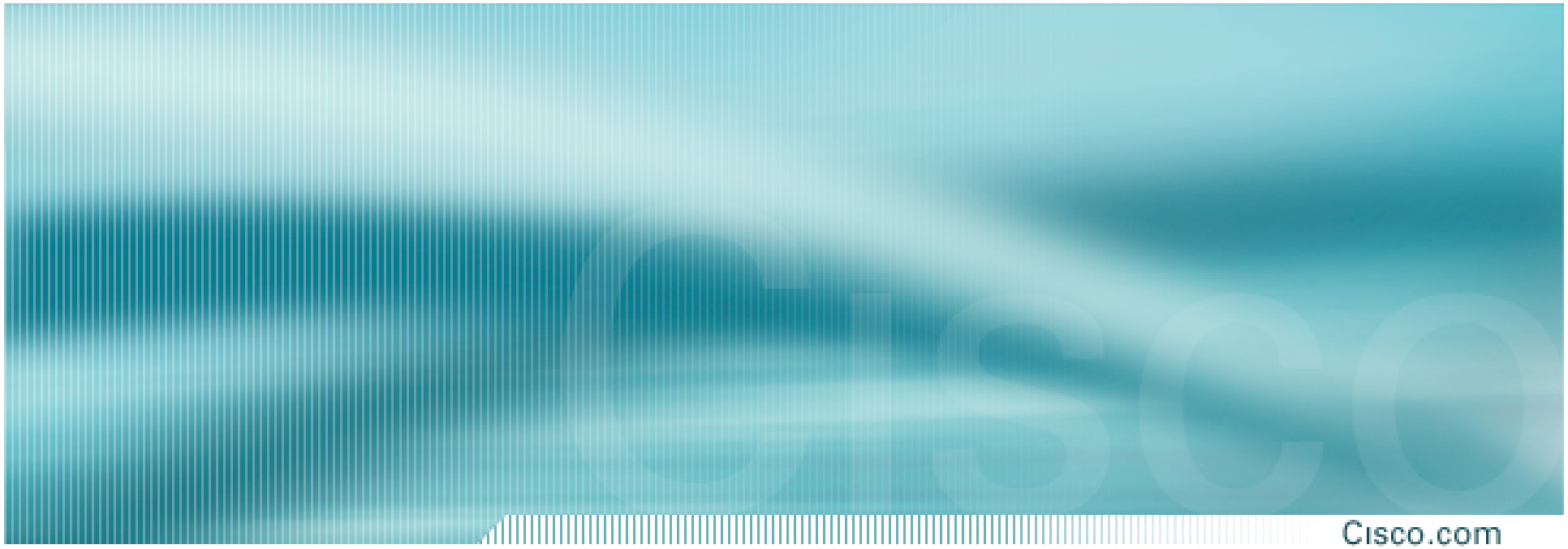


DOS Mitigation LAB Exercises

Version 0.1 DRAFT

Nick Satsia nsatsia@cisco.com

Seo Boon Ng sbng@cisco.com

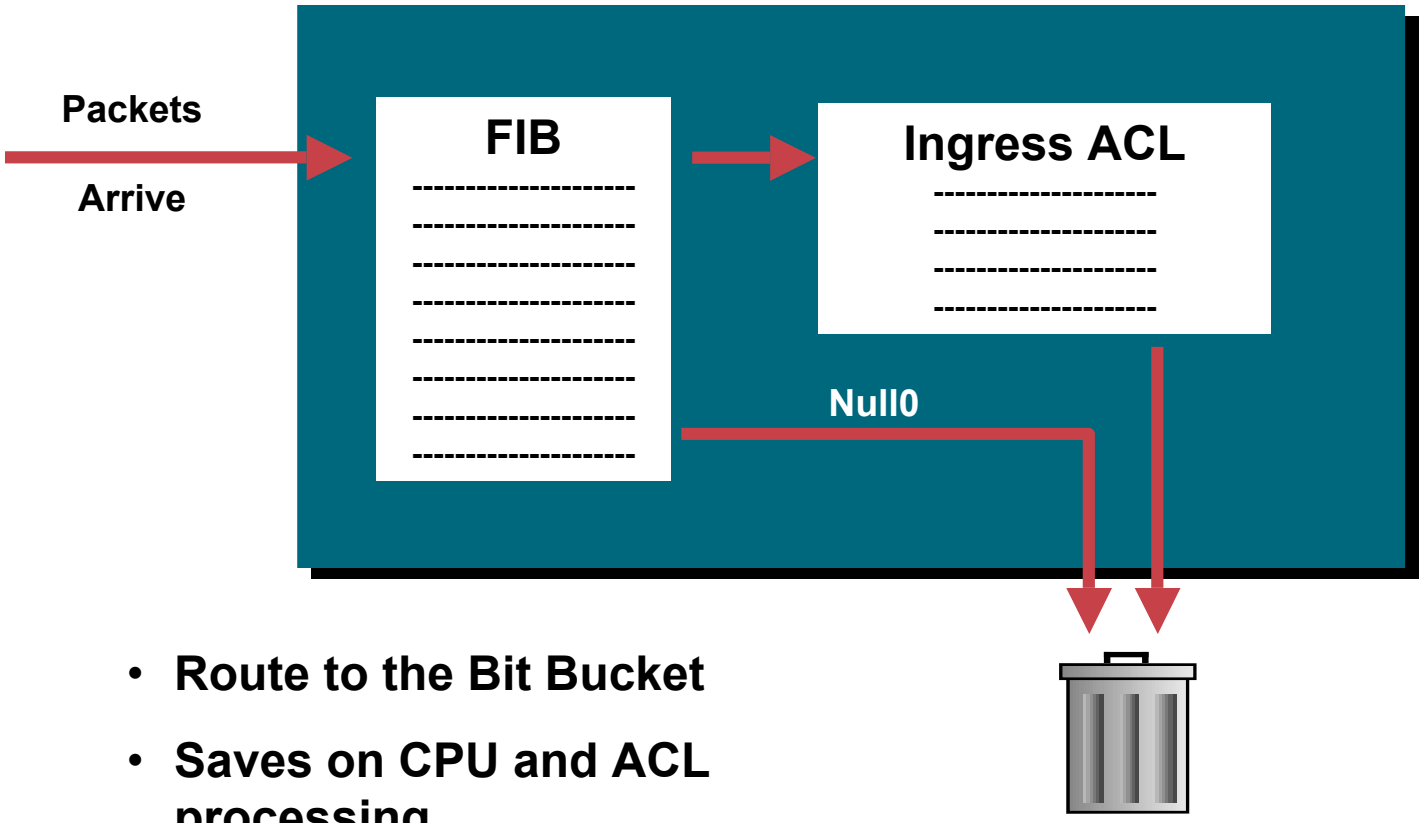
Agenda

- Mitigation Technique
- Lab setup
- Configuration detail
- Commonly seen attacks
  - ✓ DOS attack
  - ✓ DDOS attack
  - ✓ Infrastructure attacks
  - ✓ Collateral damage

