BGP Traceback: Um Novo Método para Identificação de Origem de Ataques na Internet

Denilson Vedoveto Martins
denilson@ravel.ufrj.br

Estrutura

- Introdução
- Visão Geral do IP Traceback
- BGP Traceback
- Simulações e Resultados
- Considerações Finais

Introdução

- Crescente aumento de ataques DoS e DDoS
- Sofisticação das técnicas de evasão
- Poucos utilizam boas práticas de segurança para configuração de equipamentos
- Métodos convencionais não identificam o ataque ou o caminho do ataque

Introdução

- Necessidade de métodos mais avançados de identificação
- Surgimento do *IP Traceback*
- Definição:

> *"IP Traceback é um conjunto de mecanismos utilizados para identificar a origem real ou o caminho do ataque"*

IP Traceback

- Diversos métodos propostos, nenhum utilizado como padrão
  - Link Testing
  - Probabilistic Packet Marking (PPM)
  - Deterministic Packet Marking (DPM)
  - ICMP Traceback
  - Hash-Based IP Traceback

IP Traceback

- Diferentes problemas em cada método:
  - Tráfego extra imposto a rede
  - Sobrecarga no processamento dos roteadores
  - Grande necessidade de interação humana
  - Resultados pouco eficientes
  - Incompatibilidade com tecnologias atuais
  - Problemas de segurança

IP Traceback

- Demais problemas já foram abordados exceto Segurança
- Realizado estudo detalhado dos métodos encontrados atualmente
- Problemas encontrados:
  - Vulneráveis ao IP Spoofing
  - PPM permite marcações falsas
  - PPM marca pacotes não pertencentes a ataques

BGP Traceback

- Proposta de um novo método
- Funciona no protocolo BGP
- Acrescenta 2 mensagens ao BGP
  - Traceback Request
  - Traceback Reply
- Alterações no mecanismo de escolha da mensagem a ser marcada (PPM)
- Foco principal: Segurança

BGP Traceback (cont.)

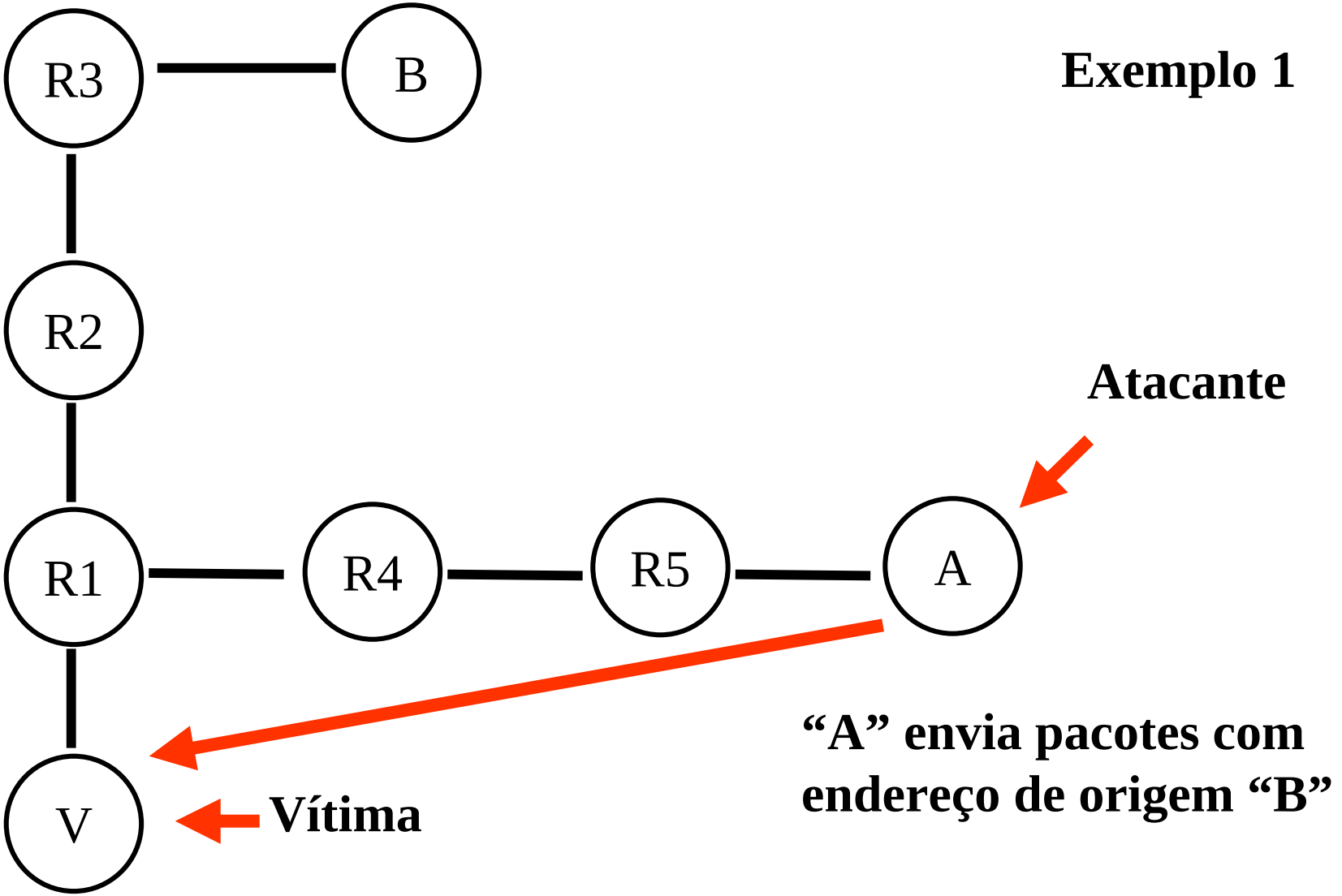
- Utilização do S-BGP (Proposta de um BGP Seguro) [IEEE JSAC 2000]
  - Garante a troca segura entre vizinhos BGP
  - Incorpora mecanismos de segurança como PKI e IPSec
- Mensagens do BGP Traceback são trocadas como mensagens nativas do BGP, por isso tem toda a proteção do S-BGP

