TR-069, UMA SOLUÇÃO FLEXÍVEL PARA GERENCIAMENTO DE CPE

Lucas Miranda Gaspar[1]
Luiz Claudio Theodoro[2]

Resumo

Os avanços tecnológicos fizeram com que se reduzissem as distâncias, um exemplo claro, é a *Internet*. Esta evolução das comunicações gerou uma grande demanda de *links* de acesso à rede mundial de computadores (*Internet*), tanto acessos xDSL (*Digital Subscriber Line* – Linha Digital de Assinantes), os quais são assíncronos, ou seja, tem uma velocidade de solicitação *(upload)*, diferente da velocidade de resposta *(download)*, tomando como referência o ambiente do cliente, quanto acessos dedicados de *Internet Links* e VPNs (*Virtual Private Networks* – Redes Privadas Virtuais), cujas velocidades são síncronas, possuem a mesma velocidade de *download* e *upload*. O crescente número de equipamentos na rede, fez surgir a necessidade de ferramentas de gerenciamento capazes de suportar tamanha demanda. Com isso, surgiu o TR-069, desenvolvido pelo *BroadBand Forum*, com a missão de efetuar um gerenciamento completo da estrutura de rede das operadoras, abrangendo, por exemplo, aprovisionamento (reserva) de recursos para ativação de novos clientes, diagnósticos da rede, controle da versão de sistema operacional dos equipamentos *(firmware)*. No entanto, para realizar esta tarefa, é necessário que este tenha flexibilidade para incorporar todos equipamentos e tecnologias atuantes no mercado atual. Objetivando demonstrar estas situações, foi elaborado este artigo descrevendo algumas configurações e equipamentos que devem ser gerenciados juntamente com detalhes do protocolo.

Palavras-chave: CPE; *Scripts;* TR-069.

1. Introdução

[1] Aluno do Curso de Especialização em Engenharia de Telecomunicações e Redes de Computadores. Graduado no Curso Superior de Tecnologia em Redes de Computadores. Atua profissionalmente como técnico de comunicação de dados. E-mail: lucasmirandagp@hotmail.com.

[2] Professor Mestre em Engenharia Elétrica, Coordenador do Curso de Especialização em Engenharia de Telecomunicações e Redes de Computadores, Líder de Open Inovation da Algar Telecom, Professor do Curso de Engenharia Elétrica da UFU – Universidade Federal de Uberlândia. E-mail: lcaudio@feelt.ufu.br

A *Internet* possibilitou a redução de distâncias, o compartilhamento de informações, o tráfego de voz e vídeo. Além disso, com o desenvolvimento desta, novos recursos foram acoplados, como as aplicações em nuvem por exemplo. As aplicações na nuvem são programas armazenados em servidores que podem ser acessados de qualquer lugar em que se tenha acesso à *Internet.*

Diante de tamanho desenvolvimento, expandiu-se a procura por um acesso a mesma, seja por meio de cabos metálicos, fibras ópticas ou mesmo por sistemas sem fios, como o 3G por exemplo.

O aumento na utilização da *Internet* tanto em ambientes comerciais quanto residências fez com que os prestadores destes serviços desenvolvessem métodos e tecnologias para agilizar o processo de entrega e manutenção dos serviços. Some-se a isso, o fato de termos o gerenciamento de “tudo” que está conectado à sua rede.

Quando se fala em gerenciamento, cada vez se pensa na automação deste processo, uma vez que considerando-se a quantidade de pontos de acesso existentes, percebe-se a dificuldade de um ser humano dar suporte a tudo. Com isso, cria-se ferramentas que segue instruções baseada nas mais diversas possibilidades de situações já vivenciadas pelos técnicos que gerenciam este “universo”.

Um modelo de ferramentas que ajuda a resolver estes problemas foi desenvolvido pelo BroadBand Forumm, denominado de TR-069 será apresentado neste artigo. Ele foi planejado inicialmente para gerenciamento e autoconfiguração de dispositivos de acesso DSL (*Digital Subscriber Line* – Linha de Assinantes Digital), que é o acesso à *Internet* por meio dos pares metálicos já existentes das linhas telefônicas.

Além da ferramenta supracitada, serão apresentados os detalhes que devem estar bem desenvolvidos neste tipo de instrumento, tais como a parte física, levando em conta a capacidade de memória, do processador, a quantidade e quais tipos de interfaces suporta e a parte lógica, que vem a ser os *scripts* de configurações.

Diante disto, serão apresentados os CPEs (*Customer Premises Equipment* – que é o equipamento do ambiente do cliente), as interfaces que podem ser utilizadas para fornecer funcionalidades específicas ou simplesmente para ampliar recursos, assim como, os *scripts* de configurações que fazem com que todo esse conjunto de “peças” trabalhe como desejado.

2. Equipamentos

2.1. CPEs

O NAP *(Network Access Provider* – Provedor de Acesso à Rede*)* é responsável por fornecer um meio de conexão à rede, seja por par metálico, cabo coaxial, fibra ou wireless (conexão sem fio). Como exemplo, se pode citar meios fornecidos por empresas como CTBC, OI, GVT, etc. O NSP *(Network Service Provider* – Provedor de Serviços de Rede*)* é quem fornece serviços aos consumidores, como o acesso à Internet como exemplo. Dentre estes prestadores de serviços podemos citar; *Netsite, Uol, Terra,* etc.

A sigla CPE é o equipamento que fica no ambiente do cliente interligando-o à infraestrutura de rede do NAP na terminação de um serviço prestado pelo NSP, Vyncke e Hogg (2009).

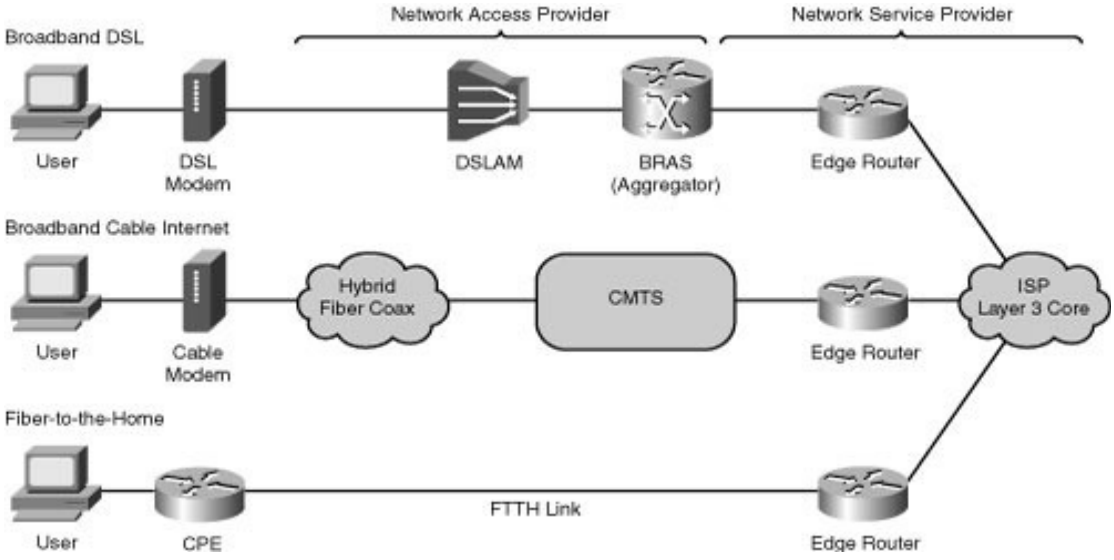


Imagem 1: Topologia de provedor de acesso à banda larga

Fonte: Vyncke e Hogg (2009).

