnologia Ltda., como segue por escrito no Anexo A.

4.1. iK1 Tecnologia Ltda

Fundada em 2004, por um grupo de profissionais experientes, a iK1 é uma empresa especializada em soluções de TI com ênfase em gerenciamento de processos e telecomunicações para o mercado corporativo. O principal diferencial está no conjunto de soluções de baixo custo de instalação (baseadas em Software Livre), o que inclui o desenvolvimento de aplicações sob medida para Internet e Web Services. A partir da parceria com a estrangeira DrayTek, em meados de 2005, a iK1 ingressou no ramo de produtos, com a comercialização de roteadores e equipamentos para redes, VPNs e VoIP. Já em 2010 iniciou a parceria com a empresa espanhola, Visual Tools, uma das líderes de desenvolvimento e comercialização de soluções digitais em vídeo-vigilância para o mercado profissional. A iK1 também tem uma linha de produtos próprios, adaptados às necessidades do mercado brasileiro. Na sede, em São Paulo, funcionam as áreas de distribuição, treinamento e suporte para canais, além de consultoria e fábrica de software.

4.2. Draytek Corp.

A DrayTek Corp. foi fundada em 1997, reunindo algumas das principais lideranças da emergente indústria de banda-larga e telecomunicações. A sua linha de produtos abrange Firewalls de segurança para empresas; Redes de dados criptografados (VPN) para trabalho remoto; modems ADSL; roteadores ADSL, wireless LAN (WLAN), VoIP, Multi-WAN (até quatro links de internet simultâneos); entre outras soluções inovadoras, oferecendo

redução de custo, flexibilidade e grande eficácia. Com tantos fabricantes produzindo produtos de banda larga, a DrayTek se esforça continuamente para lançar produtos inovadores, inspirando o mercado com novas ideias, desenvolvendo combinações eficazes e aperfeiçoamentos das soluções existentes. Esta excelência técnica é reconhecida em elogios frequentes nos meios de comunicação, bem como em prêmios de desempenho. Desde a sua fundação em 1997, a empresa tem trabalhado em colaboração com seus parceiros de desenvolvimento e distribuição na Europa e, por ter escritórios regionais em contato direto com os usuários finais, os engenheiros de desenvolvimento da DrayTek podem criar produtos e acessórios adaptados às reais demandas e necessidades do mercado. No Brasil, a distribuição dos equipamentos DrayTek é de responsabilidade da iK1 Tecnologia Ltda. que, além da venda, oferece suporte, treinamentos e eventos para os seus clientes.

4.3. Vigor 2110 series

4.3.1. Descrição

Figura 10 - Roteador Vigor 2110 series Draytek

Os roteadores de banda larga da série Vigor2110 (figura 10) oferecem diversas ferramentas para configurar, monitorar e proteger sua rede, dentre elas, um poderoso firewall embutido, dois túneis de VPN e CSM (*Content Security Management*). Os modelos n e Vn compartilham a rede via Wireless 802.11n usando a tecnologia MIMO (*Multiple IN Multiple OUT*), que melhora seu desempenho e alcance, e o modelo Vn suporta telefonia VoIP e ainda backup de telefonia convencional.

Todos os roteadores da série Vigor2110 contam com 1 porta USB para o compartilhamento de impressora, disco USB, e modem 3G USB, que pode ser usado como backup da WAN principal, caso esta falhe (*fail-over*).

4.3.2. Especificação técnica

4.3.2.1. Interface de Hardware

- Throughput de 70MB
- 10.000 Sessões NAT Simultâneas
- 4 Portas10/100M LAN Switch, RJ-45
- 1 porta 10/100M WAN , RJ-45
- USB 1 Porta para Ligação de Impressora/modem3G e/ou Disco USB (c/ possibilidade de ligação de Hub USB energizado)
- Recursos de Rede
- IGMP Proxy/ Snooping
- DHCP Client/Relay/Server
- DNS Dinâmico
- NTP Client
- RADIUS Client
- UPnP
- Protocolo de Roteamento Rota Estática/RIP V2

4.3.2.2. LAN

- VLAN Baseada em Portas
- 4-port 10/100 M Ethernet Switch

4.3.2.3. Protocolo WAN

- DHCP Client
- IP Fixo
- PPPoE
- BPA
- L2TP

4.3.2.4. VPN

- Até 2 túneis de VPN
- Dead Peer Detection (DPD)
- VPN Pass-through
- Autenticação: MD5, SHA-1
- Autenticação IKE: Chave Pré-Compartilhada e Assinatura Digital (X.509)
- LAN-to-LAN, Teleworker-to-LAN
- DHCP sobre IPSEC
- Protocolo: PPTP, IPSec, L2TP, L2TP sobre IPSec

4.3.2.5. Firewall

- Multi-NAT, DMZ Host, Redirecionamento e Abertura de Portas
- Endereço IP Anti-spoofing
- E-Mail de Alerta e Registro Via Syslog
- Vincular IP ao MAC Address
- Bloqueio de Aplicações IM /P2P
- Filtro de URL por Palavras-Chave (Lista Branca e Lista Negra)
- GlobalView Web Content Filter (Commtouch)

4.3.2.6. Gerenciamento de Banda

- QoS
- Garantia de Banda Larga por Categorias Definidas pelo Usuário
- Ponto de Classificação de Código de Serviços Diferenciados (DiffServ)
- 4 níveis de Prioridade para Cada Direção (Inbound/Outbound)
- Limite de Sessão/Banda Larga

4.3.2.7. USB

- 3G USB Modem como WAN2
- Compartilhamento de Impressora
- Sistema de Arquivos

- Suporte a Sistemas de Arquivos FAT32/FAT16
- Suporte a Função de FTP para Compartilhamento de Arquivos e Pastas
- Suporte a Samba para Windows para Compartilhamento de Arquivos

4.3.2.8. Gestão de Redes

- Interface Web (HTTP/HTTPS)
- CLI (Command Line Interface, Telnet/SSH)
- Administração de Controle de Acesso
- Configuração de Backup/Restauração
- Funções de Diagnósticos Integradas
- Atualização de Firmware Através de TFTP/FTP/Web/TR-069
- TR-069 Management
- Log Via Syslog
- SNMP Management MIB-II

4.4. Software VigorACS SI

O VigorACS SI, é um poderoso sistema de gestão centralizada (CMS), que permite ao integrador de sistemas, gerir dispositivos Draytek de um modo mais conveniente a longo prazo. Baseado na especificação TR-069, o VigorACS SI possui um interface de utilização amigável de modo a que a configuração de dispositivos seja um processo fácil. Como um "prestador de serviços de valor agregado", o integrador de sistemas pode ajudar o utilizador a configurar ligações VPN, serviços VoIP e diminuir o custo de gestão do cliente, ao abordar mensagens em tempo real a partir de VigorACS SI (Visus, 2012).

Além disso, a lógica de gestão, simples de compreender, pode permitir ao pessoal de TI um forma fácil de assistir os clientes. O VigorACS SI simplifica as tarefas de gestão através do tipo de produto e as definições das funcionalidades de recursos como IPSec / PPTP VPN. Assim são necessários menos conhecimentos técnicos para implementar um ambiente VPN, ao utilizar o assistente de VPN incluído, na criação de parâmetros complexos como IPSec ou PPTP. (Visus, 2012)

4.4.1. Principais Características (Visus, 2012)

- Suporta séries de roteadores Vigor com especificação TR-069
- Nível de rede ilimitada para grupos CPE
- Auto provisionamento remoto e monitorização de estado
- Serviço de provisionamento dinâmico e agendável
- Assistente VPN para configuração fácil
- Relatório diário e de desempenho para revisão
- Sistema de log ao sistema
- Gestão de alarme em tempo real
- Gestão de Topologia
- Gestão de firmware avançado
- Gestão de grupos de utilizadores e de segurança

4.4.2. Arquitetura do sistema

A figura 11 mostra uma visão geral da aplicação entre o VigorACS e os dispositivos CPE. Através do protocolo TR-069, o VigorACS SI, pode se comunicar e gerenciar dispositivos com facilidade. (Manual VigorACS SI, 2010)

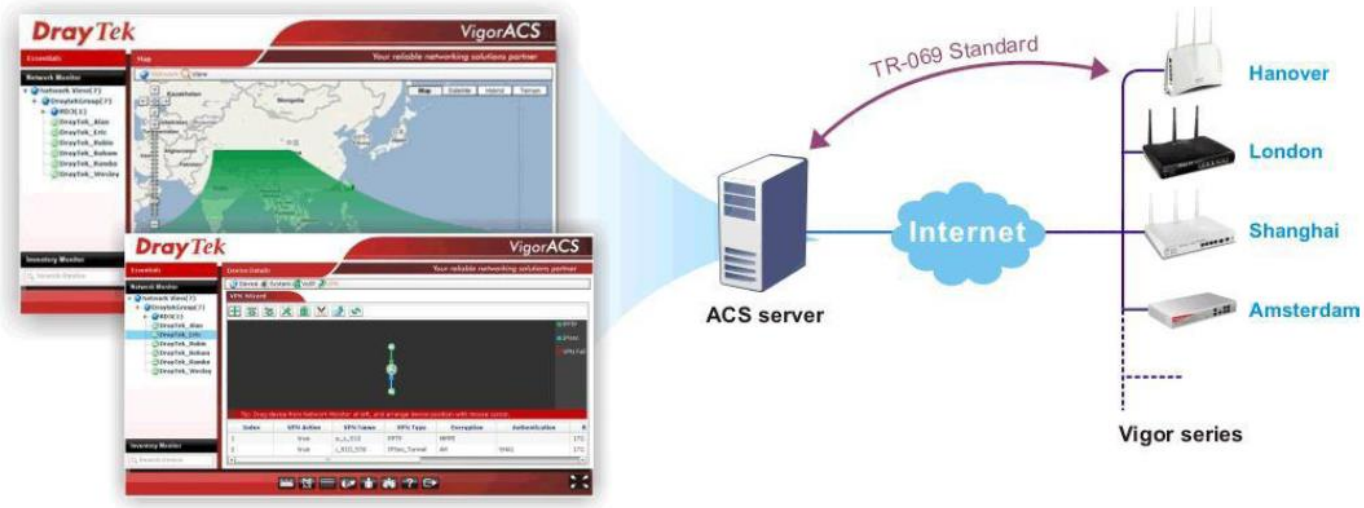

Figura 11 - Visão geral da comunicação entre ACS e CPE

4.4.3. Serviço Web

"[...] **Web Service** é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes. Com esta tecnologia é possível que novas aplicações possam interagir com aquelas que já existem e que sistemas desenvolvidos em plataformas diferentes sejam compatíveis. Os Web Services são componentes que permitem às aplicações enviar e receber dados em formato XML. Cada aplicação pode ter a sua própria linguagem, que é traduzida para uma linguagem universal, o formato XML. O Web Service faz com que os recursos da aplicação do software estejam disponíveis sobre a rede de uma forma normalizada.

Utilizando esta tecnologia, uma aplicação pode invocar outra para efetuar tarefas simples ou complexas mesmo que as duas aplicações estejam em diferentes sistemas e escritas em linguagens diferentes. Por outras palavras, os Web Services fazem com que os seus recursos estejam disponíveis para que qualquer aplicação cliente possa operar e extrair os recursos fornecidos pelo Web Service.

As bases para a construção de um Web Service são os padrões XML e SOAP. O transporte dos dados é realizado normalmente via protocolo HTTP ou HTTPS para conexões seguras (o padrão não determina o protocolo de transporte). Os dados são transferidos no formato XML, encapsulados pelo protocolo SOAP.

