ALEXANDRE JOSÉ BARBIERI DE SOUSA

Implementação de um PTT para comutar tráfego entre sistemas autônomos.

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, para obtenção do título de Mestre em Engenharia da Computação. Área de concentração: Redes de Computadores.

São Paulo

2004

ALEXANDRE JOSÉ BARBIERI DE SOUSA

Implementação de um PTT para comutar tráfego entre sistemas autônomos.

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, para obtenção do título de Mestre em Engenharia da Computação. Área de concentração: Redes de Computadores.

Orientador: Dr. Antonio Luiz Rigo

São Paulo

2004

Sousa, Alexandre José Barbieri de
Implantação de um PTT para comutar tráfego entre sistemas autônomos./ Alexandre José Barbieri de Sousa. São Paulo, 2004.
136p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores

Orientador: Prof. Dr. Antonio Luiz Rigo

1. Ponto de troca de tráfego (redes) 2. Protocolo BGP 3. Protocolo de roteamento 4. Servidor de roteamento Zebra 5. Servidor de roteamento Gated 6. Internet 7. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Centro de Aperfeiçoamento Tecnológico II. Título

CDU 004.738.5.057.4(043)
S725i

Agradecimentos

Ao meu orientador, Professor Doutor Antonio Luiz Rigo, cuja paciência contribuiu para a organização das idéias e a melhor forma de expressá-las.

Ao professor Dr. Sérgio Takeo Kofuji, pela sabedoria e precisão nos detalhes.

Ao professor Dr. Prof. Dr. Enrico Giulio Franco Polloni, pela colaboração.

À minha querida esposa Andrea Aumond, pelo incentivo e excelentes sugestões.

À Diveo Telecomunicações do Brasil, que me permitiu a realização deste trabalho, e especialmente aos colegas de trabalho João Batista Toni, Átila de Almeida Carvalho e Laurence Stendard, pelas sugestões e confiança.

Àqueles a quem dedico muito amor - meus pais Jair e Eneida, e minha avó Lenora - que não mediram esforços no apoio à minha formação pessoal e cultural.

Aos funcionários do Instituto de Pesquisas Tecnológicas de São Paulo - IPT/USP, Adilson, Éster, Mary e, especialmente, ao coordenador e professor do mestrado, Dr. Mário Yoshikazu Miyake.

RESUMO

Sousa, Alexandre José Barbieri. Implementação de um PTT para comutar tráfego entre sistemas autônomos.Trabalho final apresentado ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, para obtenção do título de Mestre em Engenharia da Computação. São Paulo, 2004.

A Internet não pára de conquistar novas empresas e mentes, ocupando espaços cada vez mais amplos na vida das pessoas, acomodando tecnologias de comunicação emergentes e superando todas as expectativas de crescimento possíveis de ser definidas em projetos. Diante desse fato, qualquer contribuição que otimize o uso da banda da rede adquire enorme importância.

Com base nessa premissa, desenvolveu-se o processo de construção de um PTT com o intuito de adquirir e disponibilizar conhecimento que permita criar e modificar um modelo de PTT e, ainda, selecionar um software de código aberto para utilizá-lo em um ponto de troca tráfego existente.

Os PTT´s surgiram com as primeiras iniciativas de expansão da Internet, possibilitando ganhos significativos em termos de qualidade de acesso e redução de custos com *backbone*. Quando os provedores os utilizam corretamente, consegue-se caminhos alternativos (redundância) mais curtos entre duas localidades, possibilitando uma economia significativa de *links* para Internet.

Esta pesquisa se inicia com a revisão da literatura sobre o PTT, do protocolo de roteamento BGP e dos servidores de roteamento Gated e Zebra. Familiarizado com esses assuntos, o leitor poderá iniciar a leitura pelo capítulo 4. O núcleo do trabalho foi realizado em duas fases distintas:

- na primeira, realizaram-se dois experimentos para comprovar a funcionalidade da troca de rotas e dos filtros de anúncios oferecidos pelo Zebra. Simulou-se um PTT com endereços e rotas fictícias;
- na segunda fase, tratou-se do planejamento, migração e otimização, para Zebra, do servidor de roteamento de um PTT em produção.

O protocolo de roteamento BGP foi explorado com a finalidade de otimizar a política de roteamento e aumentar o tráfego trocado no PTT, ou seja, utilizar a estrutura de forma mais eficaz. A configuração do servidor Gated pré-existente no PTT – e em operação – foi adaptada para o servidor Zebra implementado em um laboratório, onde se simulou o ambiente de produção com dois participantes.

A migração da plataforma de servidor de roteamento Gated para Zebra foi executada sem afetar a operação do PTT, e melhorou a interatividade do usuário com a estrutura, permitindo o ajuste de novas políticas de roteamento e de segurança.

Com base nos experimentos realizados, na migração e na observação do PTT em produção, foram propostas diretrizes que ajudam na formulação de um modelo de construção e funcionamento do PTT. Elas, resumidamente, abordam informações do *switch*, do servidor de roteamento, dos participantes, do endereçamento, dos tipos de acordos, do roteamento, da segurança e do gerenciamento no PTT.

Palavras-chave: PTT; servidor de roteamento; Zebra; Gated; BGP; roteamento; tráfego; política de roteamento; anúncios; filtros; rotas; Internet; *links*; protocolo de roteamento.

ABSTRACT

Sousa, Alexandre José Barbieri. Implementation of a NAP to traffic switch between autonomous systems, based on a Master´s Thesis in Computer Engineering, presented at the Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT. São Paulo, 2004.

The Internet keeps on conquering new companies and new minds, playing a bigger and bigger role in people's lives, accommodating emergent communication technologies and overcoming all expectations of growth that are possible to be defined in projects. Consequently, any contribution that optimizes the use of the network bandwidth becomes greatly important.

Based on this premise, a process was developed in order to acquire and offer knowledge that allows to create and modify a model of NAP (Network Access Point) and, still, select an open code software to use it as an exchange point of existing traffic.

The use of NAPs (Network Access Points) began when the Internet started to spread, and it enabled significant improvements in the quality of access and reduction of backbone costs. When providers use them correctly, they get shorter alternative routes (redundancy) between locations, enabling significant savings in Internet links.

This work began with a review of the literature regarding NAP, BGP routing protocol and Gated and Zebra servers. If the reader is already familiarized with these subjects he/she can go directly to chapter 4. The core of this study has two distinct phases:

- In the first phase, two experiments were performed to prove the functionality of rout changing and of advertisement filters offered by Zebra. A NAP was simulated with fictitious addresses and routs
- In the second phase, planning, test and migration, to Zebra from a Gated routing server of a NAP in production, were made.

The BGP routing protocol was explored in order to optimize the routing policy and increase the NAP traffic exchange, that is, using the structure in a more effective way. The pre-existing and operating configuration of the Gated server at the NAP was adapted to the Zebra server implemented in a laboratory, where an environment of production with two participants was simulated.

The platform migration of the routing server, from Gated to Zebra was executed without affecting the NAP operation, and it improved the interactivity of the user and the structure, allowing the adjustment of new routing and security policies.

Guide lines to formulate a NAP construction and operating model were proposed, based on the performed experiments, the migration and observation of a NAP in production. These guide lines, in short, employ information from the switch, routing server, participants, addressing, kinds of protocols, routing, security and management at the NAP.

Key-words: NAP; router server; Zebra; Gated; BGP; routing ; traffic; routing police; announce; filters ; routes; Internet; links; routing protocol.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARIN	American Registry for Internet Numbers
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
BGP	Border Gateway Protocol
CIDR	Classless Inter Domain Routing
DoD	Department of Defense
DNS	Domain Name System
EGP	External Gateway Protocol
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
IGP	Internal Gateway Protocol
IP	Internet Protocol
ISP	Internet Service Provider
ISIS	Intermediate System to Intermediate System
MED	Multi Exit Discriminator
NAP	Network Access Point
NMS	Network Management System
NSF	National Science Foundation
NSFNET	National Science Foundation Network
OSPF	Open Shortest Path First
PTT	Ponto de Troca de Tráfego
RA	Router Arbiter
RFC	Request for Comment
RIP	Routing Information Protocol
RS	Router Server
SR	Servidores de Roteamento
SNMP	Simple Network Management Protocol
TCP	Transfer Control Protocol

SUMÁRIO

Capítulo 1. INTRODUÇÃO

A utilização da Internet, seja por *e-mail, sites, e-commerce, banking,* hoje em dia é tão importante quanto o uso da rede telefônica e elétrica. O número de transações que exigem desempenho (rapidez) e disponibilidade aumentam cada vez mais na Internet.

O artigo de Prado (2002) revela como as pessoas dependem da Internet para viver.

> "Quanto maior for a penetração da Internet nas empresas e na vida das pessoas, maior a dependência que esse canal de comunicação acaba gerando. Quantos de nós já deixamos para pagar uma conta no dia de seu vencimento, confiando exclusivamente no sistema de Internet Banking."

Desde o surgimento da Internet existe uma grande preocupação com o congestionamento dos *links* entre os provedores. Para diminuir o congestionamento, tornou-se fundamental a criação do Ponto de Troca de Tráfego- PTT, ou seja, uma rede de alta velocidade, em que os roteadores podem se conectar com a finalidade de troca de tráfego dos seus clientes.

Muitos provedores utilizam Ponto de Troca de Tráfego - PTT. A utilização correta de um PTT permite ganhos de tempo de entrega pelo uso de caminhos alternativos (redundância) mais curtos entre as localidades, possibilitando uma economia significativa em *links* Internet.

Atualmente, existem PTT(s) públicos e privados, criados por instituições nacionais e internacionais, que diferem nos seus modelos de construção. Explorando esta perspectiva, o presente trabalho tem como preocupação realizar o processo da construção de um PTT que pode ser implementado de várias formas e proporcionar uma administração distinta a cada organização, de acordo com o modelo de negócio do participante.

1.1 Objetivo

Construir um PTT para alcançar os seguintes objetivos específicos:

1.1.2 Objetivos específicos

- Realizar experimentos com servidores de roteamento Zebra, que permitirão testar a funcionalidade do PTT, ou seja, garantir a troca de rotas e aplicação dos filtros dos anúncios.
- Planejar e migrar o servidor de roteamento de um PTT em produção, visando substituir o servidor Gated pelo Zebra, e avaliar as vantagens da migração.
- Explorar o protocolo BGP para ajustar o roteamento do PTT e dos participantes. O entendimento e domínio do protocolo permitirão otimizar a troca de tráfego no PTT.
- Definir diretrizes para a implementação de um PTT.

1.2 Justificativa da escolha do assunto

O tema escolhido "a análise do uso do PTT na comutação entre sistemas autônomos" justifica-se pelo crescimento da Internet e, conseqüentemente, pela necessidade de construir uma estrutura paralela para os provedores trocarem tráfego dos seus clientes, gerando também economia em banda. Pode-se ver, no artigo "Abranet cria um novo ponto de tráfego" (2001), uma justificativa do uso de PTT.

> ".....que a nova solução de acesso à Internet realiza a troca de tráfego por meio de conexões dedicadas, de forma direta e controlada, o que permite aos participantes – provedores de Internet, operadoras de telecomunicações e empresas associadas – melhoria na qualidade de acessos e redução significativa dos custos com *backbone*."

É possível constatar, por meio da publicação do PTT da Fapesp (ver ANEXO A), os provedores que estão participando do PTT. Pode-se ver também, nas estatísticas (ver ANEXO B), a quantidade de dados trocada entre os participantes.

Esses fatores mostram a importância do uso de um PTT, justificando a pesquisa de seu funcionamento e construção.

O presente trabalho permitiu realizar a análise e migração de um servidor de roteamento de um PTT existente.

Justifica-se, ainda, pela possibilidade de a pesquisa contribuir e despertar a consciência dos demais provedores quanto a participar e/ou construir PTT privados.

1.3 Organização do trabalho

Para atender aos objetivos da pesquisa, o trabalho está estruturado em seis capítulos: introdução, fundamentação teórica no capítulo dois e três, método e material de pesquisa, análise dos resultados e considerações finais.

No primeiro capítulo, intitulado introdução, formula-se o problema, a justificativa do trabalho, o objetivo geral e os objetivos específicos, bem como a estrutura do trabalho.

No capítulo dois, realiza-se a revisão da literatura, apresentando o contexto em que o PTT está inserido, mostrando o início dos PTT(s), a sua definição, seus participantes, o projeto Routing Arbiter, a definição e o uso de servidores de roteamento e a caracterização do uso do PTT com base na disponibilidade, capacidade, escalabilidade e o seu tráfego.

No capítulo três, em seqüência à revisão literária, explica-se o que é um *Autonomous System*, um breve conceito de roteamento e o protocolo BGP: sua definição, operação e depuração. Ainda neste capítulo, apresentam-se as configurações do BGP dos servidores de roteamento Zebra e Gated usados no trabalho.

No capítulo quatro, define-se o método de pesquisa utilizado, bem como os laboratórios a serem executados e os equipamentos necessários para a realização dos testes.

No capítulo cinco, são apresentados os resultados dos experimentos e os objetivo específicos:

- Funcionalidade do PTT usando o servidor de roteamento Zebra.

- Migração do Gated para Zebra.
- Estruturação da política de roteamento no PTT.
- Diretrizes para construção para o PTT.

No capítulo seis, estão expostas as considerações finais.

Capítulo 2. O USO DO PTT NA TROCA DE TRÁFEGO ENTRE OS SISTEMAS AUTÔNOMOS

2.1 O início dos PTTs

Para entender a história dos PTTs, é necessário fazer uma retrospectiva na evolução da Internet.

O embrião da Internet surgiu de uma iniciativa do DoD (Departamento de Defesa) dos EUA, que necessitava de uma rede de comunicação segura, capaz de sobreviver a ataques nucleares. No final de 1960, o DoD solicitou à ARPA experimentos conectando a rede de computadores a universidades e empresas privadas.

Em dezembro de 1969, a rede experimental de pesquisas tinha quatros nós conectados por circuitos de 56k. A nova tecnologia teve grande sucesso, e proporcionou a criação de duas redes militares similares; uma nos Estados Unidos e a outra na Europa.

O projeto ARPA estimulou a pesquisa de redes de satélites e o envio de pacotes por redes sem fio, criando, assim, múltiplas redes e protocolos de acesso.

Posteriormente, milhares de *hosts*, usuários e, conseqüentemente, redes privadas como universidades e governos, já estavam conectados na Arpanet. Contudo, foi proibido o uso da Internet para finalidades comerciais. A Arpanet começou a ter problemas de crescimento, pois já estava com seus *links* congestionados. Devido a isso, a National Science Foundation (NSF) começou a desenvolver a NSFNET. A NSFNET foi composta por múltiplas redes e vizinhos conectados a um *backbone* maior, que formava o seu núcleo (FIGURA 1).

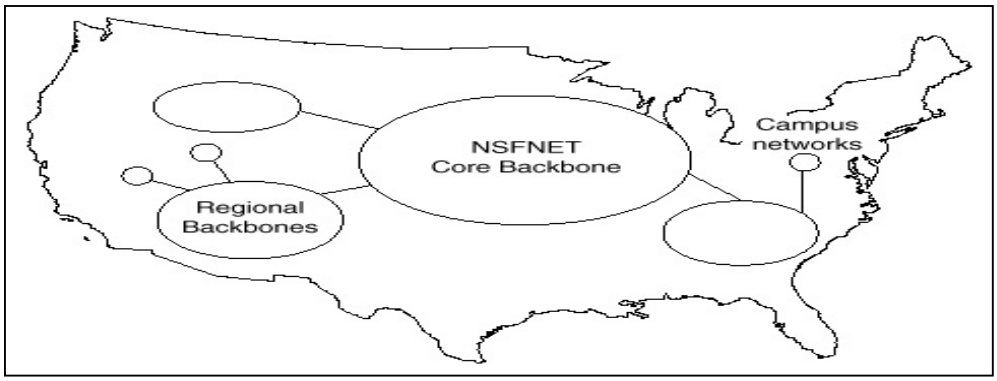


FIGURA 1 - NSFNET Halabi e Mc Pherson (2000).

Em 1986, a NSFNET ampliou sua rede, ligando 6 centros de computação a um *backbone* principal. Os *links* originais de 56k foram migrados em 1988 para circuitos T1(s) (1.544 Mbps) .

Por volta de 1989 ocorre uma das grandes revoluções da Internet, com a invenção da *World Wide Web,* trazendo o conceito do uso de imagem e texto.

Devido ao grande crescimento e congestionamento de seus *links*, a NSF solicitou, por volta de 1991, o *upgrade* dos *links* do *backbone* para circuitos T3(s) (44.736 Mbps).

Em 1993 foi lançado o Mosaic, o primeiro navegador comercial para Internet; que tornou a interface mais amigável e, conseqüentemente, aumentou o seu uso.

Com o intuito de fazer um modelo de Internet mais robusto, em maio de 1993 a NSF solicitou a denominada NSF93-52. Dentre os itens presentes no texto da NSF93-52, destacam-se:

- Criar PTT(s), aos quais os provedores conectem suas redes para trocar tráfego.
- Conectar os PTT(s).
- Estabelecer políticas para conectar os PTT(s).
- Prover servidor de roteamento.
- Prover um banco de dados Routing Arbiter.
- Prover NMS de serviço para gerenciar equipamento.

- Organizar *sites* de acesso e segurança para engenheiros de redes dos provedores.
- Prover expansão e *upgrade* dos PTT(s).

Atualmente, observa-se que o modelo de um PTT espelha-se na solicitação da NSF em 1993.

2.2 O que é um PTT

Um PTT pode ser definido como uma rede de alta velocidade ou um *switch* onde roteadores podem conectar-se a fim de trocar tráfego, segundo Halabi e Mc Pherson (2000).

O artigo "Fapesp transfere operação de ponto de troca de tráfego" (2002) define PTT como um ponto de troca na Internet: "um ponto neutro de interconexão na Internet, onde provedores de acesso, concessionárias de telecomunicações e grandes clientes trocam, de forma direta, tráfego de dados de clientes comuns."

Os participantes de um PTT, que na maioria das vezes são provedores, fazem uso do PTT com o objetivo de trocar tráfego de forma direta entre os participantes e de acordo com a política de roteamento implementada no PTT e nos participantes. Essa política de roteamento é feita por meio da complexidade do protocolo de roteamento BGP, a ser mencionado posteriormente.

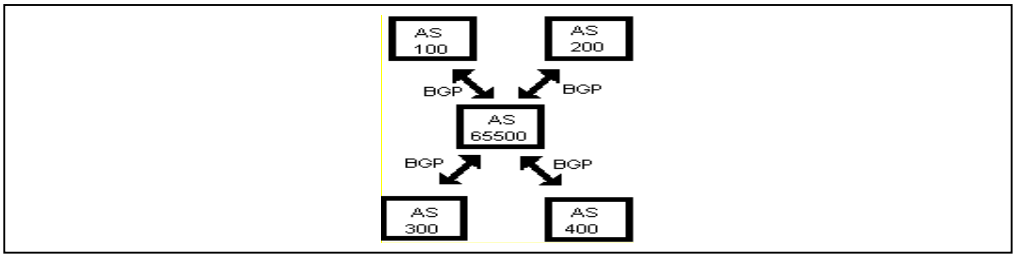


FIGURA 2- Exemplo de troca de tráfego dos participantes

Ao analisar a FIGURA 2, observa-se um PTT central que recebe as rotas de todos os participantes e divulga as rotas aprendidas. É importante ressaltar que o tráfego dos participantes não passa pelo PTT, somente a tabela de rotas trocada é que o faz.

Na mesma figura, vê-se cada participante com seu respectivo *Autonomous System* – AS, conforme Halabi e Mc Pherson (2000). *Autonomous System* é formado pelo "conjunto de roteadores com a mesma política de roteamento e que estão sob um único controle administrativo."

Os *Autonomous Systems - AS* estão ligados numa estrutura de *multiaccess*, na qual todos os participantes estão conectados com todos os participantes, operando como um segmento Ethernet típico.

Caso o participante com o AS 100 necessite acessar o AS 300, o tráfego irá diretamente do AS100 para o AS300, sem passar pelo AS65500 do servidor de roteamento.

2.3 Participantes do PTT

Os candidatos do PTT devem ter conexão permanente com a Internet e possuir um *Autonomous System* - AS. O critério de escolha de um participante pode ser diferente, de acordo com o número de caminhos de um endereço IP dentro do seu AS. Filho (2000)

É importante ressaltar que o PTT não provê conexão para a Internet e não garante a presença ou conectividade de um determinado provedor na Internet.

O PTT troca anúncios entre os participantes, fazendo com que eles aprendam as rotas do PTT, inserindo-as em suas tabelas de roteamento. Cada rota representa um atalho que interliga diretamente um participante aos demais participantes, resultando em ganho na velocidade da troca de tráfego e economia no dimensionamento dos seus *links* de Internet.

2.4 Projeto Router Arbiter

O Router Arbiter – RA, uma das solicitações da NSF usadas na maioria dos PTT(s) existentes atualmente, consiste em um banco de dados de rotas para prover escalabilidade e gerência das redes. Existe um modelo de PTT no qual cada provedor mantém uma conexão direta com os demais provedores.

A desvantagem deste modelo é a necessidade de conexão entre todos os participantes, não sendo possível manter uma administração e gerenciamento centralizado.

No modelo de PTT usado atualmente, todos os participantes são conectados em um sistema central chamado “servidor de roteamento”. O servidor de roteamento manterá um banco de dados com todas as rotas recebidas que serão enviadas de acordo com a política implementada.

Na FIGURA 2, o AS 65500 centraliza todas as rotas e as divulga de acordo com a política de roteamento aplicada pelo administrador do PTT, facilitando a gerência de cada participante.

2.5 Servidor de roteamento

Os servidores de roteamento são computadores executando um software que realiza as funções de troca e processamento de rotas Filho (2000). O servidor de roteamento recebe as rotas, processa-as de acordo com a política de roteamento implementada e, finalmente, as distribui para cada participante. Os servidores de roteamento usam o BGP como protocolo de roteamento.

Um fator muito importante é que os servidores de roteamento não roteiam os pacotes entre as redes conectadas no PTT. Eles usarão a capacidade do BGP de distribuir as rotas com o próximo destino, apontando para o roteador que anunciou a rota. Portanto, o tráfego é trocado diretamente entre os participantes.

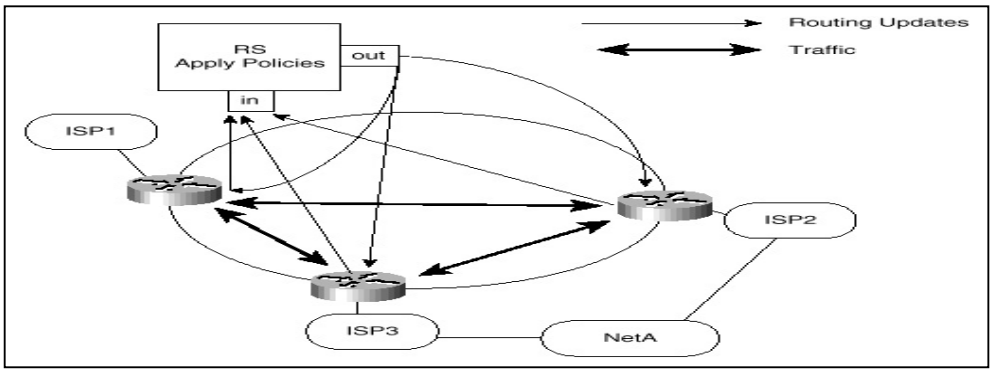


FIGURA 3 - Troca de rotas no servidor de roteamento Halabi e Mc Pherson (2000).

Na FIGURA 3, os Internet Service Providers – ISP(s), ou seja, provedores de Internet anunciam suas redes para o PTT. O servidor de roteamento recebe as rotas, e as divulga para todos os participantes, com um atributo do protocolo de roteamento BGP ajustado para que o tráfego não passe pelo servidor de roteamento. Com isto, além de não sobrecarregar o servidor de roteamento, o PTT torna-se transparente para os usuários.

2.5.1 Tipos de servidores de roteamento

Neste trabalho serão estudados dois servidores de roteamento – o Zebra, um software livre, e o Gated, um software proprietário.

2.5.1.1 Servidor de roteamento Zebra

O Zebra é um software livre, distribuído através da GPL (Licença Pública Geral) GNU, que controla protocolos de roteamento baseados no TCP/IP.

Seu projeto teve início em 1996, com o intuito de gerar um novo tipo de software de roteamento de qualidade.

O Zebra, quando instalado, funciona como um roteador, permitindo a troca de rotas com outros roteadores.

Este software é baseado em uma arquitetura monolítica, que remove o processamento das funções de roteamento da CPU, não-sobrecarregando o servidor.

Suporta o protocolo BGP-4, assim como RIPv1, RIPv2 e OSPF. O Zebra é original em seu projeto, pois tem um processo para cada protocolo, no qual cada módulo pode ser tratado independentemente do outro.

O Zebra tem o seu código aberto para alterações; além disso, não é comercializado. No entanto, já existem empresas que fizeram servidores de roteamento com base no Zebra, incluindo funções adicionais e ganhando os direitos de comercialização do serviço.

2.5.1.2 Servidor de roteamento Gated

O Gated é um software modular, desenvolvido para executar roteamento dinâmico através de serviços e protocolos. Ele foi usado primeiramente para interconectar a NSFNET, com as suas implementações de filtros e roteamento baseados nas políticas aplicadas.

O controle da importação e exportação de informações de roteamento pode ser feito através de um protocolo, controlando-se parâmetros como origem e destino de AS; origem e destino da interface; ou um endereço de destino específico.

O BGP foi o primeiro protocolo de roteamento disponível no Gated. Existem outros protocolos disponíveis no Gated, como IS-IS, OSPF, Ripv1, Ripv2, entre outros.

2.6 Caracterização do uso de um PTT

No uso do PTT é fundamental a preocupação com a confiabilidade da estrutura, a capacidade, a escalabilidade e a estimativa do tráfego trocado. A seguir, uma síntese da caracterização do uso de um PTT baseado no PTT de um provedor.

2.6.1 Disponibilidade

O conceito de alta disponibilidade refere-se ao tipo de soluções redundantes de equipamento e serviços, quanto ao aspecto de manter o funcionamento contínuo desses sistemas. Pode-se considerar como um sistema alternativo de segurança aquele que entra em funcionamento logo que o sistema (ou parte do sistema) principal (operacional) falha, mantendo, dessa forma, a disponibilidade do serviço.

A disponibilidade está relacionada à redundância da estrutura do PTT, à segurança do local de hospedagem, ao dimensionamento adequado da infra-estrutura, à qualidade do gerenciamento da operação, à estabilidade do software do servidor de roteamento e à confiabilidade na estrutura.

2.6.1.2 Local para hospedagem

É importante preocupar-se com a estrutura em que o PTT será instalado. Os seguintes aspectos devem ser observados:

- **Redundância em fornecimento de energia**

É importante ter, no *rack* em que será instalado o PTT, duas réguas de tomadas redundantes, ou seja, as réguas devem estar em redes elétricas diferentes.

- **Gerador/No break**

É imprescindível ter um sistema de gerador, de preferência redundante, para garantir a disponibilidade do PTT.

- **Sistemas de ar condicionado**

A sala onde o PTT estiver instalado deverá ser refrigerada, não deixando a temperatura ultrapassar 20 graus Celsius. Este sistema de refrigeração deve ser redundante.

- ***Racks***

O servidor de roteamento e o *switch* em que estão conectados os roteadores de cada participante devem estar acondicionados em um *rack* independente. Os *racks* devem ser fechados. Isto permite que um participante faça manutenções nos seus equipamentos sem manter contato físico com os equipamentos dos demais.

- **Piso e cabeamento**

O piso deve ser elevado e o cabeamento, devidamente identificado.

- **Segurança no ambiente**

A sala deve ter acesso restrito, monitorado através de câmeras e controlado por meio de senhas e cartões magnéticos. Os participantes do PTT, mediante autorização, podem ter acesso 24 horas.

- **Suporte operacional 24 por 7**

É importante ter uma equipe operacional local com condições de manter a estrutura em operação.

Com base nos itens anteriores, sugere-se hospedar o PTT em um Datacenter, pois este já dispõe da estrutura requerida pelo PTT, possibilitando um custo menor para sua implantação.

2.6.1.3 Redundância do PTT

Replicar toda a estrutura do PTT:

- Dois servidores executando servidor de roteamento.

  Obs.: Neste caso, colocam-se endereços Ip(s) diferentes.

- Dois *switches.*
- Dois *Firewalls* (Caso o PTT tenha *Firewall*).

Desta forma, cada participante estará conectado a dois *switches*, e manterá a seção BGP com os dois servidores de roteamento, recebendo as rotas dos dois. No entanto, terá na sua tabela de roteamento somente a rota mais antiga ou com maior preferência (dependendo da configuração do PTT). Caso falhe um dos *switches* ou um dos servidores, o PTT continuará funcionando. Esta topologia é somente um modelo proposto.

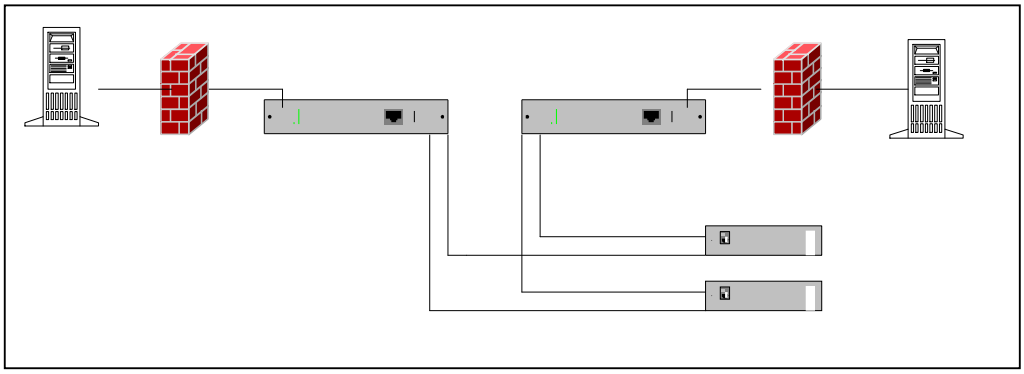


FIGURA 4 – Estrutura do PTT redundante

2.6.2 Capacidade

A capacidade de troca de tráfego na estrutura do PTT e nos participantes depende dos seguintes itens:

- *Link* do PTT até o roteador do participante.
- Interface física do roteador de cada participante.
- Memória e processamento do roteador do participante.
- Interface física do *switch*.

O tráfego do PTT, como já mencionado, não passará pelo servidor de roteamento. Desta forma, o servidor de roteamento não será o fator limitante da capacidade de tráfego. Por exemplo, caso o *switch* do PTT suporte portas de 100 Mbps, os roteadores de participantes tenham portas *fast ethernet* e o *link* até o participante seja de 34 Mbps, a capacidade máxima para esse participante será a capacidade do *link* de 34 Mbps.

2.6.3 Escalabilidade

O projeto Router Arbiter, como já mencionado, solicita a centralização das rotas para facilitar a escalabilidade. O PTT, por ter as rotas centralizadas no servidor de roteamento, facilita a escalabilidade. A seguir, observa-se a expansão do PTT relacionado ao *switch*, servidor de roteamento, endereçamento e participante.

Switch do PTT

A escalabilidade no *switch* do PTT pode ser conseguida por meio do aumento do número de portas do *switch* ou da inserção de mais *switches* na estrutura do PTT.

Participante do PTT

Quanto ao participante, deve-se analisar o roteador que está sendo usado e o *link* que está contratado. Por exemplo, um participante que tem um *link* E1 (2 Mbps) pode expandir para outros *links* E1(s), sendo necessário fazer o balanceamento destes. Contudo, o roteador deve ter *slots* vazios para aceitar essas interfaces E1(s). Caso o tráfego ultrapasse 10 Mbps, será necessário verificar se a interface do roteador com o *switch* suporta 100 Mbps. Caso não atenda, o participante deverá trocar o roteador ou limitar o tráfego de entrada e saída através dos filtros.

Servidor de roteamento

Como o tráfego do PTT não passa pelo servidor de roteamento, seu consumo de disco-memória é muito pequeno, permitindo a entrada de novos participantes sem afetar o desempenho do servidor.

Endereço IP

É recomendado estipular uma classe de endereço que permita um crescimento. Caso isso não seja feito, será necessário mudar o endereço de todos participantes para incluir uma nova classe.

2.6.4 Tráfego

É interessante que cada provedor tenha uma idéia da quantidade de tráfego trocado com o PTT. A análise pode ser feita previamente ou após o participante entrar na estrutura do PTT. A intenção de tráfego pode ser usada para negociar a entrada em um PTT, além de ajudar a dimensionar o *link* e o roteador colocado para cada participante. A análise de tráfego pode ser feita na rede interna de cada participante. Com a análise de tráfego, o provedor consegue conhecer o seu tráfego.

