CSE508  Network Security

9/14/2017  Core Protocols: BGP

Michalis Polychronakis
Stony Brook University
IP Addressing and Forwarding

Packets are routed based on their dst. IP address

Router’s task: for every possible IP address, forward packet to the next hop

  Table lookup for each packet in a routing table

For 32-bit addresses, $2^{32}$ possibilities! $\Rightarrow$ impractical

**Solution:** hierarchical address scheme

<table>
<thead>
<tr>
<th>IP:</th>
<th>Network</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Known by all routers* $\quad$ *Known by edge/internal (LAN) routers*
## IPv4 Address Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Subnet Mask</th>
<th>Host Bits</th>
<th>Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0 7 8 15 16</td>
<td>Host</td>
<td>1.0.0.0 to 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>10 11 12 13</td>
<td>Host</td>
<td>128.0.0.0 to 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>110 111 112</td>
<td>Host</td>
<td>192.0.0.0 to 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td>1110 1111</td>
<td>Multicast</td>
<td>224.0.0.0 to 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td>1111</td>
<td>Reserved</td>
<td>240.0.0.0 to 255.255.255.255</td>
</tr>
</tbody>
</table>
This chart shows the IP address space on a plane using a fractal mapping which preserves grouping -- any consecutive string of IPs will translate to a single compact, contiguous region on the map. Each of the 256 numbered blocks represents one /8 subnet (containing all IPs that start with that number). The upper left section shows the blocks sold directly to corporations and governments in the 1990s before the RIRs took over allocation.
Autonomous Systems

AS: collection of connected IP routing prefixes belonging to a single administrative entity

- Presents a common routing policy to the internet

AS number defined as 16-bit integer

- ~47,000 ASNs as of 2014, assigned by IANA
Map of the internet, 1982

Ovals: sites/networks
Rectangles: routers

Created by Jon Postel
CAIDA’s IPv4 AS Core
AS-level INTERNET GRAPH

Skitter January 2000

copyright © 2000 UC Regents. all rights reserved.
Internet Routing

Routers speak to each other to establish internet paths
  Exchange topology and cost information
  Calculate the best path to each destination

*Intra-domain* routing: set up routes within a single network/AS

  **RIP** (Routing Information Protocol): distance vector
  **OSPF** (Open Shortest Path First): link state

*Inter-domain* routing: set up routes between networks

  **BGP** (Border Gateway Protocol)
  Advertisements contain a prefix and a list of ASes to traverse to reach that prefix
Internet Routing
BGP

The de facto standard inter-AS routing protocol in today’s Internet

Main goals

Obtain subnet reachability information from neighboring ASs
Propagate the reachability information to all internal routers
Determine “good” routes to subnets based on the reachability information and AS policy

BGP is what enables subnets to advertise their existence to the rest of the Internet
Root Causes of BGP Security Issues

No authentication of path announcements
  Neighbor adjacencies can be “secured” using MD5 digests

BGP messages are sent over TCP connections
  All the usual problems: eavesdropping, content manipulation, …

Misconfigurations are easy
  BGP is a complex protocol, with complex interactions

**Attackers can lie to other routers**
Routing Attacks

Blackholing
False route advertisements to attract and drop traffic

Redirection
Force traffic to take a different path, either for interception (MitM) or to cause congestion

Instability
Frequent advertisements and withdrawals and/or increased BGP traffic to cause connectivity outages

How?
Configuration mistakes
Insider attacks
Compromised routers
BGP traffic manipulation
Prefix Hijacking

Announce someone else’s prefix

Victim prefers the *shortest* path
Prefix Hijacking

Announce a more specific prefix than someone else

Victim prefers the *more specific* path

![Diagram showing Prefix Hijacking]

User

AS1

AS2

AS3

AS4

AS5

10.0.0/24

10.0.0/25
BGP leak causing Internet outages in Japan and beyond.

Posted by Andree Toonk – August 25, 2017 - BCP instability - No Comments

Yesterday some internet users would have seen issues with their internet connectivity, experiencing slowness or parts of the Internet as unreachable. This incident hit users in Japan particularly hard and it caused the Internal Affairs and Communications Ministry of Japan to start an investigation into what caused the large-scale internet disruption that slowed or blocked access to websites and online services for dozens of Japanese companies.

In this blog post we will take a look at the root cause of these outages, who was affected and what networks were involved.

Starting at 03:22 UTC yesterday (Aug 25) followers of @BGPstream would have seen an increase in alerts involving Google. The BGPstream alerts were informing us that Google was announcing the peering lan prefixes of a few well known Internet exchanges. This in itself is actually a fairly common type of incident and typically indicates something isn’t quite right within the networks hijacking those prefixes and so these alerts were the first clues that something wasn’t quite right with Google’s BGP advertisements.
Pakistan’s Accidental YouTube Re-Routing Exposes Trust Flaw in Net

BY RYAN SINGEL  02.25.08 | 10:37 AM | PERMALINK

Secure Your Cloud

Free download: Best Practices For Ensuring Cloud Compliance.

Threat Protection Tool
C++ Static Analysis
AVG® Business Research
Security White Papers
Cisco® ACI Virtualization
IoT Security Explained
Immediate Risk Assessment
Government: you have to block this YouTube video

Pakistan Telecom: OK

Use URL filtering?
No

Change the DNS record?
No

Use IP blocking?
No

Blackhole 208.65.153.0/24?
Yes!
AS36561 (YouTube) announces 208.65.152.0/22
The prefix 208.65.153.0/24 is not announced on the Internet before the event.
AS17557 (Pakistan Telecom) announces 208.65.153.0/24
Other Notable Incidents

April 2010: China Telecom announced bogus paths to 50,000 IP prefixes
   Enabled traffic interception

February 2014: hijacking of 51 networks (incl. Amazon, Digital Ocean, OVH)
   Miner connections were redirected to an attacker-controlled mining pool
   Attacker collected the miners’ profit (est. $83,000 in 4 months)
Mitigating BGP Threats

Neighbor authentication

Only authorized peers can establish a given BGP neighbor relationship

TTL check

Most external peering sessions established between adjacent routers
Good idea: set TTL=1 ➔ an attacker X hops away can still set TTL=1+X
Better idea: set TTL=255 and accept only packets with TTL=255 ➔ an attacker further away cannot spoof such a packet

BGP prefix restrictions and filtering

Accept only a certain number of prefixes, ignore unwanted/illegal prefixes, limit the number of accepted AS path segments, …

ACLs to explicitly permit only authorized BGP traffic

According to existing security policies and configurations
Securing BGP

Secure BGP (S-BGP)
  Each node signs its announcements

Resource Public Key Infrastructure (RPKI)
  Certified mapping from ASes to public keys and IP prefixes

Secure origin BGP (soBGP)
  Origin authentication + trusted database that guarantees that a path exists

BGPPSec
  Allow recipients to validate the AS path included in update messages

Many deployment challenges
  No complete, accurate registry of prefix ownership
  Need for a public-key infrastructure
  Cannot react rapidly to changes in connectivity
  Cost of cryptographic operations
  Incremental deployment not always possible