Novas Demandas na Gerência do Protocolo BGP4

IX Congresso Argentino de Ciencias de la Computación

Andrey Vedana Andreoli[1] , Leandro Márcio Bertholdo[1] , Liane Tarouco[1],

Ana Benso da Silva [2], Fábio Rodrigues [2]

[1] Ponto de Presença da RNP no Rio Grande do Sul – POP-RS

RSiX – Ponto de Troca de Tráfego do Rio Grande do Sul

Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul

Ramiro Barcelos, 2574 – Porto Alegre – RS – Brasil

[2] Pontifícia Universidade Católica do Rio Grande do Sul – Faculdade de Informática

Avenida Ipiranga, 6681 – Porto Alegre – RS – Brasil

{andrey,berthold,liane}@penta.ufrgs.br,{benso,ji202379}@inf.pucrs.Br

Resumo. *Este artigo descreve e analisa as necessidades de monitoração do protocolo BGP, demonstrando algumas formas de acesso aos dados deste protocolo para monitoramento. É feito então um estudo de caso na monitoração do BGP em um Ponto de Troca de Tráfego, implementando e validando um sub-agente que complementa o conjunto de informações importantes deste protocolo. Dentre os resultados obtidos frente ao problema apresentado, esse artigo propõem modificações na MIB BGP incluindo novas funcionalidades.*

Palavras chave: Roteamento, BGP, Pontos de Troca de Tráfego, Gerência de redes.

1. Informações Gerais

A Internet deixou de ser um simples meio de comunicação acadêmico para se tornar uma fonte de serviços e negócios. Ela deixou de ser uma opção e é atualmente uma necessidade para empresas e instituições acadêmicas, sendo utilizada desde crianças até adultos. O leque de serviços que tem surgido a partir desse crescimento desafia os profissionais de TI a buscarem continuamente subsídios para dar suporte desde aplicações tradicionais como web, e-mail, até transações financeiras, e-commerce, e-learning, videoconferência, telefonia e telemedicina.

Acompanhando esse crescimento, o modelo conhecido como hierárquico, constituído por uma rede centralizada que conectava redes secundárias, foi substituído por um modelo distribuído. A partir destas mudanças, grandes redes e backbones passaram a ser vistos, perante a Internet, como sistemas autônomos, também chamados de ASes. Tal definição faz com que as

operações internas a um AS não sejam conhecidas pelos demais Sistemas Autônomos, diminuindo a complexidade da Internet global.

O protocolo que iniciou a utilização desse conceito, e permanece até os dias de hoje, é o BGP (Border Gateway Protocol), que está atualmente na versão 4 [1]. Para trabalhar de uma forma eficiente diante da complexidade da Internet, o BGP conta com uma série de atributos que são utilizados para fazer uso dos melhores caminhos, de acordo com as políticas de tráfego de cada sistema autônomo. Adicionalmente, com o surgimento do Multicast e da entrada gradual do IPv6, o BGP tem acompanhado tais inovações, formando o Multiprotocol BGP [2], ou simplesmente MBGP, capaz de atuar não somente sobre IPv4, mas também com IPv6 e Multicast de uma forma integrada e robusta.

Com essa necessidade, a monitoração do protocolo BGP tem se tornado uma forma importante de avaliar e gerenciar o comportamento de um sistema autônomo perante os demais sistemas autônomos presentes na Internet. Este controle tem como objetivos fornecer informações importantes capazes de conduzir a gerência de um AS de uma forma mais facilitada, sinalizando eventuais anormalidades.

