Testes diagnósticos problemas de conectividade.

Intuito desse documento é auxiliar nos diagnósticos de problemas relacionados a conectividade IP.

- Os testes devem ser realizados de uma estação cabeada.
- Verificar se não existem aplicativos consumindo toda banda disponível
- Verificar conectividade até a borda onde encontrasse o Link da operadora.

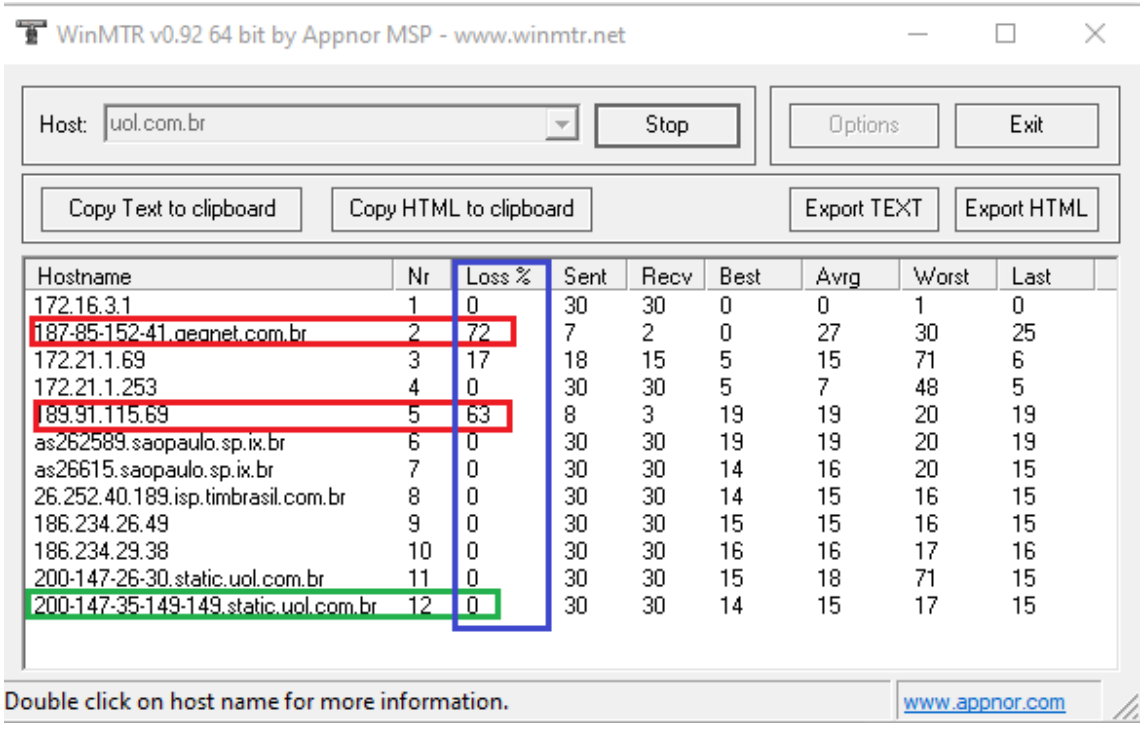
Primeiro passo nos diagnósticos é utilizar a ferramenta MTR nessa vai testar todos os saltos até os destinos o proposito dessa ferramenta é identificar onde se inicia o LOSS de pacotes.

Link de Download: https://winmtr.br.uptodown.com/windows/download

A Ferramenta é autoexecutável, existe também para Linux, chamada de somente MTR.

Uma observação muito importante: roteadores de transito normalmente tem filtro de ICMP na control-plane tanto Cisco,Huwei e Juniper tem aplicam esses filtros, pois todo pacote ICMP precisa subir para CPU para ser processado.

Então precisamos nos atentar, observe o seguinte cenário:



O que podemos observar que 2 nós estão com LOSS porem o destino não, isso é característica de filtro ICMP na control-plane nos elementos de rede.

