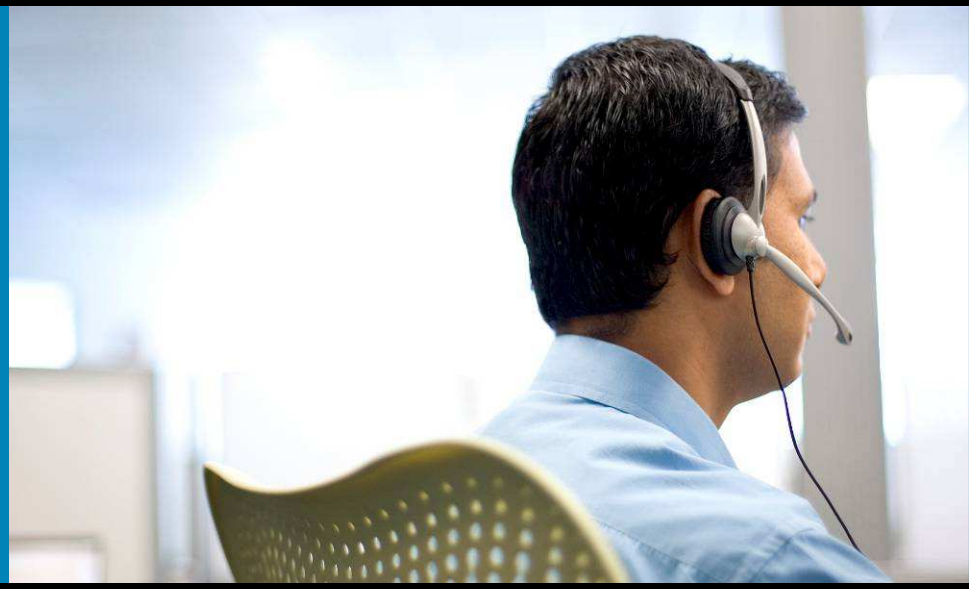
Ataques de Negação de Serviço (DoS / DDoS)

Técnicas de Mitigação utilizando a Rede



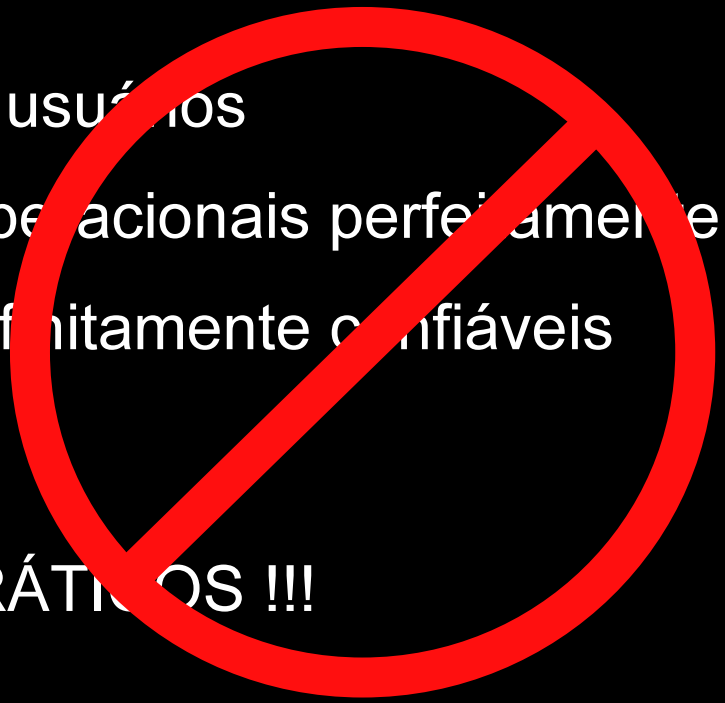
Andrey Lee
Engenheiro de Sistemas
Service Providers

Agenda

- Introdução
- Anatomia dos Ataques
- Mecanismos de Defesa, Detecção e Mitigação
- Conclusão

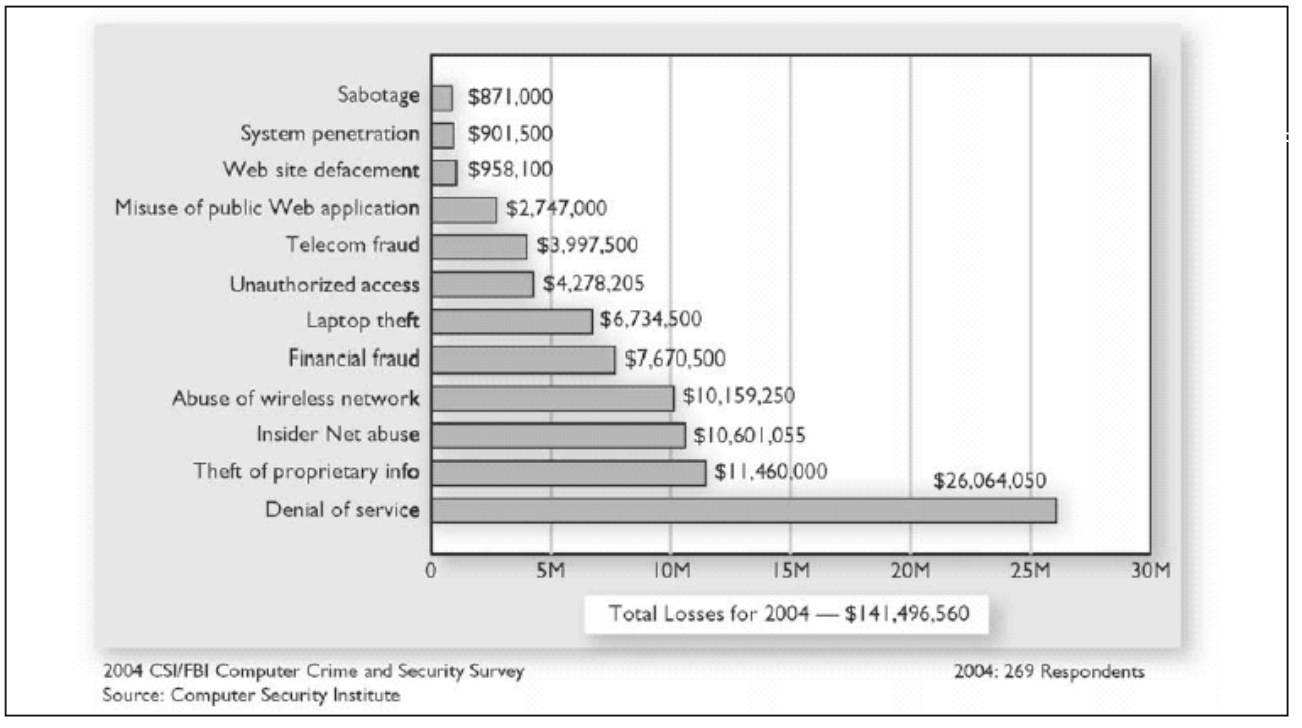
Solução para ataques de N.d.S.

- Eliminar os usuários
- Sistemas Operacionais perfeitamente seguros
- Hardware infinitamente confiáveis



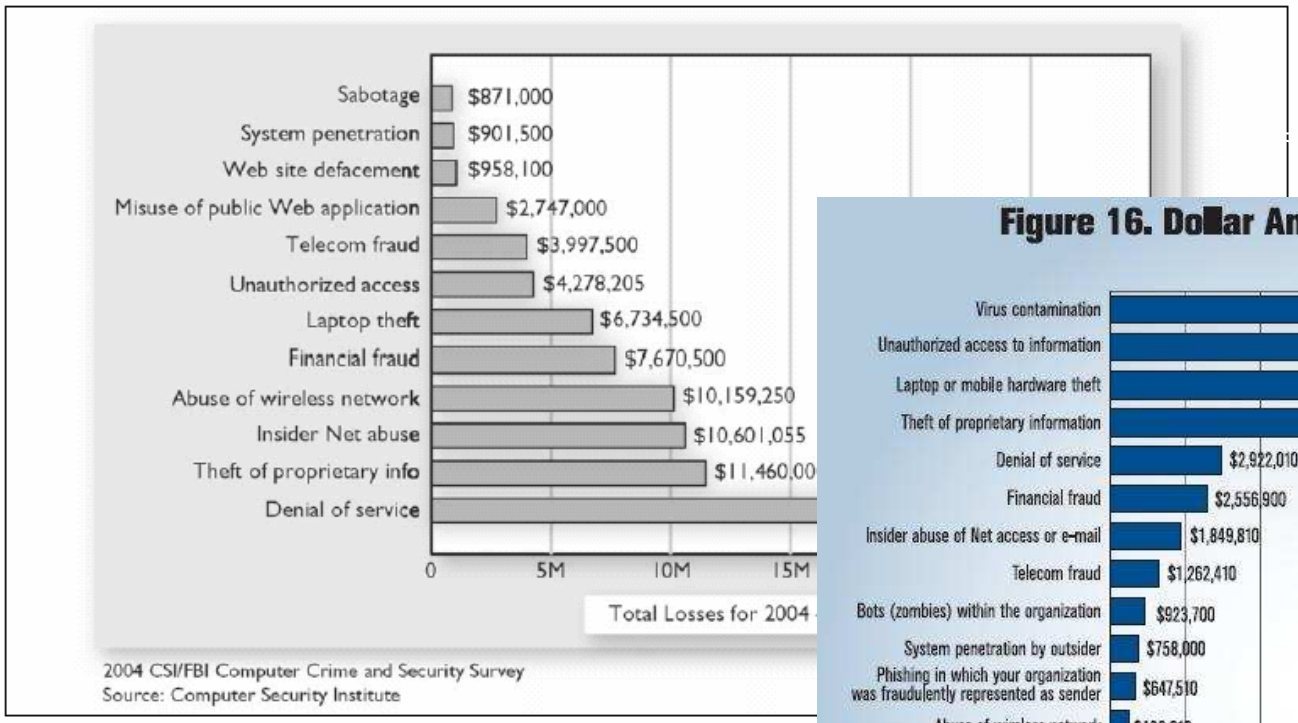
Vamos ser PRÁTICOS !!!