BGP Traceback (cont.)

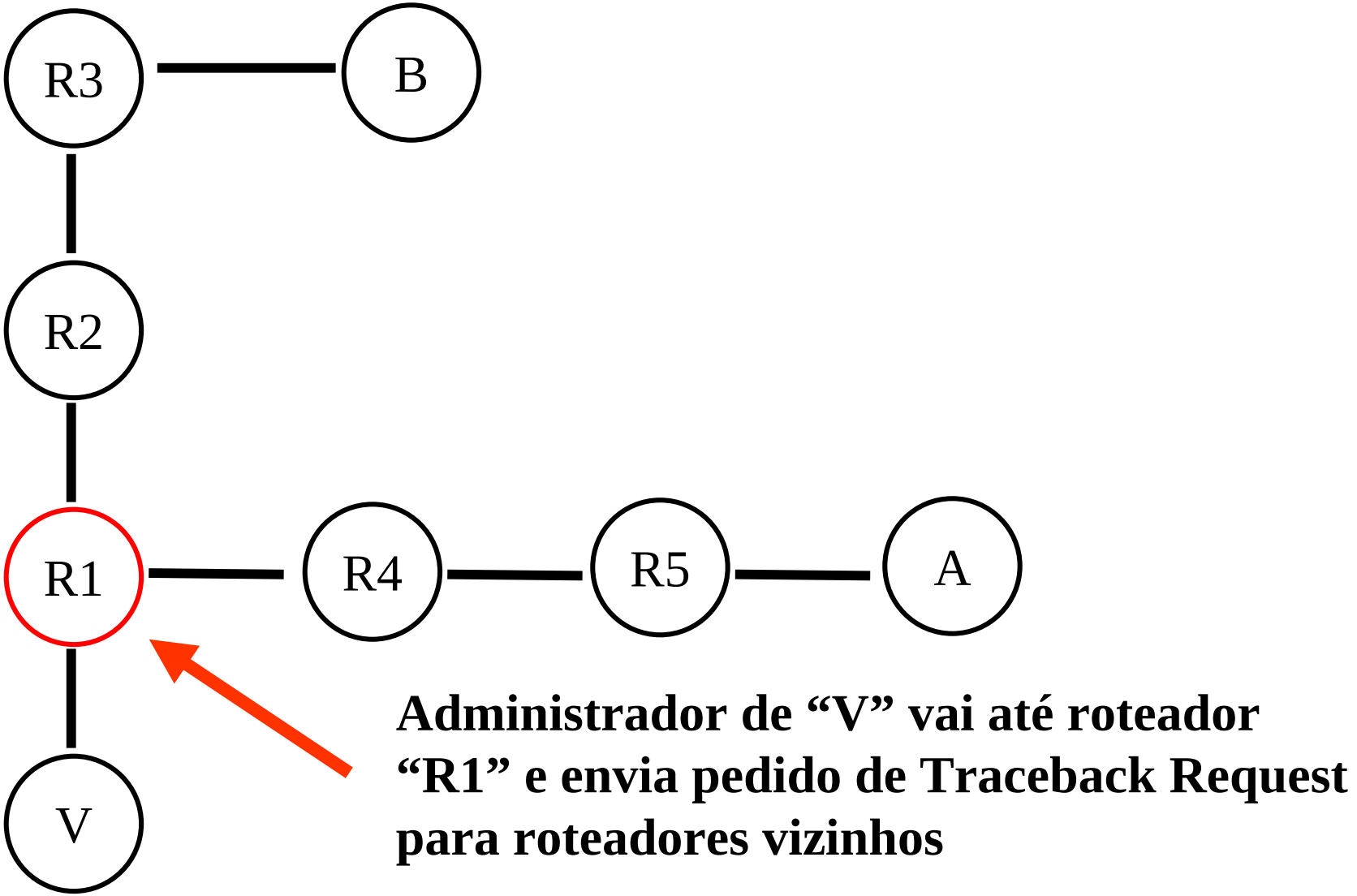
- Para identificar a origem de um ataque o administrador utiliza seu roteador para enviar o pedido de Traceback Request para seus vizinhos BGP
- Vizinhos BGP recebem a mensagem e adicionam o endereço numa lista de endereços a serem rastreados

BGP Traceback (cont.)