Para este monitoramento, diversas abordagens têm sido propostas e utilizadas. As principais abordagens serão expostas a seguir, relatando brevemente a estrutura que cada uma destas necessita para seu funcionamento, bem como seus benefícios e limitações:

- Sniffing: Baseada na captura das mensagens BGP entre os roteadores, esta abordagem não interfere no roteamento, tampouco inclui algum atraso na comunicação, mas necessita que seja implementada a decodificação das mensagens BGP para manter sua tabela de rotas coerente com a existente nos roteadores. Surgem algumas limitações na própria captura dos dados, visto que freqüentemente o meio em que circulam as mensagens não é compartilhado, exigindo configurações como “port mirroring” para permitir a captura das mensagens entre roteadores que fazem uso do BGP.
- Sessões interativas: Utiliza scripts que periodicamente fazem login no equipamento, coletando a seguir toda a tabela de roteamento BGP para posterior processamento e interpretação dos dados. Tratando-se de um grande número de rotas na Internet hoje, a transferência dessas informações de roteamento torna-se um processo que pode sobrecarregar a rede e aumentar a utilização da CPU do equipamento em monitoramento.
- Participação na malha de roteamento: Esta é uma das abordagens muito utilizadas por sua flexibilidade e escalabilidade. Baseia-se em participar na malha de roteamento, ou seja: uma estação de trabalho com um software que implementa o protocolo BGP, mantém uma sessão BGP com o roteador a ser monitorado. Esse nodo atua somente no recebimento dos anúncios, sem enviar nenhum anúncio. Dessa forma, uma vez tendo a tabela BGP e a possibilidade de análise das mensagens BGP, pode ser realizado o processamento necessário para o controle efetivo do BGP. Como ponto negativo, existe a necessidade de utilizar uma estação de trabalho específica, dedicado a este fim. Outro ponto é que uma vez que se possua uma tabela de rotas BGP completa, deve existir um software que faça o dump da tabela BGP, processando-a para fornecer os dados para o monitoramento. Por fim, a interface com o usuário é geralmente feita via web, não obedecendo a nenhum padrão pré-definido, como o SNMP. Dois projetos amplamente conhecidos que utilizam essa abordagem são o RouteViews [3] e o BGP Table Data da Telstra [4]. Os dados podem ser consultados e acessados através do site

de cada projeto, permitindo um conjunto de consultas sobre diversos atributos do BGP global. Também esses projetos têm permitido que estudos sobre a agregação de blocos, distribuição de ASes e total de anúncios BGP sejam produzidos e disponibilizados para toda a comunidade. No entanto, é um abordagem complexa pela estrutura que deve ser utilizada e pelas ferramentas que devem ser integradas até fornecer os dados para o monitoramento efetivo.

- MIB BGP: Baseia-se em uma solução que é implementada no próprio equipamento que utiliza o protocolo BGP, disponibilizando os dados para monitoração através de uma MIB específica, sendo acessível de forma padrão via SNMP. Os pontos fortes dessa abordagem são sua simplicidade, pois não requer a adição de nenhum outro equipamento ou ferramenta, fornecendo uma forma de acesso padrão. Isso permite que os dados sejam obtidos por qualquer sistema de gerência que faça uso do SNMP. Essa abordagem também não adiciona nenhuma sobrecarga de processamento ao equipamento, visto que como ele já atua na interpretação de mensagens BGP, das sessões BGP e a própria tabela BGP, o processamento adicionado para armazenar os dados da MIB é desprezível [5].

Como se pode notar, a abordagem utilizando a MIB BGP é a mais simples e a que apresenta uma relação custo x benefício melhor, visto que já vem implementada na maioria dos equipamentos de redes que utilizam o protocolo BGP.

A partir do equipamento que utiliza o protocolo BGP, geralmente o próprio roteador de borda de um sistema autônomo, é possível obter um conjunto de objetos pertencentes a MIB BGP. A MIB BGP é definida pela RFC 1657 [6]. Basicamente, seus objetos podem ser divididos em dois grupos. O primeiro deles disponibiliza informações sobre cada sessão BGP e o segundo grupo fornece informações sobre cada prefixo contido na tabela de roteamento BGP. Alguns exemplos de objetos desta MIB são apresentados na figura 1 abaixo:

