BCOP Around the World

RIPE69, London England, UK, 3-11-2014

Aaron Hughes, 6connect

About

- The Best Current Operational Practice (BCOP) project is collecting the best practices known within the operations community and capturing those practices in a series of documents. These “living documents” are peer reviewed by technology experts who actually deploy and manage these environments. We believe the best documentation is when it is based on real-world implementations.
- This is a community project and is open to all to participate and get involved. We welcome your participation and look forward to working together to build better documentation for the entire community.

NANOG BCOP Committee

- The Best Common Operator Practice Ad Hoc Committee is responsible for creating industry recognized publications via the NANOG BCOP website. BCOP is a NANOG community project and open to all that wish to participate and get involved.
- Chair: Chris Grundemann, Vice Chair: Aaron Hughes
- Members: Bill Armstrong, Mark Calkins, Yardiel Fuentes, Shawn Hsiao, Erik Muller
- Participants: Anyone, you. Open to the world.

NANOG62 Update

- 6 Oct 2014:
- DDoS/DoS Attack (Yardiel Fuentes)
- eBGP Configuration (Bill Armstrong)
- Public Peering Exchange (Shawn Hsiao)
- Ethernet OAM (Mark Calkins)
- BCP38 / Anti Spoof WIP
- BCOP Around the world
- Call for Appeals (http://bcop.nanog.org/index.php/Appeals)
- Call for SMEs
- Open mic

DDoS/DoS Attack BCOP

Yardiel Fuentes, NANOG 62 - Baltimore, MD

Participants

- Shepherd: Yardiel Fuentes
- Current SMEs:
  - Rich Compton
  - Prabhu Gurumurthy
  - Damon Fortune
  - John W
  - Yardiel Fuentes
- Other contributions from:
  - Link King

BCOP Summary

- This BCOP aims to share practices which have performed in production environments as a guide on what to do before, during, and after a DDoS/DoS attack.

- This BCOP document focuses on providing, in a vendor-agnostic framework, guidelines at the different stage of dealing with DDoS/DoS attacks

- Check out http://bcop.nanog.org/index.php/BCOP_Drafts

BCOP Background

- This BCOP is needed because of the increase number and intensity of DDoS/DoS attacks NANOG engineers have to willing or unwillingly deal with.
- The need for practical info obtained from defending production networks
- Effort was triggered by multiple requests for information, the NANOG email list “frequent topics” and track recommendations

Draft BCOP Outline

- What to do prior to a DDoS/DoS attack:
  - Customized packet filtering (Firewall Filters, ACLs)
  - Disable open recursion for internal DNS with explicit external trusted DNS servers.
  - Identify and mitigate open relays (open resolver/ Shadowserver) including in your customer's networks
  - Consider DDoS/DoS mitigation subscription services
  - Be familiar with your network's normal session traffic patterns

Draft BCOP Outline

- What to do during a DDoS/DoS attack:
  - Implement passive collection of data (Jflow, net flow, port mirroring, taps)
  - Establish baselines of normal traffic as reference for identifying DDoS/DoS flood traffic
  - Deploy DoS mitigation solutions and additional options (including Flowspec) for NLRI rate-limiting
  - Seek to identify the Type of DDoS attack (TCP win 0, Synfloods, single-source UDP/LOIC-based, botnet, etc)

Draft BCOP Outline

- What to do after a DDoS/DoS attack:
  - Identify the type of DDoS/DoS attack via collected data analysis. Port-mortem analysis is useful
  - Check if FFs/ACLs could be fine tuned to prevent re-occurrences
  - (controversial point) If decision is to notify authorities, the IC3 and FBI official stand is that they are interested in being informed about these.
  - Share your DDoS/DoS attack details with NANOG community (such as this BCOP)

“Nice to have” Content

- What sensible approaches or steps in addressing DoS/DDoS attacks are not as effective as initially considered ?
- Have you found legal or law enforcement agencies helpful at all ? — names/details welcome…
- Should an FAQ or brief educational session be included in this BCOP ?
- Comments Welcome — email me…

Join Us!