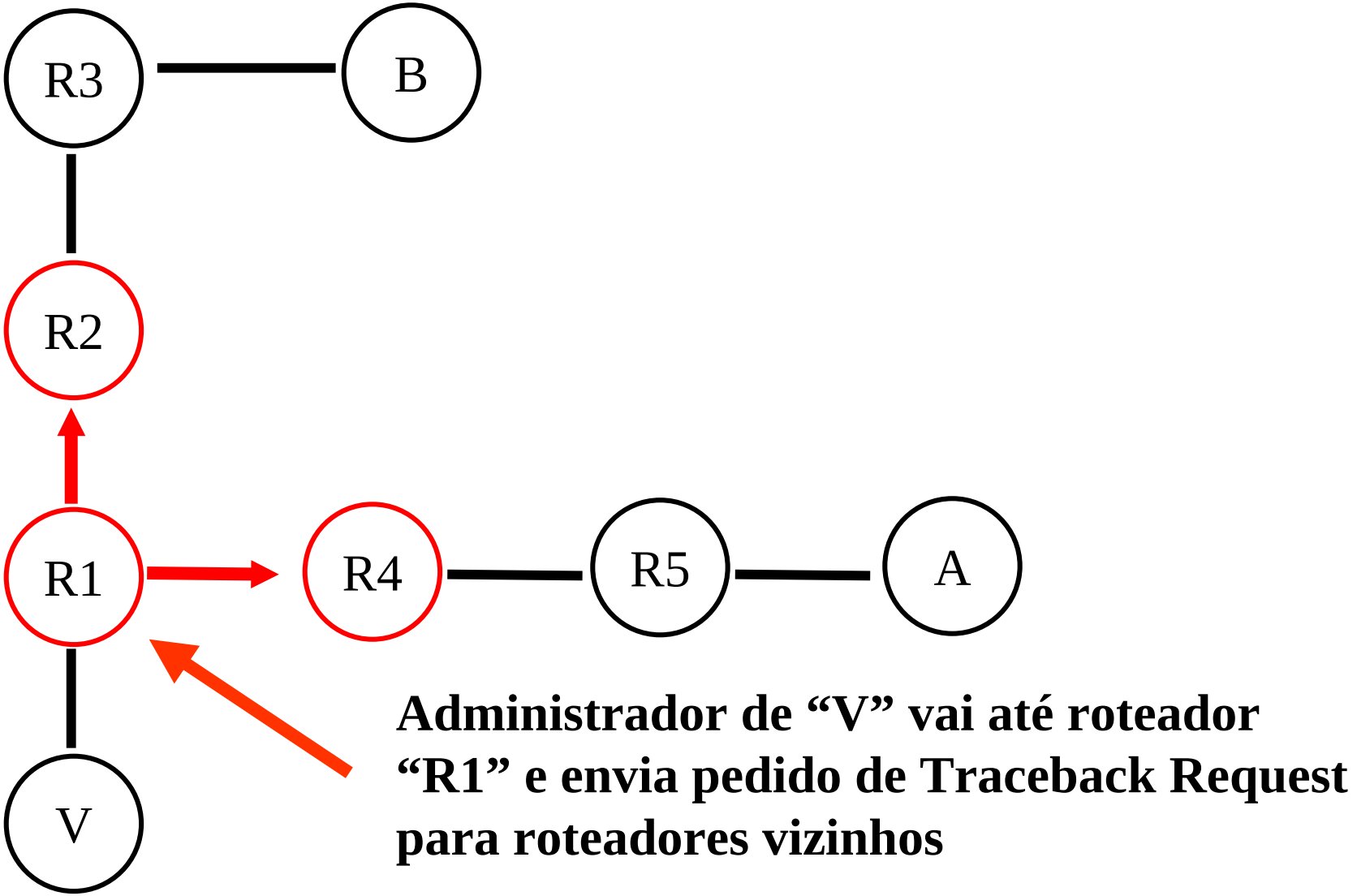
- Todo pacote encaminhado pelo roteador deverá ser verificado para ver se existe um pedido para o endereço de destino do pacote
- Se existir será escolhido com probabilidade "*p*" a geração de uma mensagem de Traceback Reply
- Outros roteadores devem incluir seu endereço nesta mensagem de Reply


R3
B
R2
R1
R4
R5
A
V
Atacante
Vítima
“A” envia pacotes com endereço de origem “B”