O Custo da Negação de Serviço

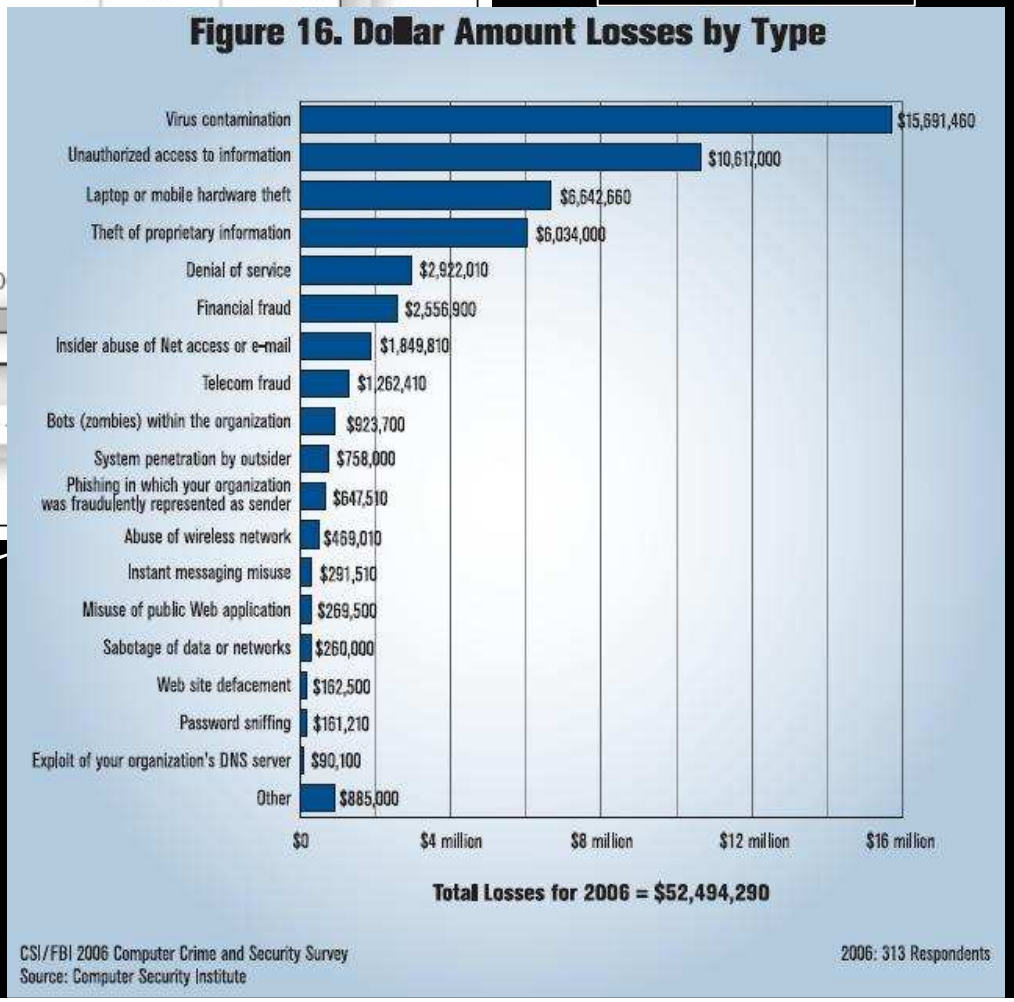


2004: #1
26 MUSD

O Custo da Negação de Serviço

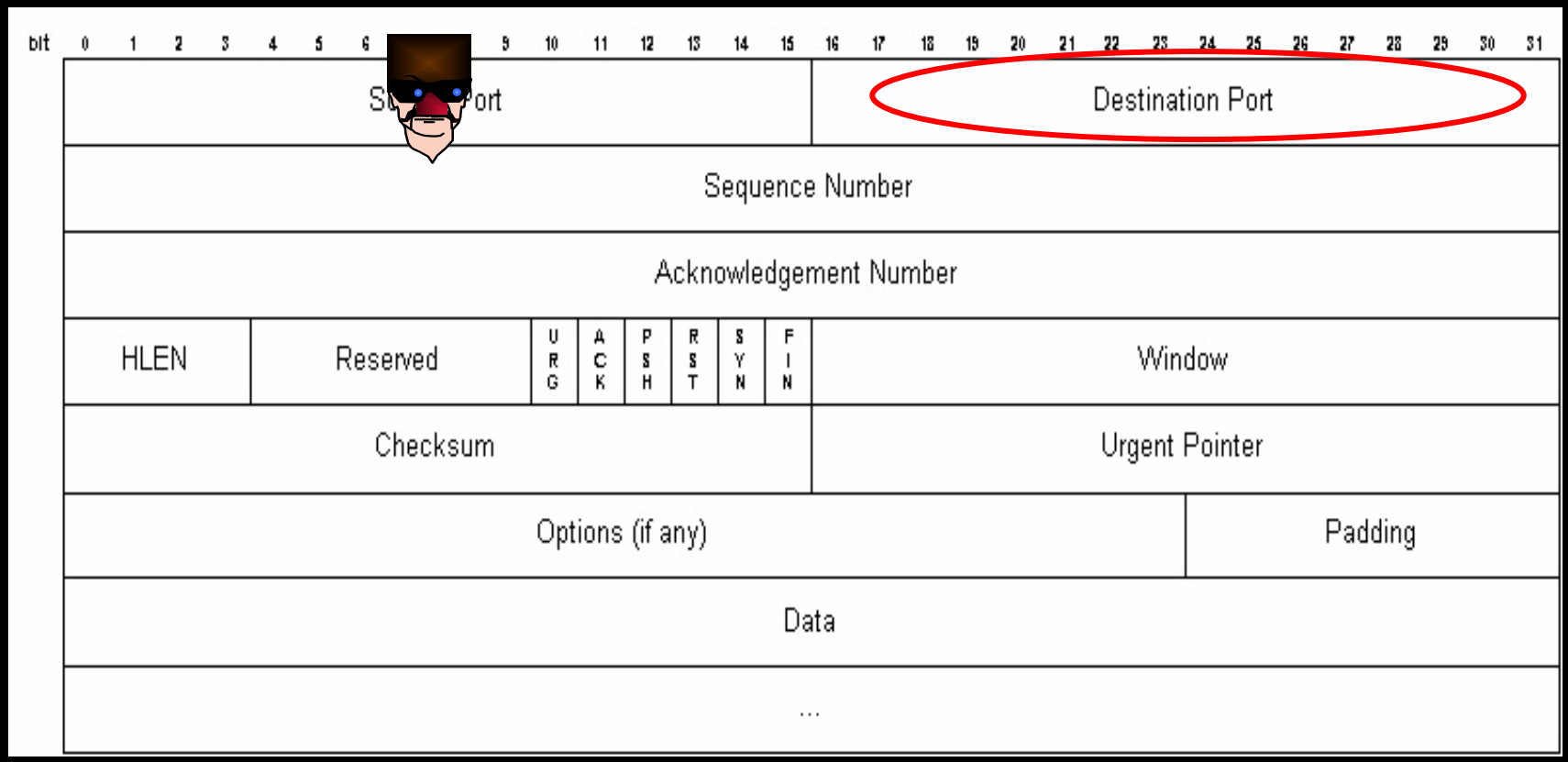


2004: #1
26 MUSD



2006: #5
3 MUSD

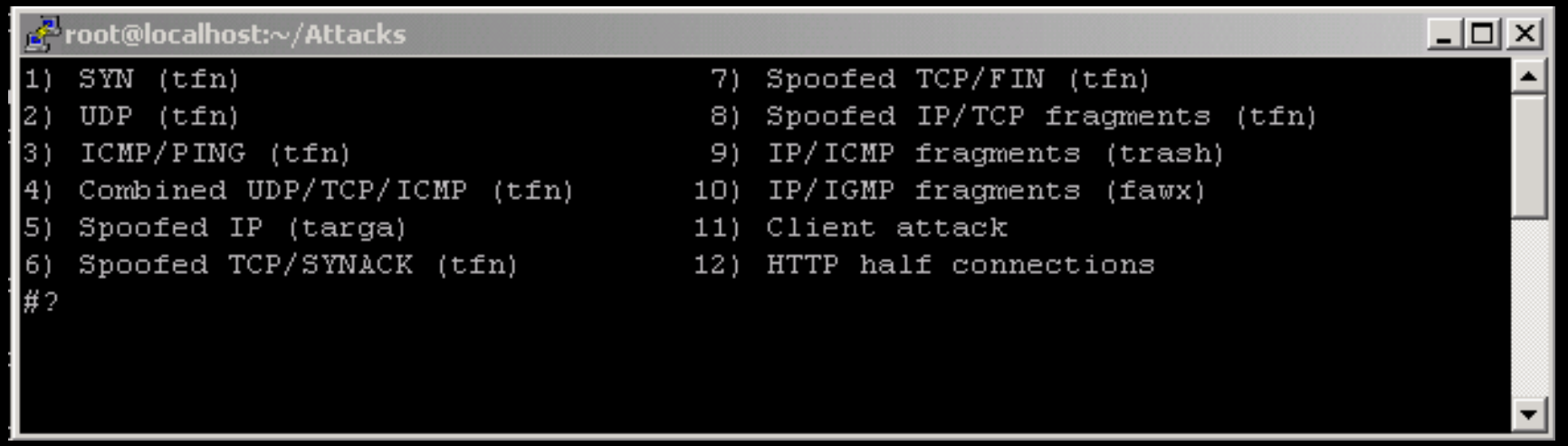
A principal causa dos ataques N.d.S.



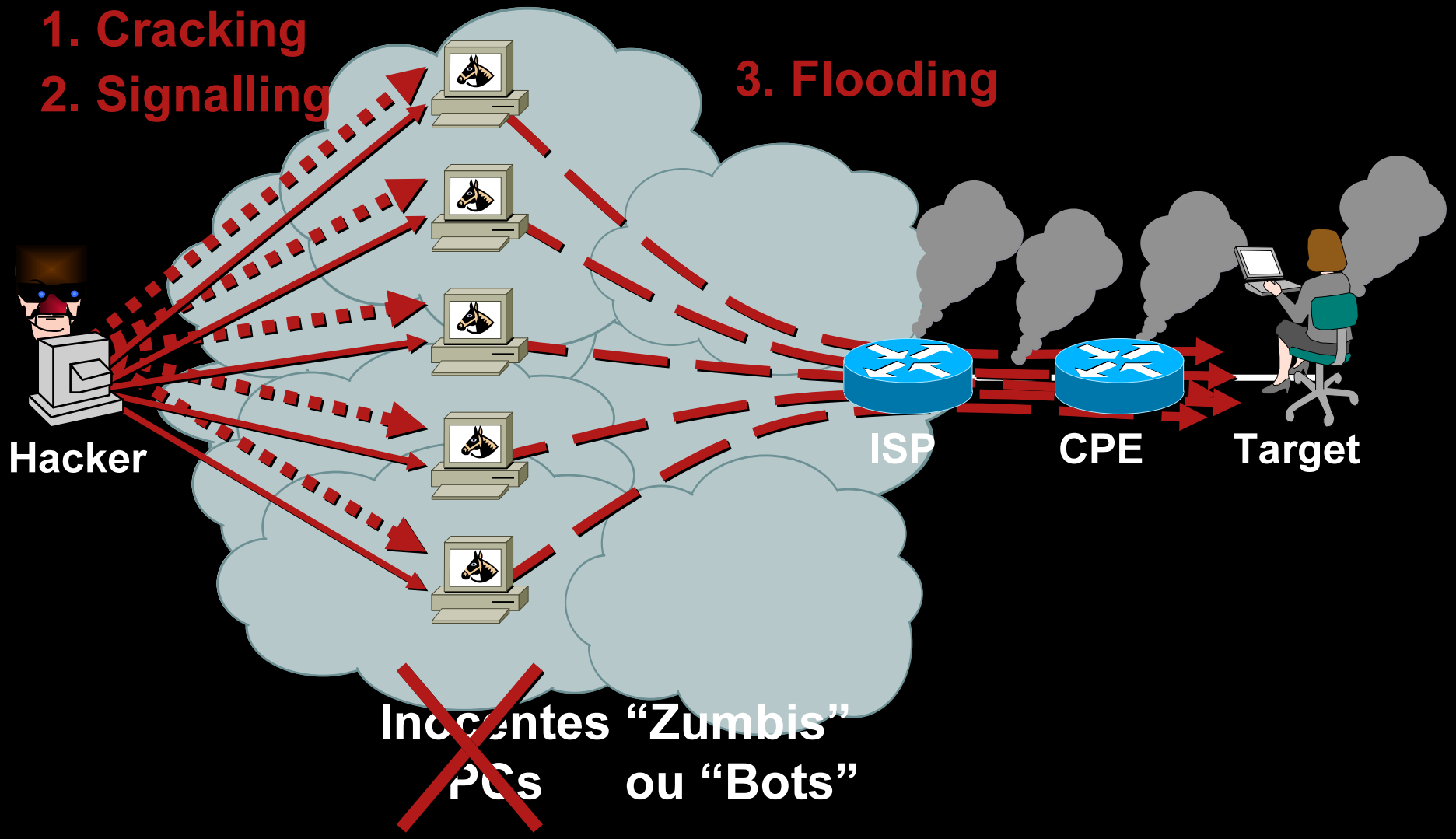
SPOOFING

Tipos de Ataques de N.d.S

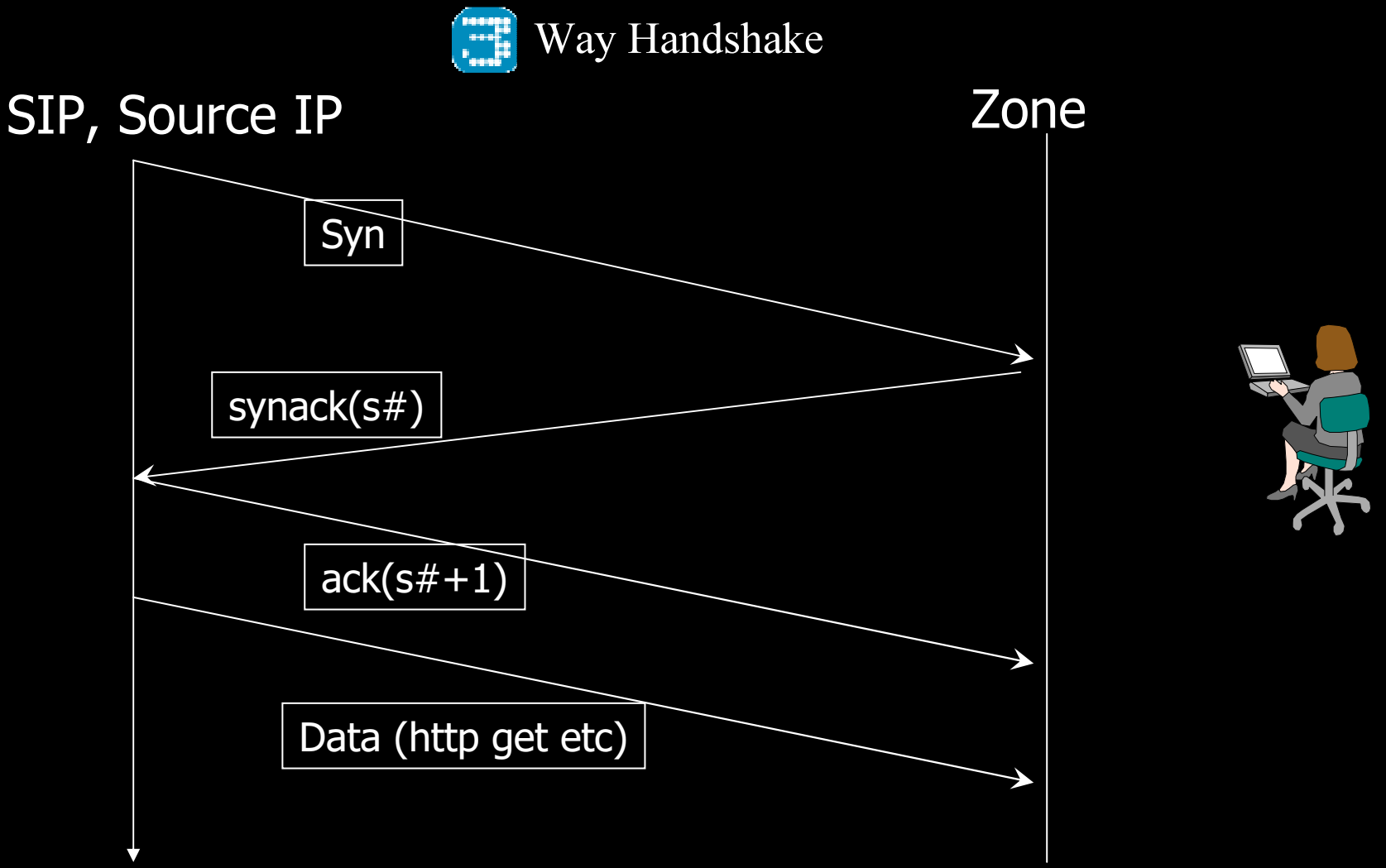
- Ataques por Inundação
- Ataques por Refletor
- Ataques por Vulnerabilidade
- Ataques Distribuídos (DDoS)