São identificados por um URI (Uniform Resource Identifier), descritos e definidos usando XML (Extensible Markup Language). Um dos motivos que tornam os Web Services atrativos é o facto deste modelo ser baseado em tecnologias padrões, em particular XML e HTTP (Hypertext Transfer Protocol). São utilizados para disponibilizar serviços interativos na Web, podendo ser acessados por outras aplicações usando, por exemplo, o protocolo SOAP (Simple Object Access Protocol).

Para a representação e estruturação dos dados nas mensagens recebidas/enviadas é utilizado o XML (eXtensible Markup Language). As chamadas às operações, incluindo os parâmetros de entrada/saída, são codificadas no protocolo SOAP (Simple Object Access Protocol, baseado em XML). Os serviços (operações, mensagens, parâmetros, etc.) são descritos usando a linguagem WSDL (Web Services Description Language). O processo de publicação/pesquisa/descoberta de *Web Services* utiliza o protocolo UDDI (Universal Description, Discovery and Integration).

Enquanto que o SOAP especifica a comunicação entre um cliente e um servidor, o WSDL descreve os serviços oferecidos. [...]" (Wikipedia, 2009)

4.4.4. Instalação e execução do VigorACS SI

Para a instalação do Software VigorACS SI, as tecnologias necessárias são:

- JDK 1.5 ou maior;
- MySQL 5.1.41 ou maior;
- Software VigorACS SI

Após realizado o passo anterior, é só abrir qualquer Browser de navegação e executar a seguinte URL:

- http://localhost/web/ACS.html

4.5. Testes

Para os testes do protocolo CWMP, está sendo utilizada a ferramenta VigorACS SI da empresa DayTrek, junto ao CPE DrayTek Vigor 2110. Ambos foram escolhidos, pois já implementam a especificação técnica TR-069, assim podendo demonstrar facilmente seu funcionamento com o objetivo de concluir o seu uso.

Apesar de ser um protocolo para gerenciamento padrão de CPE, independentemente do fabricante, o software VigorACS SI, faz gerenciamento TR-069 somente de equipamentos do fabricante DrayTek.

Inicialmente, a DrayTek havia desenvolvido o software VigorACS para que pudesse gerenciar qualquer tipo de CPE, que implementasse o padrão TR-069. Porém, para facilitar o gerenciamento completo dos seus equipamentos, não só gerenciamento TR-069, transparecendo aos gerentes determinadas configurações, a empresa decidiu criar o software VigorACS SI (Sistemas Integrados), facilitando as configurações de todos os recursos disponíveis nos equipamentos DrayTek.

Por esse motivo, atualmente, o software VigorACS SI, gerencia apenas CPE Draytek.

4.5.1. Arquitetura de Teste

A arquitetura definida para testes do equipamento e do software está representada pela figura 12.

URL de acesso:
http://192.168.0.10/web/ACS.html

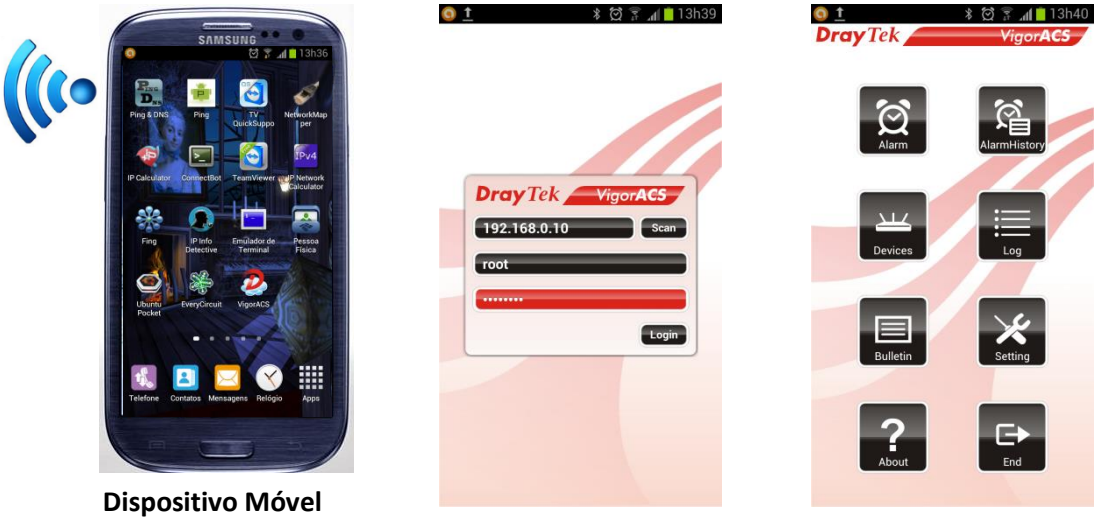

Figura 12 - Arquitetura para testes do protocolo CWMP

O Roteador TP-Link recebe o link na porta WAN e foi definido como o gateway padrão da rede, utilizando o IP 192.168.0.1. O Roteador Vigor 2110 Draytek, está sendo

alimentado com link através do TP-Link, utilizando o IP 192.168.0.103. O notebook ficou definido como Servidor de Gerenciamento, pois é nele que hospeda o software VigorACS SI, utilizando o IP 192.168.0.10. O dispositivo móvel está registrado com o IP 192.168.0.105, e estará utilizando o VigorACS Móvel, que fará papel de Cliente ACS, onde através dele, obterá alguns dos resultados de métodos invocados através do servidor de autoconfiguração.

4.5.2. Configurando TR-069 no CPE Vigor 2110 series

As configurações do CPE Vigor 2110 series, são realizadas através de qualquer browser, digitando na barra de endereços o IP padrão 192.168.1.1 e autenticando com o usuário e senha padrões, *admin* e *admin*, respectivamente, podendo ser alterados.

Para que funcione corretamente a comunicação do ACS com o CPE, são necessárias algumas configurações iniciais na área de gerência do CPE, na aba TR-069 Setting, como é mostrado na figura 13.

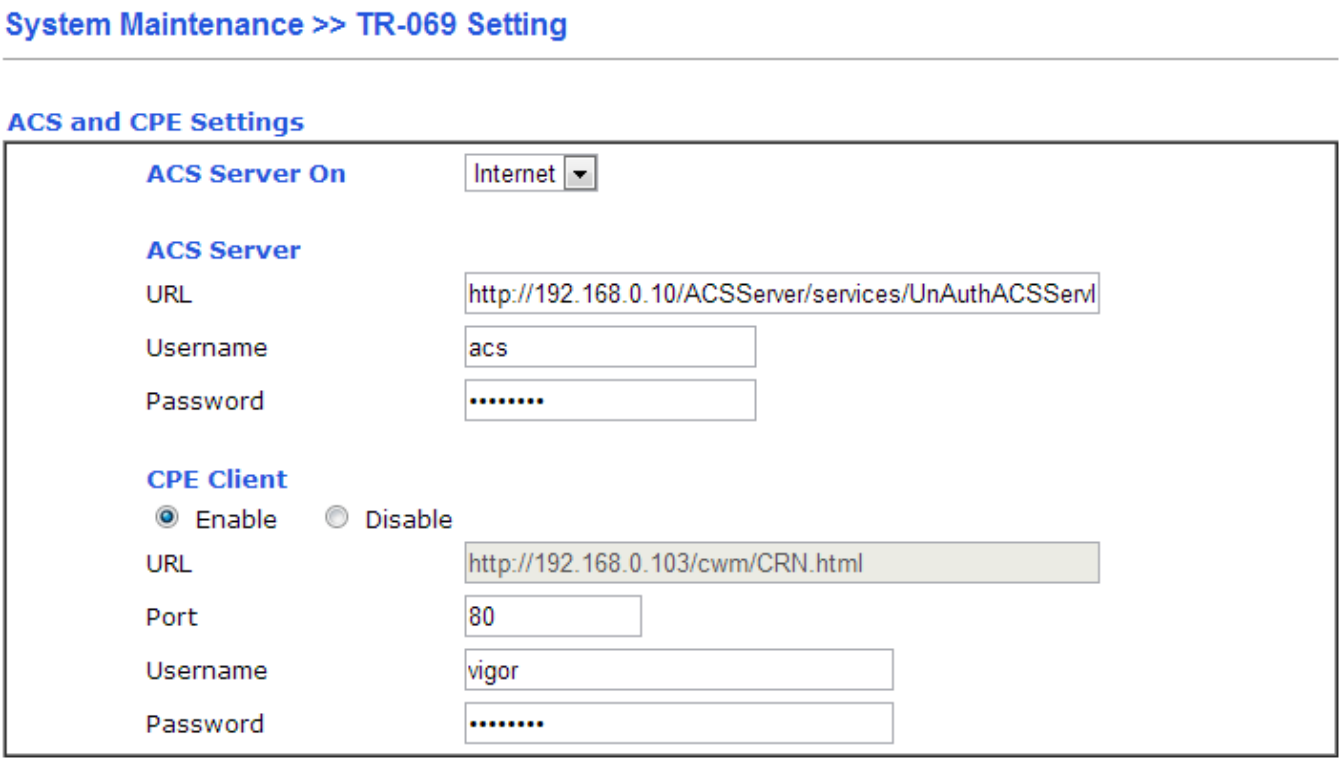

Figura 13 - Configuração TR-069 no CPE Vigor 2110 series

Descrição das configurações mostradas na figura 13.

ACS Server

- URL – endereço no qual o CPE faz autenticação com o ACS.
- Username – usuário da rede criada no ACS, onde o CPE será hospedado.
- Password – senha da rede criada no ACS, onde o CPE será hospedado.

CPE Server

- Enable ou Disable – habilita ou desabilita o gerenciamento TR-069 do CPE.
- URL – endereço único no qual o ACS gerencia o CPE.
- Port – porta pela qual o ACS, se autenticará e gerenciará o CPE.
- Username – usuário necessário para o ACS autenticar e gerenciar o CPE.
- Password – senha necessária para o ACS autenticar e gerenciar o CPE.

4.5.3. Utilizando o software VigorACS SI

A figura 14, mostra a utilização do software VigorACS SI, já com o CPE Vigor 2110 series autenticado.

