Sink Hole Deployments
Is it time to change our BGP BCPs?

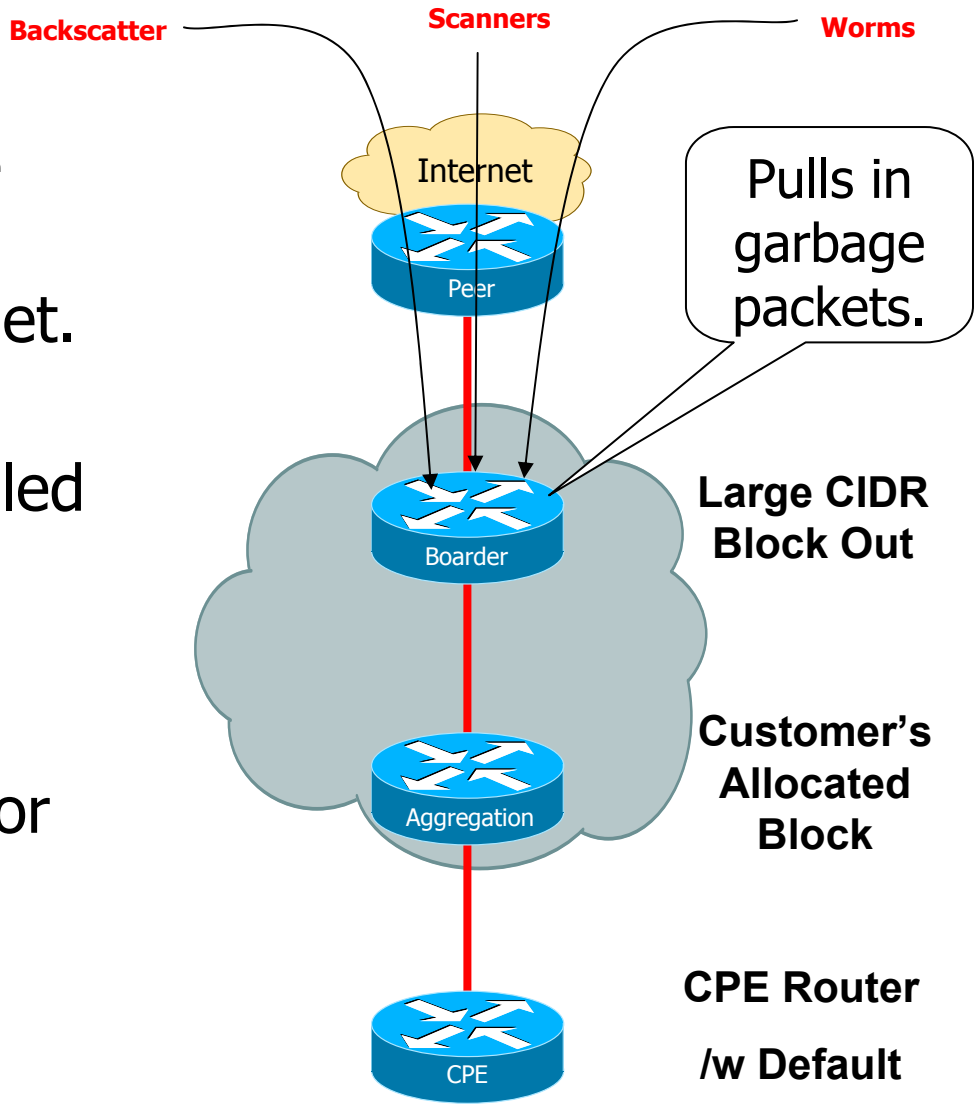
Barry Raveendran Greene
bgreene@senki.org

Sink Hole Deployments and BCPs

- Sink Holes are proving to be valuable ISP Security Tool.
- One of the reasons for this value is built on the premise that you sink undesirable packets to a planned location.
- This same characteristic is created with the BCP techniques used to advertise CIDR prefixes into the Internet.
- Is time to re-look at our BCPs for advertising prefixes?
- Is it time to update RFC 1812 - Requirements for IP Version 4 Routers?

