



Núcleo de Informação  
e Coordenação do  
Ponto BR

Comitê Gestor da  
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

# Ferramentas essenciais para administradores de redes

Tiago Jun Nakamura

IX Fórum Regional Campo Grande

ceptron.br nic.br egi.br

# Motivação

- A área de redes é uma área
  - Complexa
  - Desafiadora
  - Crítica
- Decisões precisam ser tomadas
  - De maneira rápida
  - Com inteligência



# Motivação

- Mas nem todo super herói usa capa!!



SUporte

DEVIDO A UMA MANUTENÇÃO, IREMOS FICAR ALGUMAS HORAS SEM INTERNET.

TUDO BEM.

MAS O E-MAIL VAI FUNCIONAR NORMALMENTE, NE?

NAO. O E-MAIL TAMBÉM NÃO VAI FUNCIONAR.

QUER DIZER QUE VOU FICAR AQUI TODO ESSE TEMPO SEM PODER TRABALHAR?

EXATAMENTE. PROCURE FAZER ALGO PRA SE DISTRAIR.

PODE SER NO YOUTUBE?

# Motivação

- Cenários problemáticos
  - Não consigo acessar determinado site
  - Muitos clientes estão sem acesso
  - Alguns clientes estão com a Internet lenta
- Cenários gerenciais
  - Devo expandir a minha rede?
  - Devo procurar mais parceiros de peering?
  - Devo criar um serviço novo?



# Motivação

- Ferramentas
  - Nos trazem informação
  - Nos ajudam na **tomada de decisão**
  - Resolvem alguns problemas simples
  - Ajudam a prever alguns cenários
- Mas elas não fazem tudo sozinhas!



