Observatory of Internet Resilience in France

François Contat

ANSSI

Agence nationale de la sécurité des systèmes d'information

http://www.ssi.gouv.fr/en

RIPE 68 - May 12th, 2014

ANSSI and Observatory

Created on July 7th 2009, the ANSSI is the national cyberdefence agency.

Main missions are:

- Prevention
- Defence of information systems

Internet resilience is one of its priority.

In 2011, The Observatory of Internet resilience in France is created.

Publications:

- Two reports of Internet status in France
- BGP BCP

http://www.ssi.gouv.fr/en/

BGP Best Current Operational Practices

Why?

Motivations

- BGP BCPs present in multiple documents
- No single reference document
- No adjustment depending on BGP interconnection type:
  - Transit
  - Peering
  - Customer

Who?

ANSSI

- Pierre Lorinquer (main author)
- Observatory Team (G. Valadon, M. Feuillet, F. Contat)

Operators

- Association Kazar
- France-IX
- Jaguar Network
- Neo Telecoms
- Orange
- RENATER
- SFR

How?

First step: internal work

- Classify BGP interconnections and define AS relationships
- Draft a first recommendations list

Second step: collaborative work

- Propose the recommendations list
- Debate the importance of each recommendation

Third step: publication

- Implement Operators comments
- Publish on October 1st, 2013

BGP Best Current Operational Practices Document

Structure

Definitions

- Interconnection types
- As relationships

Recommendations levels

Recommendations

- Description
- Examples

Definitions

Interconnection types

- Direct interconnection
- IXP Peering
- IXP Route-server
- Multihop

AS relationships

- Transit / Customer (leaf)
- Transit / Small transit
- Peering

Definitions

Interconnection types

- Direct interconnection
- IXP Peering
- IXP Route-server
- Multihop

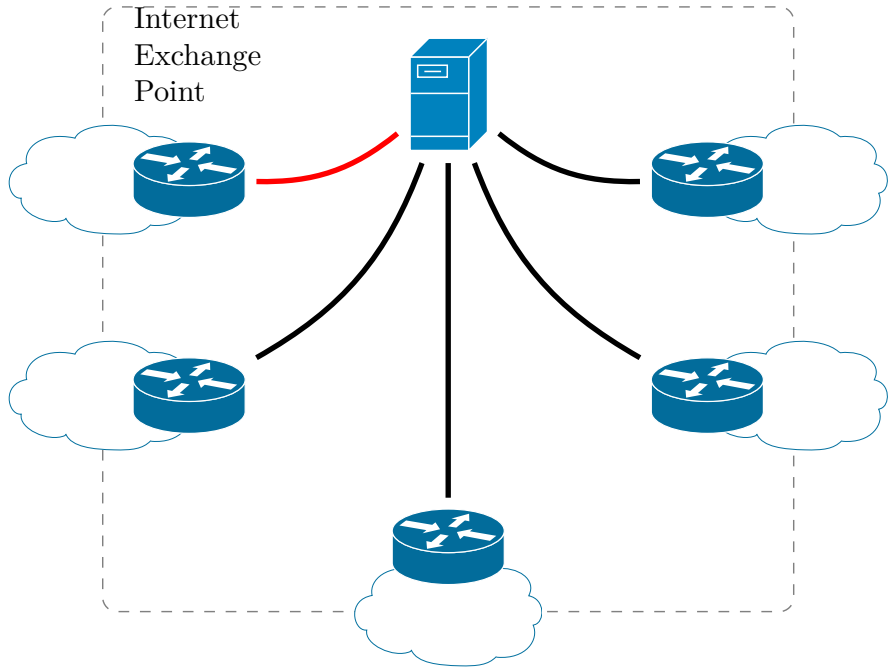
AS relationships

- Transit / Customer (leaf)
- Transit / Small transit
- Peering

Definitions

Interconnection types

- Direct interconnection
- IXP Peering
- IXP Route-server
- Multihop



AS relationships

- Transit / Customer (leaf)
- Transit / Small transit
- Peering

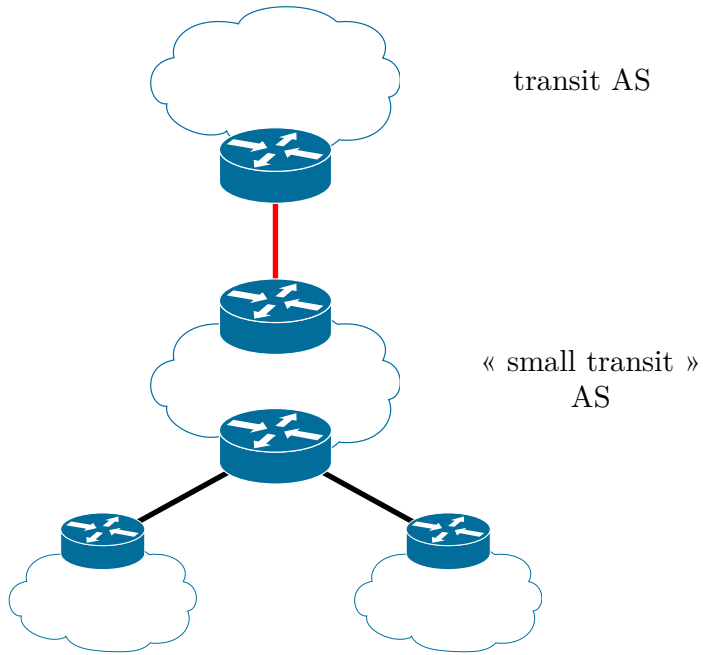
Definitions

Interconnection types

- Direct interconnection
- IXP Peering
- IXP Route-server
- Multihop

AS relationships

- Transit / Customer (leaf)
- Transit / Small transit
- Peering



Recommendations

AS relationship dependant

- TCP-Authentication
- AS-PATH filtering
- Prefixes filtering (route objects)
- Max-prefix
- Private AS removing

General recommendations

- Martians filtering
- Bogons filtering
- Default route filtering
- Log
- Graceful restart

Recommendation example

<table>
<tr><th>BCP name</th><th>AS relationship</th><th>Recommendation level</th><th>Remarks</th></tr>
<tr><td rowspan="5">Prefixes filtering allocated to peer</td><td rowspan="2">Transit / Customer (leaf)</td><td>Transit side:
  </td><td rowspan="5">Systematic filtering for « leaf » AS.</td></tr>
<tr><td>Customer side: –</td></tr>
<tr><td rowspan="2">Transit / small Transit</td><td>Transit side:
  </td></tr>
<tr><td>Customer side: –</td></tr>
<tr><td>Peering</td><td>  </td></tr>
</table>

Recommendation implementation

Routers configurations

- Each recommendation has configuration sample
- Configuration examples for:

Operating system	Version
SR-OS (Alcatel-Lucent)	10.0r5
IOS (Cisco)	15.2(4)S
Junos (Juniper)	11.4R3.7
OpenBGPD (OpenBSD)	5.3

- Cisco, Juniper made by ANSSI
- Alcatel and openBGPd configuration given by Operators

Conclusion

How did it work?

- Got feedbacks from French nog members
- Minors errors hilighted by readers after publication

The next report

- Translate the document in English
- Propose new recommendations (ex: GTSM)
- Propose route object/ROA declaration
- Review old and new recommendations with operators
  - Keep or remove
  - Change recommendation level
  - Update configuration examples (IOS XE/XR, etc.)
  - ...

Questions?