BGP Peer Table : Informações sobre as sessões BGP:

```
bgpPeerState OBJECT-TYPE
                    SYNTAX     INTEGER {
                                        idle(1),
                                        connect(2),
                                        active(3),
                                        opensent(4),
                                        openconfirm(5),
                                        established(6)
                               }
                    MAX-ACCESS read-only
                    STATUS     current
                    DESCRIPTION
                            "The BGP peer connection state."
                    ::= { bgpPeerEntry 2 }

bgpPeerRemoteAs OBJECT-TYPE
                    SYNTAX     INTEGER (0..65535)
                    MAX-ACCESS read-only
                    STATUS     current
                    DESCRIPTION
                            "The remote autonomous system number."
                    ::= { bgpPeerEntry 9 }

bgpPeerFsmEstablishedTime OBJECT-TYPE
                    SYNTAX     Gauge32
                    MAX-ACCESS read-only
                    STATUS     current
                    DESCRIPTION
                            "This timer indicates how long (in
                            seconds) this peer has been in the
                            Established state or how long
```

```
                            since this peer was last in the
                            Established state.  It is set to zero when
                            a new peer is configured or the router is
                            booted."

                    ::= { bgpPeerEntry 16 }
```

BGP Received Path Attribute Table : Informações sobre os anúncios e seus atributos da tabela BGP:

```
bgpPathAttrDestNetwork OBJECT-TYPE
                    SYNTAX     IpAddress
                    MAX-ACCESS read-only
                    STATUS     obsolete
                    DESCRIPTION
                            "The address of the destination network."
                    ::= { bgpPathAttrEntry 2 }

bgp4PathAttrPeer OBJECT-TYPE
                    SYNTAX     IpAddress
                    MAX-ACCESS read-only
                    STATUS     current
                    DESCRIPTION
                            "The IP address of the peer where the path
                            information was learned."
                    ::= { bgp4PathAttrEntry 1 }

bgpPathAttrASPath OBJECT-TYPE
                    SYNTAX     OCTET STRING (SIZE (2..255))
                    MAX-ACCESS read-only
                    STATUS     obsolete
                    DESCRIPTION
                            "The set of ASs that must be traversed to
                            reach the network.  This object is
                            probably best represented as SEQUENCE OF
                            INTEGER.  For SMI compatibility, though,
                            it is represented as OCTET STRING.  Each
                            AS is represented as a pair of octets
                            according to the following algorithm:

                                first-byte-of-pair = ASNumber / 256;
                                second-byte-of-pair = ASNumber & 255;"
                    ::= { bgpPathAttrEntry 4 }

bgp4PathAttrIpAddrPrefix OBJECT-TYPE
                    SYNTAX     IpAddress
                    MAX-ACCESS read-only
                    STATUS     current
                    DESCRIPTION
                            "An IP address prefix in the Network Layer
                            Reachability Information field.  This object

                            is an IP address containing the prefix with
                            length specified by
                            bgp4PathAttrIpAddrPrefixLen.
                            Any bits beyond the length specified by
                            bgp4PathAttrIpAddrPrefixLen are zeroed."
                    ::= { bgp4PathAttrEntry 3 }
```

Figura 1: Exemplos de objetos encontrados na MIB BGP em ASN.1.

Baseado nestes recursos disponíveis pela MIB BGP passou-se a buscar um cenário em que o monitoramento do BGP fosse bastante crítico e onde os recursos deveriam ser otimizados. Pensou-se então no Ponto de Troca de Tráfego do Rio Grande do Sul (RSiX) [7], que por possuir diversos sistemas autônomos presentes, seria um ótimo cenário para a aplicação do projeto.

Assim sendo, antes de apresentarmos as necessidades de gerência encontradas em um PTT, extensíveis a qualquer sistema autônomo da Internet, estaremos de forma breve apresentando algumas características relevantes ao seu uso em PTTs.

De forma resumida, PTTs tratam-se de pontos onde um conjunto de ASs se conectam localmente afim de trocar tráfego, visando diminuir o tempo de acesso e seus gastos com conectividade a longa distância, que são considerados hoje fatores críticos para sobrevivência e sucesso de sistemas autônomos.