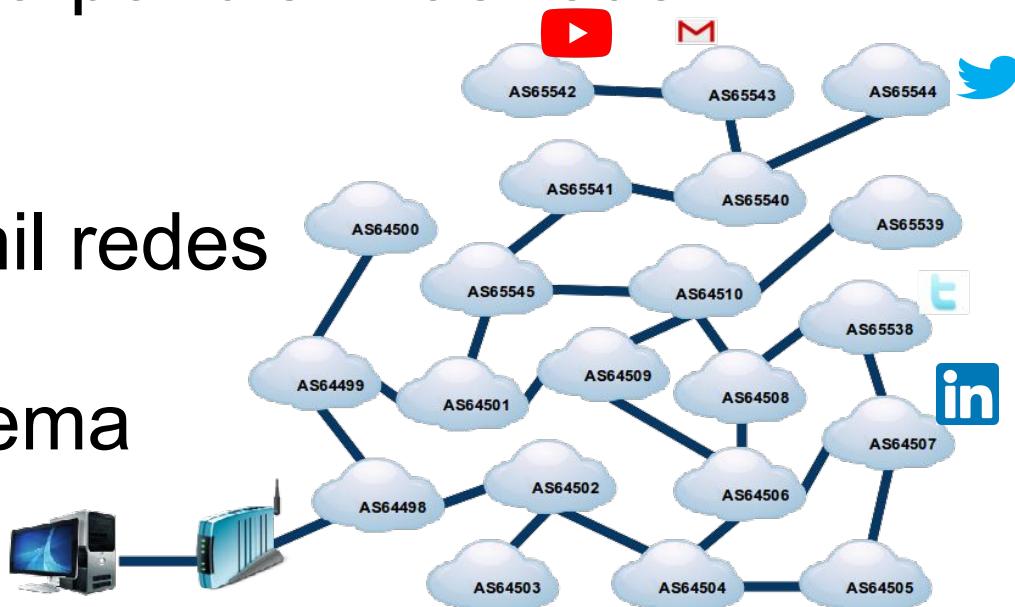
# *Ferramentas: Comandos Básicos*



# Conceito

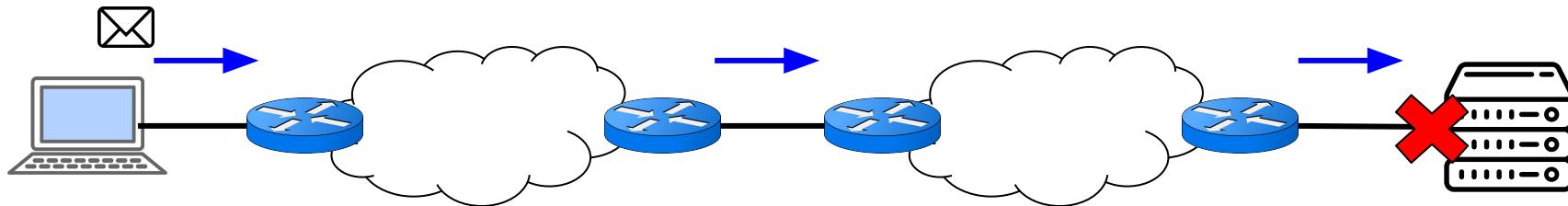
- A Internet é formada por distintas redes interconectadas
  - São mais de 100 mil redes
  - Chamadas de Sistema Autônomo

The diagram illustrates the Internet's architecture as a complex network of Autonomous Systems (ASes). It features several light blue cloud icons, each representing an AS and labeled with a unique identifier: AS65542, AS65541, AS64500, AS65545, AS64499, AS64501, AS64509, AS64498, AS64502, and AS64497. These clouds are interconnected by a dense web of dark blue lines, symbolizing the peering and transit relationships between different ASes. In the bottom left corner, there is a small icon of a computer monitor and a router, further emphasizing the network infrastructure.



# Problema

- Determinada máquina não consegue se comunicar com outra?



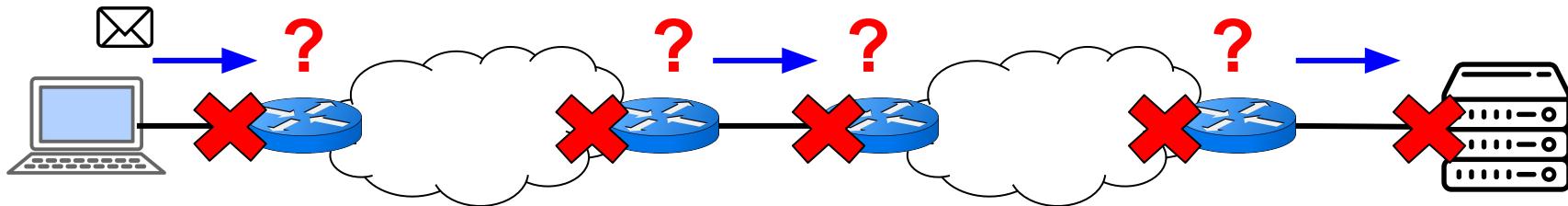
# Comando Ping

- Mensagem tipo ICMP ou ICMPv6
  - Echo Request e Echo Reply
  - Cuidado: Muitos bloqueiam!
- Serve para
  - Fazer um teste de conectividade simples.
- Onde usar
  - Da sua máquina
  - De um Looking Glass



# Problema

- Determinada máquina não consegue se comunicar com outra?