Ataques de N.d.S Distribuídos



TCP – Protocolo orientado a conexão

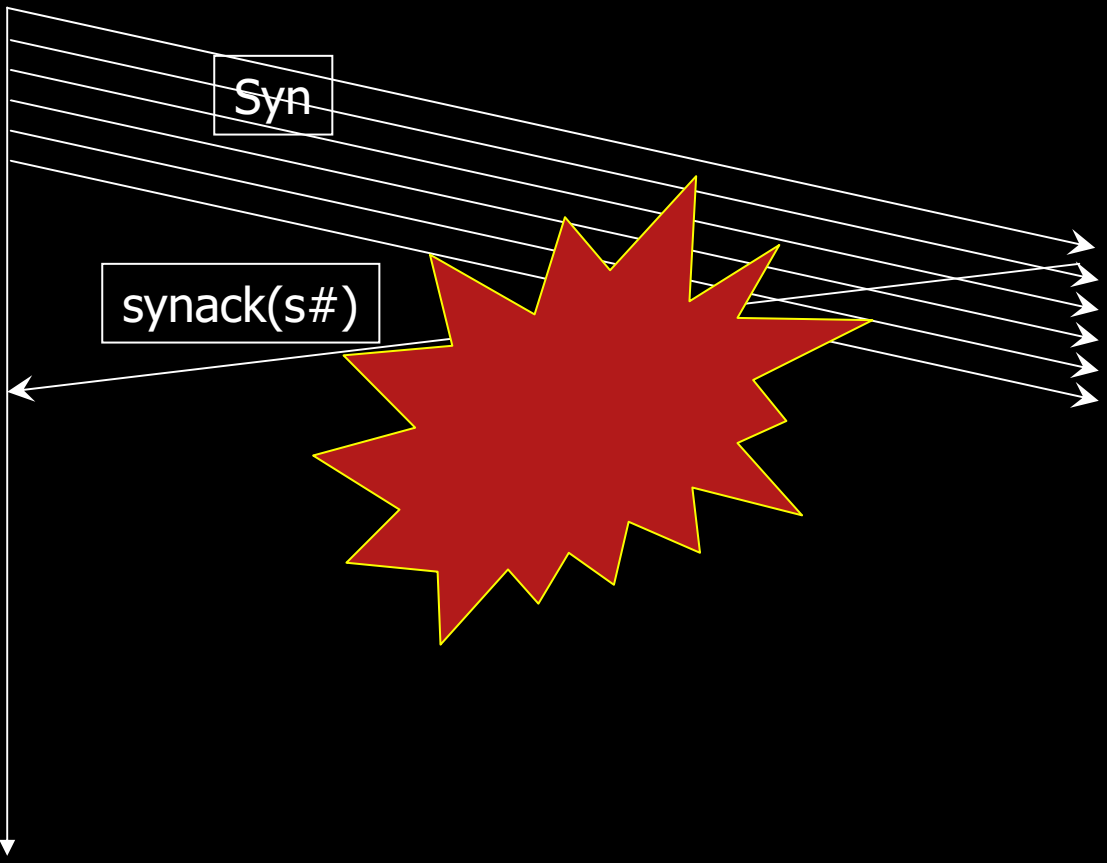


TCP Syn Flood

Way Handshake

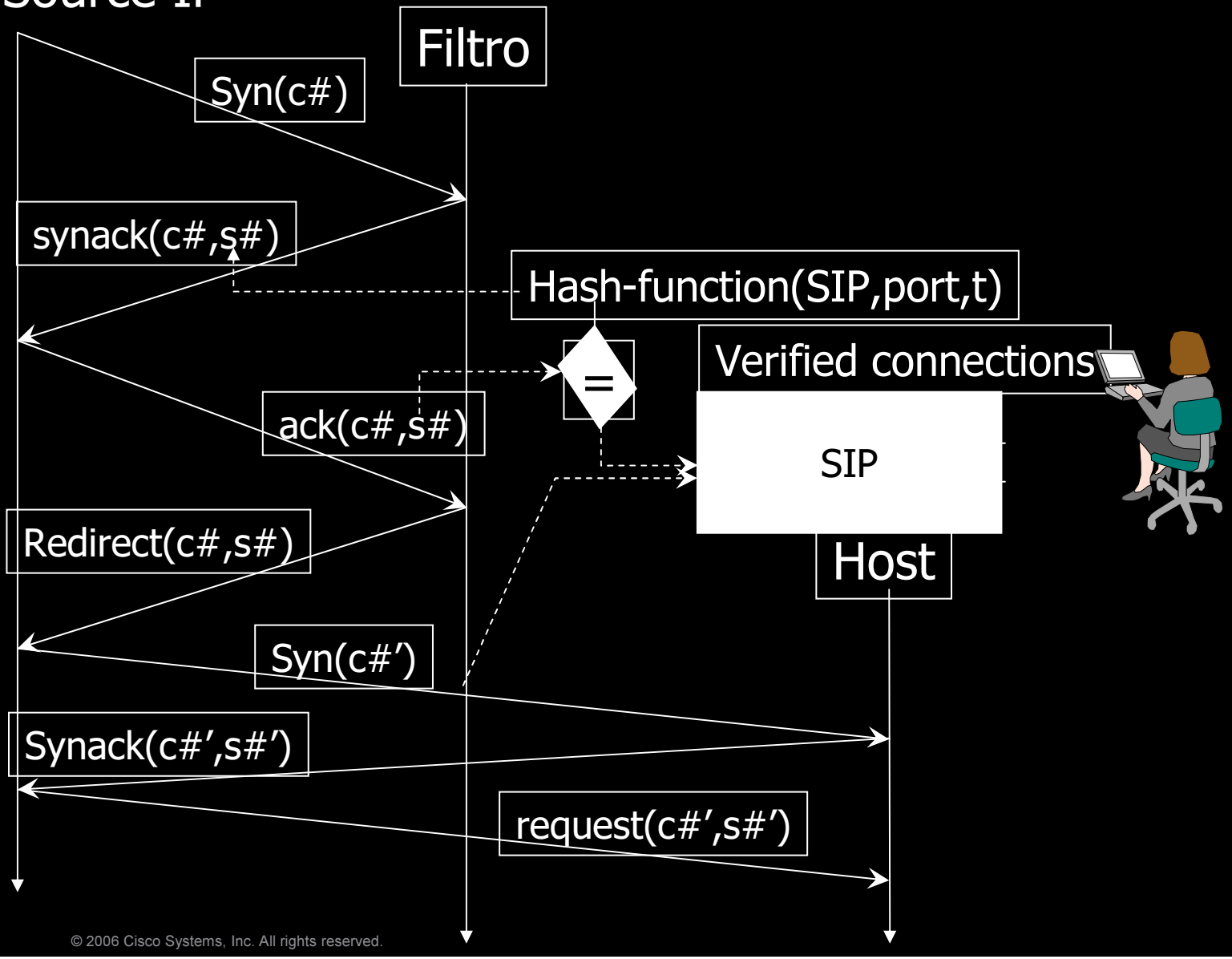
SIP, Source IP

Zone



Filtros Anti-Spoofing

SIP, Source IP



As 6 fases de resposta ao ataque

Preparação / Prevenção

- Manter Sistemas Operacionais atualizados
- Elementos de segurança: Stateful Firewalls, IPS / IDS, criptografia de dados e outros
- Limitar banda por tipo tráfego (QoS)
- Endereços IP não utilizados (Dark IP)
- Contingência
- Anycast

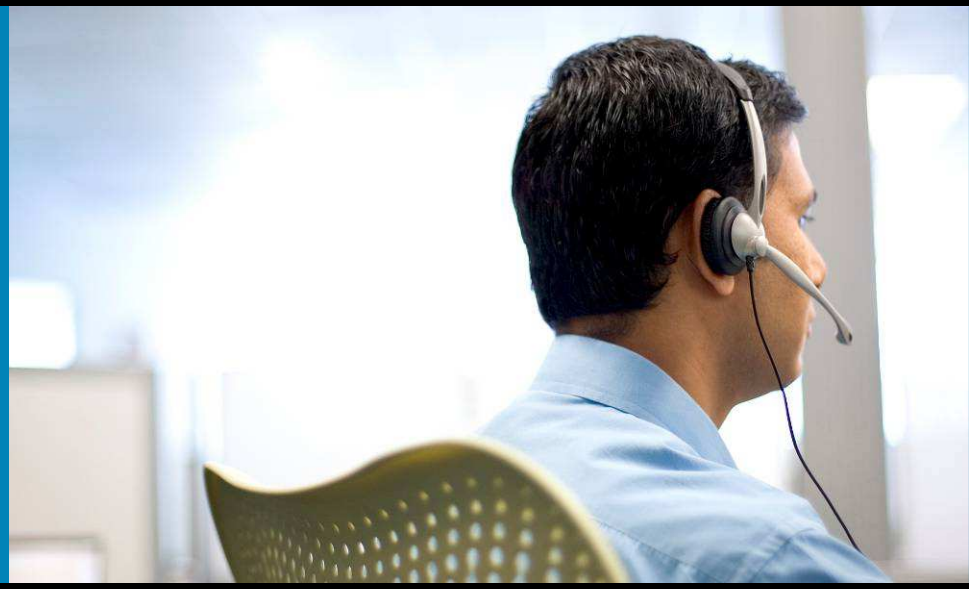
Identificação / Detecção

- Reclamações de Usuários
- Monitoração da CPU (SNMP)
- Monitoração do Tráfego (IP Flow)
- Backscatter

Exemplos de Gráficos do MRTG / RRDTool

Fontes: mrtg.org
http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

A Rede como uma Ferramenta de Segurança



Usando a rede como ferramenta contra ataques N.d.S

- A Rede IP pode ser utilizada como um meio para manipular o tráfego malicioso:

  Listas de Acesso (ACLs)

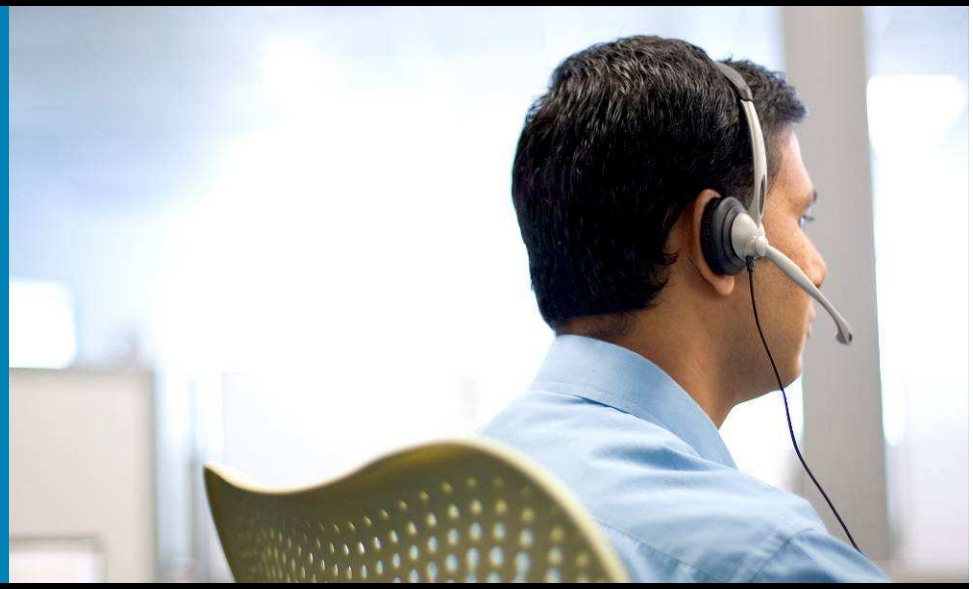
  Black Hole

  Sink Hole

  uRPF

  IP Flow

Listas de Acesso



Identificando ataques com ACLs

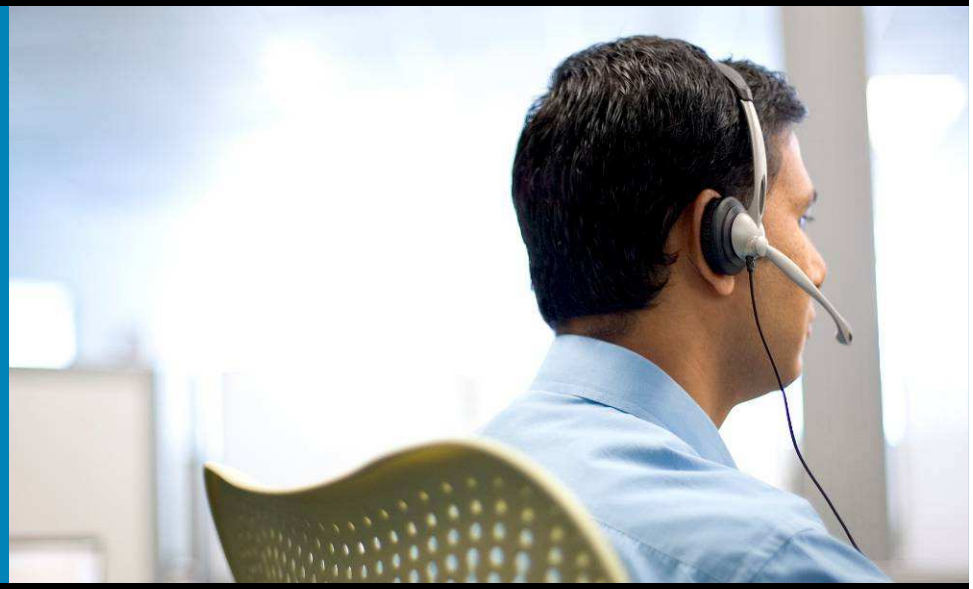
- Requer que a ACL esteja configurada (para detecção)

