nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

Tiago Jun Nakamura

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

Automação BGP: utilizando o protocolo BMP para monitorar a Internet

ceptro.br nic.br cgi.br

Agenda

- O que é BMP
- Troubleshooting com BMP
- Incidentes de Segurança
- Arquitetura BMP

O que é BMP?

O que é BMP?

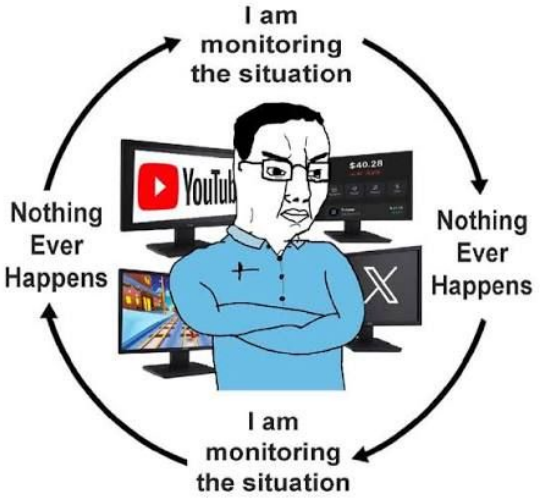
- **BGP Monitoring Protocol**
- **RFC 7854** de **2016**
- Protocolo que **coleta dados da operação do BGP** em tempo real para um sistema de monitoramento
- É um protocolo estritamente **observacional**
  - Ele não interfere nas decisões de roteamento
  - Apenas exporta informações

Motivação para usar BMP

- **SNMP com MIB** relacionada ao BGP
  - **Trabalha com requisições** e não com eventos
  - **Chamadas periódicas** podem perder informação
- Captura de dados via **CLI**
  - Precisa entrar na configuração dos roteadores
  - **Se forem muitos roteadores?**
  - **Capturas periódicas** podem perder informação
- São complementares
  - **SNMP** pode ajudar com o monitoramento do equipamento (CPU, memória, etc…)
  - **CLI** consegue uma visão de outras funções do equipamento e alterar alguma configuração (log, interfaces, etc..)

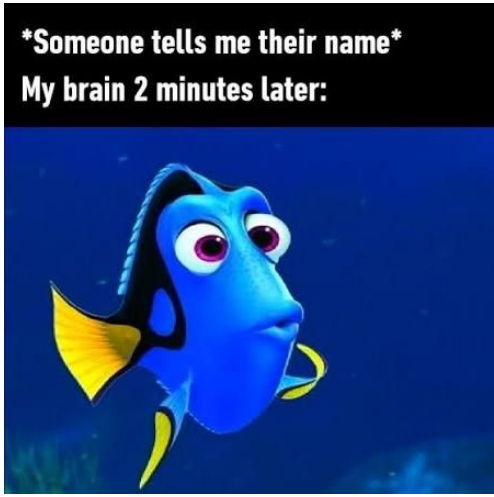
Motivação para usar BMP

- Melhor entendimento das **políticas BGP**
  - Visibilidade **Pré e Pós**
- Monitoramento **em tempo real**
  - Sessão BGP
  - Todas as rotas
  - Estatísticas
- **Troubleshooting** de problemas de redes
  - Incidentes de segurança
  - Erros de configuração



Pontos de atenção

- Memória
  - **Precisa armazenar muitas informações**
    - Tabela global IPv4 (atual)
      - Mais de 1.000.000 rotas
    - Tabela global IPv6 (atual)
      - Mais de 250.000 rotas
- Processamento
  - **Recebe muitas mensagens** de diferentes roteadores
  - Mensagens agrupadas **por peer e por acesso a RIB**



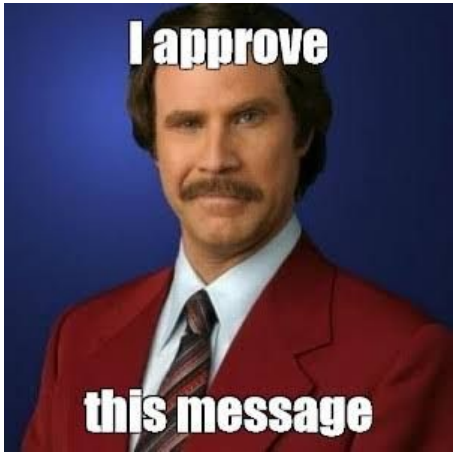
Funcionamento do BMP

- Opera sobre o **TCP**
- Tudo é configurado e enviado do **ponto de vista do roteador**
- O roteador pode conversar **com um ou mais coletores**
  - **Principal e Backup**
- Pode se monitorar **quantas sessões BGP quiser no roteador**
- **Um coletor pode centralizar** os dados de todas sessões BGP de todos os roteadores

Mensagens BMP

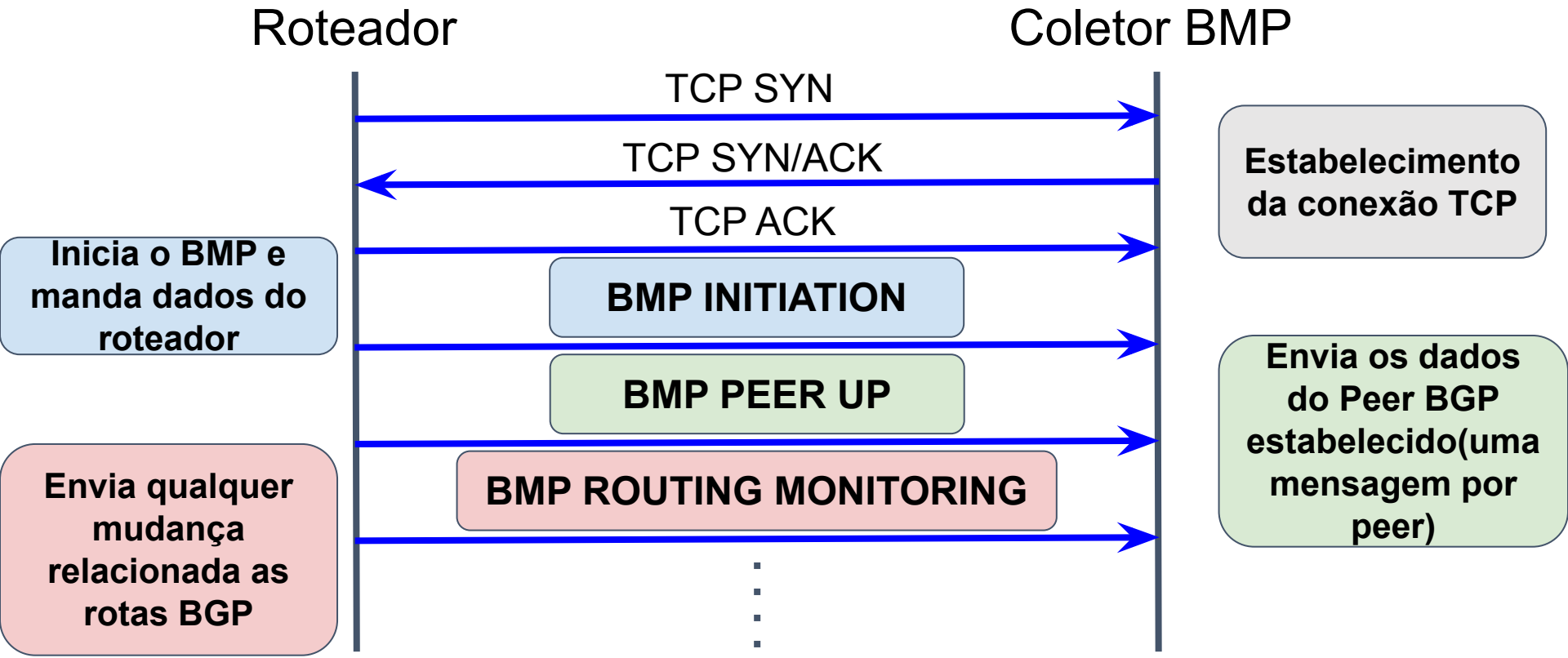
1. **Route Monitoring**
   - Serve para enviar todas as **informações de rotas de um peer**
2. **Statistics Report**
   - Reporta de forma **estatística as atividades BGP** do roteador
3. **Peer Down Notification**
   - Indica o **término de uma sessão BGP** com um peer junto com seu motivo
4. **Peer Up Notification**
   - Indica o **estabelecimento de uma sessão BGP** com um peer junto com as informações trocadas na sessão