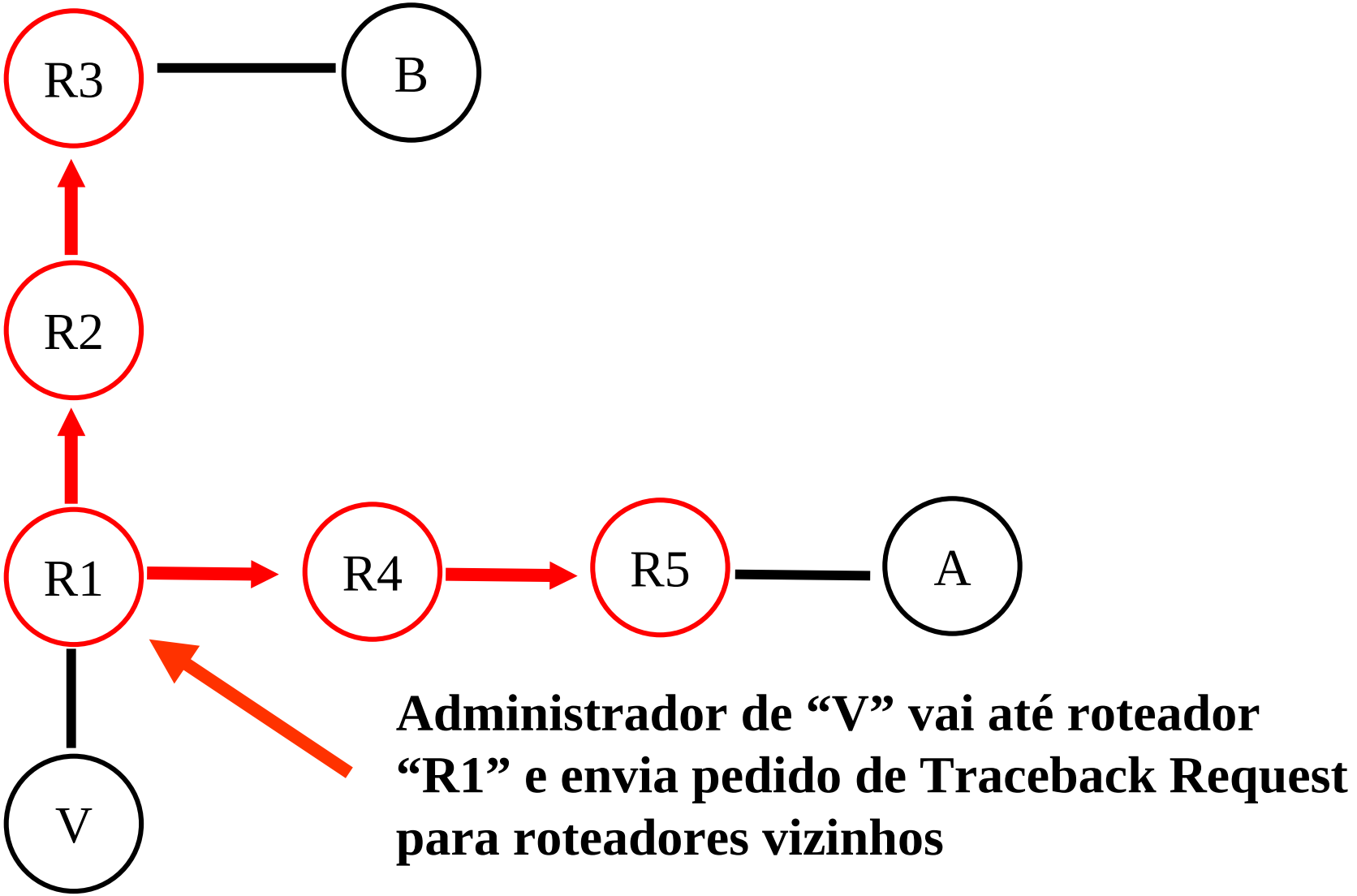
Exemplo 1



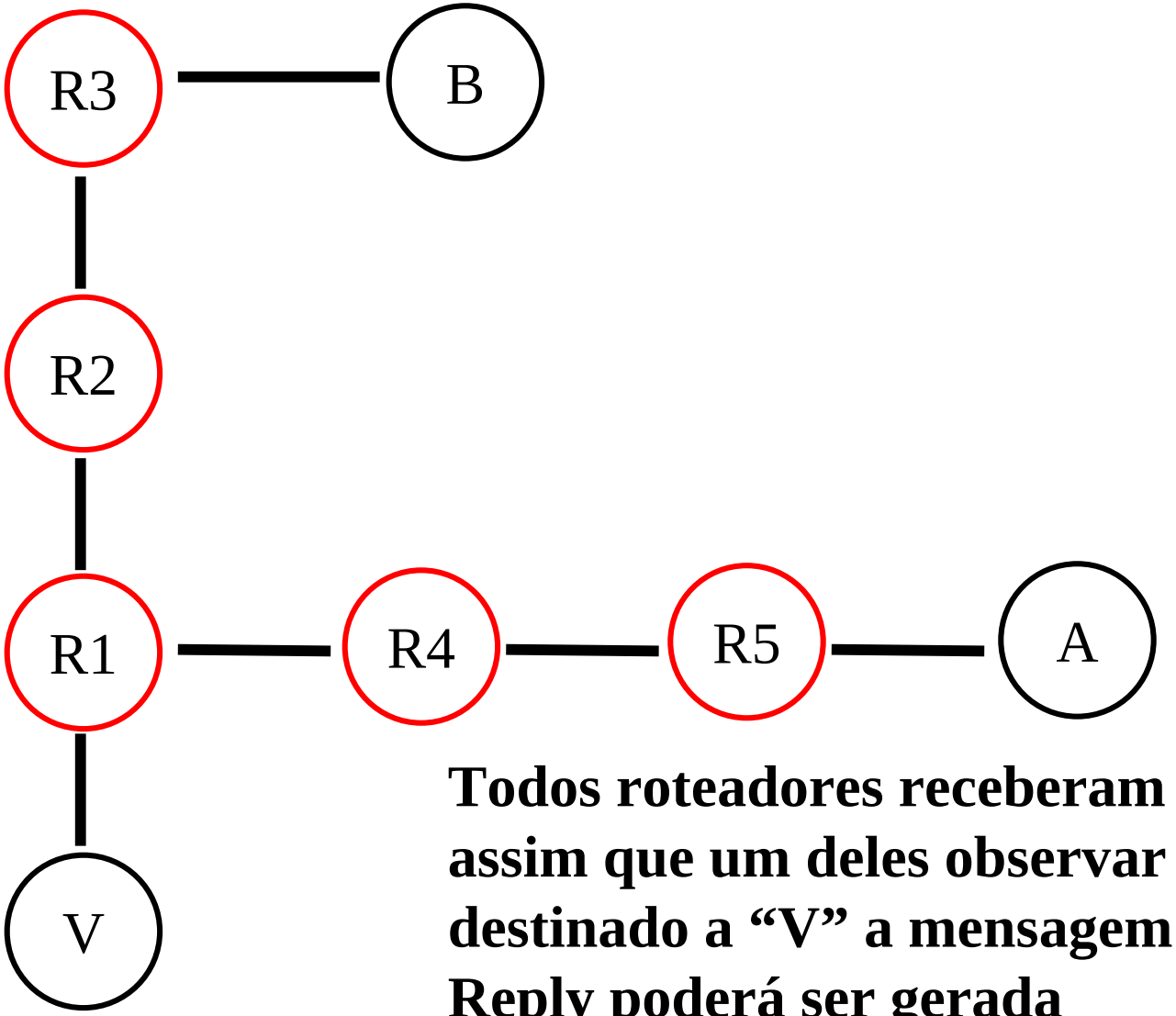
Administrador de “V” vai até roteador “R1” e envia pedido de Traceback Request para roteadores vizinhos