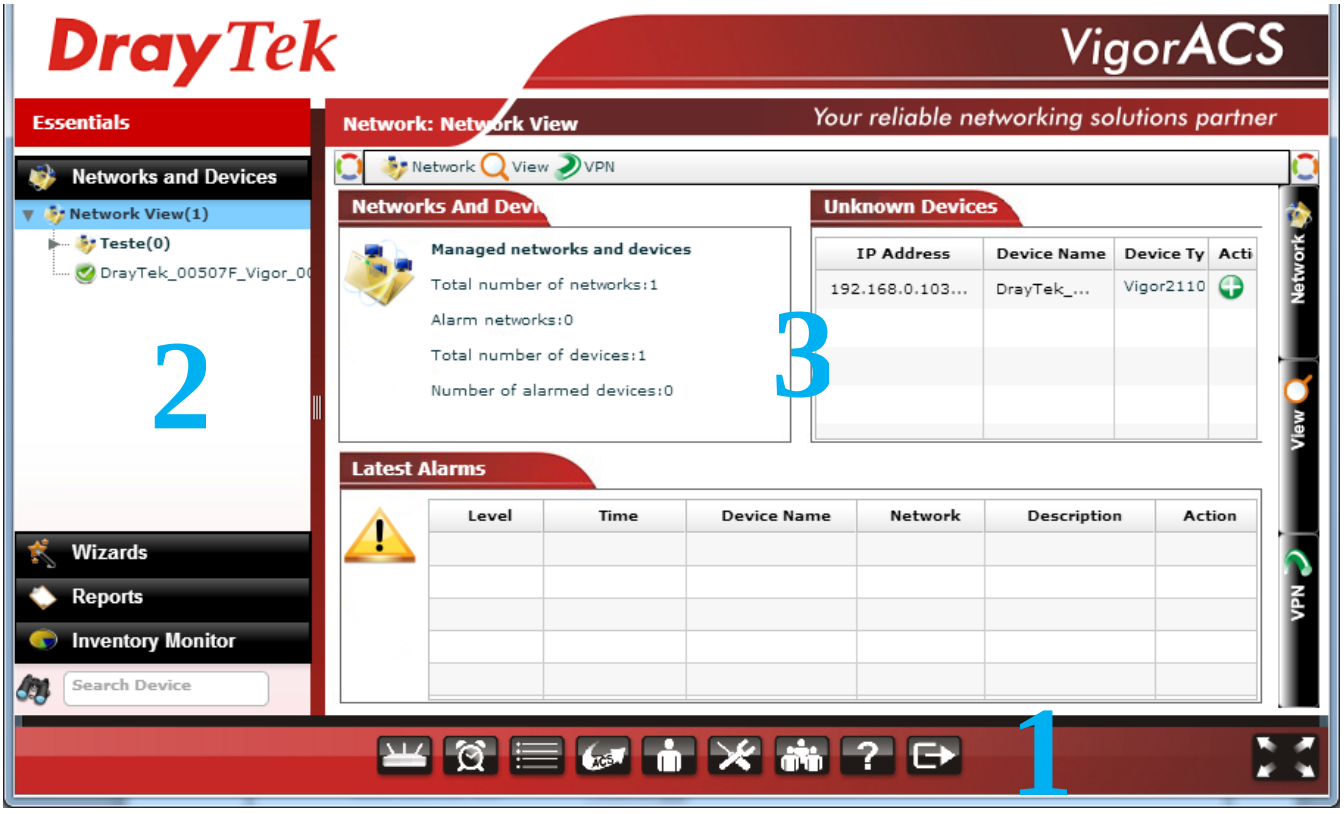

Figura 14 - Tela inicial do VigorACS SI

Tabela 4 - Descrição da tela inicial do VigorACS SI

Parte 1	Essa área apresenta diferentes modos de operação. Cada modo tirará parâmetros diferentes para configuração ou informações diferentes. Basta passar o mouse sobre cada um deles para abrir a página web correspondente. 
Parte 2	Essa área exibe listas hierárquicas de acordo com modo de operação selecionado.
Parte 3	Essa área exibe as informações detalhadas de acordo com o parâmetro selecionado na Parte 2.

4.5.3.1. Testes de Provisionamento

Neste item, serão demonstrados os funcionamentos dos principais métodos já citados no item 3.2, tais como, *Reboot*, Atualização de Firmware (*Upload*) e Configuração de Serviço (*SetParameterValues*) e Falha de energia (*Inform*).

4.5.3.1.1. Reboot

O método *Reboot*, pode ser invocado por ambas as partes. Através do ACS, é possível invocar este método, como também é possível diretamente do CPE. Ambas as formas são registradas no servidor de autoconfiguração. Como mostram as figuras 17 e 18. Se executado através do CPE, é enviada uma mensagem de registro para o ACS.