Mensagens BMP

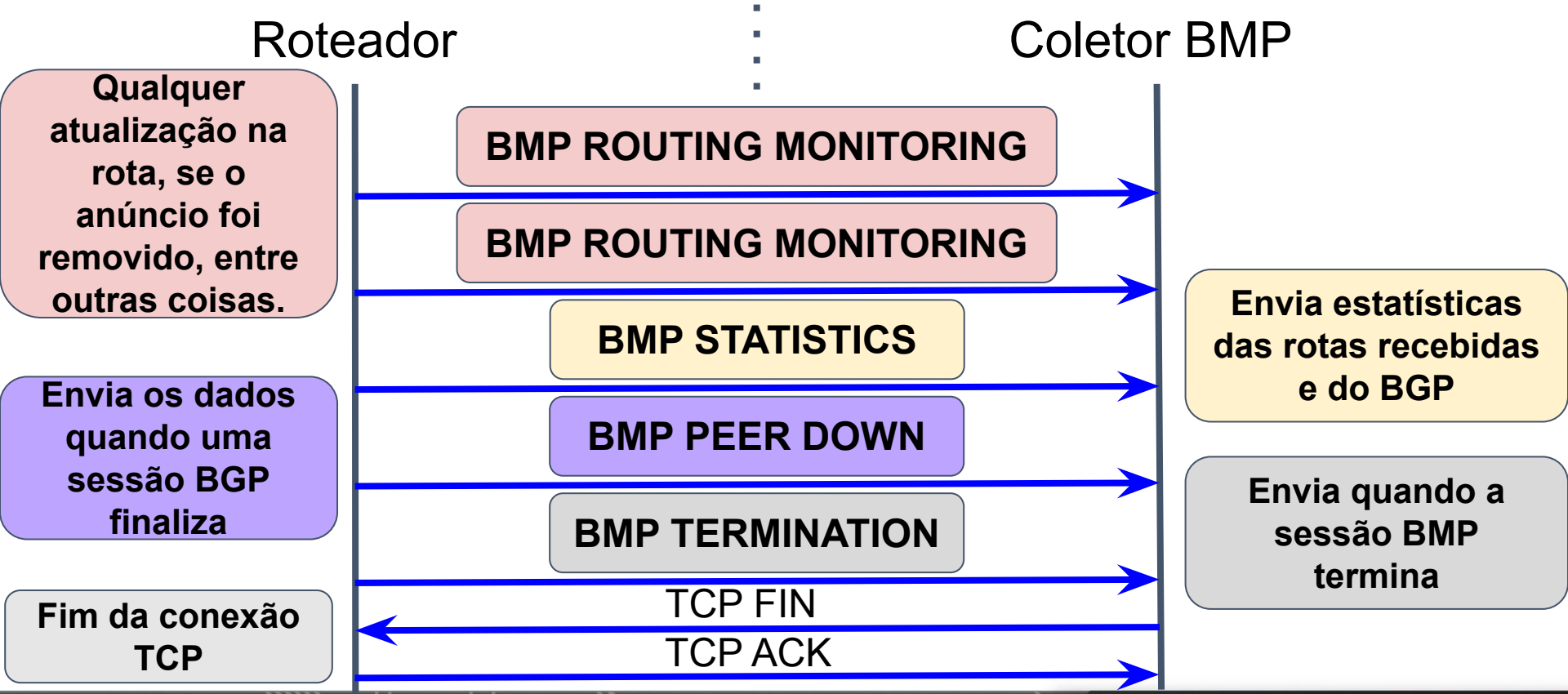


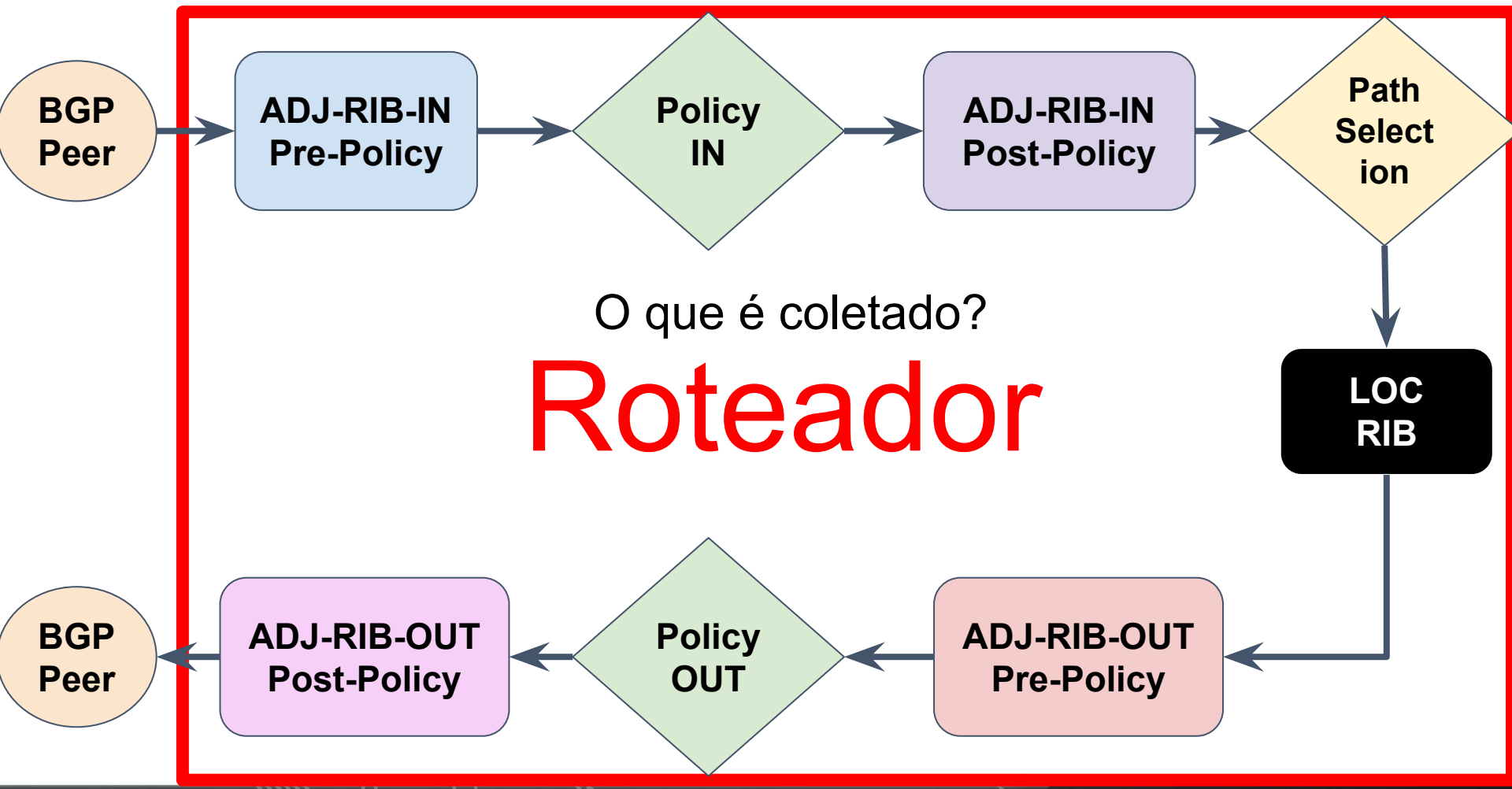
5. **Initiation Message**
   - Uma maneira informar ao coletor **dados sobre o roteador** como sobre seu fabricante, versão de software, etc..
6. **Termination Message**
   - Uma forma do roteador informar ao coletor o **término da sessão BMP** junto com o seu motivo
7. **Route Mirroring Message**
   - Um mecanismo que permite ao roteador monitorado **enviar duplicatas idênticas das mensagens**, exatamente como foram recebidas.