- Are you interested in DDoS/DoS Attacks?
- Do you have real-world experience with DoS Attacks?
- Are you interested in helping the NANOG community address DoS attacks ?
- Get involved!
  - Flexible time commitment (all interactions done via email)
  - Contribute as much or as little as you can
  - The more voices we can include the better
  - Email yardiel@gmail.com to join this BCOP team

eBGP Configuration BCOP

Bill Armstrong, NANOG 62, Baltimore, MD, 10-6-2014

The Wire Edition

BCOP Summary

- This BCOP aims to provide a singular, consistent view of industry standard eBGP interconnection methodologies
- This BCOP will also document pre and post turn-up validation practices and IRR Etiquette
- The primary focus of this BCOP is eBGP KNOW-HOW

BCOP Background

- Although eBGP peering sessions are turned up everyday the one you turn up tomorrow could be the other guy's first. This BCOP is needed to make sure the other guy knows what to expect.

- The creation of this BCOP was prompted after reading through a sordid 6 day cut-over that played out on the NANOG List
  - *Despite best laid plans by the OP the remote Peer was unable to stay up*
  - *Common expectations between peers were not set*
  - *The final resolution was only a max-prefix adjustment away*

- Doing things inconsistently CONSUMES TIME
  - No peering session should take 6 days to come up
  - No one should have to play Russian roulette when it comes to something as fundamental as a Peering turn up.

Draft BCOP Outline

1 BCOP Summary (Appeal)
2 BCOP Background / History
3 BCOP
3.1 What is BGP
3.1.1 Who needs BGP
3.1.2 Internal BGP (ibgp)
3.1.3 External BGP (ebgp)
3.1.4 Route Advertisement in IBGP vs EBGP
3.1.4.1 IBGP
3.1.4.2 EBGP
3.1.5 Loop avoidance mechanism in IBGP vs EBGP
3.1.5.1 IBGP
3.1.5.2 EBGP
3.1.6 BGP best Path selection refresher
3.1.6.1 Juniper
3.1.6.2 Cisco
3.2 Pre-turn-up considerations
3.2.1 Relationship Types
3.2.1.1 Transit
3.2.1.2 Peering
3.2.2 Interconnection Types
3.2.2.1 Point to Point Interface peering
3.2.2.2 eBGP Multi-hop peering
3.2.2.3 Load sharing
3.3 Policy Considerations
3.3.1 Inbound policy classification approach.
3.3.2 Inbound policy definitions and examples.
3.3.2.1 Transit inbound filters both for IPv4 and IPv6
3.3.2.2 Transit inbound IPv4 filters
3.3.3 Transit inbound IPv6 filters=
3.3.3.1 Communities
3.3.3.1.1 Downstream Communities
3.3.3.1.2 Transit Communities
3.3.4 IRR\PeeringDB
3.3.4.1 IRR basic building blocks
3.3.4.1.1 Maintainer Object
3.3.4.1.2 Route/Route6 Object
3.3.4.1.3 AS-set object
3.3.5 Getting Started
3.3.5.1 Choose a IRR database
3.3.5.1.1 Gather information about our network
3.3.5.1.2 Create maintainer object
3.3.5.1.3 Create route/route6 objects
3.3.5.1.4 Create a as-set object
3.3.5.1.5 Notify your peers
3.4 Turning up eBGP Peering
3.4.1 Testing and Validation - NEED MORE INFO
4 BCOP Conclusion

Participants

- Shepherd: Bill Armstrong
- Current SMEs:
  - Alex Saroyan
  - Mannan Venkatesan
  - Courtney Smith
  - Raghav Bhargava
  - Nina Bargisen
  - Brian Schleeper
  - Umair Arshad
  - Russell Harrison
- Other contributions from:
  - Karsten Thomann

Current Status

- The Draft is posted:
  - http://http://bcop.nanog.org/index.php/EBGP_Configuration_BCOP_v0.1
- We have a decent amount of information but we NEED SOME HELP!
  - Are we headed in the right direction?
  - WHAT ARE WE MISSING?!
  - The “Testing and Validation” section has very little in there and is perhaps the MOST critical portion of the document.