Figura 15 - Invocando método Reboot através do ACS

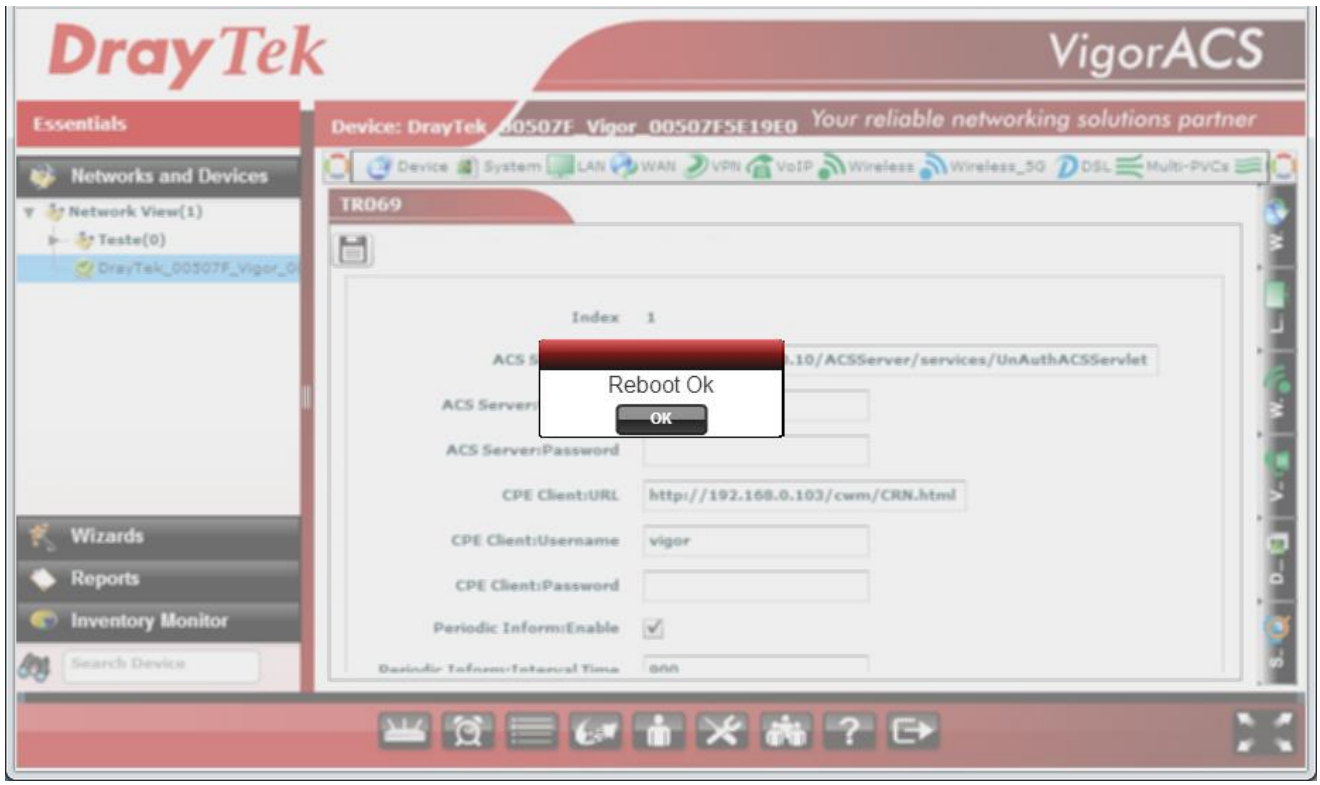

Figura 16 - Mensagem de retorno do método Reboot

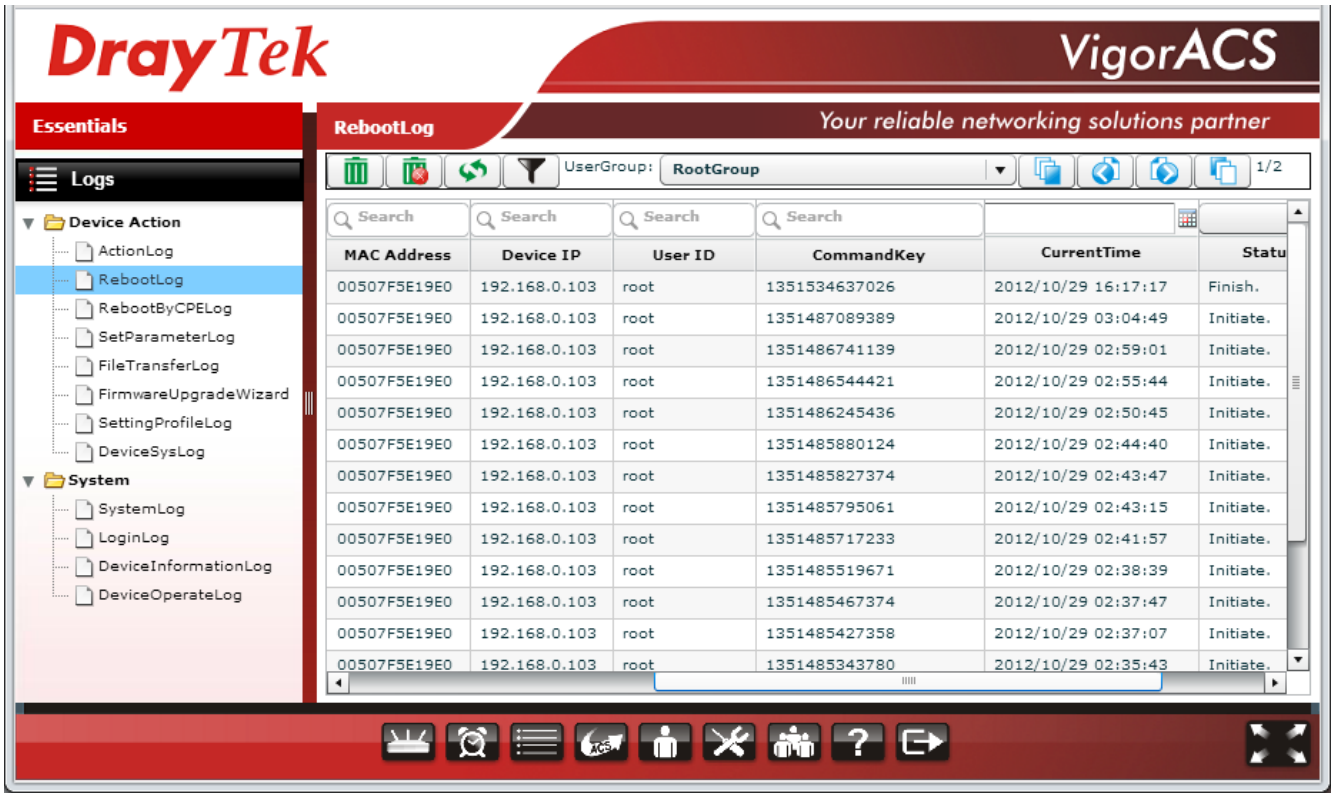

Figura 17 - Logs de invocação do método Reboot pelo ACS

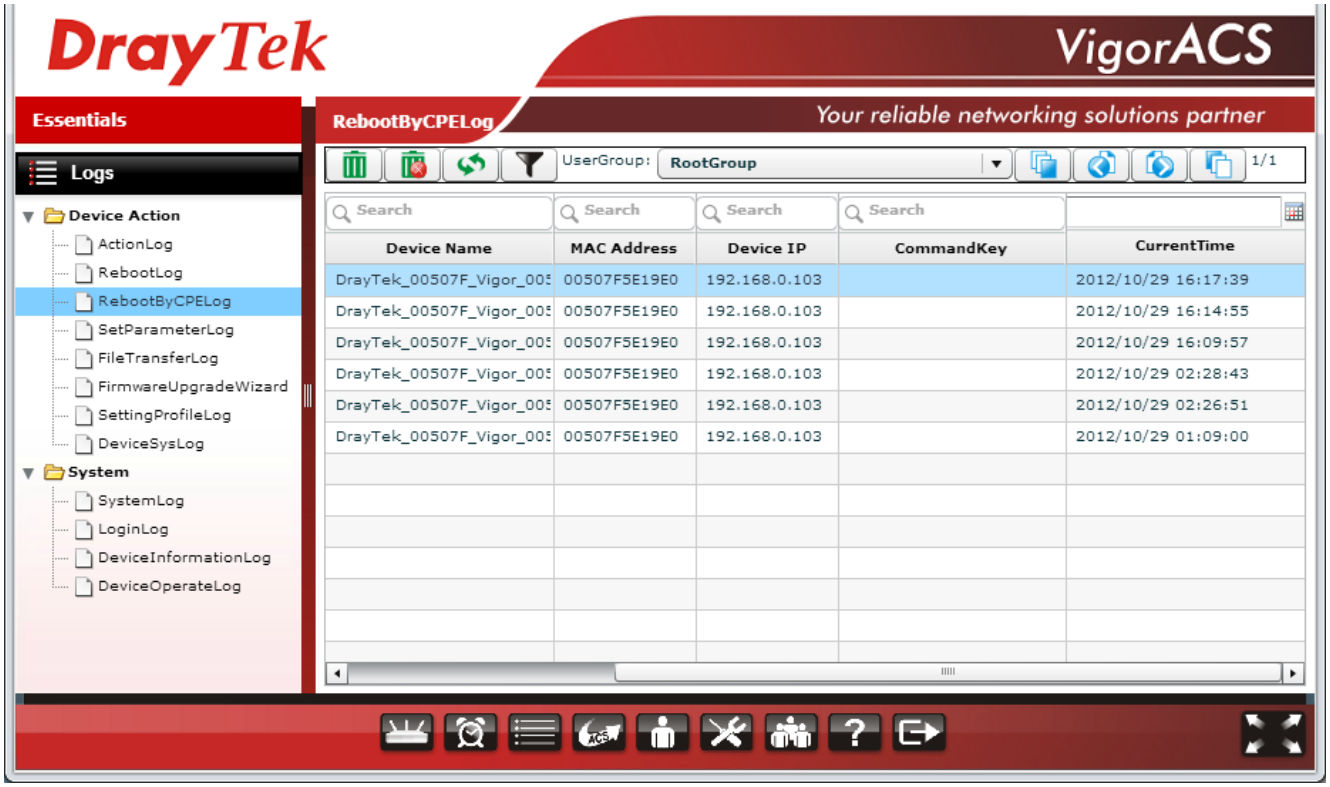

Figura 18 - Logs de invocação do método Reboot pelo CPE

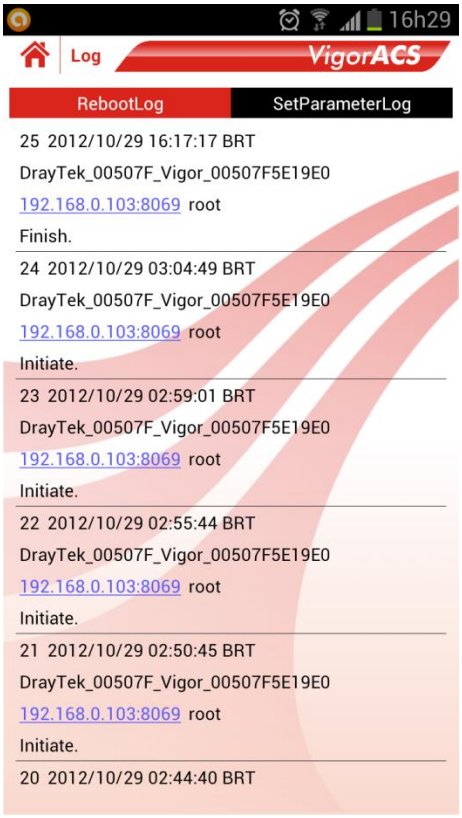

Figura 19 - Logs do método Reboot no aplicativo móvel

4.5.3.1.2. Atualização de firmware (Upload)

A figura 20, mostra como verificar versão do firmware do CPE.

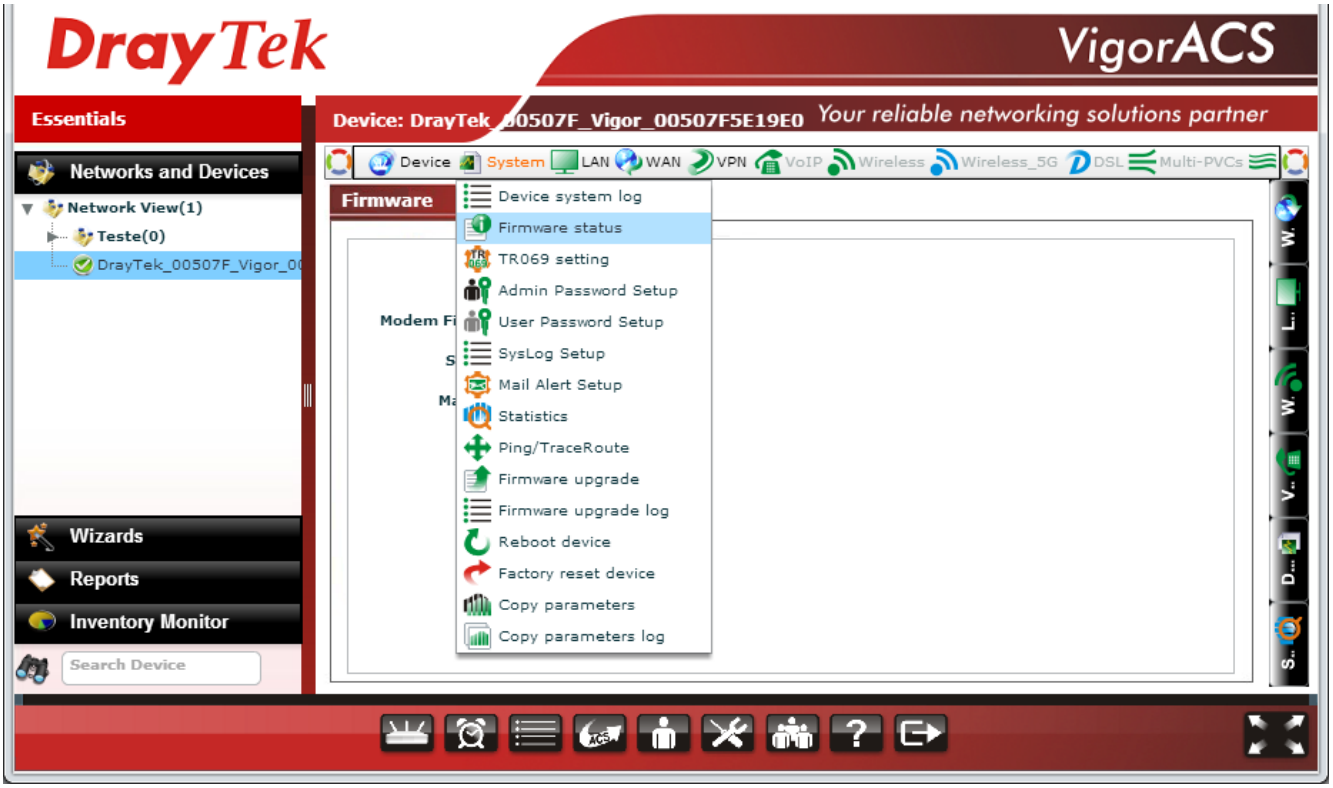

Figura 20 - Firmware status

A figura 21, após invocado o método de verificação de versão de firmware, é mostrada, no ACS, a versão do firmware utlizada pelo Vigor 2110 series. Apesar da versão 3.3.7 ser a mais atual disponível no site da Draytek, o teste de atualização de firmware foi executado.

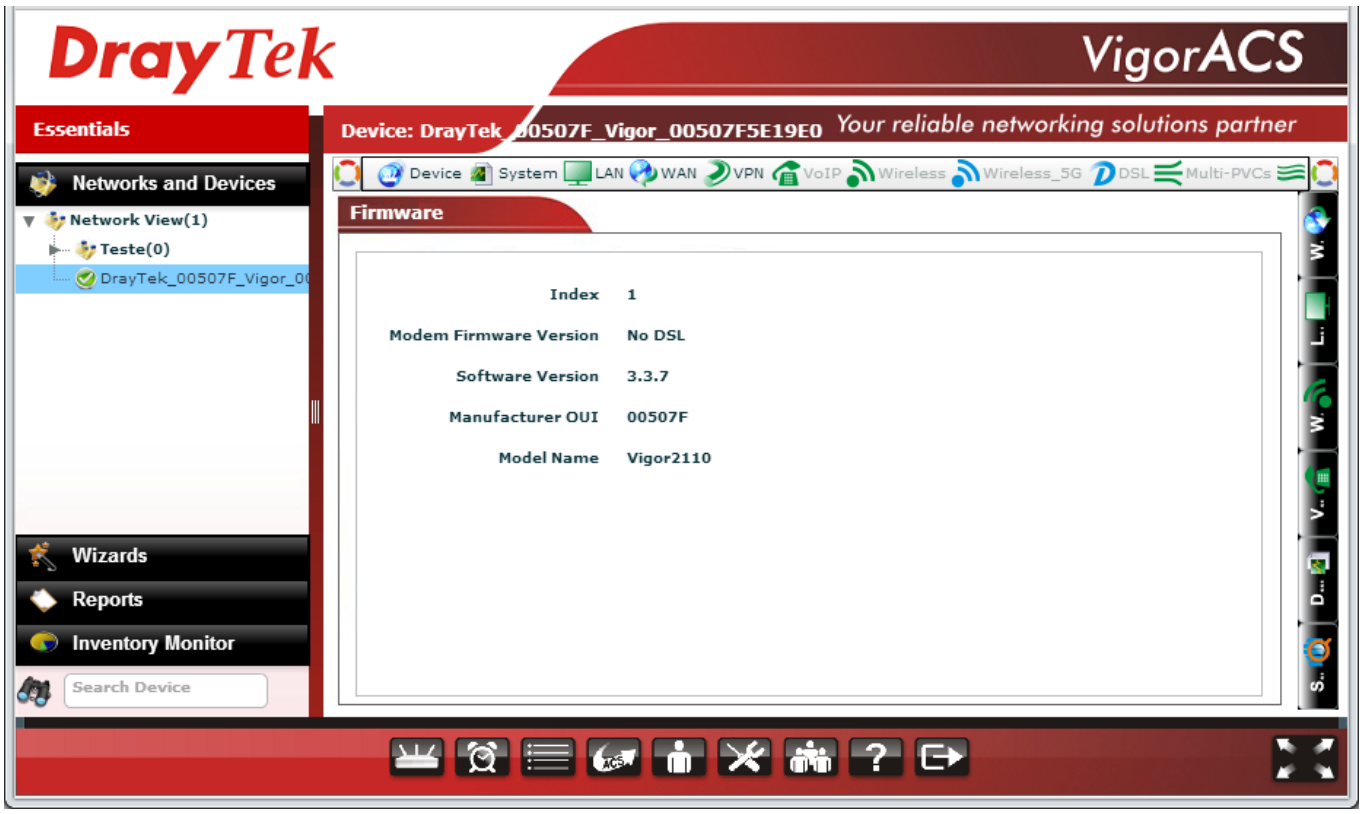

Figura 21 - Versão do firmware

A figura 22, mostra o momento do upload do firmware para atualização do CPE.

Figura 22 - Firmware upload

A figura 23, mostra o momento em que o ACS fica aguardando o término do upgrade do CPE.