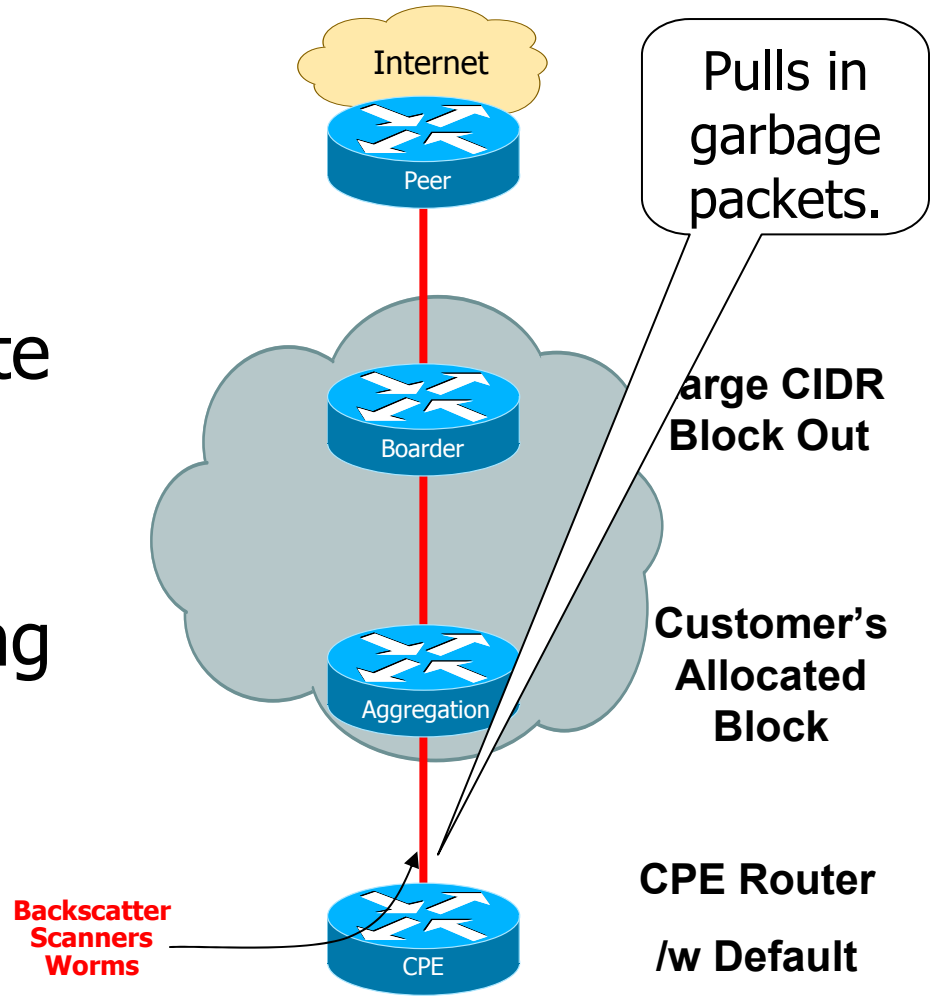
Simple Sink Holes – Internet Facing

- BCP is to advertise the whole allocated CIDR block out to the Internet.
- Left over unallocated Dark IP space gets pulled into the advertising router.
- The advertising router becomes a Sink Hole for garbage packets.