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches
```

Detectado:
- **Tipo de Ataque**
- **Interface**

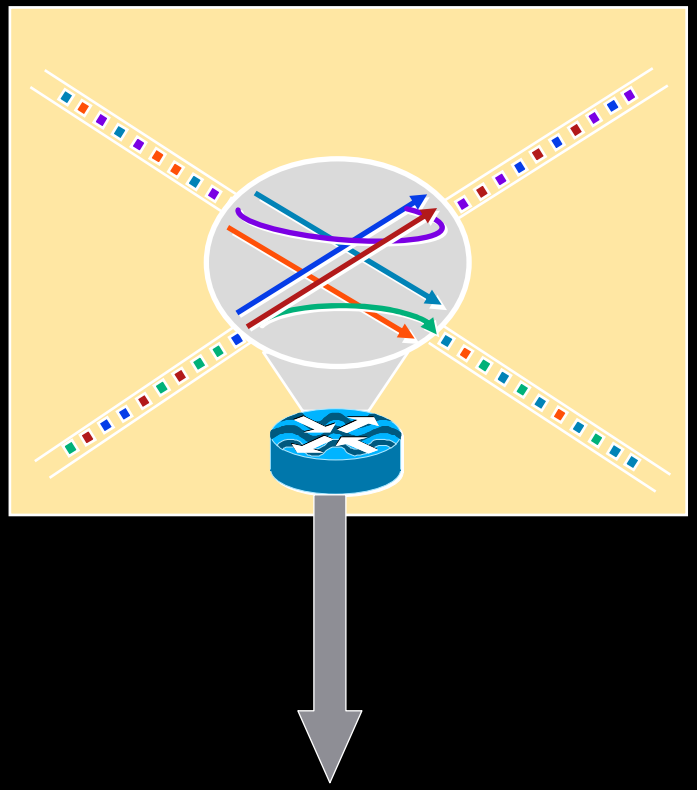
- Usada sob demanda (reativo)
- Mais utilizada para identificar do que detectar
- Depende do roteador

IP Flow



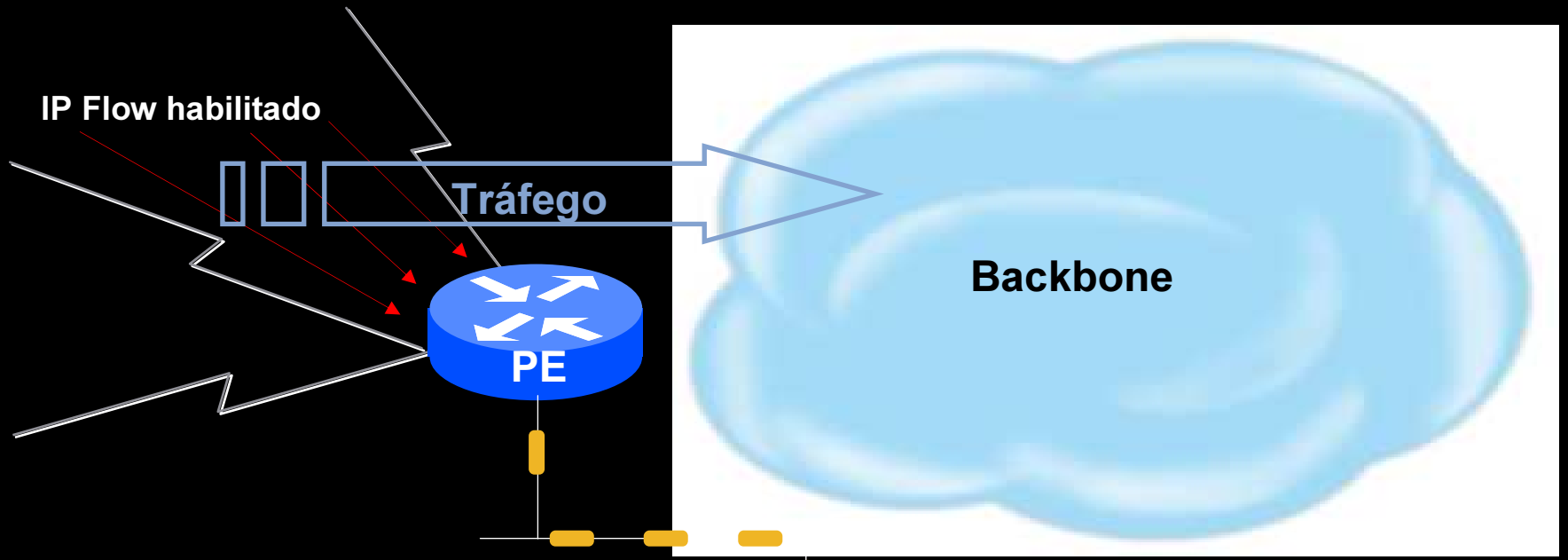
O que é um Fluxo (Flow) ?

- Um flow é definido por sete informações:
  - Source IP address
  - Destination IP address
  - Source port
  - Destination port
  - Layer 3 protocol type
  - TOS byte (DSCP)
  - Input logical interface (ifIndex)



Dado Exportado

Criando Pacotes para Exportação



Pacotes Exportados

- Approximadamente 1500 bytes
- Typicamente contém 20-50 fluxos de informação
- A frequência de envio aumenta se o tráfego aumenta nas interfaces

Coletor
NFC, cflowd, flow-tools, Arbor

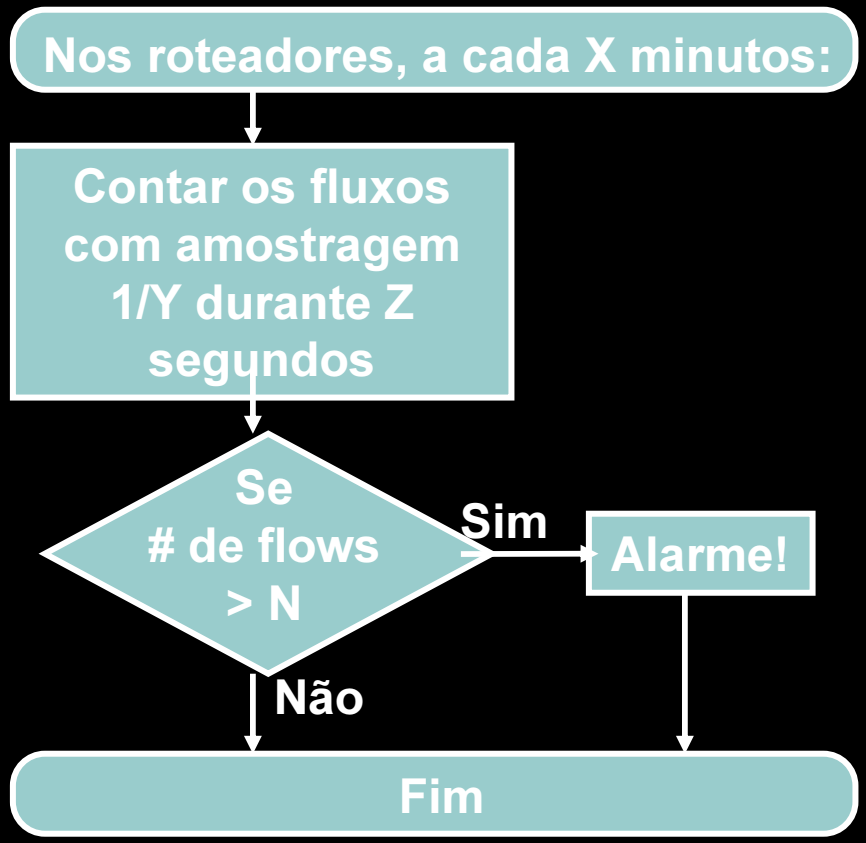
Aplicação Gráfica
Arbor, FlowScan

Princípios do IP Flow v9

- A Versão 9 é um formato exportável
- Modelo ‘Push’
- Envia as informações regularmente (configurável)
- Independe do protocolo base, pode também ser utilizado por qualquer protocolo confiável (TCP, SCTP)

Detectando ataques com o IP Flow

- Base: IP Flow ativado na rede



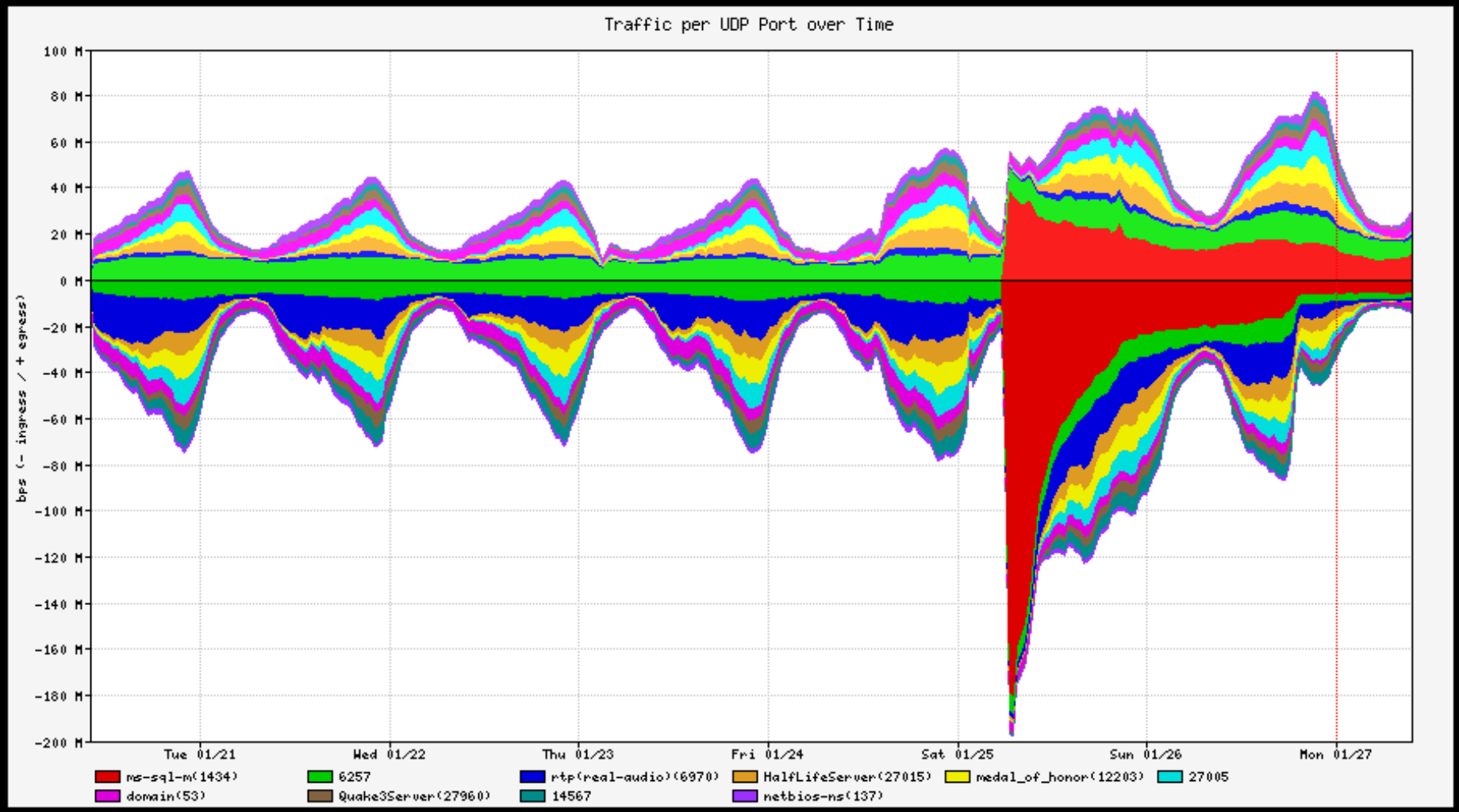
Examplo:
X=15 min, Y=200,
Z=10 seg, N=10

Valores empíricos

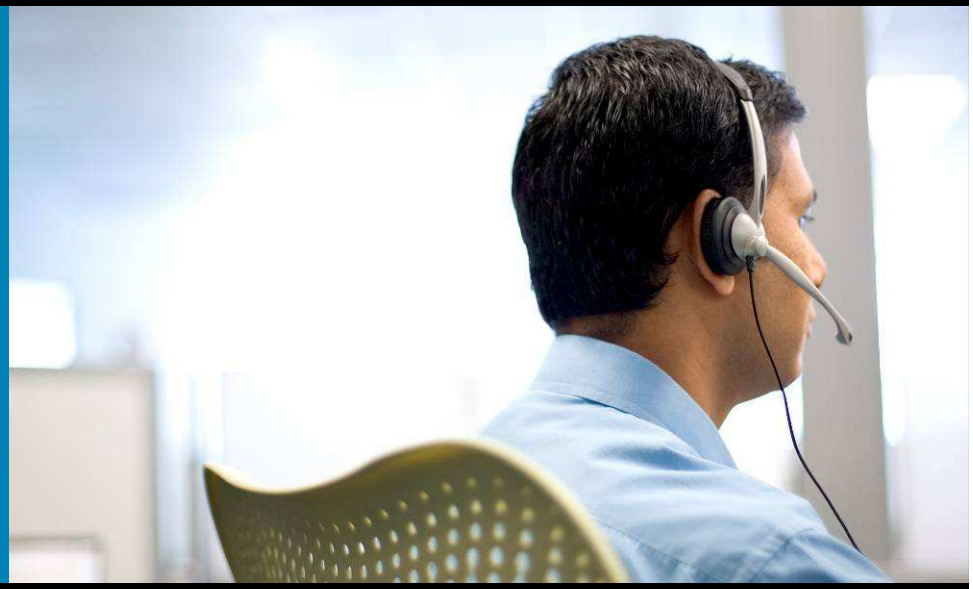
Ferramentas IP Flow

- OSU Flow-Tools
