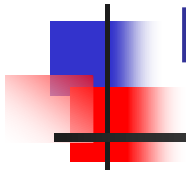
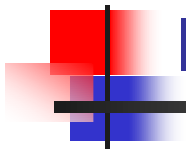


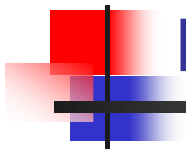
# BGP Security Update

Is the Sky Falling?



# Is the Sky is Falling

- Post 9/11 – lots or people looking at “critical infrastructure”
- Lots of people see the Internet as “critical infrastructure”
- What’s critical to the operations of the Internet:
  - BGP
  - DNS
  - Caffeine
- Is there a *security* problem with BGP?
- There is S-BGP, hence there must be a problem.



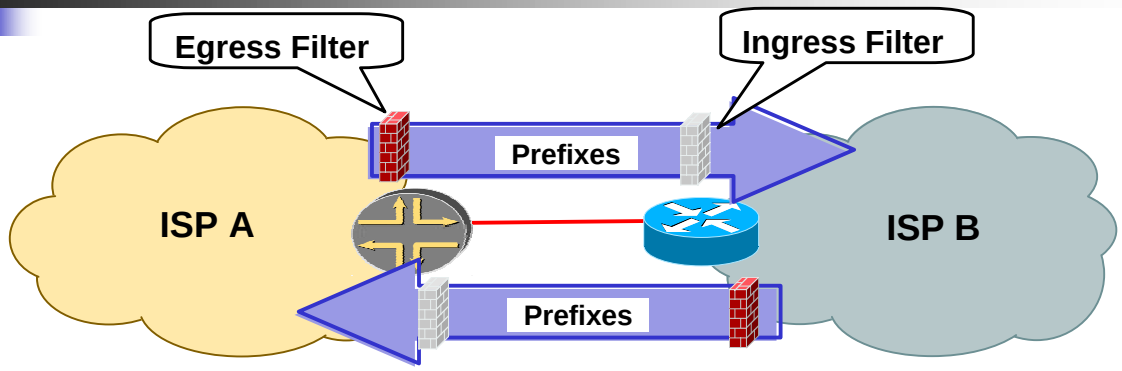
# Background

- Perception that we have a big BGP security problem.
- Comparison of CERT, FIRST, and Cisco PSIRT data was not demonstrating the evidence.
- US Government Pressure – Secure BGP (not the same as S-BGP)
- Answer – lets do some work and really evaluate the risk.

# The Good News

- Our *Luck* still hold outs.
- BGP *Security* is a by-product from our hard learned operational lessons:
  - CIDR
  - Dampening
  - Ingress/Egress Filtering
- BCP Principles for how you configure BGP in an ISP builds a lot of resistance into the Network.

# Guarded Trust




- ISP A trust ISP B to send X prefixes from the Global Internet Route Table.
- ISP B Creates a egress filter to insure only X prefixes are sent to ISP A.
- ISP A creates a mirror image ingress filter to insure ISP B only sends X prefixes.
- ISP A's ingress filter reinforces ISP B's egress filter.

# What are we trying to achieve?

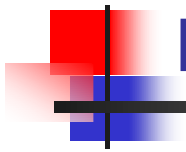
- Walk through the perceived risk.
- Remind people what we should be doing (BCPs).
- Encourage participate in the “what’s next” efforts.

# Spoofing Risk

- “It is really easy to send a TCP RST and drop the BGP session.”
- Harder than you think.
- Successful Spoof may require:
  - Match source address
  - Match source port
  - Match destination port
  - Match TTL
  - Match Sequence Number

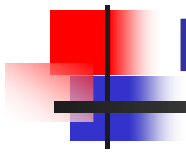
# Spoofing Risk

- Multiple items need to be spoofed. Take time, takes some crafting, and may need direct access to the L1/L2 medium.
- Still can be done, but it is not something you will find in a script kiddy tool.
- And then there is MD5 – adding more resistance.



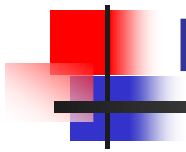
# Hijacking Risk

- “Hey, I can spoof and insert a BGP update into the router.”
- Successful spoof is required.
- Update has to match the ISP’s ingress policy (if iBGP)
- If successful, some interesting things might happen.
  - See work by Sandra Murphy in the references section.