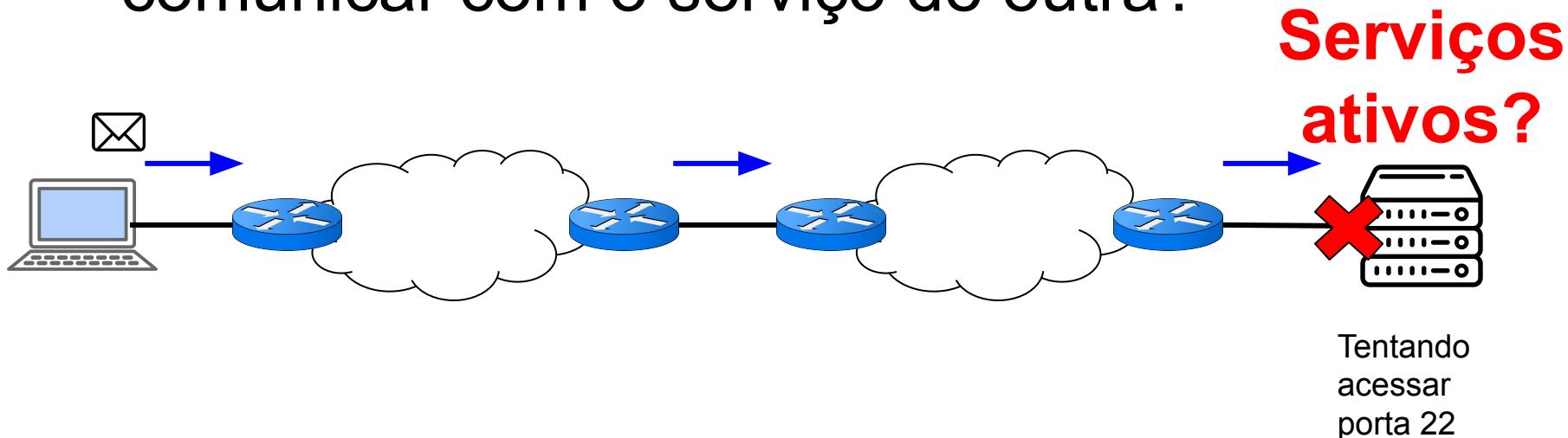
# Comando Traceroute

- Implementação mais comum
  - Usa o comando PING
  - Variando o TTL
- Serve para
  - Contar os saltos de um caminho
  - Identificar onde o problema está
- Onde usar
  - Da sua máquina
  - De um Looking Glass



# Problema

- Determinada máquina não consegue se comunicar com o serviço de outra?



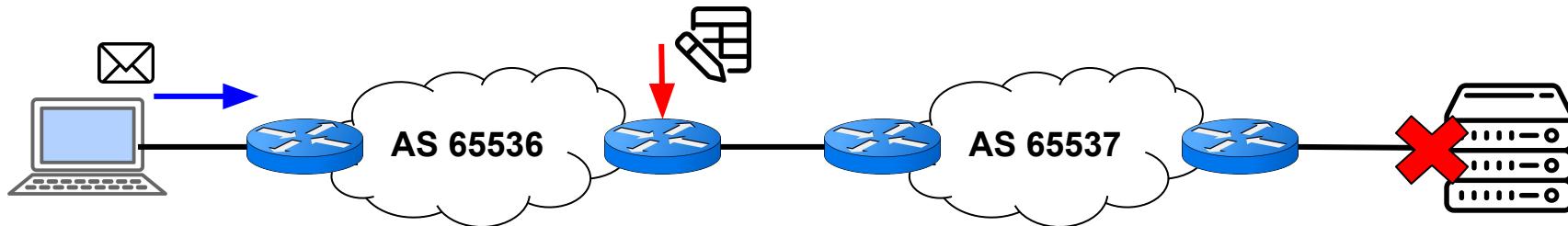
# Comando Nmap

- Implementação mais comum
  - Vários protocolos
- Serve para
  - Escanear endereços IPs e portas numa rede
  - Detectar programas instalados e que estão funcionando no momento
- Onde usar
  - Da sua máquina
- Zenmap - interface gráfica



# Problema

- Sem Conectividade?
  - Pode ser um problema de rota!
- O meu roteador aprendeu a rota no BGP?
- Olhar o Full Routing!!!