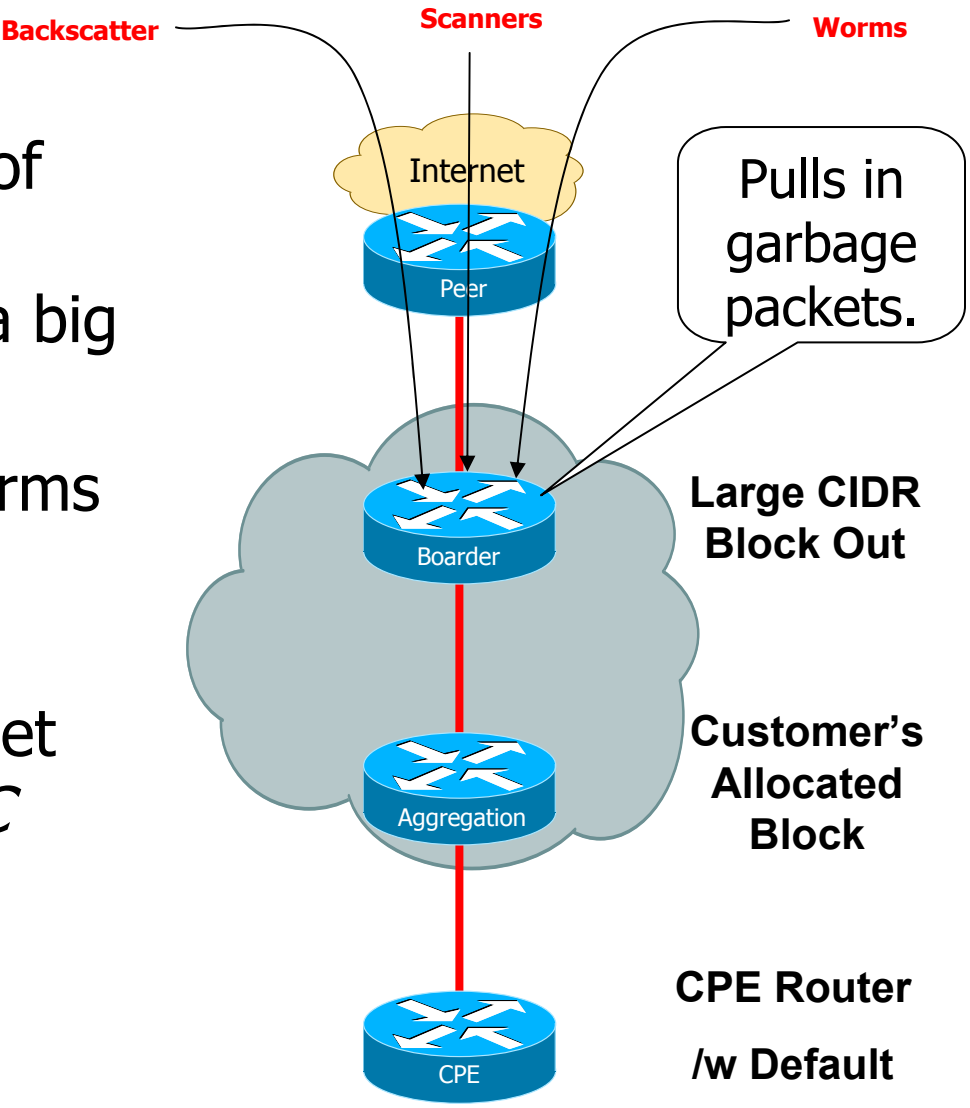
Simple Sink Holes – Customer Facing

- Defaults on CPE devices pull in everything.
- Default is the ultimate packet vacuum cleaner
- Danger to links during times of security duress.



