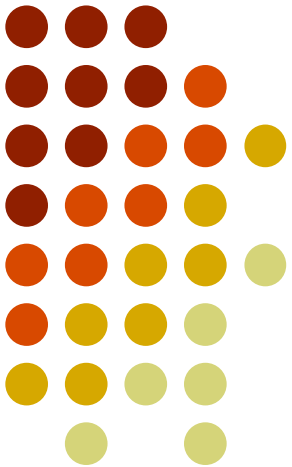
BOGONS AND BOGON FILTERING

Dave Deitrich

Team Cymru
team-cymru@cymru.com
NANOG33 - 01 Feb 2005



The 2-Minute Bogon Tutorial

- A BOGON is a prefix that should never appear in the Internet routing table
- Different types of bogons
  - MARTIANS - private (RFC 1918) and reserved addresses (multicast, loopback)
  - UNALLOCATED - address space that has not yet been assigned to an RIR by IANA
- Just because an address is a bogon doesn't mean it can't be used in a private network

Why filter bogons?

- Prevent private address space in your network from leaking out into the Internet
- Often used in Spam and DDoS attacks
  - In 2001 roughly 60% of attacks came from bogon source addresses
    http://www.cymru.com/Presentations/60Days.ppt
  - In Jan 2005 during one DDoS attack 12% of the source addresses were bogons (Anonymous)
- Miscreants use what works!

Why not filter bogons?

- Actual email received by Team Cymru on December 2nd, 2004:

  I am the Director of Network Services at [University]. We just changed our ISP and in the change received a new set of IP numbers (70.[xxx.xxx.xxx]/25). In the first three days we were on the new IP range, we encountered 6 places that seem to be using your "bogon" list and have not updated it since 70/8 was taken off in January of this year.

- 70/8 allocated to ARIN on January 16, 2004

Why not filter bogons?

- Bogon filters occasionally need to be updated
- Unallocated space doesn't remain unallocated forever

August 2004	71/8 and 72/8 allocated to ARIN
April 2004	85/8 thru 88/8 allocated to RIPE
April 2004	58/8 and 59/8 allocated to APNIC
Jan 2004	70/8 allocated to ARIN
Nov 2003	83/8 and 84/8 allocated to RIPE
April 2003	201/8 allocated to LACNIC
April 2003	60/8 allocated to APNIC
April 2003	223/8 DE-ALLOCATED from APNIC

Why not filter bogons?

- Martians occasionally change as well
  - RFC 3068: 192.88.99.0/24 allocated for use by 6to4 relays (June 01)
- For best results use an automated method to keep your bogon filters up-to-date
- Know your network! Don’t block “bogons” by accident!
  - Example: Internal SMTP Relays

Bogon Route Server Project

- Advertises a list of bogon prefixes via eBGP
- Peers can configure their routers to automatically filter bogon traffic based on prefixes received
- Prefixes are withdrawn as routes are assigned by IANA to an RIR or RFC
- Best of all, you don't have to do anything!

http://www.cymru.com/BGP/bogon-rs.html

Bogon Route Server Project

- Currently 6 route servers online
  - 4 in US, 2 in EMEA
  - Looking for hosting opportunities in AsiaPac
- 507 peering sessions across 228 ASNs

- All route servers use Secure IOS and BGP templates (see www.cymru.com/Documents)

IOS Config Example

```
ip bgp-community new-format
!
ip route 192.0.2.1 255.255.255.255 null0
!
ip community-list 10 permit 65333:888
!
route-map CYMRUBOGONS permit 10
  match community 10
  set ip next-hop 192.0.2.1
```

JunOS Config Example 1

```
routing-options {
    static {
        route 192.0.2.1/32 {
            discard; no-readvertise; retain;
        }}}

policy-options {
    community CYMRU-bogon-community members
      [ no-export 65333:888 ];
    as-path CYMRU-private-asn 65333;
```

JunOS Config Example 2

```
policy-statement CYMRU-bogons-in {
    term 1 {
        from {
            protocol bgp;
            as-path CYMRU-private-asn;
            community CYMRU-bogon-community;
        } then {
            next-hop 192.0.2.1;
            accept;
        }}
     then reject; }
```

More Config Examples

- Examples for Cisco IOS, Juniper JOS and OpenBGP available at: http://www.cymru.com/BGP/bogon-rs.html
- Use communities to filter types of bogons
  - 65333:888 - All bogons
  - 65333:890 - Martians only
  - 65333:892 - Unallocated only
- Use prefix lists to block announcements for bogons that you use internally

Other Methods

- Bogon lists are also available as:
  - Text lists (aggregated & unaggregated)
  - BIND Templates
  - Prefix Lists (Juniper/Cisco)
  - RADB, RIPE NCC, DNS
  - Mailing list for change announcements
- Visit http://www.cymru.com/Bogons/ for details

Please Don't Do This

From: System Administrator
Sent: Monday, August 16, 2004 5:05 PM
To: <person@someisp.net>
Subject: Undeliverable: test

The following recipient(s) could not be reached:
<person@someisp.net> on 8/16/2004 5:05 PM

451 Contact Team Cymru
<team-cymru@cymru.com> for questions.

Useful Links

http://www.iana.org/assignments/ipv4-address-space

http://www.cymru.com/Bogons/

http://www.completewhois.com/bogons/

http://www.sixxs.net/tools/grh/bogons/

http://www.cidr-report.org/#Bogons

Useful Links

http://www.ris.ripe.net/debogon

ftp://ftp-eng.cisco.com/cons/isp/security/

- Remote-Triggered-Black-Hole-Filtering-02.pdf
- Ingress-Prefix-Filter-Templates

http://www.cymru.com/gillsr/documents/

- junos-isp-prefix-filter-loose.htm
- junos-isp-prefix-filter-strict.htm

THANK YOU!

If you have any comments or questions please feel free to contact us at:

team-cymru@cymru.com

http://www.cymru.com