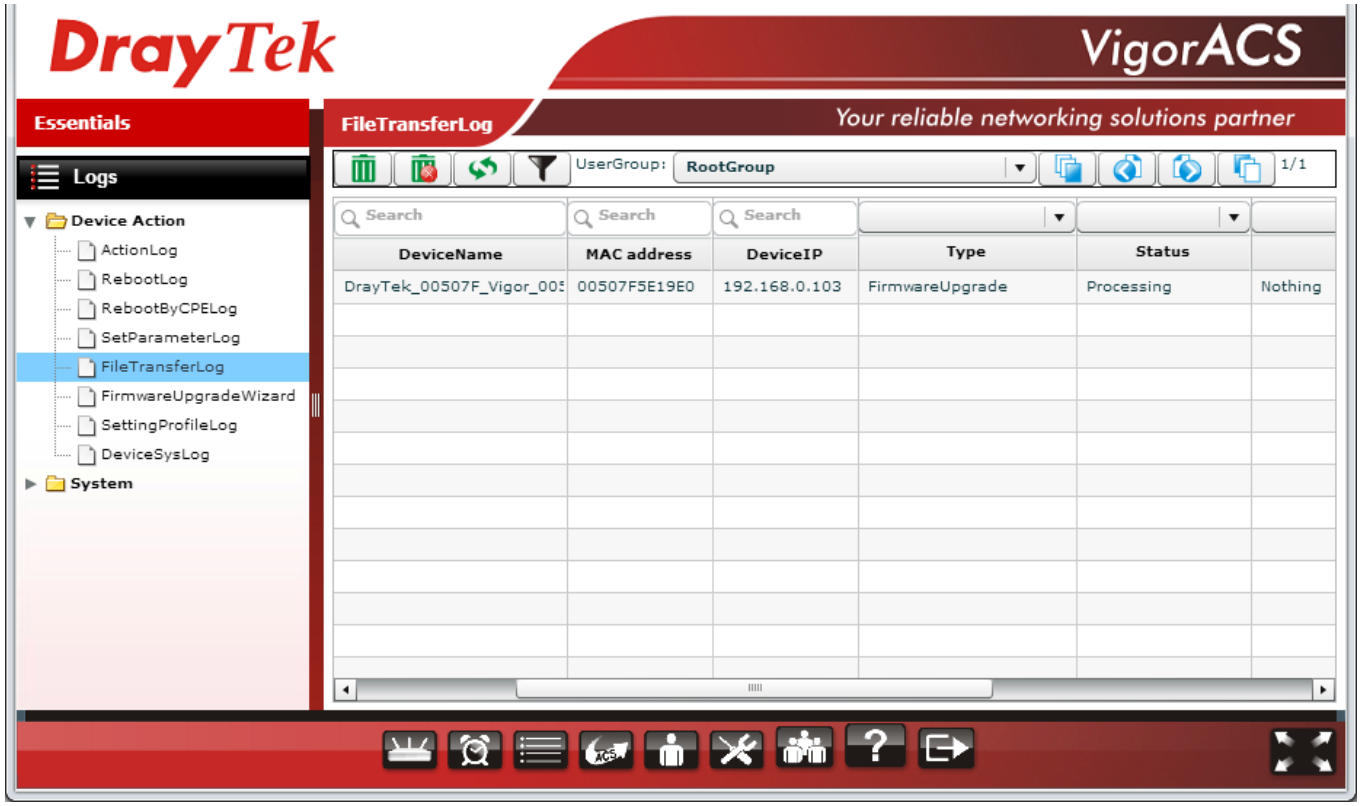

Figura 23 - Firmware sendo processado

Após o término, o CPE envia uma mensagem ao ACS mostrando que o firmware foi atualizado com sucesso. A figura 24, mostra tal evento.

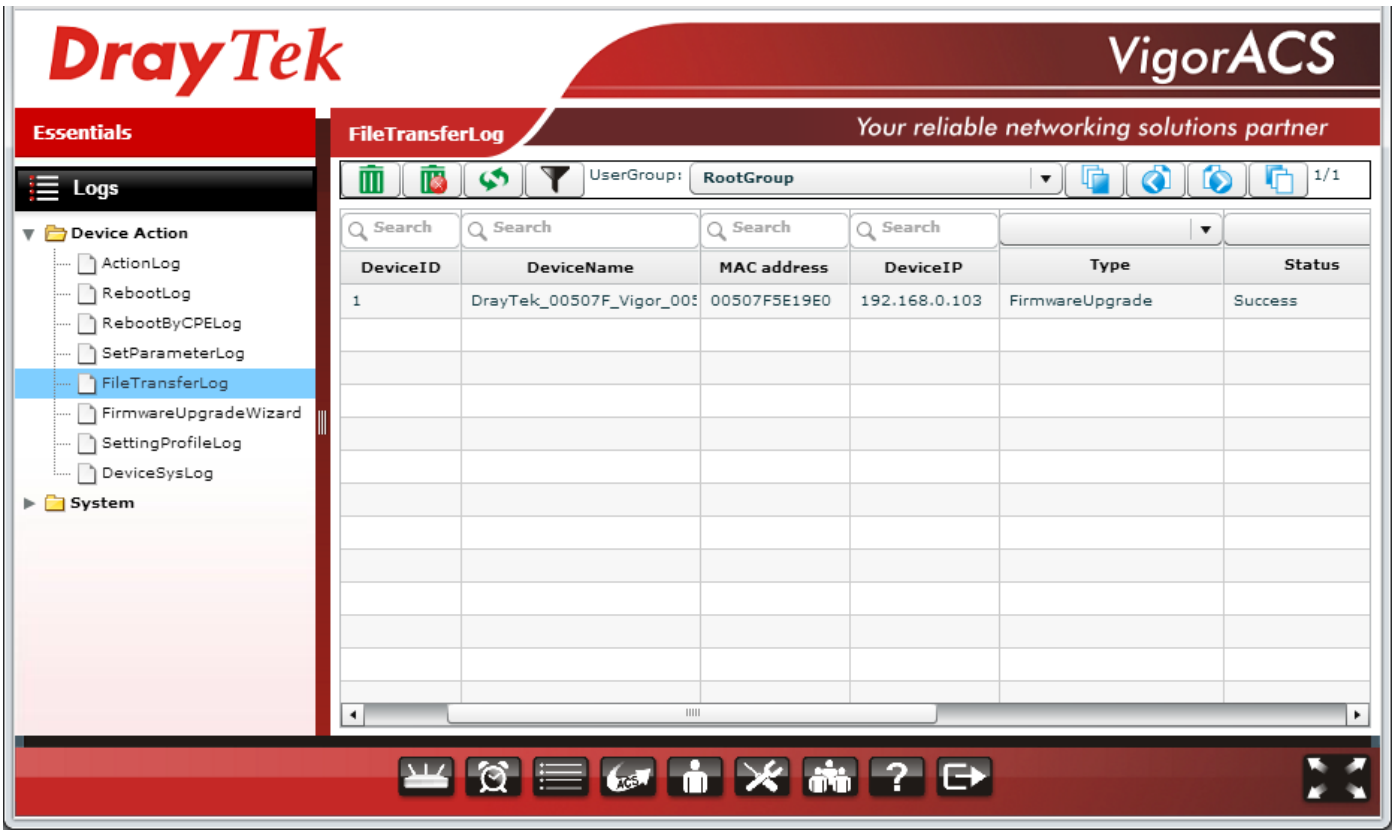

Figura 24 - Atualização de firmware realizada com sucesso

4.5.3.1.3. Configuração de Serviço (SetParameterValues)

A figura 25 mostra uma alteração nas configurações TR-069 do CPE através do ACS, invocando o método *SetParameterValues*, passando por parâmetro todas as informações alteradas.

Nesta mesma figura, observe que no ACS existe uma Rede *Network View* e uma Sub Rede *Teste*. Para que tenha um CPE incluído na Rede *Network View*, é necessário que na configuração TR-069, internamente no CPE, seja colocado o usuário e senha dessa Rede, onde neste caso são *acs* e *password*, respectivamente. Desta forma, ao logar, o CPE será hospedado na rede indicada.

A figura 25, mostra alterando os valores do campos ACS Server:Username e ACS Serve:Password. Nesta figura, mostra o CPE hospedado na Rede *Network View*. A Sub Rede *Teste*, foi criada com usuário *teste* e senha *teste*, assim, alterando para esses valores, fará com que o CPE autentique e seja hospedado na Sub Rede *Teste*. Veja a diferença na hierarquia comparando as figuras 25 e 26, na parte 2, *Networks and Devices.*

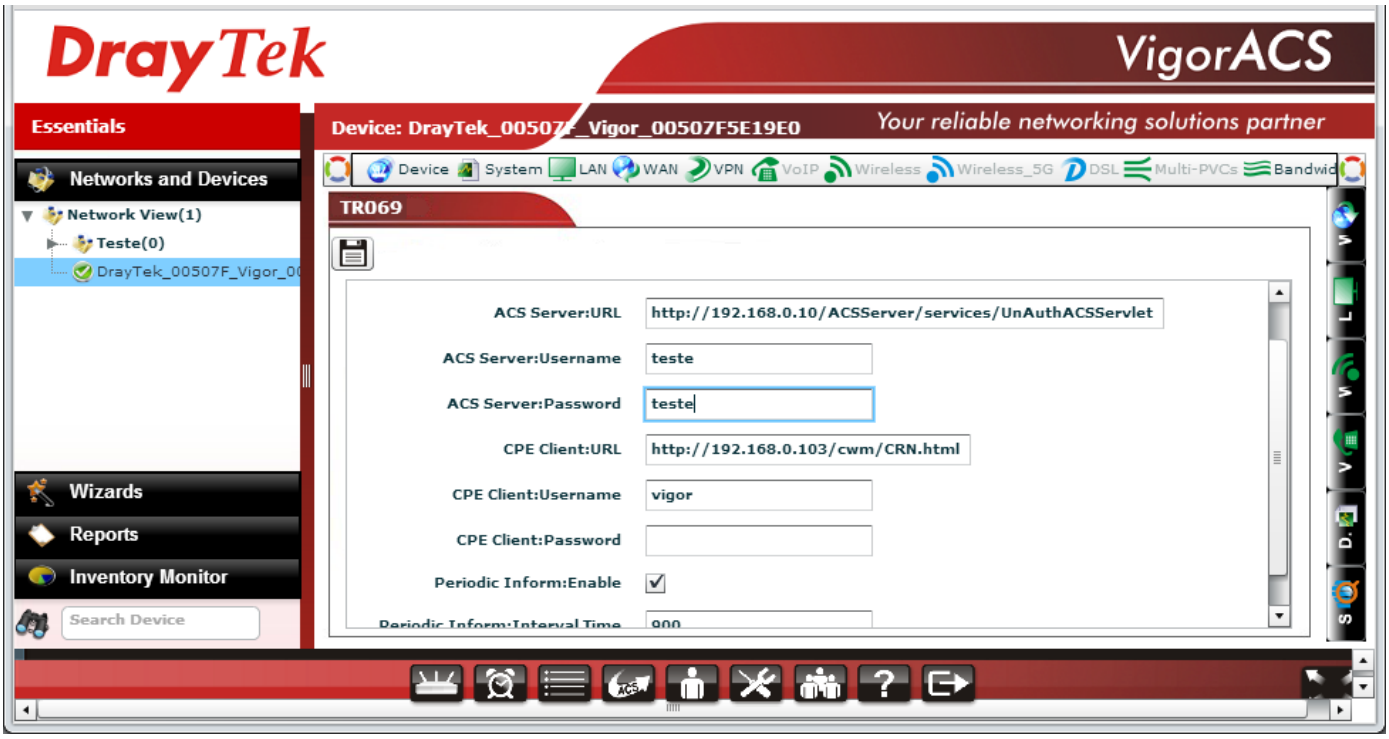

Figura 25 - Alterando configuração de Username e Password no CPE

A figura 26 mostra a validação da alteração realizada através do método *SetParameterValues*. O CPE, após a alteração, é hospedado na Sub Rede *Teste*.