Perante tais benefícios, o número de PTTs tem aumentado consideravelmente. No Brasil existem mais de 6 PTTs, sendo que o primeiro destes foi implementado em 1998 pela ANSP [8] e no ano de 2000 o Ponto de Troca de Tráfego do Rio Grande do Sul (RSiX) iniciou sua operação. Outros PTTs mais recentes também em operação, administrados pela Rede Nacional de Pesquisa (RNP) ou seus pontos de presença, são eles: o PRiX [9] o FiX [10]. Esse crescimento é reforçado pela orientação do Comitê Gestor da Internet-BR [11].

Os pontos de troca de tráfego são formados basicamente por um switch que atua como comutador, interligando roteadores de diferentes sistemas autônomos com o intuito de trocar tráfego. As sessões BGP entre os participantes de um sistema autônomo podem ser estabelecidas diretamente entre os participantes do PTT, formando uma relação de troca de tráfego bilateral, ou pode existir um componente no PTT chamado de Route Server. Tal componente faz com que as sessões BGP sejam estabelecidas diretamente com o Route Server e este anuncie aos demais ASes. Essa relação é definida como troca de tráfego multilateral, já que os Route Servers divulgam os anúncios a todos os participantes que pertencem a determinado Acordo de Tráfego Multilateral (ATM). Grande parte dos PTTs existentes no Brasil adota a política de troca de tráfego multilateral.

Na figura 2 é apresentada a topologia de um PTT. São apresentados dois Route Servers (RSD1 e RSD2), onde cada participante estabelece sessões BGP com estes, a fim de anunciar seus prefixos e receber os anúncios dos demais participantes. Vale lembrar que apenas o tráfego do protocolo BGP passa pelos Route Servers. O tráfego trocado entre os participantes passa diretamente entre os roteadores dos participantes envolvidos na troca de tráfego. O componente Looking Glass (LG) é utilizado para verificar os anúncios e conectividade do PTT por parte dos participantes e por possíveis interessados na entrada do PTT. Em geral é permitida a consulta dessas informações via uma interface WEB.

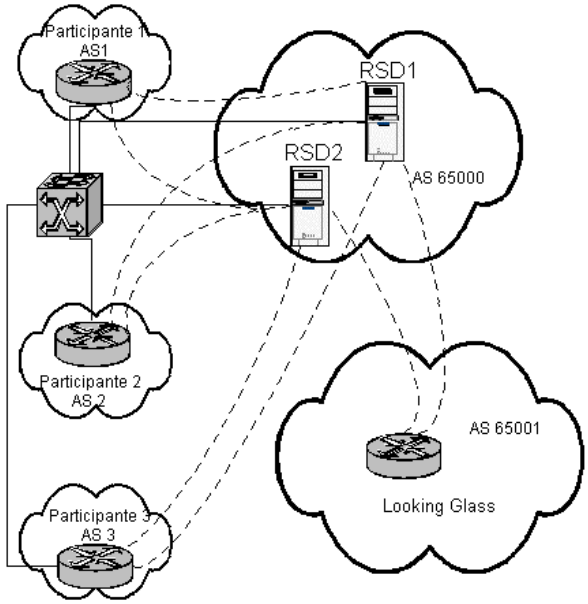


Figura 2: Topologia de um PTT

Quanto ao acesso aos equipamentos do PTT, cada participante é responsável pela configuração e suporte ao roteador presente no PTT, não sendo acessível por parte da equipe de administração do PTT. Neste contexto, apenas os Route Servers, o Switch e o Looking Glass estão sob o domínio da equipe de administração do PTT. Isso significa que as informações que poderiam ser utilizadas para a gerência do PTT devem ser coletadas em um destes três componentes. Cada um destes componentes possui as seguintes informações:

- Switch: Atuando em nível 2, este componente pode fornecer o volume de tráfego de cada participante, já que ele faz o papel de comutador da rede local do PTT. Essas informações são obtidas através da MIB II [12].
- Looking Glass: Este componente possui todos os anúncios presentes no PTT, visto que possui sessões BGP com os Route Servers. Isso poderia ser obtido através da MIB-BGP, caso o equipamento suporte tal recurso.
- Route Servers: Possui todas as informações que podem ser fornecidas pelo Looking Glass, com adição do estado das sessões BGP de cada participante, já que ele próprio estabelece sessões com todos os participantes. Estas informações também são acessíveis via MIB-BGP, desde que o componente suporte tal recurso. No caso do RSiX, é utilizado o software Zebra [13] que tem suporte a MIB-BGP e torna possível o acesso a essas informações.