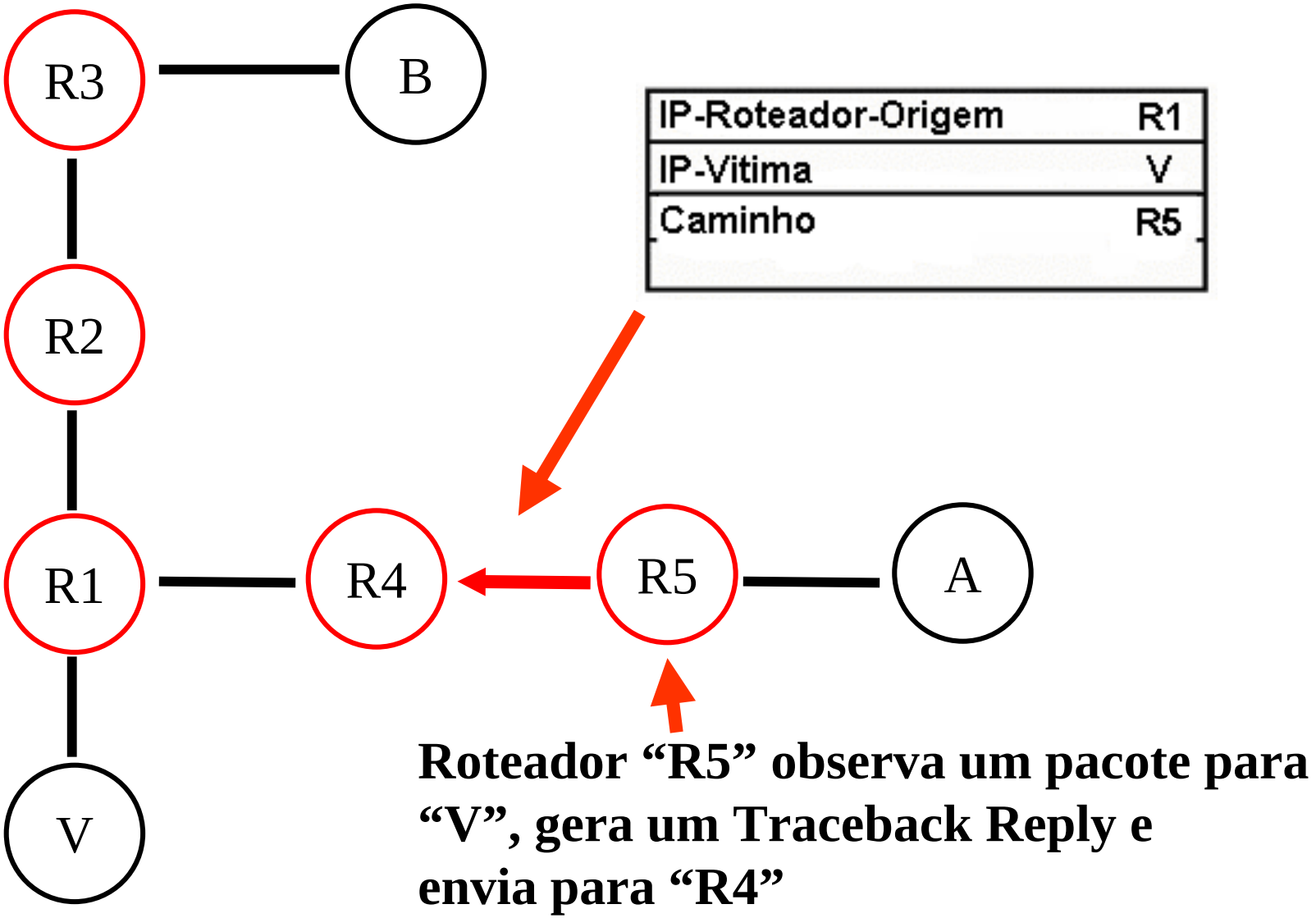
Administrador de “V” vai até roteador “R1” e envia pedido de Traceback Request para roteadores vizinhos