Mitigation Technique

- Sink Hole
- Remote trigger black hole
- Back Scatter

Black Hole Filtering

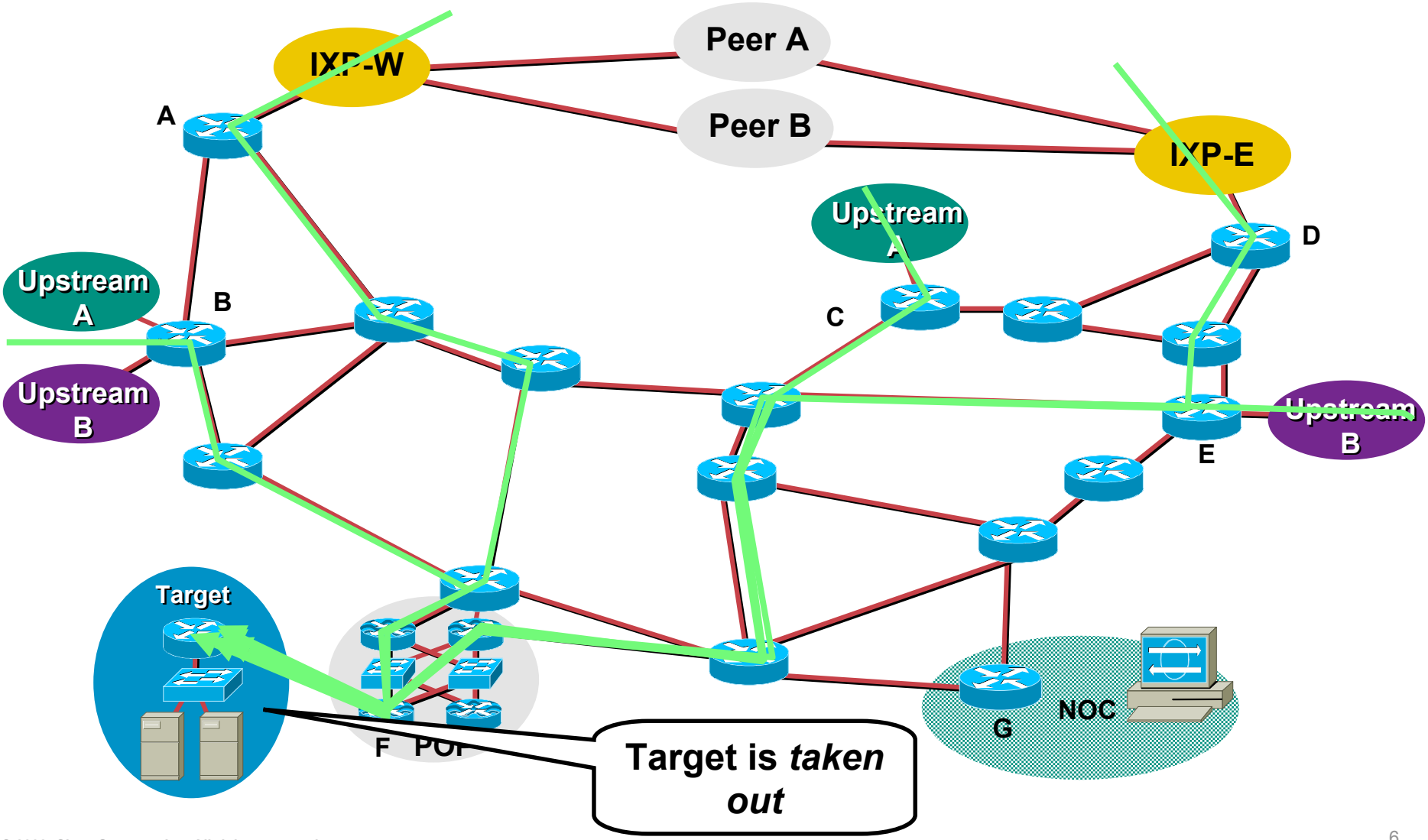


- Route to the Bit Bucket
- Saves on CPU and ACL processing

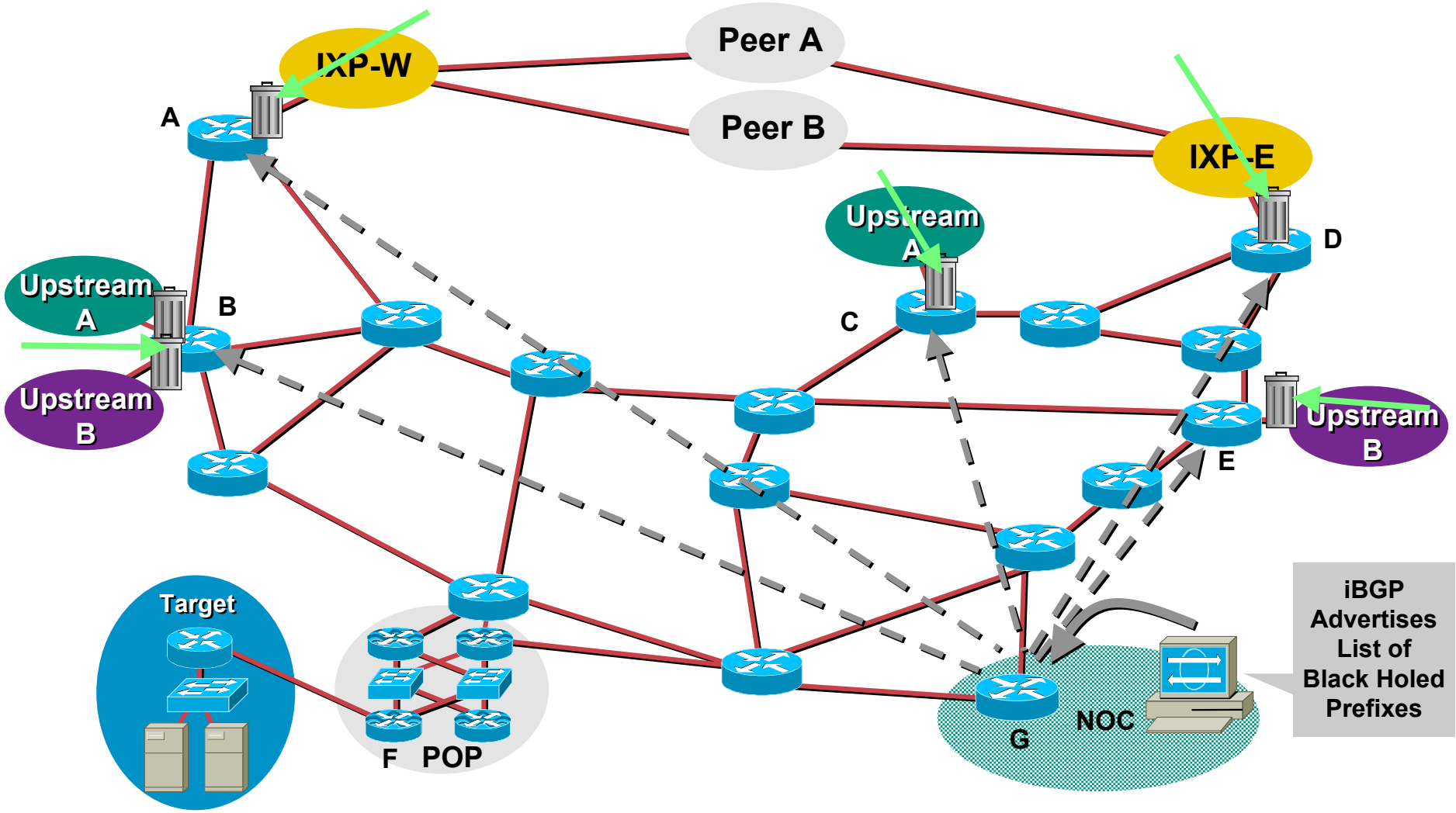
Remotely Triggered Black Hole Filtering

- We use BGP to trigger a network wide response to an attack flow.
- A simple static route and BGP will allow an ISP to trigger network wide black holes as fast as iBGP can update the network.
- This provides ISPs a tool that can be used to respond to security related events or used for DOS/DDOS Backscatter Tracebacks.

Network Wide Black Hole of an Attack Flow - Before



Network Wide Black Hole of an Attack Flow - Before



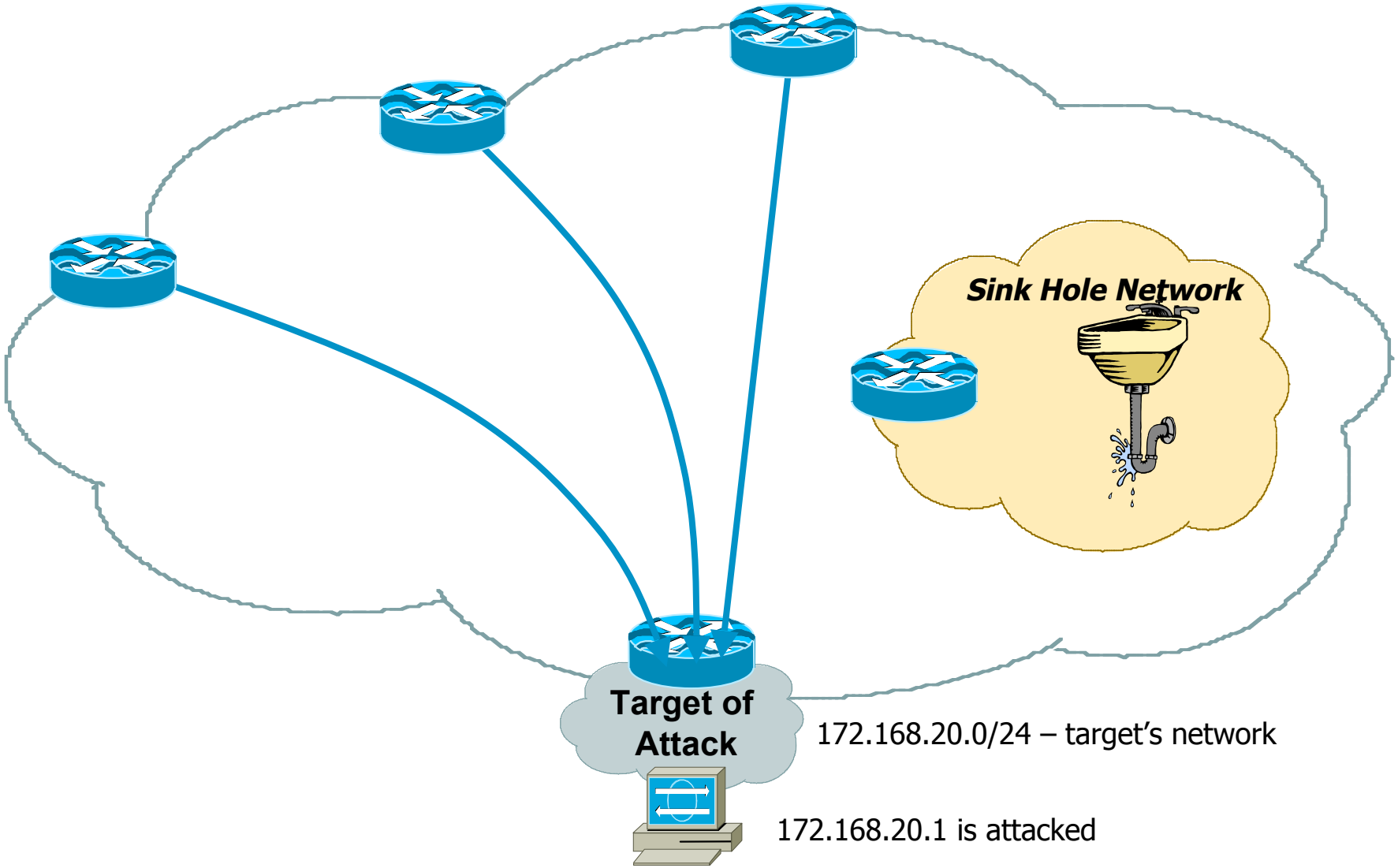
Remote Triggered Black Hole

- **Remote Triggered Black Hole filtering is the foundation for a whole series of techniques to traceback and react to DOS/DDOS attacks on an ISP's network.**
- **Preparation does not effect ISP operations or performance.**
- **It does adds the option to an ISP's *security toolkit.***