A imagem acima apresenta alguns métodos pelos quais são possibilitadas as conexões entre CPEs (clientes) e os provedores (PEs). Quando se trata dos DSL modens, utilizam-se os pares metálicos como meio de interconexão dos equipamentos. Os *cable modens* são utilizados num meio híbrido, que consiste de um cabo com fibra e coaxial juntos. O FTTH é um link de fibra óptica que interconecta o PE ao CPE, tendo a

necessidade ou não de um conversor óptico/*ethernet* em cada ponta, dependendo do modelos dos equipamentos.

Os equipamentos podem ser dos mais diversos, em funcionalidades e capacidades, bem como de fabricantes. De acordo com a BIZI, empresa americana que comercializa equipamentos de rede, os fabricantes mais populares são: *3Com, Alcatel, Arista Networks, Cisco Systems, Enterasys / Cabletron, Extreme Networks, Foundry Networks, H3C, Juniper Networks, LG-Ericsson, Marconi / Fore Systems, Nortel Networks.*

Dentre os fabricantes supracitados, *Cisco e 3Com*, que foi adquirida pela HP, são os mais utilizados como CPEs. Vale destacar também a utilização de equipamentos da *Digitel* neste segmento, conforme análise da estrutura de uma operadora de telecom.

Ainda segundo esta análise, observou-se que os modelos mais utilizados são: *3Com* A-*MSR2011, 3Com 5012, Cisco 1841, Digitel NR-2G 3211 e NR-2G 3238*. Também foi incorporado à planta o *HP MSR20-40 Router* em substituição ao modelo *3Com 5012.*

A utilização de cada modelo está diretamente ligada ao produto final do cliente, oferecendo-lhe a melhor relação custo/benefício.

O roteador A-*MSR2011* que possui um processador *RISC* capaz de trabalhar a 333 MHz vem com 256 MB de memória SDRAM DDR, 32 MB de memória flash. Este por sua vez pode ser utilizado para entrega de *Internet links*, *VPNs*, circuitos *VOIP* sobre *IAD (Integrated Access Devices* – dispositivos de acesso integrado*).*

O *Cisco 1841* é um roteador dotado de duas interfaces fast ethernet e dois *slots* de expansão para *HWIC, WIC, VWIC* (interfaces de dados), memória *FLASH* de 32MB expansível até 128MB, memória *DRAM* de 128MB expansível até 384MB (em dois *Slots*). Este pode ser utilizado nos mesmos serviços providos pelo A-*MSR2011*.

O modelo *3Com 5012* cuja memória *SDRAM* é de 128MB e a *FLASH* de 32MB, vem com uma interface *WAN* e uma *ethernet* e três *slots* de expansão, sendo dois *SICs* e um *MIM*. Através do *slot MIM* é possível oferecer ao cliente um link de voz sobre *IP (VOIP)* com *IP* compartilhado ou não compartilhado, além dos serviços supracitados.

Quando se fala em IP compartilhado, diz-se da possibilidade de dividir recursos de banda do *Internet link*, por exemplo, para passar o tráfego de voz. No *IP* não

compartilhado, ocorre a implantação de um link com dedicação exclusiva ao tráfego de voz sobre *IP.*

O roteador *HP MSR20-40* é capaz de suportar todos os serviços dos modelos supracitados. Para suportar estes serviços, ele conta com 4 *slots* de expansão SIC e 2 portas WAN 10/100 com conector RJ-45. Além disso, dispõe de um processador *RISC* a 400 MHz, 256 MB de *compact flash* e 256 MB de *SDRAM*.

Os equipamentos da *Digitel*, modelos *NR-2G 3211 e NR-2G 3238*, podem ser utilizados para oferecer os mesmos serviços que *3COM A-MSR20-11*, no entanto limitado à clientes com *links* de velocidade até 4Mb. O 3211 possui 16MB de memória *FLASH* e 32MB de *RAM*. Devido ao fato de ter apenas duas interfaces, sendo uma *LAN* e uma *WAN*, ele não pode ser utilizado na rede *Metroethernet.* Já o 3238, vem com duas interfaces *WAN* e duas portas *LAN*, o que viabiliza seu uso numa rede *Metroethernet.*

As informações supracitadas, referentes às especificações dos equipamentos empregados como *CPEs* foram obtidas diretamente do *site* dos fabricantes. Os dados de uso por serviço foram baseados na análise estrutural desta operadora.

2.2. Interfaces

Os roteadores modulares, ou seja, aqueles nos quais se podem acrescentar módulos (placas) de expansão, podem suportar diversos tipos de interfaces. As interfaces seriais, por exemplo, são muito utilizadas para atender os clientes cujas velocidades não ultrapassem 2Mbps, segundo estudo de caso.

Nestes casos para que tal situação seja possível, o circuito deve estar aprovisionado em uma rede TDM (*Time Division Multiplexing*, ou Multiplexação por Divisão de Tempo) utilizando por inteiro um E1, que é um canal de 2Mbps de uma rede PDH (*Plesiochronous Digital Hierarchy* ou Hierarquia Digital Plesiócrona), ou parte deste, o chamado estruturado.

Esse tipo de aprovisionamento requer a utilização de um meio de conversão de G703 – interface padrão de recomendação ITU-T – para interface V35, que também é recomendado pelo mesmo, viabilizando assim a comunicação dos roteadores.

O cabo serial utilizado para conectar o roteador ao conversor ou ao gabinete é apresentado nas figuras abaixo.

Imagem 1 – Cabo serial
Fonte: Google.

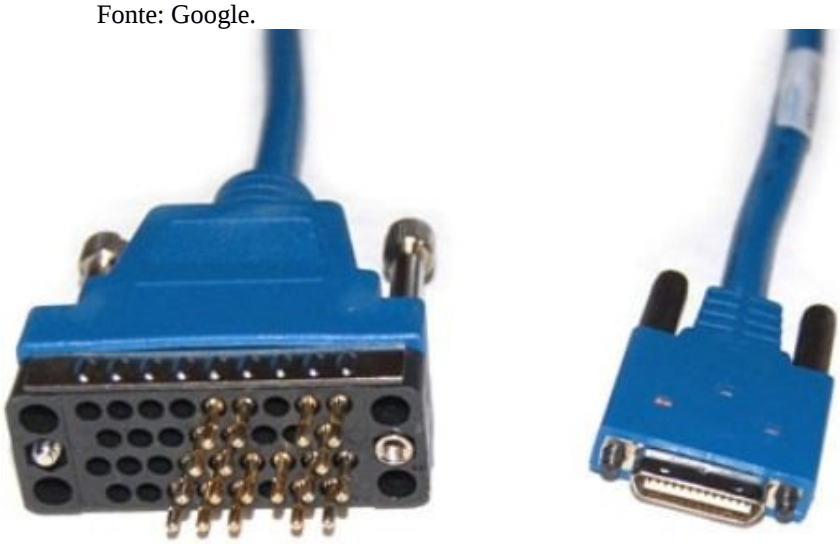


Imagem 2 – Cabo serial
Fonte: Google.

A imagem 1 apresenta o cabo necessário para conectar o roteador à V35 mediante uso do módulo WIC-1T, cuja velocidade máxima atingida é de 2Mbps. Enquanto isso, a imagem 2 mostra o cabo adequado para a interface HWIC-1T, na qual o tráfego máximo é de 8Mbps.

Imagem 3 – Interface WIC-1T
Fonte: Google.