Troca de Mensagens BMP



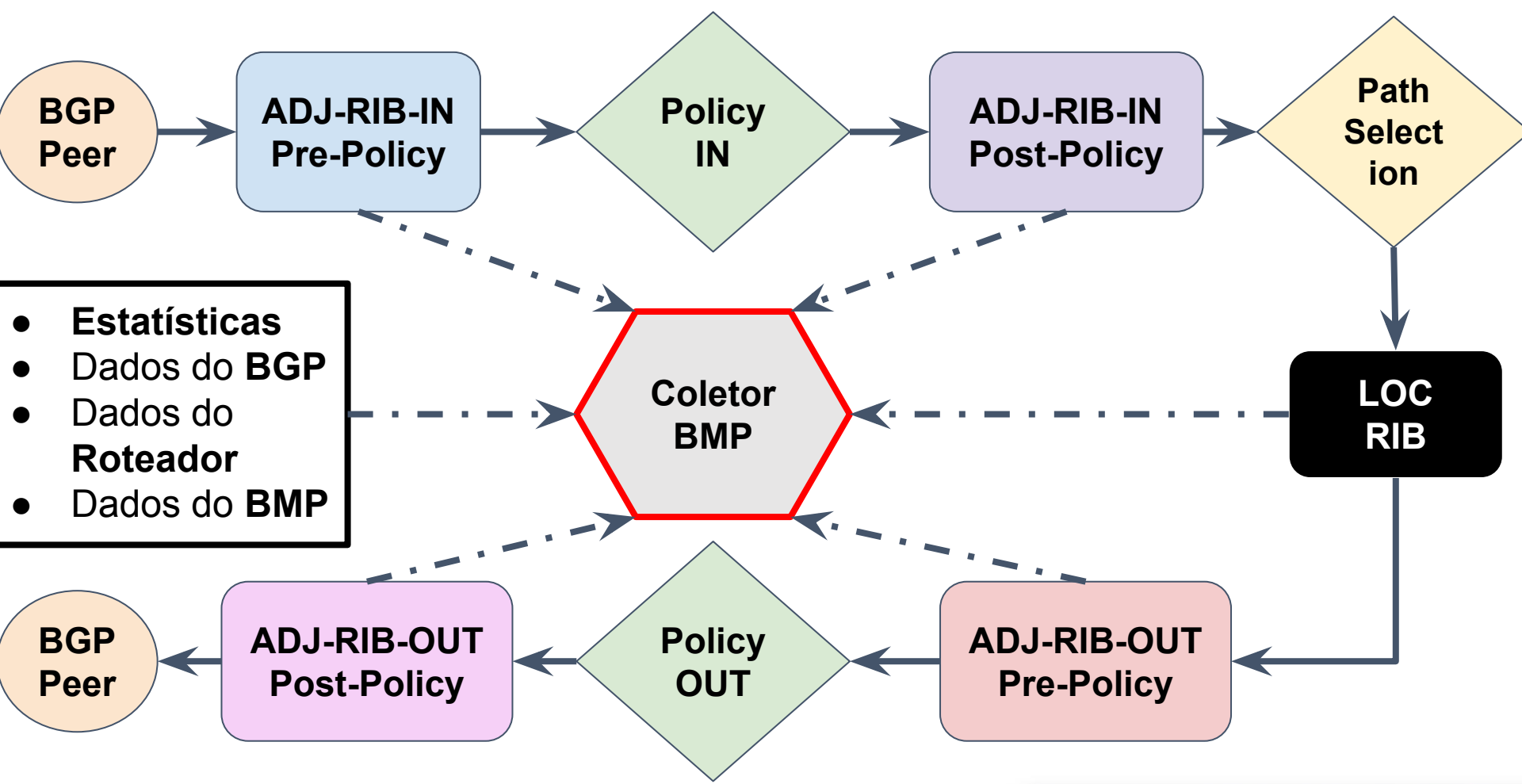
Troca de Mensagens BMP



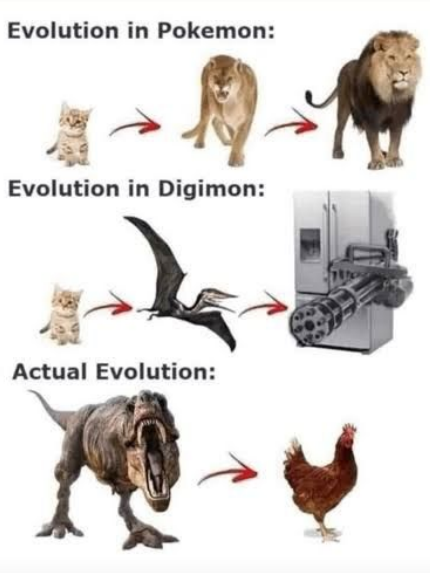


O que é coletado?

Roteador


BGP Peer
ADJ-RIB-IN Pre-Policy
Policy IN
ADJ-RIB-IN Post-Policy
Path Selection
Estatísticas
Dados do BGP
Dados do Roteador
Dados do BMP
Coletor BMP
LOC RIB
BGP Peer
ADJ-RIB-OUT Post-Policy
Policy OUT
ADJ-RIB-OUT Pre-Policy

Evolução do BMP



- **Presente**
  - As implementações estão usando a **versão 3**
  - Nem todos os roteadores implementam todas as RFCs lançadas sobre BMP
    - RFC 8671 - Suporte Adj-RIB-Out (2019)
    - RFC 9069 - Suporte Local RIB (2022)
    - RFC 9972 - Suporte avançado de estatísticas (2026)
- **Futuro**
  - Está em discussão a **versão 4 do BMP** (draft)
    - BMP v4: Extended TLV Support for BGP Monitoring Protocol (BMP)
    - https://datatracker.ietf.org/doc/draft-ietf-grow-bmp-tlv/

Troubleshooting com BMP

ceptro.br nic.br cgi.br

Problema:
Perda de conectividade

ceptro.br nic.br cgi.br

Problema: Perda de conectividade

- Sexta feira 5 horas da tarde
- Ticket aberto
  - **Desde as 16:23 não consigo acessar o site da universidade. IPv6 2001:db8::113**.
- **O que será que aconteceu?**
  - A rota nunca existiu?
  - A rota existia e foi retirada?
  - Um filtro removeu a rota?
  - O vizinho BGP (peer) caiu?
  - Houve um roubo de prefixo ou vazamento de rota?

Como identificar: Perda de conectividade

- BMP
  - Basta consultar a rota no coletor
  - Entrada (será que recebemos a rota?)
    - Procura a **rota no histórico** (Recebemos ela no passado?)
    - Procura ver se a **sessão BGP** por onde deveria a rota **está operando** (o trânsito/peer está operando?) - **Mensagem Peer Down Notification**
    - Analisa o **ADJ-RIB-IN Pre-Policy** para ver se recebeu a rota (recebemos ela agora?)
    - Observa se o filtro foi aplicado corretamente **ADJ-RIB-IN Post-Policy** (Aplicamos filtros?)

Problema:
Sessão BGP Caiu

ceptro.br nic.br cgi.br

Problema: Sessão BGP caiu

- Quarta feira 21 horas - horário do jogo
- **Monitoramento:**
  - **Alerta sessão BGP caiu**
- **O que será que aconteceu?**
  - Qual será o motivo da sessão ter caído?
  - É um problema do meu lado?
  - É um problema do vizinho/trânsito?