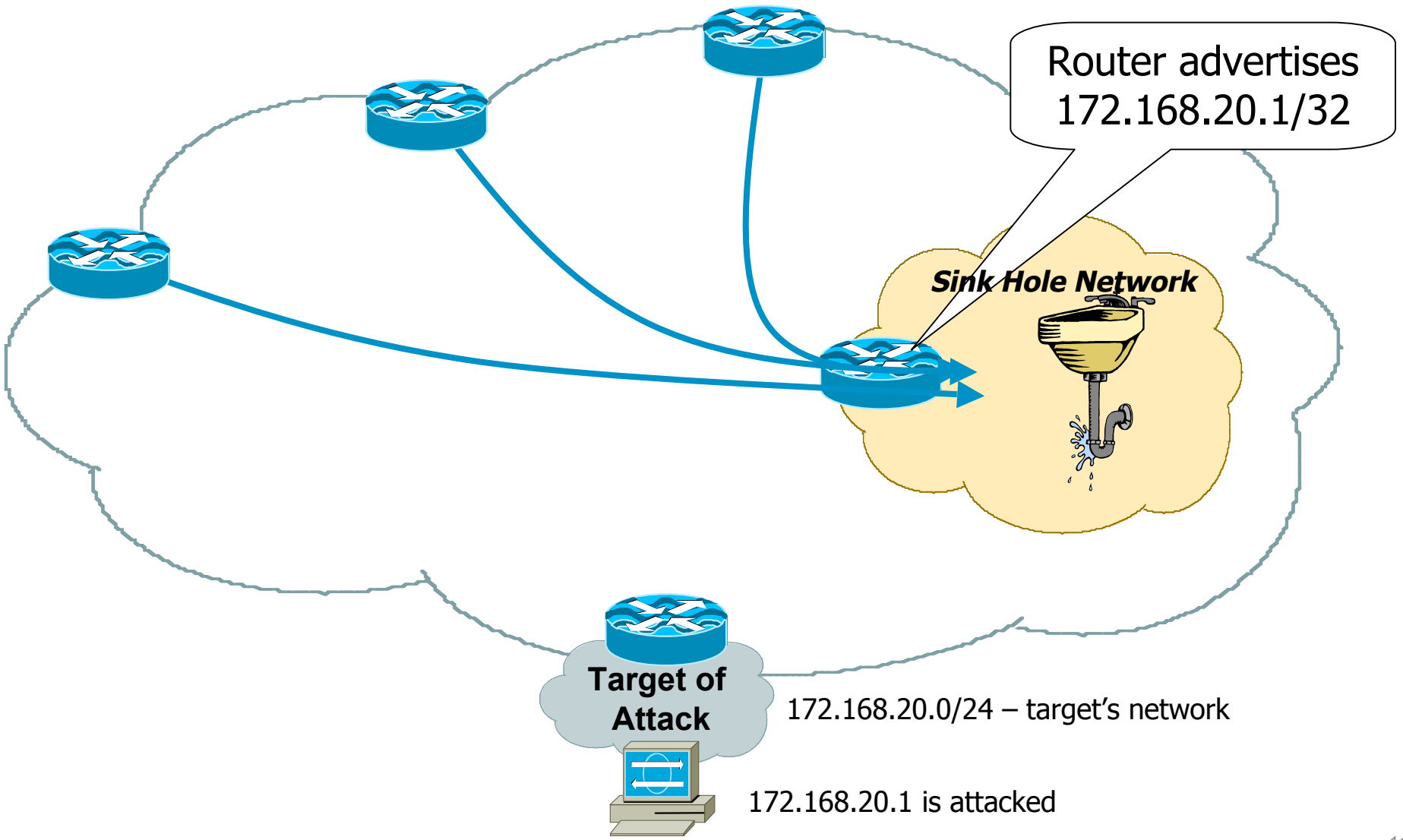
Sink Hole Routers/Networks

- **Sink Holes are a the network equivalent of a honey pot.**
  - ✓ **BGP speaking Router or Workstation that built to *suck in* attacks.**
  - ✓ **Used to redirect attacks away from the customer – working the attack on a router built to withstand the attack.**
  - ✓ **Used to monitor *attack noise, scans,* and other activity (via the advertisement of default)**

Sink Hole Routers/Networks

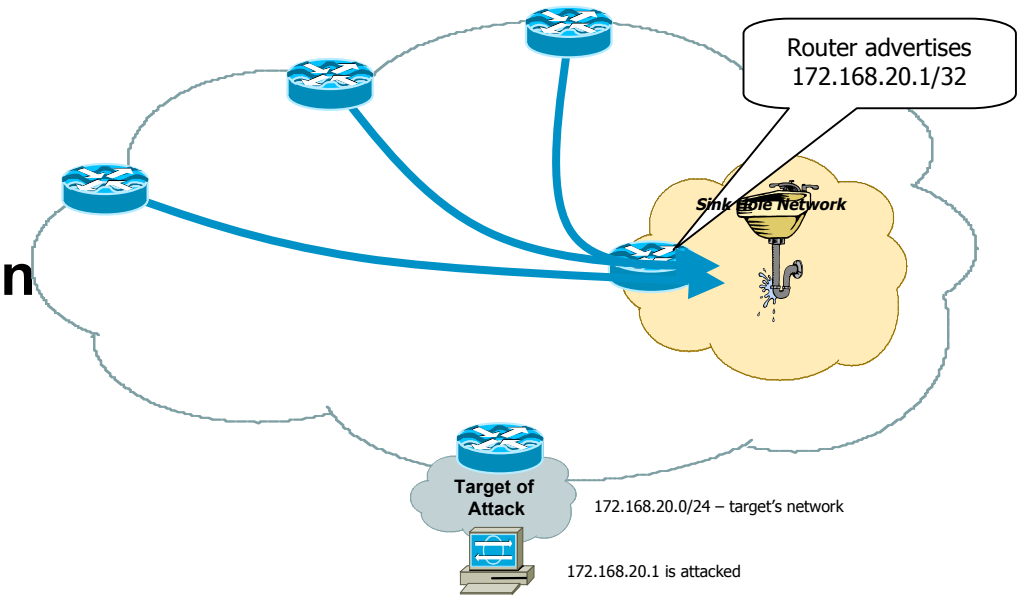


Sink Hole Routers/Networks



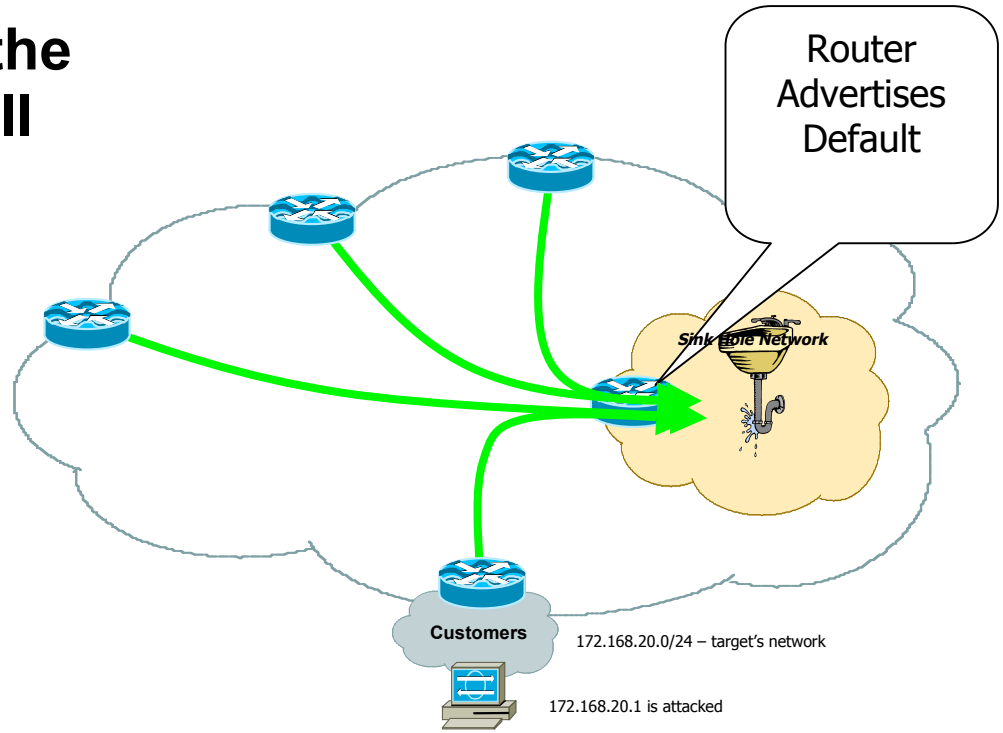
Sink Hole Routers/Networks

- Attack is pulled off customer and your aggregation router.
- Can now do classification ACLs, Flow Analysis, Sniffer Capture, Traceback, etc.
- Objective is to minimize the risk to the network while working the attack incident.