A GLOBAL EFFORT

NANOG\RIPE\JANOG BGP Configuration BCOP world domination plan

- A number of the other ‘NOGs are looking at similar BCOPs and for the time being, will move toward individual drafts\ratification.
- Once these documents mature the hope is that through some inter-area coordination, a GRAND UNIFYING MULTI-LINGUAL BGP BCOP can be created…

Join Us!

- Are you an expert in eBGP Configuration and Testing?
- Do you have real-world experience with eBGP Policy 'Stuff'?
- Are you interested in eBGP Configuration best Practices?

- Get involved!
  - Flexible time commitment
  - Contribute as much or as little as you can
  - The more voices we can include the better
  - PLEASE Email wrarmstrong@gmail.com to be included

Public Peering Exchange Participant BCOP

Shawn Hsiao, NANOG 62, Baltimore MD, 10.06.2014

BCOP Summary

- This BCOP aims to update current “Public Peering Exchange" BCOP
  - Add IXP prefix handling advice
  - Remove information pertaining to the operation of an exchange into a separate document, and re-focus the document toward exchange participants
  - Other updates as needed

BCOP Background

- From a discussion thread in 01-15-2014 regarding handling of IXP prefixes, there are several approaches discussed and different opinions raised. The update to BCOP aims to document and analyze these approaches, and make recommendations
- There are also other topics that would be beneficial for the participants
  - Also sharing and cross-reference contents from eBGP Configuration BCOP

Participants

- Shepherd: Shawn Hsiao
- Current SMEs:

Draft BCOP Outline

- Other considerations, e.g,
  - Check IXP policy on prefix distribution
  - Not accepting IXP routes from other AS
  - BGP Resiliency via BGP Timers or BFD
  - Traffic engineering and peering in multiple locations with a same peer

Needed BCOP Content

- Document and analyze approaches for handling of IXP prefixes, and make recommendations
- Sharing and cross-referencing contents from eBGP Configuration BCOP

Next Steps

- Looking for SME who wants to help!
- Finish both below by Dec 5th 2014 for Candidate BCOP submission
- Document and analyze approaches for handling of IXP prefixes, and make recommendations
  - Collaborating with eBGP Configuration BCOP team

Join Us!

- Are you an expert in Public Exchange Peering?
- Do you have real-world experience with Public Exchange Peering as a participants?
- Are you interested in Public Exchange Peering?
- Get involved!
  - Flexible time commitment
  - Contribute as much or as little as you can
  - The more voices we can include the better
  - Email phsiao@tripadvisor.com to be included

Ethernet OAM BCOP

Mark Calkins, NANOG62, Baltimore, 10.6.2014

BCOP Summary

- This BCOP aims to provide insight into how Ethernet OAM is best deployed within todays service provider networks.
- This BCOP will try to capture current and emerging best practices for uses of Ethernet OAM technologies.
- The primary focus of this BCOP is to de-mystify EOAM protocols and practices.

BCOP Background

- This BCOP is needed because Ethernet OAM is not widely understood outside of the service provider community.

Participants

- Shepherd: Mark Calkins
- Current SMEs:
  - Voitek Kozak
  - Jean-François Lévesque
  - Mark Calkins

Current Draft BCOP Outline

- General EOAM BCOPs
  - High level, What, When, Where
- Link Level EOAM BCOPs
  - How LFM functions, why it is good
  - Best practices for LFM's link monitoring
- Service Layer EOAM BCOPs
  - Service Layer OAM orientation
  - How CFM functions, why it is good
  - Fault Management
  - Performance Management
- ~~Ethernet Ring Protection Switching BCOPs~~
  - Not even attempted yet

BCOP Content for Review

- Ethernet OAM orientation
- Link Level OAM
- Service Level OAM
  - Fault Management
  - Performance Management

Needed BCOP Content

- More Service Layer OAM BCOPs
  - Y1731 standard and MEF frameworks are more extensive than what is covered here so far.
- Ethernet Ring Switching Protection
  - Not even attempted, an ambitious SME is needed.