O Netflow pode ser um exemplo de ferramenta de análise de tráfego. O seu funcionamento baseia-se na execução de um *Probe* no roteador de borda do provedor, e em um servidor-coletor que armazena informações, tais como endereço de origem e destino, porta origem e destino, entre outras. Estas informações podem ser analisadas para gerar o perfil do tráfego de cada provedor.

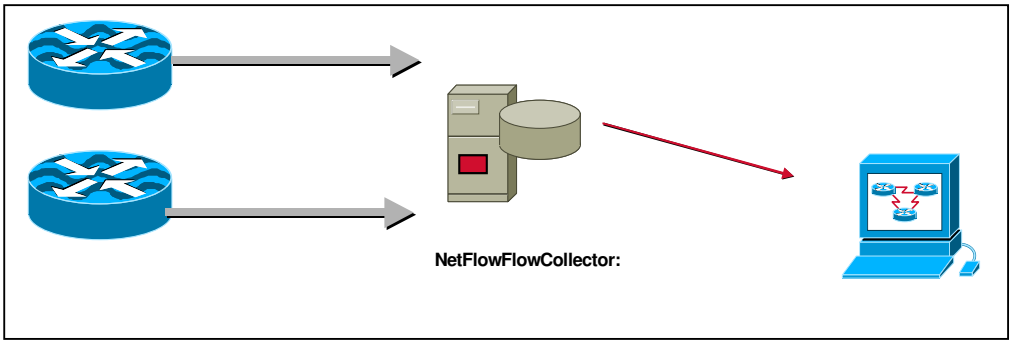


FIGURA 5 –Exemplo de coletagem do netflow

Na estrutura do PTT pode ser usada também uma ferramenta de gerenciamento de tráfego, a fim de saber o tráfego total do PTT, ou seja, quanto está entrando e saindo para cada participante.

O responsável pela administração do PTT gerencia o tráfego do *switch,* e cada participante deve gerenciar o seu roteador. Pode-se usar uma ferramenta de monitoração de tendência em séries temporais, como por exemplo o MRTG e o Cricket.

Capítulo 3. ROTEAMENTO E PROTOCOLO BGP

3.1 Conceitos de roteamento

"Roteamento pode ser definido como o processo de transmissão de um pacote de dados de um lugar para outro." (CISCO, 2000).

Na Internet, o roteador é responsável por receber e encaminhar pacotes. Cada roteador decide o melhor caminho, com base nas condições físicas da Internet informadas pelos protocolos de roteamento. (STALLINGS, 1997).

O roteamento geralmente é feito por roteadores; no entanto, pode também ser realizado pelos servidores de roteamento. Neste trabalho, serão usados servidores de roteamento nos PTT(s) e roteadores nos participantes.

3.1.1 Protocolo de roteamento

A função do protocolo de roteamento é determinar qual a melhor rota para cada destino e distribuir as informações de roteamento entre as redes, a melhor rota dentro do mesmo *Autonomous System*. Os protocolos de roteamento estão divididos em dois grupos: os protocolos internos, Internal Gateway Protocol - IGP e os externos, External Gateway Protocol – EGP.

O anúncio das redes dentro de um sistema autônomo é feito por meio de um protocolo de roteamento interno, como por exemplo o RIP (Routing Information Protocol) e o OSPF (Open Shortest Path First).

Os protocolos de roteamento externo – EGP são responsáveis por descrever os caminhos disponíveis para transmissão do tráfego entre provedores diferentes. Estes protocolos estão preocupados em isolar as redes, a fim de evitar problemas de roteamento dentro de um provedor, para que um não interfira em outro. Os protocolos EGP e BGP são exemplos de protocolos EGP, conforme a Multirede (2000).

Existem três famílias de protocolos de roteamento: o Distance Vector, o *Link* State e o Path Vector.

- **Distance Vector:** cada roteador recebe toda a tabela de roteamento, escolhendo a melhor rota com base na distância de dois pontos. O RIP versão 1 é um exemplo de protocolo Distance Vector.
- **Link State:** cada roteador mantém uma topologia da rede, atualizada por meio de anúncios sobre os estados dos *links* e pontos de rede. O OSPF é um exemplo de protocolo Link State.
- **Path Vector:** cada roteador recebe informações com o caminho para chegar a cada rede. Por meio de atributos recebidos, pode-se definir o melhor caminho para cada destino. O BGP é um exemplo de protocolo Path Vector.

3.1.2 Tipos de rotas

As rotas são usadas para definir o próximo destino (*next hop*) de cada rede. A seguir, definições dos tipos de rotas:

- **Rotas estáticas:** são rotas para um destino colocadas manualmente ou estaticamente no roteador. O tráfego será roteado para o *next hop* da rota estática.

- **Rotas default:** o tráfego para um destino que não seja conhecido pelo roteador vai ser roteado através da rota *default.*

- **Rotas dinâmicas**: são rotas que são aprendidas por meio de um protocolo de roteamento externo ou interno. Caso o *next hop* não esteja acessível, as rotas desaparecem da tabela de roteamento.

3.2 Autonomous System – AS

O *Autonomous System* – AS, pode ser compreendido também pela definição de Nemeth (1995), como uma coleção de redes sob o controle de uma única autoridade central.

Na Internet, um *Autonomous System* – AS está, na maioria dos casos, associado a um provedor que fornece infra-estrutura de transmissão e acesso para uma região.

Cada AS é reconhecido por um número decimal utilizado pelo protocolo de roteamento BGP. O AS pode ser privado ou público. Caso seja público, deve ser devidamente registrado por um provedor em um órgão de registro.

A administração e registro dos AS(s) devem ser feitos na American Registry for Internet Numbers – ARIN. No Brasil, ela é representada pela Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP.

A faixa de valores válidos para identificação de um AS varia de 1 a 65.535, sendo a subfaixa de 64.512 a 65.535 reservada para uso privado.

3.3 Protocolo de roteamento BGP v4

O protocolo BGP é usado para troca de rotas entre os participantes do PTT. Seu conhecimento é fundamental para a implementação e operação de um PTT.

O BGP é um protocolo de roteamento entre *Autonomous Systems* (REKHTER, 1995), que teve sua versão original datada de 1989, com o BGP-1. Posteriormente, em 1993, o BGP-4 começou a ser implementado.

Conforme Parkhurst (2001) "o BGP é um protocolo de roteamento robusto e escalável. Como evidência há o fato de o BGP ser o protocolo usado na Internet". Atualmente, a Internet tem em sua tabela de rotas BGP mais de 125.000 anúncios.

Segundo a Multirede (2000), "o protocolo BGP está especificado nas RFCs 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, 2439."

O BGP é um protocolo baseado no algoritmo Distance Vector. Usa o protocolo Transport Control Protocol – TCP na porta 179 – e por isso, o transporte das mensagens não precisa ser feito pelo BGP. O BGP no PTT é responsável pela política de roteamento aplicada, ou seja, gerenciar situações, tais como:

- Um participante não quer importar para sua tabela de roteamento todas as rotas aprendidas.

- Um participante não quer anunciar todas as rotas da sua tabela de roteamento para os outros participantes.
- Um participante deseja modificar informações associadas a uma rota.

O controle do tráfego de entrada e saída do participante no PTT é realizado pela configuração do BGP no servidor de roteamento e no roteador do participante.

Dois roteadores que formam uma conexão TCP com a finalidade de trocar rotas, são chamados de *neighbors*, ou seja, vizinhos.

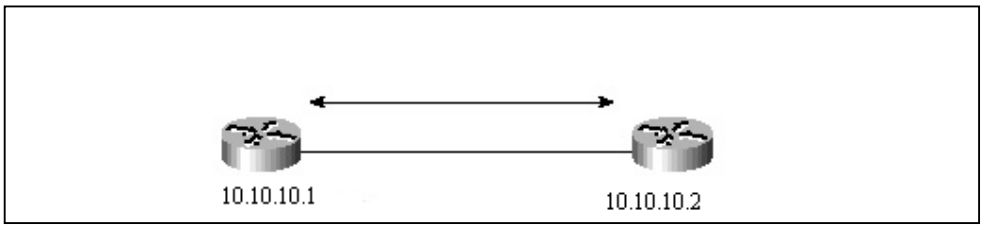


FIGURA 6 - Roteadores vizinhos

Na FIGURA 6, dois roteadores que estabelecem uma seção BGP. Observa-se que cada roteador tem um endereço IP e ambos podem pertencer ao mesmo AS ou AS diferentes.

Os vizinhos do BGP estabelecem seções que podem ser External BGP, no caso vizinhos de AS diferentes, ou Internal BGP, se eles forem vizinhos do mesmo AS.

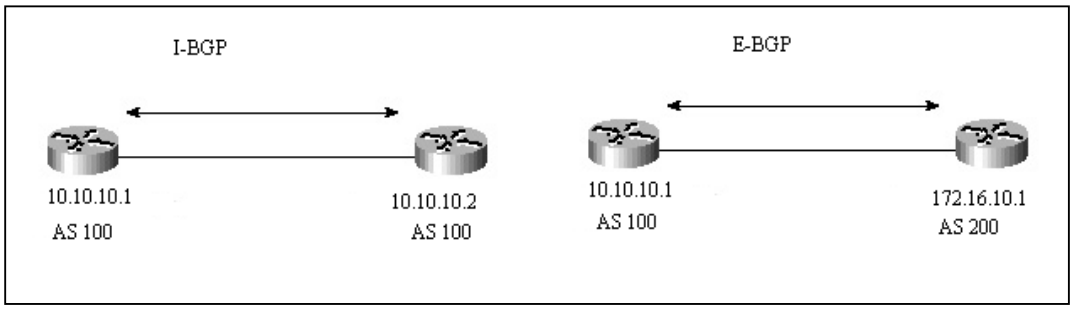


FIGURA 7 - Exemplo de seções BGP

3.3.1 Cabeçalho do BGP

Segundo Rekhter (1995), “o cabeçalho do BGP é formado com 16 bytes seguidos de 2 bytes, um destinado ao tamanho e um byte para identificar seu tipo”.

Todas as mensagens do BGP são compostas de, no mínimo, um cabeçalho e, opcionalmente, uma parte de dados.

O menor pacote de mensagem do BGP não pode ser menor que 19 bytes, ou seja, 16 bytes de cabeçalho, 2 bytes de tamanho e 1 byte de tipo.

No campo do tipo da mensagem existem quatro possibilidades, Open, Update, Notification e Keepalive.

3.3.2 Mensagens do BGP

O BGP possui quatro tipos de pacotes de mensagens que utilizam um cabeçalho em comum. A seguir, apresenta-se cada um:

3.3.2.1 Mensagem Open

Após estabelecer uma conexão TCP, os vizinhos BGP trocam mensagens open para criar uma conexão BGP. Depois do estabelecimento de uma conexão BGP, os vizinhos trocam outras mensagens BGP e dados com informações de roteamento, conforme Juniper (2003).

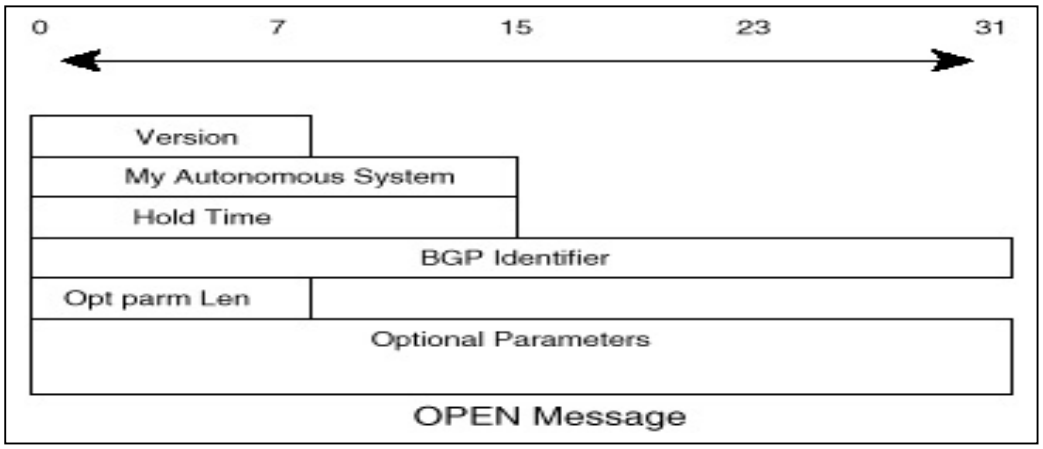


FIGURA 8 - Open Message Format , Halabi e Mc Pherson (2000).

Os parâmetros da Mensagem Open descritos por Rekhter (1995) são:

- **Version:** 1 byte que indica a versão do protocolo BGP, que pode ser BGP-3 ou BGP-4. Geralmente, usa-se a versão 4.

- **My Automous System:** 2 *bytes* que indicam o número do AS do roteador que originou a mensagem.

- **Hold Timer:** 2 *bytes* que indicam o tempo máximo em segundos entre o recebimento sucessivo do Keepalive e da mensagem de Update, através de um contador. Quando for recebido um *Keepalive* ou uma mensagem Update, automaticamente o Hold Timer é zerado. Com este mecanismo pode-se perceber se um vizinho está ativo.

- **BGP Identifier:** 4 *bytes* que indicam o endereço IP, identificando quem enviou. Esta identificação pode ser criada pelo roteador ou pelo endereço do roteador (endereço de *loopback*) mais alto que iniciou a conexão.

- **Optional Parameter Length:** 1 byte que indica a quantidade de *bytes* do *Optional Parameter field*; caso for 0, indica que não tem esse parâmetro.

- **Optional Parameter:** indica uma lista de parâmetros usados na negociação do BGP. É subdividido em três campos: *parameter type, parameter length e parameter value*. Estes parâmetros podem ser utilizados para a autenticação do BGP.

3.3.2.2 Mensagem Update

A mensagem de Update é responsável pelo transporte de roteamento entre os vizinhos BGP. "Cada update contém um anúncio de caminho com seus atributos e destinos." Juniper (2003). Estas informações estão distribuídas em três partes da

mensagem Update. As mensagens com o mesmo atributo devem ser agrupadas em um mesmo Update.

3.3.2.3 Mensagem Notification

A mensagem de notificação é sempre enviada quando um erro é percebido; após esse evento, a conexão com o vizinho é desfeita. A mensagem Notification consiste de:

- Cabeçalho BGP.
- Código do erro.
- Subcódigo.
- Dados que descrevem o erro.

TABELA 1 - Códigos de erro

Tipos	**Mensagem**
1	Message header error
2	Open message error
3	Update message error
4	Hold timer expired
5	Finite state machine error
6	Cease

3.3.2.4 Mensagens de Keepalive

As mensagens de Keepalive são periodicamente trocadas, para certificar que a conexão continua estabelecida. O pacote do Keepalive tem 19 *bytes* e não prejudica o uso de banda ou aumento de CPU do equipamento, diferentemente das mensagens de Updates que contêm trocas de informações de redes.

3.3.3 Máquina de estados do BGP

O processo de conexão TCP destinado a trocar mensagens de roteamento está representado pela máquina de estado finita, na qual ocorre o estabelecimento da vizinhança e, posteriormente, a troca de mensagens de roteamento.

Tal processo é usado entre os vizinhos do PTT.

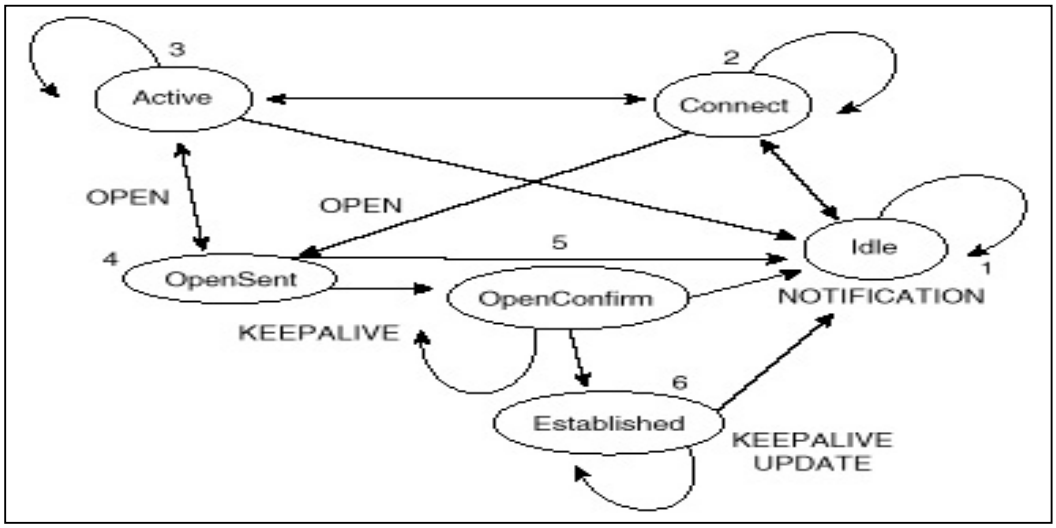


FIGURA 9 - Máquina de estado do BGP, Halabi e Mc Pherson (2000).

A máquina de estado do BGP tem os seguintes estados de negociação:

- **Idle:** é o primeiro estágio da conexão TCP. Esse estado aguarda um evento para iniciar o processo de conexão.

- **Connect:** aguarda a conexão TCP ser completada. Caso a conexão TCP obtenha sucesso, será enviada uma mensagem OPEN, passando para o estado Open Sent. Caso contrário, irá para o estado Active. No caso do tempo de espera ter sido ultrapassado, o estado volta para Connect. Em qualquer outro evento, retorna-se para Idle.

- **Active:** neste estágio ocorre uma tentativa da conexão TCP. Caso haja sucesso, será enviada uma mensagem de Open, passando para o próximo estado: o OpenSent. Se esta tentativa não for bem-sucedida pelo motivo de expiração do tempo, por exemplo, o estado passa para Connect. Caso não consiga a conexão, serão realizadas outras tentativas, até a expiração do número de tentativas, passando para o estado de Idle.

- **OpenSent:** Aguarda pela mensagem de Open e faz uma checagem de seu conteúdo. Caso seja encontrado algum erro, como número de AS incoerente, não esperado ou a própria versão do BGP, envia-se uma mensagem tipo Notification e volta ao estado de Idle. Quando a mensagem Open é recebida, é enviado um pacote Keepalive, reinicializando o contador de Keepalives e passando para o estado de OpenConfirm.

- **OpenConfirm:** aguarda a mensagem Keepalive ou Notification. Caso seja recebida a mensagem Keepalive, a conexão será estabelecida, passando para o estado Established. Caso seja recebida a mensagem Notification*, o* estado passará para Idle.

- **Established** é o último estado de negociação. É nesse estado que pacotes de Update e Keepalive são enviados. Caso seja recebido o pacote de Notification, a conexão será desfeita passando para o estado de Idle.

3.3.4 Atributos do BGP

O protocolo BGP, ao receber as atualizações de rotas de diferentes AS, repassa somente aquela que for considerada a melhor. O processo de decisão consiste em diferentes atributos, como o next-hop, administrative weights, local-preference, route origin, path length, origin code e metric, que serão vistos mais adiante. Estes atributos serão usados para definir a política de roteamento do PTT.

Os atributos classificados como well-known devem ser conhecidos pelos vizinhos;os opcionais, não necessariamente. Os atributos well-known são:

- **Mandatory:** são atributos de presença obrigatória em todos os anúncios de prefixos.
  - AS - PATH (TYPE=2)
  - ORIGIN (TYPE=1)
  - NEXT - HOP (TYPE=3)

- **Discretionary:** são atributos que não necessariamente estão presentes nos anúncios dos prefixos.
  - LOCAL-PREFERENCE (TYPE=5)

Os atributos opcionais são:

- **Transitive**: são propagados para todos os vizinhos. No entanto, o vizinho precisa ter configurado um parâmetro para aceitar esses atributos.
  - COMMUNITY (TYPE=8)
  - AGGREGATOR (TYPE=7)

- **Nontransitive:** caso não reconhecido pelo vizinho, será descartado.
  - MED (TYPE=4)

3.3.4.1 Tipos de atributos

Os atributos são um conjunto de parâmetros que descrevem as características das rotas. O processo de decisão do BGP faz uso dos atributos para escolher a melhor rota para cada destino. A seguir, apresentam-se os principais atributos:

- **AS-PATH:** quando a rota é propagada pelos AS, a informação do caminho é armazenada. O atributo AS-Path é usado para detecção de *loop*, pois contém a lista de AS percorridos da origem até o destino. É muito importante na definição da política de roteamento.

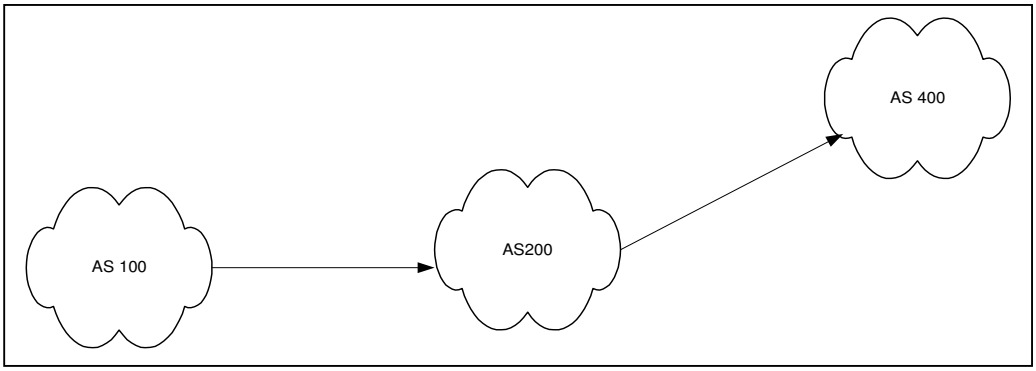


FIGURA 10 – Exemplo de AS PATH

A FIGURA 10 indica a rota anunciada pelo AS 100, passando pelo 200 e 400 e chegando ao destino. No AS-PATH a seqüência é registrada como 400, 200, 100.

- **NEXT - HOP**: este parâmetro informa o endereço IP do roteador que anunciou a rota. Este parâmetro não será modificado quando as rotas forem propagadas por uma conexão IBGP.

- **LOCAL–PREFERENCE:** o atributo local-preference é conhecido por vizinhos de um AS e usado para determinar o melhor caminho de saída. O caminho que tiver o local-preference maior será escolhido. O valor-padrão para esse atributo é 100.

- **MULTI-EXIT DESCRIMINATOR–MED:** determina o melhor caminho para o tráfego que estará entrando no AS. Para se usar este parâmetro deverá haver um acordo entre os AS(s), pois sua inclusão exige configuração em ambos os lados.

- **WEIGHT**: é um atributo proprietário dos equipamentos Cisco, possibilitando atribuir peso para cada vizinho do roteador não divulgado pelo BGP. Seu valor-padrão é 32768. É para uso interno do próprio roteador.

- **ORIGIN:** este atributo, como visto, é obrigatório, sendo responsável para definir a informação da rota de origem. Este atributo pode ser classificado em:

    - **IGP:** quando a rota for originada dentro do próprio AS pelo comando network do BGP.
    - **EGP:** quando a rota for aprendida através do protocolo EGP.
    - **Incomplete:** caso a rota tenha sido inserida na tabela do BGP por redistribuição.

- **COMMUNITY:** é usado para caracterizar um conjunto de rotas de um cliente e controlar o seu anúncio.

O BGP tem um algoritmo para escolha das rotas. Os atributos do BGP têm diferentes prioridades, de acordo com a tabela abaixo:

TABELA 2 - Prioridade do atributo do BGP

1 – Next-hop	Caso não esteja acessível, não haverá anúncio.
2 – Weight	Maior valor do parâmetro weight.
3 – Local-Preference	Maior valor do local-preference.
4 – (Local)	Em caso de empate: rota originada pelo roteador local.
5 – As-path	Caso não seja interna: rota com o As-path mais curto.
6 – Origin	Melhor precedência (IGP<EGP<INCOMPLETE).
7 – MED	Menor valor do parâmetro MED.
8 – EBGP –IBGP	Caminho externo.
9 – Vizinho mais próximo	Vizinho mais próximo (*next-hop*).
10 – Rota antiga	Rota mais antiga.
11 – Route ID	Menor valor do router ID.

3.3.5 Sincronização do BGP

Para evitar *loops* e "buracos negros", quando o tráfego é roteado internamente e não atinge o seu objetivo, usa-se a sincronização do BGP. O BGP precisa estar sincronizado com o protocolo interno (IGP). Isto significa que o BGP espera que a rota seja aprendida pelo IGP antes de divulgá-la para os vizinhos. Pode-se desabilitar a sincronização quando todos os roteadores rodando BGP entre si.

3.3.6 Configurando BGP

Os dois exemplos de configuração estão relacionados a equipamentos Cisco. Posteriormente serão vistos os comandos nos servidores de roteamento Zebra e Gated.

3.3.6.1 Comandos iniciais

O primeiro passo para ativação do BGP é definir o AS a que o roteador pertence. Pode-se fazer isso com o comando **Router bgp.**

- **Comando: Router bgp** *Autonomous System*

Ex.: Router bgp 100 (este comando inicia o processo BGP relacionado ao AS 100).

O próximo passo é informar quais rotas deverão ser divulgadas pelo BGP através do comando **Network**. No caso de roteadores Cisco, se a sincronização estiver habilitada, só serão divulgadas se estiverem presentes na tabela de roteamento IP.

- **Comando: Network** *número da rede* **mask** *máscara da rede.*

Ex.: network 10.10.10.0 mask 255.255.255.0 (Anunciando a rede 10.10.10.0 255.255.255.0)

Como já citado, na máquina de estado os roteadores serão vizinhos quando existir uma conexão TCP entre eles. Estabelecida a conexão, serão trocadas as informações de roteamento.

Para a definição de um vizinho, usa-se o comando **Neighbor.**

- **Comando: Neighbor** *ip address* **remote-as** *as-number*

Ex:

neighbor 10.10.10.2 remote-as 100

neighbor 172.17.10.1 remote-as 200

No exemplo acima define-se o vizinho 10.10.10.2 referente ao AS 100, ou seja, conforme visto é uma seção IBGP (mesmo AS), e o vizinho 172.16.10.1 referente ao AS200, seção EBGP (AS diferente).

Para identificar o vizinho, utiliza-se o endereço IP da interface ou o endereço da *loopback* (endereço do roteador).

Com os comandos descritos, já se pode configurar o BGP de um roteador Cisco, ou seja, um possível participante do PTT conforme a TABELA 3.

TABELA 3 – Configuração inicial do BGP

Comandos	**Definição**
Router bgp 100	Definir processo BGP do AS 100.
Network 10.10.10.0 mask 255.255.255.0	Divulgar a rede 10.10.10.0/24.
Neighbor 10.10.10.2 remote-as 100	Configurar um vizinho do AS.
Neighbor 172.17.10.1 remote-as 200	Configurar um vizinho de outro AS.

3.3.6.2 Implementando políticas de roteamento no PTT

É fundamental definir a política de roteamento, tanto no PTT quanto nos participantes. Consegue-se manipular os atributos do BGP para controle das rotas enviadas e recebidas, monitorando, desta forma,o tráfego de entrada e saída.

3.3.6.3 Expressões AS-PATH

O responsável pelo roteamento do AS deve determinar quais blocos serão anunciados e recebidos pelos seus vizinhos, por meio de expressões AS-PATH que serão usadas para criar os filtros de AS nos roteadores Cisco e nos servidores de roteamento Zebra e Gated.

Foram definidos alguns símbolos para auxiliar a criação dos filtros:

TABELA 4 – Símbolos para criação de filtros

Símbolos	**Definição**
.	Qualquer caractere unitário.
.^	Especifica a primeira *string*.
$	Especifica a última *string*.
\caractere	Especifica a *string* em qualquer posição.
[5-9]	Especifica uma faixa de AS.
*	Qualquer especificação, incluindo vazio.
+	Qualquer especificação não vazia.
?	Caractere específico.
-	Separa os extremos de uma faixa de AS.
_	Representa uma vírgula (,) chaves ({ }), parênteses, início da *string*, fim da *string* ou espaço em branco.

TABELA 5 – Exemplos de expressões AS-PATH

Expressões	Definição
.*	Representa todo o conjunto de rotas BGP.
^$	Representa somente as rotas locais do próprio AS.
^100$	Somente as rotas pertencentes ao AS100.
_100$	Rotas que foram originadas no AS100.
^100_	Rotas terminadas no AS100.
_100_	Rotas que atravessaram o AS100.

3.3.6.4 Filtros BGP

Os filtros BGP servem para controlar o fluxo de entrada e saída de atualizações de rotas do protocolo, ou seja, eles podem ser aplicados tanto para anúncios enviados (*outbound*) quanto para os recebidos (*inbound*) . O uso de filtro é de grande importância no PTT, pois garante as rotas recebidas e enviadas no roteador de cada participante e no servidor de roteamento. Existem os seguintes métodos de filtragem:

- *AS-Path filtering* (por AS-PATH).
- *Distribute-List filtering* (por lista de acesso).
- *Prefix filtering* (por prefixo).
- *Route Map filtering* (por Route-Map).

Filtro por AS-Path Filtering

Com este filtro podem-se usar as expressões AS-PATH vistas anteriormente, ou seja, podem-se fazer filtros com base nos AS(s). Com o uso de um comando associado a um vizinho, pode-se selecionar as rotas de acordo com as condições definidas pelas regras da expressão, permitindo-se ou não a sua divulgação. A seguir, uma breve descrição dos comandos.

Comandos de filtro AS-PATH

Comando: **ip as-path access-list** *número da lista de acesso* **deny/permit** *expressão*

É criada uma lista de acesso relacionada à expressão AS-PATH.

No exemplo a seguir a construção da lista de acesso 1, permitindo que sejam aceitas as redes originadas pelo AS 200.

Ip as-path acess-list 1 permit ^200$

Comando: **Neighbor** *endereço IP* **filter-list** *número da lista de acesso* **in/out**

Associar ao vizinho, identificando se vai ser aplicado na entrada (recebimento) ou saída (divulgação).

No exemplo, a aplicação desta lista na entrada do vizinho 10.10.10.2

Neighbor 10.10.10.2 filter-list 1 in

A TABELA 6 mostra uma seqüência de comandos executados para configurar um filtro AS-PATH.

TABELA 6 – Configuração de filtro AS-PATH no BGP

Comandos	**Definição**
Router bgp 100 Neighbors 172.17.10.1 remote-as 200 neighbors 172.17.10.1 filter-list 10 in Ip as-path acess-list 10 permit ^200$	Configura o vizinho 172.17.10.1 para receber somente as rotas originadas pelo AS 200.

Filtro por distribute-list

O filtro por distribute-list precisa da criação de uma lista de acesso estendida, ou seja, precisa ser usado quando se deseja fazer filtros pelo endereço IP. A seguir, a descrição dos comandos.

Comandos de filtro por distribute-list

Comando: Access-list *number* **deny/permit** *ip origem ip destino*

É construída uma lista de acesso através dos parâmetros deny (nega) e permit (permite) do endereço origem para destino.

No exemplo, a construção da lista de acesso 199 negando a entrada da rota 0.0.0.0

Access-list 199 deny ip host 0.0.0.0 any
Access-list 199 permit ip any any

Comando: **Neighbor** *endereço IP* **distribute-list** *número da lista de acesso* **in/out**

É associado a uma lista de acesso ao vizinho, identificando se vai ser aplicado na entrada (recepção) ou na saída (divulgação*).*

No exemplo, a associação da lista de acesso 199, aplicado na entrada do vizinho 10.10.10.3

Neighbor 10.10.10.3 distribute-list 199 in
Voltando ao exemplo inicial:

TABELA 7 – Configuração de filtro Distribute-list

Comandos	**Definição**
Router bgp 100 Neighbor 172.17.10.1 remote-as 200 Neighbor 172.17.10.1 distribute-list 199 in	Configura o vizinho 172.17.10.1 para não receber a rota 0.0.0.0.

Access-list 199 deny ip host 0.0.0.0 any Access-list 199 permit ip any any	

Filtro por prefix

Este filtro foi disponibilizado pela Cisco a partir da versão de IOS 12.0. Tem algumas vantagens, como melhoria de CPU e facilidade para inserir e remover uma lista. No entanto, não serão utilizados estes tipos de experimentos no presente trabalho. Serão feitas as experiências usando os dois filtros vistos anteriormente, ou seja, por expressão AS-PATH, por distribute-list e o filtro por Route-maps, que será visto a seguir.

Filtro por route-maps

Route-map é o método usado para manipular informações de roteamento. Funciona como uma lista de acesso avançada, muito utilizada no BGP para controlar ou modificar as informações de roteamento. Podem-se controlar os valores dos atributos.