Sink Hole Routers/Networks

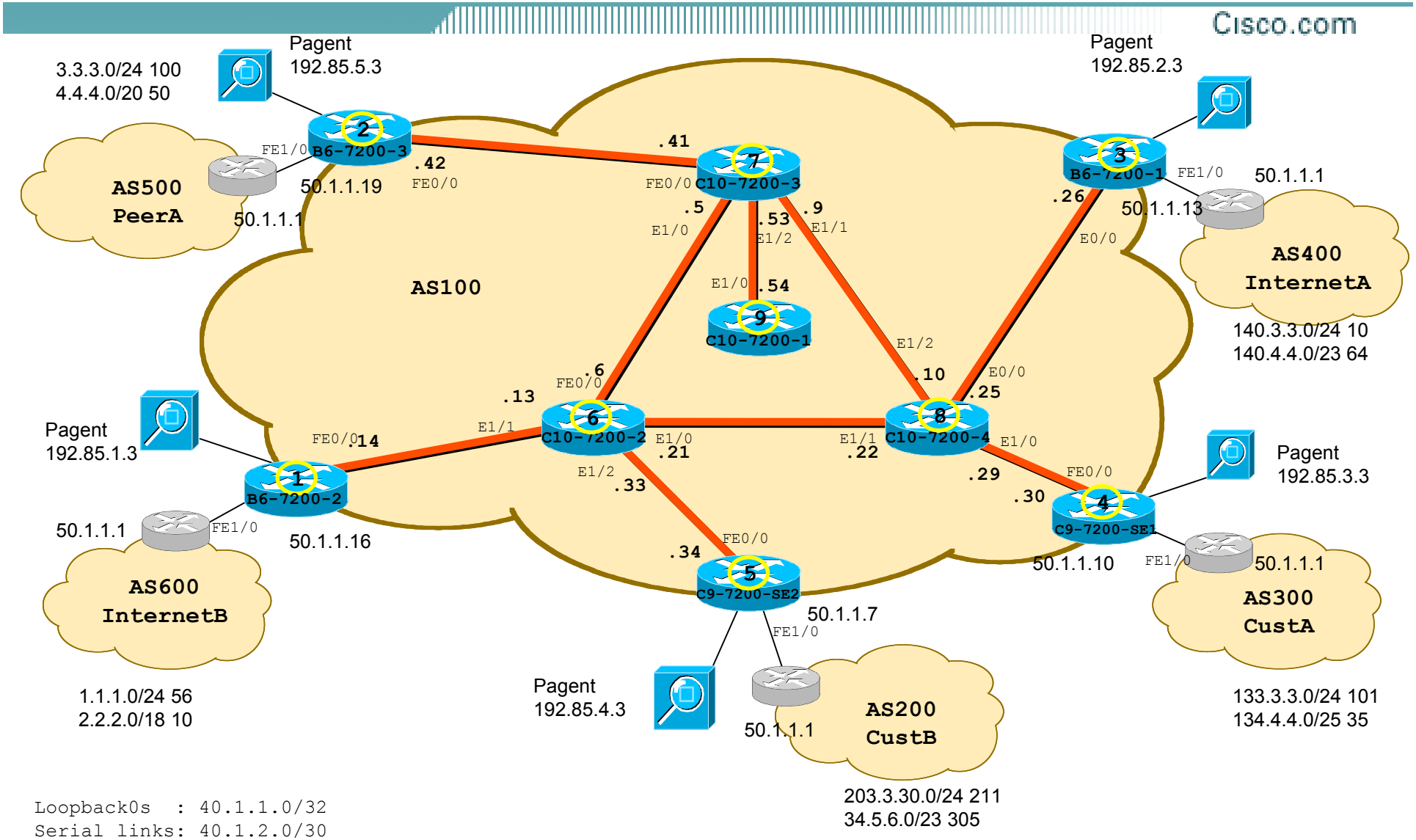
- **Advertising Default from the Sink Hole will pull down all sort of *junk* traffic.**
  - ✓ **Customer Traffic when circuits flap.**
  - ✓ **Network Scans**
  - ✓ **Failed Attacks**
  - ✓ **Code Red/NIMDA**
  - ✓ **Backscatter**
- **Can place tracking tools and IDA in the Sink Hole network to monitor the noise.**



Back Scatter traceback

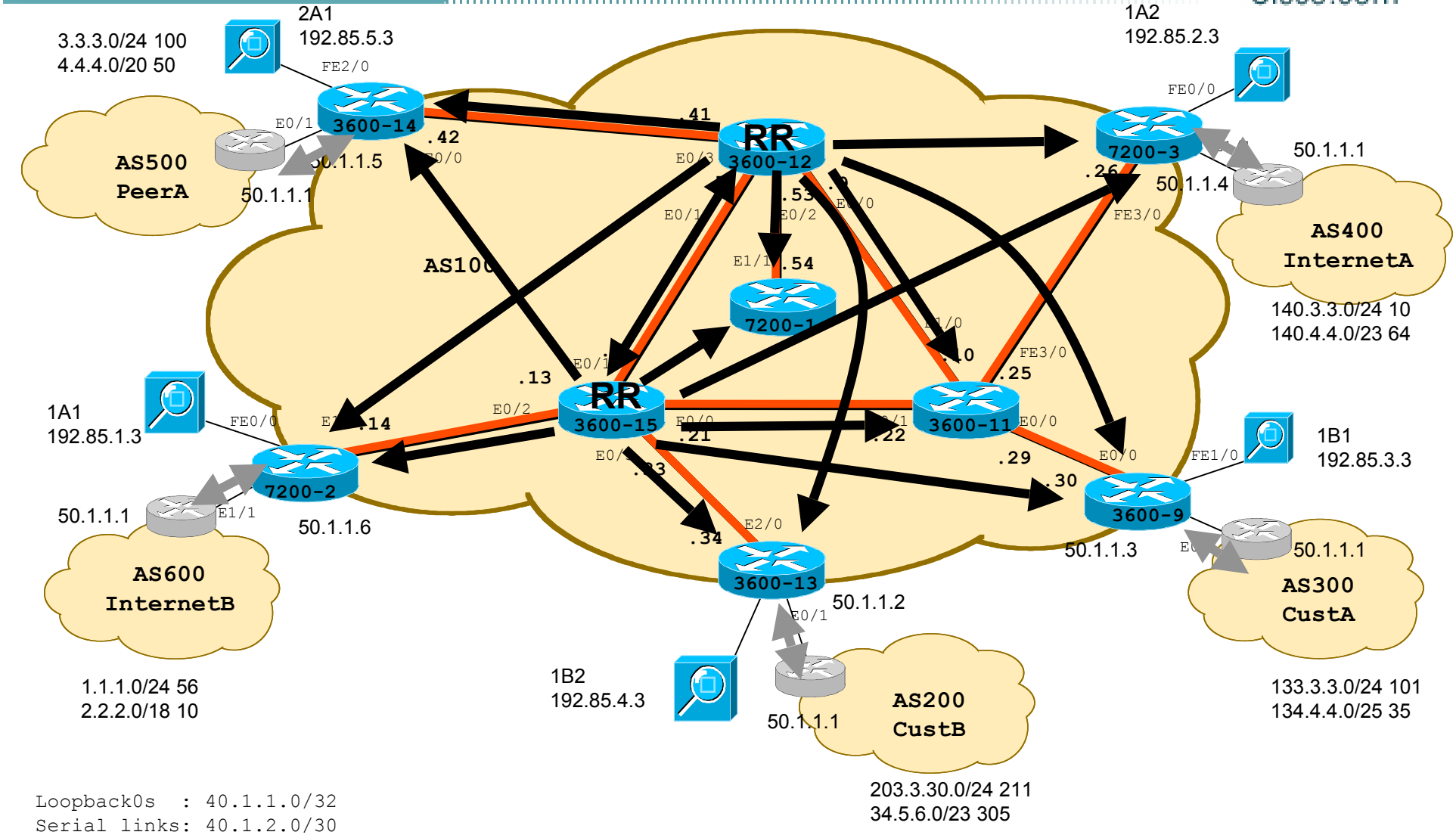
- Work in conjunction with sinkhole and remote-trigger blackhole router
- Pull in icmp unreachable in order to help identify the border router where the attacks comes from
- Blackhole the victim while pulling in the icmp unreachable onto the sinkhole router

LAB Network



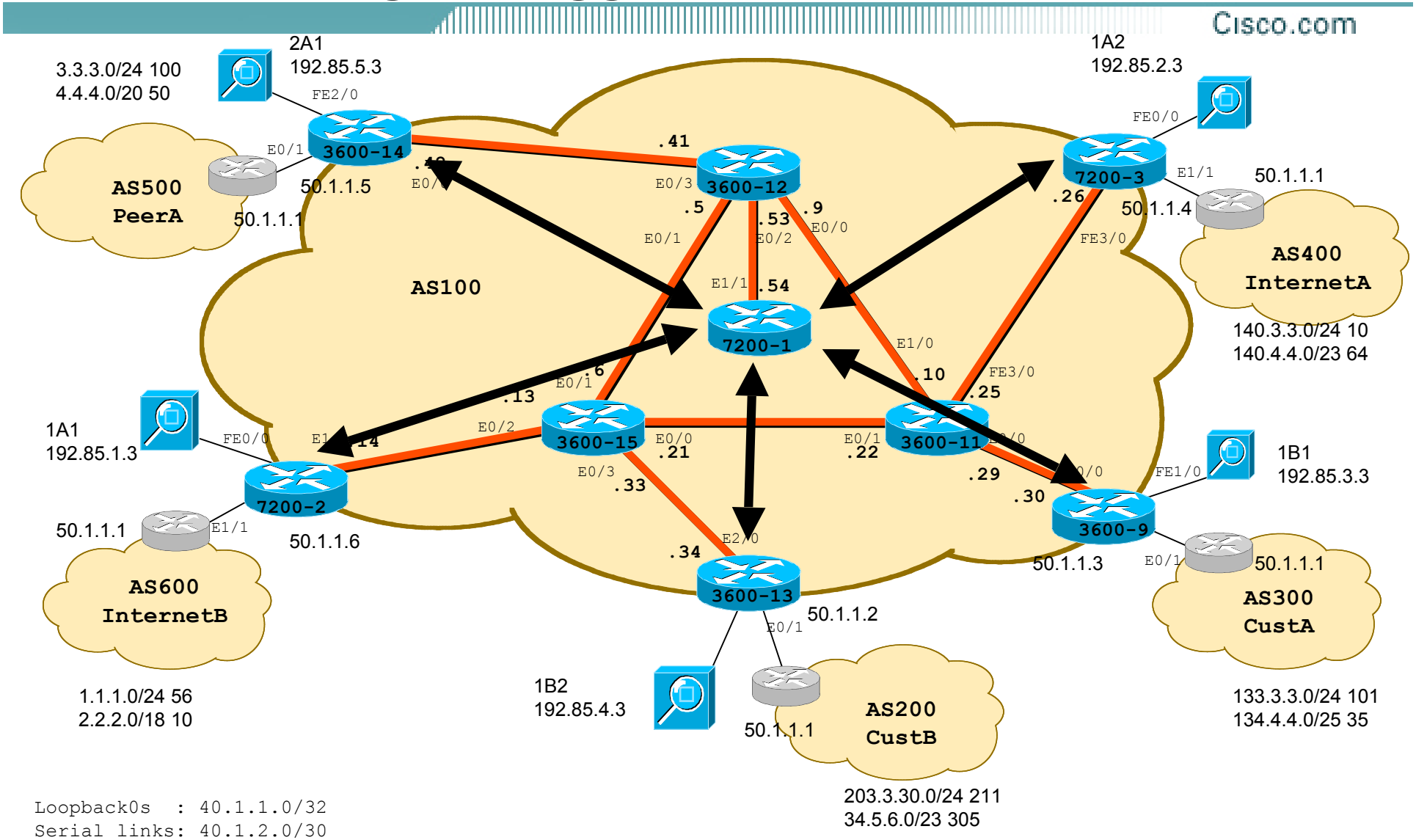

```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

LAB Network
iBGP Peering to RRs and eBGP to RouteM




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

LAB Network
BGP Peering to Trigger Router




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

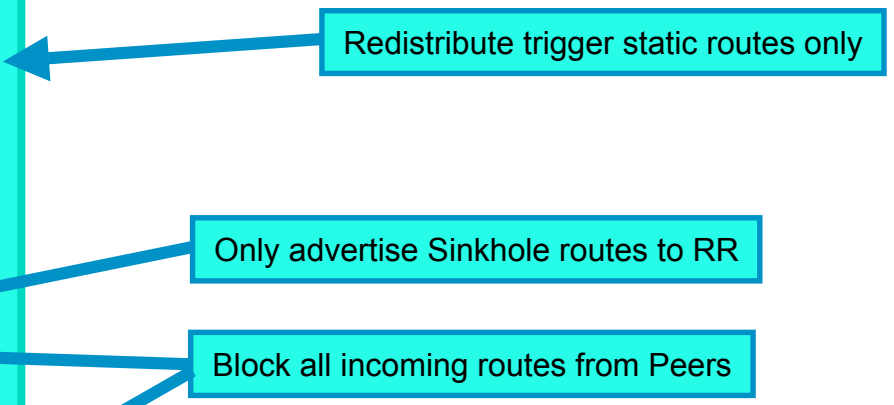
Trigger Router Security Policy Trigger

IP add	Community	Gateway
40.99.99.99	100:7799	ALL
40.99.99.02	100:7702	gw-7200-2
40.99.99.03	100:7703	gw-7200-3
40.99.99.09	100:7709	gw-3600-9
40.99.99.13	100:7713	gw-3600-13
40.99.99.14	100:7714	gw-3600-14

Tag	Action
664	Blackhole
665	Sinkhole
668	CAR
669	CAR + Sinkhole

Trigger Router Security Policy
BGP Config