  - Open source IP Flow collection and retrieval tools
  - Developed and maintained by Mark Fullmer, available from http://www.splintered.net/sw/flow-tools/
  - Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
  - Data can be batched and imported into database such as Oracle, MySQL, Postgres, etc.
- Flow Scan
  - Open source IP Flow graphing/visualization tools
  - Developed and maintained by Dave Plonka, available from http://net.doit.wisc.edu/~plonka/FlowScan/
  - Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
  - Makes use of IP Flow data collected via flow-tools to build traffic graphs

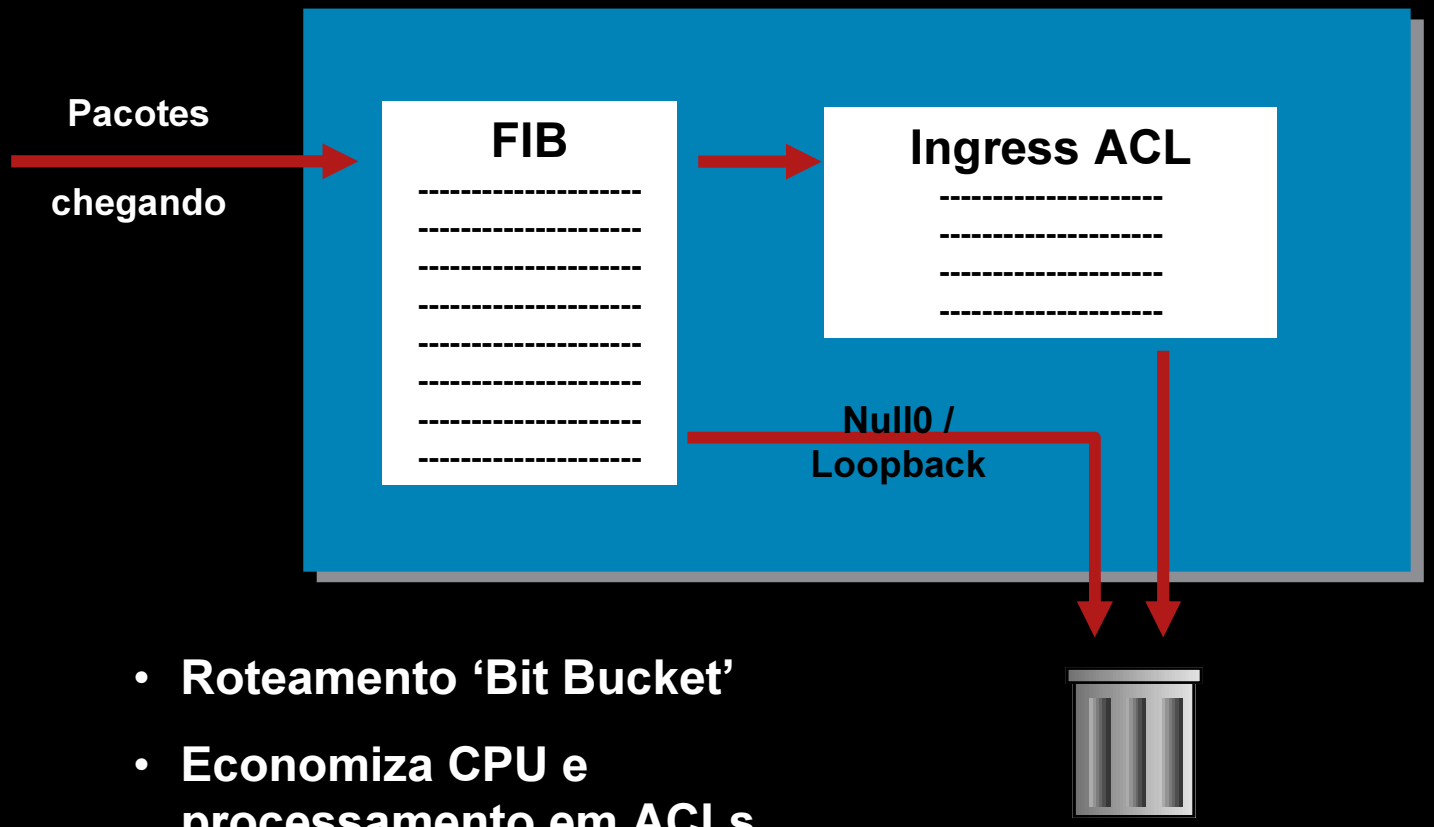
Exemplo – Gráfico baseado no IP Flow



Filtragem via Buraco Negro

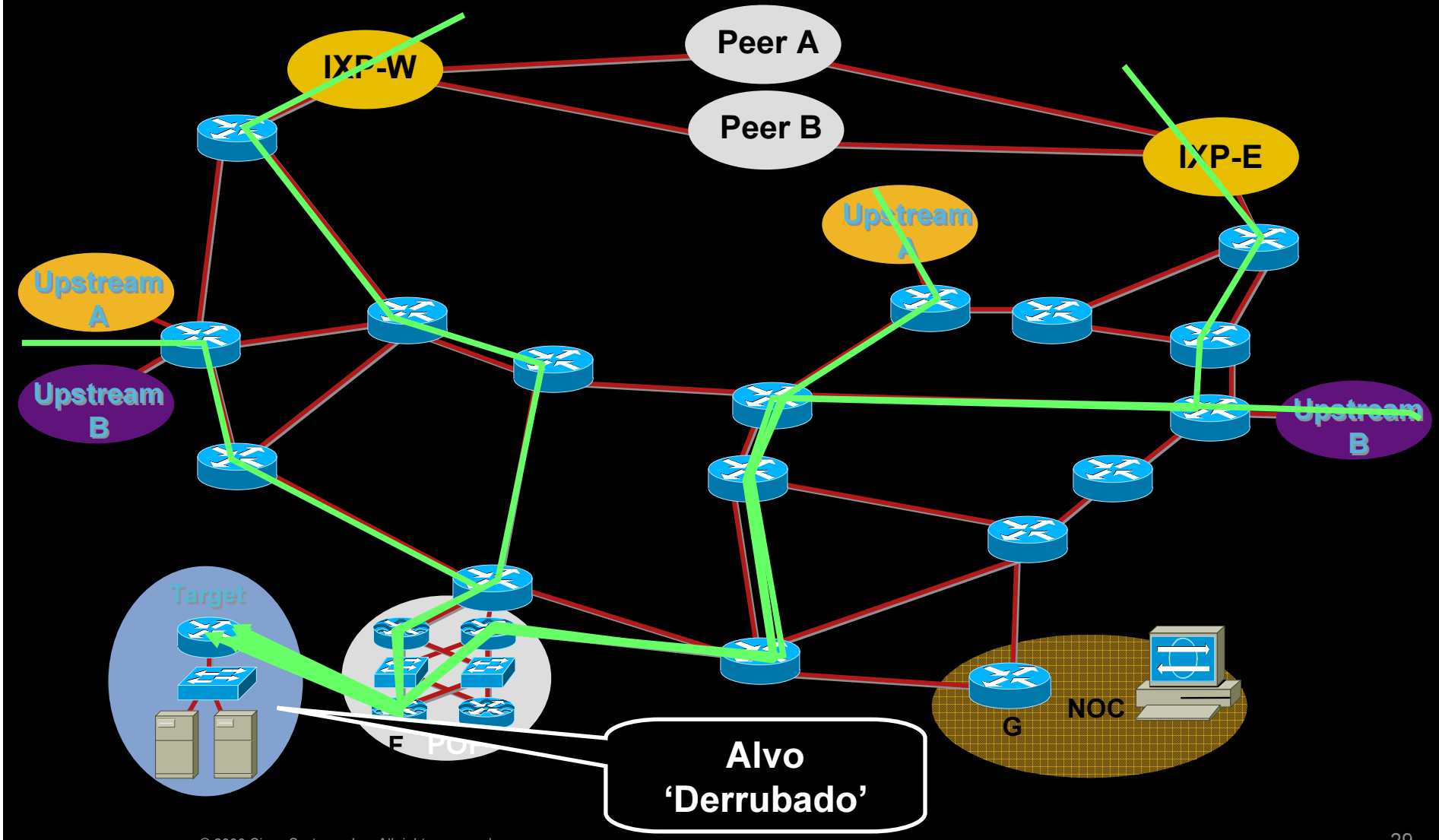


Filtragem Black Hole (Buraco Negro)

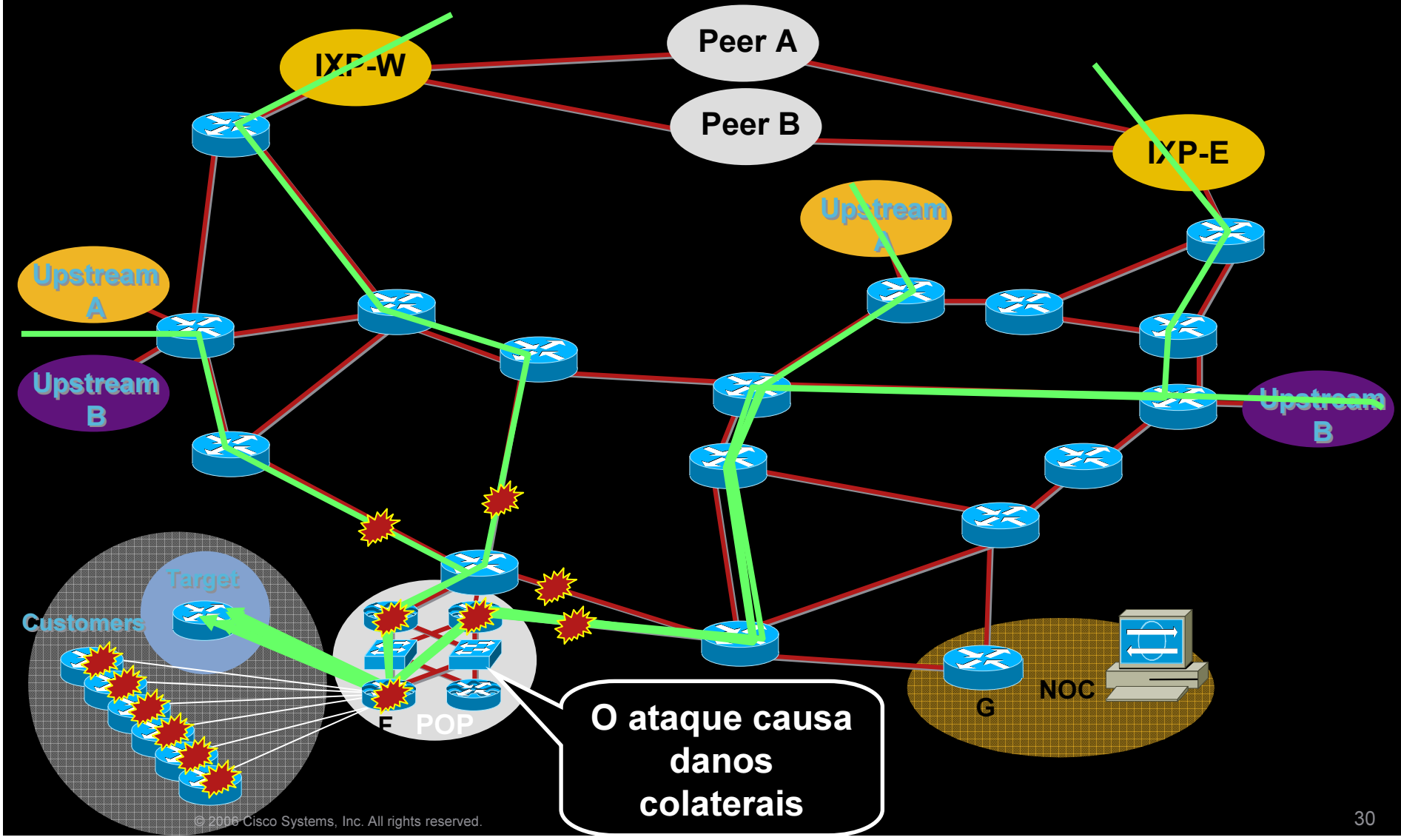


- Roteamento ‘Bit Bucket’
- Economiza CPU e processamento em ACLs

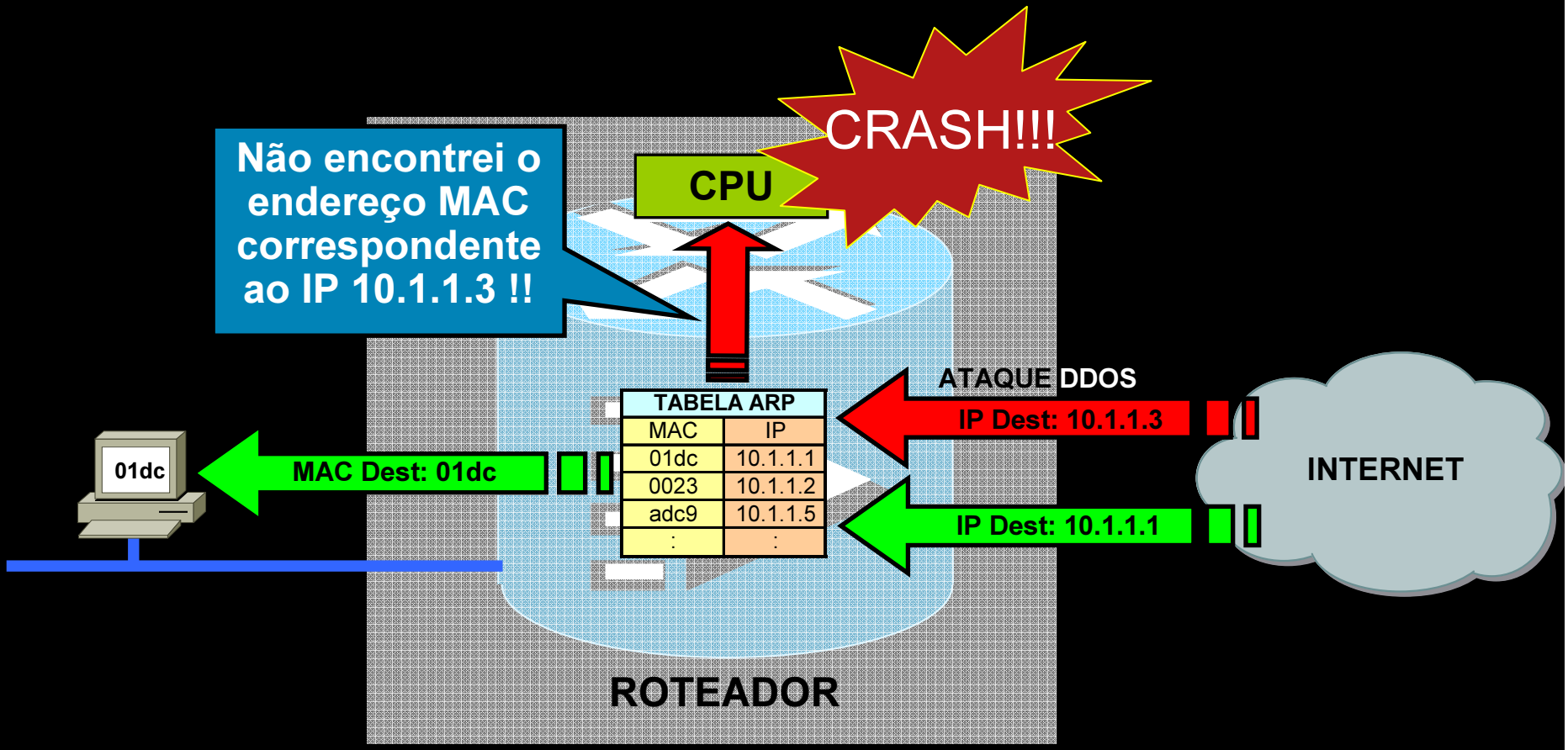
Rede sob Ataque – Antes



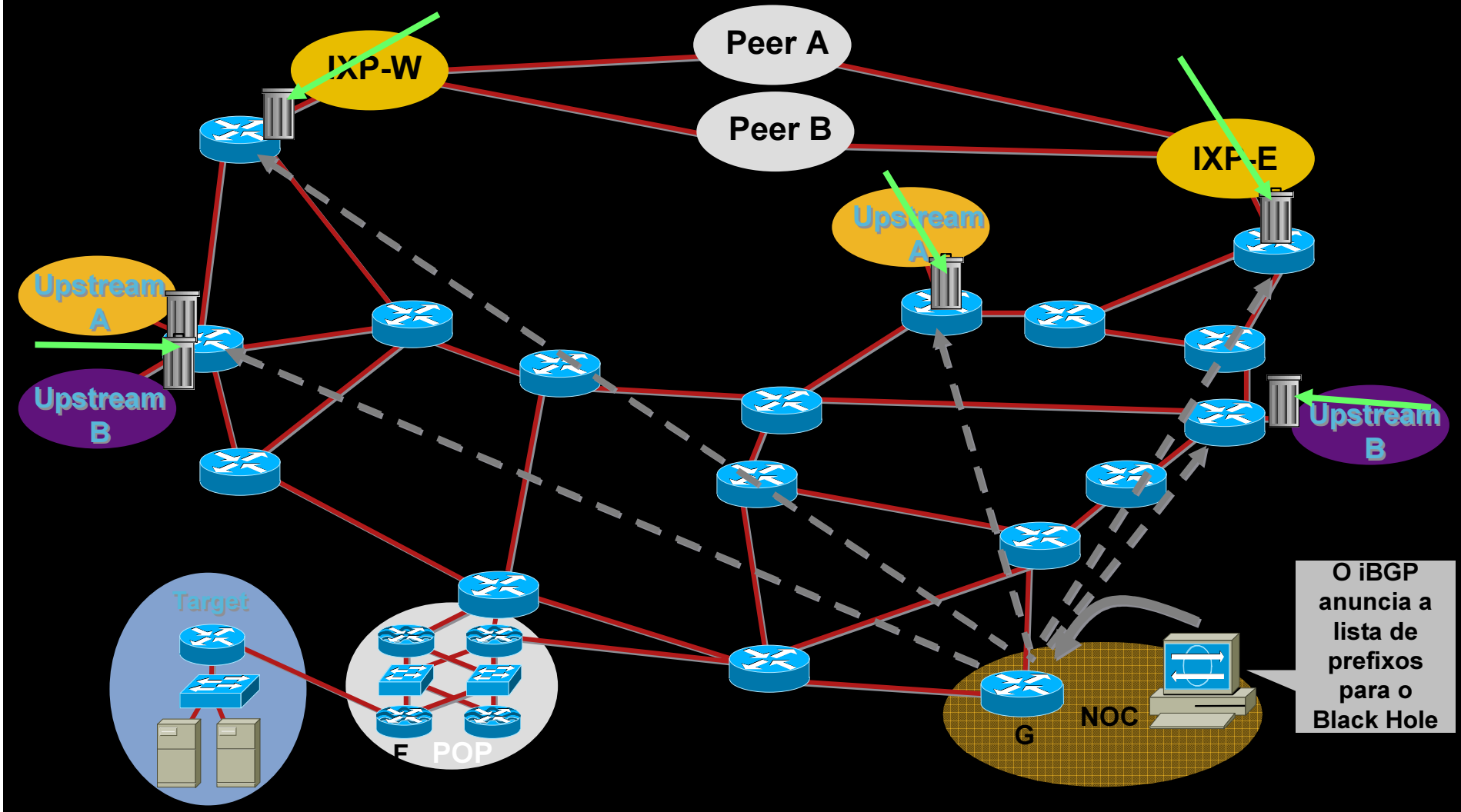
Rede sob Ataque – Antes – Danos Colaterais



Rede sob Ataque – Antes – Danos Colaterais no Roteador



Rede sob Ataque – Depois – O ataque é descartado na entrada



Remote Triggered Black Hole (RTBH)

- Filtragem por ‘Remote Triggered Black Hole’ é a base para uma série de técnicas de rastreamento e mitigação a ataques de Negação de Serviço nas redes dos Provedores Internet.