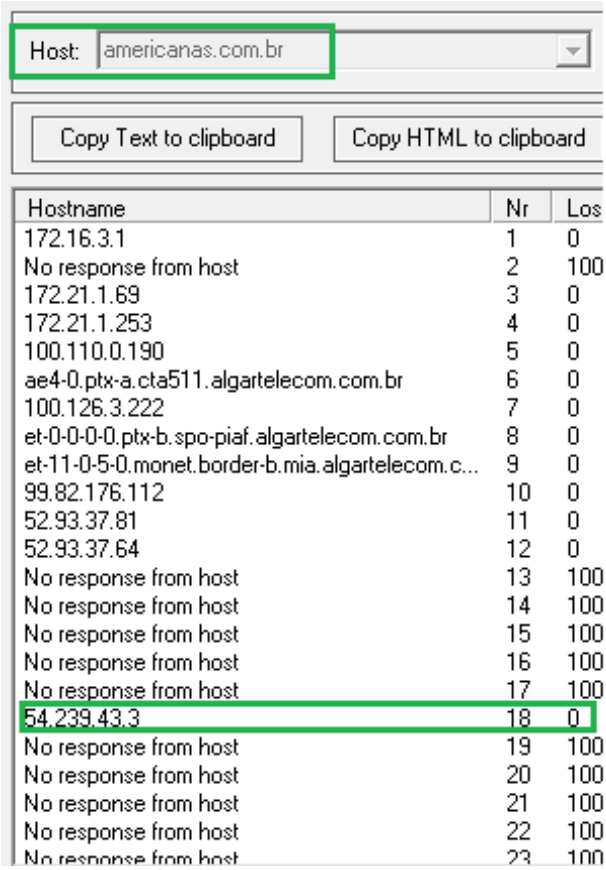
Testes onde existem filtro de ICMP.

Alguns servidores de conteúdo ou aplicações tem filtro ICMP com isso impossibilita os testes de ICMP de serem realizados fim a fim.
Nesse caso devemos prosseguir da seguinte forma:

- Realizar o MTR e observar qual o último salto que responde ICMP.

Realizar uma consulto no whois, observar se o ultimo IP com resposta pertente ao mesmo ASN de destino.

Exemplo:



Hostname	Nr	Los
172.16.3.1	1	0
No response from host	2	100
172.21.1.69	3	0
172.21.1.253	4	0
100.110.0.190	5	0
ae4-0.ptx-a.cta511.algartelecom.com.br	6	0
100.126.3.222	7	0
et-0-0-0-0.ptx-b.spo-piaf.algartelecom.com.br	8	0
et-11-0-5-0.monet.border-b.mia.algartelecom.c...	9	0
99.82.176.112	10	0
52.93.37.81	11	0
52.93.37.64	12	0
No response from host	13	100
No response from host	14	100
No response from host	15	100
No response from host	16	100
No response from host	17	100
54.239.43.3	18	0
No response from host	19	100
No response from host	20	100
No response from host	21	100
No response from host	22	100
No response from host	23	100

ping americanas.com.br
Disparando americanas.com.br [34.226.172.51] com 32 bytes de dados:

Whois utilizado: http://lacnic.net/cgi-bin/lacnic/whois?lg=EN
Whois do registro.br só consulta ASN do Brasil!