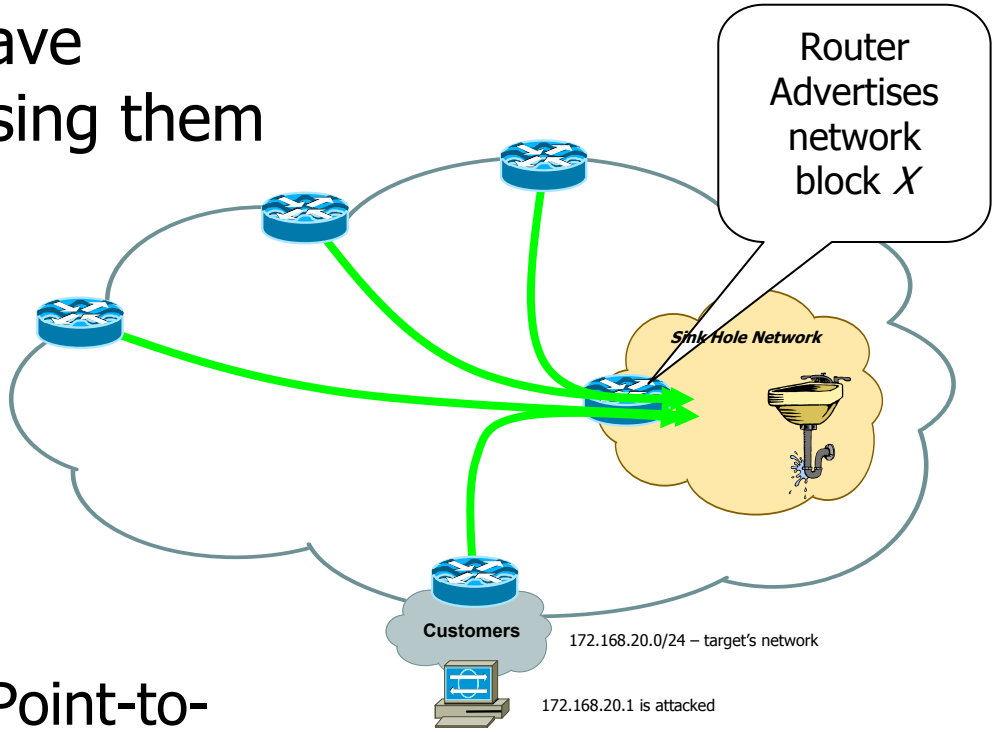
Simple Sink Holes – Impact Today

- In the past, this issue of pulling down garbage packets has not been a big deal.
- GigBots and Turbo Worms changes everything
- Even ASIC based forwarding platforms get impacted from the *RFC 1812 overhead.*

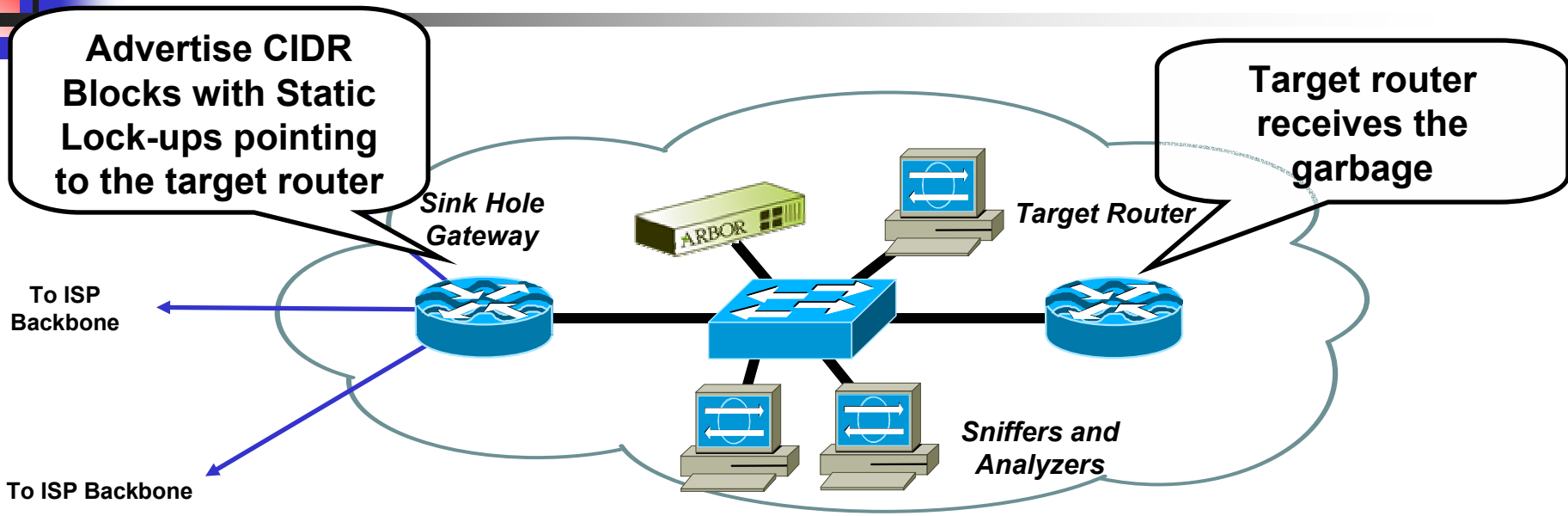


Sink Hole Routers/Networks

- We know that ISPs who have deployed Sink Holes are using them for
  - Attack Mitigation
  - Network Scans
  - Failed Attacks
  - Worm Infection Detection
  - Backscatter
  - Protecting the Backbone Point-to-Point Interface addresses.
  - Managing DOS Flaps
  - Customer Traffic when circuits flap.