# Regex

- Também chamada de Expressão Regular
- A primeira vista assusta:

```
(([0-9a-fA-F]{1,4}(:)){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}(:){1,7}:[0-9a-fA-F]{1,4}(:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}(:){1,5}:[0-9a-fA-F]{1,4}(:){1,2}|([0-9a-fA-F]{1,4}(:){1,4}(:[0-9a-fA-F]{1,4}(:){1,3}|([0-9a-fA-F]{1,4}(:){1,3}(:[0-9a-fA-F]{1,4}(:){1,4}|([0-9a-fA-F]{1,4}(:){1,2}(:[0-9a-fA-F]{1,4}(:){1,5}|[0-9a-fA-F]{1,4}(:((:[0-9a-fA-F]{1,4}(:){1,6})|(:([0-9a-fA-F]{1,4}(:){1,7}|:)))
```



# Regex



# Regex

- Caracteres especiais
  - . - significa qualquer carácter uma vez só
  - [] - significa qualquer carácter listado dentro uma vez só
    - [0-9] - um dígito só
    - [a-z] - uma letra minúscula só
    - [A-Z] - uma letra maiúscula só
  - [^] - significa negação de qualquer carácter listado
    - [^0-9] - não pode ser dígito



# Regex

- Caracteres especiais
  - `_` - identifica espaço
  - `|` - define um ou outro
  - `()` - agrupa parte da regex, divide em escopos
    - `(IPv4) | (IPv6)` - procura a palavra IPv4 ou IPv6
- Marcadores de posição
  - `^` - marca o começo da linha
  - `$` - marca o fim de linha



# Regex

- Quantificadores
  - **?** - o que anteceder pode aparecer 0 ou 1 vez
    - A? - vazio ou A
  - **\*** - o que anteceder pode aparecer 0 ou mais vezes
    - A\* - vazio ou A ou AA ou AAA ou AAAA ...
  - **+** - o que anteceder pode aparecer 1 ou mais vezes
    - A+ - A ou AA ou AAA ou AAAA ...
  - **{}** - o que anteceder é repetido a quantidade de vezes que estiver dentro
    - A{4} - AAAA : A{1,3} - A, AA, AAA



# Regex Prontas para BGP

- Comandos de visualização
  - Ex: sh ip bgp regexp ...
- Basta só mudar o seu ASN - exemplo: AS 22548
  - **^\$** - Busca rotas criadas localmente (sem nada no AS Path) - **no meu roteador**
  - **\_22548\_** - Busca todas as rotas que foram originadas no nosso AS e as que passaram por nós. - **no looking glass**
  - **\_22548\$** - Busca rotas originadas pelo nosso AS - **no looking glass**



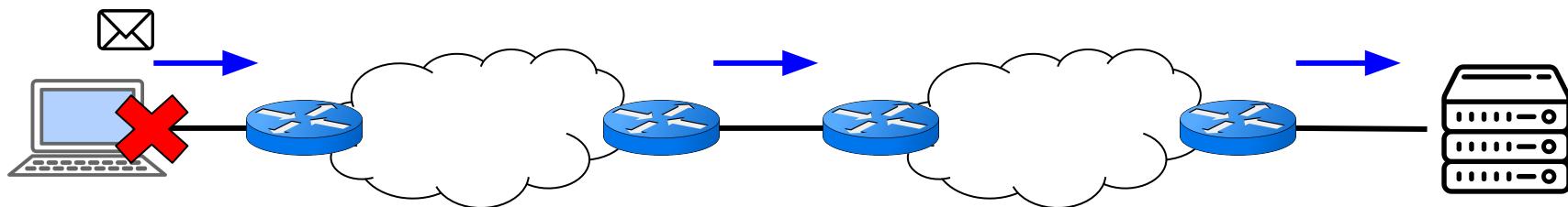
# Regex Prontas para BGP

- Basta só mudar o seu ASN - exemplo: AS 22548
  - **\_22548\_([0-9]+)\$** - Busca rotas dos clientes em que o nosso AS é trânsito direto. - **no looking glass**
    - Se o cliente tiver prepend não vai funcionar
      - **\_22548\_** nesse caso serve apesar de aparecer mais informações
- Regex também podem ajudar nas configurações!
  - Diminui a quantidade de linhas



# Problema

- Um cliente meu não consegue acessar os meus serviços?
  - Como posso enxergar o ponto de vista dele?