- A preparação não afeta a performance ou a operação da rede.
- Uma ferramenta essencial de segurança

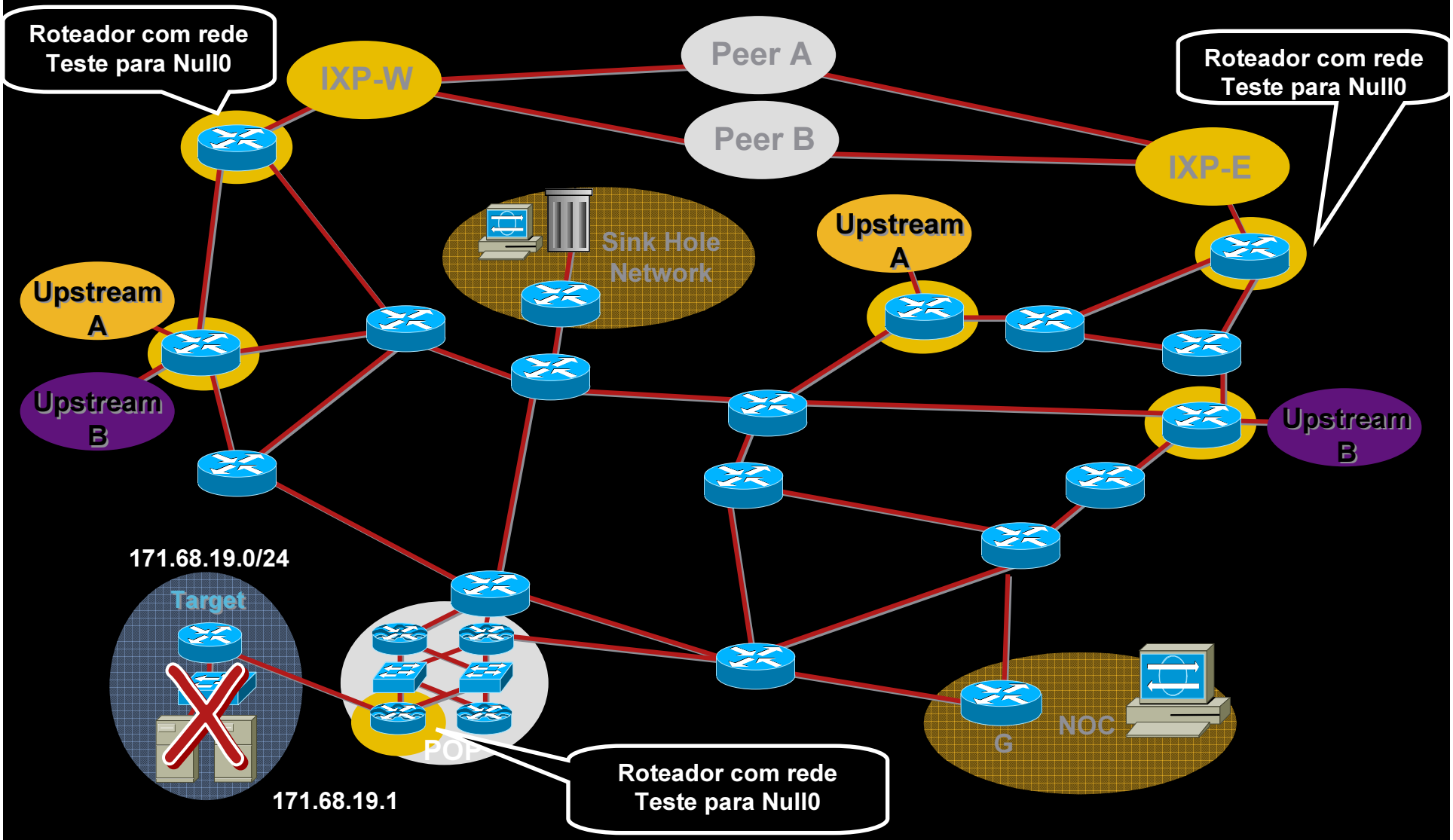
Passo 1- Preparar todos os roteadores com o ‘gatilho’

Selecione um pequeno bloco de endereços que não será utilizado para nada a não ser filtragem Black Hole. A rede de teste (192.0.2.0/24) é ideal pois não é válida na Internet e dificilmente é utilizada.

Coloque uma rota estática na rede de teste – 192.0.2.0/24 para Null 0 em cada roteador da rede:

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Passo 1- Preparar todos os roteadores com o ‘gatilho’



Passo 2 – Preparar o roteador gatilho

- O roteador gatilho é o dispositivo que injetará a rota iBGP na rede.

  Deve ser parte da malha iBGP – mas não deve ter rotas válidas

  Pode ser um roteador à parte (recomendado)

  Pode ser um roteador de produção (alguns provedores implementam dessa forma)

  Pode ser uma estação com capacidade de roteamento (interface com Perl scripts ou outras ferramenta).

Passo 3 – Ativar o Black Hole

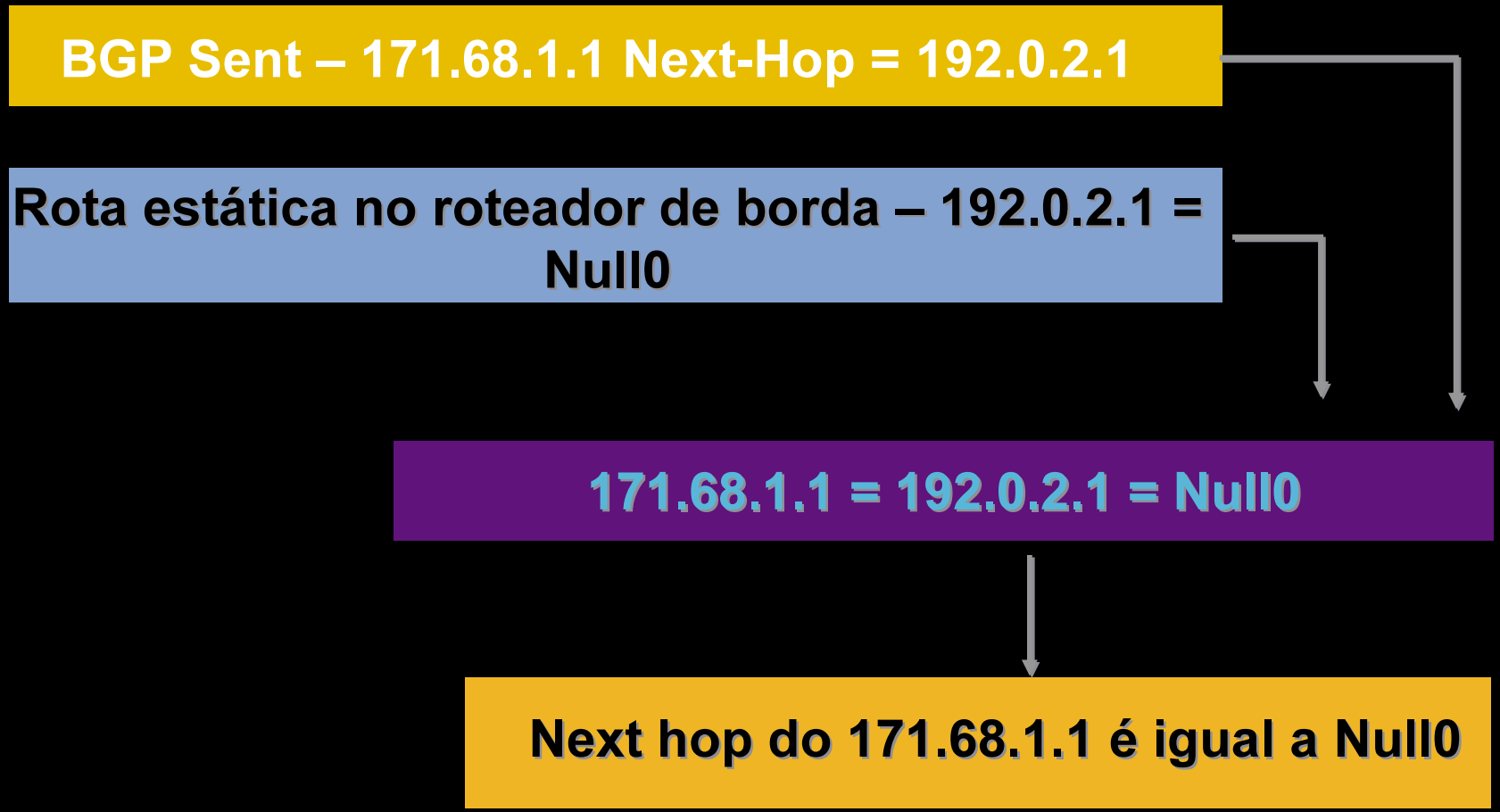
O administrador da rede insere uma rota estática para o endereço destino cujo tráfego ele queira enviar ao black hole. A rota é adicionada com um “tag” para identificar essa rota de outras rotas estáticas da tabela de roteamento.