2. Necessidade de gerência de um PTT x Recursos da MIB BGP

A partir da definição das possíveis fontes de informação da administração do PTT, enumeram-se algumas informações relevantes do protocolo BGP que poderiam ser utilizadas para a efetiva administração do PTT. Algumas delas podem ser encontradas em [14] [15] [16]. São elas:

- Contabilização dos anúncios de cada participante e do número total de anúncios do PTT. Isso facilita a relação dos anúncios com o padrão de tráfego de cada participante, além de permitir que seja analisado o crescimento do PTT.
- Contabilização dos prefixos anunciados no PTT classificados por seu tamanho, afim de permitir que seja fornecido um panorama específico dos anúncios do PTT de cada participante e seu crescimento. Também auxilia o controle e histórico da ocorrência de anúncios muito específicos, de acordo com as regras do PTT.
- Monitoramento das sessões BGP como um todo, ou seja, contabilização do número de sessões agrupadas por seu estado, visando identificar facilmente problemas isolados de instabilidades globais.

Através do acesso pela console dos Route Servers, algumas dessas informações poderiam ser obtidas facilmente, mas a necessidade é que tais informações estejam disponíveis através de uma interface SNMP para permitir que diferentes ferramentas possam obtê-las e analisá-las, permitindo também alguma forma de histórico para esses valores.

A partir desses pontos mais importantes para monitoração, observou-se que os objetos da MIB BGP não forneciam de forma direta tais informações. No entanto, como já foi visto que a abordagem de busca de informações utilizando a MIB BGP era a mais adequada, os esforços foram concentrados em propor um sub-agente que atuaria em um nível acima da MIB BGP, fornecendo as informações citadas acima, fazendo uso e processamento APENAS dos objetos existentes na MIB BGP. Isso seria um protótipo que serviria para validar e comprovar se tais informações poderiam ser incluídas nos objetos padrão da MIB BGP. E dessa forma, a partir do próximo item, serão demonstradas as características e a forma em que o sub-agente foi implementado.

3. Protótipo

Analisando as fontes de informação e as necessidades listadas anteriormente, apresenta-se na figura 3 a interface do sub-agente chamado de BGPe. Em relação a MIB BGP, caso os objetos requisitados sejam pertencentes a ela, o acesso será direto, sem passar pelo sub-agente. Apenas as requisições de objetos extras são processados pelo sub-agente, que se encarrega de recebê-las, acessando a MIB BGP em busca de informações úteis, processando-as e retornando os valores ao requisitante. No caso da ilustração, o requisitante é a própria estação de gerência. A interface do sub-agente, da mesma forma que é com a MIB BGP, é feita através de SNMP, por intermédio do software Net-SNMP[17].

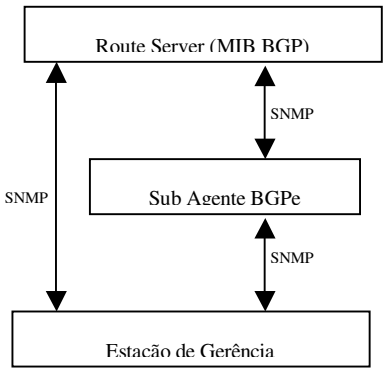


Figura 3: Cenário do sub-agente BGPe.