34.226.172.51 -> Consultando no whois pertence a Amazon

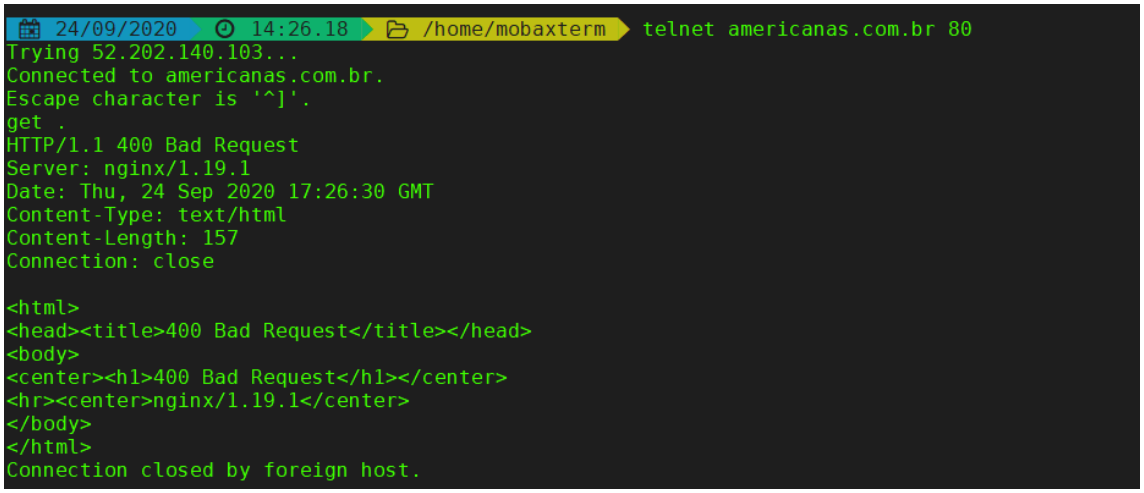
54.239.43.3 -> Consultando também pertence a Amazon.

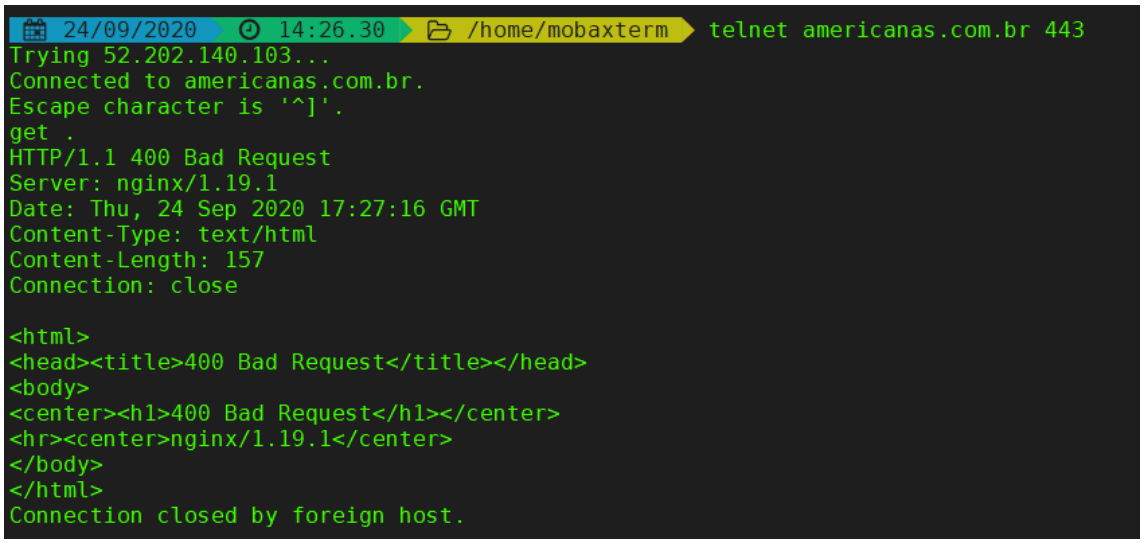
Com isso podemos constatar que até algum elemento de rede da Amazon está com a conectividade OK, possivelmente se existem algum problema é na aplicação do site ou na própria Amazon.

Verificação de aplicação quando o ICMP é filtrado:

Vamos pegar esse exemplo da americanas.com.br

Nesse caso o ICMP é bloqueado, primeiro teste é verificar a porta 80 e 443 isso pode ter testado com um simples telnet:





Nesse caso podemos observar que tanto a porta 80 como 443 estão respondendo caso o site não para podemos certificar que o problema não é rede e sim a aplicação.