# Route Flapping Risk

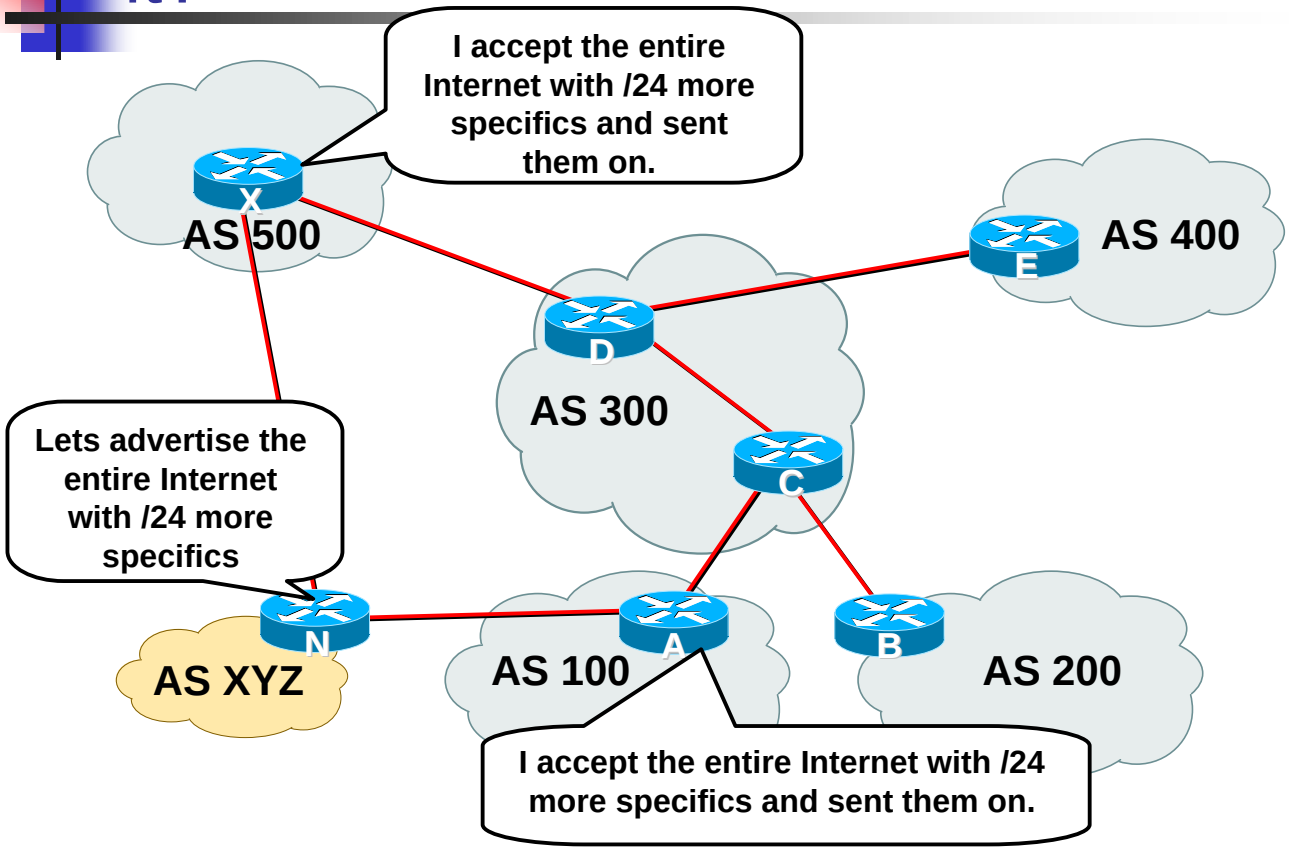
- Route Flapping is an operational risk that could be turned into a security risk ..... If you ignore the BCPs.
- RIPE-229 - *RIPE Routing-WG Recommendations for Coordinated Route-flap Damping Parameters*