```
ip route 171.68.1.1 255.255.255.255 Null0 Tag 66
```

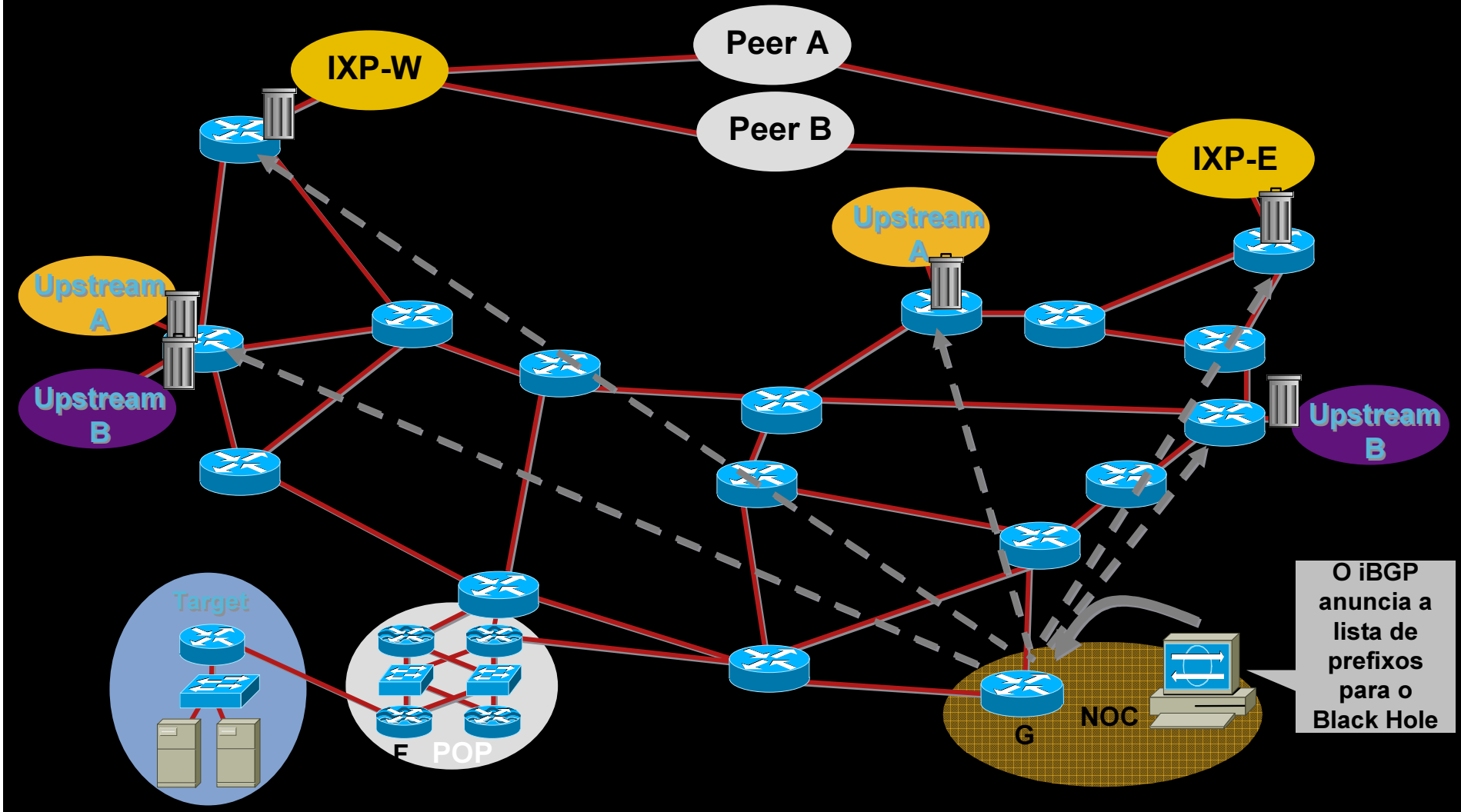
O anúncio BGP irá para os roteadores que falam BGP.

O roteador recebe o anúncio, insere a rota na tabela e muda o next-hop para a interface Null0 – habilitando o Black Hole.

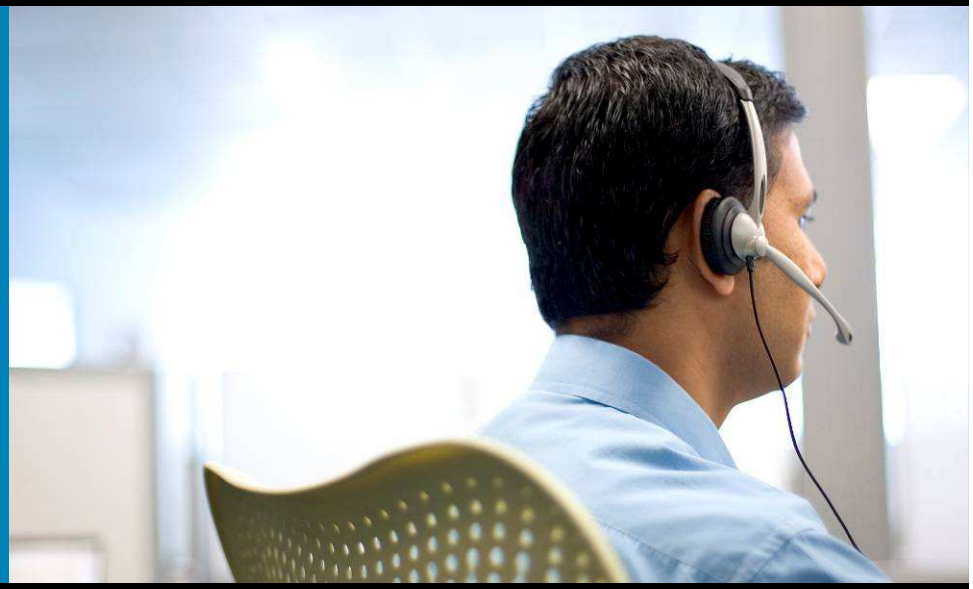
Passo 3 – Ativar o Black Hole



Passo 3 – Ativar o Black Hole

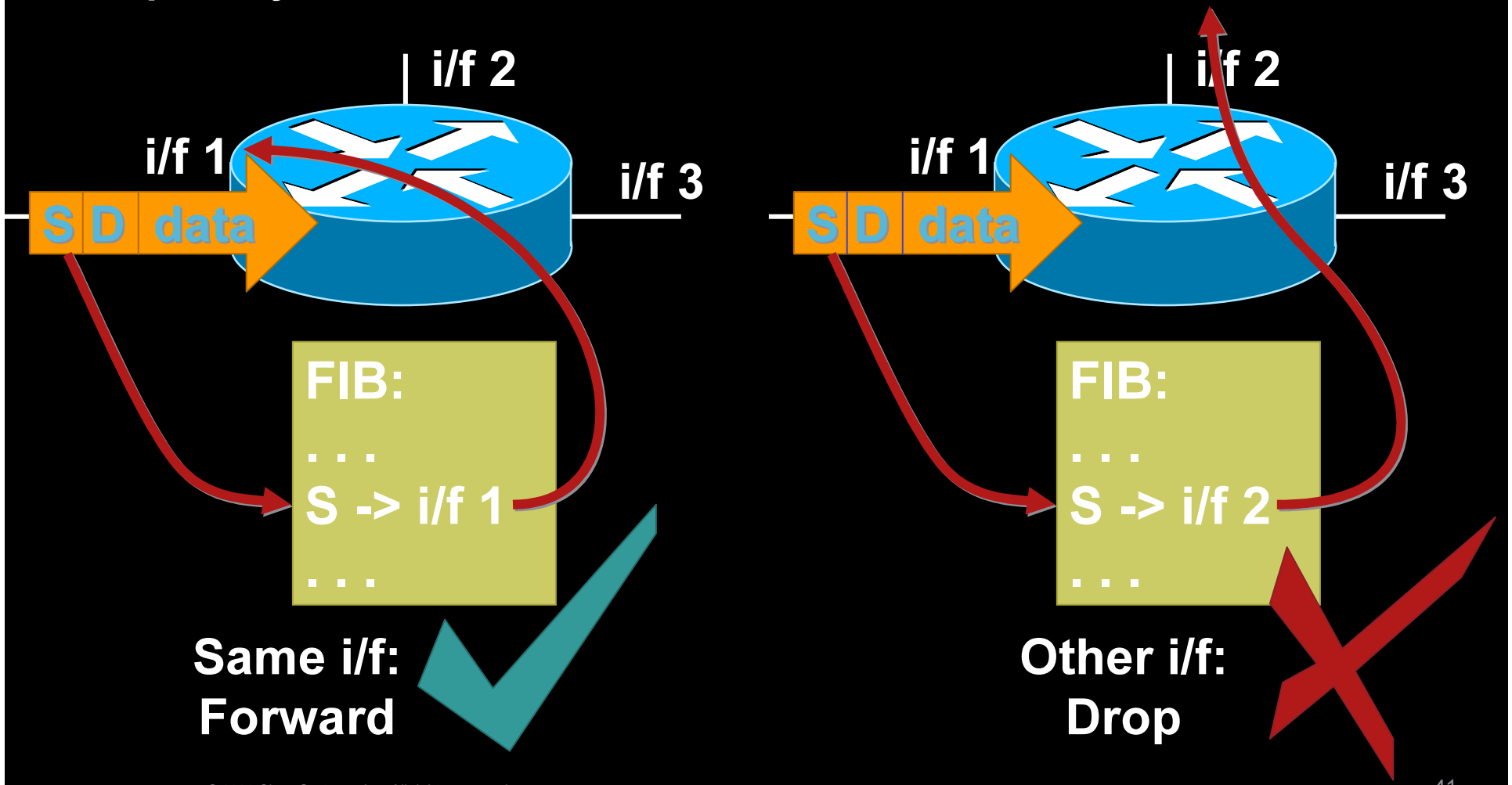


URPF
Checando autenticidade da origem



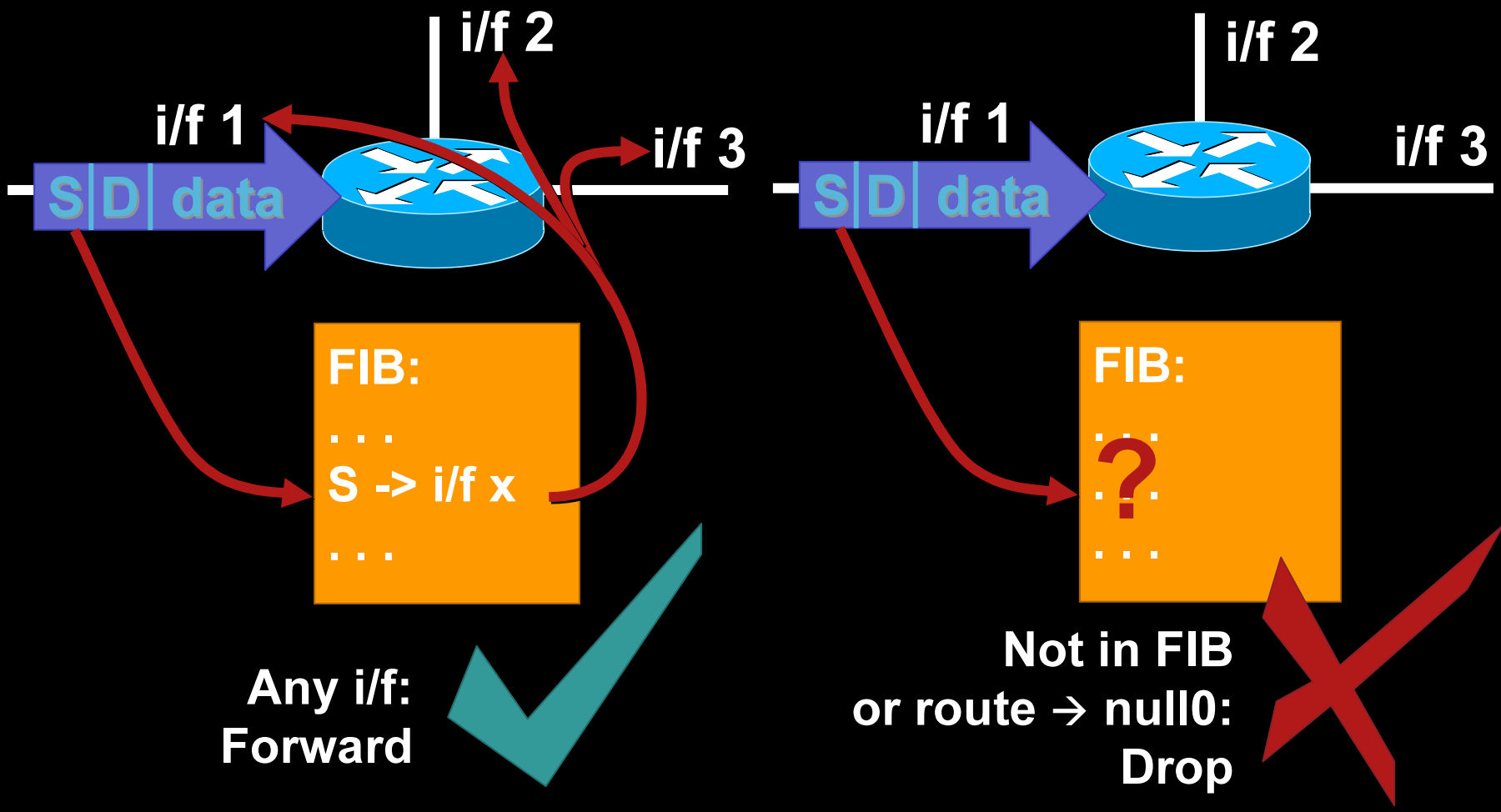
Strict uRPF (Unicast Reverse Path Forwarding)

router(config-if)# ip verify unicast reverse-path
or: ip verify unicast source reachable-via rx



Loose uRPF
(Unicast Reverse Path Forwarding)

router(config-if)# ip verify unicast source reachable-via any



Source Based Remote Triggered Black Hole Filtering

- Que mecanismos temos até agora ?

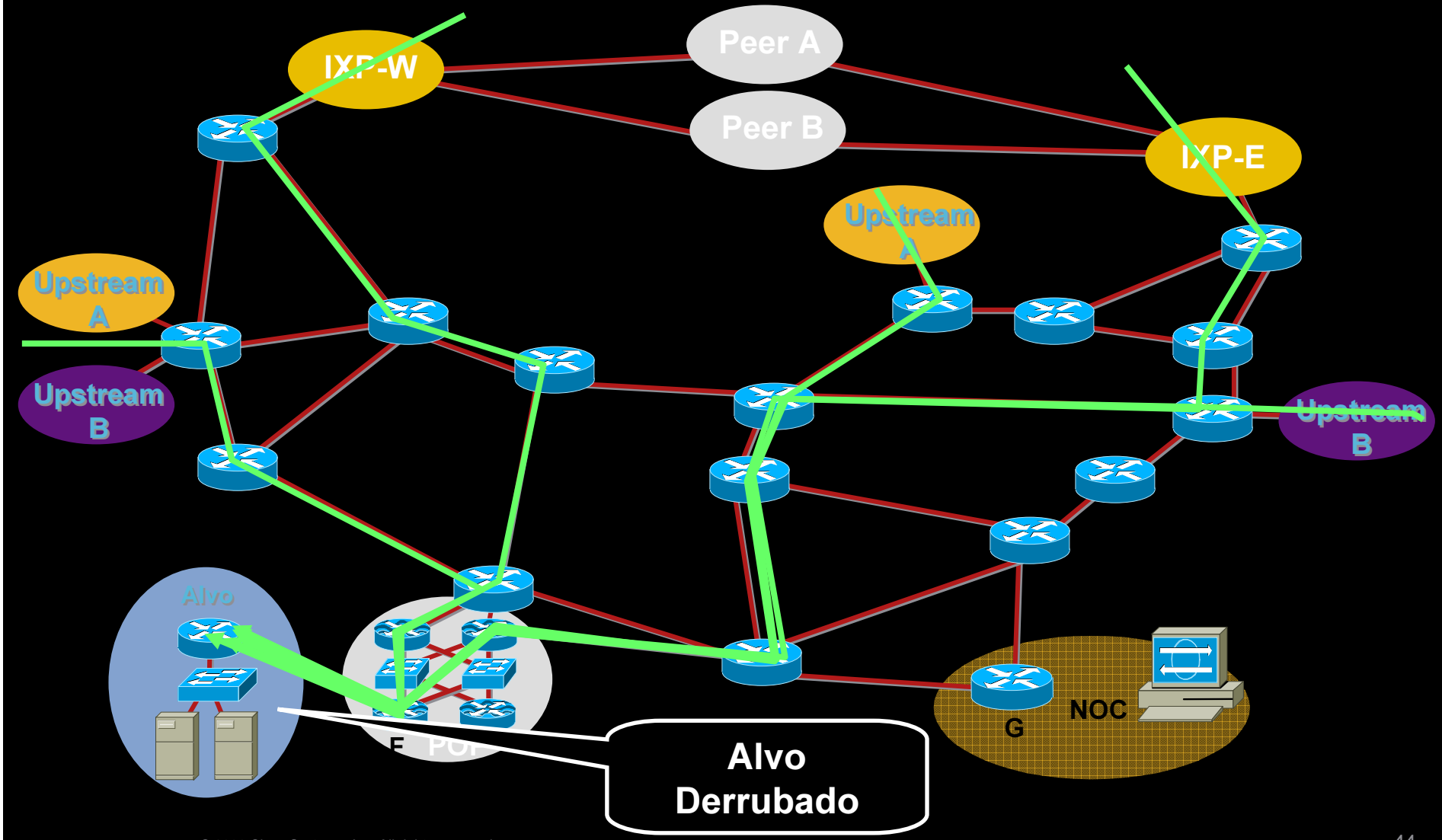
  Filtragem Black Hole **– Se o endereço destino é igual a Null 0 então descarte o pacote.**

  Ativação Remota **– Ativa um prefixo igual a Null 0 nos roteadores através da rede pelo iBGP.**

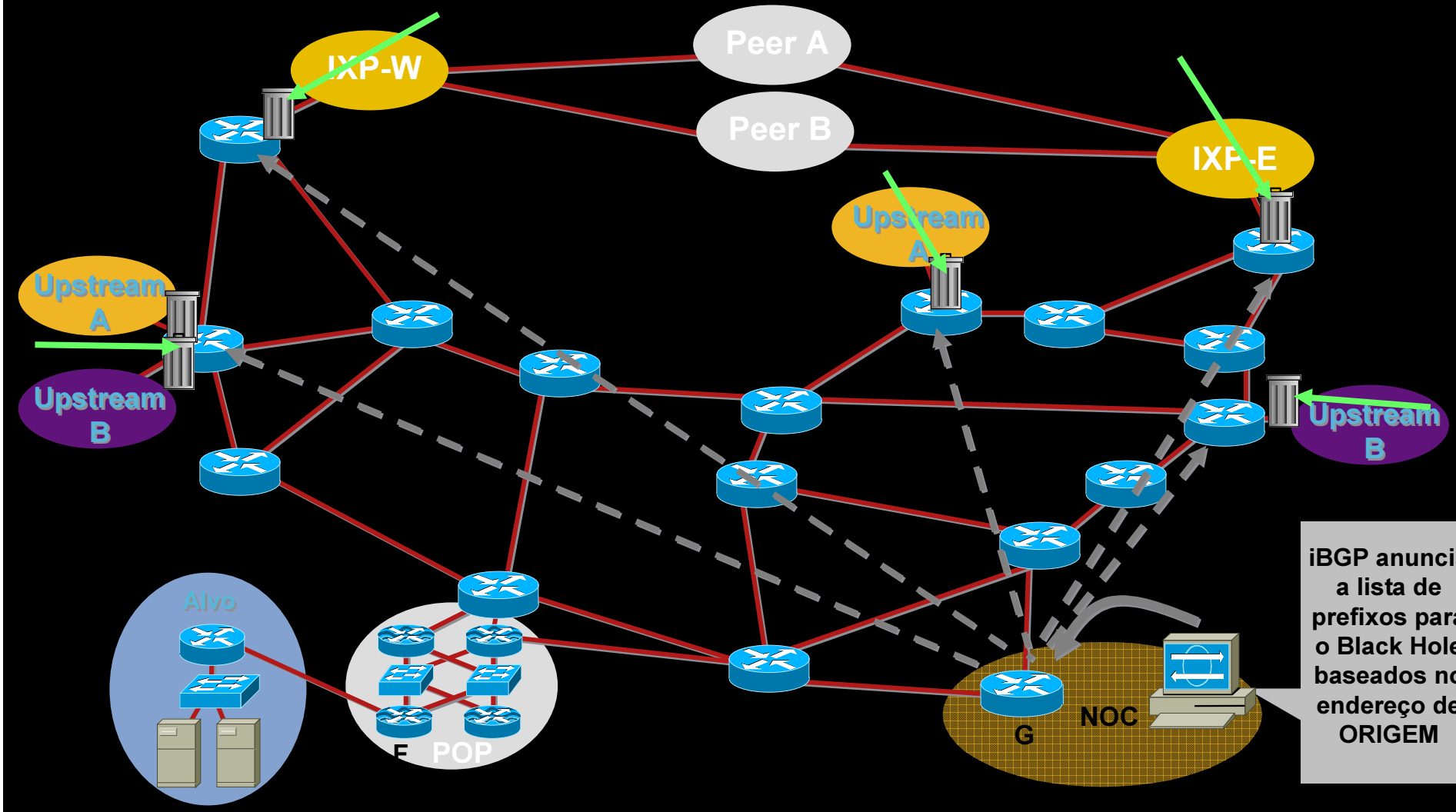
  uRPF Loose Check – **Se o endereço de origem for igual a Null 0, então descarte o pacote.**

- Juntando todos esses mecanismos, teremos uma ferramenta que pode ativar o descarte de pacotes vindos da rede cujo endereço de destino e de origem seja igual a Null 0!

Rede sob Ataque – Antes

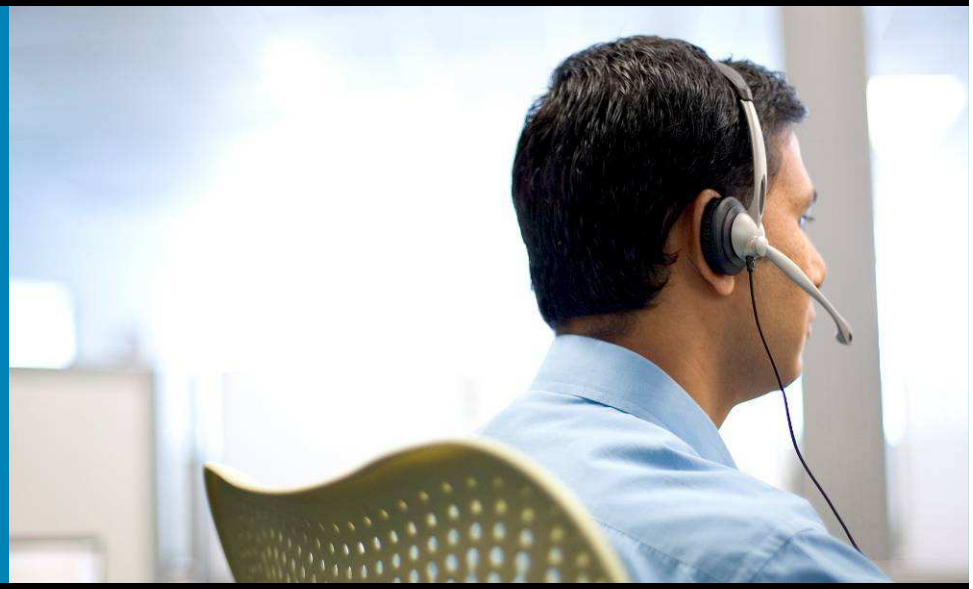


Rede sob Ataque – Depois

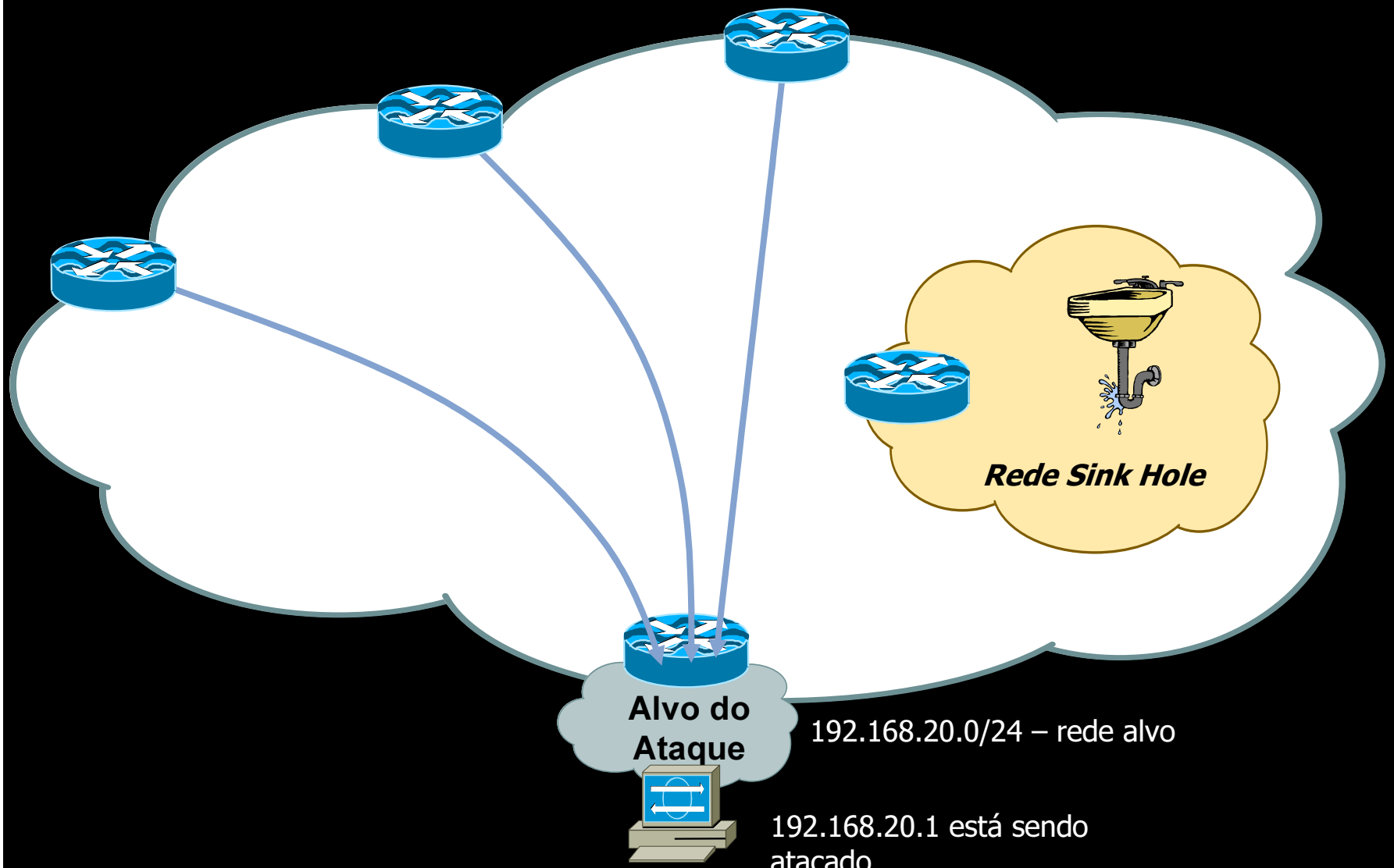


iBGP anuncia a lista de prefixos para o Black Hole baseados no endereço de ORIGEM

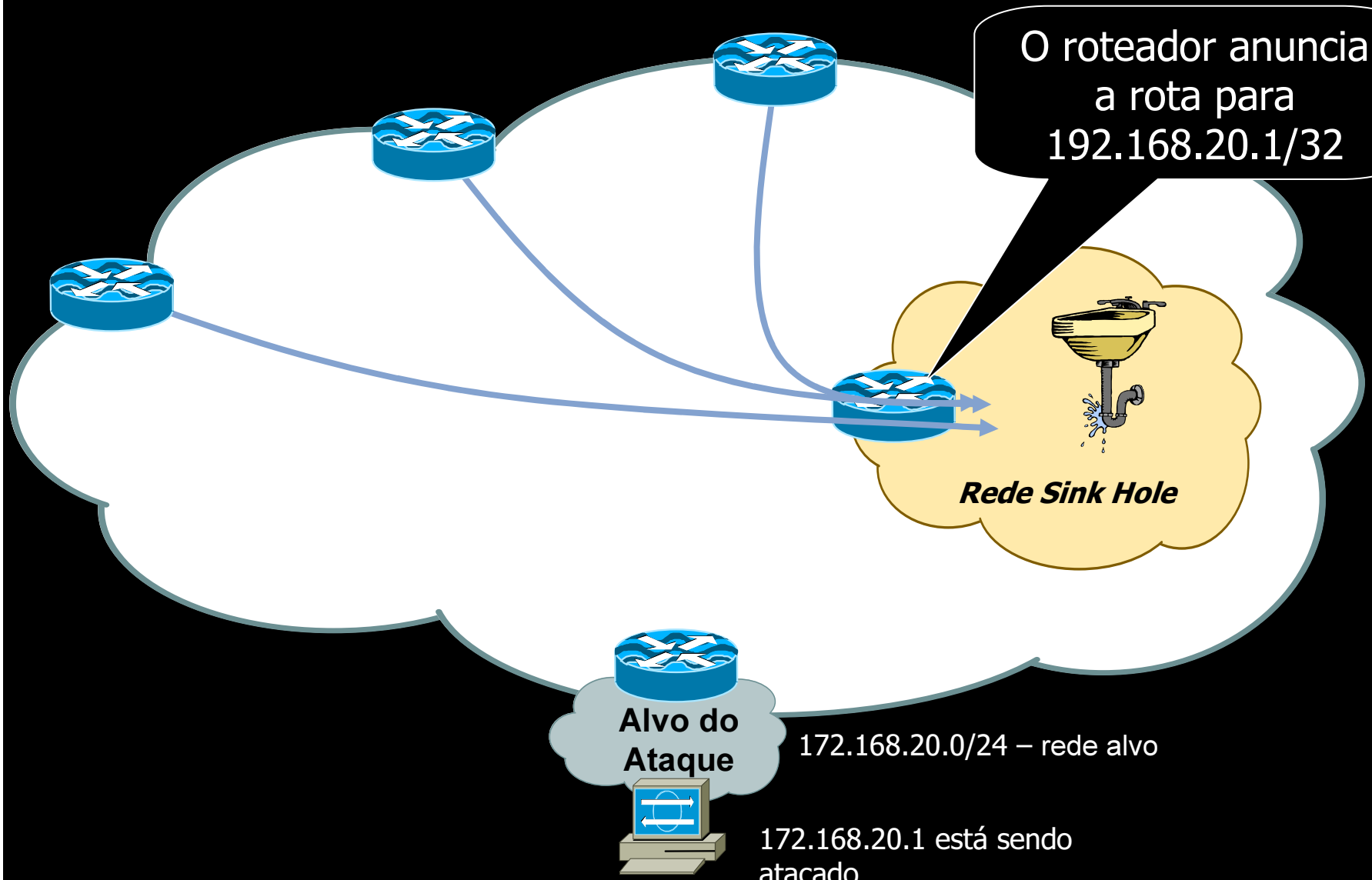
Sink Holes



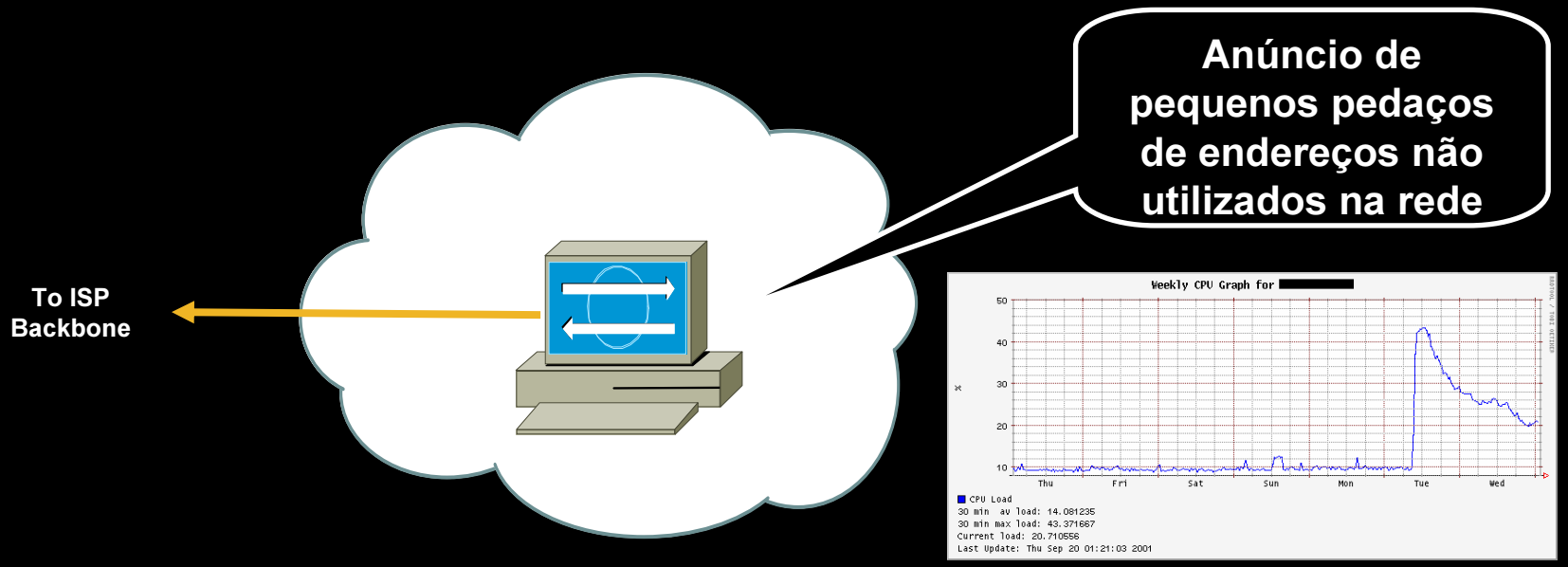
Sink Hole



Sink Hole



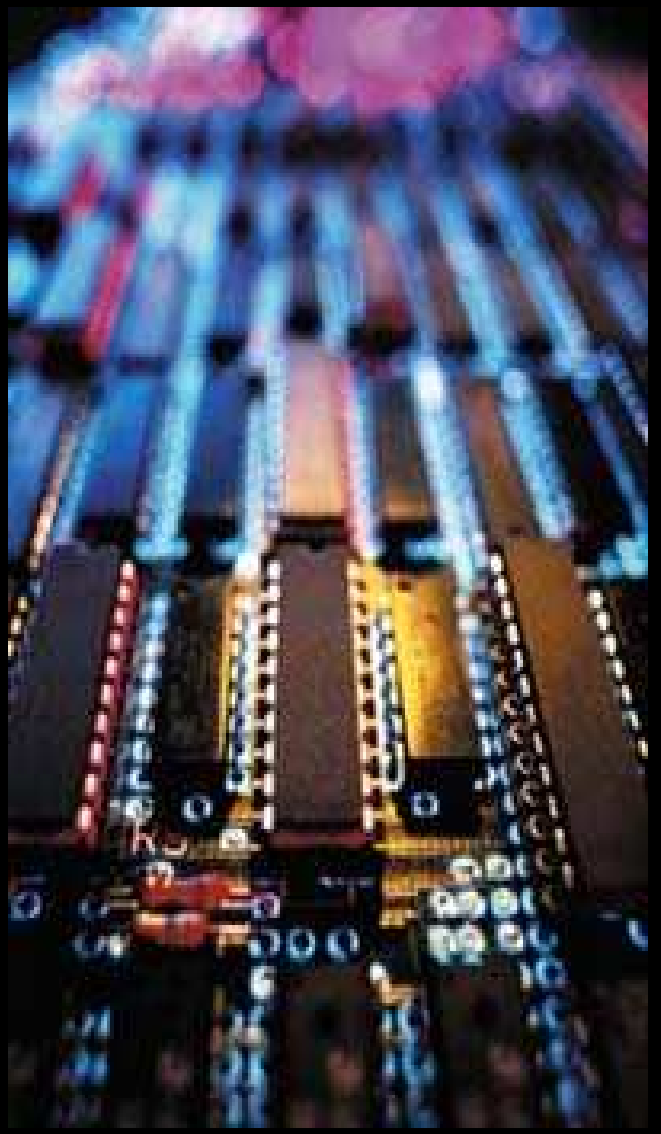
A função do Sink Hole



- Sinks Holes não precisam ser complicados.
- Alguns dos grandes provedores começaram com um Sink Hole composto apenas de uma estação sobressalente com free unix, Zebra, Ethereal ou TCPdump.
- Com alguma ferramenta gráfica, como MRTG graphing, você já tem um Sink Hole eficiente.

Conclusão - Recomendações

- Prevenção é essencial
  - ACLs, uRPF, …