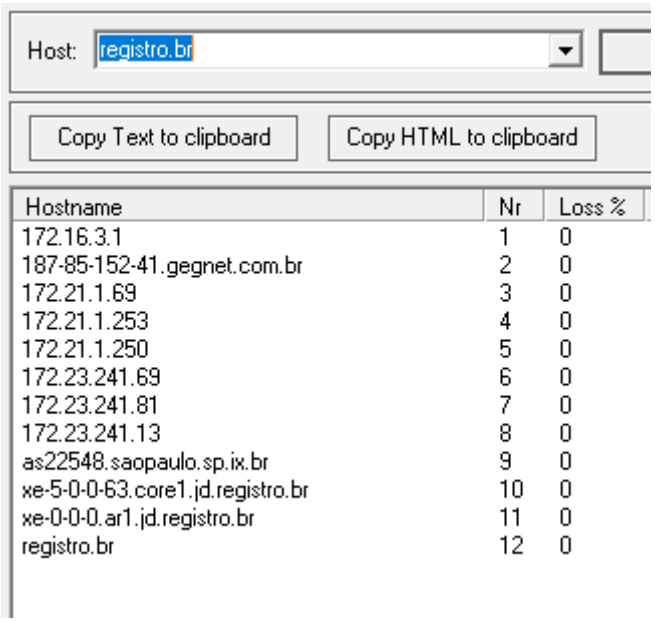
Outras portas podem ser descobertas com o software NMAP:
https://nmap.org/

Deve ser observado que caso host em questão tenha alguma porta com resposta significa que o problema é em aplicações especificas e não em conectividade IP.

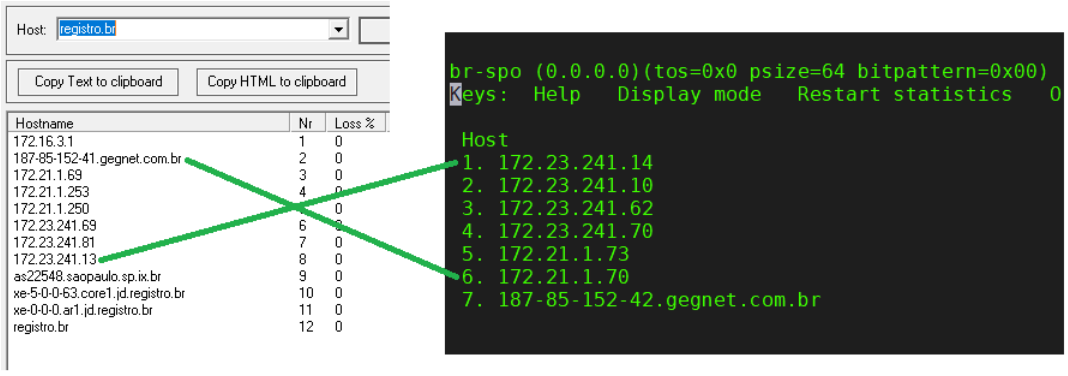
Assimetria:

Assimetria ocorre quando o caminho de requisição (Upload) é realizado por um caminho e o retorno é realizado por outro, os testes que realizamos estão sempre vendo o UPLOAD do caminho, não quer dizer que a volta seja pelo mesmo caminho. Em si a internet é assimétrica, mas devemos nos atendar isso na hora de identificar um problema.

Exemplo:



Nosso UPLOAD está indo via IX para desse destino, para testar o DOWLONAD é necessário um MTR ao contrário, ou seja, da origem para o destino, outra maneira é observar em um Looking Glass (LG) o anúncio.