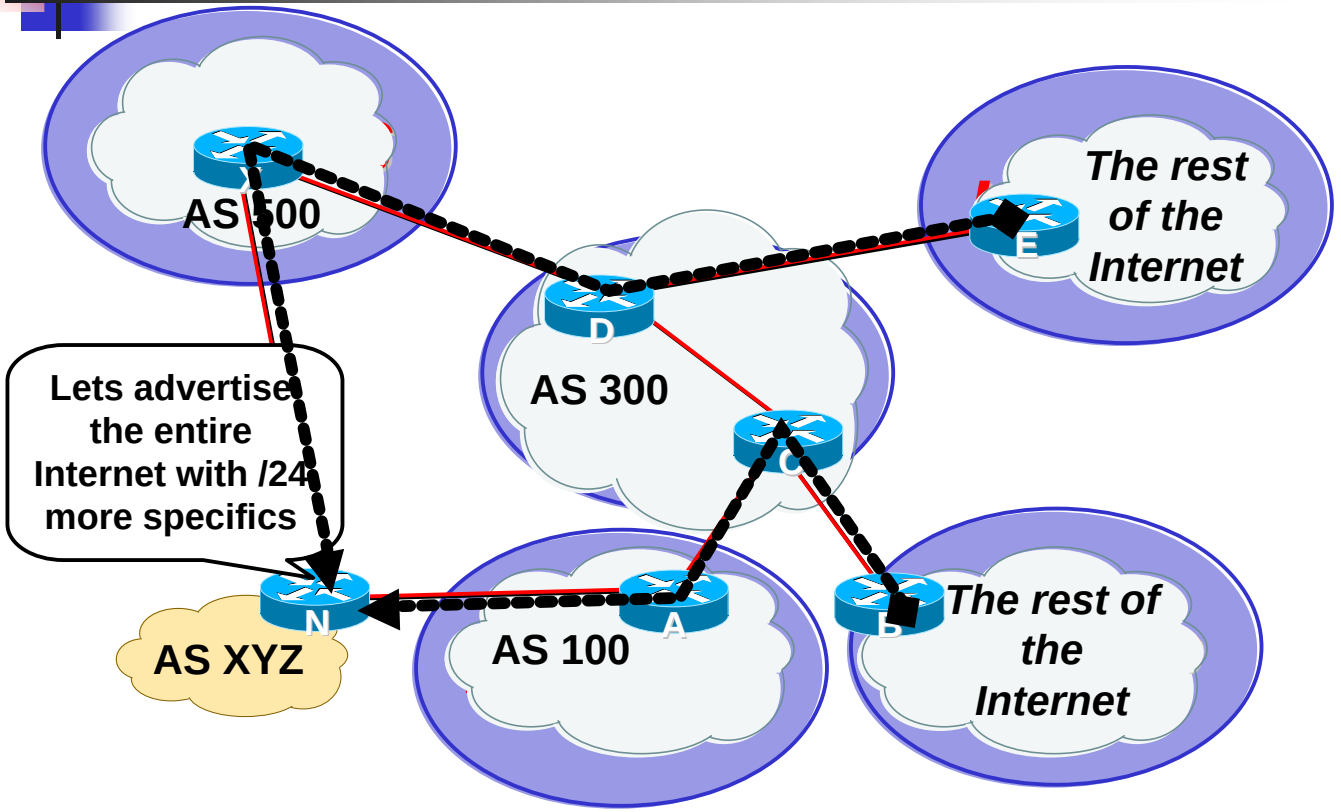
# De-Aggregation Risk

- AS 7007 incident used as an attack.
- Multihomed CPE router is violated and used to “de-aggregate” large blocks of the Internet.
- Evidence collected by several CERTs that hundreds of CPEs are violated.