# Looking Glass Públicos

- Roteador em outro AS/IX com comandos limitados
  - Ping
  - Traceroute
  - BGP (visualização e às vezes REGEX)
- Conexão
  - Linha comando
  - Interface gráfica



# Hurricane Electric BGP Toolkit

- Aplicação web da Hurricane Electric
- Usa dados do BGP da HE, Routeviews e outras fontes
- Grafos de conectividade de ASes
- Gráficos de anúncios de prefixos
- Informações dos ASNs
- Peers conectados
- E outras coisas mais



HURRICANE ELECTRIC  
INTERNET SERVICES



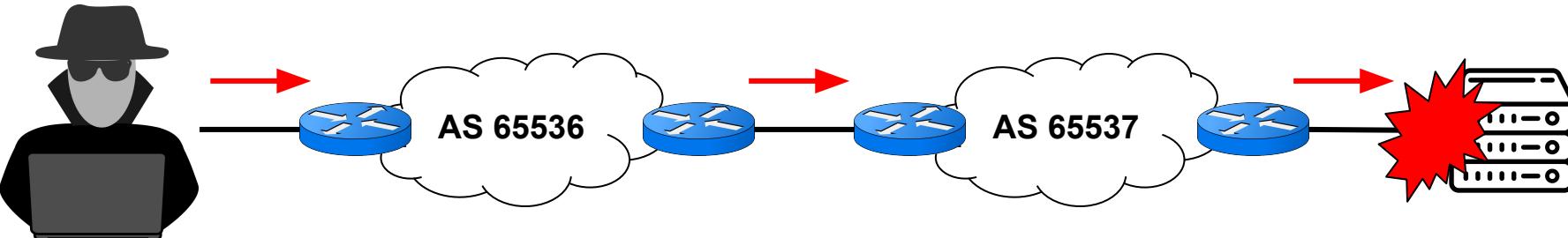
# Looking Glasses públicos

- Lista de Looking Glasses públicos
  - [https://wiki.brasilpeeringforum.org/w/Looking\\_Glass](https://wiki.brasilpeeringforum.org/w/Looking_Glass)
- Looking Glass IX.br
  - <https://lg.ix.br>



# Problema

- Estou recebendo um ataque de outra máquina?
- Seria bom investigar o responsável pelo IP do pacote que está atacando.



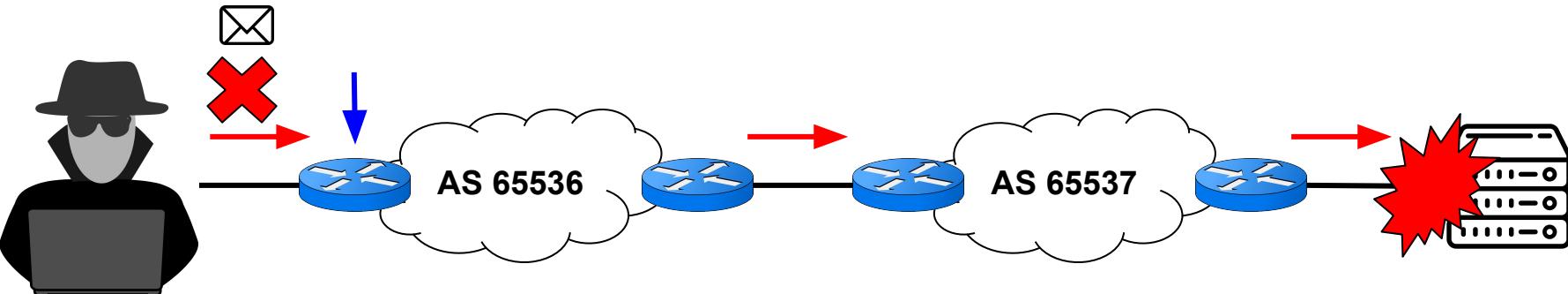
# WhoIS

- Banco de dados
  - Domínios
  - IP
  - ASN
  - Outras Informações
- Servidores espalhados pelo mundo
  - Às vezes precisa procurar em mais de um lugar