Como identificar: Perda de conectividade

- BMP
  - **Mensagem Peer Down Notification**
    - Type = 0 é reservado.
    - Type = 1 sessão fechada localmente anexando BGP NOTIFICATION PDU (Protocol Data Unit)
    - Type = 2: sessão fechada localmente anexando o evento FSM (Finite State Machine) do BGP
    - Type = 3: sessão fechada remotamente anexando BGP NOTIFICATION PDU (Protocol Data Unit)
    - Type = 4: sessão fechada remotamente, sem dados
    - Type = 5: Peer desconfigurado

Problema:
Oscilação no BGP

ceptro.br nic.br cgi.br

Problema: Oscilação no BGP

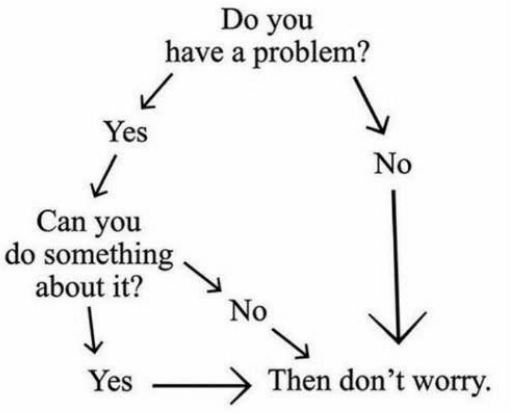
REALTIME Sep 07, 2026, 07:00:00 AM GMT-3 - Sep 07, 2026, 08:46:23 AM GMT-3

Flapping Prefixes	
Prefix	Count
72.48.108.0/24	375
2a0c:b642:ace::/48	14978
130.137.140.0/24	288
216.82.212.0/24	311
5.42.164.0/22	14948
2408:4016:1::/48	494
2602:faae::/40	6531
2804:8240:8000::/34	271
2800:540:2000::/44	9196
72.48.82.0/23	375

Flapping Prefixes By ASN	
ASN	Count
668	151
205710	562
17561	209
26787	68269
29733	14281
265566	10365
265573	200
41897	1606
20940	15481
28403	669

https://bgp.he.net/report/netstats?utm_source=chatgpt.com#_flap

Como identificar: Oscilação no BGP



- BMP
  - **Olha as estatísticas**
    - Por peer BGP (frequência de flaps)
    - Por informações do BGP (UPDATE/WITHDRAW)
    - Por prefixo (frequência de flaps)
- **Oscilação no BGP é um custo elevado para a Internet**
  - Alguns Sistemas Autônomos filtram quem fica com as rotas oscilando