Comandos route-map

Comando: Route–map *nome route-map* **[permit |deny]** *[número da seqüência]*

O route-map tem várias sentenças organizadas com números que permitem as condições de seleção de rotas e regras para adequação dos valores relacionados aos seus atributos. Cada sentença possui o verbo *permit* ou *deny*.

No exemplo, a construção do route-map teste negando

Route-map teste deny 10

Comando: **match** *parâmetro*

Comando: set *parâmetros*

O parâmetro do comando match seleciona as rotas. O parâmetro do comando set define valores para os atributos.

No exemplo, apresentam-se todas as rotas da lista de acesso 199, e posteriormente ajusta-se o atributo da community para 50.

Math ip address 199
Set community 50

Comando: **Neighbor** *endereço IP* **route-ma**p *nome do route-map* **{in/out} :**
Associa o route-map no vizinho, definindo o seu sentido.

No exemplo, é vista a aplicação do route-map na entrada do vizinho 10.10.10.2

Neighbor 10.10.10.2 route-map teste in

Voltando ao exemplo inicial:

TABELA 8 – Configuração por Route-Map

Comandos	**Definição**
Router bgp 100 Neighbor172.17.10.1 remote-as200 Neighbor 172.17.10.1 route-map teste in Neighbor 172.17.10.1 send-community Route-map teste permit 10 Match-as-path 10 Set community 50 Ip as-path access list 10 permit ^200$	Nesse exemplo, em todas as rotas originadas no AS 200 o atributo community é ajustado para 50, ou seja, poderia ser útil para classificar essas rotas. A partir desta classificação, pode-se implementar uma política de roteamento.

No decorrer deste trabalho, exemplificam-se alguns desses atributos. A seguir, apresenta-se a tabela das possibilidades para o Match e o Set utilizadas na criação de route-maps.

TABELA 9 – Parâmetros usados no Match

Match as-path
Match ip address
Match ip route-source
Match route-type
Match community
Match ip next-hop
Match metric
Match tag

Os parâmetros usados com o comando set:

TABELA 10 - Parâmetros usados com o SET

Set as-path
Set community
Set local preference
Set metric-type
Set origin
Set weight
Set ip next-hop
Set ip preference
Set level
Set metric
Set ip next-hop
Set tag

3.3.7 Configuração do BGP nos servidores de roteamento Zebra e Gated

O BGP é um dos protocolos usados no PTT. A construção e a manutenção do servidor de roteamento dependem do domínio desse protocolo. A configuração do Zebra é muito semelhante à dos roteadores Cisco, enquanto que o Gated tem uma sintaxe bem distinta.

3.3.7.1 Comandos do servidor de roteamento Zebra

O servidor de roteamento Zebra usa vários *daemons* simultâneos, um *daemon* para cada protocolo de roteamento. Não há necessidade de esses *daemons* serem executados na mesma máquina.

O uso da arquitetura multiprocessamento traz benefícios, tais como manutenção, ampliação e modularidade. Ao mesmo tempo, o Zebra usa vários arquivos de configuração e terminais. Por exemplo, para configurar rotas estáticas deve-se configurar o módulo Zebra.

O Zebra tem um método de administração do sistema diferente do Unix. Dentro do terminal existem dois modos, o normal e o *enable*. No modo normal, o usuário pode ver o status do sistema; no modo *enable,* o usuário (administrador) pode alterar a configuração. Este modo é usado também nos roteadores Cisco.

Nos experimentos do PTT será usado o Zebra como servidor de roteamento, pois seus comandos são muito parecidos com os da Cisco, que é o produto mais conhecido no mercado. A seguir, seguem alguns comandos para configuração de um PTT.

3.3.7.1.1 Definir hostname

Comando: Hostname *nome do hostname*

Define o hostname usado no servidor de roteamento.

Ex.**:** Hostname PTT (define PTT como hostname).

3.3.7.1.2 Definir o processo BGP

Comando: router bgp *número do AS*
Definir o processo BGP do roteador
Ex.: Router bgp 100 (inicia o processo BGP do AS 100)

3.3.7.1.3 Definir vizinho do BGP

Comando: neighbor *endereço IP* **remote-as** numero do AS
Definir o vizinho BGP.
Ex.: neighbor *10.10.10.1* remote-as 200 (definir o vizinho 10.10.10.1 do AS 200)

3.3.7.1.4 Anúncio das redes

Comando: network rede mascára binária
Definir as redes que vão ser anunciadas; neste caso a máscara é binária.(ANEXO C).
Ex.: network **10.10.10.0/8** (anuncia a rede 10.0.0.0 255.0.0.0)

3.3.7.1.5 Definir vizinho como transparente

Comando: neighbor *endereço IP* **attribute-unchanged as-path next-hop**
Definir o vizinho como transparente.
Ex.: neighbor 10.10.10.3 attribute-unchanged as-path next-hop (As redes recebidas por este vizinho serão exportadas para os participantes sem a inclusão do AS do servidor de roteamento; desta forma, conforme explicado, o tráfego não passará pelo servidor de roteamento).

3.3.7.1.6 Associação dos filtros no vizinho do servidor de roteamento

Comando: Neighbor *ip vizinho* **filter-list** *nome access* **in/out**

O objetivo é a associação de um filtro para permitir receber rotas de uma expressão regular, o filtro aplicado na entrada (recepção) ou saída (divulgação).

Ex.: neighbor 10.10.10.3 filter-list routera in (associa o filtro *routera* no vizinho 10.10.10.3)

3.3.7.1.7 Construção de um filtro

O objetivo é a construção de um filtro para permitir receber rotas de uma expressão regular; após a construção, o filtro pode ser aplicado em um vizinho, como no comando anterior.

Comando: ***ip as-path access-list*** *nome da lista de acesso* ***permit*** *expressão regular*

Ex: Ip as-path access-list routera permit ^7677$

No exemplo a seguir foi criada a lista de acesso *routera,* permitindo somente as rotas originadas do AS 7677.

3.3.7.1.8 Configurar o endereço do servidor de roteamento

Comando: bgp router-id *endereço IP*

Definir o endereço IP do servidor de roteamento.

Ex.: bgp router-id 10.10.10.2 (definir o endereço do servidor de roteamento como 10.10.10.2).

3.3.7.1.9 Configurar um arquivo para receber os logs

Comando: Log file *nome do arquivo*

Definir um arquivo para receber os logs que ocorreram no servidor de roteamento.

Ex.: log file bgpd.log (redireciona o log para o arquivo bgpd.log).

TABELA 11- Exemplo de configuração do filtro no servidor de roteamento Zebra

Comandos	**Definição**
hostname router	Define hostname como router.
router bgp 7675	Inicia o processo BGP do AS7675.
bgp router-id 10.10.10.2	Define o endereço do servidor de roteamento como 10.10.10.2.
neighbor 10.10.10.3 remote-as 7677	Define o vizinho 10.10.10.3 referente ao as 7677.
neighbor 10.10.10.3 filter-list routera in	Aplica filtro routera na entrada do vizinho 10.10.10.3.
neighbor 10.10.10.3 attribute-unchanged as-path next-hop	Configura para o vizinho 10.0.10.3 para não receber as rotas com o endereço IP do Servidor de roteamento.
ip as-path access-list routera permit ^7677$	Criar filtro routera, permitindo somente rotas originadas pelo AS 7677.

3.3.7.2 Comandos do servidor de roteamento Gated

Os comandos do Gated são diferentes dos comandos do Cisco e do Zebra; no entanto, o conceito do BGP é o mesmo.

Diferentemente do Zebra, o Gated versão R3_5 tem suas configurações somente em um arquivo, não permitindo modos de acesso para alterar as configurações.

3.3.7.2.1 Definir o processo BGP

Comando: AS *número do AS*
Definir o processo BGP do roteador.
Ex.:AS 100 (inicia o processo BGP do AS 100).

3.3.7.2.2 Ativar o BGP

Comando: bgp on
Ativa o processo BGP no Gated.

3.3.7.2.3 Definir vizinho do BGP

Comando: **peer** *endereço IP;*
Ex.: peer 10.10.10.1; (definir o vizinho 10.10.10.1)

3.3.7.2.4 Associar o vizinho ao AS como transparente

Comando: group type external peeras numero do AS **transparent** *{*
peer endereço IP*;*
};
Associar o vizinho ao AS definindo como transparente.
Ex.: group type external peeras 6000 transparent {
peer 10.10.10.1 ;
};.
(associa um AS ao vizinho, definindo o AS como transparente, ou seja, o AS do PTT não será anunciado na rota. Pode-se observar, no exemplo, a

associação do vizinho 10.10.10.1 ao AS 6000, não passando as rotas do PTT para esse AS).

3.3.7.2.5 Associação e construção dos filtros

Comando: import proto bgp aspath *número do AS* ***origin*** *any* ***{***

all; ***};***

Importar todas as rotas originadas do AS específico.

Ex.: *Import proto bgp aspath* 65000 *origin any {*

all; };

(O exemplo mostra a importação de todas as rotas do AS 65000.)

TABELA 12 - Configuração do filtro no servidor de roteamento Gated

Comando	**Definição**
import proto bgp aspath 7671 origin any { all; };	Importar as rotas originadas do AS 7671.

TABELA 13 - Exemplo de configuração do filtro no servidor de roteamento Gated

Comando	**Definição**

as 7675;
routerid 10.10.10.2;
 	
bgp on {
group type external peeras 7677 transparent {
peer 10.10.10.3 ;
};
};
view {
	Define o AS do servidor de roteamento.
	Define o endereço do servidor de roteamento.
	Inicia o processo BGP.
	Declara o vizinho 10.10.10.3 referente ao AS7677, configurando o vizinho como transparente.

peer 10.10.10.3;
import proto bgp aspath 7677 origin any {
all; };
};
;
	Declara endereço do vizinho.
	Importa as rotas originadas pelo AS 7677.

3.3.7.3 Comandos de análise do roteamento

Existem comandos que permitem analisar o roteamento. Estes comandos podem ser aplicados no diagnóstico de eventuais problemas de roteamento.

Seguem os principais comandos utilizados nos experimentos do PTT, tanto nos roteadores Cisco usados pelos participantes, quanto nos servidores de roteamento Zebra.

Verificando as rotas da tabela de roteamento

3.3.7.3.1 Verificar rota em uso

Comando: show ip route ***rede***

Para verificar a rota que está em uso, ou seja, a que está na tabela de roteamento, este comando é muito utilizado. Pode-se verificar através dele se um participante do PTT tem na sua tabela de roteamento uma rota específica.

Ex.: show ip route 10.10.10.0 (Este comando vai mostrar a interface de destino para chegar na rede 10.10.10.0).

3.3.7.3.2 Verificar rota no BGP

Comando: show ip bgp *rede*

Para verificar a rota que foi aprendida pelo protocolo BGP.

Ex.: Show ip bgp 10.10.10.0 (Verificar se a rede 10.10.10.0 foi aprendida pelo protocolo BGP).

3.3.7.3.3 Verificando os vizinhos e a quantidade de rotas recebidas

Comando: show ip bgp summary

O comando show ip bgp summary mostrará a relação dos vizinhos BGP, com as rotas recebidas.

Ex.: show ip bgp summary

3.3.7.3.4 Verificando as rotas recebidas de um vizinho

Comando: sh ip bgp neighbor *endereço do vizinho* **route**

Este comando mostrará todas as rotas recebidas de um vizinho específico.

Ex.: sh ip bgp neighbor 10.10.10.1 route – Neste exemplo, mostram-se todas as redes recebidas de um vizinho específico. Pode ser usado para ver as redes recebidas em um servidor de roteamento e/ou um participante do PTT.

3.3.7.3.5 Verificando as rotas anunciadas por um vizinho

Comando: sh ip bgp neighbor *endereço do vizinho* **advertised-routes**

Este comando mostrará todas as rotas anunciadas de um vizinho específico.

Ex.: sh ip bgp neighbor 10.10.10.1 advertised-routes – Este exemplo mostrará todas as redes anunciadas para um vizinho específico. Pode ser usado para ver as redes anunciadas em um servidor de roteamento e/ou um participante do PTT.

3.3.7.3.6 Limpar a tabela de roteamento do BGP

Comando: clear ip bgp *Endereço IP do Vizinho*

Este comando limpa as redes recebidas e anunciadas por este vizinho.

Ex.: Clear ip bgp 10.10.10.2 – Neste exemplo as rotas recebidas e enviadas do vizinho 10.10.10.2 serão limpas.

Capítulo 4. METODOLOGIA E MATERIAL DE PESQUISA

Este capítulo apresenta o percurso metodológico utilizado para responder ao objetivo geral desta pesquisa.

4.1 Detalhamento da pesquisa

A metodologia utilizada neste trabalho foi baseada na pesquisa exploratória. Segundo Mattar (1996), "a pesquisa exploratória visa prover o pesquisador de mais conhecimento sobre o tema ou problema de pesquisa em perspectiva" ou, ainda, "tem a finalidade de formular problemas e hipóteses para estudos posteriores", Martins (2002).

O método usado foi o experimental, ou seja, "aquele em que variáveis são manipuladas de maneira pré-estabelecida, e seus efeitos suficientemente controlados. Tentam descobrir relações casuais. São precedidos de planejamentos experimentais, ou delineamento de experimentos", Martins (2002).

Segundo informação do principal PTT do Brasil (Fapesp), os servidores-padrão de roteamento usados são o Gated e o Zebra. Por meio de um estudo de revisão da literatura, foram analisados os PTT(s); o protocolo de roteamento BGP; e os servidores de Roteamento Gated e Zebra.

Na primeira fase foi feito um experimento em laboratório, construindo-se um PTT central com três participantes, usando o servidor de roteamento Zebra. Nesta fase, foi avaliada a construção do servidor de roteamento, desde a escolha do sistema operacional até a instalação e configuração do Zebra.

Neste experimento, foi explorada a capacidade do protocolo BGP para garantir os anúncios das rotas, criar as políticas de roteamento, e aplicar pontos de segurança tanto no PTT quanto nos participantes.

Na segunda fase, ocorreu a configuração do Zebra e o planejamento para a migração do Gated para o Zebra, visando substituir o software de roteamento de um PTT em uso por um provedor ativo.

Nesta fase, foram avaliados os pontos positivos e negativos da migração do Gated para o Zebra, e, em seguida, foi ajustada a política de roteamento para aumentar a quantidade de tráfego trocada no PTT.

Por fim, com o uso das informações dos experimentos executados e observação do PTT em produção, foram propostas diretrizes para a construção de um PTT apontando suas características de gerenciamento e segurança, roteamento e implementação.

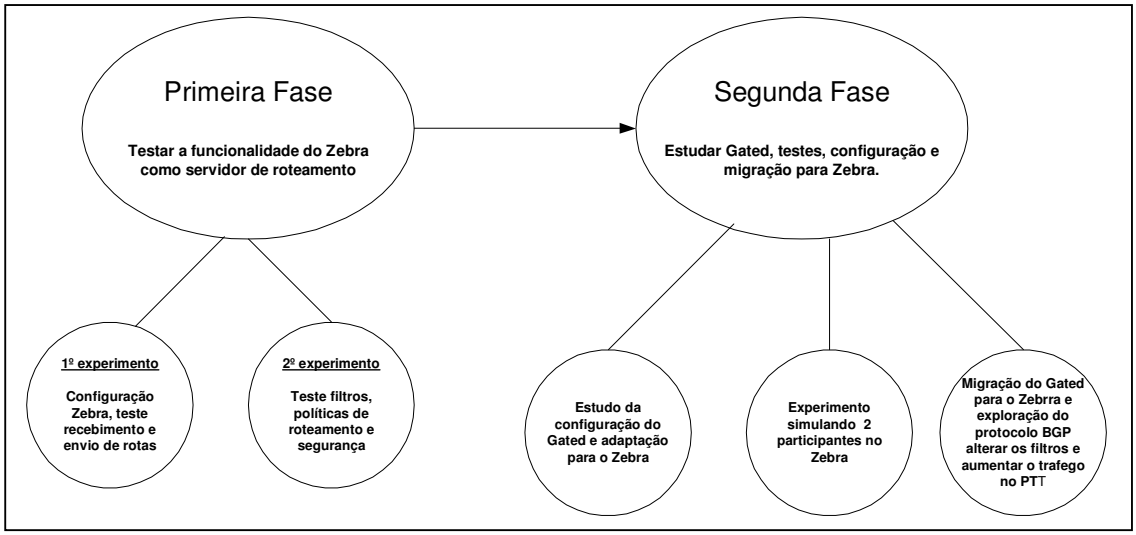


FIGURA 11 - Diagrama com as fases

4.2 Equipamentos utilizados

- 1 Servidor Netfinity –IBM - instalação do Zebra
- 1 *Switch* 2924 da Cisco
- 3 Roteadores Cisco 2501

Experimentos

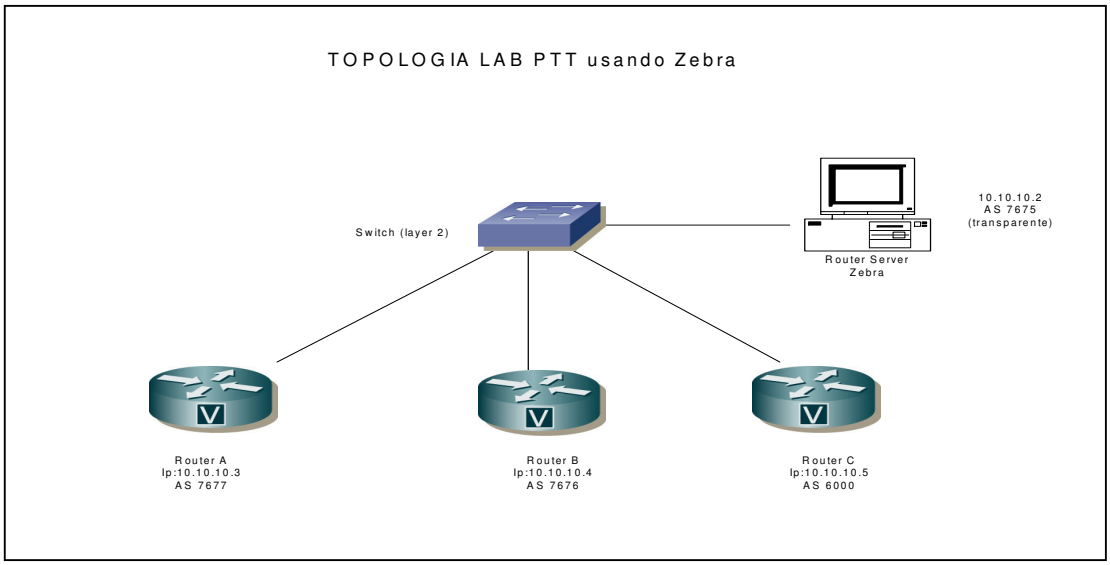


FIGURA 12 - Topologia do experimento – Primeira fase

Na primeira fase, serão três participantes, trocando rotas através do servidor de roteamento Zebra. Os participantes, AS e as redes escolhidas serão fictícios, ou seja, somente para análise.

Na primeira fase, três participantes trocam rotas através do servidor de roteamento Zebra. Os participantes AS(s) e as redes escolhidas são fictícios, ou seja, somente para análise.

Cada participante tem sua política de roteamento implementada anunciando suas redes para o servidor de roteamento que aceita todas as redes, distribuindo-as para os demais participantes. Nesta fase, é necessário o uso de comandos de análise de roteamento,para verificar cada anúncio e analisar as questões:

1- Qual a melhor configuração para o servidor de roteamento?
2- Os participantes estão exportando suas redes?
3- Os participantes estão recebendo as redes dos outros AS?
4- O servidor de roteamento está sendo transparente para o anúncio das redes?
5- Qual a melhor configuração para cada participante?

A topologia sofreu modificações a fim de testar os filtros implementados no servidor de roteamento.

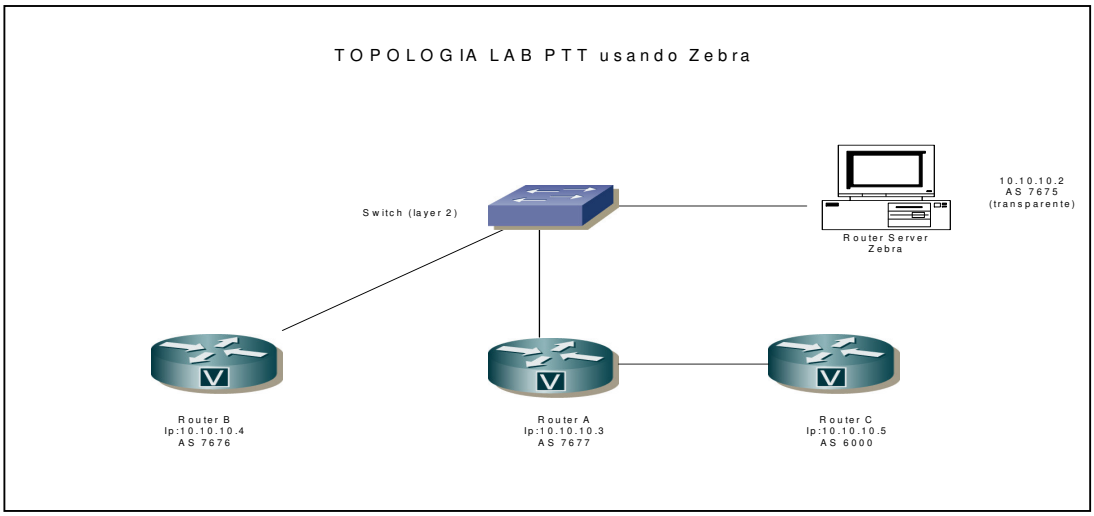


FIGURA 13 - Topologia do experimento – Explorando o BGP no PTT

Nessa etapa foram testados os filtros no servidor de roteamento para controlar o recebimento e envio dos anúncios. Foram analisadas as seguintes questões:

1- O servidor de roteamento está recebendo as rotas dos participantes que não estão conectados diretamente?

2- O servidor de roteamento está sendo transparente para o participante não conectado?

3- Quais são as políticas de segurança implementadas através dos filtros BGP no participante e nos servidores de roteamento?

Capítulo 5. ANÁLISE DOS RESULTADOS

Neste capítulo encontram-se os resultados da pesquisa realizada através dos dois experimentos. Os resultados estão classificados conforme os objetivos específicos:

5.1 Funcionalidade do PTT usando o servidor de roteamento Zebra

Na primeira fase do experimento foram analisadas as seguintes questões (vide item 4.1):

- Os participantes estão exportando suas redes?
- Os participantes estão recebendo as redes dos outros AS?
- O servidor de roteamento está sendo transparente para o anúncio das redes?
- Qual a melhor configuração para cada participante?
- Qual a melhor configuração para o servidor de roteamento?

Essas questões são a base para o funcionamento do Zebra como servidor de roteamento, ou seja, se atendidas, conclui-se que o Zebra atende aos requisitos do PTT em produção.

O experimento iniciou-se com a instalação do Linux Red Hat 9.0 em um servidor, com a seguinte configuração:

- Servidor Netfinity –IBM
- Pentium 3 – 929 MHZ
- 2 discos de 18 Gb
- 512Mb de memória
- 2 fontes

Nos servidores, configurou-se o espelhamento nos discos, ou seja, o *Raid* nível 1 para haver redundância e preservação dos dados em caso de falha de um disco.

Após a instalação do Linux e a respectiva atualização dos *patches*, foi instalada a última versão disponível do Zebra, a **Zebra-03.b.**

No diretório-raiz do servidor criou-se um subdiretório com o nome Zebra, no qual se descompactou o arquivo **zebra-0.93b.tar**, que contém o código-fonte do Zebra. Foram executados os seguintes comandos para a instalação do Zebra.

./configure (Configuração do Zebra)
make (Compilar os pacotes necessários)
make install (Instalar)

Finalizada a instalação do Zebra no Linux, foi necessário configurar os arquivos zebra.conf (arquivos de configuração do roteador Zebra) e o bgpd.conf (arquivo de configuração do BGP). Estes arquivos estão gravados no diretório **usr\local\etc**.

Configuração do Zebra

hostname Router	Define o hostname
password zebra	Definir senha
enable password zebra	Definir senha enable (mais recursos)
interface lo	Interface loopback
interface eth2	Interface de rede eth2

Configuração do BGPD

hostname bgpd	Define o hostname
password zebra	Definir senha
enable password teste	Definir senha enable (mais recursos)
log file bgpd.log	Direciona o log para o arquivo bgpd.log

Os modos de roteamento e do BGP devem ser ativados através dos comandos:

Zebra –d

Bgpd –d

Obs.: No Zebra e no **bgpd** a opção de execução –d significa que foi executado em modo *daemon,* ou seja, caso a sessão feche, o processo continua sendo executado. Depois da execução dos processos foi confirmado que eles estavam rodando através do seguinte comando:

```
[root@Nap etc]# ps -ef | grep zebra
root      1908     1  0 Aug21 ?        00:00:00 /usr/local/sbin/zebra -d
root     11024 10942  0 11:07 pts/1    00:00:00 grep zebra

[root@Nap etc]# ps -ef | grep bgpd
root     11019     1  0 11:04 ?        00:00:00 bgpd -d
root     11026 10942  0 11:07 pts/1    00:00:00 grep bgpd
```

Os comandos de execução foram inseridos no arquivo **etc/rc.d/rc.local,** a fim de que sejam executados automaticamente em caso de reincialização da máquina.

/usr/local/sbin/zebra –d

/usr/local/sbin/bgpd –d

Pode-se entrar no modo roteamento e/ou no processo BGP do servidor de roteamento através de suas portas. O BGPD usa a porta 2605 e o Zebra, a 2601. No servidor de roteamento usa-se o *localhost* (127.0.0.1) para acesso às portas.

telnet 127.0.0.1 2601 - modo roteamento Zebra

telnet 127.0.0.1 2505 - modo protocolo BGP

Configurando o ambiente do primeiro experimento

Em um *switch* 2900 foram conectados 3 roteadores 2500 e o servidor de roteamento, de acordo com a topologia abaixo:

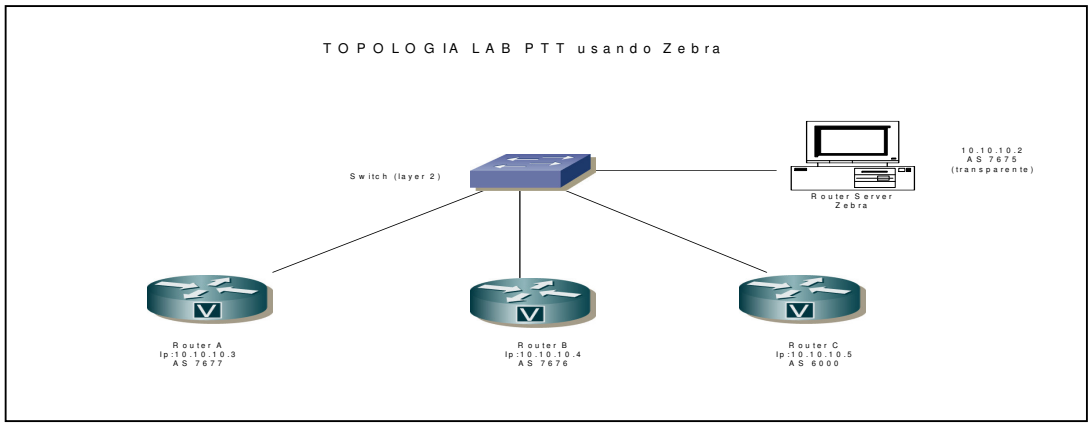


FIGURA 14 -Topologia inicial do experimento

Obs.: Tanto na porta do *switch* quanto no servidor de roteamento foram ajustadas a velocidade 100 Mbps e o modo *Full-duplex*, a fim de garantir a performance de transmissão do servidor.

Nas portas do *switch* não foram realizados estes ajustes para conectar os roteadores, pois eles só suportavam a velocidade 10 Mbps.

Em cada roteador foram realizados anúncios de redes, conforme a tabela abaixo. É bom ressaltar que os endereços e os AS(s) usados nos experimentos eram fictícios.

TABELA 14 - Bloco de endereços do experimento

Roteador A AS7677 Ip 10.10.10.3	Roteador B AS 7676 Ip 10.10.10.4	Roteador C AS 6000 Ip 10.10.10.5	Servidor Roteamento Ip 10.10.10.2
120.0.0.0/24	130.0.0.0/8	150.0.0.0/8	1.0.0.0/8
121.0.0.0/24	131.0.0.0/8	151.0.0.0/8	2.0.0.0/8
122.0.0.0/24	132.0.0.0/8	152.0.0.0/8	3.0.0.0/8
123.0.0.0/24	133.0.0.0/8	153.0.0.0/8	4.0.0.0/8
124.0.0.0/24	134.0.0.0/8	154.0.0.0/8	5.0.0.0/8
125.0.0.0/24	135.0.0.0/8	155.0.0.0/8	6.0.0.0/8
	136.0.0.0/8	156.0.0.0/8	7.0.0.0/8
número de rotas: 6	137.0.0.0/8		8.0.0.0/8

	138.0.0.0/8 139.0.0.0/8 140.0.0.0/8 número de rotas:11	número de rotas:7	9.0.0.0/8 10.10.10.0/24 19.0.0.0/8 29.0.0.0/8 39.0.0.0/8 49.0.0.0/8 59.0.0.0/8 69.0.0.0/8 79.0.0.0/8 89.0.0.0/8 número de rotas :18

Obs.: As redes anunciadas não foram sumarizadas.

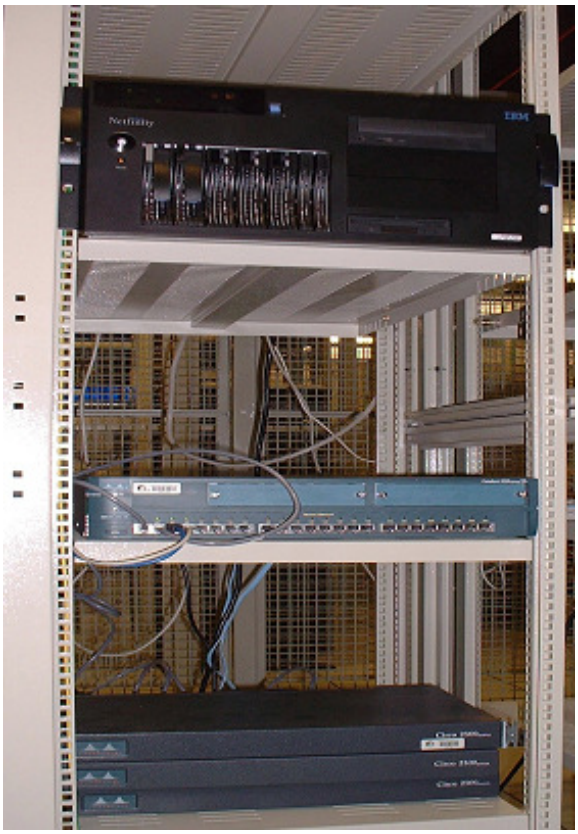


FIGURA 15- Rack do experimento

Esta foto mostra o *rack* do experimento com os seguintes equipamentos (de cima para baixo):

-O servidor de roteamento, máquina Netfinity.

-O *switch* de 24 portas Cisco 2924

- 3 roteadores Cisco 2501

É necessário ressaltar que todos os participantes têm como vizinho BGP, o servidor de roteamento.

A configuração dos roteadores dos participantes e do servidor de roteamento está devidamente explicada no APÊNDICE A.

Análise do funcionamento do BGP no PTT

- **As redes recebidas pelos participantes**

Verificou-se se os participantes estabeleceram a sessão BGP com o servidor de roteamento, e se receberam suas rotas através do comando (**sh ip bgp summary**). Foi necessário entrar nos roteadores dos participantes e/ou verificar diretamente no servidor de roteamento. A análise foi realizada de duas maneiras: na primeira, a verificação nos roteadores dos participantes deverá mostrar o recebimento das rotas de todos os outros participantes; na segunda, no servidor de roteamento, a verificação mostrará as redes de todos participantes.

```
routerA#sh ip bgp summary
BGP table version is 342, main routing table version 342
42 network entries (42/126 paths) using 8736 bytes of memory
4 BGP path attribute entries using 388 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.2      4  7675    1188    1184      342    0    0 02:54:44       36
```

Pode-se notar que o roteador A estabeleceu a seção BGP com o servidor de roteamento endereçado pelo IP 10.10.10.2 (coluna Neighbor). A conexão foi estabelecida por duas horas e cinqüenta e quatro minutos (coluna up/down),

recebendo 36 rotas (coluna State/PfxRcd). Pode-se ver, ainda, o número 7675 de identificação do Autonomous System do servidor de roteamento (coluna AS) e a quantidade de mensagens trocadas (colunas MsgRcvd e MsgSent).