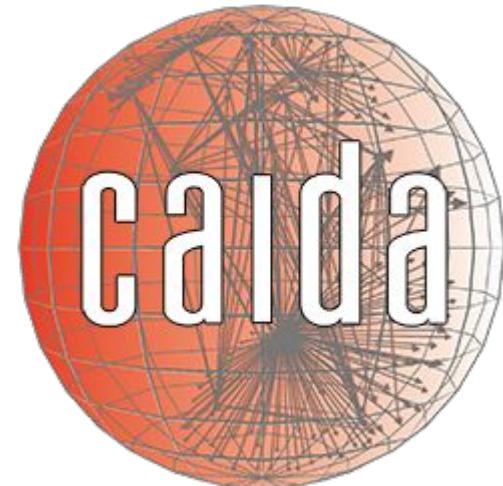
# Problema

- Será que dá minha rede pode sair pacotes com endereços spoofados?
- Os meus filtros estão funcionando



# Center for Applied Internet Data Analysis (CAIDA) Spoofer

- Software opensource
- Realiza testes se um pacote spoofado pode sair da sua rede
- Gera relatório
- Se os pacotes passarem
  - Precisa aplicar técnicas de antispoofing

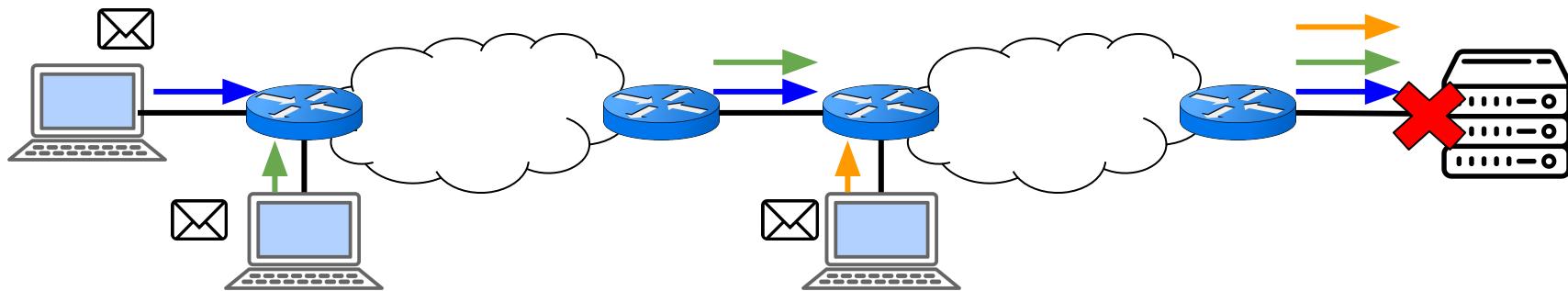


# *Ferramentas: Sites Importantes*



# Problema

- Uma determinada máquina não consegue se comunicar com outra?
- É um problema só meu ou de outros usuários na Internet?