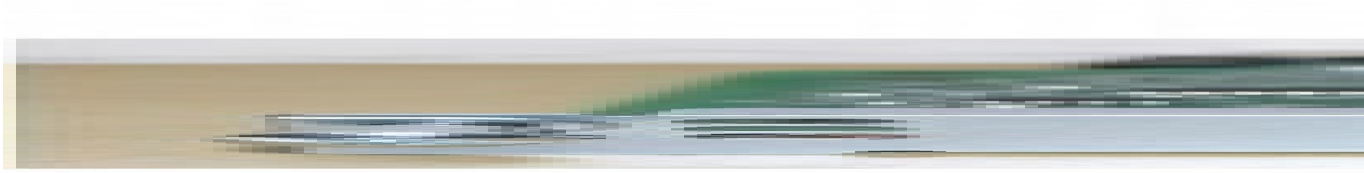


Imagem 4 – Interface HWIC-1T
Fonte: Google.

Existem ainda, módulos específicos para o tráfego de voz, as interfaces E1s. Estas fazem a conversão de uma sinalização R2 ou ISDN do PABX para pacotes IP.

Assim como nos CPEs, os dados técnicos das interfaces, foram retirados dos sites dos fabricantes, bem como as informações de utilização.

3. *Scripts* de Configuração

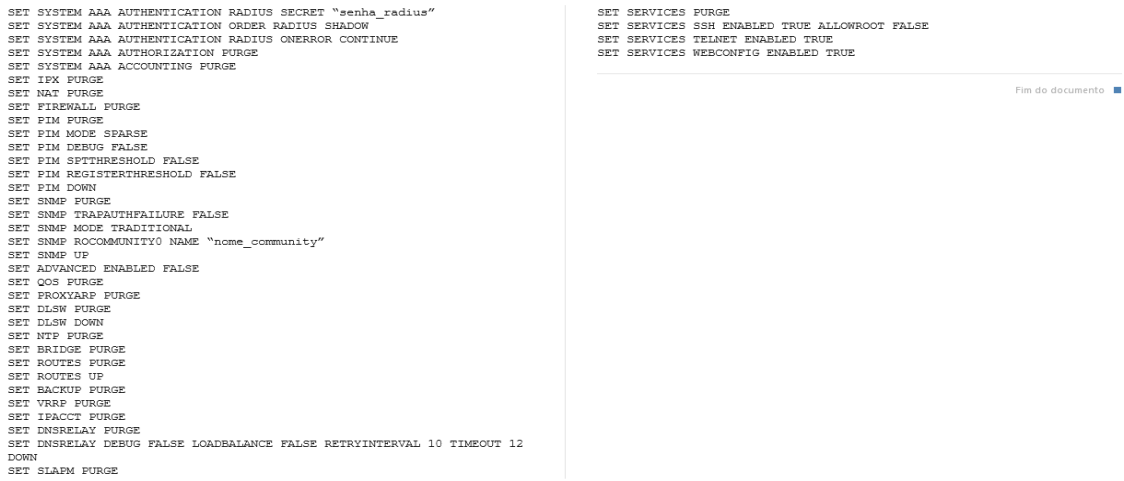
Os *scripts* de configuração são arquivos de texto que contêm as configurações dos roteadores. A vantagem de se utilizar *scripts* está na agilidade e padronização das configurações a serem aplicadas. Eles podem ser editados com um editor de textos comum, tal como bloco de notas do Windows (notepad), o *Microsoft office word*, *notepad++*, Gedit, Vi, entre outros tantos disponíveis no mercado.

As imagens abaixo (5 e 6) apresentam um exemplo de configuração do roteador Digitel 3211.

```
SET LAN LAN0 PURGE
SET LAN LAN0 MODE AUTO
SET LAN LAN0 IP "xxx.xxx.xxx.xxx" MASK "xxx.xxx.xxx.xxx" BROADCAST
"xxx.xxx.xxx.xxx"
SET LAN LAN0 COMMENT [Rede Interna do Cliente]
SET LAN LAN0 TUN6TO4 NO
SET LAN LAN0 UP
SET LOOPBACK PURGE
SET WAN WAN0 PURGE
SET WAN WAN0 PROTO PPPS DEBUG FALSE VJ FALSE
SET WAN WAN0 COMMENT [conexão com provedor]
SET WAN WAN0 MTU 1520 MRU 1520 HOLDOFF 15 PPPDEFROUTE TRUE AUTH NONE
SET WAN WAN0 IPCP ENABLED TRUE
SET WAN WAN0 IPCP MAXCONFIGURE 10 MAXFAILURE 10 MAXTERMINATE 3 RESTART
3
SET WAN WAN0 IPCP LOCALIP ENABLED TRUE ADDRESS "xxx.xxx.xxx.xxx" MASK
255.255.255.252
SET WAN WAN0 IPCP REMOTEIP ENABLED TRUE ADDRESS "xxx.xxx.xxx.xxx"
SET WAN WAN0 LCP ECHOFAILURE 7 ECHOINTERVAL 3 MAXCONFIGURE 10 MAXFAI-
LURE 10 MAXTERMINATE 3 RESTART 3
SET WAN WAN0 CLOCK EXTERNAL TXINV FALSE UP
SET L2TP PURGE
SET PPPOE PURGE
SET IPSEC PURGE
SET GRE PURGE
SET PPTP PURGE
SET RIP PURGE
SET RIP REDIST-STATIC TRUE REDIST-CONNECTED TRUE REDIST-OSPF FALSE DE-
FAULTMETRIC 1 VERSION 2
SET RIP LAN0 ENABLED TRUE TYPE ACTIVE
SET RIP LAN0 AUTH TYPE NONE
SET RIP WAN0 ENABLED TRUE TYPE ACTIVE
SET RIP WAN0 AUTH TYPE NONE
SET RIP UP
SET OSPF PURGE
```

```
SET BGP PURGE
SET DDNS PURGE
SET IPLOG PURGE
SET DHCP PURGE
SET STATS PURGE
SET XOT PURGE
SET SYSTEM HOSTNAME "nome_do_roteador" PURGEDNS
SET SYSTEM LOG PURGE
SET SYSTEM LOG ENTRY0 FACILITY ALL PRIORITY EMERG OUTPUTTYPE REMOTE
HOST "xxx.xxx.xxx.xxx"
SET SYSTEM LOG UP
SET SYSTEM BANNER PURGE
SET SYSTEM BANNER LINES
[++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++

                              A T E N C A O

        *** Permitido o uso somente para pessoas autorizadas ***

A utilizacao indevida ou a operacao que exceda o nivel de autorizacao
permitido,
estara sujeita a monitoramento.


++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++]
SET SYSTEM DESCRIPTION PURGE
SET SYSTEM WEBAUTH PURGE
SET SYSTEM TIMEZONE PURGE
SET SYSTEM UPDATE SERVER 0.0.0.0
SET SYSTEM AAA AUTHENTICATION PURGE
SET SYSTEM AAA AUTHENTICATION SHADOW UP
SET SYSTEM AAA AUTHENTICATION RADIUS UP DEBUG FALSE SERVER
xxx.xxx.xxx.xxx TIMEOUT 0
```