```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 bgp dampening
!
redistribute static route-map static-to-dos-trigger
!
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal password 7 045802150C2E
 neighbor internal update-source Loopback0
 neighbor internal next-hop-self
 neighbor internal send-community
 neighbor internal route-map sink-all out
 neighbor internal route-map block-all in
!
 neighbor dosclient peer-group
 neighbor dosclient remote-as 100
 neighbor dosclient password 7 045802150C2E
 neighbor dosclient update-source Loopback0
 neighbor dosclient send-community
 neighbor dosclient route-map block-all in
!
 neighbor 40.1.1.2 peer-group dosclient
 neighbor 40.1.1.3 peer-group dosclient
 neighbor 40.1.1.9 peer-group dosclient
 neighbor 40.1.1.12 peer-group internal
 neighbor 40.1.1.13 peer-group dosclient
 neighbor 40.1.1.14 peer-group dosclient
 neighbor 40.1.1.15 peer-group internal
 no auto-summary
```



Trigger Router Security Policy
Static Trigger Route-Map (All Gateways)

Blackhole

Sinkhole

CAR

CAR + Sinkhole

```
access-list 99 permit 40.99.99.99
!
route-map static-to-dos-trigger permit 100
 match ip next-hop 99
 match tag 664
 set ip next-hop 192.0.2.1
 set local-preference 50
 set origin igp
 set community 100:664 100:7799 no-export
!
route-map static-to-dos-trigger permit 102
 match ip next-hop 99
 match tag 665
 set ip next-hop 40.1.1.1
 set local-preference 50
 set origin igp
 set community 100:665 100:7799 no-export
!
route-map static-to-dos-trigger permit 104
 match ip next-hop 99
 match tag 668
 set ip next-hop 40.1.1.1
 set local-preference 50
 set origin igp
 set community 100:668 100:7799 no-export
!
route-map static-to-dos-trigger permit 106
 match ip next-hop 99
 match tag 669
 set ip next-hop 40.1.1.1
 set local-preference 50
 set origin igp
 set community 100:669 100:7799 no-export
!
```

Set next hop = test-net ➔ Null0

Set next hop = Sinkhole (self)

Set action and gateway communities

Trigger Router Security Policy
Static Trigger Route-Map (per Gateway)

Blackhole

CAR

```
access-list 64 permit 40.99.99.14
!
route-map static-to-dos-trigger permit 150
 match ip next-hop 64
 match tag 664
 set ip next-hop 192.0.2.1
 set local-preference 50
 set origin igp
 set community 100:664 100:7714 no-export
!
route-map static-to-dos-trigger permit 154
 match ip next-hop 64
 match tag 668
 set ip next-hop 40.1.1.1
 set local-preference 50
 set origin igp
 set community 100:668 100:7714 no-export
!
```

Set next hop = test-net ➔ Null0

Set action and gateway communities

Gateway Router Security Policy
QPPB for CAR


```
!
interface FastEthernet0/0
 ip address 192.85.2.1 255.255.255.0
 ip verify unicast source reachable-via any
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 bgp-policy destination ip-qos-map
 rate-limit input qos-group 99 64000 5000 5000 conform-action transmit exceed-action drop
 ip route-cache flow
 load-interval 30
!
router bgp 100
 .
 table-map qos-group-map
 .
!
ip community-list 168 permit _100:668_.*(100:7799|100:7703)
ip community-list 168 permit _100:669_.*(100:7799|100:7703)
!
route-map qos-group-map permit 10
 match community 168
 set ip qos-group 99
!
```

Enable QPPB on eBGP interface for destination IP addresses

Rate limit packets with qos-group 99

Enable QPPB and specify route-map

Set QOS group CEF attribute for selected networks

Trigger Router Security Policy
Static Gateway Route-Map

Sample config from gw-7200-3

Sinkhole Blackhole

```
!
ip route 192.0.2.1 255.255.255.255 Null0 254
!
ip community-list 164 permit _100:664_.*(100:7799|100:7703)
ip community-list 165 permit _100:665_.*(100:7799|100:7703)
ip community-list 165 permit _100:669_.*(100:7799|100:7703)
ip community-list 168 permit _100:668_.*(100:7799|100:7703)
ip community-list 168 permit _100:669_.*(100:7799|100:7703)
!
ip as-path access-list 1 permit ^$
!
route-map block-all deny 10
!
!
route-map dos-trigger permit 10
 match as-path 1
 match community 164
 set ip next-hop 192.0.2.1
!
!
!
route-map dos-trigger permit 20
 match as-path 1
 match community 165
 set ip next-hop 40.1.1.1
!
!
!
route-map dos-trigger deny 65535
!
```

Set next hop = test-net ➔ Null0

Make sure it is an iBGP route (i.e. empty path list)

Set next hop = Sinkhole

Attack types

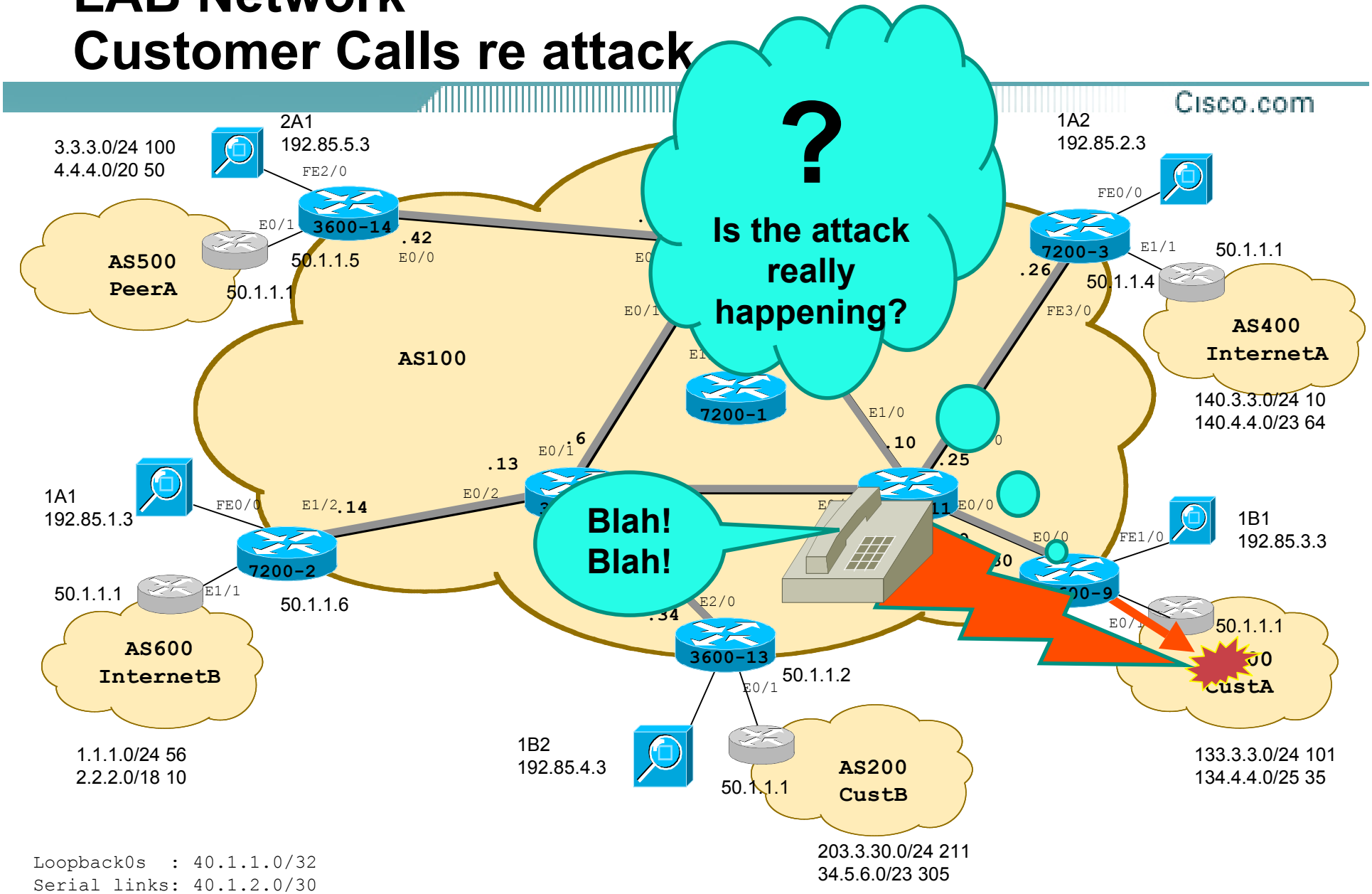
Cisco.com

- DOS or DDOS
- Source and/or Destination Spoofed
- Internet to Customer
- Customer to Internet
- Customer to Customer

Attack 1: Internet to Customer DOS

- Real addresses
- 1A2 dst=133.3.3.1 src=140.3.3.1
- Customer calls
- Identify attack using
- Confirm are real addresses
- For assymetric routes may need backscatter.
- A crude way would be to use MRTG to identify
- Options:
  - ✓ URPF (Loose)
  - ✓ Blackhole customer

LAB Network
Customer Calls re attack




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

Check bordering Gateway 9