Next Steps

- Continue SME recruitment
- Compile feedback received and modify document as required
- Complete Service EOAM
- Wiki-tize document

Join Us!

- Are you an expert in Ethernet OAM?
- Do you have real-world experience with Ethernet OAM?
- Are you interested in getting your name attached to public facing documentation?

- Get involved!
  - Flexible time commitment
  - Contribute as much or as little as you can
  - The more voices we can include the better
  - Email mark.calkins@gmail.com to be included

BCP38 / Anti-Spoof BCOP

- Work is underway to augment the existing work already done and shown in bcp38.info and RIPE
- Intent is to provide more detailed operator input on workarounds for known vendor bugs in vendor equipment
  - If more operators are aware of bugs, perhaps provide a better collective voice for fixes
  - Assist new operators not running into the same issues
- Focus on detailed configuration information from a variety of common vendors and architectural scenarios for the ISP and Enterprise spaces.

Anti-Spoof scope

- ISPs, Enterprises and Ixs
- I always dislike the BCP38 reference and call it anti-spoofing since BCP38 refers to ingress filtering by ISPs whereby I think enterprises and customers also have a role to play with appropriate egress filters. The gist is provide anti-spoofing wherever you are able and don't just make it one segment's problem.

Anti-Spoof state

- Rough draft completed and vetted with portion of the security community.
- If you are interested in working on this project, please send e-mail on list.

BCOP Other locations.. What I know of.

BCOP activity around the world:

- http://www.internetsociety.org/deploy360/about/bcop/

- Africa region: A BCOP group was started under AfNOG, lead by Douglas Onyango
- Asia: BCOP Task Force started at JANOG, co-chaired by Seiichi Kawamura and Yoshinobu Matsuzaki, NZNOG BCOP starting up, lead by Dean Pemberton
  - No whole-region effort started yet
- Europe: RIPE BCOP Task Force created, co-chaired by Benno Overeider and Jan Žorž
- Latin America: A BCOP Task Force was started under LACNOG, lead by Luis Balbinot and Pedro R Torres Jr.
- North America: NANOG BCOP Committee established, lead by Aaron Hughes and Chris Grundemann

AfNOG BCOP

- In Africa, the BCOP initiative was first introduced in May of 2013. Since then, there has been growing interest which culminated into to a BoF in Abidjan, (AfriNIC19 meeting), and a subsequent session and BoF at the AIS/AfriNIC 20 meeting in Djibouti (June 2014).
- The BCOP effort is led by Douglas Onyango and the current focus is to put in place a mailing list, an online BCOP document repository as well as development of two or more drafts that can be discussed during a session at AFRINIC 21 in Mauritius (Nov 2014).

RIPE BCOP

- RIPE BCOP Task Force charter page:
- http://www.ripe.net/ripe/groups/tf/best-current-operational-practices-task-force
- Mailing-list:
- https://www.ripe.net/mailman/listinfo/bcop
- BCOP candidate documents:
- RIPE-554
- IPv6 troubleshooting for helpdesks

LACNOG BCOP

- **Latin America and Carribean (LAC) regional BCOP Task Force:**
- A BCOP Task Force is started under LACNOG, co-chaired by Luis Balbinot and Pedro R Torres Jr. The group asked for a mailing list and a webpage under LACNOG umbrella, we'll publish it here as soon as any data becomes available. At the meeting the policy and procedures of the group was discussed and some topics identified. The group still has to decide on primary language of the produced documents (Spanish/Portuguese/English).

Asia Region BCOP

- JANOG started a BCOP Task Force with Seiichi Kawamura and Yoshinobu Matsuzaki co-chairing it.

Forums

- NANOG
- RIPE
- ENOG
- MENOG
- AfriNOG/AfriNIC
- LACNOG/LACNIC
- CaribNOG
- Southeast Europe RIPE Regional Meeting (SEE)
- UKNOF
- PLNOG

Questions?

- Aaron Hughes, CEO 6connect
- aaron@6connect.com