No roteador B, pela mesma análise do roteador A, observa-se o recebimento de 31 rotas, o tempo de conexão e a quantidade de mensagens trocadas.

```
routerB#sh ip bgp summary
BGP table version is 250, main routing table version 250
42 network entries (42/126 paths) using 8736 bytes of memory
4 BGP path attribute entries using 424 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.2      4  7675    1230    1223      250    0    0 03:01:42
31
```

No roteador C, constata-se o recebimento de 35 rotas.

```
routerC#sh ip bgp summary
BGP table version is 286, main routing table version 286
42 network entries (42/126 paths) using 8736 bytes of memory
4 BGP path attribute entries using 492 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.2      4  7675    1207    1205      286    0    0 03:03:20
35
```

E, para concluir a análise:

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
4 BGP AS-PATH entries
0 BGP community entries

Neighbor        V     AS   MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677     187     190        0    0    0    0 03:04:07        6
10.10.10.4      4  7676     187     190        0    0    0    0 03:04:08       11
10.10.10.5      4  6000     187     190        0    0    0    0 03:04:07        7
```

O servidor de roteamento recebe as rotas de cada participante, ou seja, dos roteadores A (AS 7677), B (AS 7676) e C (AS 6000). O último quadro mostra que o servidor de roteamento (10.10.10.2) recebeu 6 rotas do roteador A (10.10.10.3), 11 do roteador B (10.10.10.4) e 7 do roteador C (10.10.10.5), totalizando 24 rotas.

Observa-se que o servidor de roteamento anunciou 18 rotas. Chega-se a esse número analisando-se os demais resultados.

O roteador A recebeu 36 rotas, ou seja, a soma de 11 rotas do roteador B, com 7 rotas do roteador C e 18 rotas do servidor de roteamento.

O roteador B recebeu 31 rotas, a soma das 6 rotas do roteador A, com 7 rotas do roteador C e 18 rotas do servidor de roteamento.

O roteador C recebeu 35 rotas, ou seja, a soma das 6 rotas do roteador A, com 11 rotas do roteador B e 18 rotas do servidor de roteamento.

Tabela de roteamento do servidor de roteamento Zebra

Através do comando sh ip bgp, verificou-se a tabela de rotas BGP do servidor de roteamento.

Pode-se observar todas as redes pertencentes a cada participante, e o atributo *next-hop* de cada rota, ou seja, o endereço IP do participante que a anunciou. Portanto, rotas originadas no IP 10.10.10.3 foram anunciadas pelo roteador A; no IP 10.10.10.4 foram anunciadas pelo roteador B; no IP 10.10.10.5 foram anunciadas

pelo roteador C e no IP 0.0.0.0 foram anunciadas pelo próprio servidor de roteamento. Verifica-se, também, o AS de cada participante, ou seja, AS 7677 provenientes do roteador A; AS 7676 do roteador B; e AS 6000 do roteador C, além das rotas do próprio servidor de roteamento.

```
bgpd# sh ip bgp
BGP table version is 0, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0                  0         32768 i
*> 2.0.0.0          0.0.0.0                  0         32768 i
*> 3.0.0.0          0.0.0.0                  0         32768 i
*> 4.0.0.0          0.0.0.0                  0         32768 i
*> 5.0.0.0          0.0.0.0                  0         32768 i
*> 6.0.0.0          0.0.0.0                  0         32768 i
*> 7.0.0.0          0.0.0.0                  0         32768 i
*> 8.0.0.0          0.0.0.0                  0         32768 i
*> 9.0.0.0          0.0.0.0                  0         32768 i
*> 10.10.10.0/24    0.0.0.0                  0         32768 i
*> 19.0.0.0         0.0.0.0                  0         32768 i
*> 29.0.0.0         0.0.0.0                  0         32768 i
*> 39.0.0.0         0.0.0.0                  0         32768 i
*> 49.0.0.0         0.0.0.0                  0         32768 i
*> 59.0.0.0         0.0.0.0                  0         32768 i
*> 69.0.0.0         0.0.0.0                  0         32768 i
*> 79.0.0.0         0.0.0.0                  0         32768 i
*> 89.0.0.0         0.0.0.0                  0         32768 i
*> 120.0.0.0        10.10.10.3               0             0 7677 i
*> 121.0.0.0        10.10.10.3               0             0 7677 i
*> 122.0.0.0        10.10.10.3               0             0 7677 i
*> 123.0.0.0        10.10.10.3               0             0 7677 i
*> 124.0.0.0        10.10.10.3               0             0 7677 i
*> 125.0.0.0        10.10.10.3               0             0 7677 i
*> 130.0.0.0/8      10.10.10.4               0             0 7676 i
*> 131.0.0.0/8      10.10.10.4               0             0 7676 i
*> 132.0.0.0/8      10.10.10.4               0             0 7676 i
*> 133.0.0.0/8      10.10.10.4               0             0 7676 i
*> 134.0.0.0/8      10.10.10.4               0             0 7676 i
*> 135.0.0.0/8      10.10.10.4               0             0 7676 i
*> 136.0.0.0/8      10.10.10.4               0             0 7676 I
*> 137.0.0.0/8      10.10.10.4               0             0 7676 i
*> 138.0.0.0/8      10.10.10.4               0             0 7676 i
*> 139.0.0.0/8      10.10.10.4               0             0 7676 i
*> 140.0.0.0/8      10.10.10.4               0             0 7676 i
*> 150.0.0.0/8      10.10.10.5               0             0 6000 i
*> 151.0.0.0/8      10.10.10.5               0             0 6000 i
*> 152.0.0.0/8      10.10.10.5               0             0 6000 i
*> 153.0.0.0/8      10.10.10.5               0             0 6000 i
*> 154.0.0.0/8      10.10.10.5               0             0 6000 i
*> 155.0.0.0/8      10.10.10.5               0             0 6000 i
*> 156.0.0.0/8      10.10.10.5               0             0 6000 i

Total number of prefixes 42
```

Pode-se verificar o recebimento de rotas de um vizinho específico através dos comandos de análise:

sh ip bgp neighbors (IP servidor de roteamento) route

O próximo quadro mostra as rotas recebidas pelo roteador A:

```
routerA#sh ip bgp neighbors 10.10.10.2 routes
BGP table version is 342, local router ID is 10.10.10.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          10.10.10.2               0             0 7675 i
*> 2.0.0.0          10.10.10.2               0             0 7675 i
*> 3.0.0.0          10.10.10.2               0             0 7675 i
*> 4.0.0.0          10.10.10.2               0             0 7675 i
*> 5.0.0.0          10.10.10.2               0             0 7675 i
*> 6.0.0.0          10.10.10.2               0             0 7675 i
*> 7.0.0.0          10.10.10.2               0             0 7675 i
*> 8.0.0.0          10.10.10.2               0             0 7675 i
*> 9.0.0.0          10.10.10.2               0             0 7675 i
*> 10.10.10.0/24    10.10.10.2               0             0 7675 i
*> 19.0.0.0         10.10.10.2               0             0 7675 i
*> 29.0.0.0         10.10.10.2               0             0 7675 i
*> 39.0.0.0         10.10.10.2               0             0 7675 i
*> 49.0.0.0         10.10.10.2               0             0 7675 i
*> 59.0.0.0         10.10.10.2               0             0 7675 i
*> 69.0.0.0         10.10.10.2               0             0 7675 i
*> 79.0.0.0         10.10.10.2               0             0 7675 i
*> 89.0.0.0         10.10.10.2               0             0 7675 i
   Network          Next Hop            Metric LocPrf Weight Path
*> 130.0.0.0/8      10.10.10.4                             0 7676 i
*> 131.0.0.0/8      10.10.10.4                             0 7676 i
*> 132.0.0.0/8      10.10.10.4                             0 7676 i
*> 133.0.0.0/8      10.10.10.4                             0 7676 i
*> 134.0.0.0/8      10.10.10.4                             0 7676 i
*> 135.0.0.0/8      10.10.10.4                             0 7676 i
*> 136.0.0.0/8      10.10.10.4                             0 7676 i
*> 137.0.0.0/8      10.10.10.4                             0 7676 i
*> 138.0.0.0/8      10.10.10.4                             0 7676 i
*> 139.0.0.0/8      10.10.10.4                             0 7676 i
*> 140.0.0.0/8      10.10.10.4                             0 7676 i
*> 150.0.0.0/8      10.10.10.5                             0 6000 i
*> 151.0.0.0/8      10.10.10.5                             0 6000 i
*> 152.0.0.0/8      10.10.10.5                             0 6000 i
*> 153.0.0.0/8      10.10.10.5                             0 6000 i
*> 154.0.0.0/8      10.10.10.5                             0 6000 i
*> 155.0.0.0/8      10.10.10.5                             0 6000 i
*> 156.0.0.0/8      10.10.10.5                             0 6000 i
```

Com este comando observou-se a tabela de roteamento do roteador A, no qual constam as rotas enviadas pelo servidor de roteamento, pelo roteador B e pelo roteador C, respectivamente.

Os roteadores B, C e servidor de roteamento mostram:

Roteador B – Rotas anunciadas pelos roteadores A, C e servidor de roteamento.

Roteador C – Rotas anunciadas pelos roteadores A, B e servidor de roteamento.
Servidor de roteamento – Rotas anunciadas pelos roteadores A,B e C.

- **As redes exportadas pelos participantes**

No item anterior foi visto que os participantes enviaram suas rotas através da tabela de roteamento do servidor de roteamento. No entanto, pode-se confirmar as redes anunciadas de cada participante através da execução do comando abaixo:

sh ip bgp neighbors (IP servidor de roteamento) advertised-routes

Verificam-se as rotas anunciadas pelo roteador A:

```
routerA#sh ip bgp neighbors 10.10.10.2 advertised-routes
BGP table version is 342, local router ID is 10.10.10.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 120.0.0.0        0.0.0.0                  0         32768 i
*> 121.0.0.0        0.0.0.0                  0         32768 i
*> 122.0.0.0        0.0.0.0                  0         32768 i
*> 123.0.0.0        0.0.0.0                  0         32768 i
*> 124.0.0.0        0.0.0.0                  0         32768 i
*> 125.0.0.0        0.0.0.0                  0         32768 i
```

O roteador A anunciou 6 redes, começando pela **120 .0.0.0 até a 125.0.0.0**
Pode-se repetir o exemplo acima para cada participante, da seguinte forma:

As rotas anunciadas pelo roteador B:

```
routerB# sh ip bgp neighbors 10.10.10.2 advertised-routes
BGP table version is 250, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 130.0.0.0/8      0.0.0.0                  0         32768 i
*> 131.0.0.0/8      0.0.0.0                  0         32768 i
*> 132.0.0.0/8      0.0.0.0                  0         32768 i
*> 133.0.0.0/8      0.0.0.0                  0         32768 i
*> 134.0.0.0/8      0.0.0.0                  0         32768 i
*> 135.0.0.0/8      0.0.0.0                  0         32768 i
*> 136.0.0.0/8      0.0.0.0                  0         32768 i
*> 137.0.0.0/8      0.0.0.0                  0         32768 i
*> 138.0.0.0/8      0.0.0.0                  0         32768 i
*> 139.0.0.0/8      0.0.0.0                  0         32768 i
*> 140.0.0.0/8      0.0.0.0                  0         32768 i
```

O roteador B anunciou 11 redes, ou seja, de 130 até a 140. Pode-se ver, ainda, que todas as máscaras eram /8 que corresponde à máscara 255.0.0.0. A tabela de máscara binária pode ser vista no ANEXO C.

O roteador C anuncia 7 redes, começando da 150 até a 156 com máscara /8 também.

```
routerC#sh ip bgp neighbors 10.10.10.2 advertised-routes
BGP table version is 286, local router ID is 3.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 150.0.0.0/8      0.0.0.0                  0         32768 i
*> 151.0.0.0/8      0.0.0.0                  0         32768 i
*> 152.0.0.0/8      0.0.0.0                  0         32768 i
*> 153.0.0.0/8      0.0.0.0                  0         32768 i
*> 154.0.0.0/8      0.0.0.0                  0         32768 i
*> 155.0.0.0/8      0.0.0.0                  0         32768 i
*> 156.0.0.0/8      0.0.0.0                  0         32768 i
```

Da mesma forma, pode-se verificar se o servidor de roteamento divulgou rotas para os participantes:

```
bgpd# sh ip bgp neighbors 10.10.10.3 advertised-routes
BGP table version is 0, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          10.10.10.2               0         32768 i
*> 2.0.0.0          10.10.10.2               0         32768 i
*> 3.0.0.0          10.10.10.2               0         32768 i
*> 4.0.0.0          10.10.10.2               0         32768 i
*> 5.0.0.0          10.10.10.2               0         32768 i
*> 6.0.0.0          10.10.10.2               0         32768 i
*> 7.0.0.0          10.10.10.2               0         32768 i
*> 8.0.0.0          10.10.10.2               0         32768 i
*> 9.0.0.0          10.10.10.2               0         32768 i
*> 10.10.10.0/24    10.10.10.2               0         32768 i
*> 19.0.0.0         10.10.10.2               0         32768 i
*> 29.0.0.0         10.10.10.2               0         32768 i
*> 39.0.0.0         10.10.10.2               0         32768 i
*> 49.0.0.0         10.10.10.2               0         32768 i
*> 59.0.0.0         10.10.10.2               0         32768 i
*> 69.0.0.0         10.10.10.2               0         32768 i
*> 79.0.0.0         10.10.10.2               0         32768 i
*> 89.0.0.0         10.10.10.2               0         32768 i
*> 130.0.0.0/8      10.10.10.4                         0 7676 i
*> 131.0.0.0/8      10.10.10.4                         0 7676 i
*> 132.0.0.0/8      10.10.10.4                         0 7676 i
*> 133.0.0.0/8      10.10.10.4                         0 7676 i
*> 134.0.0.0/8      10.10.10.4                         0 7676 i
*> 135.0.0.0/8      10.10.10.4                         0 7676 i
*> 136.0.0.0/8      10.10.10.4                         0 7676 i
*> 137.0.0.0/8      10.10.10.4                         0 7676 i
*> 138.0.0.0/8      10.10.10.4                         0 7676 i
*> 139.0.0.0/8      10.10.10.4                         0 7676 i
*> 140.0.0.0/8      10.10.10.4                         0 7676 i
*> 150.0.0.0/8      10.10.10.5                         0 6000 i
*> 151.0.0.0/8      10.10.10.5                         0 6000 i
*> 152.0.0.0/8      10.10.10.5                         0 6000 i
*> 153.0.0.0/8      10.10.10.5                         0 6000 i
*> 154.0.0.0/8      10.10.10.5                         0 6000 i
*> 155.0.0.0/8      10.10.10.5                         0 6000 i
*> 156.0.0.0/8      10.10.10.5                         0 6000 i

Total number of prefixes 36
```

Verificam-se as redes anunciadas do servidor de roteamento para o roteador A:

O servidor de roteamento anunciou as primeiras 18 redes que foram geradas por ele e as redes pertencentes ao roteador B e C . Verificou-se, também, o AS que cada participante anunciou. As configurações dos roteadores e do servidor de roteamento estão no APÊNDICE A.

```
bgpd# sh ip bgp neighbors 10.10.10.4 advertised-routes
BGP table version is 0, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          10.10.10.2               0         32768 i
*> 2.0.0.0          10.10.10.2               0         32768 i
*> 3.0.0.0          10.10.10.2               0         32768 i
*> 4.0.0.0          10.10.10.2               0         32768 i
*> 5.0.0.0          10.10.10.2               0         32768 i
*> 6.0.0.0          10.10.10.2               0         32768 i
*> 7.0.0.0          10.10.10.2               0         32768 i
*> 8.0.0.0          10.10.10.2               0         32768 i
*> 9.0.0.0          10.10.10.2               0         32768 i
*> 10.10.10.0/24    10.10.10.2               0         32768 i
*> 19.0.0.0         10.10.10.2               0         32768 i
*> 29.0.0.0         10.10.10.2               0         32768 i
*> 39.0.0.0         10.10.10.2               0         32768 i
*> 49.0.0.0         10.10.10.2               0         32768 i
*> 59.0.0.0         10.10.10.2               0         32768 i
*> 69.0.0.0         10.10.10.2               0         32768 i
*> 79.0.0.0         10.10.10.2               0         32768 i
*> 89.0.0.0         10.10.10.2               0         32768 i
*> 120.0.0.0        10.10.10.3                         0 7677 i
*> 121.0.0.0        10.10.10.3                         0 7677 i
*> 122.0.0.0        10.10.10.3                         0 7677 i
*> 123.0.0.0        10.10.10.3                         0 7677 i
*> 124.0.0.0        10.10.10.3                         0 7677 i
*> 125.0.0.0        10.10.10.3                         0 7677 i
*> 150.0.0.0/8      10.10.10.5                         0 6000 i
*> 151.0.0.0/8      10.10.10.5                         0 6000 i
*> 152.0.0.0/8      10.10.10.5                         0 6000 i
*> 153.0.0.0/8      10.10.10.5                         0 6000 i
*> 154.0.0.0/8      10.10.10.5                         0 6000 i
*> 155.0.0.0/8      10.10.10.5                         0 6000 i
*> 156.0.0.0/8      10.10.10.5                         0 6000 i

Total number of prefixes 31
```

Verificam-se as redes anunciadas para o roteador B:

Para os roteadores B pode-se ver o anúncio das redes do servidor de roteamento e as dos roteadores A e C.

Verificam-se as rotas anunciadas para o roteador C:

```
bgpd# sh ip bgp neighbors 10.10.10.5 advertised-routes
BGP table version is 0, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          10.10.10.2               0         32768 i
*> 2.0.0.0          10.10.10.2               0         32768 i
*> 3.0.0.0          10.10.10.2               0         32768 i
*> 4.0.0.0          10.10.10.2               0         32768 i
*> 5.0.0.0          10.10.10.2               0         32768 i
*> 6.0.0.0          10.10.10.2               0         32768 i
*> 7.0.0.0          10.10.10.2               0         32768 i
*> 8.0.0.0          10.10.10.2               0         32768 i
*> 9.0.0.0          10.10.10.2               0         32768 i
*> 10.10.10.0/24    10.10.10.2               0         32768 i
*> 19.0.0.0         10.10.10.2               0         32768 i
*> 29.0.0.0         10.10.10.2               0         32768 i
*> 39.0.0.0         10.10.10.2               0         32768 i
*> 49.0.0.0         10.10.10.2               0         32768 i
*> 59.0.0.0         10.10.10.2               0         32768 i
*> 69.0.0.0         10.10.10.2               0         32768 i
*> 79.0.0.0         10.10.10.2               0         32768 i
*> 89.0.0.0         10.10.10.2               0         32768 i
*> 120.0.0.0        10.10.10.3                         0 7677 i
*> 121.0.0.0        10.10.10.3                         0 7677 i
*> 122.0.0.0        10.10.10.3                         0 7677 i
*> 123.0.0.0        10.10.10.3                         0 7677 i
*> 124.0.0.0        10.10.10.3                         0 7677 i
*> 125.0.0.0        10.10.10.3                         0 7677 i
*> 130.0.0.0/8      10.10.10.4                         0 7676 i
*> 131.0.0.0/8      10.10.10.4                         0 7676 i
*> 132.0.0.0/8      10.10.10.4                         0 7676 i
*> 133.0.0.0/8      10.10.10.4                         0 7676 i
*> 134.0.0.0/8      10.10.10.4                         0 7676 i
*> 135.0.0.0/8      10.10.10.4                         0 7676 i
*> 136.0.0.0/8      10.10.10.4                         0 7676 i
*> 137.0.0.0/8      10.10.10.4                         0 7676 i
*> 138.0.0.0/8      10.10.10.4                         0 7676 i
*> 139.0.0.0/8      10.10.10.4                         0 7676 i
*> 140.0.0.0/8      10.10.10.4                         0 7676 i
Total number of prefixes 35
```

No roteador C, pode-se ver as redes do servidor de roteamento, do roteador A e B, respectivamente.

Concluindo, pode-se analisar, através dos três exemplos anteriores, que todos os participantes receberam todas as rotas, com exceção da sua própria rota.

- **O servidor de roteamento é transparente nos anúncios de rotas**

Entrando em um dos participantes e verificando as redes recebidas, observou-se que o servidor de roteamento está sendo transparente.

Por exemplo, entrando no roteador B e verificando as rotas recebidas, obteve-se:

```
routerB#sh ip bgp neighbors 10.10.10.2 routes
BGP table version is 250, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          10.10.10.2               0             0 7675 i
*> 2.0.0.0          10.10.10.2               0             0 7675 i
*> 3.0.0.0          10.10.10.2               0             0 7675 i
*> 4.0.0.0          10.10.10.2               0             0 7675 i
*> 5.0.0.0          10.10.10.2               0             0 7675 i
*> 6.0.0.0          10.10.10.2               0             0 7675 i
*> 7.0.0.0          10.10.10.2               0             0 7675 i
*> 8.0.0.0          10.10.10.2               0             0 7675 i
*> 9.0.0.0          10.10.10.2               0             0 7675 i
*> 10.10.10.0/24    10.10.10.2               0             0 7675 i
*> 19.0.0.0         10.10.10.2               0             0 7675 i
*> 29.0.0.0         10.10.10.2               0             0 7675 i
*> 39.0.0.0         10.10.10.2               0             0 7675 i
*> 49.0.0.0         10.10.10.2               0             0 7675 i
*> 59.0.0.0         10.10.10.2               0             0 7675 i
*> 69.0.0.0         10.10.10.2               0             0 7675 i
*> 79.0.0.0         10.10.10.2               0             0 7675 i
*> 89.0.0.0         10.10.10.2               0             0 7675 i
   Network          Next Hop            Metric LocPrf Weight Path
*> 120.0.0.0        10.10.10.3                             0 7677 i
*> 121.0.0.0        10.10.10.3                             0 7677 i
*> 122.0.0.0        10.10.10.3                             0 7677 i
*> 123.0.0.0        10.10.10.3                             0 7677 i
*> 124.0.0.0        10.10.10.3                             0 7677 i
*> 125.0.0.0        10.10.10.3                             0 7677 i
*> 150.0.0.0/8      10.10.10.5                             0 6000 i
*> 151.0.0.0/8      10.10.10.5                             0 6000 i
*> 152.0.0.0/8      10.10.10.5                             0 6000 i
*> 153.0.0.0/8      10.10.10.5                             0 6000 i
*> 154.0.0.0/8      10.10.10.5                             0 6000 i
*> 155.0.0.0/8      10.10.10.5                             0 6000 i
*> 156.0.0.0/8      10.10.10.5                             0 6000 i

Total number of prefixes 31
```

Pode-se ver que o atributo *nexthop* de cada rota indica o participante que a anunciou. O servidor de roteamento não assume a autoria para todas. Isto é muito importante, pois o tráfego não passou pelo servidor de roteamento.

- **A configuração adequada para os roteadores dos participantes e servidor de roteamento.**

As configurações dos roteadores e do servidor de roteamento encontram-se no APÊNDICE A.

Para analisar as próximas questões, foi necessário alterar a topologia do experimento.

- 1- O servidor de roteamento recebe as rotas do participante que não está conectado diretamente?
- 2- O servidor de roteamento é transparente para o participante não conectado?

Na nova topologia, os roteadores A e B continuam tendo como vizinho o servidor de roteamento. O roteador C foi desconectado do *switch* e conectado apenas ao roteador A. O roteador C tem como vizinho somente o roteador A.

Pode-se ver esta nova topologia na figura 16:

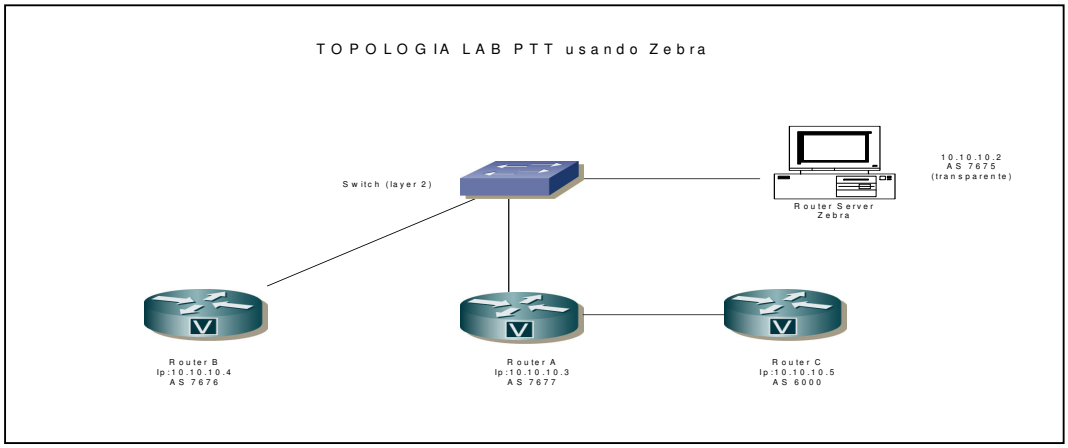


FIGURA 16 -Topologia segundo o experimento

Para a construção da topologia acima, foi necessário alterar a configuração dos roteadores A e C para incluir os respectivos vizinhos BGP, roteadores C e A.

Também foi necessário excluir o servidor de roteamento, como vizinho BGP ativo, da configuração do roteador C.

Com a nova arquitetura de vizinhança estabelecida, foram acompanhados alguns estados de conexão de modo semelhante ao que foi visto anteriormente, na máquina de estado do BGP, ou seja, através do comando **sh ip bgp summary**. Essa análise de estados, que foi feita após a alteração da configuração, encontra-se no APÊNDICE B.

- **O recebimento de rotas pelo servidor de roteamento do participante que não esteve diretamente conectado.**

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
4 BGP AS-PATH entries
0 BGP community entries

Neighbor        V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677      40      45        0    0    0 00:02:42      6
10.10.10.4      4  7676      34      41        0    0    0 00:31:04     11
```

Observou-se que o servidor de roteamento não recebeu redes do roteador C, pois só recebeu 6 rotas do A. Isto é devido ao filtro que estava configurado no servidor de roteamento. A seguir, mostra-se o filtro:

ip as-path access-list routera permit ^7677$ (permite apenas as redes originadas do Autonomous System do roteador A).

Alterou-se o filtro no servidor de roteamento para receber as rotas do roteador C:

ip as-path access-list routera permit *_7677_* (Rotas que atravessam o roteador A).

Para validar o filtro, foi necessário reiniciar a conexão BGP com o roteador A.

Clear ip bgp 10.10.10.3

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
4 BGP AS-PATH entries
0 BGP community entries

Neighbor          V      AS  MsgRcvd  MsgSent     TblVer   InQ  OutQ  Up/Down
State/PfxRcd
10.10.10.3        4  7677     40       45          0    0    0 00:02:46      13
10.10.10.4        4  7676     34       41          0    0    0 00:31:08      11
```

Confirmou-se o recebimento dos anúncios:

Nota-se que o servidor de roteamento passou a receber 13 rotas do roteador A e não 6.

- **A transparência AS do servidor de roteamento para o participante não conectado.**

Neste caso, foi necessário verificar a tabela de roteamento bgp do roteador C.

No roteador C

```
routerc#sh ip bgp
BGP table version is 746, local router ID is 3.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          192.168.10.2                           0 7677 7675 i
*> 2.0.0.0          192.168.10.2                           0 7677 7675 i
*> 3.0.0.0          192.168.10.2                           0 7677 7675 i
*> 4.0.0.0          192.168.10.2                           0 7677 7675 i
*> 5.0.0.0          192.168.10.2                           0 7677 7675 i
*> 6.0.0.0          192.168.10.2                           0 7677 7675 i
*> 7.0.0.0          192.168.10.2                           0 7677 7675 i
*> 8.0.0.0          192.168.10.2                           0 7677 7675 i
*> 9.0.0.0          192.168.10.2                           0 7677 7675 i
*> 10.10.10.0/24    192.168.10.2                           0 7677 7675 i
*> 19.0.0.0         192.168.10.2                           0 7677 7675 i
*> 29.0.0.0         192.168.10.2                           0 7677 7675 i
*> 39.0.0.0         192.168.10.2                           0 7677 7675 i
*> 49.0.0.0         192.168.10.2                           0 7677 7675 i
*> 59.0.0.0         192.168.10.2                           0 7677 7675 i
*> 69.0.0.0         192.168.10.2                           0 7677 7675 i
*> 79.0.0.0         192.168.10.2                           0 7677 7675 i
*> 89.0.0.0         192.168.10.2                           0 7677 7675 i
*> 120.0.0.0        192.168.10.2             0             0 7677 i
*> 121.0.0.0        192.168.10.2             0             0 7677 i
*> 122.0.0.0        192.168.10.2             0             0 7677 i
*> 123.0.0.0        192.168.10.2             0             0 7677 i
*> 124.0.0.0        192.168.10.2             0             0 7677 i
*> 125.0.0.0        192.168.10.2             0             0 7677 i
*> 130.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 131.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 132.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 133.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 134.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 135.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 136.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 137.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 138.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 139.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 140.0.0.0/8      192.168.10.2                           0 7677 7676 i
*> 150.0.0.0/8      0.0.0.0                  0         32768 i
*> 151.0.0.0/8      0.0.0.0                  0         32768 i
*> 152.0.0.0/8      0.0.0.0                  0         32768 i
*> 153.0.0.0/8      0.0.0.0                  0         32768 i
*> 154.0.0.0/8      0.0.0.0                  0         32768 i
*> 155.0.0.0/8      0.0.0.0                  0         32768 i
*> 156.0.0.0/8      0.0.0.0                  0         32768 i
routerc#
```

Confirma-se, por meio do atributo AS-PATH, que o roteador C alcança o roteador B, sem que o tráfego passe pelo servidor de roteamento, ou seja, para

alcançar a rede 130.0.0.0/8, o fluxo que sai do roteador C, passa pelo AS 7677 (roteador A) e, posteriormente, pelo AS7676 (roteador B).

***> 130.0.0.0/8 192.168.10.2 0 7677 7676 i**

- **Com base nas pesquisas dos principais PTT(s), aplicaram-se políticas de segurança através dos filtros BGP no participante e no servidor de roteamento**

A maioria das políticas de segurança foi feita com a utilização de filtros no BGP.

Bloqueio rota default

Uma questão muito importante para a segurança, tanto dos participantes quanto do servidor de roteamento, é bloquear o recebimento da rota *default*.

O recebimento da rota *default* por um participante ou pelo servidor de roteamento certamente gera um problema de roteamento. Pode-se resolver isto através dos filtros no servidor de roteamento e/ou nos participantes.

Neste experimento, foi aplicado um filtro na conexão BGP do servidor de roteamento com o roteador A, de modo a não permitir o recebimento da rota *default* pelo servidor de roteamento. Posteriormente, foi configurado o anúncio da rota *default* no roteador A, e verificou-se que o servidor de roteamento não aprendeu a rota *default*. Após isto, foi retirado o filtro aplicado no servidor de roteamento e observado que ele recebeu a rota *default*.

Filtro configurado no servidor de roteamento:

neighbor 10.10.10.3 distribute-list 199 in
access-list 199 deny ip host 0.0.0.0 any
access-list 199 permit ip any any

Anúncio da rota *default* configurado no roteador A:

network 0.0.0.0

ip route 0.0.0.0 0.0.0.0 Null0 (para o roteador ter a rota na sua tabela de roteamento e divulgá-la).

Conferiu-se a rota default divulgada pelo roteador A:

```
routerA#sh ip bgp neighbors 10.10.10.2 advertised-routes
BGP table version is 581, local router ID is 10.10.10.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          0.0.0.0                  0         32768 i
*> 120.0.0.0        0.0.0.0                  0         32768 i
*> 121.0.0.0        0.0.0.0                  0         32768 i
*> 122.0.0.0        0.0.0.0                  0         32768 i
*> 123.0.0.0        0.0.0.0                  0         32768 i
*> 124.0.0.0        0.0.0.0                  0         32768 i
*> 125.0.0.0        0.0.0.0                  0         32768 i
*> 150.0.0.0/8      192.168.10.1             0             0 6000 i
*> 151.0.0.0/8      192.168.10.1             0             0 6000 i
*> 152.0.0.0/8      192.168.10.1             0             0 6000 i
*> 153.0.0.0/8      192.168.10.1             0             0 6000 i
*> 154.0.0.0/8      192.168.10.1             0             0 6000 i
*> 155.0.0.0/8      192.168.10.1             0             0 6000 i
*> 156.0.0.0/8      192.168.10.1             0             0 6000 i
```

Fez-se a conferência das rotas recebidas pelo servidor de roteamento. Constatou-se que o servidor de roteamento não recebeu a rota *default*:

```
bgpd# sh ip bgp 0.0.0.0
% Network not in table
```

Removeu-se o filtro para verificar se o servidor de roteamento recebeu a rota *default*.

Router bgp 7675

no Neighboors 10.10.10.3 distribute-list 199 in

clear ip bgp 10.10.10.3 (limpando o BGP para forçar o recebimento dos novos anúncios).

Após a exclusão do filtro, a rota *default* foi encontrada na tabela de roteamento do servidor de roteamento:

```
bgpd# sh ip bgp 0.0.0.0
BGP routing table entry for 0.0.0.0/0
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  10.10.10.4
  7677
    10.10.10.3 from 10.10.10.3 (10.10.10.3)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Last update: Fri Aug 22 15:03:01 2003
```

O filtro aplicado no servidor de roteamento também pode ser usado ao lado dos participantes.

- **Bloqueio da quantidade de redes divulgadas**

Outra questão importante foi garantir que os participantes não divulgassem muitas redes para o servidor de roteamento. As redes devem ser sumarizadas para facilitar a administração da tabela de roteamento e diminuir o processamento do roteador. Além disso, é necessário evitar o recebimento da tabela completa de rotas do BGP, que tem mais do que cem mil rotas e consome CPU e memória. O comando **maximum-prefix** limita o recebimento da quantidade de redes; caso receba mais redes do que o mencionado no comando, a conexão BGP é interrompida. Neste experimento, o recebimento foi limitado a 10 anúncios, através do comando:

neighbor *Endereço Ip Vizinho* **maximum-prefix** *número máximo de prefixos*

O servidor de roteamento recebe no máximo 10 anúncios do roteador A.

neighbor 10.10.10.3 maximum-prefix 10

Após esta inclusão, foram feitos mais 4 anúncios no roteador A, totalizando 11 anúncios. Fixado este limite, a conexão BGP foi interrompida ao atingir 10 anúncios.

Redes anunciadas no Roteador A:

network 120.0.0.0
network 121.0.0.0
network 122.0.0.0
network 123.0.0.0
network 124.0.0.0
network 125.0.0.0
network 126.10.10.0 mask 255.255.255.252
network 126.10.10.4 mask 255.255.255.252
network 126.10.10.8 mask 255.255.255.252
network 126.10.10.12 mask 255.255.255.252

Observando a conexão BGP:

No servidor de roteamento pode-se observar que o vizinho 10.10.10.3 possui o parâmetro **(PfxCt)** , ou seja, a quantidade de anúncios ultrapassou o limite.

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677    1415    1425        0    0    0 00:10:20 Idle (PfxCt)
10.10.10.4      4  7676    1412    1423        0    0    0 23:29:39       11
10.10.10.5      4  6000       0       0        0    0    0 00:01:28 Active
```

Removeram-se os anúncios do roteador A para verificar o que acontece com a conexão.

router bgp 7677

no network 126.10.10.0 mask 255.255.255.252

no network 126.10.10.4 mask 255.255.255.252

no network 126.10.10.8 mask 255.255.255.252

no network 126.10.10.12 mask 255.255.255.252

Verificou-se no servidor de roteamento que a conexão do vizinho 10.10.10.3 restabeleceu-se:

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677    1422    1442        0    0    0 00:00:02        6
10.10.10.4      4  7676    1419    1429        0    0    0 23:36:07       11
10.10.10.5      4  6000       0       0        0    0    0 00:01:56 Active
```

Conclusão da primeira fase do experimento

Com os experimentos realizados, verificou-se que o servidor de roteamento Zebra atendeu aos requisitos do funcionamento do PTT, ou seja :

- Proporcionou melhor configuração para cada participante e para o servidor de roteamento.
- Confirmou-se que os participantes exportam suas redes e recebem as redes dos outros AS.
- O AS do servidor de roteamento é transparente aos participantes conectados diretamente ou não.
- Dispõe de filtros para evitar que um participante não conectado diretamente receba (ou não) as rotas.
- Permite aplicar políticas de seguranças de bloqueio de rotas e limite de anúncios.

5.2 Migração Gated para Zebra

A segunda fase do experimento começou com o estudo da configuração do Gated e adaptação para o Zebra. Posteriormente, foi testada a configuração do Zebra em ambiente de produção, por meio da simulação de dois participantes.

Concluída a simulação, o servidor de roteamento Zebra foi preparado para a mudança, e o servidor de roteamento Gated foi desconectado e substituído pelo servidor de roteamento Zebra.

Após a mudança, as sessões BGP reinicializaram-se e não foi necessário alterar quaisquer configurações dos participantes.

Estudo do Gated no Provedor

O Gated no provedor tem uma configuração simples. Ele aceita somente as redes originadas dos participantes e, posteriormente, divulga para todos de maneira transparente. A maior dificuldade é a inclusão de novos participantes e políticas de roteamento. Isto ocorre porque toda a configuração é feita por meio de uma linguagem própria, sendo necessária a compilação do arquivo a cada alteração, diferentemente do Zebra, que tem uma console muito parecido com os roteadores Cisco.

O uso do Gated dificulta a alteração das políticas de roteamento e segurança que devem ser feitas periodicamente.

Nos experimentos executados, foi testado o funcionamento do Zebra como servidor de roteamento; no entanto, foi necessário estudar o ambiente de produção do Gated para planejar a migração.

Primeiramente, foi analisada a topologia do PTT existente no provedor.

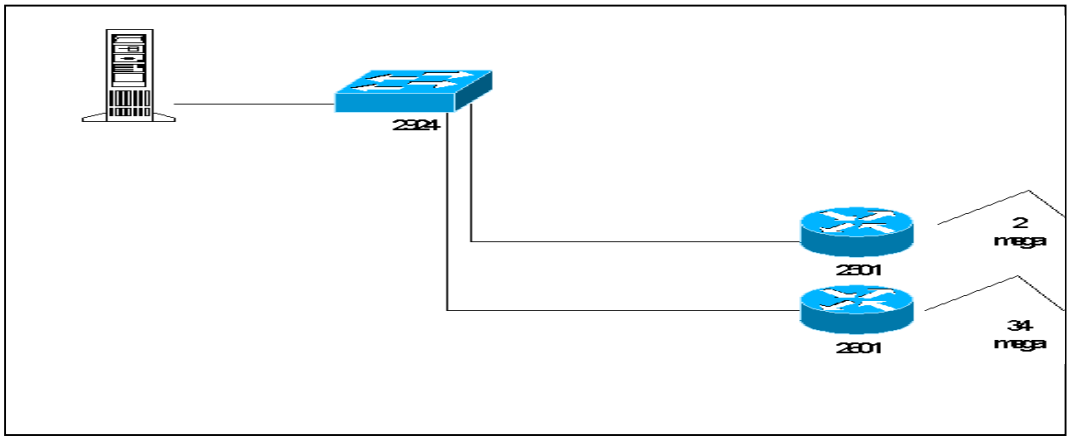


FIGURA 17 - Topologia do PTT em produção

Na topologia do PTT todos os participantes foram conectados diretamente no *switch,* juntamente com o servidor de roteamento Gated. Não serão citados os nomes dos participantes; no entanto, pode-se ver abaixo a quantidade de participantes e sua respectiva conexão física.

Participantes do PTT

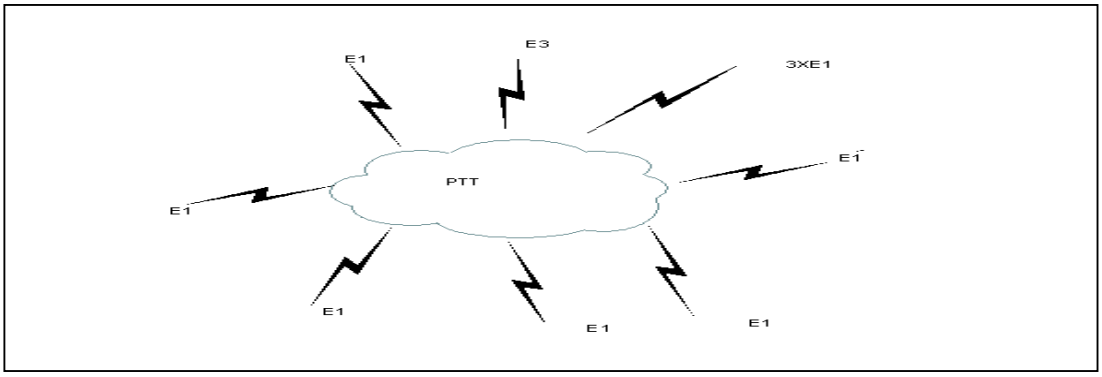


FIGURA 18- Participantes do PTT

O PTT tem 8 participantes, 6 deles usam um *link* E1 (2 Mbps), um usa 3 E1 totalizando 6 Mbps, e o maior usa E3 (34 Mbps).

Preparação do servidor Zebra para a mudança

Antes de iniciar a configuração do Zebra, foi necessário entender a configuração do Gated. A configuração do Gated pode ser encontrada no arquivo **gated.conf** .

TABELA 15 – Configuração do Gated

Configuração Original Gated	**Explicação dos principais comandos para ativação de um participante**

traceoptions nostamp normal route general state parse adv;
as 65500;
routerid 200.215.186.2;
bgp on {
traceoptions packets open update keepalive;
preference 50;
group type external peeras 16397 transparent {
peer 200.215.186.4 ;
};
group type external peeras 13878 transparent {
peer 200.215.186.7 ; #
};
group type external peeras 14026 transparent {
peer 200.215.186.3
};
group type external peeras 18747 transparent {
peer 200.215.186.5 ;
};
group type external peeras 14346 transparent {
peer 200.215.186.6 ;
};
group type external peeras 13591
	Definir AS.
	Definir endereço do servidor de roteamento.
	Ativar o BGP.
	
	Configuração do AS do participante.
	Definir o participante como transparente.
	
	Associar o endereço IP e o AS do vizinho.

transparent {
peer 200.215.186.9
};
group type external peeras 13874
transparent {
peer 200.215.186.12 ;
};
group type external peeras 14571
transparent {
peer 200.215.186.11 ;
};
group type external peeras 15180
transparent {
peer 200.215.186.10 ;
};
group type external peeras 5772
transparent {
peer 200.215.186.14 ;
};
group type external peeras 19182
transparent {
peer 200.215.186.13 ;
};
group type external peeras 16735
transparent {
peer 200.215.186.15 ;
};
 	
};	

view {
peer 200.215.186.4;
peer 200.215.186.3;
peer 200.215.186.5;
peer 200.215.186.6;
peer 200.215.186.7;
peer 200.215.186.11;
peer 200.215.186.9;
peer 200.215.186.12;
peer 200.215.186.10;
peer 200.215.186.14;
peer 200.215.186.13;
peer 200.215.186.15;
import proto bgp aspath <16397> origin any {
all; };
import proto bgp aspath <13878> origin any {
	Associar os endereços Ip(s) dos vizinhos.
	
	Criar filtro importando todas as redes com origem ao AS 16397.

all; };
import proto bgp aspath <14571>
origin any {
all; };
import proto bgp aspath <14346>
origin any {
all; };
import proto bgp aspath <14026>
origin any {
all; };
import proto bgp aspath <18747>
origin any {
all; };
import proto bgp aspath <13591>
origin any {
all; };
import proto bgp aspath <13874>
origin any {
all; };
import proto bgp aspath <15180>
origin any {
all; };
import proto bgp aspath <5772>
origin any {
all; };
import proto bgp aspath <19182>
origin any {
all; };
import proto bgp aspath <16735>
origin any {
all; };
 	
# import proto bgp aspath <13878 	
15180> origin any {
# all; }; 	
};
;	

Obs.:

A configuração tem participantes que não estavam ativos; contudo, no processo de migração foi usada a configuração original.

Configuração adaptada para o Zebra

Por meio do estudo dos comandos do Zebra e Gated realizou-se a adaptação da configuração existente no Gated para o Zebra.

TABELA 16 – Configuração do Zebra

Configuração adaptada para o Zebra	**Explicação dos principais comandos para ativação de um participante.**
Current configuration: ! **hostname Nap** **password teste** **enable password teste123** **log file bgpd.log** log stdout ! bgp multiple-instance ! **router bgp 65500** **bgp router-id 200.215.186.2** neighbor 200.215.186.3 remote-as 14026 neighbor 200.215.186.3 filter-list provedor1 in neighbor 200.215.186.3 attribute-unchanged as-path next-hop neighbor 200.215.186.4 remote-as 16397	Definir hostname como Nap. Definir senha. Definir senha de enable (mais recurso). Enviar eventos para o arquivo bgpd.log Definir processo BGP e o AS. Definir endereço do servidor de roteamento. Definir endereço IP do vizinho e seu AS. Associar o respectivo filtro na entrada. Definir vizinho como transparente.

neighbor 200.215.186.4 filter-list provedor2 in neighbor 200.215.186.4 attribute-unchanged as-path next-hop neighbor 200.215.186.5 remote-as 18747 neighbor 200.215.186.5 filter-list provedor3 in neighbor 200.215.186.5 attribute-unchanged as-path next-hop neighbor 200.215.186.6 remote-as 14346 neighbor 200.215.186.6 filter-list provedor4 in neighbor 200.215.186.6 attribute-unchanged as-path next-hop neighbor 200.215.186.7 remote-as 13878 neighbor 200.215.186.7 filter-list provedor5 in neighbor 200.215.186.7 attribute-unchanged as-path next-hop neighbor 200.215.186.9 remote-as 13591 neighbor 200.215.186.9 filter-list provedor6 in neighbor 200.215.186.9 attribute-unchanged as-path next-hop neighbor 200.215.186.10 remote-as 15180 neighbor 200.215.186.10 filter-list provedor7 in neighbor 200.215.186.10 attribute-unchanged as-path next-hop neighbor 200.215.186.11 remote-as 14571 neighbor 200.215.186.11 filter-list provedor8 in	

neighbor 200.215.186.11 attribute-unchanged as-path next-hop **ip as-path access-list provedor4 permit ^14346$** ip as-path access-list provedor2 permit ^16397$ ip as-path access-list provedor7 permit ^15180$ ip as-path access-list provedor5 permit ^13878$ ip as-path access-list provedor3 permit ^18747$ ip as-path access-list provedor8 permit ^14571$ ip as-path access-list provedor6 permit ^13591$ ip as-path access-list provedor1 permit ^14026$! line vty end	Criar filtro, permitindo tudo originado do AS 14346.

Configuração do servidor de roteamento Zebra para migração

Nesta etapa, o Zebra foi configurado da mesma forma que no item anterior (configuração para migração).

Antes de fazer a migração, foram executados alguns comandos de análise no Zebra, para verificar se estavam corretos. Seguem os comandos e a análise:

Sh ip bgp summary

Neste exemplo foram conferidos os IP(s) AS(s):

```
bgpd# sh ip bgp summary
BGP router identifier 200.215.186.2, local AS number 65500
0 BGP AS-PATH entries
0 BGP community entries

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
200.215.186.3   4 14026      0       0       0    0    0 00:00:01 Active
200.215.186.4   4 16397      0       0       0    0    0 00:00:02 Active
200.215.186.5   4 18747      0       0       0    0    0 00:00:04 Active
200.215.186.6   4 14346      0       0       0    0    0 00:00:01 Active
200.215.186.7   4 13878      0       0       0    0    0 00:00:02 Active
200.215.186.9   4 13591      0       0       0    0    0 00:00:03 Active
200.215.186.10  4 15180      0       0       0    0    0 00:00:06 Active
200.215.186.11  4 14571      0       0       0    0    0 00:00:06 Active
200.215.186.13  4 19182      0       0       0    0    0 00:00:03 Active
200.215.186.14  4  5772      0       0       0    0    0 00:00:06 Active
200.215.186.15  4 16735      0       0       0    0    0 00:00:04 Active
```

Obs.: Percebe-se que as seções BGP não estão estabelecidas.

Teste do servidor de roteamento Zebra com dois participantes

Para completar o processo de migração, estudou-se a configuração de cada participante. Foi realizado um novo experimento com dois participantes, no qual a configuração dos roteadores foi replicada, mantendo-se os mesmos endereços IP(s), AS(s) e filtros. Este ambiente de teste foi isolado do ambiente de produção e sem conexão com a Internet, para evitar problemas e não afetar o funcionamento do PTT em produção.

Após a configuração, foram confirmados, com sucesso, os mesmos resultados do experimento anterior.