```
gw-3600-9#sh ip cache flow
IP packet size distribution (28540231 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416
   .000 .000 .000 .000 .000 .000 .000 .995 .000 .000 .000 .004 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 37 added
  32324 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow
TCP-BGP             11      0.0         2    69      0.0       1.1
IPINIP              24      0.0   1183436   242    374.8    1326.9       6.4
Total:              35      0.0    811499   241    374.8     910.2       9.3

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP  DstP  Pkts
  .
  .
Et0/0         140.3.3.1       Fa1/0         133.3.3.1       04 0000 0000   138K
  .
  .
gw-3600-9#
```

?

What does this Gateway see?

From Gateway 3

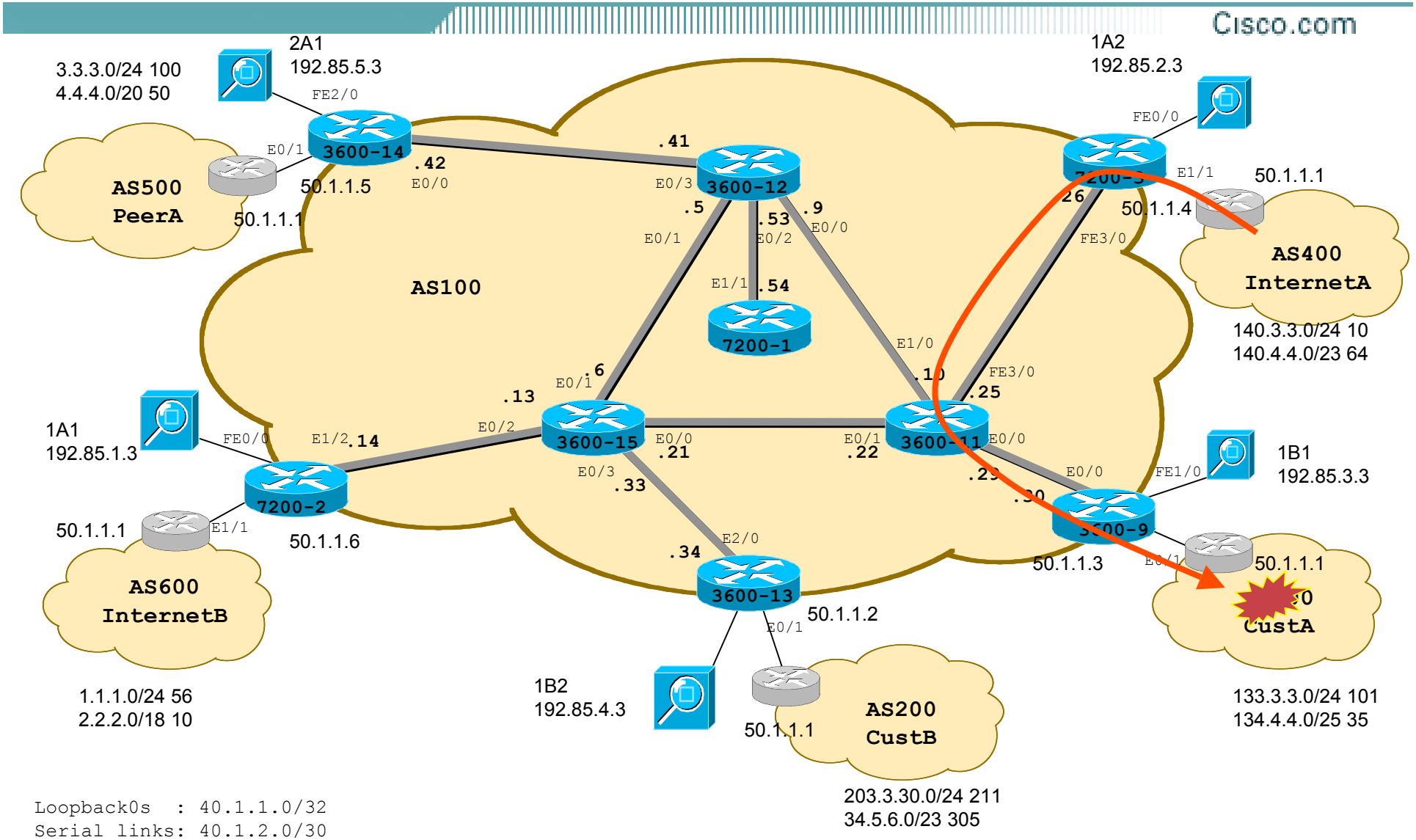
Check bordering Gateway 3


```
gw-7200-3#show ip cache flow
IP packet size distribution
   1-32   64   96  128  160
   .002 .000 .000 .000 .00

    512  544  576 1024 1
   .000 .000 .000 .00

IP Flow Switching Ca
  1 active, 65535 ina
  91105 ager polls, 0 1
  Active flows timeout
  Inactive flows timec
  last clearing of sta
Protocol         Total                                    (Sec)
--------         Flows                                    Flow
TCP-Telnet          49      0.                            14.1
TCP-BGP           3949      0.0                    0.2    15.3
UDP-TFTP             6      0.0                   27.4    15.2
ICMP                 3      0.0        6    67         14.8    15.5
IPINIP              20      0.       164   242    154.9  1291.9     6.9
Total:            4027      0.       76    241    155.4     6.8    15.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
   .
   .
Fa0/0         140.3.3.1       Fa3/0         133.3.3.1       04 0000 0000   355K
   .
   .
gw-7200-3#
```

!

Flow from customer under attack…..
Must be real source address used.
(w.r.t. your NWs perspective)

LAB Network
Internet to Customer Attack Flow




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

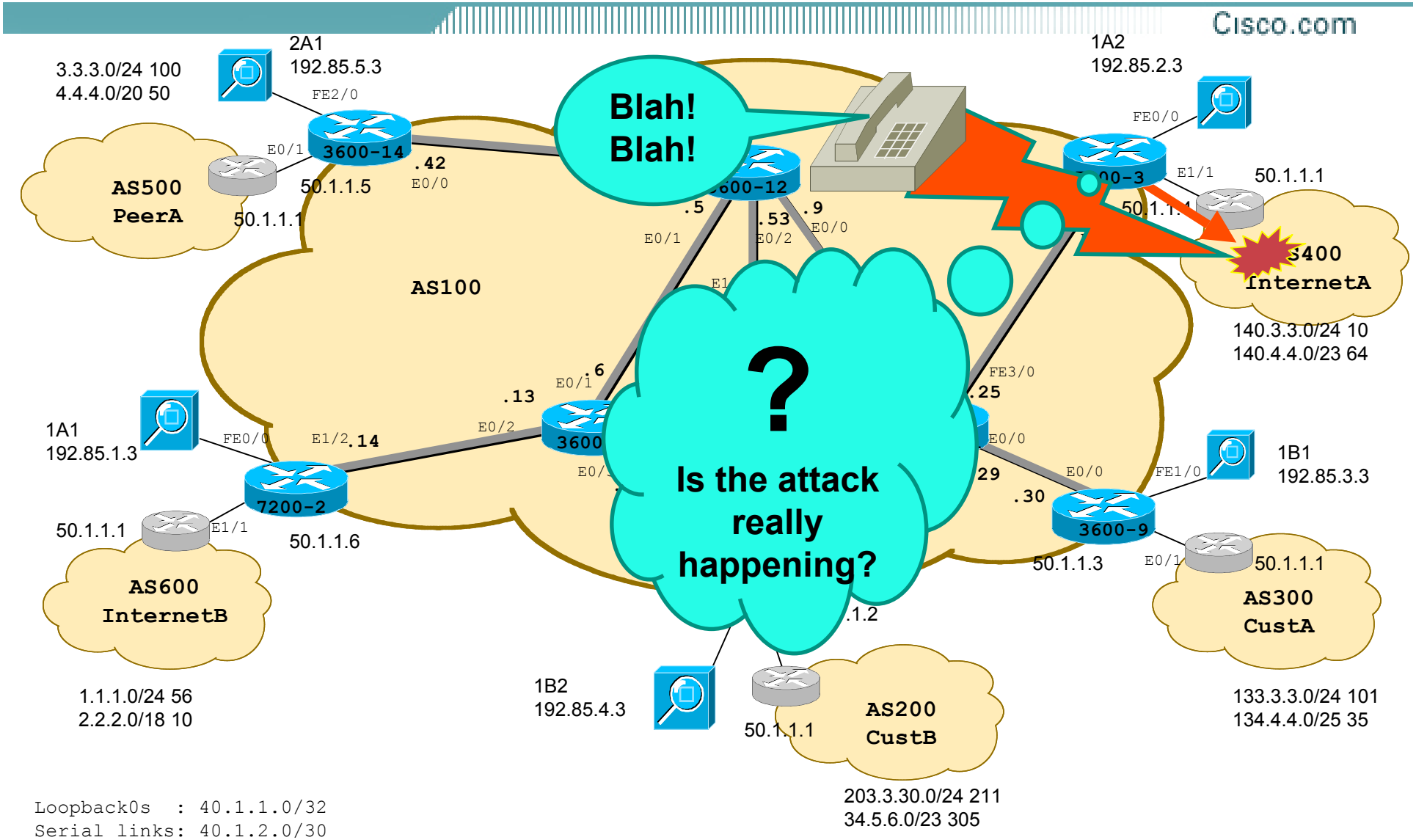
Mitigation Options

- Black hole destination at all gateways or ingress gateway only
- Sinkhole the destination or source of attack
- Use Loose uRPF on source address
- Use ACLs to filter traffic

Attack 2: Customer to Internet DDOS

- Reflective attack on source address
- Spoofed source and destination
- 1B1 dst=2.2.2.1 src=140.3.3.1
- 1B1 dst=34.5.6.1 src=140.3.3.1
- SP calls??
- Identify attack using NF
- Confirm are real addresses? How?
  - ✓ Look at backscatter. and/or
  - ✓ Look at GWs in and out of your NW
- Find source GW
- Options
  - ✓ Blackhole destination at all GWs
  - ✓ LURPF spoofed source
  - ✓ Shutdown Customer connection

LAB Network
SP Calls re attack




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

Check bordering Gateway 3