Os objetos extras fornecidos pelo sub-agente são apresentados abaixo:

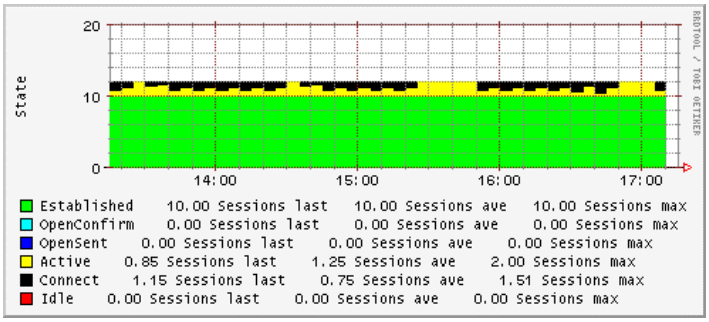
- BGPeTotalPathGlobal: Total de anúncios, globais ao PTT;
- BGPeLenGlobal: Total de anúncios do PTT agrupados por seu tamanho, a partir da especificação do tamanho do bloco desejado em notação CIDR.
- BGPeStates: Total de sessões BGP de um dos 6 estados possíveis definidos da máquina de estados do protocolo BGP[2].
- BGPeTotalPath: Total de anúncios agrupados por cada participante do PTT.
- BGPeLen: Total de anúncios de determinado tamanho, agrupados também por cada participante do PTT.

A implementação deste sub-agente foi feita em linguagem C, adaptado como MIB estendida ao NET-SNMP.

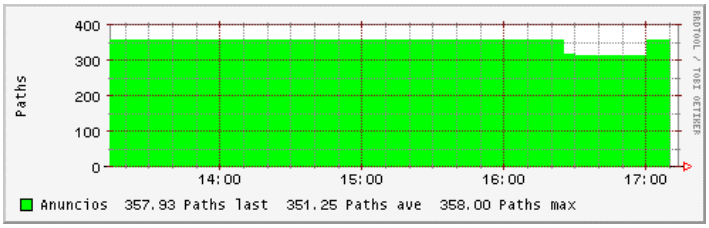
3.1. Resultados obtidos

A partir da utilização deste sub-agente e do software RRDTool [18] foi possível criar alguns gráficos que vem sendo utilizados para a administração do RSiX. Tais informações tem auxiliado em 90% dos problemas envolvendo participantes do PTT. Abaixo são exibidos alguns exemplos:

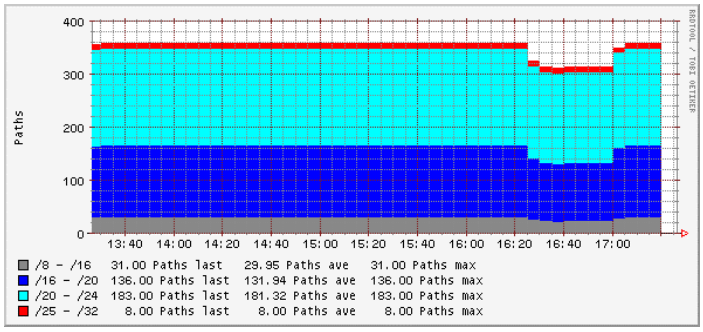
Número de sessões BGP agrupadas por seu estado