Imagem 5 – *Script* Digitel 3211 parte 1.
Fonte: *Print screen* do roteador.



```
SET SYSTEM AAA AUTHENTICATION RADIUS SECRET "senha_radius"
SET SYSTEM AAA AUTHENTICATION ORDER RADIUS SHADOW
SET SYSTEM AAA AUTHENTICATION RADIUS ONERROR CONTINUE
SET SYSTEM AAA AUTHORIZATION PURGE
SET SYSTEM AAA ACCOUNTING PURGE
SET IPX PURGE
SET NAT PURGE
SET FIREWALL PURGE
SET PIM PURGE
SET PIM MODE SPARSE
SET PIM DEBUG FALSE
SET PIM SPTTHRESHOLD FALSE
SET PIM REGISTERTHRESHOLD FALSE
SET PIM DOWN
SET SNMP PURGE
SET SNMP TRAPAUTHFAILURE FALSE
SET SNMP MODE TRADITIONAL
SET SNMP ROCOMMUNITY0 NAME "nome_community"
SET SNMP UP
SET ADVANCED ENABLED FALSE
SET QOS PURGE
SET PROXYARP PURGE
SET DLSW PURGE
SET DLSW DOWN
SET NTP PURGE
SET BRIDGE PURGE
SET ROUTES PURGE
SET ROUTES UP
SET BACKUP PURGE
SET VRRP PURGE
SET IPACCT PURGE
SET DNSRELAY PURGE
SET DNSRELAY DEBUG FALSE LOADBALANCE FALSE RETRYINTERVAL 10 TIMEOUT 12
DOWN
SET SLAPM PURGE
```

```
SET SERVICES PURGE
SET SERVICES SSH ENABLED TRUE ALLOWROOT FALSE
SET SERVICES TELNET ENABLED TRUE
SET SERVICES WEBCONFIG ENABLED TRUE
```

Fim do documento

Imagem 6 – *Script* Digitel 3211 parte 2.
Fonte: *Print screen* do roteador.

As imagens 5 e 6 apresentam as configurações completas para se colocar um roteador Digitel em produção. Ressalte-se porém que, onde deveria estar um número de IP e uma máscara de rede na configuração, foi inserida, respectivamente as expressões “xxx.xxx.xxx.xxx” e “yyy.yyy.yyy.yyy” por questão de ética e segurança.

Para se chegar a este resultado de configuração em um roteador Digitel, não se faz necessário digitar todas as linhas ilustradas nas imagens 5 e 6. Para tal é preciso o seguinte:

- Configurar interface *LAN*:

```
1. SET LAN LAN0 PURGE
2. SET LAN LAN0 MODE AUTO
3. SET LAN LAN0 IP “xxx.xxx.xxx.xxx” MASK “yyy.yyy.yyy.yyy”
4. SET LAN LAN0 COMMENT [Rede Interna do Cliente]
5. SET LAN LAN0 UP
```

Na linha 1, o comando serve para limpar as configurações da interface afim de se evitar alguma “sujeira” na configuração. A linha 2 é referente ao modo de negociação da porta, que pode ser *AUTO* (automático), 100FD (100 Mbps *full duplex*) e 100HD (100 Mbps *half duplex*). O comando para determinar um IP para a interface é apresentado na lina 3 na qual “xxx.xxx.xxx.xxx” é um endereço IP e “yyy.yyy.yyy.yyy” sua respectiva máscara de rede. A linha 4 permite que seja feito uma descrição da interface, onde descreve-se com quem ela está conectada para facilitar na organização e manutenção da rede. Para habilitar a interface, basta executar o comando da linha 5. Se o objetivo for desabilitar, substitua a palavra *UP* no final da linha 5 por *DOWN*.

- Configurar interface *WAN*:

```
1. SET WAN WAN0 PURGE
2. SET WAN WAN0 PROTO PPPS
3. SET WAN WAN0 IP “xxx.xxx.xxx.xxx” MASK “yyy.yyy.yyy.yyy”
4. SET WAN WAN0 COMMENT [conexão com provedor]
5. SET WAN WAN0 UP
```

As configurações da interface *wan* diferenciam-se da *lan* na linha 2 onde se define qual protocolo está sendo utilizado para conexão com o provedor.

- Configurar roteamento:
  - Configurar roteamento *RIP*:

```
1. SET RIP PURGE
2. SET RIP VERSION 2
3. SET RIP REDIST-STATIC TRUE REDIST-CONNECTED TRUE REDIST-
   OSPF FALSE DEFAULTMETRIC 1
4. SET RIP LAN0 ENABLED TRUE TYPE ACTIVE
5. SET RIP LAN0 AUTH TYPE NONE
6. SET RIP WAN0 ENABLED TRUE TYPE ACTIVE
7. SET RIP WAN0 AUTH TYPE NONE
8. SET RIP UP
```

Inicialmente remove-se todas as configurações do roteamento *RIP*, depois define-se sua versão como sendo a 2, em seguida ele é orientado a redistribuir as rotas estáticas e também as redes conectadas no roteador, porém é proibido redistribuir rotas do protocolo de roteamento *OSPF*. O passo seguinte é habilitá-lo na interface *LAN0* (linha 4) e informá-lo de que não há necessidade de autenticação naquela interface (linha 5). Para configurar o *RIP* nas demais interfaces, apenas substitua o nome da interface conforme linhas 6 e 7. Após declaradas todas às interfaces, inicie-o com a linha 8.

  - Configurar roteamento estático:

```
1. SET ROUTES PURGE
2. SET ROUTES DEFAULT GW1 “xxx.xxx.xxx.xxx”
3. SET ROUTES UP
```

Utilizando a linha 1 pode-se limpar as configurações de roteamento estático. Com a linha 2 se define o *Gateway* padrão 1 (endereço IP de saída da rede). Por fim,

inicia-se o roteamento estático com a linha 3 e para interrompe-lo substitui-se *UP* no fim da linha por *DOWN*.

- Configurar SNMP *(Simple Network Management Protocol)*:

```
1. SET SNMP PURGE
2. SET SNMP TRAPAUTHFAILURE FALSE
3. SET SNMP MODE TRADITIONAL
4. SET SNMP ROCOMMUNITY0 NAME “nome_community”
5. SET SNMP UP
```

O *SNMP* é um protocolo de gerenciamento de rede que possibilita várias informações e ações sobre os equipamentos na rede. Para configurá-lo, inicialmente limpe qualquer configuração que venha a existir, em seguida informe-o para não enviar *TRAP FAILURE* (mensagens de falha do protocolo *snmp*). Define-se o modo de operação como tradicional na linha 3, e o tipo de *community* na linha 4, como *rocommunity ou rwcommunity,* onde a primeira é somente leitura e a segunda leitura e escrita. A inicialização do serviço se dá pela linha 5 e a interrupção através da substituição de *UP* por *DOWN* no fim da linha.

- Configurar *banner*:

```
1. SET SYSTEM BANNER PURGE
2. SET SYSTEM BANNER LINES %++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++++++++++++++++++++++
3.
4.                                A T E N C A O
5.
6.          *** Permitido o uso somente para pessoas autorizadas
   ***
7.
8. A utilizacao indevida ou a operacao que exceda o nivel de
   autorizacao permitido,
9. estara sujeita a monitoramento.
10.
11.
12.++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++%
```

O *banner* serve para alertar quem está tentando acessar o equipamento seja por *telnet*, protocolo de acesso remoto, ou pela console, interface local de gerenciamento. A linha limpa as configurações de *banner*, e para criar um novo utiliza-se a linha 2, onde tem uma característica importante a ser observada; o caractere de abertura e fechamento da mensagem. No exemplo acima, o caractere é “%”, e uma boa prática é usar para tal

caracteres especiais pois quando inicia-se a mensagem, na primeira ocorrência do caractere de abertura à mensagem será encerrada.

- Configurar usuário:

1. `SET SYSTEM USER1 TYPE ADMINISTRATOR`
2. `SET SYSTEM USER1 LOGIN “nome” PASS “senha”`

A primeira instância define o usuário como administrador e em seguida define-se o nome e a senha para o mesmo.