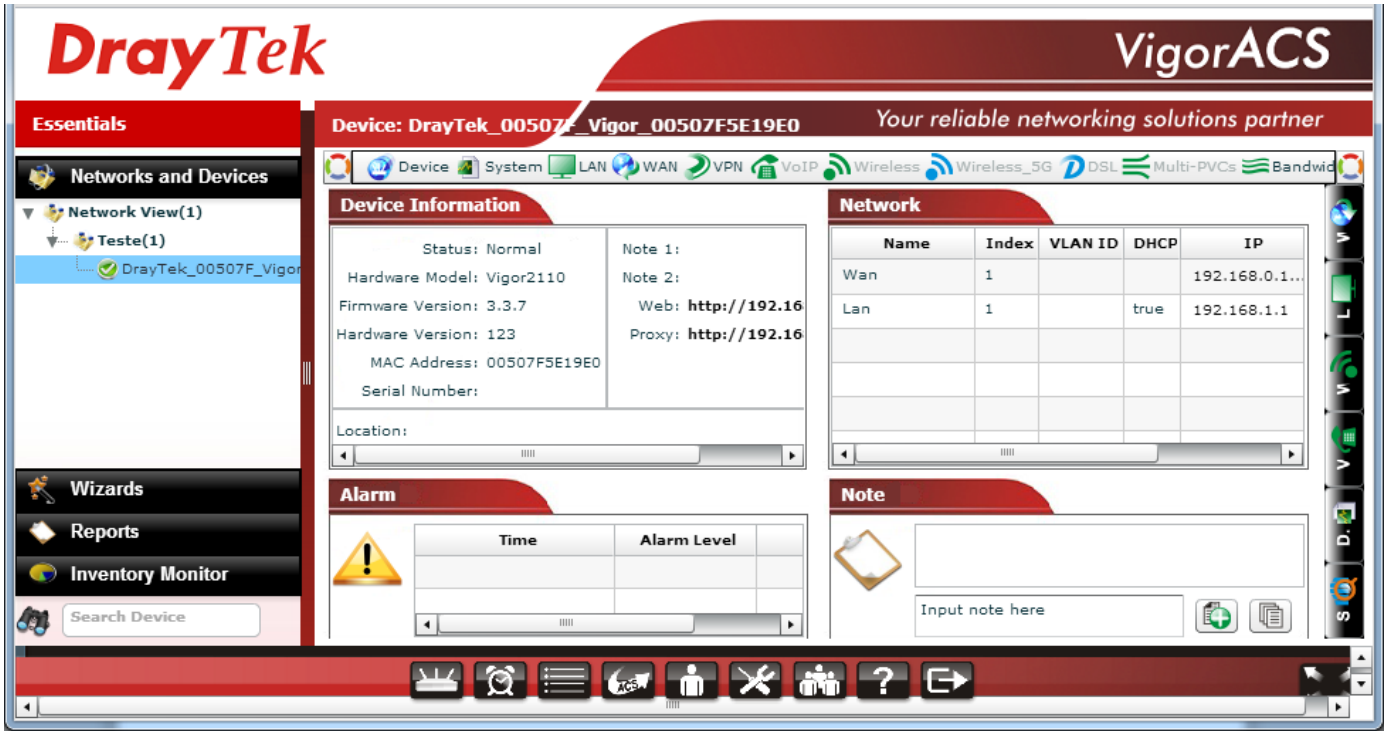

Figura 26 - CPE hospedado na Sub Rede *Teste*

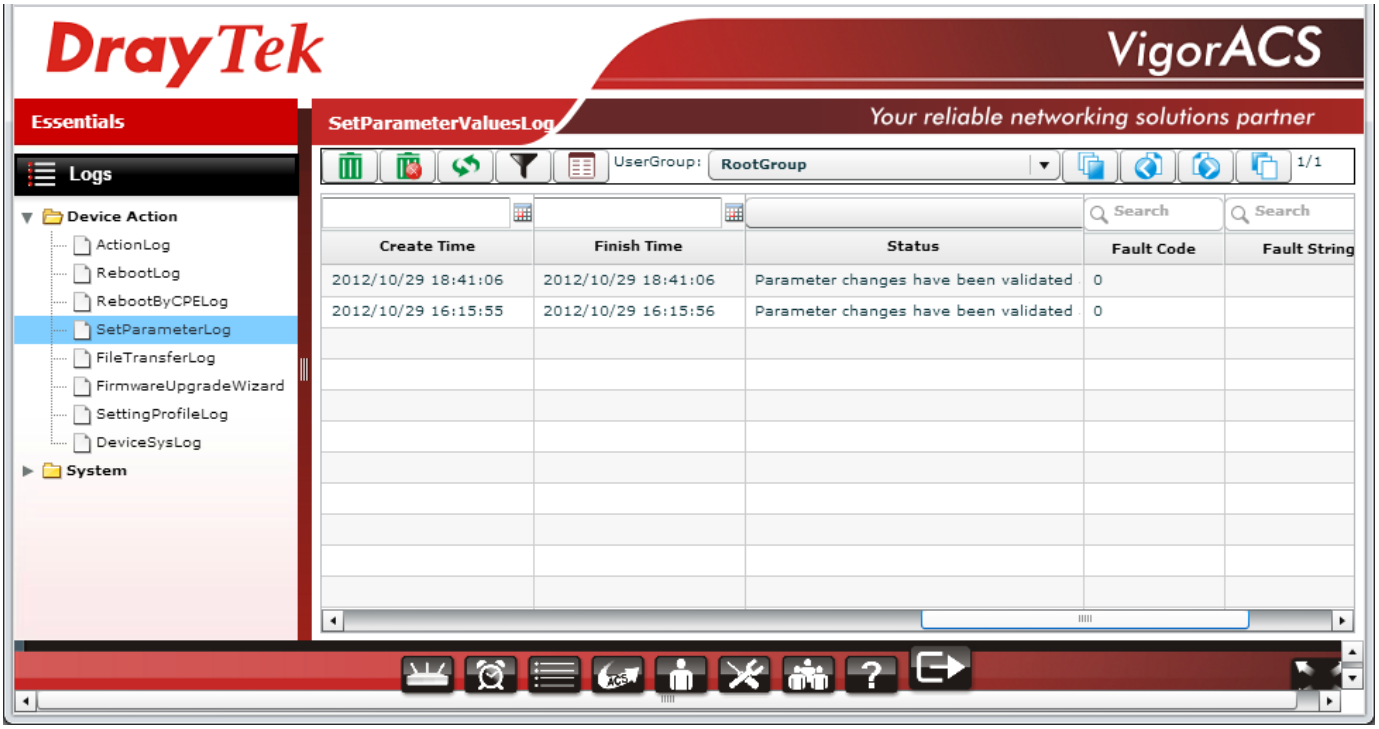

Figura 27 - Logs do método SetParameterValues

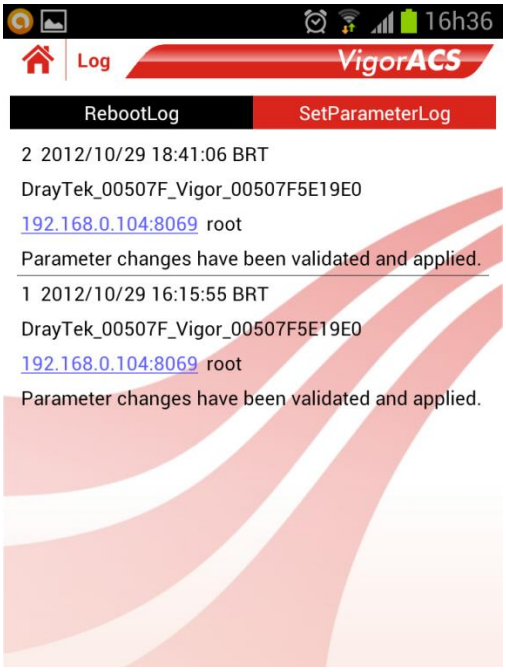

Figura 28 - Logs do método SetParameterValues no aplicativo móvel

4.5.3.1.4. Detecção de falha de energia (*Inform*)

Neste item é forçado o teste de falha de energia ou perda de conexão. A figura 29 mostra que o evento BOOT foi executado e o método *Inform* foi invocado, informando o ACS que houve perda de conexão ou falha de energia:

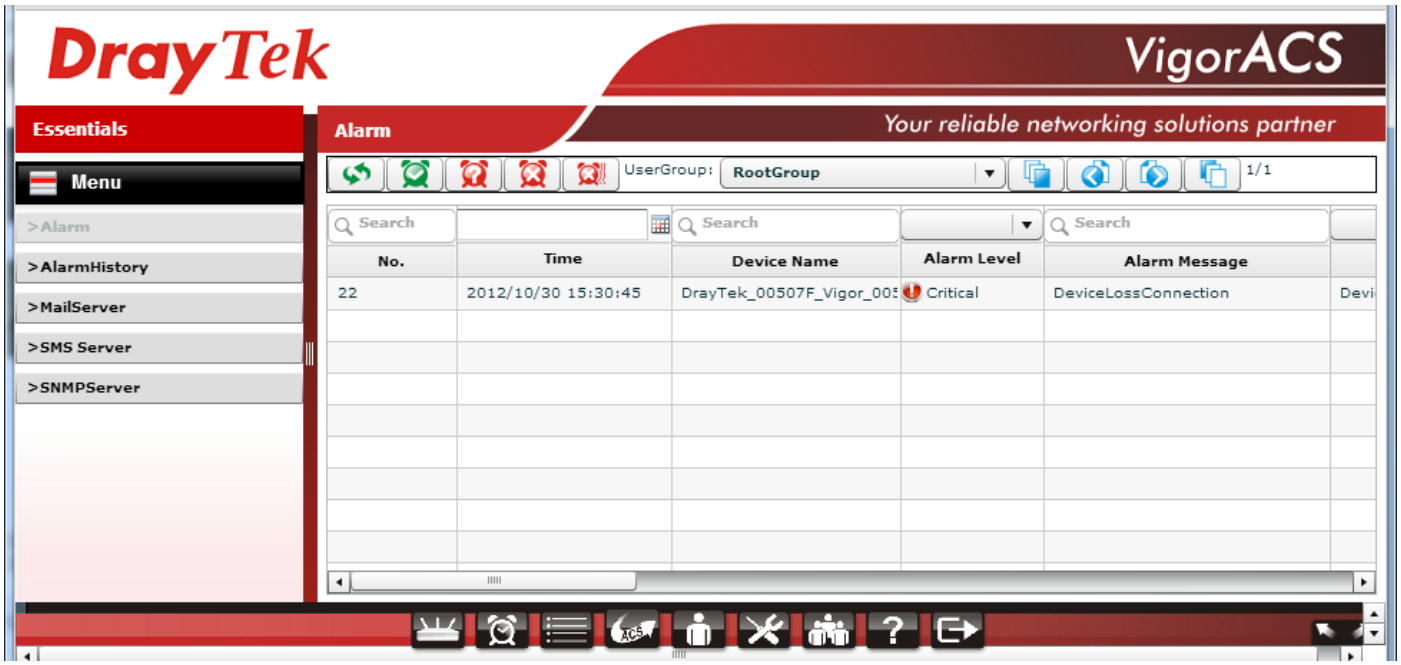

Figura 29 - Método Inform invocado

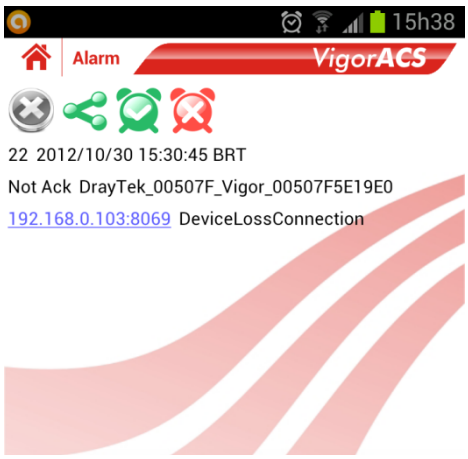

Figura 30 - Teste do método Inform no aplicativo móvel

4.5.3.1.5. Gráficos de Consumo

A figura 31 mostra o consumo Tx (*transfer*) e Rx (*receive*), da CPE selecionada.