```
gw-7200-3#show ip cache flow
IP packet size distribution (575785 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416
   .050 .006 .005 .000 .000 .000 .000 .936 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  4 active, 65532 inactive, 3316 added
  55014 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive                     econds
  last clea                    ver
Protocol                           Packets B                     ec)
--------                            /Flow                        w
TCP-Telnet                            44                        .7
TCP-BGP                50     0.0        1                0.0    0.1     15.3
UDP-TFTP                6     0.0     4888                0.4   27.4     15.2
ICMP                    3     0.0        6          7     0.0   14.8     15.5
IPINIP                  4     0.0     404         242     2.4  205.3     15.2
Total:               3312     0.0                 205     3.0    0.7     15.2

SrcIf         S  IPaddress    Dst             DstIPaddress     Pr SrcP DstP  Pkts

SrcIf         Sr IPaddress     stIf           DstIPaddress     Pr SrcP DstP  Pkts
  .
  .
Fa3/0         2.2.2.1         Fa0/0           140.3.3.1        04 0000 0000   350K
Fa3/0         34.5.6.1        Fa0/0           140.3.3.1        04 0000 0000    28K
  .
  .
gw-7200-3#
```

From Gateway 2

From Gateway 13

?

What do these Gateway see?

Check bordering Gateway 2

Cisco.com

```
gw-7200-2#sh ip cache flow
IP packet size distributio
   1-32   64   96  128                                        480
   .000 .000 .000 .000                                          0

    512  544  576 1024
   .000 .000 .000 .0

IP Flow Switching
  2 active, 6553
  3675 ager polls
  Active flows time
  Inactive flows t
  last clearing of
Protocol         T                                         dle(Sec)
--------         Fl                                          /Flow
TCP-BGP             9                                         15.5
IPINIP              4                                         11.8
Total:             13                                  252.8  14.3

SrcIf          SrcIPaddress                    ress    Pr SrcP DstP  Pkts
  .
  .
Fa0/0          2.2.2.1           t1/2          140.3.3.1     04 0000 0000    39K
Et1/2          140.3.3.1         Fa0/0         2.2.2.1       04 0000 0000   138K
  .
  .
gw-7200-2#
```

?

Flow from SP under attack…..
But no flow seen on Gateway 3?
Must be spoofed source!

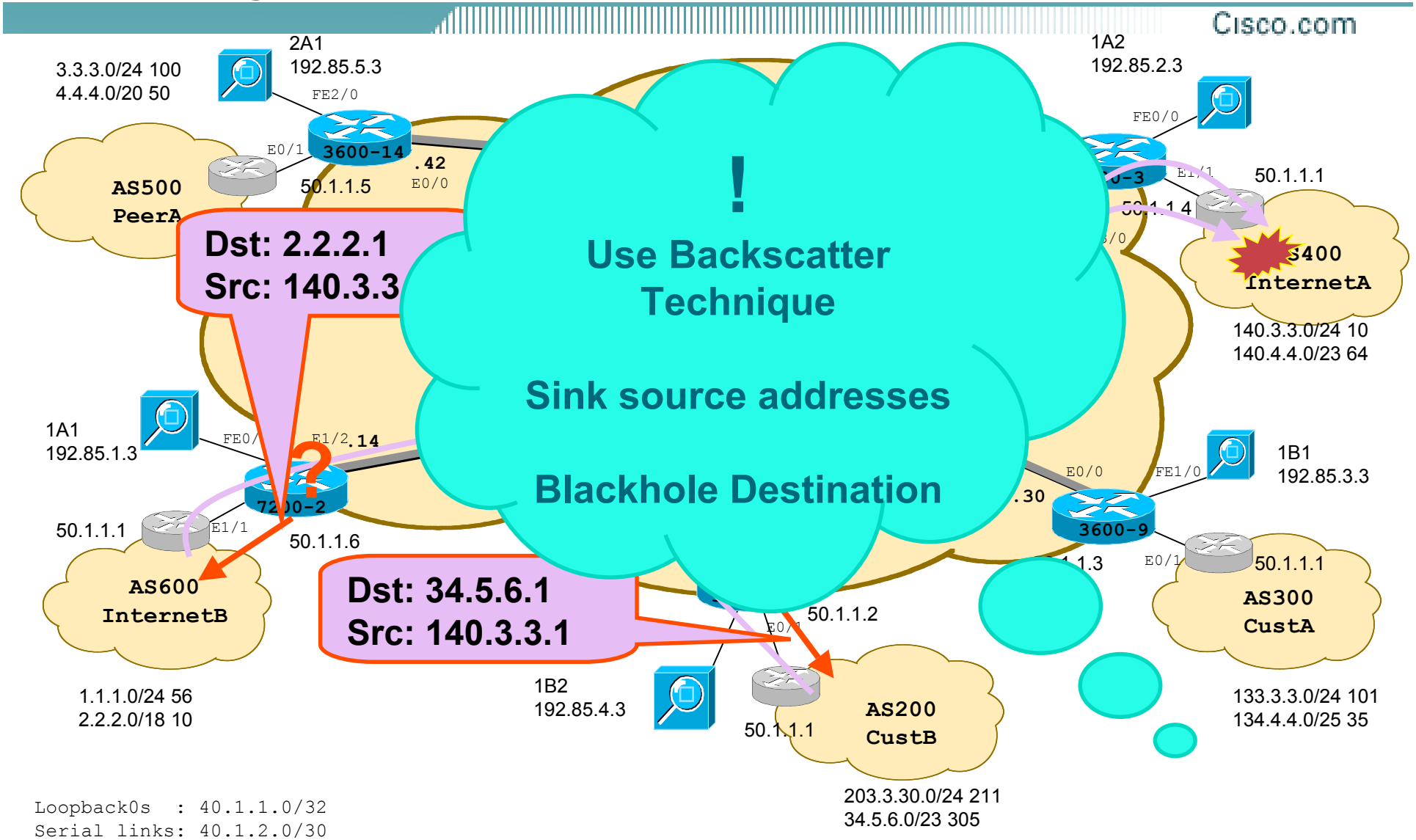
Check bordering Gateway 13


```
gw-3600-13#sh ip cache flow
IP packet size distributio
   1-32   64   96  128                                                  480
   .000 .009 .001 .000                                                    0

    512  544  576 1024
   .000 .000 .000 .0

IP Flow Switching
  4 active, 4092
  128270 ager pol
  Active flows time
  Inactive flows t
  last clearing of
Protocol          T                                                   dle(Sec)
--------          Fl                                                  /Flow
TCP-Telnet         54                                                  14.7
TCP-BGP           4463                                                 15.4
TCP-other            3                                      8.9        15.3
UDP-DNS             10       0.0       4                .0   7.6        15.6
UDP-TFTP             4       0.0       6           0.0      0.0        15.8
UDP-other         1817                 1    323    0.0      0.0        15.4
IPINIP              10              0622    242   27.0   1012.4        10.8
Total:            6850               268    239   27.5      2.9        15.3