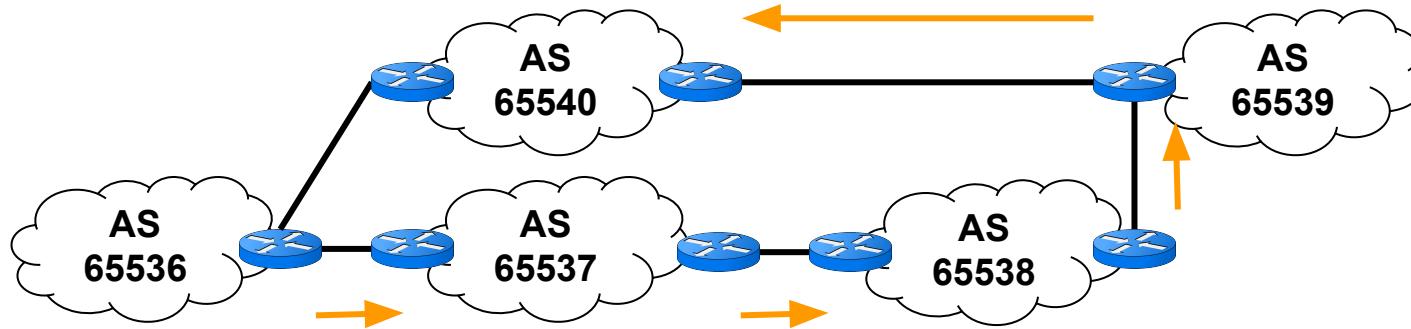
# Detecção de Problema em Terceiros

- Downdetector
  - Pode se identificar o serviço que está com problema
  - <https://downdetector.com.br/>
- Down for Everyone or Just Me
  - Pode se verificar se o site está funcionando ou não
  - <https://downforeveryoneorjustme.com/>



# Problema

- Internet ficou lenta?
  - A sua rota pode ter vazado por um caminho maior!



O AS 65537 era um peer mas virou trânsito, mudando o caminho de comunicação para o AS 65540

# BGPmon

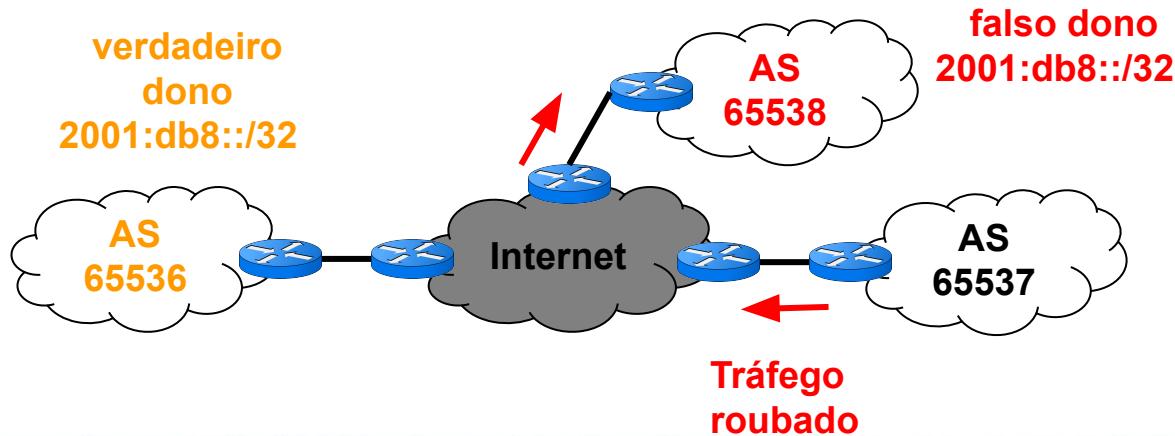
- Ferramenta da CISCO
- Monitora os prefixos que você listar
  - Parte gratuito - 5 prefixos
- Identifica e alerta
  - Roubo de prefixo
  - Instabilidade nas rede
  - Vazamento de rotas

BGPMon is Now Part of  
**Crosswork**Cloud



# Problema

- Teve muitos chamados e você não sabe o que aconteceu?
  - Passou um tempo e tudo voltou ao normal



Você desconfia que  
roubaram o seu  
prefixo. Mas tudo já  
se arrumou!

# BGPlay

- Aplicação Javascript WEB
- Usa o Route Views
- Apresentação gráfica do que aconteceu no roteamento ao longo do tempo
  - Intervalo de tempo
  - IPs/ Prefixo
  - Sistemas Autônomos



# Problema

- Existe algum lugar em que posso encontrar muitas informações de forma condensada?
  - Dados do ASN
  - Quem alocou os dados
  - Atividades no BGP
  - Se tem informações em lista de bloqueio
  - Outras coisas mais



# RIPEstat

- Plataforma do RIPE NCC
- Coleção de vários bancos de dados
- Pode se buscar num intervalo de tempo
- Busca
  - IP/Prefixo
  - ASN
  - Código de país
  - Hostname