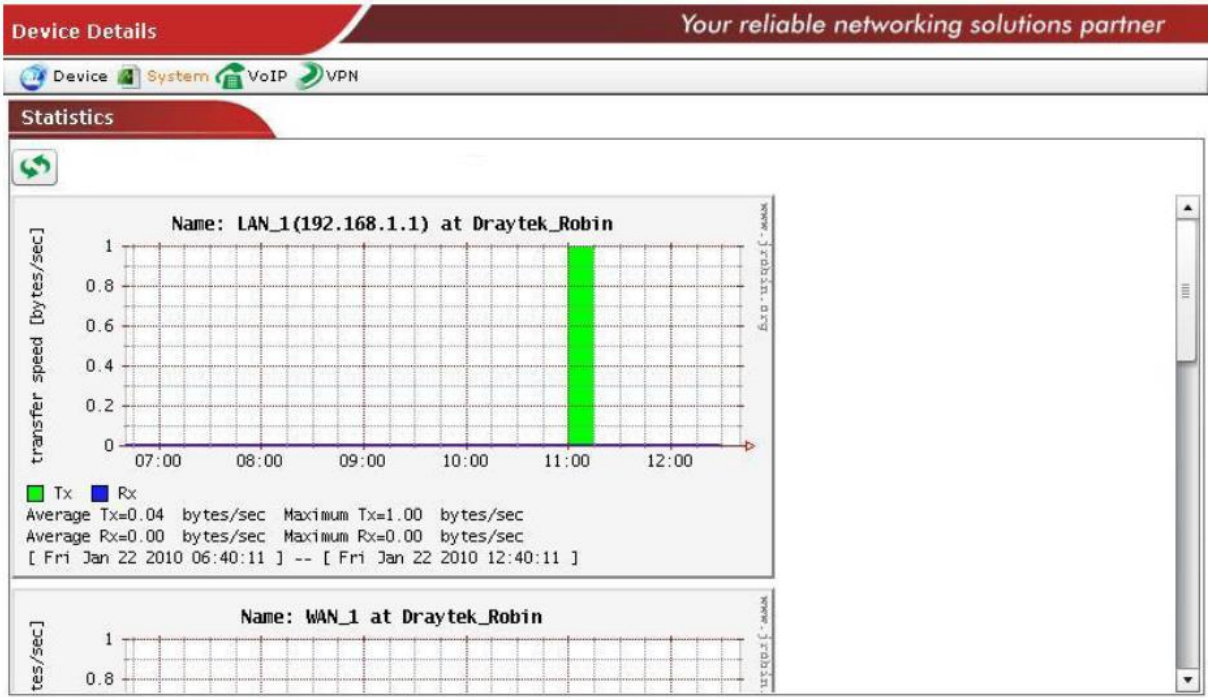

Figura 31 - Gráfico de consumo por CPE (Manual VigorACS SI, 2010)

4.5.3.1.6. Outros resultados – Android

A figura 32, mostra o resultado da localização do CPE através da API do Google Maps. É interessante mostrar localizações, devido ao fato do ACS estar monitorando e gerenciamento milhares de CPE.

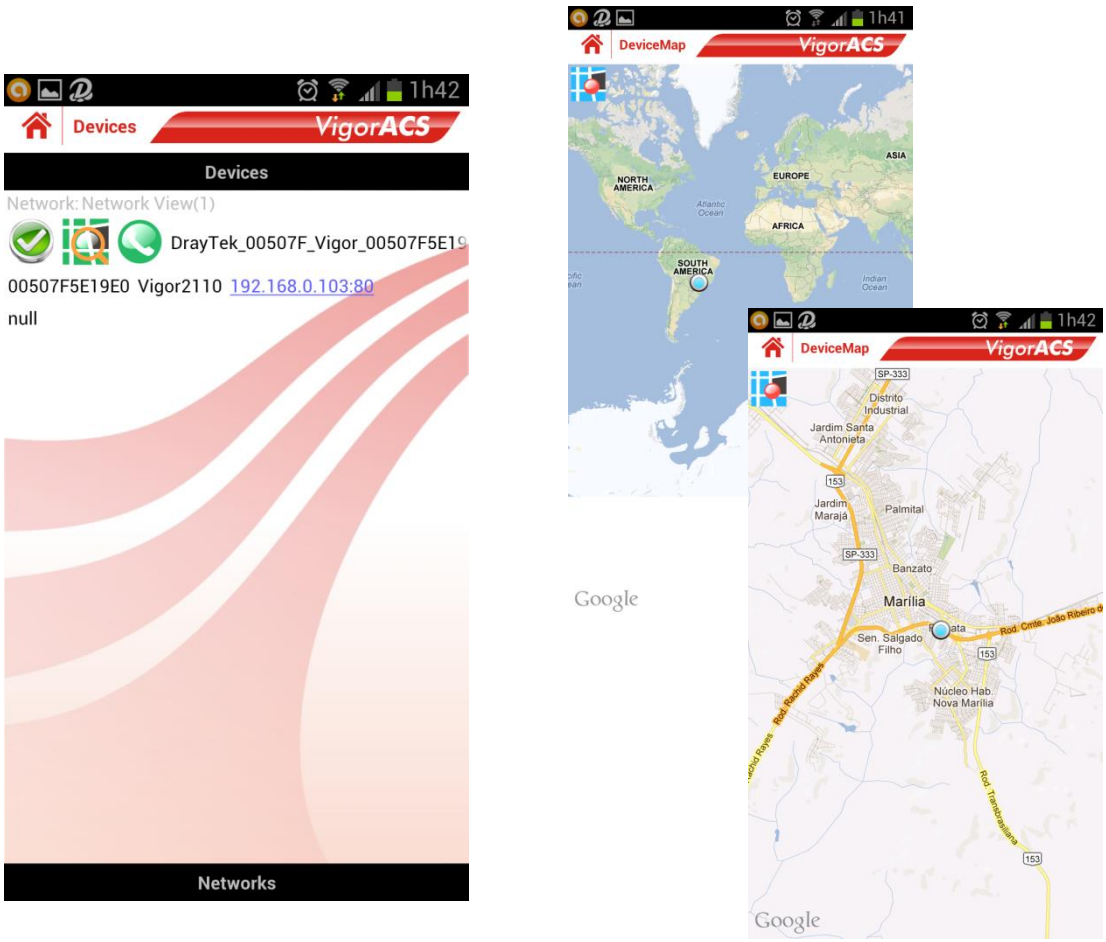

Figura 32 - Testes de localização de CPE

Capítulo 5

5.1. Vantagens

Atualmente, o SNMP, o CLI e o NetConf, no Brasil, são os mecanismos de gerenciamento mais utilizado pelos ISP.

O TR-069 apresenta diversas vantagens sobre esses protocolos, tais como:

- Utiliza TCP como protocolo de transporte ao invés de datagramas UDP usados no SNMP, resultando em maior confiabilidade que é uma característica importante num protocolo de configuração;
- O SNMP trabalha numa troca de informações entre o gestor e a MIB do agente, e o principal problema do SNMP é que as MIBs variam entre fabricantes;
- O CLI é um mecanismo pouco extensível, pois só gerencia os equipamentos para o qual foi desenvolvido, assim causando um grande problema quando se tem vários equipamentos diferentes;
- O TR-069 não utiliza conexões TCP persistentes entre o ACS e o CPE, permitindo que o ACS seja capaz de gerenciar uma alta quantidade de CPE simultaneamente, ao contrário de implementações de NetConf, que necessita manter a conexão de gestão sempre aberta com o equipamento que está gerenciando;
- Comparando ao NetConf, o TR-069 apresenta bastante flexibilidade visto existirem extensões que o colocam compatível com tecnologias modernas tais como o UPnP, conseguindo assim alcançar equipamentos das LAN e equipamentos não TR-069. Em termos de flexibilidade de operacionalidade o TR-069 incorpora um mecanismo que proporciona que tanto o ACS como o CPE seja capaz de iniciar sessões TR-069.
- O TR-069 foi também projetado para promover um elevado nível de segurança e para impedir a manipulação ilícita das operações efetuadas entre um CPE e seu respectivo ACS. (Silva, 2009)
- Fornece ainda confidencialidade para essas operações, e permite vários níveis de autenticação. (Silva, 2009)

5.2. Conclusões e Trabalhos Futuros

A recente convergência dos diversos serviços (voz, dados, TV e wireless) num mesmo canal de acesso (Triple Play ou Quadruple Play) e a grande quantidade de aplicações tem dificultado a gestão, segurança e garantia do QoS nas redes, provocando assim a procura de novas soluções.

Visto que no Brasil, o padrão TR-069 é uma tecnologia pouco difundida, o desenvolvimento deste projeto, abrirá portas para novas soluções.

A realização deste trabalho iniciou uma pesquisa em busca de uma nova forma de gerenciamento de dispositivos CPE para a empresa Interfocus. O TR-069 vem tornar cada vez mais o protocolo padrão na gestão e configuração remota de CPE, permitindo configurar remotamente equipamentos de clientes sem que estes necessitem de conhecimentos técnicos. Permite também a configuração de equipamentos de variadíssimos fabricantes, desde que suportem as normas TR-069 ou TR-064 (protocolo que possibilita interação entre os protocolos UPnP e o padrão TR-069).

É importante ressaltar, que o protocolo CWMP pode ser implementado em ferramentas que possibilitem o uso com outros protocolos, tais como: SNMP, CLI e outros, tornando possível a gerência de equipamentos não só TR-069 numa mesma ferramenta.

Atualmente, muitos fabricantes estão implementando este protocolo nas interfaces de seus equipamentos, abrindo espaço para a criação de ferramentas que gerenciam o CWMP (TR-069).

Dentre esses fabricantes, os que mais aparecem no mercado são: D-Link, Cisco, TP-Link, Huawei, Motorola e Draytek.

Segundo a Draytek, o software VigorACS SI, opera, sem problemas de tráfego, com até cinco mil CPE. Porém, testes com sete mil dispositivos já foram realizados pela empresa e nenhum problema foi constatado.

Por fim, conclui-se que existem muitas vantagens na utilização do CWMP, favorecendo operadores e operandos.

O trabalho gerou publicação no Congresso Nacional de Iniciação Científica de 2012 (Anexo B ao final da monografia), como também, o início para o aperfeiçoamento do desenvolvimento de ferramentas que automatizam a gestão de CPE TR-069.

Com este projeto, novos projetos poderão ser criados e desenvolvidos contribuindo para a ciência e mercado tecnológicos.