# *Garbage in – Garbage Out:* What is it?

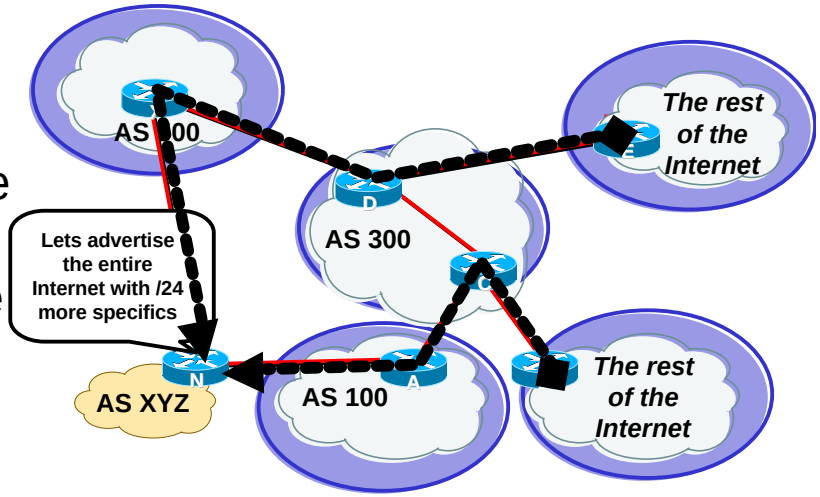


# *Garbage in – Garbage Out:* Results



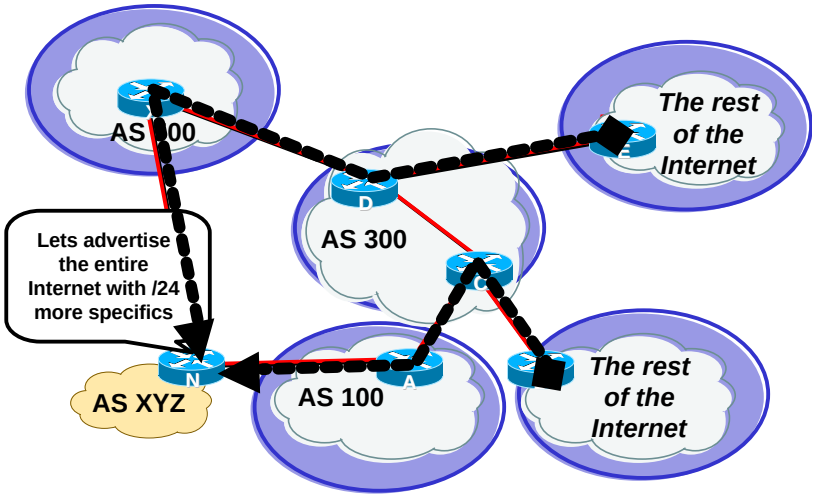
# *Garbage in – Garbage Out:* Impact

- Garbage in – Garbage out does happen on the Net
- AS 7007 Incident (1997) was the most visible case of this problem.
- Key damage are to those ISPs who pass on the garbage.
- Disruption, Duress, and Instability has been an Internet wide effect of Garbage in – Garbage out.



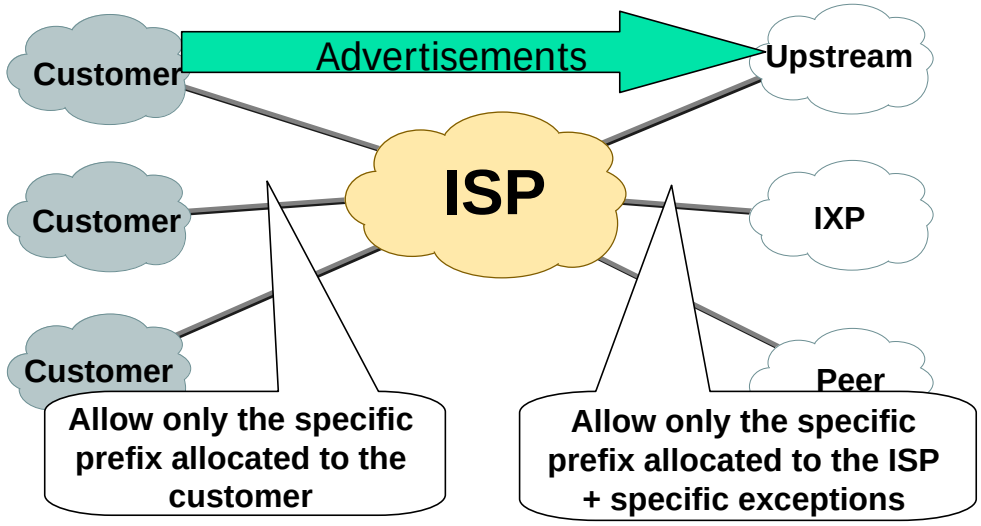
# *Garbage in – Garbage Out:* What to do?