- Configurar usuário:

1. `CONFIG SAVE`

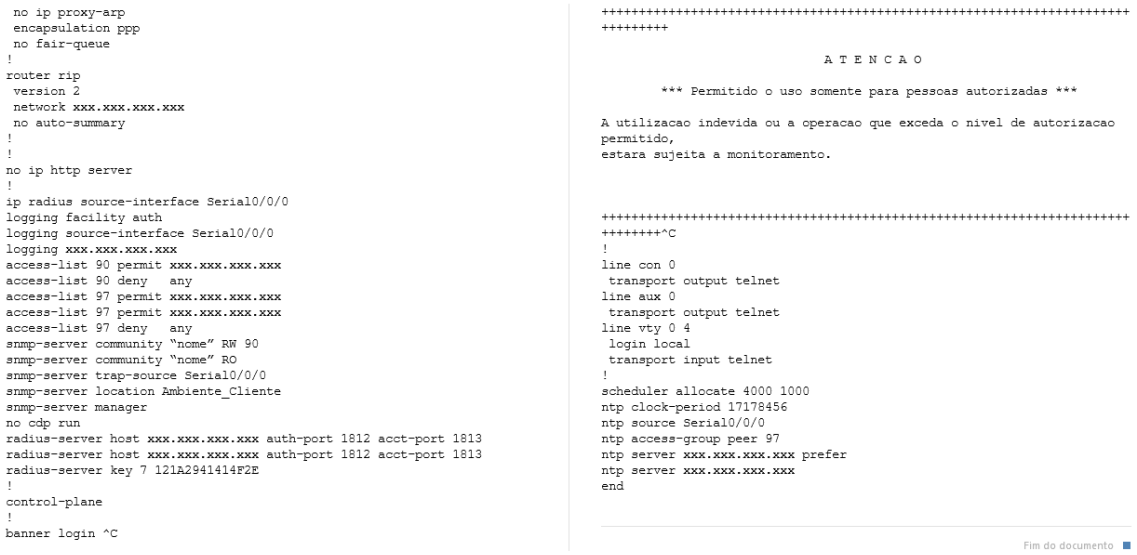
Por fim o comando acima salva as configurações realizadas.

As configurações exemplificadas acima para o roteador Digitel 3211 servem tanto para *Internet link* quanto *vpn*, o que vai diferenciar um do outro é a faixa IP, IP público e IP privado respectivamente. O modelo 3238 da Digitel segue o mesmo modelo de configuração sendo diferenciado do outro na quantidade de interfaces em que este possui, 2 *LANs* e 2 *WANs.*

```
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime localtime
service password-encryption
service sequence-numbers
!
hostname “nome_do_roteador”
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 4096 notifications
enable secret 5 $1$zGuI$6GbYs4DIv9ZwSIDt7FpwK1
!
aaa new-model
!
!
aaa authentication login default group radius local
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
!
aaa session-id common
clock timezone BSB -3
clock summer-time Horario_verao date Oct 14 2007 0:00 Feb 16 2008 0:00
no ip source-route
ip cef
!
!
!
```

```
!
no ip bootp server
no ip domain lookup
username “usuario” secret “senha”
!

ip tcp synwait-time 10
ip tftp source-interface Serial0/0/0
!
!
interface Null0
 no ip unreachables
!
interface FastEthernet0/0
 description Ambiente do cliente
 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 speed 100
 full-duplex
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 !
interface Serial0/0/0
 description conexao com operadora
 bandwidth 1024
 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
 no ip redirects
 no ip unreachables
```

Imagem 7 – *Script* Cisco 1841 parte 1.
Fonte: *Print screen* do roteador.



```
 no ip proxy-arp
 encapsulation ppp
 no fair-queue
!
router rip
 version 2
 network xxx.xxx.xxx.xxx
 no auto-summary
!
!
no ip http server
!
ip radius source-interface Serial0/0/0
logging facility auth
logging source-interface Serial0/0/0
logging xxx.xxx.xxx.xxx
access-list 90 permit xxx.xxx.xxx.xxx
access-list 90 deny   any
access-list 97 permit xxx.xxx.xxx.xxx
access-list 97 permit xxx.xxx.xxx.xxx
access-list 97 deny   any
snmp-server community "nome" RW 90
snmp-server community "nome" RO
snmp-server trap-source Serial0/0/0
snmp-server location Ambiente_Cliente
snmp-server manager
no cdp run
radius-server host xxx.xxx.xxx.xxx auth-port 1812 acct-port 1813
radius-server host xxx.xxx.xxx.xxx auth-port 1812 acct-port 1813
radius-server key 7 121A2941414F2E
!
control-plane
!
banner login ^C
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++

                              A T E N C A O

        *** Permitido o uso somente para pessoas autorizadas ***

A utilizacao indevida ou a operacao que exceda o nivel de autorizacao
permitido,
estara sujeita a monitoramento.



++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++^C
!
line con 0
 transport output telnet
line aux 0
 transport output telnet
line vty 0 4
 login local
 transport input telnet
!
scheduler allocate 4000 1000
ntp clock-period 17178456
ntp source Serial0/0/0
ntp access-group peer 97
ntp server xxx.xxx.xxx.xxx prefer
ntp server xxx.xxx.xxx.xxx
end

Fim do documento
```

Imagem 8 – *Script* Cisco 1841 parte 2.
Fonte: *Print screen* do roteador.

Um exemplo de configuração dos roteadores Cisco 1841 é apresentado nas imagens 7 e 8.

Abaixo serão expostos e explicados os comandos, básicos e avançados, para configurar e colocar em operação o roteador. Para executar os comandos básicos nestes roteadores é preciso navegar entre os modos de configuração, modo usuário, modo privilegiado e modo de configuração global.

A diferenciação dos modos está na terminação do cursor no *prompt* da interface de linha de comandos do roteador.

O modo usuário, cujas autorizações dão direito à visualizar algumas informações do roteador, é o ponto de partida ao acessá-lo e termina o cursor com “>” (*router>*). Para se chegar ao modo privilegiado, no qual o cursor se encerra com “#” (*router#*) e que possibilita visualizar informações, salvar ou apagar configurações por exemplo, é necessário digitar o comando *enable (router> enable)*. Em seguida, digitando-se o comando *configure terminal (router# configure terminal)*, se chega ao modo de configuração global (*router(config)#*). Neste nível se pode alterar todas as configurações do equipamento navegando entre seus submodos.

- Configurar interface *LAN* (*router(config)#*):

1. *interface FastEthernet0/0*
2. *description “rede_lan”*
3. *ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy*
4. *speed 100*

5. *duplex full*
6. *no shutdown*

A primeira linha faz referência a qual interface se vai configurar, em seguida, como uma boa prática faz-se uma descrição da mesma, após define-se o endereço IP e máscara de rede para à interface. O modo de operação da interface por padrão é auto, no qual o equipamento negocia com o outro a melhor forma de operar. No entanto, pode-se forçar o modo operacional com a linha 4, que especifica a velocidade com que se deseja que a porta opere, neste caso 100 Mbps, e linha 5 que indica a direção do tráfego, *duplex full* que permite enviar e receber informação simultaneamente ou *duplex half*, no qual um equipamento envia ou recebe. Por fim, com a linha 6, se habilita a interface.

- Configurar interface *WAN* (*router(config)#*):

1. *interface Serial0/0/0*
2. *description "conexao_com_provedor"*
3. *ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy*
4. *encapsulation ppp*
5. *no shutdown*

A interface serial segue os mesmos passos da *LAN* até a linha 3. A linha 4 vem especificar que o protocolo é *ppp (point-to-point* – ponto-a-ponto*)*. Depois a interface é ativada.