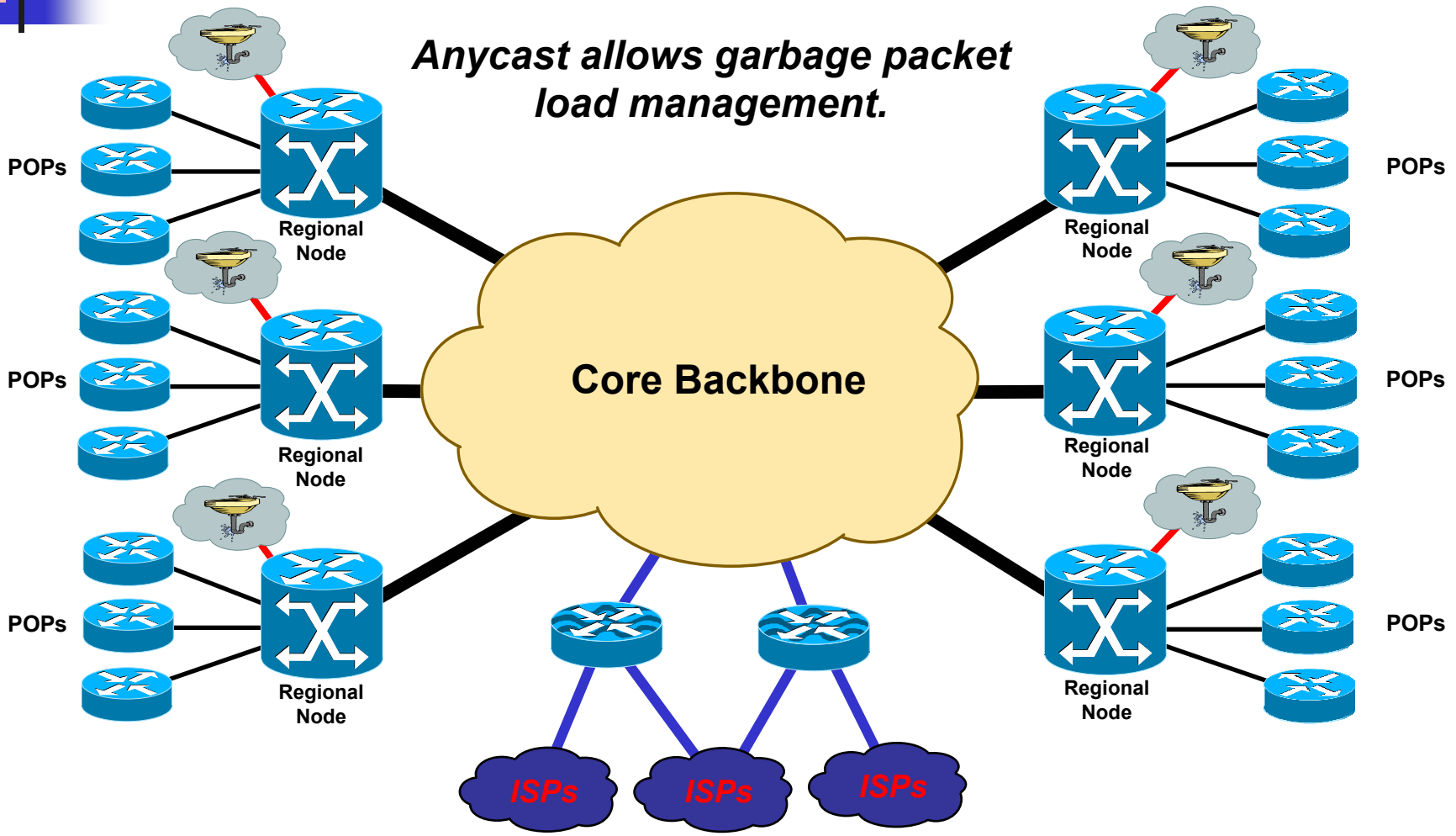


Sink Holes – Advertising Dark IP



- Move the CIDR Block Advertisements to Sink Holes.
- Does not impact BGP routing – route origination can happen anywhere in the iBGP mesh.
- Manages where you drop the packet.
- Turns the packet into a security tool.

Anycast Sink Holes to Scale



IEPG Consultation

- Is it time to change – proactively vs reactively?
- Is it time to change vendor expectations in RFC1812?
- Router Security Requirement Draft?
  - http://www.port111.com/docs/
  - ***Track down George Jones during the IETF <gmj@pobox.com>***
- ***Have you deployed your Sink Hole?***
- ***Is it time to discuss a total compartmentization of the data and control plane?***