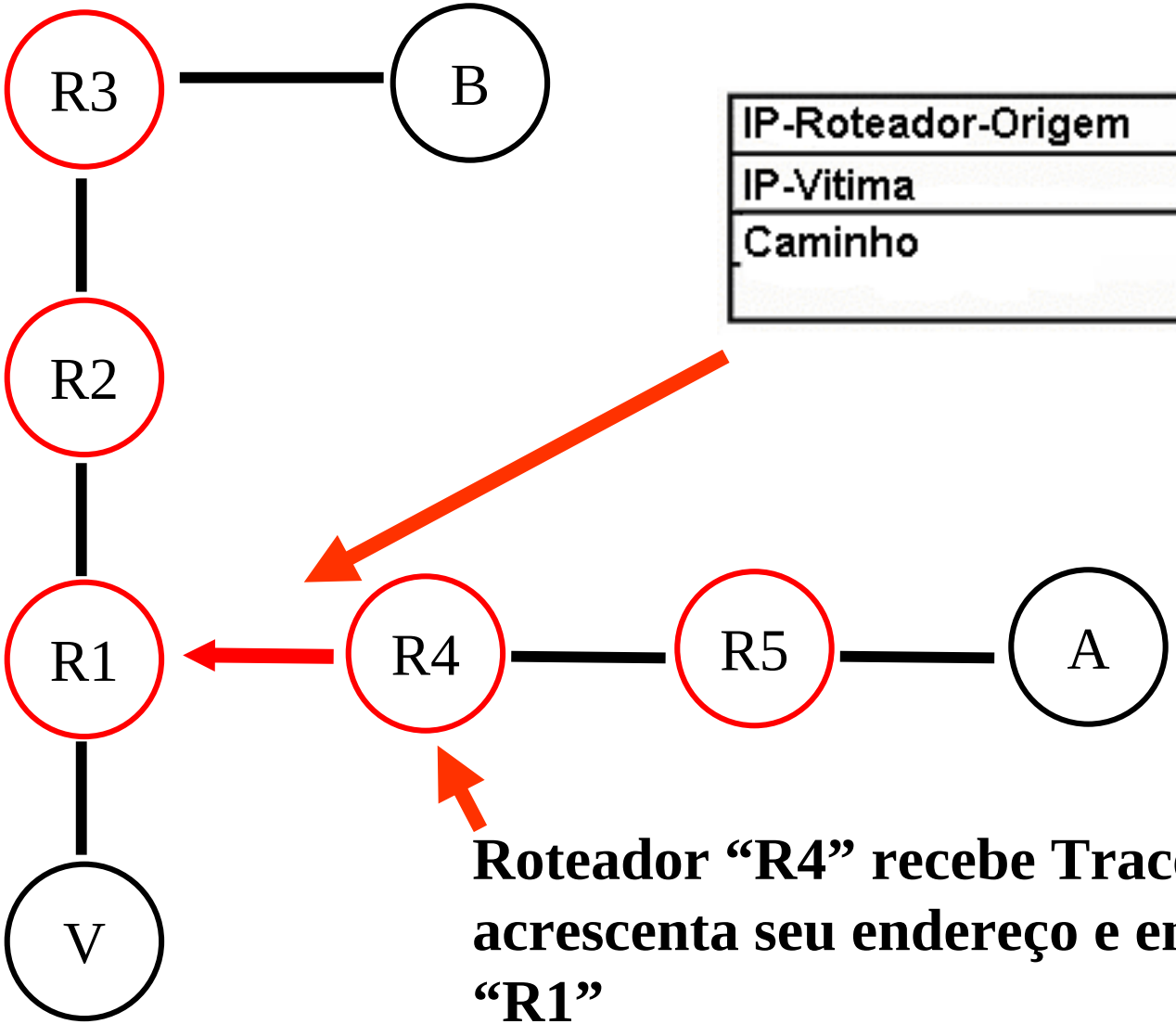
Administrador de “V” vai até roteador “R1” e envia pedido de Traceback Request para roteadores vizinhos



Todos roteadores receberam o pedido, assim que um deles observar um pacote destinado a “V” a mensagem de Traceback Reply poderá ser gerada