```
Nap# sh ip bgp summary
BGP router identifier 200.215.186.2, local AS number 65500
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
200.215.186.3   4 14026      28      28        0    0    0 00:24:08        4
200.215.186.4   4 16397      66      70        0    0    0 01:04:29        5
200.215.186.5   4 18747       0       0        0    0    0 00:00:08 Active
200.215.186.6   4 14346       0       0        0    0    0 00:00:05 Active
200.215.186.7   4 13878       0       0        0    0    0 00:00:06 Active
200.215.186.9   4 13591       0       0        0    0    0 00:00:07 Active
200.215.186.10  4 15180       0       0        0    0    0 00:00:10 Active
200.215.186.11  4 14571       0       0        0    0    0 00:00:10 Active
200.215.186.13  4 19182       0       0        0    0    0 00:00:07 Active
```

Pode-se observar que o servidor de roteamento recebe quatro rotas do 200.215.186.3 e cinco rotas do 200.215.186.4. Conforme os testes executados, o participante 200.215.186.3 recebeu cinco rotas e o participante 200.215.186.4 recebeu quatro rotas, ambos de maneira transparente. Com isto, prova-se o funcionamento do PTT no ambiente de produção.

Processo de migração

Na migração, o cabo do servidor Gated foi desconectado e, em seguida, conectado o servidor Zebra. O servidor Gated permaneceu durante um mês no local. Caso ocorresse algo que comprometesse o nível de serviço (Service Level Agreement - SLA) acordado com os clientes, o Gated retornaria à produção.

Análise pós-migração

Foi necessário confirmar as seções BGP de cada vizinho. Além disso, foi necessário analisar as rotas que eles receberam e enviaram. Com base nisso foram

usados os comandos de análise de roteamento para verificar o roteamento do PTT. A configuração do Zebra e os comandos de análise pós-migração podem ser vistas no APÊNDICE D.

Vantagens da migração do Gated para o Zebra

O Zebra é mais parecido com o Cisco (padrão de mercado), facilitando a operação e manutenção dos PTT(s).

Permitiu visualizar os vizinhos BGP de maneira mais clara, emulando um roteador.

Nesta versão, o Zebra não tem custo; entretanto, este fator para uma empresa não é tão relevante, pois o custo do Gated é relativamente baixo.

O Zebra, apesar de não ter um contrato de suporte, tem várias listas de discussão e informações facilmente encontradas na Internet.

A facilidade de alteração dos filtros permitiu um aumento significativo de tráfego no PTT.

A equipe de suporte que já dominava roteadores Cisco, pode aplicar todo o conhecimento acumulado no servidor de roteamento, suportando melhor o PTT.

Permitiu criar políticas de segurança, implementando filtros, bloqueios de rotas *default*, senhas de acesso e limite de recebimento de prefixos.

5.3 Estruturação das políticas de roteamento no PTT através do BGP

Nesta etapa, o objetivo foi explorar o BGP no Zebra a fim de otimizar o tráfego trocado, aproveitando o novo recurso de ajuste dos filtros por ele oferecido, aumentando o tráfego na estrutura do PTT.

Os clientes AS(s) dos participantes do PTT(s) não trocavam tráfego devido à dificuldade de ajustar os filtros no Gated. Com a migração para o Zebra foi possível implementar filtros para aceitar as redes dos clientes AS(S) .

Por exemplo, um provedor com AS 100 - cliente do provedor de AS 200 - não trocava as rotas com a estrutura do PTT. O filtro ^*200$* permitia trocar apenas as redes originadas do AS200, alterando esse filtro para ^*200*_. Após a alteração, conseguiu-se receber as redes do AS200, que não necessariamente eram originadas

pelo AS200. Além dessa alteração, foi necessário aplicar filtros nos participantes que têm limitação de *link* para não aceitar essas redes. Isso foi feito para que não ocorra congestionamento nos *links*. Esta estruturação dos filtros permitiu, também, a criação de acordos bilaterais ou multilaterais entre os participantes. No APÊNDICE C constam as configurações, análises e gráficos das alterações entre os dois participantes, possibilitando a visualização do aumento de tráfego trocado.

5.4 Diretrizes para construção de um PTT

Um PTT pode ser construído e administrado de maneiras diferentes. A revisão da literatura e os resultados dos experimentos proporcionaram a criação de diretrizes que estão sintetizadas na TABELA 17.

O uso do PTT na comutação de tráfego entre sistemas autônomos poderá ser otimizado quando for estruturado com base em um modelo de construção e funcionamento. As diretrizes propostas podem ajudar na criação deste modelo.

No item 1 da tabela pode-se verificar os dados encontrados no capítulo 2, abrangendo características no PTT para garantir uma melhoria na disponibilidade da estrutura, estendendo também para a capacidade, crescimento e tráfego.

No item 2, seguem as diretrizes para a estrutura do PTT, abrangendo os *switches*, servidores de roteamento, equipamentos dos participantes e endereçamento.

Nos itens 3 e 4, pode-se ver as características dos participantes e alguns tipos de acordos entre participantes.

Nos itens 5, 6 e 7 registraram-se características de roteamento, segurança e gerenciamento.

TABELA 17 - Diretrizes para construção do PTT

1- CARACTERIZAÇÃO DO USO	**DISPONIBILIDADE**	**HOSPEDAGEM** **REDUNDÂNCIA**	-Redundância de energia -Gerador -Sistemas ar condicionado -Racks fechados -Segurança -Suporte no local -2 Servidores de roteamento -2 *Switches* -2 *Firewalls* (se existir)
	CAPACIDADE	**DIMENSIONAMENTO**	-Link do participante -Roteador do participante -*Switch*
	ESCALABILIDADE	**DIMENSIONAMENTO**	-Inclusão de *switches* na estrutura. -*Upgrade* do roteador e link do participante -Escolha de uma classe de endereço IP adequada
	TRÁFEGO DO PTT	**AVALIAÇÃO**	-Escolha de participantes -*Links* -Dimensionamento
2-ESTRUTURA DO PTT	**SWITCH**	**ESCOLHA**	-Portas
	SERVIDOR DE ROTEAMENTO	**ESCOLHA**	-Gated -Zebra -Outros
	EQUIPAMENTOS PARTICIPANTES	**DIMENSIONAMENTO**	-Roteador
	ENDEREÇAMENTO IP	**DEFINIÇÃO**	-Privado, Publico -Classe
3-ESCOLHA DOS PARTICIPANTES	**TRÁFEGO**	**ESCOLHA**	-AS(s) próprios -Intenção de tráfego no PTT
4-DEFINIÇÃO TIPOS DE	**BILATERAL MULTILATERAL**	**DEFINIÇÃO**	-Responsável pelo PTT deve definir os

ACORDOS			tipos de acordos
5-POLÍTICAS DE ROTEAMENTO	**FILTROS NO PTT E NOS PARTICIPANTES**	**FILTRAR**	-Exportar rota *default* -Endereços privados -Redistribuição protocolos IGP -Redistribuir tabela completa
6-SEGURANÇA	**ACESSOS NO PTT E NOS PARTICIPANTES**	**IMPLEMENTAR**	-Listas de acesso no *switch* -Acesso SSH no servidor de rotea-mento -*Firewall* (opcional)
7-GERENCIA-MENTO	**GERENCIAMENTO DE FALHAS**	**GERENCIAR**	-Responsável pelo PTT gerenciar o *switch* e o servidor de roteamento -Participantes gerenciarem o seu roteador
	GERENCIAMENTO TRÁFEGO	**GERENCIAR**	-Responsável pelo PTT gerenciar o tráfego do switch -Participantes gerenciarem o tráfego no seu roteador.

A seguir, as diretrizes são detalhadas a partir do item 2.

Switches

No PTT, recomenda-se o uso de um *switch* com, no mínimo, 24 portas que suportem a velocidade 100 Mega Full duplex. A quantidade mínima de portas 24 refere-se ao crescimento da estrutura e à pequena diferença de custo aos *switches* com um número menor de portas.

Servidor de roteamento

O servidor de roteamento deve ter seu AS transparente nos anúncios das rotas. Sugere-se o uso de um servidor de roteamento com a configuração e comandos

semelhantes aos roteadores Cisco, que são padrões de mercado, facilitando a operação e as alterações necessárias.

Equipamentos dos participantes

Os participantes são responsáveis pela administração de seus equipamentos. O roteador deve ser escolhido de acordo com a intenção de tráfego de cada participante. O espaço para instalação do equipamento deve ser acordado com o administrador do PTT.

Endereçamento IP

Cada participante terá o seu Autonomous System e seu respectivo bloco de endereços; no entanto, o PTT precisa de um bloco de endereço, que pode ser dimensionado de acordo com a quantidade de participantes que o PTT terá. É importante escolher um bloco de endereço com uma quantidade suficiente para crescimento.

Outra questão importante é definir se o endereço IP será privado ou público. No atual modelo de PTT, recomenda-se o uso de endereço público pertencente ao provedor que está operando o PTT. A escolha do endereço público facilita o reconhecimento do endereço, a possibilidade de roteamento na Internet, e a resolução de nome pelo DNS, caso seja necessário.

Candidatos para participar do PTT

Os candidatos do PTT, como visto, devem ter AS(s) próprios, com blocos de endereço e conexão permanente com a Internet. O interesse de tráfego pelos participantes dependerá da caracterização do tráfego. Esta análise pode ser feita por meio de um software que coleta as informações e posteriormente as analisa, como por exemplo o Netflow, já mencionado.

Acordos estabelecidos

Nos modelos de PTT(s) existentes podem-se ver dois tipos de acordos:

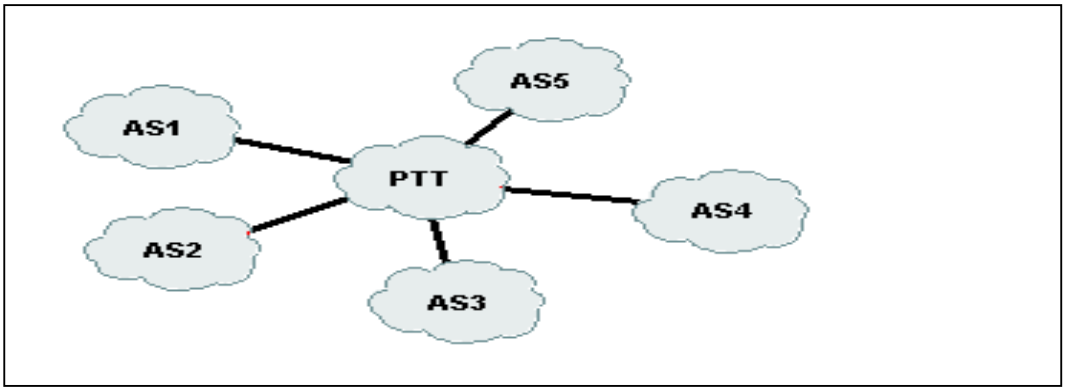


FIGURA 19 – Tipos de Acordos dos PTT(s)

Acordo Bilateral

É o acordo no qual dois participantes trocam tráfego, independentemente dos demais participantes do PTT. Na figura acima, um acordo bilateral, por exemplo, seria a troca de tráfego entre os AS2 e AS3 independentemente do tráfego trocado no PTT.

Acordo Multilateral

O acordo em que todos os participantes trocam com todos, porém cada participante tem o direito de filtrar algum anúncio que não queira receber ou enviar. Na FIGURA 19, o acordo multilateral seria, por exemplo, o envio do AS2 para o AS3, AS4, AS5 e AS1 e, conseqüentemente, o recebimento das redes desses AS.

Para iniciar o modelo do PTT, definem-se os tipos de acordos existentes no PTT. O PTT da FAPESP, por exemplo, exige que cada participante faça pelo menos dois acordos bilaterais ou um acordo de troca com todos os participantes. Já no modelo de PTT, estudado anteriormente, ocorre a troca com todos os participantes.

Políticas de anúncios de rotas

Não é permitido exportar rotas *default* e endereços privados. No entanto, é fundamental que cada participante filtre tanto as rotas *default* quanto os endereços privados.

Não é permitido redistribuir rotas IGP, como, por exemplo, OSPF e RIP dentro do BGP. Para evitar esta quantidade de rota na tabela de roteamento, é recomendado que se configure o limite de rotas recebidas nos participantes do PTT.

Segurança do PTT

Da mesma forma que ocorre no gerenciamento, a segurança do *switch* e do servidor de roteamento deve ser provida pela administração do PTT, enquanto que os participantes são responsáveis pelos seus roteadores

O primeiro passo para a segurança do PTT é incluir listas de acessos no *switch* e nos modos de acesso do Zebra, com o intuito de evitar o acesso *telnet* de outros lugares.

Lista de acesso

É necessário criar uma lista de acesso permitindo os IP(s) que farão *telnet* no *switch* e no Zebra. Na máquina do servidor de roteamento, aconselha-se disponibilizar somente o acesso SSH. Pode-se também colocar um *firewall* entre o servidor Zebra e o *switch,* liberando apenas a porta tcp 179 dos participantes para o Zebra. A porta TCP 179 é usada pelo BGP.

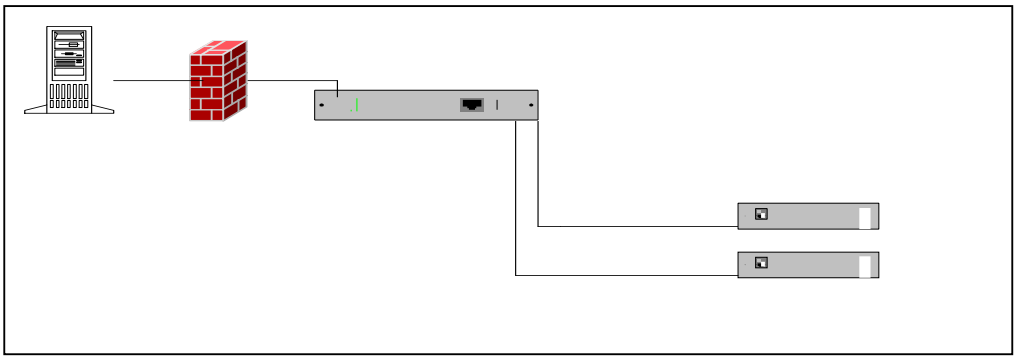


FIGURA 20 – Inclusão de Firewall para proteger o servidor de roteamento

É fundamental aplicar os filtros vistos anteriormente, não permitindo a entrada da rota *default* e endereços privados. Esses filtros podem ser aplicados no servidor de roteamento e nos roteadores dos participantes; além disso, aconselha-se limitar a quantidade de anúncios recebidos pelo servidor de roteamento, para evitar recebimento de rotas indevidas.

Gerenciamento

No gerenciamento existem dois pontos a serem considerados: o tráfego trocado e os equipamentos.

Gerenciamento de falhas

No *switch* do PTT, o servidor de roteamento e os roteadores dos participantes devem ser gerenciados. O gerenciamento do servidor de roteamento e do *switch* é responsabilidade da administração do PTT. No entanto, os participantes são responsáveis pelo gerenciamento de seus roteadores. O ideal é configurar para que os equipamentos enviem *traps* SNMP para alguma ferramenta de mercado que interprete e apresente gráficos para uma console na operação. O Netcool é um exemplo de ferramenta para gerenciar esses eventos SNMP.

Gerenciamento do tráfego

Recomenda-se que o administrador do PTT gerencie o tráfego no *switch* e que cada participante gerencie o tráfego no seu roteador. O gerenciamento pode ser realizado através de uma ferramenta de monitoração de tendências em séries temporais. As mais utilizadas nos provedores são o MRTG e o Cricket. O trabalho usa exemplos com base no Cricket. Este suporta SNMP, tendo sua aplicação baseada em WEB, que facilita a visualização. Monitora-se por longos períodos, chegando até um ano, compactando-se os dados armazenados.

Exemplo de coleta de dados:

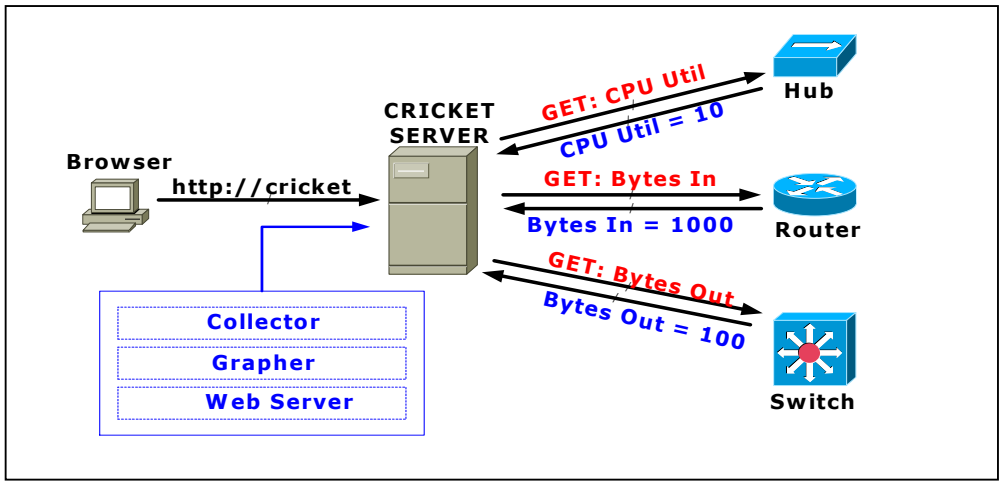


FIGURA 21 - Exemplo de gerenciamento de tráfego

Nesta figura, observa-se o acesso ao servidor do Cricket através de um browser. O cricket faz *pooling* nos equipamentos, solicitando as informações por meio do protocolo SNMP. Após a coleta, fornecem-se as informações na forma de gráficos. Pode-se gerenciar a entrada e a saída do tráfego, além da utilização da CPU, Memória e CPU. Quanto ao BGP, pode-se monitorar também as mensagens de entrada e de saída trocadas.

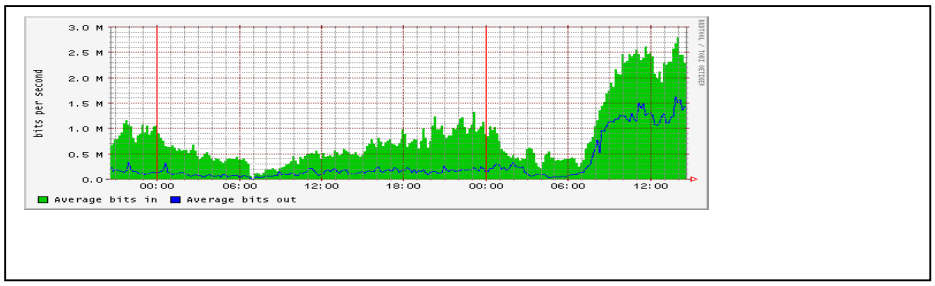


FIGURA 22 - Tráfego de entrada e saída de um participante

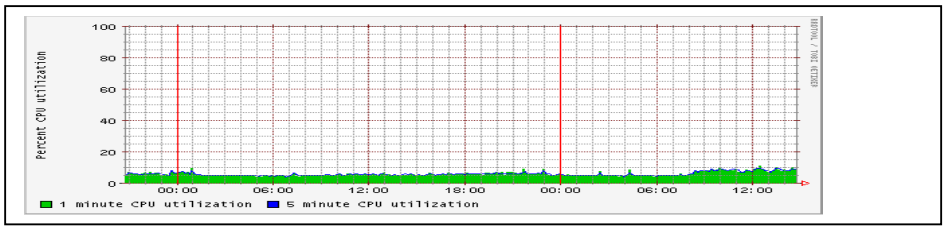


FIGURA 23 - CPU do roteador de um participante

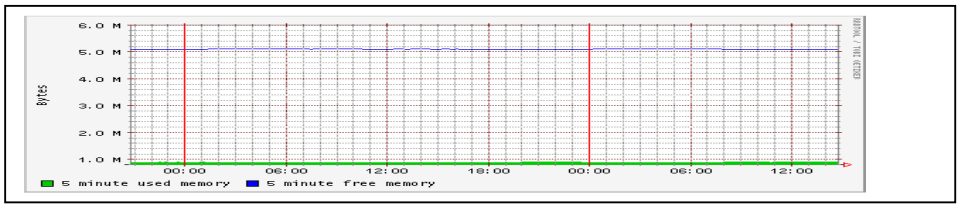


FIGURA 24 - Memória do roteador de um participante

Capítulo 6. CONSIDERAÇÕES FINAIS

A migração para o Zebra colaborou para a engenharia da empresa criar novas políticas de roteamento e filtros, permitiu a implementação de novos tipos de acordos de troca de trafego no PTT e facilitou a inclusão de novos participantes.

A exploração do protocolo BGP e o ajuste dos filtros proporcionaram a otimização do tráfego no PTT, alterando-se as políticas de roteamento de forma que fossem aceitas as redes dos clientes dos participantes. Esta alteração contribuiu para uma redução de custo, pois parte do tráfego para Internet deixou de ir pelo link pago, passando, então, para o PTT. Essa alteração trouxe também um ganho de velocidade no acesso para esses clientes.

Ao contrário do que acontecia com o Gated, devido à semelhança do Zebra com os equipamentos Cisco, após a migração a equipe de operação do provedor começou a suportar o PTT. Até então, referida equipe não tinha especialização suficiente para suportar o Gated. Os comandos de análise do BGP e as configurações parecidas com o ambiente de produção do *backbone* do provedor foram os fatores que colaboraram para o domínio da estrutura.. Como os equipamentos Cisco são padrão de mercado, provavelmente essa facilidade se estende para a maioria dos provedores.

A formulação das diretrizes permitiu oferecer novas soluções para a estrutura, como por exemplo a redundância da estrutura do PTT, formalização dos tipos de acordos com participantes, implementação de novas políticas de roteamento, questões de segurança e gerenciamento do PTT.

O experimento permitiu a documentação da construção e configuração do Zebra, caso seja necessário replicar ou refazer o servidor de roteamento dele. No caso do Gated, não existia documentação personalizada para refazer o servidor.

O Gated tinha um custo para a empresa, e suporte dado somente pelo fabricante estabelecido no exterior. O Zebra não tem custo, pois é um software livre, e embora não tenha suporte oficial, existem muitas informações e listas de discussões na Internet para suporte.

As informações contidas neste trabalho podem contribuir com o leitor na construção de um PTT, na modificação de um PTT existente ou, no mínimo, na seleção de um PTT para trocar tráfego.

6.1 Conclusão

O sucesso dos experimentos motivou a migração da plataforma do PTT, pois se percebeu a semelhança de configuração do Zebra com os equipamentos já em uso no provedor. Além disso, pôde-se replicar e validar toda a configuração pré existente no Gated, proporcionando uma migração suave, sem afetar o funcionamento do PTT.

A migração foi realizada com extremo sucesso, atendendo a todos os requisitos esperados e superando, inclusive, as expectativas do provedor

6.2 Recomendações para futuros trabalhos

6.2.1 Estudo e caracterização do tráfego do PTT e seus participantes.

O estudo do tráfego de um PTT e dos seus participantes pode ser realizado através de ferramentas e aplicações existentes, podendo se estender para escolhas de futuros candidatos. Propõe-se o desenvolvimento de metodologias e a escolha de ferramentas adequadas para o estudo e caracterização deste tráfego.

6.2.2 Análise financeira e tendência nacional e internacional do(s) PTT(s).

Realizar um estudo para dimensionar o custo e propor estratégias de implantação de PTT(s), observando, principalmente, os benefícios em substituir os links das operadoras estudando a evolução e tendências do(s) PTT(s) nacional(is) e internacional(is).

REFERÊNCIAS BIBLIOGRÁFICAS

Artigos de publicação periódicas

ABRANET cria novo ponto de tráfego. ITWEB. São Paulo, 7 de jun 2001. Disponível em < http://www.itweb.com.br >. Acesso em 18.jul.2003.

FAPESP transfere operação de ponto de troca de tráfego. ITWEB**.** São Paulo, 4 de abril 2002.Disponível em <http://www.itweb.com.br >. Acesso em 18.jul.2003.

FILHO, R. **Operação e Administração de PTTs no Brasil.** São Paulo: Comitê Gestor da Internet no Brasil, 2000.

PRADO, C. A. **Internet: o desafio em manter sua disponibilidade. ITWEB.** São Paulo, 31 de out 2002.Disponível em <http://www.itweb.com.br >. Acesso em 18.jul.2003.

Entidade coletiva

CISCO DO BRASIL.**BSCN-Building Scalable Cisco Networks**. São Paulo, 2000.

JUNIPER, C. K. **BGP v4 Tutorial**. São Paulo, abril 2003.

MULTIREDE INFORMÁTICA LTDA. **BGP Configuração e Depuração**. São Paulo, 2000.

Livros

HALABI, S.; MC PHERSON, D. **Internet Routing Architectures.** 2ª ed.: Indianapolis – USA: Cisco Press, 2000.

MARTINS, A.G. **Manual para elaboração de monografias e dissertações.** 3ª ed.: São Paulo-SP: Ed Atlas, 2002.

MATTAR, F.G. **Pesquisa de marketing**. Ed Compacta. São Paulo: Atlas, 1996.

NEMETH, E.; SNYDER, G.; SEEBASS, S; HEIN, T.R. **Unix System Administration Handbook**. Upper Saddle River, NJ: Prentice-Hall, 1995.

PARKHURST, W. Cisco BGP-4 **Command and Configuration Handbook.**

Indianapolis - USA: Cisco Press, 2001.

STALLINGS, W. Local & Metropolitan Area Network. 1ª ed.: Upper Saddle River, New Jersey; Prentice Hall, Inc, 1997.

RFC

REKHTER,Y. **RFC 1771: A Border Gateway Protocol BGP-4,T.J**. Watson Research Center, IBM Corp,T.LI , Cisco System, 1995.

Sites

GNU **Zebra.** Disponível em: < http://www.zebra.org >. Acesso em 18.jul.2003.

NEXTHOP **Suite of Routing Protocols.** Disponível em:< http://www.nexthop.com >. Acesso em 18.jul.2003.

Bibliografia Complementar

BEIJNUM, I.V. Bgp - **Building reliable networks with the border gateway protoco**l. 1ª ed.: Sebastopol, CA: OREILLY & ASSOC., 2002.

BLACK, U. **IP routing : RIP, OSPF, BGP, PNI and routing protocols**.1ª ed.: Upper Saddle River, New Jersey: Prentice Hall, 2000.

CHAPPELL, L. **Cisco Internetwork Troubleshooting**: 1ª ed.: Indianapolis - USA: Cisco Press, 1999.

CHAPPELL, L. **Introduction to Cisco Router Configuration:** 1ª ed.: Indianapolis - USA: Cisco Press, 1998.

COMER ,D. E. **Redes de Computadores e Internet**: 2ª ed.: Porto Alegre, Bookman, 2001.

STEWART III, J. W. **BGP4 Inter-Domain Routing in the Internet:**1ª ed.: Upper Saddle River, New Jersey: Addison-Wesley Networking Basics Series, 1999.

GLOSSÁRIO

Backbone	Os backbones são redes consideradas as espinhas dorsais da Internet. Garantem o fluxo da informação entre os provedores e ligam os países.
Buraco Negro	Problema de roteamento na Internet, quando ocorre a perda total de pacotes e estes não conseguem alcançar o destino.
Daemon	Um programa geralmente associado ao sistema Unix, que executa funções utilitárias sem ser requisitado, e até mesmo sem que o usuário perceba. Os daemons ficam em background e são ativados apenas quando necessário.
Enable	Modo de acesso com maior privilégio, permitindo executar mais comandos.
Firewall	Software para bloqueio de tráfego de entrada ou saída.
Host	Máquina com endereço, conectada a uma rede.
ISP	Empresa que presta serviços de acesso à Internet.
Link	Circuito de comunicação entre dois pontos.
Loop	Quando o roteamento fica variando entre dois pontos, não conseguindo alcançar o destino.
Password	Palavra-chave usada para identificação do usuário em conjunto com o login (não sendo este secreto).
Patches	Atualizações, correções.
RFC	Documentos que definem normas e protocolos para a Internet e pelos quais são feitas as discussões de nível técnico para a definição de novos protocolos.
Roteador	Os roteadores decidem o caminho que o tráfego de informações (controle e dados) deve seguir, e fazem o roteamento de pacotes entre redes locais (LAN) e de longa distância (WAN).
Software Livre	Software com o código aberto para alterações.
Software Modular	Software com módulos, que pode ser executado independentemente.
Switch	Equipamento para comutar pacotes com alta velocidade.

APÊNDICES

APÊNDICE A- Configuração dos equipamentos no primeiro experimento

TABELA 18 - Configuração do roteador A

Configuração do roteador A	**Explicação dos principais comandos**
hostname routerA	Definindo o *hostname* do roteador A.
enable secret cisco	Definir senha enable (mais recurso).
interface Ethernet0 ip address 10.10.10.3 255.255.255.0	Configurar interface que vai ser conectada no *switch.*
router bgp 7677	Definir AS e o processo BGP.
network 120.0.0.0 network 121.0.0.0 network 122.0.0.0 network 123.0.0.0 network 124.0.0.0 network 125.0.0.0	Divulgar redes.
neighbor 10.10.10.2 remote-as 7675	Definir como vizinho o servidor de roteamento.
ip route 120.0.0.0 255.0.0.0 Null0 ip route 121.0.0.0 255.0.0.0 Null0 ip route 122.0.0.0 255.0.0.0 Null0 ip route 123.0.0.0 255.0.0.0 Null0 ip route 124.0.0.0 255.0.0.0 Null0 ip route 125.0.0.0 255.0.0.0 Null0	Conhecer internamente as rotas a serem divulgadas (somente para o experimento).
line vty 0 4 password cisco login	Definir senha de *telnet.*

Obs.: Foram colocadas rotas para null 0 com o intuito de garantir o anúncio das rotas mesmo que a sincronização do BGP esteja habilitada.

TABELA 19 - Configuração do roteador B

Configuração do roteador B	**Explicação dos principais comandos**
hostname routerB	Definir o hostname.
enable secret cisco	Definir senha de *enable*.
interface Ethernet0 ip address 10.10.10.4 255.255.255.0	Configurar a interface a ser conectada no *switch.*
router bgp 7676	Definir AS e o processo BGP.
network 130.0.0.0 mask 255.0.0.0 network 131.0.0.0 mask 255.0.0.0 network 132.0.0.0 mask 255.0.0.0 network 133.0.0.0 mask 255.0.0.0 network 134.0.0.0 mask 255.0.0.0 network 135.0.0.0 mask 255.0.0.0 network 136.0.0.0 mask 255.0.0.0 network 137.0.0.0 mask 255.0.0.0	Anunciar as redes.

network 138.0.0.0 mask 255.0.0.0 network 139.0.0.0 mask 255.0.0.0 network 140.0.0.0 mask 255.0.0.0 neighbor 10.10.10.2 remote-as 7675 ip route 130.0.0.0 255.0.0.0 Null0 ip route 131.0.0.0 255.0.0.0 Null0 ip route 132.0.0.0 255.0.0.0 Null0 ip route 133.0.0.0 255.0.0.0 Null0 ip route 134.0.0.0 255.0.0.0 Null0 ip route 135.0.0.0 255.0.0.0 Null0 ip route 136.0.0.0 255.0.0.0 Null0 ip route 137.0.0.0 255.0.0.0 Null0 ip route 138.0.0.0 255.0.0.0 Null0 ip route 139.0.0.0 255.0.0.0 Null0 ip route 140.0.0.0 255.0.0.0 Null0 ip route 192.168.10.0 255.255.255.0 Ethernet0 line vty 0 4 password teste login	Conhecer internamente as redes. Definir senha de *telnet*.

TABELA 20 - Configuração do roteador C

Configuração do roteador C	**Explicação dos principais comandos**
hostname routerc enable password cisco interface Ethernet0 ip address 10.10.10.5 255.255.255.0 router bgp 6000 network 150.0.0.0 mask 255.0.0.0 network 151.0.0.0 mask 255.0.0.0 network 152.0.0.0 mask 255.0.0.0 network 153.0.0.0 mask 255.0.0.0 network 154.0.0.0 mask 255.0.0.0 network 155.0.0.0 mask 255.0.0.0 network 156.0.0.0 mask 255.0.0.0 neighbor 10.10.10.2 remote-as 7675 ip route 150.0.0.0 255.0.0.0 Null0 ip route 151.0.0.0 255.0.0.0 Null0	Definir hostname. Definir senha de *enable*. Configurar a interface que vai ser conectada com o *switch.* Definir AS e o processo BGP. Anunciar as redes. Definir o servidor de roteamento como vizinho.

ip route 152.0.0.0 255.0.0.0 Null0 ip route 153.0.0.0 255.0.0.0 Null0 ip route 154.0.0.0 255.0.0.0 Null0 ip route 155.0.0.0 255.0.0.0 Null0 ip route 156.0.0.0 255.0.0.0 Null0 ip route 157.0.0.0 255.0.0.0 Null0 ip route 158.0.0.0 255.0.0.0 Null0 ip route 159.0.0.0 255.0.0.0 Null0	Conhecer internamente as redes divulgadas.
line vty 0 4 password cisco login	Definir a senha de *telnet*.

TABELA 21 -Configuração do servidor de roteamento

Configuração do servidor de roteamento	**Explicação dos principais comandos**
hostname bgpd	Definir o hostname.
password zebra	Definir a senha.
enable password cisco	Definir a senha de *enable*.
log file bgpd.log	Criar um log para os eventos.
bgp multiple-instance router bgp 7675	Definir AS e o processo BGP.
bgp router-id 10.10.10.2	Associar o IP do servidor de roteamento.
network 1.0.0.0/8 network 2.0.0.0/8 network 3.0.0.0/8 network 4.0.0.0/8 network 5.0.0.0/8 network 6.0.0.0/8 network 7.0.0.0/8 network 8.0.0.0/8 network 9.0.0.0/8 network 10.10.10.0/24 network 19.0.0.0/8 network 29.0.0.0/8 network 39.0.0.0/8 network 49.0.0.0/8 network 59.0.0.0/8 network 69.0.0.0/8 network 79.0.0.0/8 network 89.0.0.0/8	Anunciar as redes.
neighbor 10.10.10.3 remote-as 7677	Definir o roteador A como vizinho.
neighbor 10.10.10.3 filter-list routera in	Associar o filtro routera na entrada.

neighbor 10.10.10.3 attribute-unchanged as-path next-hop	Definir o AS e *nexthop* como transparente.
neighbor 10.10.10.4 remote-as 7676 neighbor 10.10.10.4 filter-list routerb in neighbor 10.10.10.4 attribute-unchanged as-path next-hop	Definir o roteador B como vizinho. Associar o filtro routerb na entrada Definir o AS e *nexthop* como transparente.
neighbor 10.10.10.5 remote-as 6000 neighbor 10.10.10.5 attribute-unchanged as-path next-hop	Definir o roteador C como vizinho. Definir o AS e *nexthop* como transparente.
access-list all permit any ! ip as-path access-list routera permit ^7677$	Criar filtro routera, permitindo somente o que for originado do AS7677.
ip as-path access-list routerb permit ^7676$	Criar filtro routerb, permitindo somente o que for originado do AS7676.

APÊNDICE B –Configuração e análise da máquina de estado do BGP

Mudanças de configurações efetuadas:

No roteador A foi conectado a interface serial com o roteador C, configurando o endereço IP e por fim acrescentado o vizinho C através dos comandos:

interface Serial0
ip address 192.168.10.2 255.255.255.0
router bgp 7677
neighbor 192.168.10.1 remote-as 6000

No roteador C, também configurou-se o endereço e foi removido o servidor de roteamento como vizinho BGP:

interface Serial0
ip address 192.168.10.1 255.255.255.0
clockrate 7200
router bgp 6000
neighbor 192.168.10.2 remote-as 7677
no neighbor 10.10.10.2 remote-as 7675

Estado Active – Tentativa de conexão BGP, caso sucesso, passa para o estado Open Sent

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.10.10.2	4	7675	1280	1279	381	0	0	04:25:05	29
192.168.10.1	4	6000	17	19	0	0	0	00:00:26	**Active**

Estado Open Sent- Aguarda a mensagem Open do vizinho

routerA#sh ip bgp summary
BGP table version is 381, main routing table version 381
35 network entries (35/105 paths) using 7280 bytes of memory
3 BGP path attribute entries using 284 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.10.10.2	4	7675	1280	1279	381	0	0	04:25:05	29
192.168.10.1	4	6000	17	20	0	0	0	00:00:26	**OpenSent**

```
routerA#sh ip bgp summary
BGP table version is 388, main routing table version 388
42 network entries (42/126 paths) using 8788 bytes of memory
4 BGP path attribute entries using 420 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

Recebimento das rotas

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.2      4  7675    1280    1279      381    0    0 04:25:06       29
192.168.10.1    4  6000      21      25      381    0    0 00:00:00       7
```

Foi verificado no servidor de roteamento que ele não sai do estado de Active com o vizinho do roteador C, ou seja, não restabelecerá a conexão, pois foi removida a configuração do vizinho BGP do roteador C.

Acompanhamento da máquina de estado vista anteriormente no servidor de roteamento:

Idle – Primeiro estado da conexão

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677     281     278        0    0    0 04:31:07        6
10.10.10.4      4  7676     274     278        0    0    0 04:31:08       11
10.10.10.5      4  6000     248     251        0    0    0 00:00:07 Idle

Total number of neighbors 3
```

```
bgpd# sh ip bgp summary
BGP router identifier 10.10.10.2, local AS number 7675
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.10.3      4  7677     281     278        0    0    0 04:31:08        6
10.10.10.4      4  7676     274     278        0    0    0 04:31:09       11
10.10.10.5      4  6000     248     251        0    0    0 00:00:01 Active
```

APÊNDICE C – Configurações e análise dos resultados e gráficos das alterações das políticas de roteamento.

Na configuração do Zebra foi feito um filtro geral permitindo as redes de todos os AS(s).

ip as-path access-list global permit ^14346$
ip as-path access-list global permit ^19182$
ip as-path access-list global permit ^16397$
ip as-path access-list global permit ^15180$
ip as-path access-list global permit ^16735$
ip as-path access-list global permit ^13878$
ip as-path access-list global permit ^18747$
ip as-path access-list global permit ^14571$
ip as-path access-list global permit ^13591$
ip as-path access-list global permit ^5772$
ip as-path access-list global permit ^14026$

Esse filtro foi aplicado em todos os participantes com exceção dos participantes que trocarão tráfegos de seus clientes AS(s).

Ex:

router bgp 65500
neighbor 200.215.186.7 filter-list global out
neighbor 200.215.186.3 filter-list global out
neighbor 200.215.186.4 filter-list global out
neighbor 200.215.186.5 filter-list global out
neighbor 200.215.186.6 filter-list global out
neighbor 200.215.186.11 filter-list global out
neighbor 200.215.186.13 filter-list global out
neighbor 200.215.186.14 filter-list global out

Após isso, foi alterado o filtro de entrada desses participantes para receber todas as redes enviadas pelos AS sem necessariamente terem sido originadas pelo mesmo.

no ip as-path access-list filtro1
ip as-path access-list filtro1 permit ^13591_

no ip as-path access-list filtro2 permit ^15180$
ip as-path access-list filtro2 permit ^15180_

router bgp 65500
neighbor 200.215.186.9 filter-list filtro1 out
neighbor 200.215.186.10 filter-list filtro2 out

Análise das rotas através dos comandos.

Rotas recebidas (200.215.186.9) antes da mudança

Nap# sh ip bgp neighbors 200.215.186.9 routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - inte
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 200.49.77.0	200.215.186.9			0	13591 i
*> 200.142.64.0/19	200.215.186.9			0	13591 i
*> 200.142.95.0	200.215.186.9			0	13591 i
*> 200.152.192.0/19	200.215.186.9			0	13591 i
*> 200.160.224.0/19	200.215.186.9			0	13591 i
*> 200.225.64.0/20	200.215.186.9			0	13591 i

Rotas recebidas (200.215.186.9) depois da mudança

Nap# sh ip bgp neighbors 200.215.186.9 routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 63.250.176.0/23	200.215.186.9			0	13591 3300 i
*> 63.250.180.0/23	200.215.186.9			0	13591 3300 i
*> 129.222.32.0/19	200.215.186.9			0	13591 5772 i
*> 129.222.64.0/19	200.215.186.9			0	13591 5772 i
*> 148.188.174.0/24	200.215.186.9			0	13591 3300 i
*> 192.5.5.0	200.215.186.9			0	13591 22548 30122 557 i
*> 192.175.48.0	200.215.186.9			0	13591 22548 112 i
*> 192.228.80.0	200.215.186.9			0	13591 22548 30122
*> 200.49.77.0	200.215.186.9			0	13591 i
*> 200.142.64.0/19	200.215.186.9			0	13591 i
*> 200.142.95.0	200.215.186.9			0	13591 i
* 200.142.208.0/20	200.215.186.9			0	13591 16397 26602
*> 200.150.192.0/20	200.215.186.9			0	13591 26107 i
*> 200.152.192.0/19	200.215.186.9			0	13591 i
*> 200.155.15.0	200.215.186.9			0	13591 16397 i

*> 200.155.16.0/20 200.215.186.9 0 13591 16397 i
*> 200.155.96.0/20 200.215.186.9 0 13591 23002 i
*> 200.155.98.0 200.215.186.9 0 13591 23002 ?
*> 200.155.107.0 200.215.186.9 0 13591 23002 i
*> 200.155.108.0 200.215.186.9 0 13591 23002 i
*> 200.160.0.0/20 200.215.186.9 0 13591 22548 i
*> 200.160.174.0 200.215.186.9 0 13591 22341 i
*> 200.160.224.0/19 200.215.186.9 0 13591 i
*> 200.162.128.0/20 200.215.186.9 0 13591 22177 i
*> 200.169.128.0/17 200.215.186.9 0 13591 14650 i
*> 200.189.96.0/22 200.215.186.9 0 13591 18739 i
*> 200.189.100.0/22 200.215.186.9 0 13591 18739 i
*> 200.189.104.0/22 200.215.186.9 0 13591 18739 i
*> 200.189.108.0/22 200.215.186.9 0 13591 18739 i
*> 200.192.160.0/20 200.215.186.9 0 13591 19089 13935
*> 200.192.216.0/21 200.215.186.9 0 13591 14723 i
*> 200.198.184.0/23 200.215.186.9 0 13591 16397 i
*> 200.215.128.0/19 200.215.186.9 0 13591 10688 i
* 200.219.0.0/18 200.215.186.9 0 13591 16397 6543 i
*> 200.219.64.0/18 200.215.186.9 0 13591 14650 i
*> 200.219.128.0 200.215.186.9 0 13591 7313 7313 73
3 7313 7313 7313 7313 7313 7313 7313 7313 i
* 200.220.0.0/18 200.215.186.9 0 13591 5772 i
* 200.220.64.0/18 200.215.186.9 0 13591 5772 i
*> 200.225.64.0/20 200.215.186.9 0 13591 i
*> 200.225.80.0/20 200.215.186.9 0 13591 19089 i
*> 200.225.80.0/22 200.215.186.9 0 13591 19089 i
*> 200.225.84.0/22 200.215.186.9 0 13591 19089 i
*> 200.225.88.0/22 200.215.186.9 0 13591 19089 i
*> 200.225.92.0/22 200.215.186.9 0 13591 19089 i
*> 200.225.160.0/19 200.215.186.9 0 13591 14650 i
*> 200.229.16.0/20 200.215.186.9 0 13591 16736 i
*> 200.229.16.0/22 200.215.186.9 0 13591 16736 i
*> 200.229.20.0/22 200.215.186.9 0 13591 16736 i
*> 200.229.24.0/22 200.215.186.9 0 13591 16736 i
*> 207.83.96.0/20 200.215.186.9 0 13591 3300 i

Total number of prefixes 50

Rotas recebidas (200.215.186.10) antes da mudança

Nap# sh ip bgp neighbors 200.215.186.10 rou
Nap# sh ip bgp neighbors 200.215.186.10 routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - interna
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path

*> 200.99.0.0/17 200.215.186.10 0 15180 i
*> 200.99.0.0/18 200.215.186.10 0 15180 i
*> 200.99.64.0/18 200.215.186.10 0 15180 i
*> 200.162.0.0/17 200.215.186.10 0 15180 i
*> 200.162.0.0/18 200.215.186.10 0 15180 i
*> 200.162.64.0/18 200.215.186.10 0 15180 i
*> 200.198.64.0/18 200.215.186.10 0 15180 i
*> 200.198.64.0/19 200.215.186.10 0 15180 i
*> 200.198.96.0/19 200.215.186.10 0 15180 i
*> 200.202.112.0/20 200.215.186.10 0 15180 i
*> 200.202.112.0/21 200.215.186.10 0 15180 i
*> 200.202.120.0/21 200.215.186.10 0 15180 i

Total number of prefixes 12

Rotas recebidas (200.215.186.10) depois da mudança

Nap#
Nap# sh ip bgp neighbors 200.215.186.10 routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 200.99.0.0/17 200.215.186.10 0 15180 i
*> 200.99.0.0/18 200.215.186.10 0 15180 i
*> 200.99.64.0/18 200.215.186.10 0 15180 i
*> 200.142.160.0/20 200.215.186.10 0 15180 26104 i
*> 200.142.224.0/20 200.215.186.10 0 15180 26090 i
*> 200.150.0.0/21 200.215.186.10 0 15180 23106 i
*> 200.152.48.0/20 200.215.186.10 0 15180 26616 i
*> 200.152.48.0/22 200.215.186.10 0 15180 26616 i
*> 200.152.52.0/22 200.215.186.10 0 15180 26616 i
*> 200.162.0.0/17 200.215.186.10 0 15180 i
*> 200.162.0.0/18 200.215.186.10 0 15180 i
*> 200.162.64.0/18 200.215.186.10 0 15180 i
*> 200.162.176.0/20 200.215.186.10 0 15180 22129 i
*> 200.162.176.0 200.215.186.10 0 15180 22129 i
*> 200.162.177.0 200.215.186.10 0 15180 22129 i
*> 200.196.32.0/20 200.215.186.10 0 15180 11431 i
*> 200.196.32.0/22 200.215.186.10 0 15180 11431 i
*> 200.196.36.0/23 200.215.186.10 0 15180 11431 11431 1
1431 i

*> 200.196.38.0/23 200.215.186.10 0 15180 11431 i
*> 200.196.40.0/23 200.215.186.10 0 15180 11431 11431 1
1431 i
*> 200.196.42.0/23 200.215.186.10 0 15180 11431 i

*> 200.196.44.0/23 200.215.186.10 0 15180 11431 i
*> 200.196.46.0/23 200.215.186.10 0 15180 11431 11431 1
1431 i
*> 200.198.64.0/18 200.215.186.10 0 15180 i
*> 200.198.64.0/19 200.215.186.10 0 15180 i
*> 200.198.96.0/19 200.215.186.10 0 15180 i
*> 200.202.112.0/20 200.215.186.10 0 15180 i
*> 200.202.112.0/21 200.215.186.10 0 15180 i
*> 200.202.120.0/21 200.215.186.10 0 15180 i
*> 200.219.224.0/23 200.215.186.10 0 15180 14026 i
*> 200.220.141.0   200.215.186.10 0 15180 27693 i
*> 200.220.142.0   200.215.186.10 0 15180 27693 i
*> 200.229.0.0/20   200.215.186.10 0 15180 16712 16712 1
6712 i

Total number of prefixes 33

Rotas anunciadas (200.215.186.9) antes da mudança

Nap# sh ip bgp neighbors 200.215.186.9 adv
Nap# sh ip bgp neighbors 200.215.186.9 advertised-routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - in
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 63.215.188.0/22	200.215.186.7			0	13878 i
*> 148.243.64.0/21	200.215.186.7			0	13878 i
*> 157.253.0.0	200.215.186.7			0	13878 i
*> 172.16.32.0/20	200.215.186.7			0	13878 i
*> 172.16.48.0/20	200.215.186.7			0	13878 i
*> 172.16.64.0/20	200.215.186.7			0	13878 i
*> 200.3.244.0	200.215.186.7			0	13878 i
*> 200.3.245.0	200.215.186.7			0	13878 i
*> 200.3.246.0	200.215.186.7			0	13878 i
*> 200.3.247.0	200.215.186.7			0	13878 i
*> 200.23.192.0/22	200.215.186.7			0	13878 i
*> 200.23.196.0	200.215.186.7			0	13878 i
*> 200.23.197.0	200.215.186.7			0	13878 i
*> 200.31.64.0	200.215.186.7			0	13878 i
*> 200.31.65.0	200.215.186.7			0	13878 i
*> 200.31.66.0	200.215.186.7			0	13878 i
*> 200.31.67.0	200.215.186.7			0	13878 i
*> 200.31.68.0	200.215.186.7			0	13878 i
*> 200.31.69.0	200.215.186.7			0	13878 i
*> 200.31.70.0	200.215.186.7			0	13878 i

```
*> 200.31.71.0      200.215.186.7                0 13878 i
*> 200.31.72.0      200.215.186.7                0 13878 i
*> 200.31.73.0      200.215.186.7                0 13878 i
*> 200.31.74.0      200.215.186.7                0 13878 i
*> 200.31.76.0      200.215.186.7                0 13878 i
*> 200.31.77.0      200.215.186.7                0 13878 i
*> 200.31.78.0      200.215.186.7                0 13878 i
*> 200.31.79.0      200.215.186.7                0 13878 i
*> 200.31.80.0      200.215.186.7                0 13878 i
*> 200.31.81.0      200.215.186.7                0 13878 i
*> 200.31.83.0      200.215.186.7                0 13878 i
*> 200.31.84.0      200.215.186.7                0 13878 i
*> 200.31.85.0      200.215.186.7                0 13878 i
*> 200.31.86.0      200.215.186.7                0 13878 i
*> 200.57.32.0/20   200.215.186.7                 0 13878 i
*> 200.57.36.0/22   200.215.186.7                 0 13878 i
*> 200.99.0.0/17    200.215.186.10                0 15180 i
*> 200.99.0.0/18    200.215.186.10                0 15180 i
*> 200.99.64.0/18   200.215.186.10                0 15180 i
*> 200.142.208.0/20 200.215.186.4                 0 16397 i
*> 200.143.0.0/19   200.215.186.7                 0 13878 i
*> 200.143.0.0/22   200.215.186.7                 0 13878 i
*> 200.146.192.0/18 200.215.186.15                0 16735 i
*> 200.155.0.0/19   200.215.186.4                 0 16397 i
*> 200.155.128.0/18 200.215.186.5                 0 18747 i
*> 200.155.128.0/21 200.215.186.5                 0 18747 i
*> 200.155.136.0/22 200.215.186.5                 0 18747 i
*> 200.162.0.0/17   200.215.186.10                0 15180 i
*> 200.162.0.0/18   200.215.186.10                0 15180 i
*> 200.162.64.0/18  200.215.186.10                0 15180 i
*> 200.170.128.0/18 200.215.186.15                0 16735 i
*> 200.170.128.0/21 200.215.186.15                0 16735 i
*> 200.170.136.0/21 200.215.186.15                0 16735 i
*> 200.170.144.0/21 200.215.186.15                0 16735 i
*> 200.170.152.0/21 200.215.186.15                0 16735 i
*> 200.170.160.0/21 200.215.186.15                0 16735 i
*> 200.170.168.0/21 200.215.186.15                0 16735 i
*> 200.170.176.0/20 200.215.186.15                0 16735 i
*> 200.170.192.0/18 200.215.186.5                 0 18747 i
*> 200.170.224.0/20 200.215.186.5                 0 18747 i
*> 200.189.160.0/19 200.215.186.7                 0 13878 i
*> 200.189.160.0    200.215.186.7                 0 13878 i
*> 200.189.164.0/23 200.215.186.7                 0 13878 i
*> 200.195.224.0/19 200.215.186.5                 0 18747 i
*> 200.195.240.0/22 200.215.186.5                 0 18747 i
*> 200.195.246.0/23 200.215.186.5                 0 18747 i
*> 200.198.64.0/18  200.215.186.10                0 15180 i
*> 200.198.64.0/19  200.215.186.10                0 15180 i
```