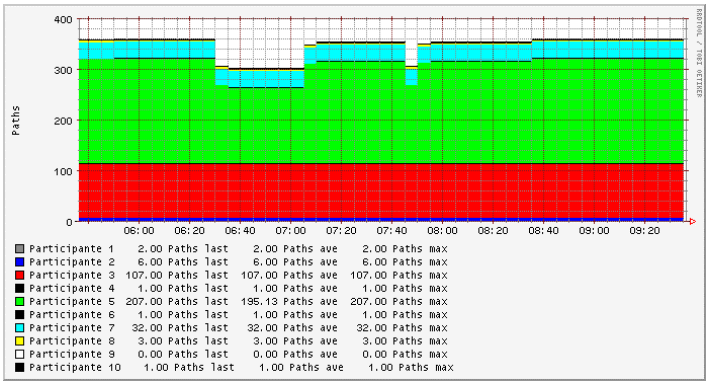
Total de anúncios da tabela BGP



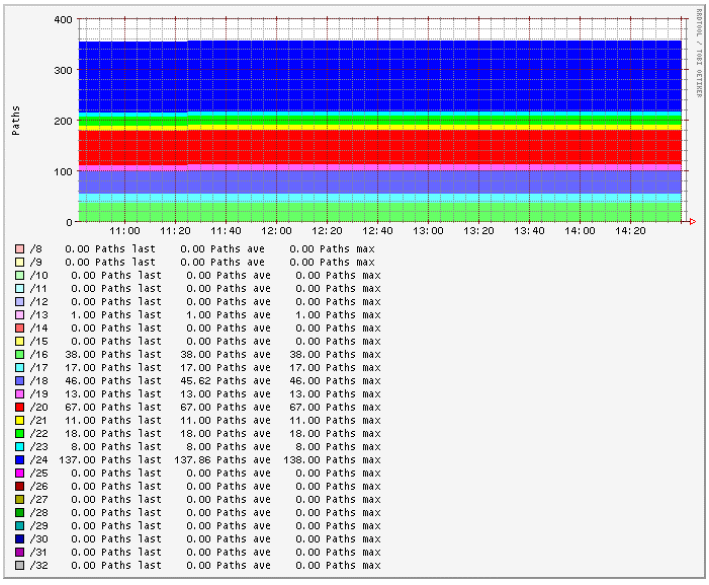
Contabilização de anúncios BGP de acordo com sua profundidade



Total de anúncios de cada participante do PTT



Total de anúncios do PTT classificados pelo seu tamanho



3.2 Limitações do protótipo

Tratando-se de um protótipo inicial, baseado na obtenção de informações via SNMP da MIB BGP, o sub-agente BGPe apresenta limitações no que tange ao número de anúncios da tabela BGP, visto que ele recebe as requisições e faz acesso a MIB BGP, buscando um conjunto de

objetos, processando-os e finalmente retornando o resultado a quem requisitou. Acima de 1000 anúncios, o sub-agente passa a ter uma latência considerável, se comparado com o tempo de acesso direto a MIB BGP. Em relação à demais funcionalidades, o sub-agente apresenta um comportamento muito bom.

4. Proposta de modificação da MIB BGP

Como foi citado no item anterior, os equipamentos que implementam o protocolo BGP podem facilmente fornecer, além dos dados da MIB BGP, as informações adicionais demonstradas no sub-agente. O esforço para tal inclusão é relativamente simples, visto que os referidos equipamentos já manipulam as mensagens do protocolo e a tabela de anúncios BGP, fornecendo também diversas informações. A figura 4 mostra um exemplo de dados obtidos via console em um roteador Cisco, encontrada também em equipamentos de outros fabricantes. Um detalhe importante é que o total de anúncios de cada participante, por exemplo, implementado pelo sub-agente, já é fornecido via console, através da última coluna da figura 4, mas não é fornecido pela MIB BGP. Isso significa que para incluir tal informação na MIB BGP seria apenas necessário instanciar tal variável como objeto da MIB.

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	**State/PfxRcd**
200.132.1.249	4	65000	53849	54569	25989698	0	0	3w4d	**612**
200.143.254.3	4	1916	4895398	1858820	25990356	0	0	1w2d	**454**
200.143.254.5	4	1916	52679	1856731	25990356	0	0	1w2d	**12**
200.143.254.8	4	1916	2290646	1859265	25990356	0	0	1w2d	**576**
200.143.254.12	4	1916	111472	1854905	25990356	0	0	1w0d	**10**
200.143.254.13	4	1916	12797636	1858071	25990356	0	0	1w2d	**2133**
200.143.254.17	4	1916	181193	1859208	25990356	0	0	1w2d	**21000**

Figura 4: Exemplo de status e informações relevantes sobre sessões BGP obtidas em roteadores Cisco.

Neste caso, a adição de novos objetos na MIB não teria grande impacto na performance do produto e principalmente tornaria a MIB BGP uma opção ainda mais consolidada na gerência efetiva do protocolo BGP, fornecendo ainda mais objetos úteis para tal tarefa.