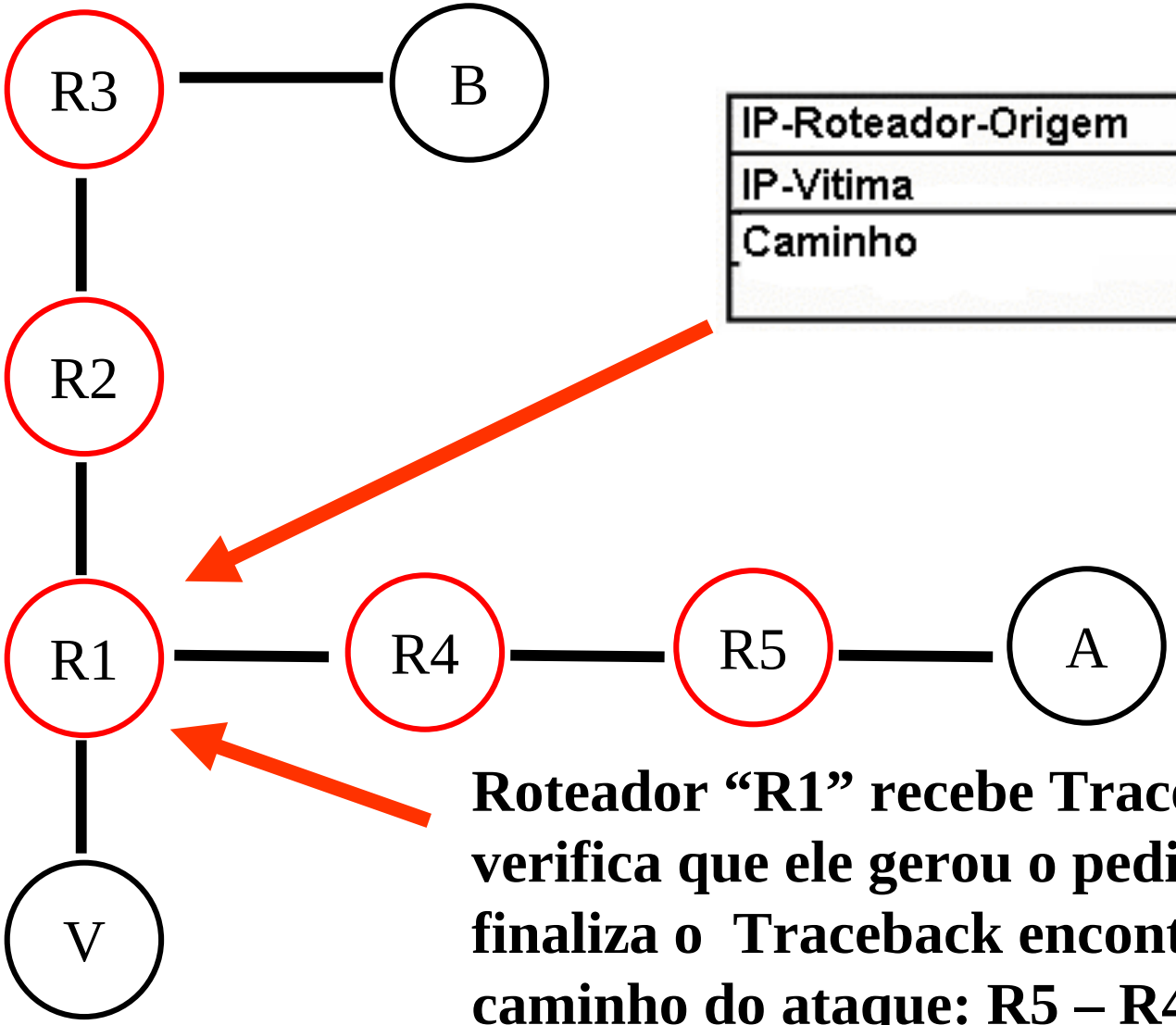


Roteador “R5” observa um pacote para “V”, gera um Traceback Reply e envia para “R4”