- Configurar roteamento

    - Configurar roteamento dinâmico (*router(config)#*):

```
1. router rip
2.  version 2
3.  network xxx.xxx.xxx.xxx
```

O primeiro passo é entrar no modo de configuração *RIP* com a linha 1, depois se escolhe a versão do mesmo, em seguida se especifica as redes que ele divulgará. Deve-se informa-lo o endereço de rede tanto da *LAN* quanto da *WAN*. Se as faixas de rede não puderem ser resumidas em uma única rede, repita o passo 3 para todas as redes necessárias.

    - Configurar roteamento estático (*router(config)#*):

```
1. ip route xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy xxx.xxx.xxx.xxx
2. ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx
```

O roteamento estático pode ser configurado de duas maneiras. Na primeira (linha 1), têm-se o modelo no qual determina-se a rota para uma rede específica. Na segunda é apresentada uma rota padrão, por todo o tráfego é encaminhado.

- Configurar usuário e senha (*router(config)#*):

1. *username “nome” secret “senha”*
2. *enable secret “senha”*

Por questão de segurança deve-se configurar usuário e senha, linha 1, que serão solicitados para acessar o modo usuário. A linha 2 cria uma senha de proteção do modo privilegiado que é requerida após o comando *enable* ser digitado no modo usuário.

- Configurar *banner* (*router(config)#*):

1. banner login ^
2. ++
3.
4. A T E N C A O
5.
6. *** Permitido o uso somente para pessoas autorizadas ***
7.
8. A utilizacao indevida ou a operacao que exceda o nivel de autorizacao permitido,
9. estara sujeita a monitoramento.
10.
11. +++^

A linha 1 apresenta o comanda para mostrar uma mensagem de alerta a quem tentar acessar o roteador, sem deixar de observar o caractere de abertura da mensagem (^) que reaparece no encerramento da mesma, no fim da linha 11.

- Configurar acessos (*router(config)#*):

1. *line con 0*
2. *login local*
3. *line vty 0 4*
4. *login local*
5. *line aux 0*
6. *login local*

A primeiro método de acesso sendo configurado é a console 0, que é a interface de gerenciamento local do equipamento, em seguida pede-se que seja feita uma autenticação local, ou seja, que se informe o usuário e senha criados anteriormente. O próximo meio de conexão é para acesso remoto através do protocolo *telnet*, com direito

à 5 seções simultâneas. A linha 5 refere-se à um método de acesso remoto através de um modem discado, o qual passa à exigir autenticação após comando em linha 6.

```
#3Com Router Software V3.12
#
 sysname "nome_do_router"
#
 super password level 3 cipher T2WL;AZ2987Q=^Q`MAF4<1!!
#
 configure-user count  2
#
 clock timezone bsb minus 03:00:00
#
 domain default enable "dominio"
#
 cpu-usage cycle 1min
#
 flow-interval 30
#
 web set-package force flash:/http.zip
#
domain system
#
local-user admin
 password cipher a"VDA'E0&,/Q=^Q`MAF4<1!!
 state block
 service-type telnet terminal
 level 3
 service-type ftp
local-user "nome_usuario"
 password cipher "senha"
 service-type telnet terminal
 service-type ftp
 service-type ppp
#
acl number 2000
 description Autenticacao do NTP
 rule 5 permit source xxx.xxx.xxx.xxx 0
 rule 10 permit source xxx.xxx.xxx.xxx 0
 rule 15 deny
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 description Rede Interna Cliente
 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
 rip version 2 multicast
#
interface Ethernet2/0
 speed 100
 duplex full
 description interligado a SW 3400
 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
 rip version 2 multicast
#
interface Serial0/0
 clock DTECLK1
 link-protocol ppp
 shutdown
#
interface NULL0
#
interface LoopBack0
 description Interface de Gerencia
#
rip
 undo summary
 network xxx.xxx.xxx.xxx
#
 FTP server enable
#
 radius nas-ip xxx.xxx.xxx.xxx
```

Imagem 9 – *Script* 3Com parte 1.
Fonte: *Print screen* do roteador.

```
#
 snmp-agent
 snmp-agent local-engineid 0000002B7F00000100006725
 snmp-agent community read "nome_community"
 snmp-agent sys-info location Ambiente_cliente
 snmp-agent sys-info version all
 snmp-agent group v3 admin read-view admin write-view admin
 snmp-agent mib-view included admin iso
 snmp-agent usm-user v3 admin admin
#
 ntp-service authentication enable
 ntp-service access peer 2000
 ntp-service unicast-peer xxx.xxx.xxx.xxx
 ntp-service unicast-server xxx.xxx.xxx.xxx
#
 header login %
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++

                              A T E N C A O

        *** Permitido o uso somente para pessoas autorizadas ***

A utilizacao indevida ou a operacao que exceda o nivel de autorizacao
permitido,
estara sujeita a monitoramento.


++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++
%
#
user-interface con 0
 authentication-mode scheme
user-interface aux 0
 authentication-mode scheme
user-interface vty 0 4
 authentication-mode scheme
#
return
```

Imagem 10 – *Script* 3Com parte 2.
Fonte: *Print screen* do roteador.

As configurações aplicadas aos roteadores 3Com seguem o mesmo padrão dos equipamentos da Cisco, diferindo em nomes dos comandos e em certas particularidades. Estas diferenças por sua vez podem ser observadas no modo de acesso aos diferentes níveis de privilégio onde no Cisco se usa *enable*, no 3Com é *super,* em vez de *configure terminal* se utiliza *system view.*

Um exemplo de configuração 3Com é apresentado nas imagens 9 e 10. A partir de então serão explicados estes comandos assim como realizado anteriormente.

- Configurar interface *LAN*:

1. *interface Ethernet0/0*
2. *description "rede_lan"*
3. *ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy*
4. *speed 100*
5. *duplex full*
6. *undo shutdown*

As configurações da interface *LAN* são idênticas as do 1841, no entanto, na linha 6 verifica-se uma diferença no início do comando que utiliza '*undo'* em vez de '*no'* para habilitar a interface.

- Configurar interface *WAN*

1. *interface Serial0/0*
2. *description "conexao_com_provedor"*
3. *ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy*
4. *link-protocol ppp*
5. *undo shutdown*

A interface serial segue os mesmos passos da *LAN* até a linha 3. A linha 4 vem especificar que o protocolo é *ppp (point-to-point* – ponto-a-ponto*).* Depois a interface é ativada.

- Configurar roteamento
    - Configurar roteamento dinâmico (*router(config)#*):

```
4. rip
5.  version 2
6.  network xxx.xxx.xxx.xxx
```

O primeiro passo é entrar no modo de configuração *RIP* com a linha 1, depois se escolhe a versão do mesmo, em seguida se especifica as redes que ele divulgará. Deve-se informa-lo o endereço de rede tanto da *LAN* quanto da *WAN*. Se as faixas de rede não

puderem ser resumidas em uma única rede, repita o passo 3 para todas as redes necessárias.

- Configurar roteamento estático (*router(config)#*):

```
1. ip route-static xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
   xxx.xxx.xxx.xxx
2. ip route-static 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx
```

O roteamento estático pode ser configurado de duas maneiras. Na primeira (linha 1), têm-se o modelo no qual determina-se a rota para uma rede específica. Na segunda é apresentada uma rota padrão, por todo o tráfego é encaminhado.

- Configurar usuário e senha (*router(config)#*):

```
1. local-user “nome_usuario”
2. password cipher “senha”
3. service-type telnet terminal
4. service-type ftp
```

Por questão de segurança deve-se configurar usuário e senha, assim na linha 1 se cria o usuário e na linha 2 é que se define a senha, diferentemente do Cisco em que é feito num único comando. Em seguida, nas linhas 3 e 4, se especifica quais protocolos de acesso remoto estão permitidos para este usuário. Com o *telnet* o equipamento poderá ser gerenciado remotamente e com *FTP* se pode transferir um IOS, arquivo de atualização do *software* do roteador, por exemplo.