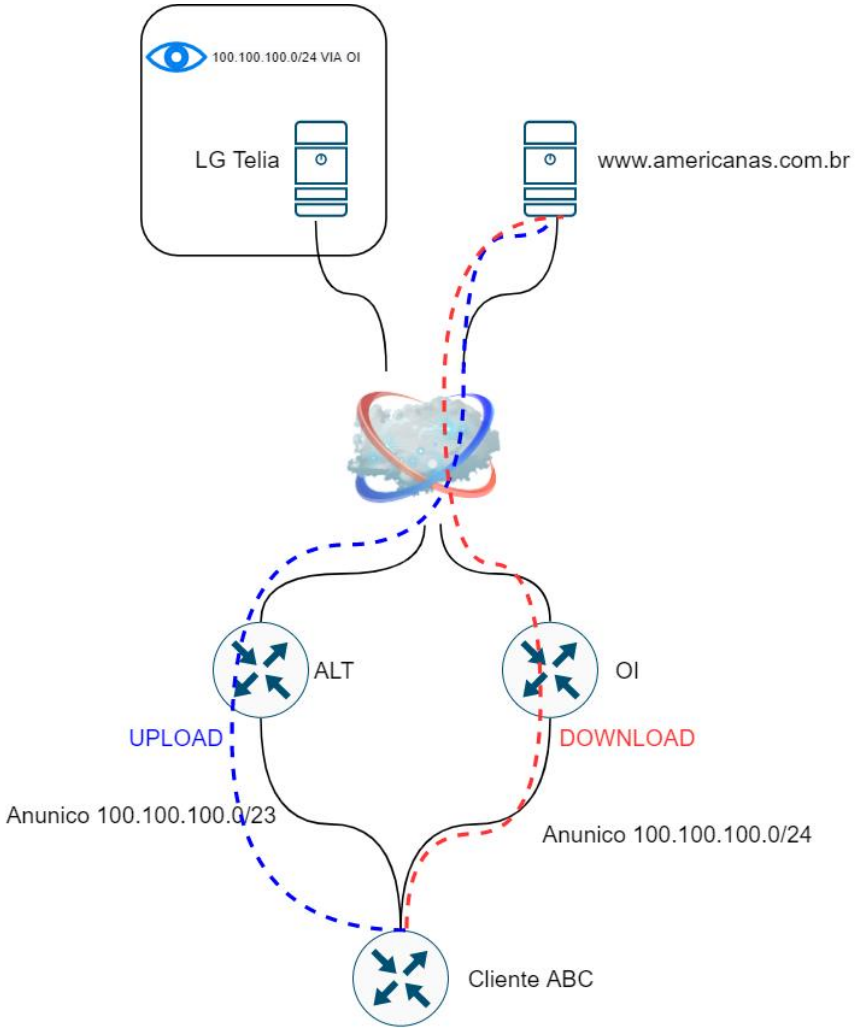


Nesse caso podemos observar um MTR ao contrario onde vemos que o trafego foi entregue pelo menos equipamento que está se conectando no IX-SPO, caso não for possível acesso a um MTR reverso é possível observar no próprio site do reistro.br onde possui uma ferramenta de traceroute (https://registro.br/tecnologia/ferramentas/traceroute/)

Outros cenários onde não sejam conexão no IX podem ser testamos pelos LG para observar como é o retorno, assimetria não é um problema no geral, mas deve ser garantia do que o UPLOAD e DOWNLOAD estejam por nosso operadora para prosseguir com os testes de uma possível falha.
Exemplo: provedor possui Link IP com a ALT e a operadora OI

Foi observado via MTR que o UPLOAD para o destino www.meuip.com.br está via operadora ALT porem foi obervado no LG que ele aprende os prefixo IP da provedor OI, com isso sabemos que o retorno vai ser via OI, o Ideal é sempre verificar no LG da operadora que possui Link se a mesma possuir, segue LG do nosso ASN:
http://lg.as53062.net.br/lg

Podemos ver o LG como um roteador que tem o ponde de vista do seu BGP local, então sempre precisamos nos assegurar que tanto o UPLOAD como o DOWNLOAD estão pela mesma operadora.