*> 200.198.96.0/19 200.215.186.10 0 15180 i
*> 200.198.176.0/20 200.215.186.4 0 16397 i
*> 200.201.128.0/19 200.215.186.5 0 18747 i
*> 200.201.144.0/20 200.215.186.5 0 18747 i
*> 200.202.112.0/20 200.215.186.10 0 15180 i
*> 200.202.112.0/21 200.215.186.10 0 15180 i
*> 200.202.120.0/21 200.215.186.10 0 15180 i
*> 200.215.176.0/20 200.215.186.7 0 13878 i
*> 200.215.176.0/22 200.215.186.7 0 13878 i
*> 200.215.180.0/22 200.215.186.7 0 13878 i
*> 200.215.182.0/23 200.215.186.7 0 13878 i
*> 200.215.182.0 200.215.186.7 0 13878 i
*> 200.215.184.0/22 200.215.186.7 0 13878 i
*> 200.215.187.0 200.215.186.7 0 13878 i
*> 200.215.208.0/20 200.215.186.5 0 18747 i
*> 200.219.0.0/18 200.215.186.4 0 16397 i
*> 200.220.0.0/18 200.215.186.14 0 5772 i
*> 200.220.64.0/18 200.215.186.14 0 5772 i
*> 200.225.192.0/18 200.215.186.15 0 16735 i
*> 200.225.192.0/21 200.215.186.15 0 16735 i
*> 200.225.200.0/21 200.215.186.15 0 16735 i
*> 200.225.208.0/21 200.215.186.15 0 16735 i
*> 200.225.212.0/22 200.215.186.15 0 16735 i
*> 200.225.216.0/21 200.215.186.15 0 16735 i
*> 200.225.224.0/21 200.215.186.15 0 16735 i
*> 200.225.232.0/21 200.215.186.15 0 16735 i
*> 200.225.240.0/21 200.215.186.15 0 16735 i
*> 200.225.248.0/21 200.215.186.15 0 16735 i
*> 200.233.128.0/18 200.215.186.15 0 16735 i
*> 209.58.74.0 200.215.186.7 0 13878 i
*> 209.58.125.0 200.215.186.7 0 13878 i
*> 216.72.229.0 200.215.186.7 0 13878 i

Total number of prefixes 100

Rotas anunciadas (200.215.186.9) depois da mudança

Nap# sh ip bgp neighbors 200.215.186.9 adv
Nap# sh ip bgp neighbors 200.215.186.9 advertised-routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next Hop Metric LocPrf Weight Path
*> 63.215.188.0/22 200.215.186.7 0 13878 i
*> 148.243.64.0/21 200.215.186.7 0 13878 i
*> 157.253.0.0 200.215.186.7 0 13878 i
*> 172.16.32.0/20 200.215.186.7 0 13878 i

```
*> 172.16.48.0/20   200.215.186.7                0 13878 i
*> 172.16.64.0/20   200.215.186.7                0 13878 i
*> 200.3.244.0      200.215.186.7                0 13878 i
*> 200.3.245.0      200.215.186.7                0 13878 i
*> 200.3.246.0      200.215.186.7                0 13878 i
*> 200.3.247.0      200.215.186.7                0 13878 i
*> 200.23.192.0/22  200.215.186.7                0 13878 i
*> 200.23.196.0     200.215.186.7                0 13878 i
*> 200.23.197.0     200.215.186.7                0 13878 i
*> 200.31.64.0      200.215.186.7                0 13878 i
*> 200.31.65.0      200.215.186.7                0 13878 i
*> 200.31.66.0      200.215.186.7                0 13878 i
*> 200.31.67.0      200.215.186.7                0 13878 i
*> 200.31.68.0      200.215.186.7                0 13878 i
*> 200.31.69.0      200.215.186.7                0 13878 i
*> 200.31.70.0      200.215.186.7                0 13878 i
*> 200.31.71.0      200.215.186.7                0 13878 i
*> 200.31.72.0      200.215.186.7                0 13878 i
*> 200.31.73.0      200.215.186.7                0 13878 i
*> 200.31.74.0      200.215.186.7                0 13878 i
*> 200.31.76.0      200.215.186.7                0 13878 i
*> 200.31.77.0      200.215.186.7                0 13878 i
*> 200.31.78.0      200.215.186.7                0 13878 i
*> 200.31.79.0      200.215.186.7                0 13878 i
*> 200.31.80.0      200.215.186.7                0 13878 i
*> 200.31.81.0      200.215.186.7                0 13878 i
*> 200.31.83.0      200.215.186.7                0 13878 i
*> 200.31.84.0      200.215.186.7                0 13878 i
*> 200.31.85.0      200.215.186.7                0 13878 i
*> 200.31.86.0      200.215.186.7                0 13878 i
*> 200.57.32.0/20   200.215.186.7                0 13878 i
*> 200.57.36.0/22   200.215.186.7                0 13878 i
*> 200.99.0.0/17    200.215.186.10               0 15180 i
*> 200.99.0.0/18    200.215.186.10               0 15180 i
*> 200.99.64.0/18   200.215.186.10               0 15180 i
*> 200.142.160.0/20 200.215.186.10               0 15180 26104 i
*> 200.142.208.0/20 200.215.186.4                0 16397 i
*> 200.142.224.0/20 200.215.186.10               0 15180 26090 i
*> 200.143.0.0/19   200.215.186.7                0 13878 i
*> 200.143.0.0/22   200.215.186.7                0 13878 i
*> 200.146.192.0/18 200.215.186.15               0 16735 i
*> 200.150.0.0/21   200.215.186.10               0 15180 23106 i
*> 200.152.48.0/20  200.215.186.10               0 15180 26616 i
*> 200.152.48.0/22  200.215.186.10               0 15180 26616 i
*> 200.152.52.0/22  200.215.186.10               0 15180 26616 i
*> 200.155.0.0/19   200.215.186.4                0 16397 i
*> 200.155.128.0/18 200.215.186.5                0 18747 i
*> 200.155.128.0/21 200.215.186.5                0 18747 i
```

```
*> 200.155.136.0/22 200.215.186.5                0 18747 i
*> 200.162.0.0/17   200.215.186.10               0 15180 i
*> 200.162.0.0/18   200.215.186.10               0 15180 i
*> 200.162.64.0/18  200.215.186.10               0 15180 i
*> 200.162.176.0/20 200.215.186.10               0 15180 22129 i
*> 200.162.176.0    200.215.186.10               0 15180 22129 i
*> 200.162.177.0    200.215.186.10               0 15180 22129 i
*> 200.170.128.0/18 200.215.186.15               0 16735 i
*> 200.170.128.0/21 200.215.186.15               0 16735 i
*> 200.170.136.0/21 200.215.186.15               0 16735 i
*> 200.170.144.0/21 200.215.186.15               0 16735 i
*> 200.170.152.0/21 200.215.186.15               0 16735 i
*> 200.170.160.0/21 200.215.186.15               0 16735 i
*> 200.170.168.0/21 200.215.186.15               0 16735 i
*> 200.170.176.0/20 200.215.186.15               0 16735 i
*> 200.170.192.0/18 200.215.186.5                0 18747 i
*> 200.170.224.0/20 200.215.186.5                0 18747 i
*> 200.189.160.0/19 200.215.186.7                0 13878 i
*> 200.189.160.0    200.215.186.7                0 13878 i
*> 200.189.164.0/23 200.215.186.7                0 13878 i
*> 200.195.224.0/19 200.215.186.5                0 18747 i
*> 200.195.240.0/22 200.215.186.5                0 18747 i
*> 200.195.246.0/23 200.215.186.5                0 18747 i
*> 200.196.32.0/20  200.215.186.10               0 15180 11431 i
*> 200.196.32.0/22  200.215.186.10               0 15180 11431 i
*> 200.196.36.0/23  200.215.186.10               0 15180 11431 11431 1
1431 i
*> 200.196.38.0/23  200.215.186.10               0 15180 11431 i
*> 200.196.40.0/23  200.215.186.10               0 15180 11431 11431 1
1431 i
*> 200.196.42.0/23  200.215.186.10               0 15180 11431 i
*> 200.196.44.0/23  200.215.186.10               0 15180 11431 i
*> 200.196.46.0/23  200.215.186.10               0 15180 11431 11431 1
1431 i
*> 200.198.64.0/18  200.215.186.10               0 15180 i
*> 200.198.64.0/19  200.215.186.10               0 15180 i
*> 200.198.96.0/19  200.215.186.10               0 15180 i
*> 200.198.176.0/20 200.215.186.4                0 16397 i
*> 200.201.128.0/19 200.215.186.5                0 18747 i
*> 200.201.144.0/20 200.215.186.5                0 18747 i
*> 200.202.112.0/20 200.215.186.10               0 15180 i
*> 200.202.112.0/21 200.215.186.10               0 15180 i
*> 200.202.120.0/21 200.215.186.10               0 15180 i
*> 200.215.176.0/20 200.215.186.7                0 13878 i
*> 200.215.176.0/22 200.215.186.7                0 13878 i
*> 200.215.180.0/22 200.215.186.7                0 13878 i
*> 200.215.182.0/23 200.215.186.7                0 13878 i
*> 200.215.182.0    200.215.186.7                0 13878 i
```

*> 200.215.184.0/22 200.215.186.7 0 13878 i
*> 200.215.187.0 200.215.186.7 0 13878 i
*> 200.215.208.0/20 200.215.186.5 0 18747 i
*> 200.219.0.0/18 200.215.186.4 0 16397 i
*> 200.219.224.0/23 200.215.186.10 0 15180 14026 i
*> 200.220.0.0/18 200.215.186.14 0 5772 i
*> 200.220.64.0/18 200.215.186.14 0 5772 i
*> 200.220.141.0 200.215.186.10 0 15180 27693 i
*> 200.220.142.0 200.215.186.10 0 15180 27693 i
*> 200.225.192.0/18 200.215.186.15 0 16735 i
*> 200.225.192.0/21 200.215.186.15 0 16735 i
*> 200.225.200.0/21 200.215.186.15 0 16735 i
*> 200.225.208.0/21 200.215.186.15 0 16735 i
*> 200.225.212.0/22 200.215.186.15 0 16735 i
*> 200.225.216.0/21 200.215.186.15 0 16735 i
*> 200.225.224.0/21 200.215.186.15 0 16735 i
*> 200.225.232.0/21 200.215.186.15 0 16735 i
*> 200.225.240.0/21 200.215.186.15 0 16735 i
*> 200.225.248.0/21 200.215.186.15 0 16735 i
*> 200.229.0.0/20 200.215.186.10 0 15180 16712 16712 1
6712 i
*> 200.233.128.0/18 200.215.186.15 0 16735 i
*> 209.58.74.0 200.215.186.7 0 13878 i
*> 209.58.125.0 200.215.186.7 0 13878 i
*> 216.72.229.0 200.215.186.7 0 13878 i

Total number of prefixes 121

Rotas anunciadas (200.215.186.10) antes da mudança

Nap# sh ip bgp neighbors 200.215.186.10 adv
Nap# sh ip bgp neighbors 200.215.186.10 advertised-routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - i
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 63.215.188.0/22 200.215.186.7 0 13878 i
*> 148.243.64.0/21 200.215.186.7 0 13878 i
*> 157.253.0.0 200.215.186.7 0 13878 i
*> 172.16.32.0/20 200.215.186.7 0 13878 i
*> 172.16.48.0/20 200.215.186.7 0 13878 i
*> 172.16.64.0/20 200.215.186.7 0 13878 i
*> 200.3.244.0 200.215.186.7 0 13878 i
*> 200.3.245.0 200.215.186.7 0 13878 i
*> 200.3.246.0 200.215.186.7 0 13878 i
*> 200.3.247.0 200.215.186.7 0 13878 i
*> 200.23.192.0/22 200.215.186.7 0 13878 i

```
*> 200.23.196.0     200.215.186.7                0 13878 i
*> 200.23.197.0     200.215.186.7                0 13878 i
*> 200.31.64.0      200.215.186.7                0 13878 i
*> 200.31.65.0      200.215.186.7                0 13878 i
*> 200.31.66.0      200.215.186.7                0 13878 i
*> 200.31.67.0      200.215.186.7                0 13878 i
*> 200.31.68.0      200.215.186.7                0 13878 i
*> 200.31.69.0      200.215.186.7                0 13878 i
*> 200.31.70.0      200.215.186.7                0 13878 i
*> 200.31.71.0      200.215.186.7                0 13878 i
*> 200.31.72.0      200.215.186.7                0 13878 i
*> 200.31.73.0      200.215.186.7                0 13878 i
*> 200.31.74.0      200.215.186.7                0 13878 i
*> 200.31.76.0      200.215.186.7                0 13878 i
*> 200.31.77.0      200.215.186.7                0 13878 i
*> 200.31.78.0      200.215.186.7                0 13878 i
*> 200.31.79.0      200.215.186.7                0 13878 i
*> 200.31.80.0      200.215.186.7                0 13878 i
*> 200.31.81.0      200.215.186.7                0 13878 i
*> 200.31.83.0      200.215.186.7                0 13878 i
*> 200.31.84.0      200.215.186.7                0 13878 i
*> 200.31.85.0      200.215.186.7                0 13878 i
*> 200.31.86.0      200.215.186.7                0 13878 i
*> 200.49.77.0      200.215.186.9                0 13591 i
*> 200.57.32.0/20   200.215.186.7                0 13878 i
*> 200.57.36.0/22   200.215.186.7                0 13878 i
*> 200.142.64.0/19  200.215.186.9                0 13591 i
*> 200.142.95.0     200.215.186.9                0 13591 i
*> 200.142.208.0/20 200.215.186.4                0 16397 i
*> 200.143.0.0/19   200.215.186.7                0 13878 i
*> 200.143.0.0/22   200.215.186.7                0 13878 i
*> 200.146.192.0/18 200.215.186.15               0 16735 i
*> 200.152.192.0/19 200.215.186.9                0 13591 i
*> 200.155.0.0/19   200.215.186.4                0 16397 i
*> 200.155.128.0/18 200.215.186.5                0 18747 i
*> 200.155.128.0/21 200.215.186.5                0 18747 i
*> 200.155.136.0/22 200.215.186.5                0 18747 i
*> 200.160.224.0/19 200.215.186.9                0 13591 i
*> 200.170.128.0/18 200.215.186.15               0 16735 i
*> 200.170.128.0/21 200.215.186.15               0 16735 i
*> 200.170.136.0/21 200.215.186.15               0 16735 i
*> 200.170.144.0/21 200.215.186.15               0 16735 i
*> 200.170.152.0/21 200.215.186.15               0 16735 i
*> 200.170.160.0/21 200.215.186.15               0 16735 i
*> 200.170.168.0/21 200.215.186.15               0 16735 i
*> 200.170.176.0/20 200.215.186.15               0 16735 i
*> 200.170.192.0/18 200.215.186.5                0 18747 i
*> 200.170.224.0/20 200.215.186.5                0 18747 i
```

*> 200.189.160.0/19 200.215.186.7 0 13878 i
*> 200.189.160.0 200.215.186.7 0 13878 i
*> 200.189.164.0/23 200.215.186.7 0 13878 i
*> 200.195.224.0/19 200.215.186.5 0 18747 i
*> 200.195.240.0/22 200.215.186.5 0 18747 i
*> 200.195.246.0/23 200.215.186.5 0 18747 i
*> 200.198.176.0/20 200.215.186.4 0 16397 i
*> 200.201.128.0/19 200.215.186.5 0 18747 i
*> 200.201.144.0/20 200.215.186.5 0 18747 i
*> 200.215.176.0/20 200.215.186.7 0 13878 i
*> 200.215.176.0/22 200.215.186.7 0 13878 i
*> 200.215.180.0/22 200.215.186.7 0 13878 i
*> 200.215.182.0/23 200.215.186.7 0 13878 i
*> 200.215.182.0 200.215.186.7 0 13878 i
*> 200.215.184.0/22 200.215.186.7 0 13878 i
*> 200.215.187.0 200.215.186.7 0 13878 i
*> 200.215.208.0/20 200.215.186.5 0 18747 i
*> 200.219.0.0/18 200.215.186.4 0 16397 i
*> 200.220.0.0/18 200.215.186.14 0 5772 i
*> 200.220.64.0/18 200.215.186.14 0 5772 i
*> 200.225.64.0/20 200.215.186.9 0 13591 i
*> 200.225.192.0/18 200.215.186.15 0 16735 i
*> 200.225.192.0/21 200.215.186.15 0 16735 i
*> 200.225.200.0/21 200.215.186.15 0 16735 i
*> 200.225.208.0/21 200.215.186.15 0 16735 i
*> 200.225.212.0/22 200.215.186.15 0 16735 i
*> 200.225.216.0/21 200.215.186.15 0 16735 i
*> 200.225.224.0/21 200.215.186.15 0 16735 i
*> 200.225.232.0/21 200.215.186.15 0 16735 i
*> 200.225.240.0/21 200.215.186.15 0 16735 i
*> 200.225.248.0/21 200.215.186.15 0 16735 i
*> 200.233.128.0/18 200.215.186.15 0 16735 i
*> 209.58.74.0 200.215.186.7 0 13878 i
*> 209.58.125.0 200.215.186.7 0 13878 i
*> 216.72.229.0 200.215.186.7 0 13878 i

Total number of prefixes 94

Rotas anunciadas (200.215.186.10) depois da mudança

Nap# sh ip bgp neighbors 200.215.186.10 advertised-routes
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 63.215.188.0/22 200.215.186.7 0 13878 i

```
*> 63.250.176.0/23  200.215.186.9                0 13591 3300 i
*> 63.250.180.0/23  200.215.186.9                0 13591 3300 i
*> 129.222.32.0/19  200.215.186.9                0 13591 5772 i
*> 129.222.64.0/19  200.215.186.9                0 13591 5772 i
*> 148.188.174.0/24 200.215.186.9                0 13591 3300 i
*> 148.243.64.0/21  200.215.186.7                0 13878 i
*> 157.253.0.0      200.215.186.7                0 13878 i
*> 172.16.32.0/20   200.215.186.7                0 13878 i
*> 172.16.48.0/20   200.215.186.7                0 13878 i
*> 172.16.64.0/20   200.215.186.7                0 13878 i
*> 192.5.5.0        200.215.186.9                0 13591 22548 30122 3
557 i
*> 192.175.48.0     200.215.186.9                0 13591 22548 112 i
*> 192.228.80.0     200.215.186.9                0 13591 22548 30122 i
*> 200.3.244.0      200.215.186.7                0 13878 i
*> 200.3.245.0      200.215.186.7                0 13878 i
*> 200.3.246.0      200.215.186.7                0 13878 i
*> 200.3.247.0      200.215.186.7                0 13878 i
*> 200.23.192.0/22  200.215.186.7                0 13878 i
*> 200.23.196.0     200.215.186.7                0 13878 i
*> 200.23.197.0     200.215.186.7                0 13878 i
*> 200.31.64.0      200.215.186.7                0 13878 i
*> 200.31.65.0      200.215.186.7                0 13878 i
*> 200.31.66.0      200.215.186.7                0 13878 i
*> 200.31.67.0      200.215.186.7                0 13878 i
*> 200.31.68.0      200.215.186.7                0 13878 i
*> 200.31.69.0      200.215.186.7                0 13878 i
*> 200.31.70.0      200.215.186.7                0 13878 i
*> 200.31.71.0      200.215.186.7                0 13878 i
*> 200.31.72.0      200.215.186.7                0 13878 i
*> 200.31.73.0      200.215.186.7                0 13878 i
*> 200.31.74.0      200.215.186.7                0 13878 i
*> 200.31.76.0      200.215.186.7                0 13878 i
*> 200.31.77.0      200.215.186.7                0 13878 i
*> 200.31.78.0      200.215.186.7                0 13878 i
*> 200.31.79.0      200.215.186.7                0 13878 i
*> 200.31.80.0      200.215.186.7                0 13878 i
*> 200.31.81.0      200.215.186.7                0 13878 i
*> 200.31.83.0      200.215.186.7                0 13878 i
*> 200.31.84.0      200.215.186.7                0 13878 i
*> 200.31.85.0      200.215.186.7                0 13878 i
*> 200.31.86.0      200.215.186.7                0 13878 i
*> 200.49.77.0      200.215.186.9                0 13591 i
*> 200.57.32.0/20   200.215.186.7                0 13878 i
*> 200.57.36.0/22   200.215.186.7                0 13878 i
*> 200.142.64.0/19  200.215.186.9                0 13591 i
*> 200.142.95.0     200.215.186.9                0 13591 i
*> 200.142.208.0/20 200.215.186.4                0 16397 i
```

```
*> 200.143.0.0/19   200.215.186.7                0 13878 i
*> 200.143.0.0/22   200.215.186.7                0 13878 i
*> 200.146.192.0/18 200.215.186.15                0 16735 i
*> 200.150.192.0/20 200.215.186.9                 0 13591 26107 i
*> 200.152.192.0/19 200.215.186.9                 0 13591 i
*> 200.155.0.0/19   200.215.186.4                 0 16397 i
*> 200.155.15.0     200.215.186.9                 0 13591 16397 i
*> 200.155.16.0/20  200.215.186.9                 0 13591 16397 i
*> 200.155.96.0/20  200.215.186.9                 0 13591 23002 i
*> 200.155.98.0     200.215.186.9                 0 13591 23002 ?
*> 200.155.107.0    200.215.186.9                 0 13591 23002 i
*> 200.155.108.0    200.215.186.9                 0 13591 23002 i
*> 200.155.128.0/18 200.215.186.5                 0 18747 i
*> 200.155.128.0/21 200.215.186.5                 0 18747 i
*> 200.155.136.0/22 200.215.186.5                 0 18747 i
*> 200.160.0.0/20   200.215.186.9                 0 13591 22548 i
*> 200.160.174.0    200.215.186.9                 0 13591 22341 i
*> 200.160.224.0/19 200.215.186.9                 0 13591 i
*> 200.162.128.0/20 200.215.186.9                 0 13591 22177 i
*> 200.169.128.0/17 200.215.186.9                 0 13591 14650 i
*> 200.170.128.0/18 200.215.186.15                0 16735 i
*> 200.170.128.0/21 200.215.186.15                0 16735 i
*> 200.170.136.0/21 200.215.186.15                0 16735 i
*> 200.170.144.0/21 200.215.186.15                0 16735 i
*> 200.170.152.0/21 200.215.186.15                0 16735 i
*> 200.170.160.0/21 200.215.186.15                0 16735 i
*> 200.170.168.0/21 200.215.186.15                0 16735 i
*> 200.170.176.0/20 200.215.186.15                0 16735 i
*> 200.170.192.0/18 200.215.186.5                 0 18747 i
*> 200.170.224.0/20 200.215.186.5                 0 18747 i
*> 200.189.96.0/22  200.215.186.9                 0 13591 18739 i
*> 200.189.100.0/22 200.215.186.9                 0 13591 18739 i
*> 200.189.104.0/22 200.215.186.9                 0 13591 18739 i
*> 200.189.108.0/22 200.215.186.9                 0 13591 18739 i
*> 200.189.160.0/19 200.215.186.7                 0 13878 i
*> 200.189.160.0    200.215.186.7                 0 13878 i
*> 200.189.164.0/23 200.215.186.7                 0 13878 i
*> 200.192.160.0/20 200.215.186.9                 0 13591 19089 13935 i
*> 200.192.216.0/21 200.215.186.9                 0 13591 14723 i
*> 200.195.224.0/19 200.215.186.5                 0 18747 i
*> 200.195.240.0/22 200.215.186.5                 0 18747 i
*> 200.195.246.0/23 200.215.186.5                 0 18747 i
*> 200.198.176.0/20 200.215.186.4                 0 16397 i
*> 200.198.184.0/23 200.215.186.9                 0 13591 16397 i
*> 200.201.128.0/19 200.215.186.5                 0 18747 i
*> 200.201.144.0/20 200.215.186.5                 0 18747 i
*> 200.215.128.0/19 200.215.186.9                 0 13591 10688 i
*> 200.215.176.0/20 200.215.186.7                 0 13878 i
```

```
*> 200.215.176.0/22 200.215.186.7                0 13878 i
*> 200.215.180.0/22 200.215.186.7                0 13878 i
*> 200.215.182.0/23 200.215.186.7                0 13878 i
*> 200.215.182.0    200.215.186.7                0 13878 i
*> 200.215.184.0/22 200.215.186.7                0 13878 i
*> 200.215.187.0    200.215.186.7                0 13878 i
*> 200.215.208.0/20 200.215.186.5                0 18747 i
*> 200.219.0.0/18   200.215.186.4                0 16397 i
*> 200.219.64.0/18  200.215.186.9                0 13591 14650 i
*> 200.219.128.0    200.215.186.9                0 13591 7313 7313 731
3 7313 7313 7313 7313 7313 7313 7313 7313 i
*> 200.220.0.0/18   200.215.186.14               0 5772 i
*> 200.220.64.0/18  200.215.186.14               0 5772 i
*> 200.225.64.0/20  200.215.186.9                0 13591 i
*> 200.225.80.0/20  200.215.186.9                0 13591 19089 i
*> 200.225.80.0/22  200.215.186.9                0 13591 19089 i
*> 200.225.84.0/22  200.215.186.9                0 13591 19089 i
*> 200.225.88.0/22  200.215.186.9                0 13591 19089 i
*> 200.225.92.0/22  200.215.186.9                0 13591 19089 i
*> 200.225.160.0/19 200.215.186.9                0 13591 14650 i
*> 200.225.192.0/18 200.215.186.15               0 16735 i
*> 200.225.192.0/21 200.215.186.15               0 16735 i
*> 200.225.200.0/21 200.215.186.15               0 16735 i
*> 200.225.208.0/21 200.215.186.15               0 16735 i
*> 200.225.212.0/22 200.215.186.15               0 16735 i
*> 200.225.216.0/21 200.215.186.15               0 16735 i
*> 200.225.224.0/21 200.215.186.15               0 16735 i
*> 200.225.232.0/21 200.215.186.15               0 16735 i
*> 200.225.240.0/21 200.215.186.15               0 16735 i
*> 200.225.248.0/21 200.215.186.15               0 16735 i
*> 200.229.16.0/20  200.215.186.9                0 13591 16736 i
*> 200.229.16.0/22  200.215.186.9                0 13591 16736 i
*> 200.229.20.0/22  200.215.186.9                0 13591 16736 i
*> 200.229.24.0/22  200.215.186.9                0 13591 16736 i
*> 200.233.128.0/18 200.215.186.15               0 16735 i
*> 207.83.96.0/20   200.215.186.9                0 13591 3300 i
*> 209.58.74.0      200.215.186.7                0 13878 i
*> 209.58.125.0     200.215.186.7                0 13878 i
*> 216.72.229.0     200.215.186.7                0 13878 i
```

Analisou-se o aumento das redes recebidas e enviadas depois da implementação do filtros.

Gráfico antes da alteração – 200.215.186.10 (Entrada 1.09 Mbps Saída 3.00 Mbps)

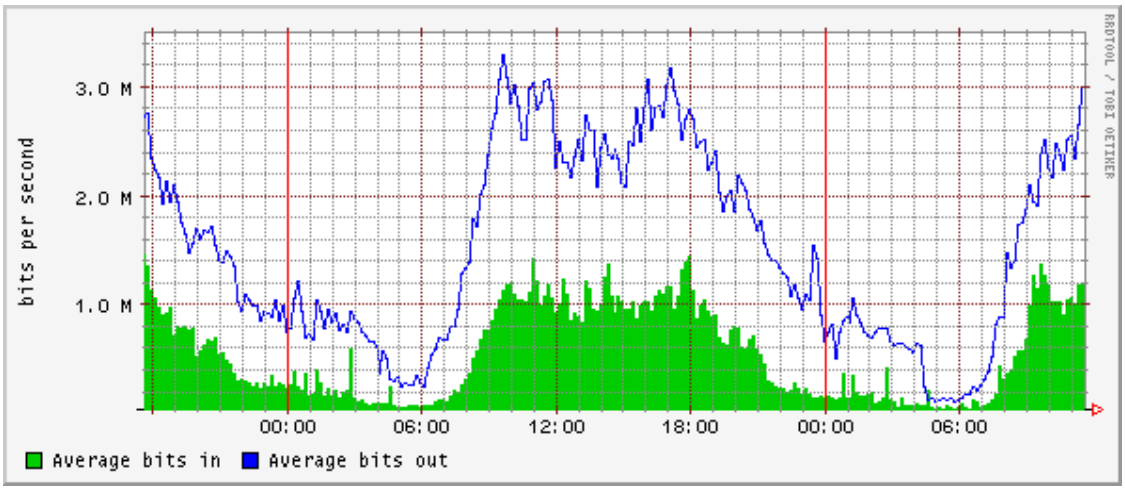


Gráfico depois da alteração – 200.215.186.10 (Entrada 2.0 Mbps Saída 3.11 Mbps)

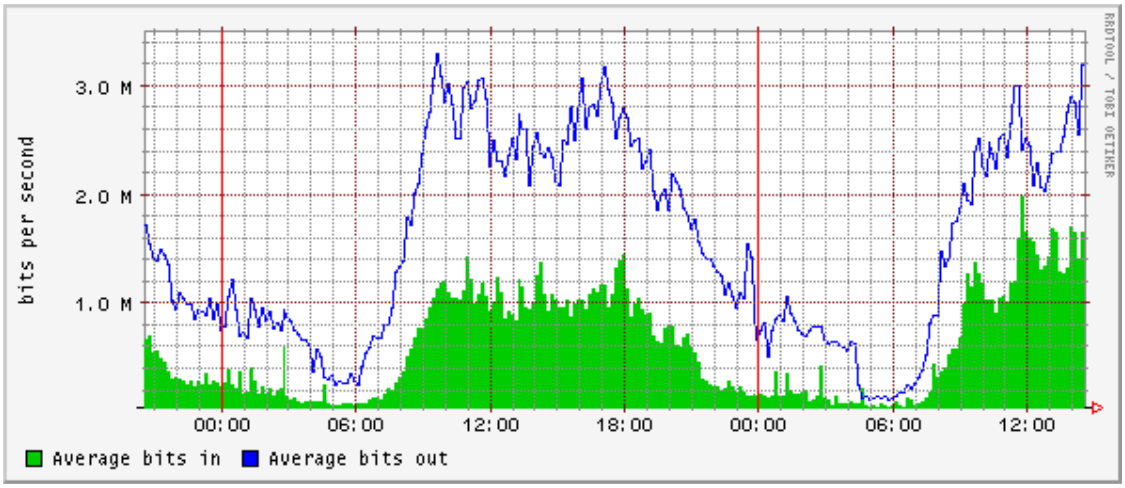


Gráfico antes da alteração - 200.215.186.9 (entrada 2.15 Mbps saída 1.73 Mbps)

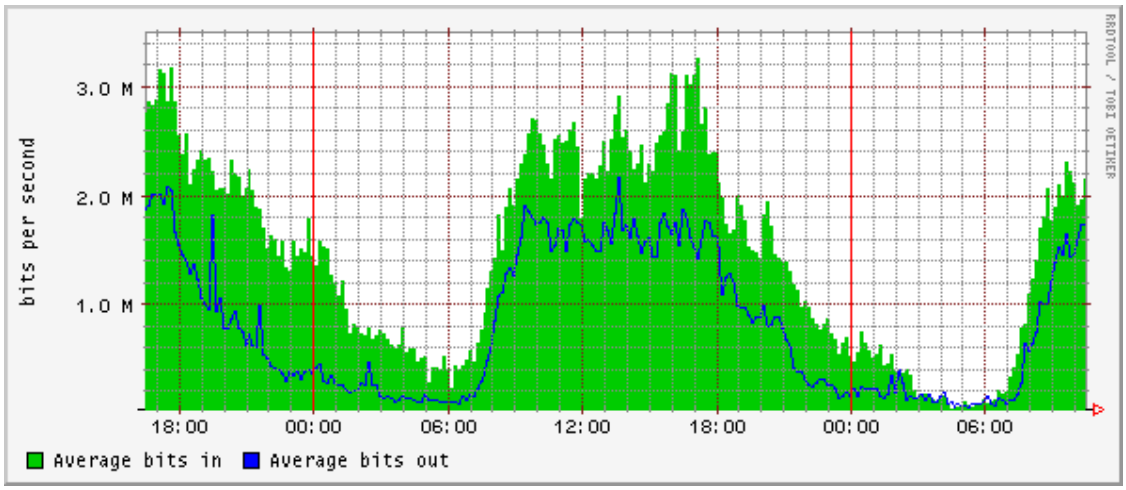
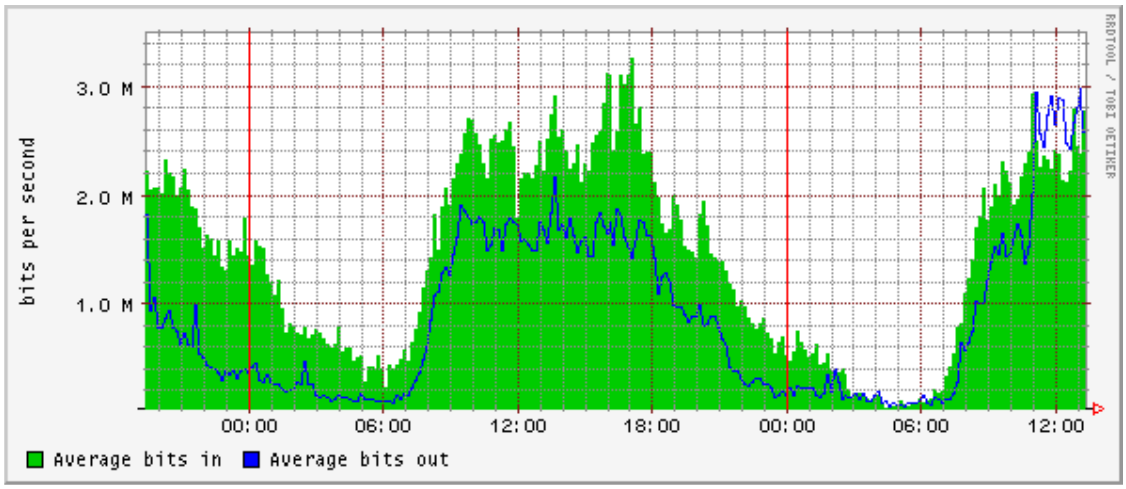


Gráfico depois da alteração – 200.215.186.9 (Entrada 2.77 Mbps Saída 2.58 Mbps)



Observou-se o aumento do tráfego depois da alteração dos filtros.