SrcIf         SrcIPaddres      stIf          DstIPaddress     Pr  SrcP DstP  Pkts
  .
  .
Et2/0         140.3.3.1        Et0/0         34.5.6.1         04  0000 0000   512K
Et0/0         34.5.6.1         Et2/0         140.3.3.1        04  0000 0000    60K
  .
  .
gw-3600-13#
```

?

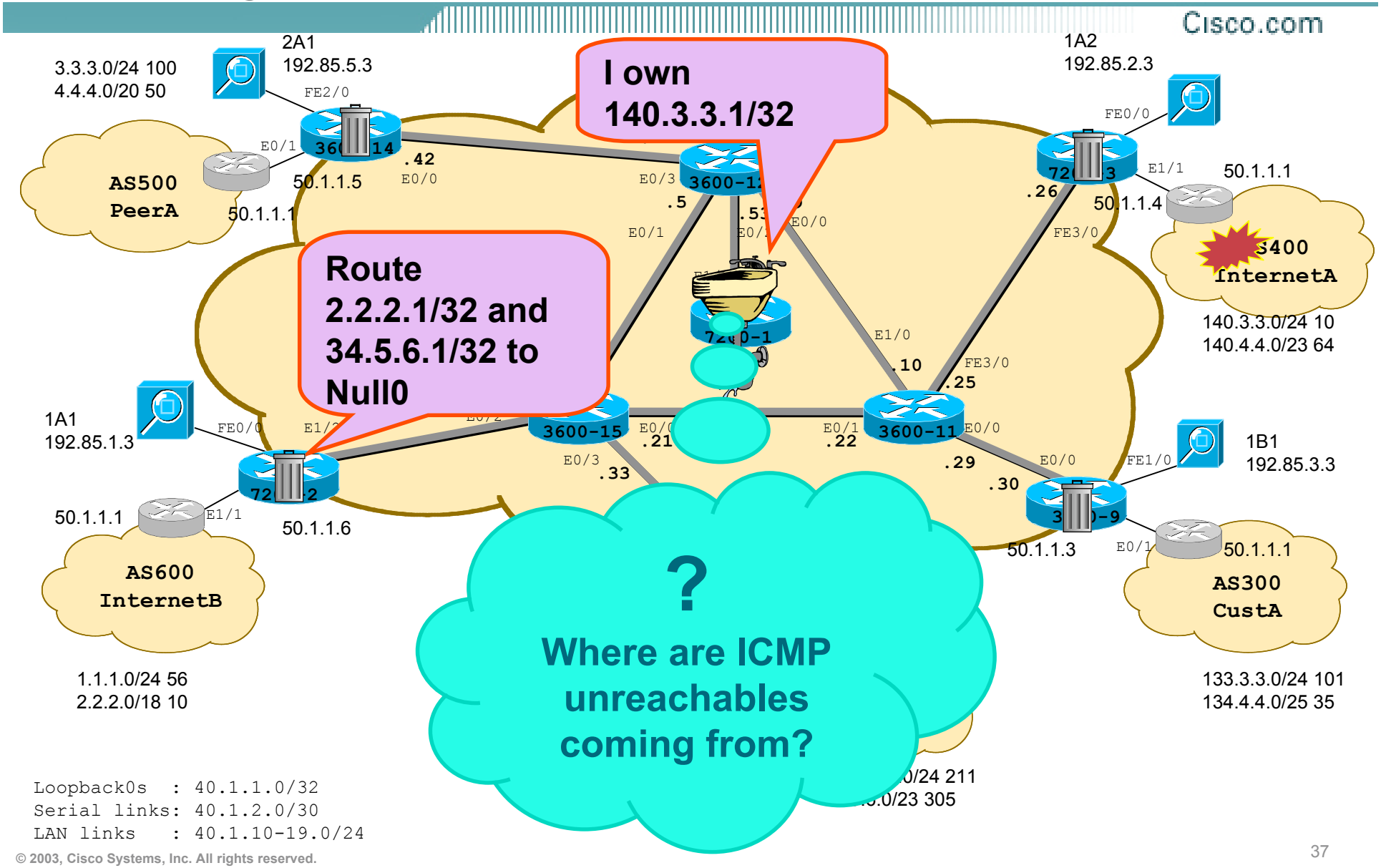
Flow from SP under attack…..
But no flow seen on Gateway 3?
Must be spoofed source!

LAB Network
Tracking down source of spoofed source addresses




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

LAB Network
Tracking down source of spoofed source addresses



Check SinkHole for ICMP unreachables


```
sink-7200-1#show log
  .
  .
*Aug  7 18:10:07.333: %SEC-6-IPACCESSLOGDP: list 170 permitted icmp 192.85.3.1 (Ethernet1/1 0030.9433.a342) ->
140.3.3.1 (0/0), 1 packet
*Aug  7 18:10:49.793: %SEC-6-IPACCESSLOGDP: list 170 permitted icmp 192.85.3.1 (Ethernet1/1 0030.9433.a342) ->
140.3.3.1 (0/0), 21 packets
*Aug  7 18:10:57.705: ICMP: dst (2.2.2.1) administratively prohibited unreachable sent to 140.3.3.1
*Aug  7 18:10:59.345: %SEC-6-IPACCESSLOGDP: list 170 permitted icmp 192.85.3.1 (Ethernet1/1 0030.9433.a342) ->
140.3.3.1 (0/0), 1 packet
*Aug  7 18:10:59.705: ICMP: dst (2.2.2.1) administratively prohibited un    hable sent to 140.3.3.1
*Aug  7 23:39:25.284: %SEC-6-IPACCESSLOGDP: list 170 permitted icmp 192     1 (Ethernet1/1 0030.9433.a342) ->
140.3.3.1 (0/0), 1 packet
*Aug  7 23:40:16.212: %SYS-5-CONFIG_I: Configured from console by cons
*Aug  7 23:45:15.984: %SEC-6-IPACCESSLOGDP: list 170 permitted icmp 1      Ethernet1/1 0030.9433.a342) ->
140.3.3.1 (0/0), 1758 packets
  .
  .
sink-7200-1#show ip access-list 170
Extended IP access list 170
    permit icmp any any log-input (29 matches)
    permit ip any any (97276 matches)
sink-7200-1#
```

192.85.3.1 is the source address of the ICMP packet. This is the address of the Gateway interface sourcing the packet.

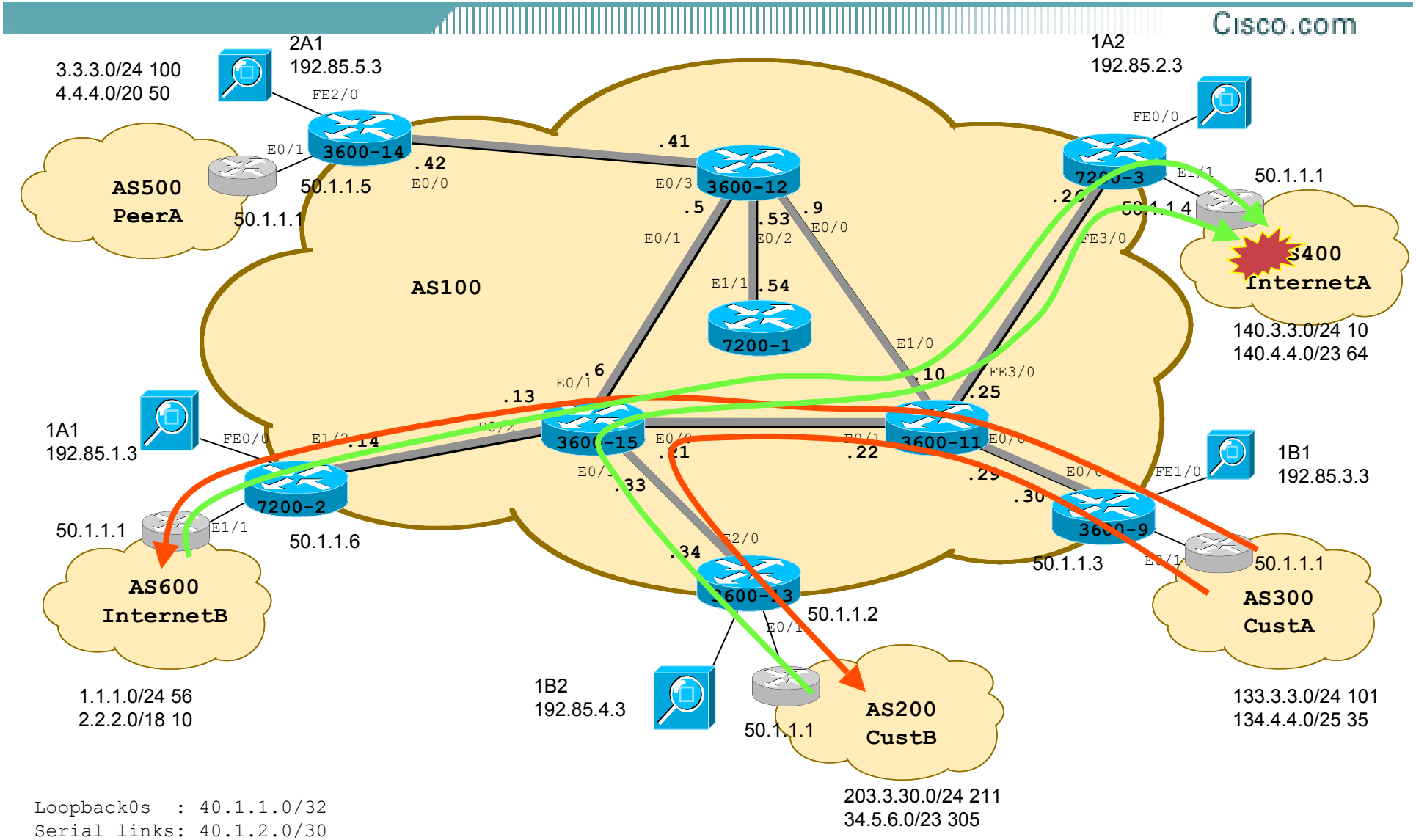
→ Gateway 9

Check bordering Gateway 9

Cisco.com

```
cr-3600-9#sh ip cache flow
IP packet size distribution (12906474 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 14 added
  14560 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IPINIP              12      0.0    949862   242    172.1    1064.8      10.3
Total:              12      0.0    949862   242    172.1    1064.8      10.3

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
  .
  .
Fa1/0         140.3.3.1       Et0/0         34.5.6.1        04 0000 0000   754K
Fa1/0         140.3.3.1       Et0/0         2.2.2.1         04 0000 0000   755K
  .
  .
cr-3600-9#
```

LAB Network
Reflective Customer to Internet Attack Flows




```
Loopback0s   : 40.1.1.0/32
Serial links: 40.1.2.0/30
LAN links    : 40.1.10-19.0/24
```

Mitigation Options

- Black hole destination at all gateways
- Use Loose uRPF spoofed source
- Use ACLs to filter traffic on the ingress interface of gateway router
- Shutdown ISP connection

Attack 6: Attack on SP infrastructure

- Attack core router
- Real source and destination
- 1B1 dst=2.2.2.1 src=140.3.3.1
- 1B1 dst=34.5.6.1 src=140.3.3.1
- NOC Alarm
- Identify attack using NF (or MRTG – CPU trend)
- Confirm are real addresses? How?
  - ✓ Look at backscatter. and/or
  - ✓ Look at GWs in and out of your NW
- Find source GW
- Options
  - ✓ Blackhole destination at all GWs
  - ✓ LURPF spoofed source
  - ✓ Shutdown Customer connection

Mitigation Option

- Increase input hold queue
- Tweak SPD
- Use receive path ACL or control plane feature
- Blackhole infrastructure address at the border router and cease announcement of the connected interfaces (Preparation)

Attack 4: Collateral Damage

- Attack on customer causing resource saturation on the egress interfaces of router
- <add diagram>

Mitigation option

- Tweak with buffer?
- QoS