IP-Roteador-Origem	R1
IP-Vitima	V
Caminho	R5 R4

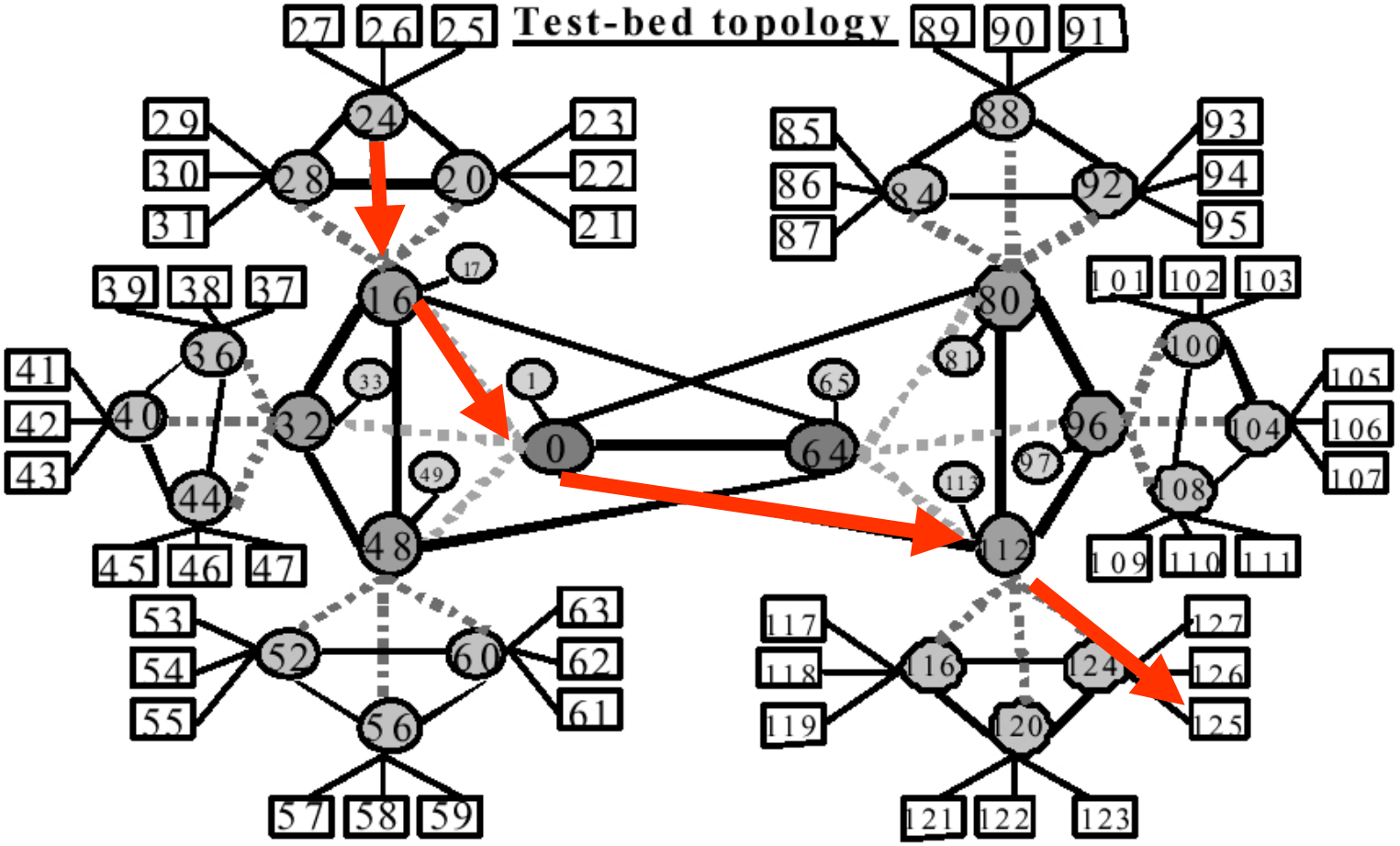
Roteador “R4” recebe Traceback Reply, acrescenta seu endereço e envia para “R1”



IP-Roteador-Origem	R1
IP-Vitima	V
Caminho	R5 R4

Roteador “R1” recebe Traceback Reply, verifica que ele gerou o pedido para “V” e finaliza o Traceback encontrando o caminho do ataque: R5 – R4 – R1

Exemplo 2


Test-bed topology
27
26
25
24
29
30
31
28
23
22
21
20
17
39
38
37
16
36
41
42
43
40
33
32
1
0
65
64
49
44
45
46
47
48
53
54
55
52
63
62
61
60
56
57
58
59
89
90
91
88
85
86
87
84
93
94
95
92
81
80
101
102
103
100
105
106
107
104
96
97
113
108
109
110
111
112
117
118
119
116
127
126
125
124
120
121
122
123

Resultados: Exemplo 2

- Comparado com ICMP Traceback
- Distância ataque: 5 roteadores
- 50 mil pacotes/seg
- Analisados 1200 primeiros pacotes do roteador da rede do atacante
  - ICMP T. gerou somente 5 pacotes destinados a vítima
  - BGP T. todos 1200 pacotes gerados são válidos

Resultados: Exemplo 2

- Primeiro pacote do ICMP T. foi gerado após o roteador encaminhar quase 6 milhões de pacotes
- BGP T. gerou primeiro pacote nos primeiros segundos de simulação
  - Isso deve-se as alterações no mecanismo de escolha dos pacotes a serem marcados
  - Isso permite reduzir o tempo de permanência dos pedidos nos roteadores e a probabilidade de marcação

Vantagens do BGP Traceback

- Somente mensagens para quem requisitou, não gerando mensagens “inúteis”
- Pode-se utilizar uma baixa probabilidade *p*
- Tráfego extra na rede é baixo
- Seguro devido ao S-BGP
- Abordagem inédita mostrou-se eficaz
- Mecanismo para pedido de Traceback é simples

Desvantagens do BGP Traceback

- Sobrecarga no processamento dos pacotes nos roteadores
- Necessário estar implantado em diversos roteadores para ter bons resultados

Considerações Finais

- Número de pacotes gerados pelo BGP Traceback:
  - Tráfego de ataque (pacotes/s): A
  - Probabilidade de Marcação: *p*
  - Tempo de permanência do pedido: T
  - Número de roteadores no caminho do ataque: n

Número pacotes 1 roteador = $A * T * p$

Número pacotes caminho do ataque = $(A * T * p) * n$

Considerações Finais (Cont.)

- Alterações propostas mostraram-se viáveis e eficazes quando se trata do mecanismo de escolha dos pacotes a serem marcados
- O método não gera pacotes “inúteis” devido as alterações propostas
- Número de pacotes gerados é baixo mas são suficientes pra identificar a origem conforme os cenários de simulação

Considerações Finais (Cont.)

- A existência do ataque é de conhecimento do administrador
- A proposta possui um mecanismo para estipular a distância máxima de alcance do Traceback Request, mas não foi apresentada para simplificar o entendimento

Contato:

Denilson V. Martins

denilson@ravel.ufrj.br