Incidentes de Segurança

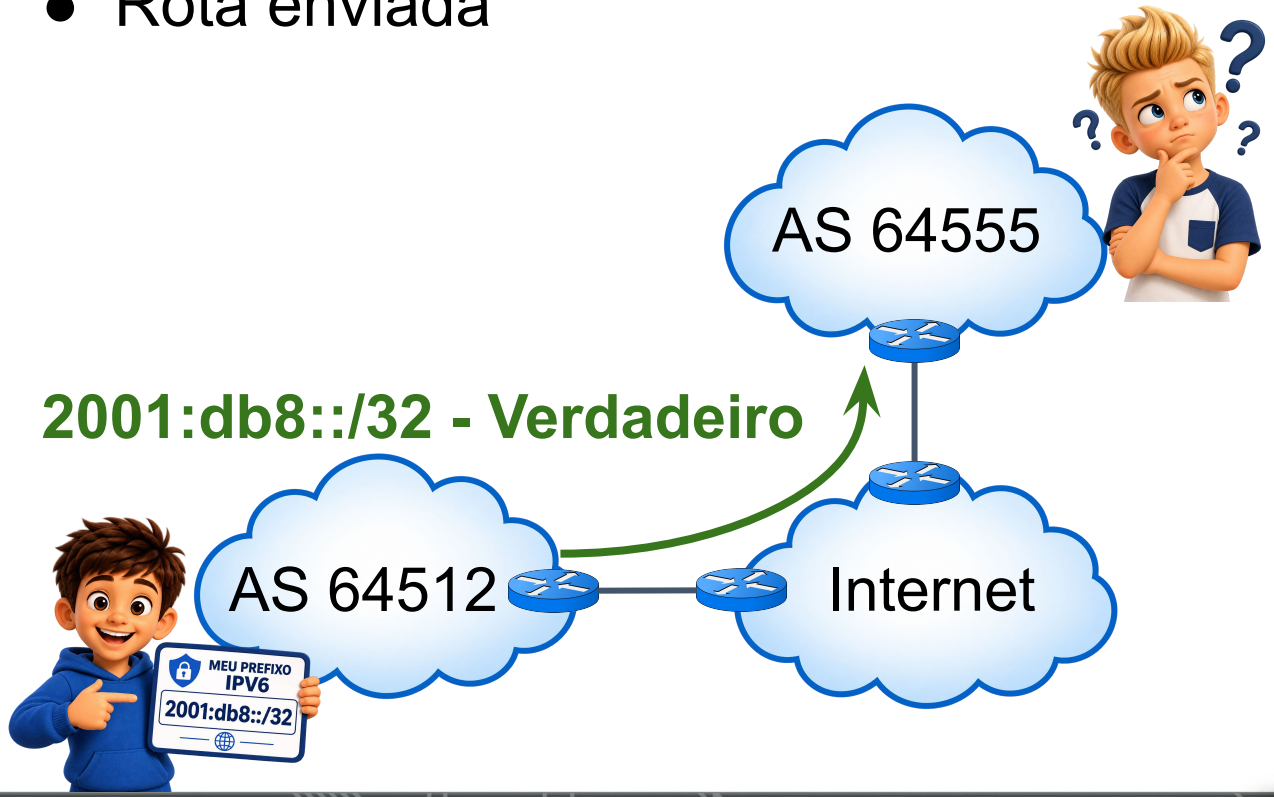
ceptro.br nic.br cgi.br

Incidente:
Roubo de prefixo

ceptro.br nic.br cgi.br

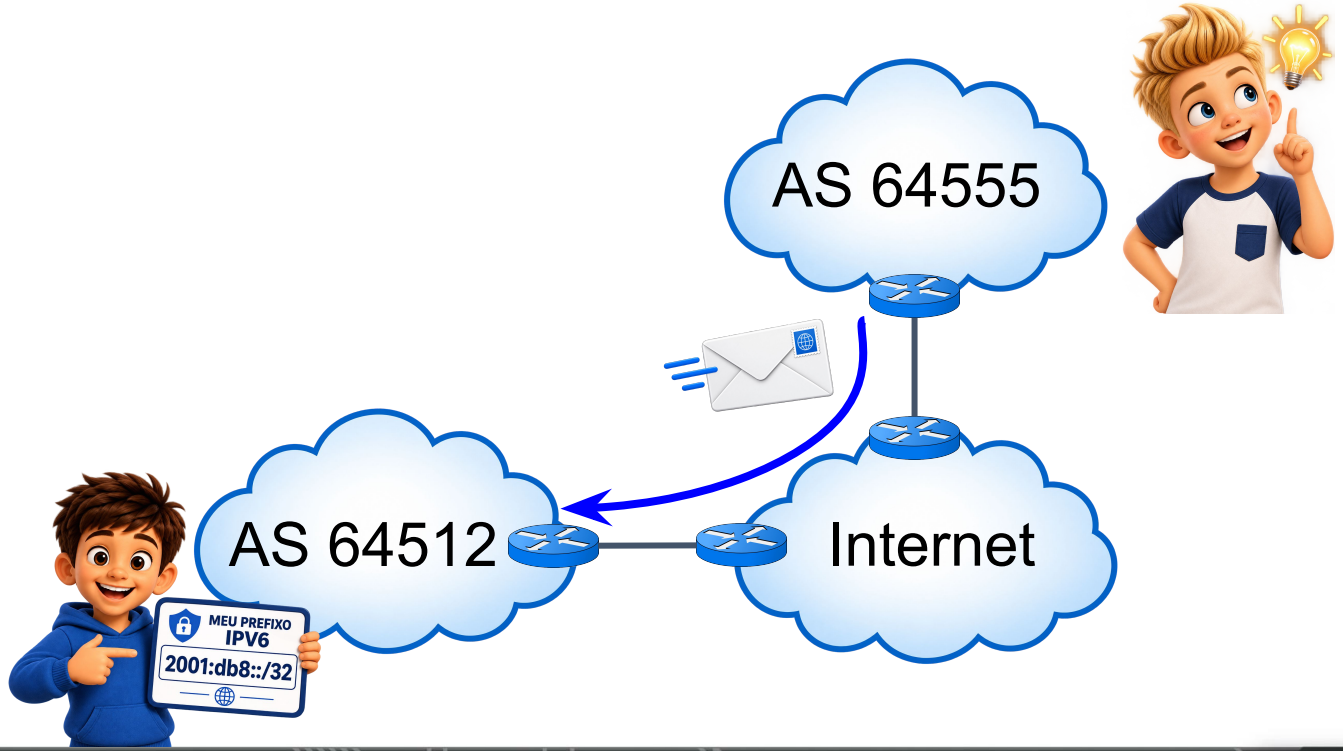
Fluxo normal

- Rota enviada



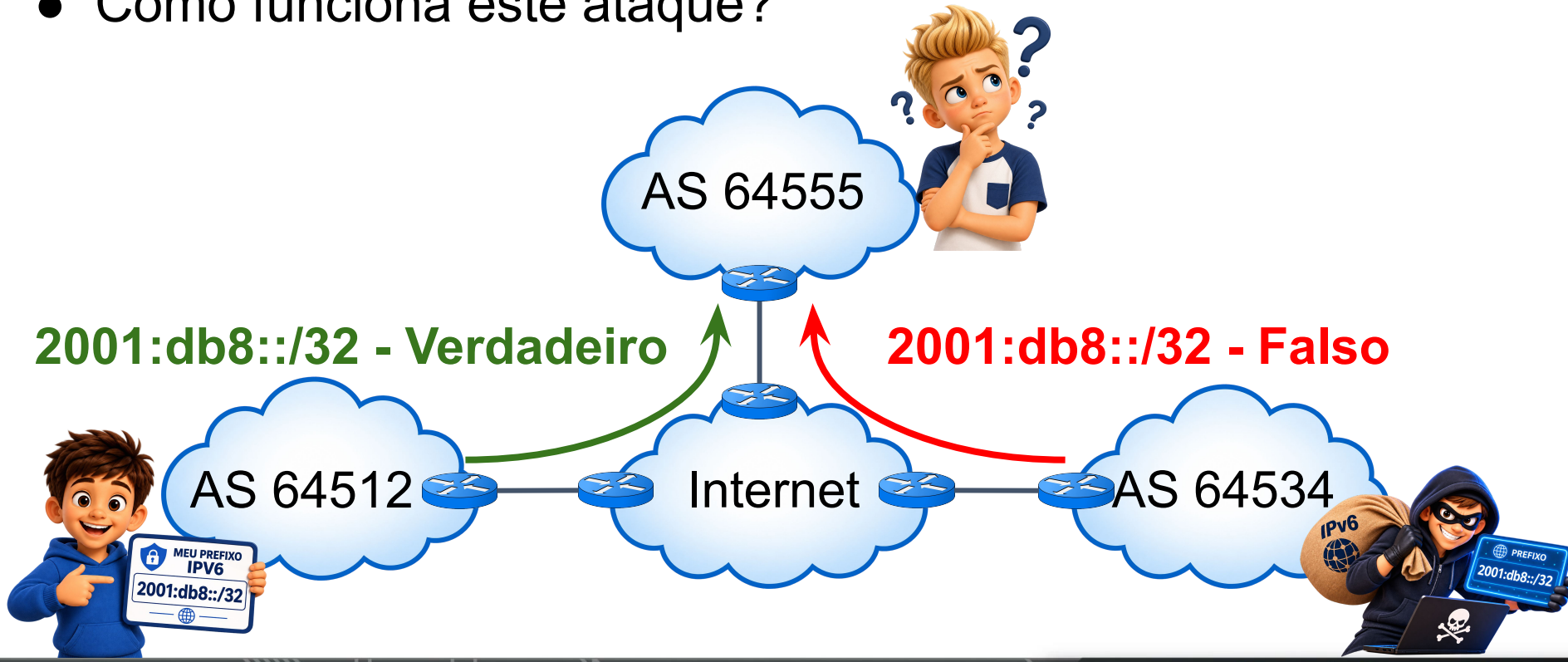
Fluxo normal

- Tráfego segue o caminho da rota



Incidente: Roubo de prefixo

- Como funciona este ataque?



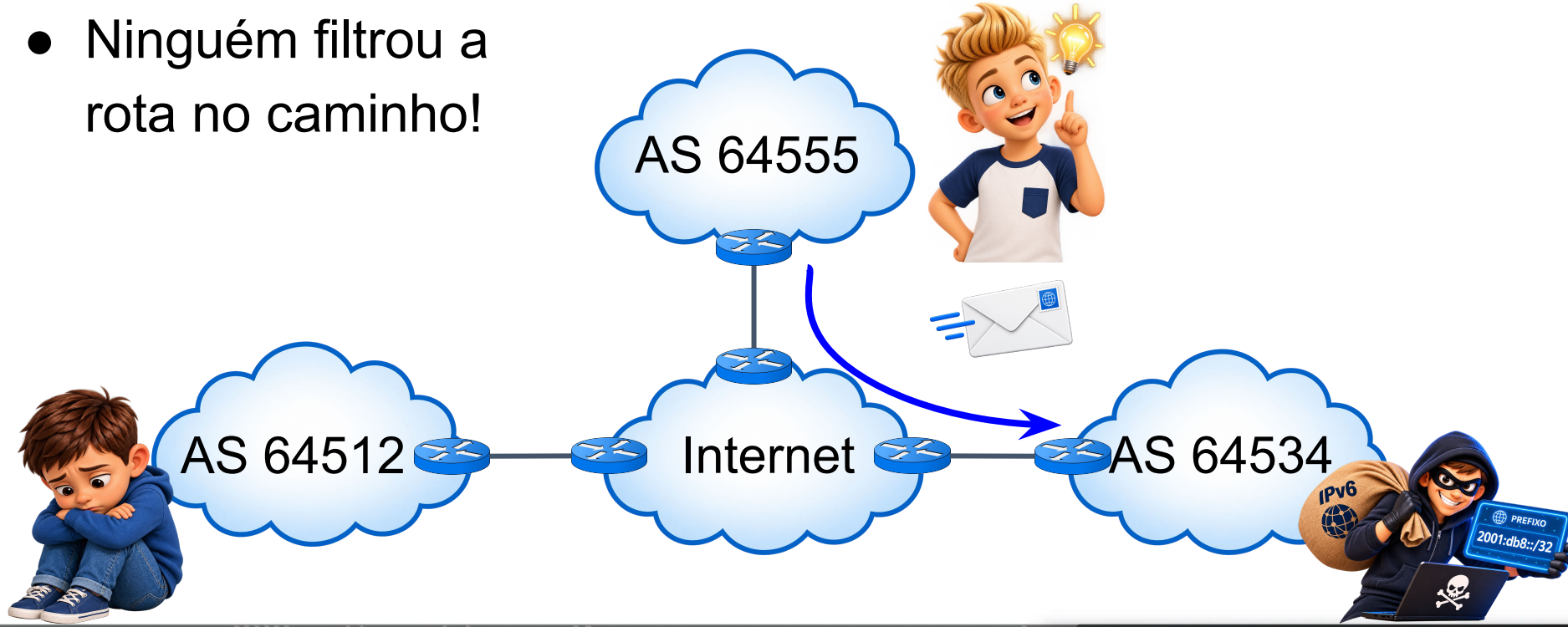
Incidente: Roubo de prefixo

- **O falso pode ser escolhido!**
  - **Caminho menor**
  - **Local preference maior**
  - **entre outros;**

Prefiro essa rota 2001:db8::/32 que veio do AS64534

Incidente: Roubo de prefixo

- Rouba o tráfego original!
- Ninguém filtrou a rota no caminho!



