



EASA
European Aviation Safety Agency

Is it safe?

BGP in ANSP context

High Level Conference Cybersecurity in Civil Aviation

Kraków, Poland

9 November 2017

Your safety is our mission.

An agency of the European Union 

TE.GEN.00409-001



What can go wrong when a router fails?

- In May 2016 an ISP did something wrong in one of its routers
 - Fat fingers?
 - Malevolent?
- Whatever...
 - When routing is disrupted, systems and servers cannot communicate
 - one of the effects this day was the closure of the country's national airspace for several hours





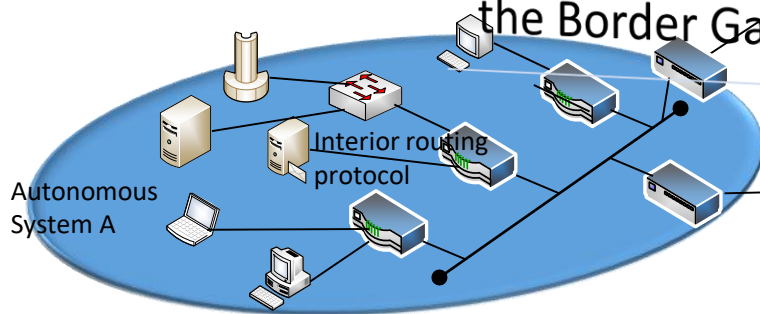
A short introduction on the backbone

Autonomous Systems (AS)

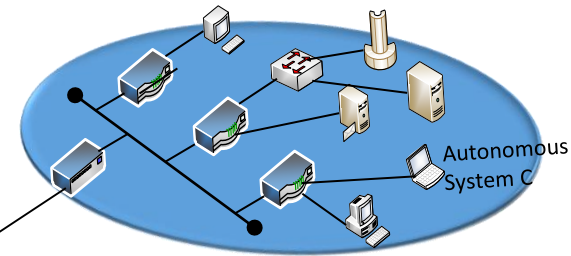
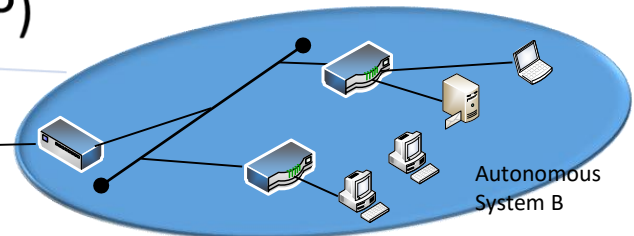
the internet is made of Autonomous Systems

each AS may have its own routing language (protocol)

At the border of each AS, there is a need to have a common language: the Border Gateway Protocol (BGP)