Não se pretende incluir um grande número de objetos na MIB, pois não é o objetivo desta MIB fornecer um mecanismo único para gerência do BGP, mas apenas disponibilizar os objetos demonstrados no sub-agente. Dessa forma, a MIB BGP poderá ser um recurso ainda mais útil para o monitoramento do BGP, sem a adição de nenhum outro componente na gerência. Tais informações mostrarão de forma muito contundente as mudanças no roteamento BGP, sinalizando a equipe de gerência para tomar as ações necessárias.

5. Conclusões

Não se pretende aqui fazer com que a MIB BGP substitua o acesso a console de roteadores, fornecendo subsídios para a detecção de todos os problemas do BGP, mas o intuito é estender seu conjunto de objetos para sinalizar anormalidades e em caso necessário, a intervenção da equipe de suporte.

Espera-se que no futuro tais objetos aqui demonstrados por intermédio do sub-agente possam ser incluídos na MIB padrão do BGP, através de discussões no IETF, sendo então

implementados pelos fabricantes de equipamentos. Essa implementação pelos fabricantes resolveria todos os problemas de performance que o sub-agente enfrentou, como já foi explicado anteriormente e se apresentaria como uma solução não só para a nossa necessidade, mas para um universo de sistemas autônomos e pontos críticos da Internet. Essa extensão na MIB BGP permitiria uma nova e efetiva forma de gerência de roteamento da malha BGP existente em diversas instituições.

6. Referências bibliográficas

[1] A Border Gateway Protocol 4 (BGP-4) – RFC 1771 – on line – 2003 - http://www.ietf.org/rfc/rfc1771.txt

[2] Sam Halabi, Danny Mcperson. Internet Routing Architectures, Second Edition. Indianapolis – USA : Cisco Press, 2000

[3] University of Oregon Route Views Project – on line – 2003 - http://www.routeviews.org/

[4] BGP Table Data – Telstra – on line – 2003 - http://bgp.potaroo.net/

[5] Stallings, William. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. Reading: Addison-Wesley, c1999. 619 p. : il.

[6] Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2 – RFC 1657 - on line – 2003 - http://www.faqs.org/ftp/rfc/rfc1657.txt

[7] RSIX - Ponto de Troca de Tráfego Internet – on line - 2003 – www.rsix.tche.br

[8] ANSP – Ponto de Troca de Tráfego da ANSP – on line – 2003 – http://www.ansp.br

[9] PRIX – Ponto de Troca de Tráfego do Paraná – on line – 2003 - http://prix.pop-pr.rnp.br/

[10] FIX - Federal Interconection of Brasilia – on line – 2003 – http://www.rnp.br

[11] Comitê Gestor Internet/BR – Operação e Administração de PTTs no Brasil – on line – 2000 - http://www.cg.org.br/grupo/operacao_ptt_v1.1.htm

[12] Management Information Base for Network Management of TCP/IP-based internets: MIB II - RFC 1213 – on line - http://www.faqs.org/ftp/rfc/rfc1213.txt

[13] GNU Zebra – routing software – on line – 2003 – http://www.zebra.org

[14] Segurança em Pontos de Troca de Tráfego – 14ª Reunião do Grupo de Trabalho em Engenharia de Redes – GTER 14 – 2001 – on line - ftp://ftp.registro.br/pub/gter/gter14/aspectos_sec_ptt_bertholdo.ppt

[15] Controle do Protocolo BGP em PTT´s – 15ª Reunião do Grupo de Trabalho em Engenharia de Redes – GTER 15 – 2003 – on line – ftp://ftp.registro.br/pub/gter/gter15/gter15-bgpe-rsix.pdf

[16] Sub-agente para Controle BGP na RNP – Workshop RNP2 – Simpósio Brasileiro de Redes – SBRC – 2003 – Natal – RN -= on line - http://www.rnp.br/_arquivo/eventos/4wrnp2/sacbr01.pdf

[17] NetSNMP Software – The Net SNMP Project Home Page – on line – 2003 – http://www.netsnmp.org

[18] RRD Tool Software – on line – 2003 – http://www.rrdtool.com