Motivação: Roubo de prefixo

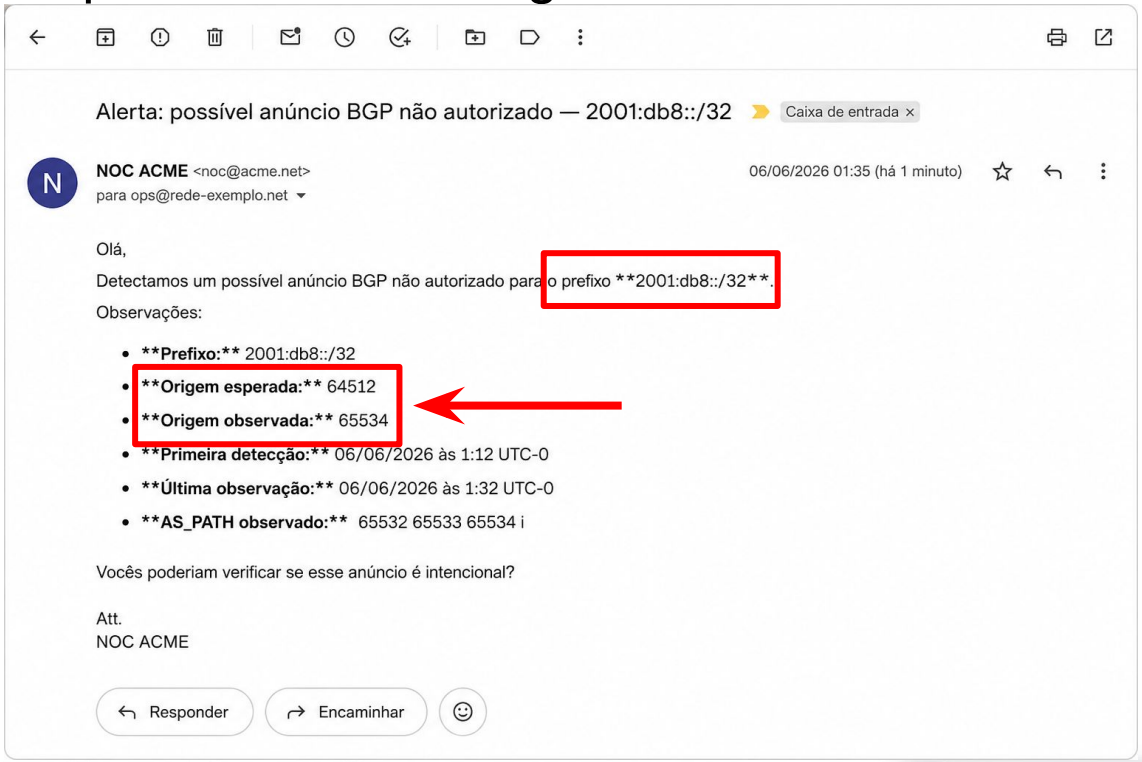
- **Por que algum AS iria roubar um prefixo?**
  - Afinal o AS fica demarcado na rota
  - Erro de configuração
  - **Mal-intencionado**
    - Ataque varia de minutos a horas
    - Invadem roteadores de borda
    - Anunciam prefixo de outro AS (por exemplo: Banco)
    - Levantam túneis GRE para destinos em provedores de hospedagem (protocolos HTTP e DNS no destino)

Solução: Roubo de prefixo

- **Precisa monitorar o BGP**
  - No seu roteador (BMP)
  - Na visão de fora (Looking Glass)
- **RPKI** (Resource Public Key Infrastructure)
  - Publicação e Validação
  - Todos precisam implementar
- **BGP Role**
  - Customer - Provider ou Peer-Peer
- **Filtros no BGP**
  - Só aceito os prefixos previamente acordados

Incidente: Roubo de prefixo (como ele acontece)

- Começa o expediente numa segunda feira com um email



Alerta: possível anúncio BGP não autorizado — 2001:db8::/32 Caixa de entrada ×

NOC ACME <noc@acme.net> 06/06/2026 01:35 (há 1 minuto)
para ops@rede-exemplo.net

Olá,

Detectamos um possível anúncio BGP não autorizado para o prefixo **2001:db8::/32**.

Observações:

- **Prefixo:** 2001:db8::/32
- **Origem esperada:** 64512
- **Origem observada:** 65534
- **Primeira detecção:** 06/06/2026 às 1:12 UTC-0
- **Última observação:** 06/06/2026 às 1:32 UTC-0
- **AS_PATH observado:** 65532 65533 65534 i

Vocês poderiam verificar se esse anúncio é intencional?

Att.
NOC ACME

Responder Encaminhar

Incidente: Roubo de prefixo

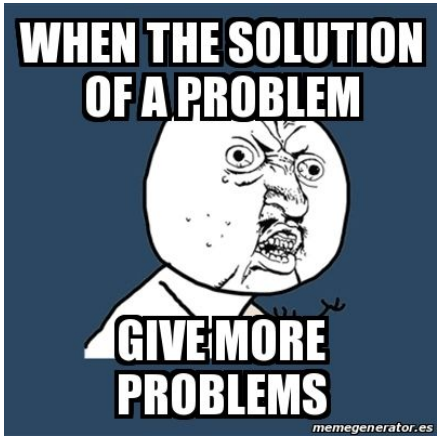
- Será que é verdade?
- Vamos olhar a CLI
  - **Não tem rota gerada 2001:db8::/32!**
- Ignoramos o email?
- Como investigar?

```
[R1] display bgp ipv6 routing-table
BGP Local router ID : 10.10.10.1
Local AS number : 64512
Total number of routes : 5
BGP table version is 189, local router ID is 10.10.10.1
Status codes: * - valid,  > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of IPv6 Routes: 5
     Network                 NextHop                 MED    LocPrf    PrefVal   Path/Ogn
*>   3fff:1::/32             2a0d:1:1:1::1           0      100       0         65532 65533 65534 i
     via TenGigE0/0/0
*>   3fff:2::/32             2a0d:1:1:1::2           0      100       0         64513 65531 65535 i
     via TenGigE0/0/1
*>   3fff:3::/32             2a0d:1:1:1::3           0      100       0         65530 65536 65537 i
     via TenGigE0/0/2
*    3fff::/20               2a0d:1:1:1::4           0      100       0         64500 i
     via TenGigE0/0/3
*i   ::/0                    2a0d:ffff:1::1          0      100       0         64500 i
     via TenGigE0/0/0

Total number of displayed routes : 5
```

Como identificar: Roubo de prefixo



- BMP
  - Observa se a rota aparece na tabela **ADJ-RIB-OUT Post-Policy**
  - Olha o **histórico de saída das rotas**
    - Para descobrir se a rota foi anunciada em determinado momento
  - **Em caso positivo, precisa se investigar** o que houve
    - Máquina foi invadida? Algum administrador mexeu nos filtros e nos anúncios de rotas?
    - O provedor de trânsito, também precisa colocar filtros.