- Monitore os roteadores
  - CPU, carga de tráfego, memória, …
- Tenha estatísticas da rede
  - IP Flow, SNMP, …
- Esteja preparado !
  - Tecnicamente: conheça sua rede
  - Operacionalmente: Tenha procedimentos engatilhados, contatos no cliente e nos provedores, certificações, …



Referências

DoS Detection:

- "Tackling Network DoS on Transit Networks": David Harmelin, DANTE, March 2001 (describes a detection method based on IP Flow) [http://www.dante.net/pubs/dip/42/42.html]
- "Inferring Internet Denial-of-Service Activity": David Moore et al, May 2001; (described a new method to detect DoS attacks, based on the return traffic from the victims, analysed on a /8 network; very interesting reading) [http://www.caida.org/outreach/papers/backscatter/index.xml]
- "The spread of the code red worm": David Moore, CAIDA, July 2001 (using the above to detect how this worm spread across the Internet) [http://www.caida.org/analysis/security/code-red/]

DoS Tracing:

- "Tracing Spoofed IP Addresses": Rob Thomas, Feb 2001; (good technical description of using IP Flow to trace back a flow) [http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html]

Other:

- "DoS attacks against GRC.com": Steve Gibson, GRC, June 2001 (a real life description of attacks from the victim side; somewhat disputed, but fun to read!) [http://grc.com/dos/grcdos.htm]

White Papers

- NetFlow

  http://www.cisco.com/warp/public/732/Tech/nmp/docs/netflow_security.pdf

  http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

- URPF

  http://www.cisco.com/warp/public/732/Tech/security/docs/urpf.pdf

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_urpf.htm

- Black Hole

  http://www.cisco.com/warp/public/732/Tech/security/docs/blackhole.pdf

Ferramentas Gratuitas e Abertas

- MRTG

  http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- RRD Tool

  http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- OSU Flow-Tools

  http://www.splintered.net/sw/flow-tools/
- Flow Scan

  http://net.doit.wisc.edu/~plonka/FlowScan/

  http://www.cisco.com/warp/public/732/Tech/security/docs/blackhole.pdf

OBRIGADO !!!

PERGUNTAS ???