APÊNDICE D – Configuração e comandos executados no PTT em produção

Configuração do Zebra

```
Current configuration:
!
hostname Nap
log file bgpd.log
log stdout
!
bgp multiple-instance
!
router bgp 65500
 bgp router-id 200.215.186.2
 neighbor 200.215.186.3 remote-as 14026
 neighbor 200.215.186.3 filter-list provedor1 in
 neighbor 200.215.186.3 filter-list global out
 neighbor 200.215.186.3 attribute-unchanged as-path next-hop
 neighbor 200.215.186.4 remote-as 16397
 neighbor 200.215.186.4 filter-list provedor2 in
 neighbor 200.215.186.4 filter-list global out
 neighbor 200.215.186.4 attribute-unchanged as-path next-hop
 neighbor 200.215.186.5 remote-as 18747
 neighbor 200.215.186.5 filter-list provedor3 in
 neighbor 200.215.186.5 filter-list global out
 neighbor 200.215.186.5 attribute-unchanged as-path next-hop
 neighbor 200.215.186.6 remote-as 14346
 neighbor 200.215.186.6 filter-list provedor4 in
 neighbor 200.215.186.6 filter-list global out
 neighbor 200.215.186.6 attribute-unchanged as-path next-hop
 neighbor 200.215.186.7 remote-as 13878
 neighbor 200.215.186.7 filter-list provedor5 in
 neighbor 200.215.186.7 filter-list globalidc out
 neighbor 200.215.186.7 attribute-unchanged as-path next-hop
 neighbor 200.215.186.9 remote-as 13591
 neighbor 200.215.186.9 filter-list provedor6 in
 neighbor 200.215.186.9 attribute-unchanged as-path next-hop
 neighbor 200.215.186.10 remote-as 15180

neighbor 200.215.186.10 filter-list provedor7 in
 neighbor 200.215.186.10 attribute-unchanged as-path next-hop
 neighbor 200.215.186.11 remote-as 14571
neighbor 200.215.186.11 filter-list provedor8 in
     neighbor 200.215.186.11 filter-list global out
 neighbor 200.215.186.11 attribute-unchanged as-path next-hop
```

```
access-list 9 permit 200.189.167.6
access-list 9 permit 200.202.114.16
access-list 9 permit 200.215.179.32
access-list 9 permit 200.215.186.2
access-list 9 permit 200.215.186.25
access-list 9 permit 200.215.186.26
access-list 9 deny any
!
ip as-path access-list provedor4 permit ^14346$
     ip as-path access-list provedor2 permit ^16397$
ip as-path access-list provedor7 permit ^15180_
ip as-path access-list global permit ^14346$
ip as-path access-list global permit ^19182$
ip as-path access-list global permit ^16397$
ip as-path access-list global permit ^15180$
ip as-path access-list global permit ^16735$
ip as-path access-list global permit ^13878$
ip as-path access-list global permit ^18747$
ip as-path access-list global permit ^14571$
ip as-path access-list global permit ^13591$
ip as-path access-list global permit ^5772$
ip as-path access-list global permit ^14026$
ip as-path access-list globalidc permit ^14346$
ip as-path access-list globalidc permit ^19182$
ip as-path access-list globalidc permit ^16397$
ip as-path access-list globalidc permit ^18747$
ip as-path access-list globalidc permit ^14571$
ip as-path access-list globalidc permit ^13591_
ip as-path access-list globalidc permit ^5772$
ip as-path access-list globalidc permit ^14026$
ip as-path access-list provedor5 permit ^13878$
ip as-path access-list provedor3 permit ^18747$

ip as-path access-list provedor8 permit ^14571$
ip as-path access-list provedor6 permit ^13591_
     ip as-path access-list provedor1 permit ^14026$
!
line vty
 access-class 9
!
end
```

Relação de participantes

```
sh ip bgp summary
BGP router identifier 200.215.186.2, local AS number 65500
38 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
  State/PfxRcd
200.215.186.3   4 14026       0       0        0    0    0 00:01:26 Active
200.215.186.4   4 16397   50493   50582        0    0    0 05w0d00h        2
200.215.186.5   4 18747   49358   49540        0    0    0 6d00h23m       11
200.215.186.6   4 14346       0       0        0    0    0 00:01:21 Active
200.215.186.7   4 13878   50504   50631        0    0    0 04w6d23h       51
200.215.186.9   4 13591   50982   50647        0    0    0 05w0d00h       50
200.215.186.10  4 15180   50755   50704        0    0    0 02w6d06h       33
200.215.186.11  4 14571   50431   50613        0    0    0 05w0d00h        0
200.215.186.13  4 19182       0       0        0    0    0 00:01:31 Active
200.215.186.14  4  5772   50447   50612        0    0    0 05w0d00h        2
200.215.186.15  4 16735   50454   50597        0    0    0 05w0d00h       20

Total number of neighbors 11
```

Todas as rotas BGP recebidas

```
sh ip bgp
BGP table version is 0, local router ID is 200.215.186.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 63.215.188.0/22  200.215.186.7                         0 13878 i
*> 63.250.176.0/23  200.215.186.9                         0 13591 3300 i
*> 63.250.180.0/23  200.215.186.9                         0 13591 3300 i
*> 129.222.32.0/19  200.215.186.9                         0 13591 5772 i
*> 129.222.64.0/19  200.215.186.9                         0 13591 5772 i
*> 148.188.174.0/24 200.215.186.9                         0 13591 3300 i
*> 148.243.64.0/21  200.215.186.7                         0 13878 i
*> 157.253.0.0      200.215.186.7                         0 13878 i
*> 172.16.32.0/20   200.215.186.7                         0 13878 i

*> 172.16.48.0/20   200.215.186.7                         0 13878 i
*> 172.16.64.0/20   200.215.186.7           0             0 13878 i
*> 192.5.5.0        200.215.186.9                         0 13591 22548 30122 3557 i
*> 192.175.48.0     200.215.186.9                         0 13591 22548 112 i
*> 192.228.80.0     200.215.186.9                         0 13591 22548 30122 i
*> 200.3.244.0      200.215.186.7                         0 13878 i
*> 200.3.245.0      200.215.186.7                         0 13878 i
*> 200.3.246.0      200.215.186.7                         0 13878 i

*> 200.3.247.0      200.215.186.7                         0 13878 i
*> 200.23.192.0/22  200.215.186.7                         0 13878 i
*> 200.23.196.0     200.215.186.7                         0 13878 i
```

```
*> 200.23.197.0     200.215.186.7                0 13878 i
*> 200.31.64.0      200.215.186.7                0 13878 i
*> 200.31.65.0      200.215.186.7                0 13878 i
*> 200.31.66.0      200.215.186.7                0 13878 i
*> 200.31.67.0      200.215.186.7                0 13878 i
*> 200.31.68.0      200.215.186.7                0 13878 i
*> 200.31.69.0      200.215.186.7                0 13878 i
*> 200.31.70.0      200.215.186.7                0 13878 i
*> 200.31.71.0      200.215.186.7                0 13878 i
*> 200.31.72.0      200.215.186.7                0 13878 i
*> 200.31.73.0      200.215.186.7                0 13878 i
*> 200.31.74.0      200.215.186.7                0 13878 i
*> 200.31.76.0      200.215.186.7                0 13878 i
*> 200.31.77.0      200.215.186.7                0 13878 i
*> 200.31.78.0      200.215.186.7                0 13878 i
*> 200.31.79.0      200.215.186.7                0 13878 i
*> 200.31.80.0      200.215.186.7                0 13878 i
*> 200.31.81.0      200.215.186.7                0 13878 i
*> 200.31.83.0      200.215.186.7                0 13878 i
*> 200.31.84.0      200.215.186.7                0 13878 i
*> 200.31.85.0      200.215.186.7                0 13878 i
*> 200.31.86.0      200.215.186.7                0 13878 i
*> 200.49.77.0      200.215.186.9                0 13591 i
*> 200.57.32.0/20   200.215.186.7                 0 13878 i
*> 200.57.36.0/22   200.215.186.7                 0 13878 i
*> 200.99.0.0/17    200.215.186.10                0 15180 i
*> 200.99.0.0/18    200.215.186.10                0 15180 i

*> 200.99.64.0/18   200.215.186.10                0 15180 i
*> 200.142.64.0/19  200.215.186.9                 0 13591 i
*> 200.142.95.0     200.215.186.9                0 13591 i
*> 200.142.160.0/20 200.215.186.10                 0 15180 26104 i
*> 200.142.208.0/20 200.215.186.9                  0 13591 16397 26602 i
*> 200.142.224.0/20 200.215.186.10                 0 15180 26090 i
*> 200.143.0.0/19   200.215.186.7                 0 13878 i
*> 200.143.0.0/22   200.215.186.7          0      0 13878 i
*> 200.146.192.0/18 200.215.186.15                 0 16735 i

*> 200.150.0.0/21   200.215.186.10                0 15180 23106 i
*> 200.150.192.0/20 200.215.186.9                 0 13591 26107 i
*> 200.152.48.0/20  200.215.186.10                0 15180 26616 i
*> 200.152.48.0/22  200.215.186.10                0 15180 26616 i
*> 200.152.52.0/22  200.215.186.10                0 15180 26616 i
*> 200.152.192.0/19 200.215.186.9                 0 13591 i
*> 200.155.0.0/19   200.215.186.4                 0 16397 i
*> 200.155.15.0     200.215.186.9                0 13591 16397 i
*> 200.155.16.0/20  200.215.186.9                 0 13591 16397 i
*> 200.155.96.0/20  200.215.186.9                 0 13591 23002 i
```

```
*> 200.155.98.0     200.215.186.9                0 13591 23002 ?
*> 200.155.107.0    200.215.186.9                0 13591 23002 i
*> 200.155.108.0    200.215.186.9                0 13591 23002 i
*> 200.155.128.0/18 200.215.186.5                0 18747 i
*> 200.155.128.0/21 200.215.186.5                0 18747 i
*> 200.155.136.0/22 200.215.186.5                0 18747 i
*> 200.160.0.0/20   200.215.186.9                0 13591 22548 i
*> 200.160.174.0    200.215.186.9                0 13591 22341 i
*> 200.160.224.0/19 200.215.186.9                0 13591 i
*> 200.162.0.0/17   200.215.186.10               0 15180 i
*> 200.162.0.0/18   200.215.186.10               0 15180 i
*> 200.162.64.0/18  200.215.186.10               0 15180 i
*> 200.162.128.0/20 200.215.186.9                0 13591 22177 i
*> 200.162.176.0/20 200.215.186.10               0 15180 22129 i
*> 200.162.176.0    200.215.186.10               0 15180 22129 i
*> 200.162.177.0    200.215.186.10               0 15180 22129 i
*> 200.169.128.0/17 200.215.186.9                0 13591 14650 i
*> 200.170.128.0/18 200.215.186.15               0 16735 i
*> 200.170.128.0/21 200.215.186.15               0 16735 i

*> 200.170.136.0/21 200.215.186.15               0 16735 i
*> 200.170.144.0/21 200.215.186.15               0 16735 i
*> 200.170.152.0/21 200.215.186.15               0 16735 i
*> 200.170.160.0/21 200.215.186.15               0 16735 i
*> 200.170.168.0/21 200.215.186.15               0 16735 i
*> 200.170.176.0/20 200.215.186.15               0 16735 i
*> 200.170.192.0/18 200.215.186.5                0 18747 i
*> 200.170.224.0/20 200.215.186.5                0 18747 i
*> 200.189.96.0/22  200.215.186.9                0 13591 18739 i
*> 200.189.100.0/22 200.215.186.9                0 13591 18739 i
*> 200.189.104.0/22 200.215.186.9                0 13591 18739 i

*> 200.189.108.0/22 200.215.186.9                0 13591 18739 i
*> 200.189.160.0/19 200.215.186.7                0 13878 i
*> 200.189.160.0    200.215.186.7                0 13878 i
*> 200.189.164.0/23 200.215.186.7                0 13878 i
*> 200.192.160.0/20 200.215.186.9                0 13591 19089 13935 i
*> 200.192.216.0/21 200.215.186.9                0 13591 14723 i
*> 200.195.224.0/19 200.215.186.5                0 18747 i
*> 200.195.240.0/22 200.215.186.5                0 18747 i
*> 200.195.246.0/23 200.215.186.5                0 18747 i
*> 200.196.32.0/20  200.215.186.10               0 15180 11431 i
*> 200.196.32.0/22  200.215.186.10               0 15180 11431 i
*> 200.196.36.0/23  200.215.186.10               0 15180 11431 11431 11431 i
*> 200.196.38.0/23  200.215.186.10               0 15180 11431 11431 11431 i
*> 200.196.40.0/23  200.215.186.10               0 15180 11431 11431 11431 i
*> 200.196.42.0/23  200.215.186.10               0 15180 11431 i
*> 200.196.44.0/23  200.215.186.10               0 15180 11431 i
```

```
*> 200.196.46.0/23  200.215.186.10                0 15180 11431 11431 11431 i
*> 200.198.64.0/18  200.215.186.10                0 15180 i
*> 200.198.64.0/19  200.215.186.10                0 15180 i
*> 200.198.96.0/19  200.215.186.10                0 15180 i
*> 200.198.176.0/20 200.215.186.4                 0 16397 i
*> 200.198.184.0/23 200.215.186.9                 0 13591 16397 i
*> 200.201.128.0/19 200.215.186.5                 0 18747 i
*> 200.201.144.0/20 200.215.186.5                 0 18747 i
*> 200.202.112.0/20 200.215.186.10                 0 15180 i

*> 200.202.112.0/21 200.215.186.10                0 15180 i
*> 200.202.120.0/21 200.215.186.10                0 15180 i
*> 200.215.128.0/19 200.215.186.9                 0 13591 10688 i
*> 200.215.176.0/20 200.215.186.7                 0 13878 i
*> 200.215.176.0/22 200.215.186.7          0      0 13878 i
*> 200.215.180.0/22 200.215.186.7                 0 13878 i
*> 200.215.182.0/23 200.215.186.7                 0 13878 i
*> 200.215.182.0    200.215.186.7                 0 13878 i
*> 200.215.184.0/22 200.215.186.7                 0 13878 i
*> 200.215.187.0    200.215.186.7                 0 13878 i
*> 200.215.208.0/20 200.215.186.5                 0 18747 i
*> 200.219.0.0/18   200.215.186.9                 0 13591 16397 6543 i

*> 200.219.64.0/18  200.215.186.9                 0 13591 14650 i

*> 200.219.128.0    200.215.186.9                 0 13591 7313 7313 7313 7313
7313 7313 7313 7313 7313 7313 7313 i
*> 200.219.224.0/23 200.215.186.10                0 15180 14026 i
*  200.220.0.0/18   200.215.186.9                 0 13591 5772 i
*>                  200.215.186.14          0      0 5772 i
*  200.220.64.0/18  200.215.186.9                 0 13591 5772 i
*>                  200.215.186.14          0      0 5772 i
*> 200.220.141.0    200.215.186.10                0 15180 27693 i
*> 200.220.142.0    200.215.186.10                0 15180 27693 i
*> 200.225.64.0/20  200.215.186.9                 0 13591 i
*> 200.225.80.0/20  200.215.186.9                 0 13591 19089 i
*> 200.225.80.0/22  200.215.186.9                 0 13591 19089 i
*> 200.225.84.0/22  200.215.186.9                 0 13591 19089 i
*> 200.225.88.0/22  200.215.186.9                 0 13591 19089 i
*> 200.225.92.0/22  200.215.186.9                 0 13591 19089 i
*> 200.225.160.0/19 200.215.186.9                 0 13591 14650 i
*> 200.225.192.0/18 200.215.186.15                0 16735 i
*> 200.225.192.0/21 200.215.186.15                0 16735 i
*> 200.225.200.0/21 200.215.186.15                0 16735 i
*> 200.225.208.0/21 200.215.186.15                0 16735 i
*> 200.225.212.0/22 200.215.186.15                0 16735 i
*> 200.225.216.0/21 200.215.186.15                0 16735 i
*> 200.225.224.0/21 200.215.186.15                0 16735 i
```

```
*> 200.225.232.0/21 200.215.186.15                0 16735 i

*> 200.225.240.0/21 200.215.186.15                0 16735 i
*> 200.225.248.0/21 200.215.186.15                0 16735 i
*> 200.229.0.0/20   200.215.186.10                0 15180 16712 16712 16712 i
*> 200.229.16.0/20  200.215.186.9                 0 13591 16736 i
*> 200.229.16.0/22  200.215.186.9                 0 13591 16736 i
*> 200.229.20.0/22  200.215.186.9                 0 13591 16736 i
*> 200.229.24.0/22  200.215.186.9                 0 13591 16736 i
*> 200.233.128.0/18 200.215.186.15                0 16735 i
*> 207.83.96.0/20   200.215.186.9                 0 13591 3300 i
*> 209.58.74.0      200.215.186.7                 0 13878 i
*> 209.58.125.0     200.215.186.7                 0 13878 i
*> 216.72.229.0     200.215.186.7                 0 13878 i
```

ANEXOS

ANEXO A- Participantes do PTT da FAPESP

[AGESTADO - 14346] Agência Estado

[AJATO - 19182] Rede Ajato Ltda.

[ANSP - 1251] FAPESP - Projeto Rede ANSP

[ATTLA - 13353] AT&T do Brasil S.A.

[BRASILTELECOM - 8167] Telegoiás Brasil Telecom.

[COMDOMINIO - 16397] ComDomínio Ltda.

[COMPUGRAF - 16594] Compugraf Servicos Ltda.

[COMSAT - 11271] COMSAT Brasil Ltda.

[CTBC - 16735] Cia. de Telecomunicações do Brasil Central

[DIALDATA - 14026] Via Networks (Dialdata)

[DIVEO - 15180] Diveo do Brasil Telecomunicações Ltda.

[DURAND - 22356] Durand do Brasil Ltda.

[GBLX - 3549] Global Crossing

[GENUITY - 279] Genuity do Brasil Ltda.

[GLOBALONE - 6505] GlobalOne Comunicações Ltda.

[GRECO - 27682] Greco Internet

[GVT - 18881] Global Village Telecom Ltda.

[IFX - 11432] IFX do Brasil Ltda.

[IMPSAT - 11415] IMPSAT Comunicações Ltda.

[KDD - 10362] KDD Nethall Ltda.

[METRORED - 13591] Metrored Telecomunicações Ltda.

[NTT - 13495] NTT do Brasil Telecomunicações Ltda.

[REGISTROBR - 22548] Entidade Administrativa Registro.br

[RNP - 1916] Rede Nacional de Pesquisa

[TELEFONICA - 10429] Telefonica S.A.

[TELEMAR - 7738] TeleNorteLeste Participações S.A.

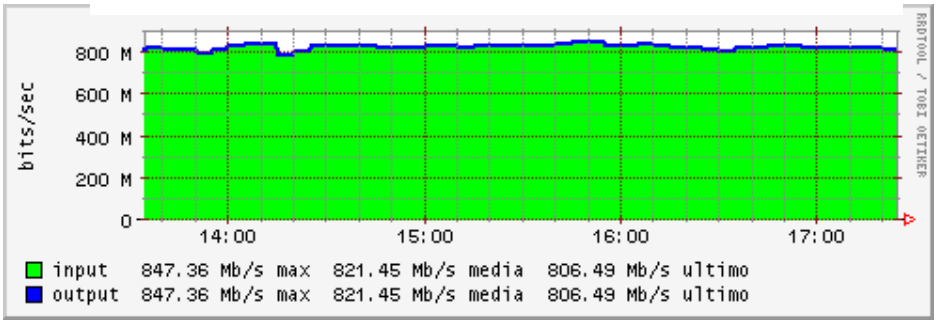
[UNISYS - 5772] Unisys Brasil

[UOL - 15201] Universo OnLine

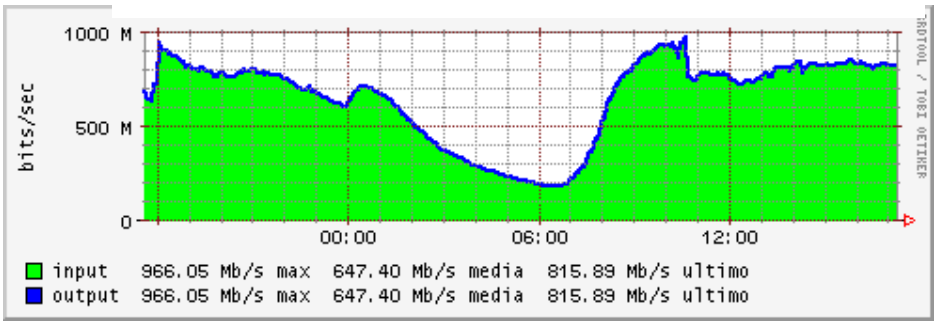
[VESPER - 20266] Vésper

ANEXO B- Exemplo de tráfego trocado no PTT da FAPESP

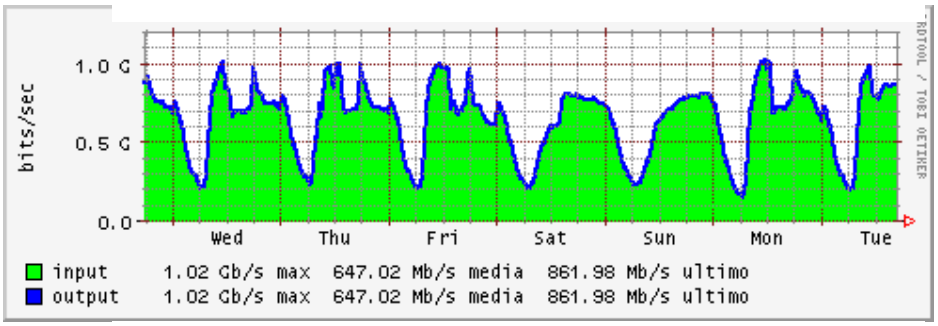
Últimas quatro horas (média de cinco minutos



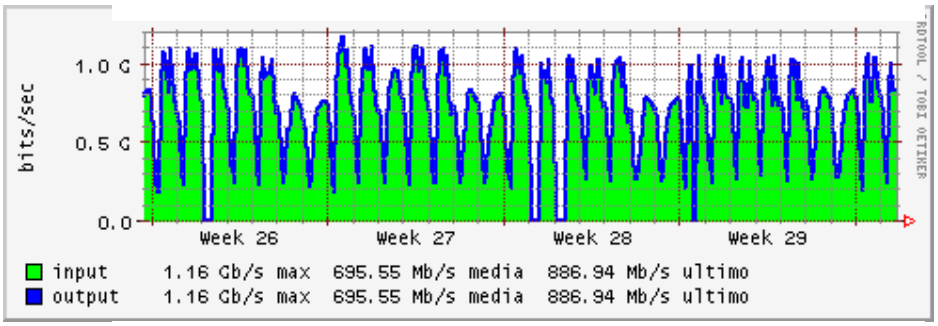
Último dia (média de cinco minutos)



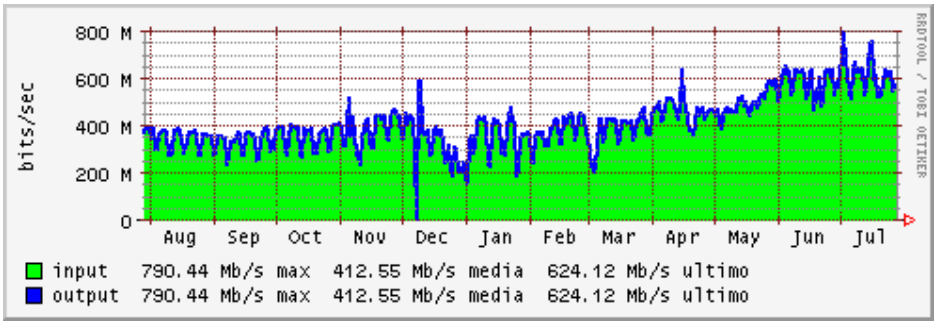
Última semana (média de 30 minutos)



Último mês (média de duas horas)



Último ano (média de um dia)


800 M
600 M
400 M
200 M
0
bits/sec
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
input 790.44 Mb/s max 412.55 Mb/s media 624.12 Mb/s ultimo
output 790.44 Mb/s max 412.55 Mb/s media 624.12 Mb/s ultimo

ANEXO C–Tabela CIDR, máscara binária

CIDR prefix length	Dotted Decimal Netmask	Hexidecimal Netmask	Inverse Netmask	Binary	Number of Classfull Networks	Number of Usable IPs
/1	128.0.0.0	80 00 00 00	127.255.255.255	1000 0000 0000 0000 0000 0000 0000 0000	128 As	2,147,483,646
/2	192.0.0.0	C0 00 00 00	63.255.255.255	1100 0000 0000 0000 0000 0000 0000 0000	64 As	1,073,741,822
/3	224.0.0.0	E0 00 00 00	31.255.255.255	1110 0000 0000 0000 0000 0000 0000 0000	32 As	536,870,910
/4	240.0.0.0	F0 00 00 00	15.255.255.255	1111 0000 0000 0000 0000 0000 0000 0000	16 As	268,435,454
/5	248.0.0.0	F8 00 00 00	7.255.255.255	1111 1000 0000 0000 0000 0000 0000 0000	8 As	134,217,726
/6	252.0.0.0	FC 00 00 00	3.255.255.255	1111 1100 0000 0000 0000 0000 0000 0000	4 As	67,108,862
/7	254.0.0.0	FE 00 00 00	1.255.255.255	1111 1110 0000 0000 0000 0000 0000 0000	2 As	33,554,430
/8	255.0.0.0	FF 00 00 00	0.255.255.255	1111 1111 0000 0000 0000 0000 0000 0000	1 A or 256 Bs	16,777,214
/9	255.128.0.0	FF 80 00 00	0.127.255.255	1111 1111 1000 0000 0000 0000 0000 0000	128 Bs	8,388,606
/10	255.192.0.0	FF C0 00 00	0.63.255.255	1111 1111 1100 0000 0000 0000 0000 0000	64 Bs	4,194,302
/11	255.224.0.0	FF E0 00 00	0.31.255.255	1111 1111 1110 0000 0000 0000 0000 0000	32 Bs	2,097,150
/12	255.240.0.0	FF F0 00 00	0.15.255.255	1111 1111 1111 0000 0000 0000 0000 0000	16 Bs	1,048,574
/13	255.248.0.0	FF F8 00 00	0.7.255.255	1111 1111 1111 1000 0000 0000 0000 0000	8 Bs	524,286
/14	255.252.0.0	FF FC 00 00	0.3.255.255	1111 1111 1111 1100 0000 0000 0000 0000	4 Bs	262,142
/15	255.254.0.0	FF FE 00 00	0.1.255.255	1111 1111 1111 1110 0000 0000 0000 0000	2 Bs	131,070
/16	255.255.0.0	FF FF 00 00	0.0.255.255	1111 1111 1111 1111 0000 0000 0000 0000	1 B or 256 Cs	65,534
/17	255.255.128.0	FF FF 80 00	0.0.127.255	1111 1111 1111 1111 1000 0000 0000 0000	128 Cs	32,766
/18	255.255.192.0	FF FF C0 00	0.0.63.255	1111 1111 1111 1111 1100 0000 0000 0000	64 Cs	16,382
/19	255.255.224.0	FF FF E0 00	0.0.31.255	1111 1111 1111 1111 1110 0000 0000 0000	32 Cs	8,190
/20	255.255.240.0	FF FF F0 00	0.0.15.255	1111 1111 1111 1111 1111 0000 0000 0000	16 Cs	4,094
/21	255.255.248.0	FF FF F8 00	0.0.7.255	1111 1111 1111 1111 1111 1000 0000 0000	8 Cs	2,046
/22	255.255.252.0	FF FF FC 00	0.0.3.255	1111 1111 1111 1111 1111 1100 0000 0000	4 Cs	1,022
/23	255.255.254.0	FF FF FE 00	0.0.1.255	1111 1111 1111 1111 1111 1110 0000 0000	2 Cs	510
/24	255.255.255.0	FF FF FF 00	0.0.0.255	1111 1111 1111 1111 1111 1111 0000 0000	1 C	254
/25	255.255.255.128	FF FF FF 80	0.0.0.127	1111 1111 1111 1111 1111 1111 1000 0000	1/2 C	126
/26	255.255.255.192	FF FF FF C0	0.0.0.63	1111 1111 1111 1111 1111 1111 1100 0000	1/4 C	62
/27	255.255.255.224	FF FF FF E0	0.0.0.31	1111 1111 1111 1111 1111 1111 1110 0000	1/8 C	30
/28	255.255.255.240	FF FF FF F0	0.0.0.15	1111 1111 1111 1111 1111 1111 1111 0000	1/16 C	14
/29	255.255.255.248	FF FF FF F8	0.0.0.7	1111 1111 1111 1111 1111 1111 1111 1000	1/32 C	6
/30	255.255.255.252	FF FF FF FC	0.0.0.3	1111 1111 1111 1111 1111 1111 1111 1100	1/64 C	2
/31	255.255.255.254	FF FF FF FE	0.0.0.1	1111 1111 1111 1111 1111 1111 1111 1110	1/128 C	0