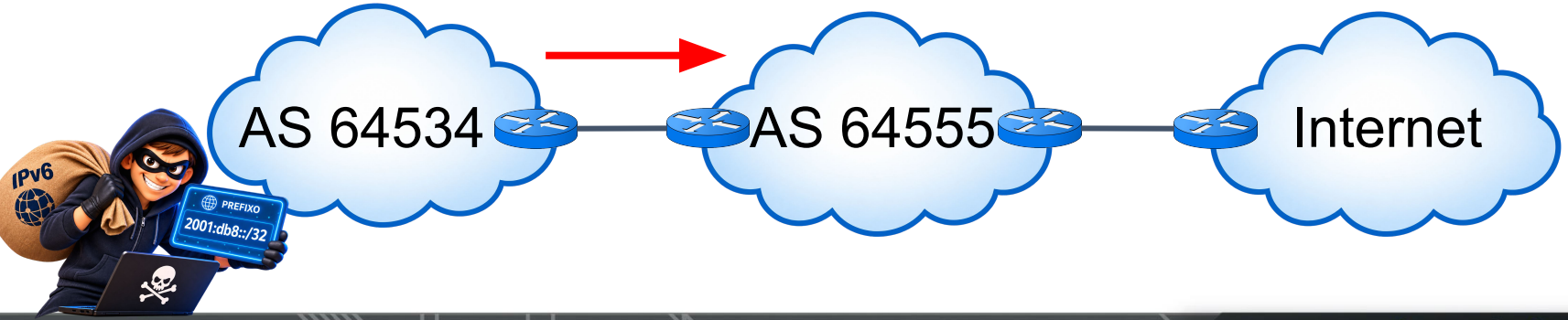
Incidente:
Vazamento de rota

ceptro.br nic.br cgi.br

Incidente: Vazamento de rota

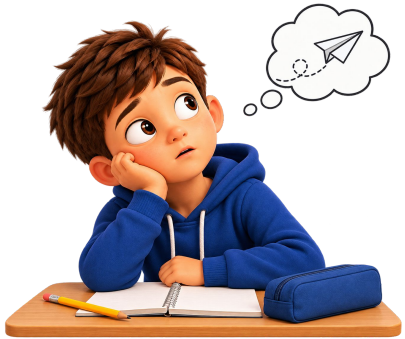
- Como funciona este ataque?

Anuncia uma rota que não é dele - Ex: 2001:db8::/32



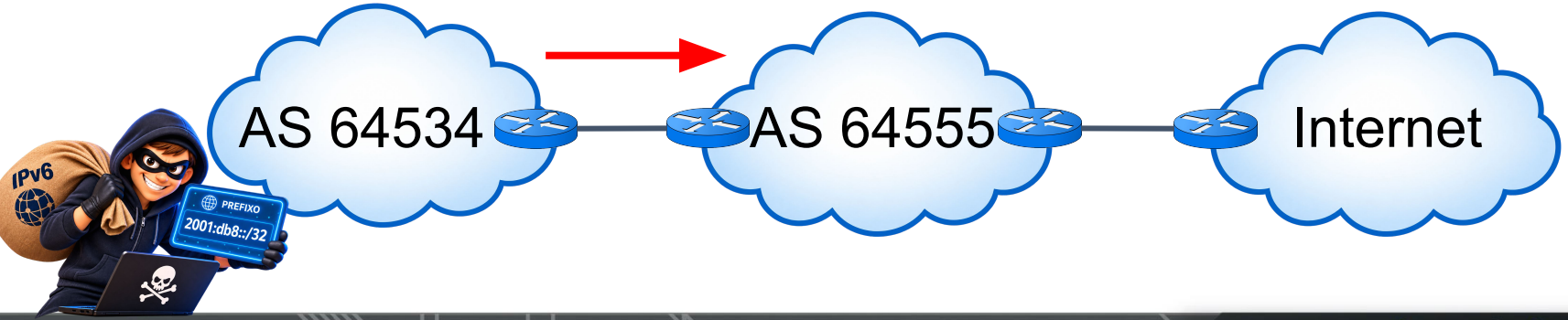
Incidente: Vazamento de rota

- Como funciona este ataque?



Esqueci de aplicar filtros no BGP!

Anuncia uma rota que não é dele - Ex: 2001:db8::/32

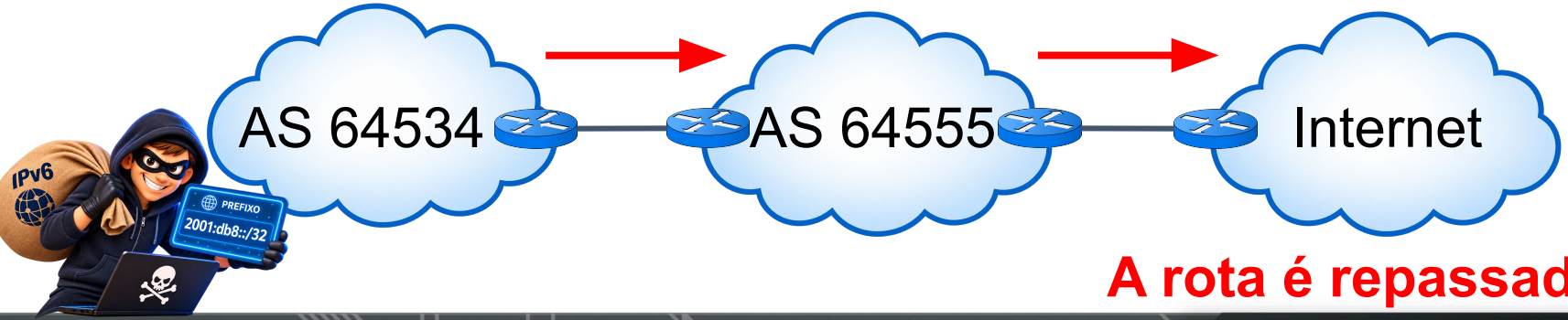


Incidente: Vazamento de rota

- Se nenhum filtro for aplicado no meio do caminho
- A rota é repassada adiante!

Esqueci de aplicar filtros no BGP!

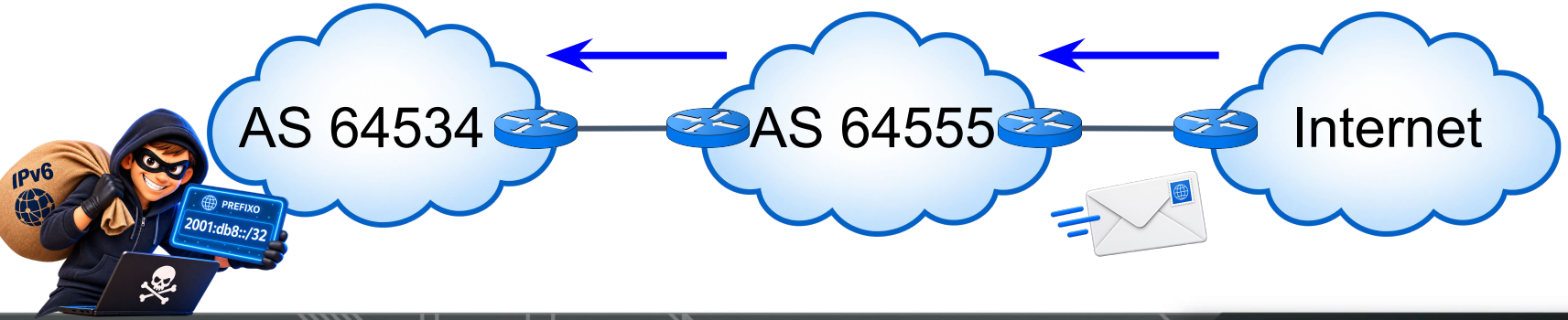
Anuncia uma rota que não é dele - Ex: 2001:db8::/32



A rota é repassada!!!