Engenharia de trafego com BGP:

Nesse primeiro exemplo temos múltiplas operadas e desejamos realizar uma manipulação do Download. Nesse caso temos algumas formas para manipular a seleção de rotas no BGP.

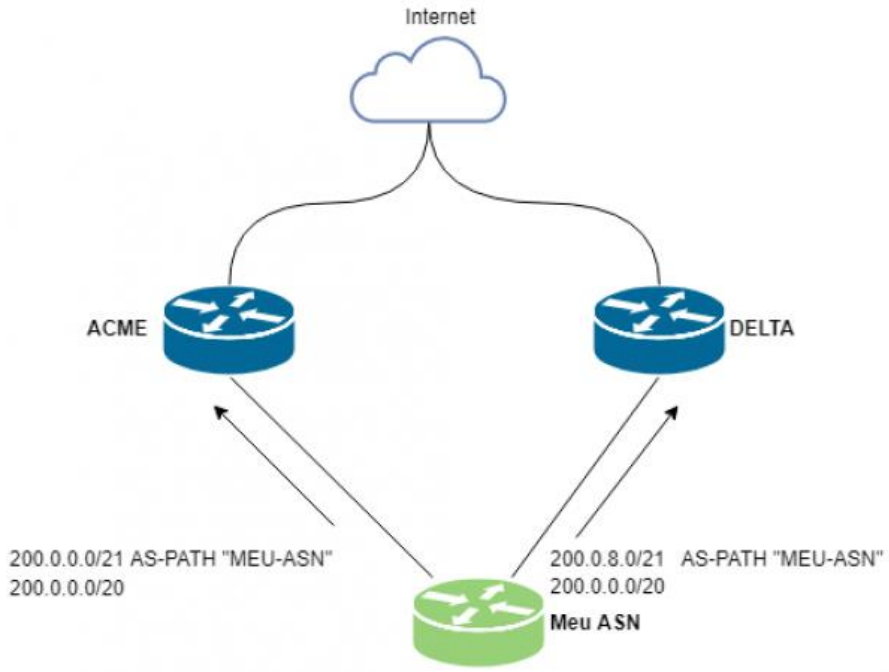
Temos três principais métodos de escolha para manipular o Download que podemos utilizar:

- Menor tamanho de prefixo.
- Menor tamanho de AS_PATH.
- Uso de communities.

O método mais simples dele consistem em divulgar o prefixo mais específico, vamos supor que nosso ASN (**1234**) e possui o prefixo **200.0.0.0/20**

Podemos fazer uma engenharia de tráfego que consiste em dividir o prefixo /20 em dois /21 porem caso uma operadora pare de funcionar, gostaríamos que todo o tráfego comute para a outra operadora.

Uma forma simples de fazer isso seria divulgando um /21 para cada operadora e o /20 para a duas, lembre-se que o prefixo mais específico é primeiro método de escolha na seleção de rotas, então uma rota mais especifica nunca iria para os outros critérios de desempate do BGP. Para esse cenário ser valido teremos que ter pelo menos uma rota default para cada uma das operadoras ou full routing com ambas.



No que condiz as rotas de saída o BGP utiliza esse critério para desempate:

Rota mais específica.