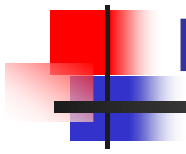
- Take care of your own Network.
  - Filter your customers
  - Filter you advertisements
- Net Police Filtering
  - Mitigate the impact when it happens
- Prefix Filtering and Max Prefix Limits



# Ideal Customer Ingress/Egress Route Filtering ….

- Ingress Customer – Allow only what their allocated
- Egress Customer – Allow only what you are allocated





# DUSA Route Injection

- Documenting Special Use Addresses (DUSA)
- IANA has reserved several blocks of IPv4 address for special use.
  - http://www.iana.org/assignments/ipv4-address-space
- These blocks of IPv4 addresses should never be advertised into the global Internet Route Table.
- Filters should be applied on the AS border for all inbound and outbound advertisements.

# Documenting Special Use Addresses (DUSA)

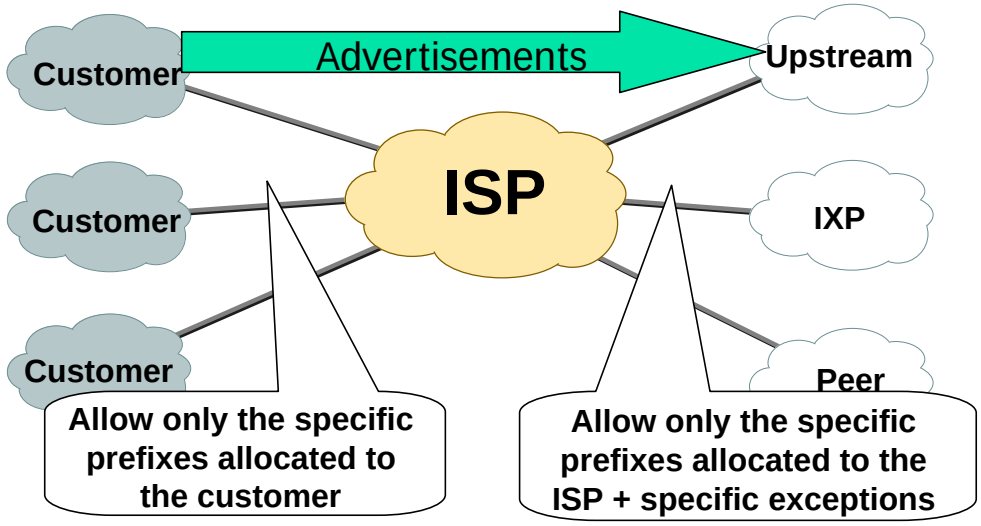
- Details are highlighted in a IETF Internet Draft:
  - http://www.ietf.org/internet-drafts/draft-manning-dsua-07.txt
  - http://search.ietf.org/internet-drafts/draft-iana-special-ipv4-03.txt
- Short cut – Rob Thomas's Templates:
  - http://www.cymru.com/Documents/

# Un-Authorized Route Injection

- “What would happen if I advertised a more specific prefix for content provider abc.com?”
- This has and will happen.
- Might turn into a double DOS – more specific shuts down traffic to “target prime” while it also sucks in traffic to the CPE.

# Un-Authorized Route Injection

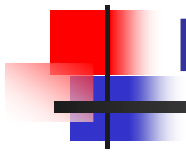
- Ingress Customer – Allow only what their allocated
- Egress Customer – Allow only what you are allocated



# Un-Allocated (Bogon) Route Injection Risk

- “What will happen if I advertise a big block of bogons?”
- One big Backscatter Collector!
- Put bogon filtering into your ingress/egress prefix filtering scheme.

# Direct DOS/DDOS Against the Router



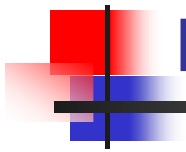
- “Lets syn flood a router on port 179.”
- Not really a “BGP” attack. Really a resource saturation attack.
- Saturating input queues will have a side effect of knocking off the routing protocols.
- Most common form of “BGP Attack.”
- Every network vendor should now be putting mitigation techniques all the way into the forwarding/feature ASIC.

# Risk related to ISP's Architecture

- Summer of 2001 - ISP Routers advertising default became Code Red and Nimda magnets.
- ISP architecture does effect security.
- Plan where you drop the garbage, so when the garbage piles up it doesn't bury your network.