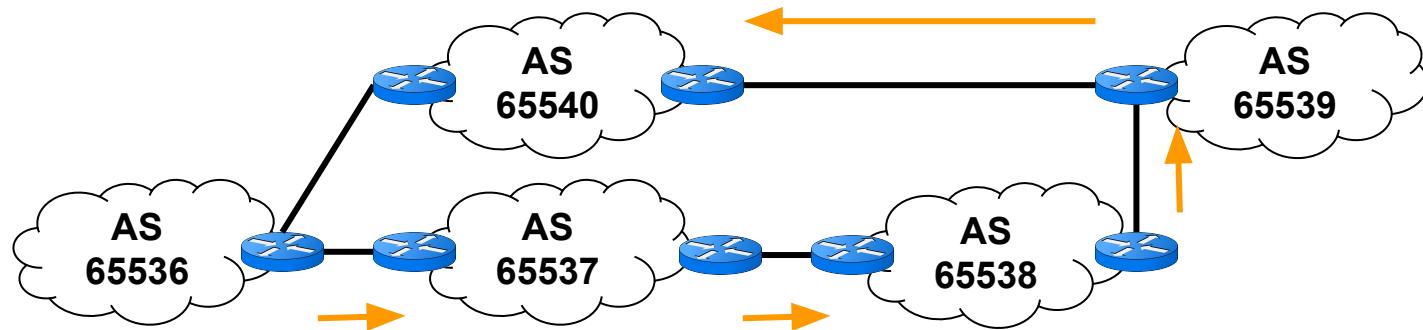
# BGP.Tools

- Coleção de vários bancos de dados
- Busca
  - IP/Prefixo
  - ASN
  - DNS
  - Looking Glass



# Problema

- Aconteceu algo com as minhas rotas?
- Tem como eu monitorar constantemente?



# BGP Alerter

- Software opensource que monitora os seus anúncios BGP na Internet e gera alertas quando ocorrem modificações
- Monitora também o RPKI
  - Se tem problema nos Trust Anchors
  - Se tem problema nos ROAs
    - Expirou, deletado, editado ou adicionado



# Link das ferramentas mostradas

- Whois - <https://registro.br/tecnologia/ferramentas/whois/>
- IX - <https://ix.br/>
- MANRS - <https://www.manrs.org/>
- INOC-DBA - <https://inoc.nic.br/>
- Downdetctor - <https://downdetector.com.br/>
- Down for Everyone or Just me -  
<https://downforeveryoneorjustme.com/>
- CETIC.br - Provedores -  
<https://cetic.br/pt/pesquisa/provedores/indicadores/>
- CETIC.br - Domicilios -  
<https://cetic.br/pt/pesquisa/domicilios/indicadores/>



# Link das ferramentas mostradas

- Anatel -  
<https://informacoes.anatel.gov.br/paineis/acessos/banda-larga-fixa>
- BGPmon - <https://www.bgpmon.net/>
- BGPlay - <https://bgplayjs.com/?section=bgplay>
- RIPEstat - <https://stat.ripe.net/app/launchpad>
- BGP.tools - <https://bgp.tools/>
- Lista de Looking Glass -  
[https://wiki.brasilpeeringforum.org/w/Looking\\_Glass](https://wiki.brasilpeeringforum.org/w/Looking_Glass)
- HE BGP Toolkit - <https://bgp.he.net/>
- PeeringDB - <https://www.peeringdb.com/>



# Link das ferramentas mostradas

- TC IRR - <https://bgp.net.br/>
- RADb - <https://www.radb.net/>
- Team cymru - <https://team-cymru.com/>
- BGPAlerter - <https://github.com/nttgin/BGPAlerter>
- CAIDA Spoof - <https://www.caida.org/projects/spoof/>



# Dúvidas?



# Obrigado !!!

✉ cursosceptro@nic.br

✉ nakamura@nic.br

14 de novembro de 2025

**nic.br cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)