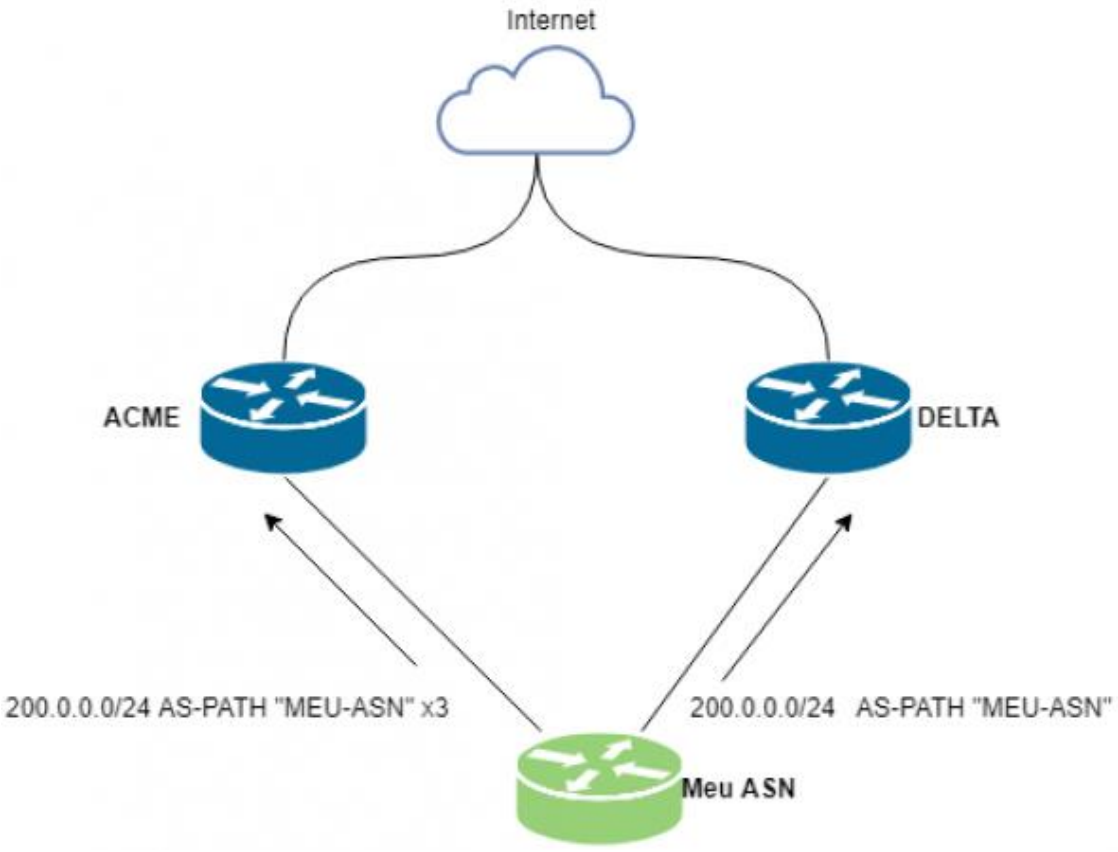
- Menor Weight.
- Maior Local-Preference.
- Menor AS-PATH
- Rota mais antiga

Link com politicas e comuinity do nosso ASN:
http://bgp.as53062.net.br/policy

Na maioria dos casos onde não temos nenhum tipo de alteração nos prefixos recebidos e recebemos full routing o critério que escolhe qual prefixo vai ser instalado é AS-PATH, pois sem nenhuma alteração nos dois primeiros critérios vamos ter uma diferença de AS-PATH, caso tenhamos um empate, a rota que estiver mais tempo instala na tabela BGP será o critério de desempate.

Algumas observações do uso de prepend.

Imagine que seja divulgado o mesmo prefixo para duas operadoras como abaixo:



Porem para a Operadora ACME foi divulgado o prefixo com prepend, mas nosso objetivo não foi atingido, o tráfego continua vindo via operadora ACME.

O que ocorre que geralmente quando divulgamos o mesmo prefixo para ambas as operadoras, mesmo que com o uso do artificio de prepend, as operadoras vão sempre preferir rotas que ela recebe de seus clientes. Imagine agora que a operadora ACME é DOWNSTREAM (CLIENTE) da operadora DELTA, mesmo divulgando o prefixo com prepend para a operadora DELTA, o tráfego vai preferir vir via essa conexão direta do cliente ao invés “atravessar” um outro ASN para chegar no meu prefixo.