Incidente: Vazamento de rota

- O tráfego passa pelo seu AS que vazou a rota

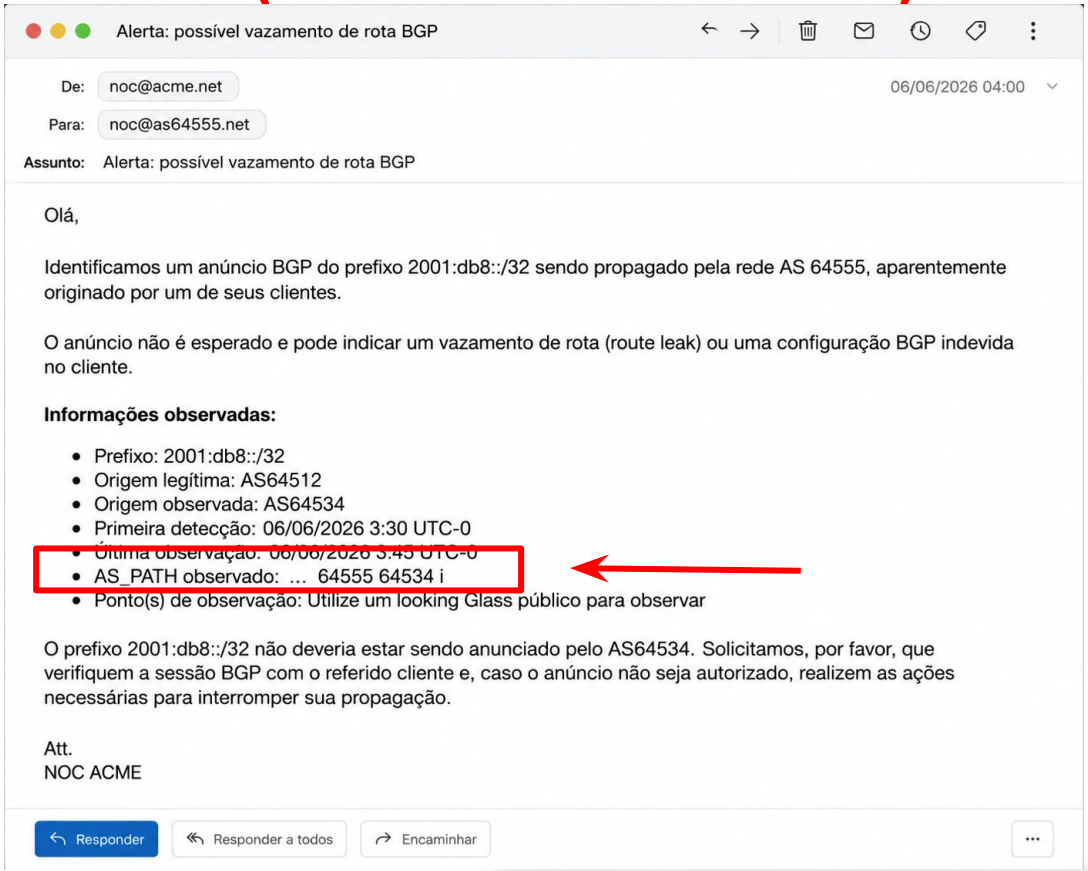


Solução: Vazamento de rota

- **Precisa monitorar o BGP**
  - No seu roteador (BMP)
- **RPKI** (Resource Public Key Infrastructure)
  - Publicação e Validação
  - **ASPA - validação do caminho**
  - Todos precisam implementar
- **BGP Role**
  - Customer - Provider ou Peer-Peer
- **Filtros no BGP**
  - Só aceito os prefixos previamente acordados

Incidente: Vazamento de rota (como ele acontece)

- Começa o expediente numa segunda feira com um email!



Alerta: possível vazamento de rota BGP

De: noc@acme.net
Para: noc@as64555.net
06/06/2026 04:00
Assunto: Alerta: possível vazamento de rota BGP

Olá,

Identificamos um anúncio BGP do prefixo 2001:db8::/32 sendo propagado pela rede AS 64555, aparentemente originado por um de seus clientes.

O anúncio não é esperado e pode indicar um vazamento de rota (route leak) ou uma configuração BGP indevida no cliente.

Informações observadas:

- Prefixo: 2001:db8::/32
- Origem legítima: AS64512
- Origem observada: AS64534
- Primeira detecção: 06/06/2026 3:30 UTC-0
- Última observação: 06/06/2026 3:45 UTC-0
- AS_PATH observado: … 64555 64534 i
- Ponto(s) de observação: Utilize um looking Glass público para observar

O prefixo 2001:db8::/32 não deveria estar sendo anunciado pelo AS64534. Solicitamos, por favor, que verifiquem a sessão BGP com o referido cliente e, caso o anúncio não seja autorizado, realizem as ações necessárias para interromper sua propagação.

Att.
NOC ACME

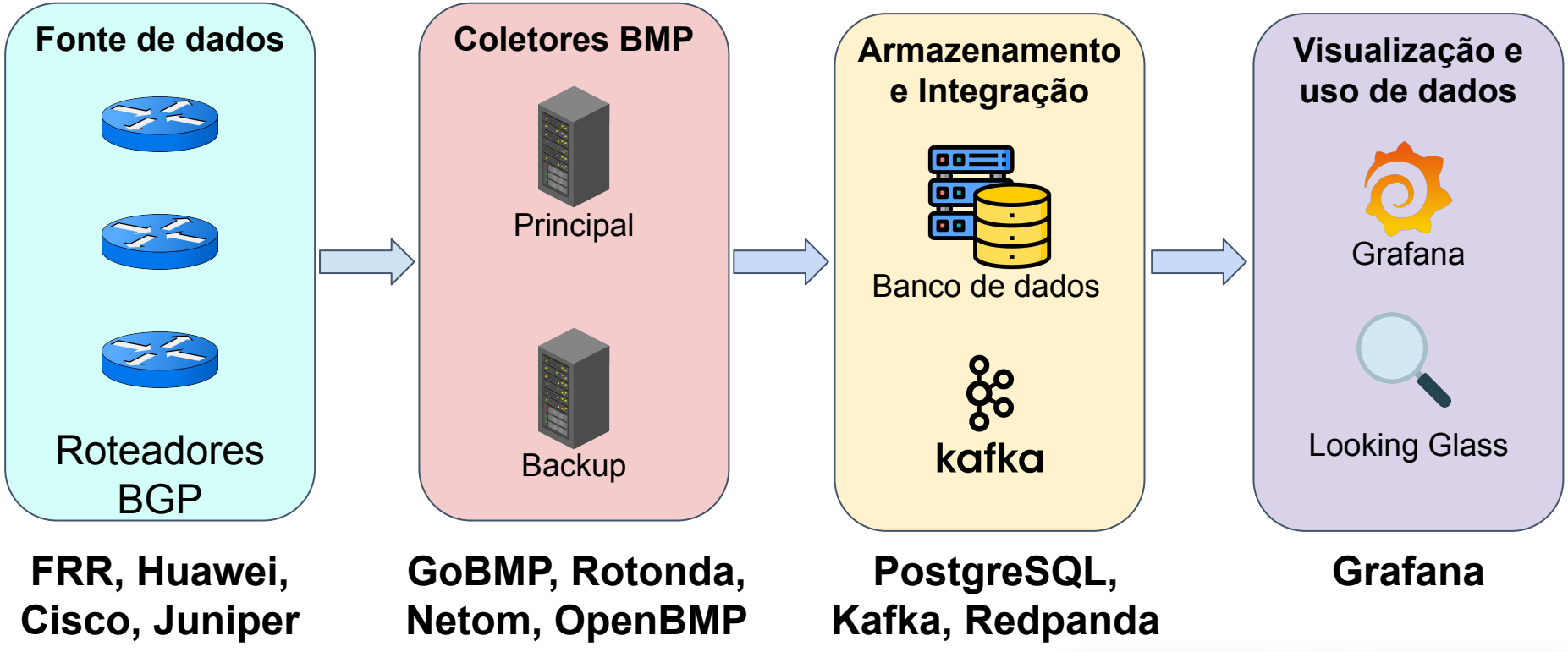
Responder | Responder a todos | Encaminhar

Como identificar: Vazamento de rota

- BMP
  - **Entrada** (será que recebemos uma rota errada?)
    - Analisa o **ADJ-RIB-IN Pre-Policy** para ver se recebeu a rota
    - Observa se o filtro foi aplicado corretamente **ADJ-RIB-IN Post-Policy**
  - **Saída** (será que repassamos adiante rota errada?)
    - Verifica se **ADJ-RIB-OUT Post-Policy** repassou a rota
  - Olhar o **histórico** para saber se houve este problema no passado

Arquitetura BMP

Arquitetura BMP



Dúvidas?

Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br

nic.br cgi.br

www.nic.br | www.cgi.br