- Configurar *banner* (*router(config)#*):

```
1. header login ^
2. ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   ++++
3.
                i. A T E N C A O
4.
5. *** Permitido o uso somente para pessoas autorizadas ***
6.
7. A utilizacao indevida ou a operacao que exceda o nivel de autorizacao permitido,
8. estara sujeita a monitoramento.
9.
10. ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   +++^
```

Semelhantemente ao 1841, o 3Com exibe uma mensagem de alerta quando se tenta acessá-lo, no entanto, difere no primeiro termo do comando, de *banner* para *header login.*

- Configurar acessos (*router(config)#*):

```
1. user-interface con 0
2.  authentication-mode scheme
3. user-interface aux 0
4.  authentication-mode scheme
5. user-interface vty 0 4
6.  authentication-mode scheme
```

A primeiro método de acesso sendo configurado é a console 0, que é a interface de gerenciamento local do equipamento, em seguida pede-se que seja feita uma autenticação local, ou seja, que se informe o usuário e senha criados anteriormente. O próximo meio de conexão é para cesso remoto através do protocolo *telnet*, com direito à 5 seções simultâneas. A linha 5 refere-se à um método de acesso remoto através de um modem discado, o qual passa à exigir autenticação após comando em linha 6.

4. TR-069

O *DSL Forum*, atualmente *Broadband Forum*, é o responsável pela publicação do relatório técnico TR-069 , que descreve um modelo de gerenciamento remoto do CPE através de sua interface WAN.

O desenvolvimento de novos relatórios, foi possibilitando a implementação do TR-69 não só para gerenciamento de CPEs DSL, como também para provisionamento de recursos na rede e gerência de equipamentos CPE *GPON* (*Gigabit Passive Optical Network* – rede gigabit óptica passiva, TR-156), e *Set-Top Box* (dispositivos IP TV – TR-135). Com isso a "família" TR-69 é também conhecida como *CWMP* (*CPE WAN Management Protocol*, "protocolo de gerenciamento *wan* de *cpe"*).

O *CWMP* suporta uma variedade de funcionalidades e dentre as quais se pode destacar; autoconfiguração e provisionamento de serviços, diagnósticos, monitoramento de desempenho e gerenciamento de software/firmware dos equipamentos.

A topologia deste protocolo é cliente/servidor na qual ACS, que é um acrônimo para *Auto-Configuration Server* (Servidor de Autoconfiguração), responde às

solicitações de configuração inicial, bem como as demais solicitações efetuadas pelo CPE.

Para que CPE faça as requisições ao ACS é preciso configurá-lo com a URL, *uniform resource locator* (localizador uniforme de recursos) que é o *link*, endereço do servidor de autoconfiguração. Esta configuração pode ser feita de maneira estática, quando o técnico acessa o equipamento e insere este endereço ou se estiver como um endereço padrão pré-estabelecido no *software/firmware* do equipamento, ou de forma dinâmica, utilizando o servidor DHCP (*Dynamic Host Configuration Protocol*), que tem por função estabelecer as configurações de IP para as máquinas, sejam elas computadores, roteadores, modens, etc.

Um servidor DHCP pode fornecer diversas configurações além das básicas de endereçamento IP para o qual foi desenvolvido, de acordo com o apresentado na RFC (*Request For Comments*, "requerimento de comentários") 2132, cujo título é *"DHCP Options and BOOTP Vendor Extensions"* ("Opções DHCP e Extensões de Vendedor BOOTP").

A inicialização de uma conexão com o ACS pode ser feita a qualquer momento pelo CPE, desde que seja atendido o parâmetro supracitado, além de um endereço IP da conexão de banda larga (IP válido para acessar a *Internet*), o IP do ACS e o código de provisionamento. Estes parâmetros serão utilizados no estabelecimento da primeira conexão e poderão ser alterados pelo ACS a partir de então.

O ACS após a conexão inicial do CPE pode a qualquer instante conectar-se a ele por meio do mecanismo de notificação de solicitação de conexão, onde o CPE deve ter um endereço IP que pode ser roteado para à *Internet*. Se por ventura o CPE estiver atrás de um *firewall*, dispositivo cuja função é a proteção da rede ou computador podendo ser este implementado apenas num programa ou no conjunto programa/máquina específicos para à função, ou *NAT (Network Address Translation* – Tradução de endereço de rede) pode ocorrer de o ACS não conseguir acessá-lo e com isso apenas o CPE inicia a sessão.

A autoconfiguração e provisionamento de serviços é realizada no momento da primeira conexão, conforme processo descrito acima. O protocolo possibilita ao cliente gerar informações que são enviadas ao servidor com objetivo de diagnosticar a conectividade ou problemas no serviço.

O monitoramento de desempenho consiste na utilização de mecanismos pré-definidos e personalizáveis segundo a flexibilidade do protocolo. Com isso tem-se a facilidade de adaptá-lo para cada equipamento e nível de monitoramento necessário. Em relação ao gerenciamento de software/firmware dos equipamentos, observa-se a capacidade de gerenciamento do protocolo, onde ele verifica no servidor qual à versão de software/firmware o cliente deve utilizar. Se estiver desatualizado, ele inicia o download e quando concluído, informa ao servidor, sucesso ou sem sucesso.

4.1. TR-069, equipamentos e utilizações

A "família" TR (*Technical Reports* – Relatórios Técnicos) conta com vários TRs para formar o TR-069, hoje *CWMP, CPE WAN Management Protocol (*Protocolo de gerenciamento WAN de CPE*).* A imagem abaixo apresenta parte desta estrutura "familiar".

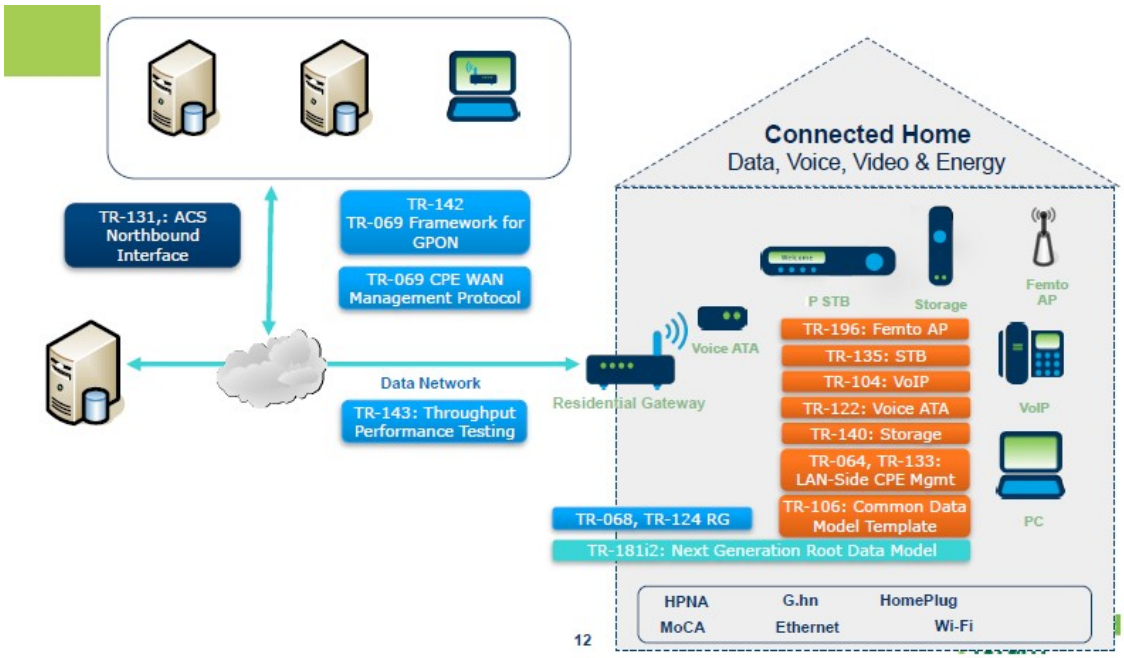


Imagem 11 – Família TR-069.
Fonte: *BroadBand Forum*, programa de certificação BBF069