# Risk related to BGP Bugs

- BGP Bugs have caused operation *issues* on the Net, but are caught and fixed before they can be used as a security exploit.
- Some vendor interaction bugs have been scary.
- Providers need to push inter-vendor compatibility/interaction testing.



# BGP Community Attribute Risk

- “What would happen if I started poking around with all those community attributes?”
- Un-explored exploit vector.
- Community filtering equivalent to prefix filtering.
- Not perceived to be a problem, but something to think about.

# What's Next?

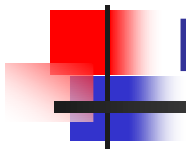
- BGP over IPSEC
- S-BGP
- Ptomaine
- RPSEC
- Router Security Requirements

# BGP over IPSEC

- “If I put BGP over IPSEC, I’ll be secure.”
- Why?
- Remember the difficulty spoofing BGP – especially with MD5.
- Wait – if most ISPs do not turn on MD5, how will IPSEC get turned on?
- Think about the problem your trying to solve.

# S-BGP

- Time to re-visit S-BGP
- Everyone one should read (or re-read) the work:
  - http://www.net-tech.bbn.com/sbgp/
- As a minimum, it covers in detail problems we have with prefix authentication.

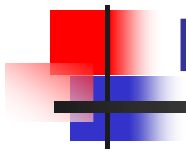


# Ptomaine

- Ptomaine and BGP Security?
- Yep – it is all about prefix filtering techniques. We know effective prefix filtering techniques help the BGP Security.
- *Prefix Taxonomy Ongoing Measurement & Inter Network Experiment* (Ptomaine)
  - General Discussion:ptomaine@shrubbery.net
  - To Subscribe: majordomo@shrubbery.net
  - In Body: subscribe ptomaine
  - Archive: http://www.shrubbery.net/ptomaine

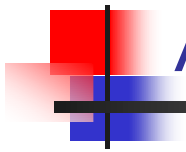
# RPSEC

- **Routing Protocol Security Requirements Working Group (rpsec)**
- **Mailing Lists:**
  - **General Discussion: rpsec@ietf.org**
  - **To Subscribe: rpsec-request@ietf.org**



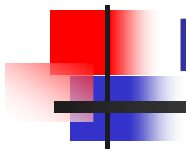
# Router Security Requirements

- *Network Security Requirements for Devices Implementing Internet Protocol* by George Jones (george@UU.NET)
- Work from UUNET that supplements RFC 1918.
- Preliminary work that will be taken to IETF (informational RFC or WG – not sure yet).
- Objective – RFC to whack Vendors with.
- Active Participation welcome:
  - `General Discussion: netsec-reqs@uu.net`
  - `To Subscribe: netsec-reqs-request@uu.net`



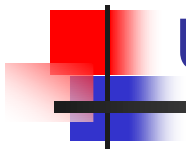
# Acknowledgements


- Rob Thomas [robt@cymru.com]
- Daniel P (Dan) Koller [dpkoller@lucent.com]
- Stephen Kent [kent@bbn.com]
- Ross Callon [rcallon@juniper.net]
- Russ White [ruwhite@cisco.com]
- Alvaro Retana [aretana@cisco.com]
- John G. Scudder [jgs@cisco.com]
- Barry Friedman [friedman@cisco.com]
- Anantha Ramaiah [ananth@cisco.com]
- Satish Mynam [mynam@cisco.com]
- Chris M. Lonvick [clonvick@cisco.com]
- Paul Donner [pdonner@cisco.com]



# References

- Secure BGP Template Version 2.1
  - http://www.cymru.com/Documents/secure-bgp-template.html
- Bogon List v1.0 04 June 2002
  - http://www.cymru.com/Documents/bogon-list.html
- BGP Security Protections
  - draft-murphy-bgp-protect-00.txt
- BGP Security Vulnerabilities Analysis
  - draft-murphy-bgp-vuln-00.txt
- Cisco ISP Essentials
  - http://www.ciscopress.com
  - http://www.ispbook.com



# Updates

- Check for updates at:
  - http://www.cisco.com/public/cons/isp/security/
  - http://www.ispbook.com