Referências Bibliográficas

PAIOSSIN, EDUARDO, HTTP://WWW.PAIOSSIN.COM/WORDPRESS/?P=193 , ACESSADO EM: 27 DE FEVEREIRO DE 2012

BRASIL, *KIOSKEA, TCP/IP,* HTTP://PT.KIOSKEA.NET/CONTENTS/INTERNET/TCPIP.PHP3#GOPREV , ACESSADO EM: 16 DE FEVEREIRO DE 2012

CRUZ, TIAGO, LEITE, THIAGO, *ET. AL.*, "UM IDS COOPERATIVO PARA REDES DE ACESSO DE BANDA LARGA" UNIVERSIDADE DE COIMBRA, 2009

WIKIPÉDIA, *MODELO OSI,* HTTP://PT.WIKIPEDIA.ORG/WIKI/MODELO_OSI, ACESSADO EM: 14 DE ABRIL DE 2012

BROADBAND FORUM (2011), "*CPE WAN MANAGEMENT PROTOCOL V1.3"*, ACESSADO EM: 14 DE ABRIL DE 2012

DELL, *"INTERFACE DE LINHA DE COMANDO CLI"*, HTTP://SUPPORT.DELL.COM/SUPPORT/EDOCS/NETWORK/TMAP1170/BP/MANAGEMENT_INTERFACES/CLI/COMMAND_LINE_INTERFACE_OVERVIEW.HTM, ACESSADO EM: 10 DE AGOSTO DE 2012

CLI IMAGE, *"NET OPTICS*, HTTP://WWW.GOOGLE.COM.BR/IMGRES?HL=PT-BR&SA=X&BIW=1241&BIH=584&TBM=ISCH&PRMD=IMVNS&TBNID=Q5BEOFTWWJWYXM:&IMGREFURL=HTTP://WWW.NETOPTICS.BR.COM/PRODUTOS/LOAD-BALANCING/XBALANCER-BALANCEADOR-DE-CARGA-10G&DOCID=PWSOTNUNJ-H-NM&IMGURL=HTTP://WWW.NETOPTICS.BR.COM/SITES/DEFAULT/FILES/CLI-XBALANCER.GIF&W=400&H=333&EI=DA5HUMZAAQ2M0QGOSID4BQ&ZOOM=1&IACT=HC&VPX=670&VPY=170&DUR=5080&HOVH=206&HOVW=247&TX=123&TY=105&SIG=117375828703073921517&PAGE=2&TBNH=130&TBNW=156&START=21&NDSP=24&VED=1T:429,R:9,S:21,I:171, ACESSADO EM: 05 DE SETEMBRO DE 2012

WIKIPÉDIA, *"XML"*, HTTP://PT.WIKIPEDIA.ORG/WIKI/XML, ACESSADO EM: 10 DE SETEMBRO DE 2012

SILVA, WILSON VIEIRA DA, "*GESTÃO DE HOME NETWORKS",* UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO, VILA REAL, 2009

CASE J. - NETWORK WORKING GROUP (1990), "*RFC 1157 – SIMPLE NETWORK MANAGEMENT PROTOCOL"*

CRAWFORD S. (2002), "*O QUE HÁ DE MELHOR NO UPNP DO WINDOWS XP?",* ACESSADO EM: 05 DE ABRIL DE 2012

ENNS R. - NETWORK WORKING GROUP (2006), "*RFC 4741 – NETWORK CONFIGURATION PROTOCOL"*

BADRA B. - NETWORK WORKING GROUP (2009), "*NETCONF OVER TRANSPORT LAYER SECURITY (TLS)"*

GODDARD T. - NETWORK WORKING GROUP (2006), "*USING THE NETWORK CONFIGURATION PROTOCOL (NETCONF) OVER THE SIMPLE OBJECT ACCESS PROTOCOL (SOAP)"*

GOUVEIA L. (1997), "*COMUNICAÇÃO DE DADOS – NORMAS"*, ACESSADO EM: 08 DE ABRIL DE 2012

WIKIPEDIA, *"BROADBAND FORUM"*, HTTP://EN.WIKIPEDIA.ORG/WIKI/BROADBAND_FORUM, ACESSADO EM: 15 DE AGOSTO DE 2012

IIJIMA T., ATARASHI Y., KIMURA H., KITANI M. - NETWORK WORKING GROUP (2008),
"*EXPERIENCE OF IMPLEMENTING NETCONF OVER SOAP"*

INTEL, *DIGITAL HOME VISION*, HTTP://IMAGES.GOOGLE.PT/IMGRES?IMGURL=HTTP://CACHEWWW.INTEL.COM/CD/00/00/27/29/272984_272984.JPG&IMGREFURL=HTTP://WWW.INTEL.COM/CD/CORPORATE/ICSC/APAC/ENG/TECH_INNOVATION/272771.HTM&USG=__IP3UCTIMVX_SMSZCXV6YEK1-NUU=&H=389&W=500&SZ=147&HL=PT-PT&START=13&TBNID=VLIKZJWPILGJAM:&TBNH=101&TBNW=130&PREV=/IMAGES%3FQ%3DUPNP%26GBV%3D2%26NDSP%3D18%26HL%3DPT-PT%26SA%3DN, ACESSADO EM: 12 DE FEVEREIRO DE 2012

BERNSTEIN J., STARK B. (2005), "*INTERNET GATEWAY DEVICE VERSION 1.1 DATA MODEL FOR TR-069*"

BROADBAND FORUM, *MODELO DE DADOS PARA EQUIPAMENTOS TR-069 (TR-106)*, HTTP://WWW.BROADBANDFORUM.ORG/TECHNICAL/RELEASEPROGRAM.PHP, ACESSADO EM: 12 DE FEVEREIRO DE 2012

BROADBAND FORUM, *MODELO DE DADOS PARA CPE VOIP (TR-104*), HTTP://WWW.BROADBAND-FORUM.ORG/TECHNICAL/RELEASEPROGRAM.PHP, ACESSADO EM: 13 DE FEVEREIRO DE 2012

KIRKSEY H. (2005), "*STANDARDS-BASED DEVICE MANAGEMENT*"

LEAR E. - NETWORK WORKING GROUP (2006), "*USING THE NETCONF PROTOCOL OVER THE BLOCKS EXTENSIBLE EXCHANGE PROTOCOL (BEEP) – RFC 4744*"

DRAYTEK BRASIL, *"SOBRE A DRAYTEK"*, HTTP://WWW.IK1.COM.BR/DYNAMICS/DRAYTEK/, ACESSADO EM: 26 DE OUTUBRO DE 2012

IK1, *"SOBRE A IK1"*, HTTP://WWW.IK1.COM.BR/DYNAMICS/DRAYTEK/, ACESSADO EM: 26 DE OUTUBRO DE 2012

NETCONF CENTRAL (2008), *OPERAÇÕES NETCONF*, HTTP://WWW.NETCONFCENTRAL.ORG/RPCLIST, ACESSADO EM: 20 DE AGOSTO DE 2012

VISUS, *"VIGORACS SI",* HTTP://WWW.VISUS.PT/DRAYTEK/VIGOR_ACS-SI.HTM, ACESSADO EM: 12 DE OUTUBRO DE 2012

IK1 TECNOLOGIA LTDA., *"MANUAL VIGORACS SI",* (2010)

ROSE M. - NETWORK WORKING GROUP (2001), "*THE BLOCKS EXTENSIBLE EXCHANGE PROTOCOL CORE – RFC 3080"*

ROYON Y., PARREND P., FRÉNOT S., PAPASTEFANOS S., ABDELNUR H., POEL D. (2007), "*MULTI-SERVICE, MULTI-PROTOCOL MANAGEMENT FOR RESIDENTIAL GATEWAYS"*

STARK B.- BROADBAND FORUM (2004), "*LAN-SIDE DSL CPE CONFIGURATION"*, ACESSADO EM: 22 DE OUTUBRO DE 2012

UPNP FORUM, HTTP://WWW.UPNP-IC.ORG/HOME, ACESSADO EM: 20 DE SETEMBRO DE 2012

UPNP FORUM (2008), "*UPNP DEVICE ARCHITECTURE 1.0*", ACESSADO EM: 20 DE SETEMBRO DE 2012

UPNP FORUM (2006), "*UPNP FORUM RELEASES ENHANCED AV SPECIFICATIONS TAKING HOME NETWORK TO THE NEXT LEVEL*", ACESSADO EM: 22 DE SETEMBRO DE 2012

UPNP STANDARDS, HTTP://WWW.UPNP.ORG/STANDARDIZEDDCPS/DEFAULT.ASP, ACESSADO EM: 22 DE SETEMBRO DE 2012

WASSERMAN M., THINGMAGIC, GODDARD T. - NETWORK WORKING GROUP (2006), "*USING THE NETCONF CONFIGURATION PROTOCOL OVER SECURE SHELL (SSH)"*

WIKIMEDIA COMMONS (2006), "*SNMP-MANAGEMENTKONSOLE.PNG*", HTTP://COMMONS.WIKIMEDIA.ORG/WIKI/FILE:SNMP-MANAGEMENTKONSOLE.PNG, ACESSADO EM: 23 DE SETEMBRO DE 2012

WIKIPEDIA, *COMMAND LINE INTERFACE*, HTTP://EN.WIKIPEDIA.ORG/WIKI/COMMAND-LINE_INTERFACE, ACESSADO EM: 25 DE SETEMBRO DE 2012

WIKIPÉDIA, *GERÊNCIA DE REDES*, HTTP://PT.WIKIPEDIA.ORG/WIKI/GER%C3%AANCIA_DE_REDES, ACESSADO EM: 27 DE SETEMBRO DE 2012

W3SCHOOLS, *SCHEMA TUTORIAL*, HTTP://WWW.W3SCHOOLS.COM/SCHEMA/DEFAULT.ASP, ACESSADO EM: 27 DE SETEMBRO DE 2012

W3SCHOOLS, *TCP/IP TUTORIAL*, HTTP://WWW.W3SCHOOLS.COM/TCPIP/DEFAULT.ASP, ACESSADO EM: 27 DE SETEMBRO DE 2012

W3SCHOOLS, *WEB SERVICES TUTORIAL*, HTTP://WWW.W3SCHOOLS.COM/WEBSERVICES/DEFAULT.ASP, ACESSADO EM: 05 DE OUTUBRO DE 2012

DRAYTEK, *AUTO CONFIGURATION SERVER SI – USER GUIDE*, 2010, VERSÃO 1.1

W3C SOAP SPECIFICATIONS, 2007, HTTP://WWW.W3.ORG/TR/SOAP/, ACESSADO EM: 07 DE NOVEMBRO DE 2012

WIKIPEDIA, *SOAP*, HTTP://PT.WIKIPEDIA.ORG/WIKI/SOAP, ACESSADO EM: 07 DE NOVEMBRO DE 2012

CRAIG HUNT.; *TCP/IP NETWORK ADMINISTRATION*; O'REILLY, 1998

WIKIPEDIA, *WEB SERVICES*, HTTP://PT.WIKIPEDIA.ORG/WIKI/WEB_SERVICE, ACESSADO EM: 15 DE NOVEMBRO DE 2012

ANEXO A

iK1 Tecnologia Ltda.

Autorização de uso das marcas IK1 e DrayTek

IK1 Tecnologia Ltda, empresa brasileira, com sede na Praça Dom José Gaspar, 134, 6.andar, Conj.64, Centro, São Paulo/SP, representante exclusiva da marca DrayTek Corp. no Brasil, autoriza o Sr. Ivan Daun Sakai, a utilização das marcas IK1 Tecnologia Ltda e DrayTek Corp. no Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2012.

São Paulo, 14 de novembro de 2012.

IK1 Tecnologia Ltda
Mauro Sgarbi dos Santos
Sócio-Administrador

iK1 Tecnologia Ltda.
Praça Dom José Gaspar, 134 • Conj. 64 • Centro • Cep. 01047-010 • São Paulo • SP
C.N.P.J. 07.055.616/0001-09 • Inscr. Estadual 116.950.254.112 • Inscr. Municipal 3.358.076-6
Tel/Fax: (11) 4062-3300 • e-mail: ik1@ik1.com.br

ANEXO B

12º Congresso Nacional de Iniciação Científica

CONIC-SEMESP

Inscrições Online

Status da Inscrição

Parabéns **Ivan Daun Sakai**,

Seu trabalho foi **aprovado** e está selecionado para concorrer no **12o CONIC-SEMESP**.

Seu trabalho intitulado **Automatização de Gerência, Monitoramento e Provisionamento de CPEs - TR-069** irá concorrer na área de conhecimento **ENGENHARIAS E TECNOLOGIAS**, sub-área **Computação e Informática**, na categoria **Trabalho Em Andamento**.

Você optou por apresentar seu trabalho em **Sala**, com apoio de **Microcomputador com projetor**.

Consulte o gradeamento do evento a partir de **19/10/2012** para saber o local e horário da sua apresentação.

O **Semesp** agradece sua inscrição e lhe deseja boa sorte.

Em caso de dúvida encaminhe um e-mail para conic@semesp.org.br.

| **retornar para a página do SEMESP** | **fazer outra inscrição** | **consultar status de inscrição já feita** |

SEMESP

Sindicato das Entidades Mantenedoras de Estabelecimentos de Ensino Superior no Estado de São Paulo

©2012 DirectWeb Tecnologia