No dia 16 de outubro de 2012, durante o *BroadBand World Forum*, Robin Mersh (CEO do *Broadband Forum*) apresentou relatório de progresso da banda larga e IPTV e lançamento da certificação (BBF.069). Este, por sua vez, relata que em 2011 mais de 147 milhões de dispositivos eram gerenciados pelo protocolo e em 2012 os prestadores de serviços já estavam gerenciando mais 624 milhões de clientes. Além de divulgar que

o protocolo TR-069 havia sido escolhido globalmente para fornecer este serviço com qualidade consistente e interoperabilidade.

Esta certificação apresenta os primeiros produtos para adquirirem a mesma. Os fabricantes destes são apresentados na imagem abaixo.

Imagem 12 – Primeiros fabricantes a tentar a certificação BBF.069.
Fonte: *BroadBand Forum*, programa de certificação BBF.069

Dentre os fabricantes exibidos na imagem 12, pode-se dividi-los em dois grupos; um com equipamento cuja função seja de roteador de rede cabeada e sem fio, onde se encaixa *D-link*, *Cisco* e *Lantiq*, o outro que, além destas, exerce a função de *modem*, no qual se encontra *Broadcom* e *Huawei.*

A diferença entre os dois grupos está no fato de que o primeiro necessita da utilização de um *modem* em conjunto para se disponibilizar o acesso à *Internet* e aos demais serviços prestados ao cliente.

Um dos equipamentos que se encaixam no primeiro grupo é o *Linksys e4200*, da *Cisco*. Ele é um roteador sem fio *dual band* (duas bandas), ou seja, que trabalha em duas frequências simultâneas, 2.4 e 5 GHz. Possui 6 antenas internas, sendo 3 para 2.4 e 3 para 5 GHz, 4 portas *Gigabit Ethernet*, para conectar à rede interna (computadores, TVs, por exemplo), uma porta *USB* que pode ser usada para conectar uma impressora e uma porta *Internet* que deve ser conectada ao *modem*, para distribuir o acesso à *Internet.*

Para exemplificar os equipamentos do segundo grupo, cita-se o *Huawei Speedport W 724V Typ A*. Conforme dados técnicos do produto, ele tem suporte ao novo padrão de redes sem fio, o 802.11ac, e pode atingir à velocidade 1,3 Gbps, de acordo com fabricantes como *Netgear, D-link, Cisco.* No entanto, ainda é compatível com os atuais padrões *wireless*, 802.11b/g/n. O dispositivo conta ainda com 4 portas *Gigabit Ethernet* e 2 portas *USB.*

As certificações da "família" TR-69 se estenderam para os equipamentos voltados para terminação em fibra óptica no ambiente do cliente (*GPON*). Com isso, foi lançada, em outubro de 2012, durante à apresentação do relatório no fórum mundial do *BroandBand*, a certificação BBF.247. A imagem abaixo expõe os fabricantes que se propuseram a tentar a certificação.

Imagem 12 – Primeiros fabricantes a tentar a certificação BBF.247.

Fonte: *BroadBand Forum*, programa de certificação BBF069

5. Considerações finais

O crescimento de uma rede de computadores ou telecomunicações exige que se tome medidas de controle especiais, tais como de segurança, por exemplo. O gerenciamento é outra medida que tem por objetivo organizar e facilitar a execução do trabalho.

Esse gerenciamento pode ser feito de várias formas e com diversas ferramentas, onde cada uma, mesmo não sendo completa, tem um papel importante numa dessas estruturas. Aliás, uma ferramenta completa para tal, considerando o ambiente de uma

operadora de telecomunicações, é difícil de ser forjada, pois nos dias atuais, o que se encontra nestes ambientes é uma grande diversidade de equipamentos, com as mais variadas funcionalidades. No entanto, tem ocorrido vários esforços para se desenvolver uma capaz de suprir as necessidades do mercado abrangendo a estrutura legada e à atual.

Atualmente, uma promessa para à tarefa é o protocolo TR-069, que surgiu com um propósito de gerenciar modens de conexão banda larga, ADSL por exemplo. Pode-se perceber o potencial deste em função dos recursos e facilidade de implementação. Sua flexibilidade é tamanha, que ao mesmo tempo em que foi lançada uma certificação para os equipamentos de acesso xDSL, também lançou-se uma certificação para dispositivos de rede GPON.

O protocolo demonstrou ser capaz de prover um excelente instrumento de gestão, com potencial de expansão e adaptação.

O intuito deste artigo é apresentar este protocolo demonstrando suas características, utilizações, bem como alguns requisitos que uma ferramenta deste tipo deve contemplar. Contudo, fica aberta a oportunidade para sejam desenvolvidos trabalhos e contribuições no desenvolvimento e divulgação deste artigo.

6. Glossário

CPE, *Customer Premises Equipment* – que é o equipamento do ambiente do cliente.

VPN, *Virtual Private Networks* – Redes Privadas Virtuais.

DSL, *Digital Subscriber Line* – Linha Digital de Assinantes.

xDSL, idem à DSL com o X representando possíveis variações, como ADSL, por exemplo, onde o A significa *Asynchronous*, Assíncrono.

TR, *Technical Reports*, Relatórios Técnicos.

TR-069, *Technical Reports 069*, Relatório Técnico 069.

GPON, *Gigabit Passive Optical Network* – rede gigabit óptica passiva.

ACS, *Auto-Configuration Server*, Servidor de Autoconfiguração.

RFC, *Request For Comments*, requerimento de comentários.

DHCP, *Dynamic Host Configuration Protocol*, Protocolo de configuração dinâmica de máquina.

IP, *Internet Protocol*, Protocolo de *Internet.*

CWMP, CPE WAN Management Protocol, Protocolo de gerenciamento WAN de CPE.

NAT, Network Address Translation, Tradução de endereço de rede.

7. Referências

Vyncke, Eric; Hogg, Scott, *"IPv6 Internet Security for Your Network"*, 2009.

http://www.cisco.com/en/US/products/ps5875/index.html (1841)

http://h10010.www1.hp.com/wwpc/br/pt/sm/WF06b/12883-12883-4172265-4172270-4172270-4176157-4199332.html?dnr=1

http://h10010.www1.hp.com/wwpc/br/pt/sm/WF06b/12883-12883-4172265-4172270-4172270-4176152-4199529.html?dnr=1

http://www.digitel.com.br/pt/produtos/produto.asp?Id=14

http://www.cisco.com/en/US/docs/routers/access/1800/1841/software/configuration/guide/b_cli.html

Mersh, Robin, "BBF 069 *Cert Launch*", 2012

Mersh, Robin, "BBF GPON *Cert Launch*", 2012

Forum, BroadBand, "*TR-069 Abstract Test Plan*", 2013

Forum, BroadBand, *"TR-069 CPE WAN Management Protocol"*, 2011