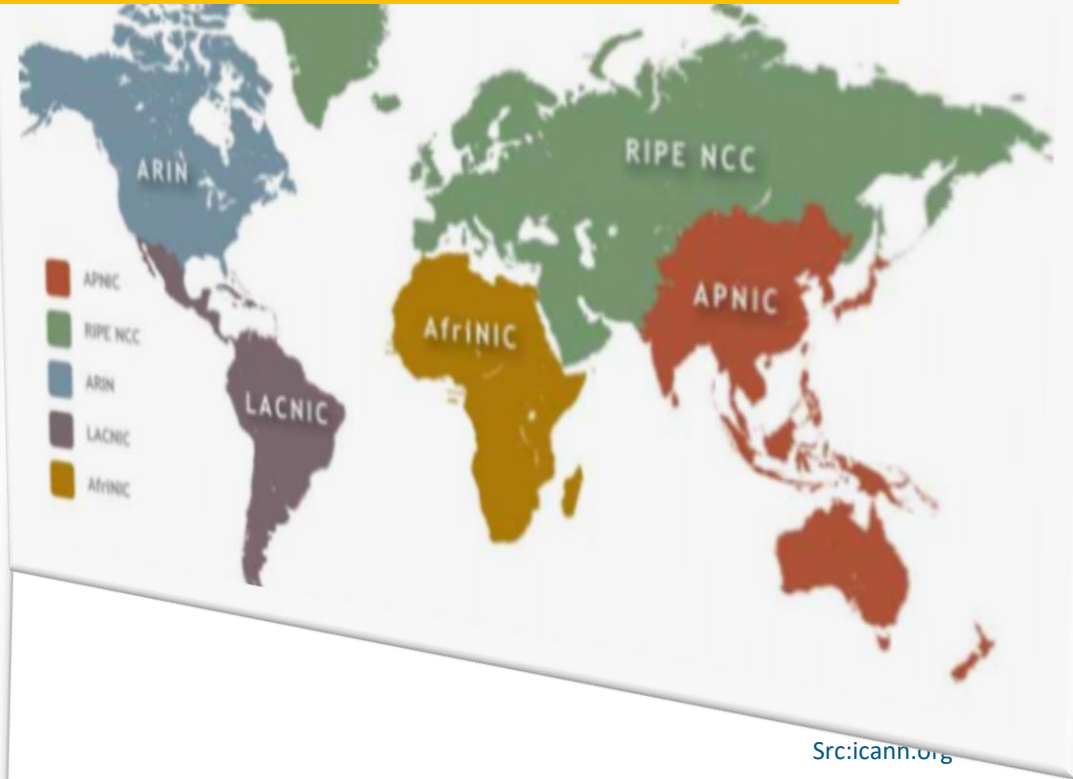
Border Gateway Protocol





Governance

IP addresses distribution is also geographical:
All european addresses are managed by the RIPE



Src:icann.org



Border Gateway Protocol (BGP)

-
- The diagram illustrates a network topology of Autonomous Systems (ASes) and their interconnections. The ASes are represented by ovals and labeled with their AS numbers. The connections are represented by directed arrows, indicating the flow of BGP information. The network is structured as follows:
- AS199541** is connected to **AS3356** and **AS174**.
 - AS3356** is connected to **AS3257**, **AS3320**, **AS1273**, **AS3549**, and **AS174**.
 - AS3257** is connected to **AS3320**.
 - AS3320** is connected to **AS6939**.
 - AS6939** is connected to **AS174**.
 - AS1273** is connected to **AS174**.
 - AS3549** is connected to **AS174**.
 - AS174** is connected to **AS6461**, **AS6453**, **AS209**, **AS12956**, **AS6762**, and **AS701**.
 - AS6461** is connected to **AS6453**.
 - AS6453** is connected to **AS209**, **AS12956**, **AS6762**, and **AS701**.
 - AS209** is connected to **AS12956**, **AS6762**, and **AS701**.
 - AS12956** is connected to **AS6762** and **AS701**.
 - AS6762** is connected to **AS701**.
- The diagram shows a complex network of connections, with many ASes having multiple incoming and outgoing links. The connections are represented by arrows, indicating the direction of BGP information flow.

Upon receiving BGP information, gateway routers choose the best route to the destination network and add it to their routing tables according to 2 rules:

- AS-Path: The shorter path (number of networks crossed to the destination) the better the route.
- 2) Prefix mask: The route with the more specific mask is preferred.

```

Mar 10/2017 11:00:00 AM: *****
Length: 53
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 25
  Path Attributes
    Path Attribute - ORIGIN: IGP
      Flags: 0x00: well-known, Transitive, complete
      ..0. .... = optional: well-known
      ..1. .... = Transitive: Transitive
      ...0. .... = Partial: Complete
      ...0. .... = Length: Regular length
      Type Code: ORIGIN (1)
      Length: 1
      Origin: IGP (0)
    Path Attribute - AS_PATH: 1
      Flags: 0x00: well-known, Transitive, complete
      ..0. .... = optional: well-known
      ..1. .... = Transitive: Transitive
      ...0. .... = Partial: Complete
      ...0. .... = Length: Regular length
      Type Code: AS_PATH (2)
      Length: 4
      AS Path segment: 1
    Path Attribute - NEXT_HOP: 192.168.12.1
    Path Attribute - MULTI_EXIT_DISC: 0
      Flags: 0x80: optional, Non-transitive, complete
      1... .. = optional: optional
      ..0. .... = Transitive: Non-transitive
      ..0. .... = Partial: Complete
      ...0. .... = Length: Regular length
      Type Code: MULTI_EXIT_DISC (4)
      Length: 4
      Multiple exit discriminator: 0
    Network Layer Reachability Information (NLRI)
      1.1.1.1/32
      NLRI prefix length: 32
      NLRI prefix: 1.1.1.1 (1.1.1.1)

```

What can possibly go wrong?





What went wrong, Case 1: Youtube shut down for hours

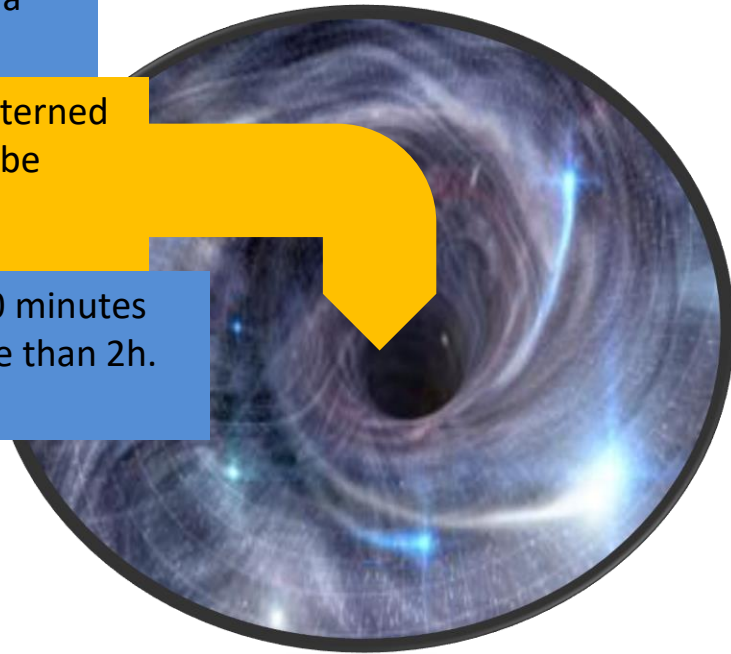
February 2008, Pakistanis gov decide to block access to youtube to its nationals because of offensive videos.

Pakistan Telecom announce that their AS owns IP address prefix allocated to Youtube.

The address range was a bit more specific than what Youtube AS announce (rule 2) resulting in a higher route priority.

In less than 3 minutes more than 2/3 of the interned learned the new route and most of the youtube traffic was redirected into a cyber black hole.

Although the outage was detected after 10 minutes and both ends trying to fix it, it lasted more than 2h.





What went wrong. Case 2 Belarusian Traffic Diversion

LEGEND



NORMAL



HIJACKED



Affected countries

- US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran



Attack frequency

**bgpstream** @bgpstream · 4h
BGP,HJ,hijacked prefix AS3786 117.52.28.0/23, LG DACOM Corporation,-,By AS57976 Blizzard Entertainment, Inc, bgpstream.com/event/113153



**bgpstream** @bgpstream · 4h
BGP,HJ,hijacked prefix AS3786 117.52.26.0/23, LG DACOM Corporation,-,By AS57976 Blizzard Entertainment, Inc, bgpstream.com/event/113152



**bgpstream** @bgpstream · 4h
BGP,OT,2471,Iles de la Guadeloupe,-,Outage affected 15 prefixes, bgpstream.com/event/113151



**bgpstream** @bgpstream · 4h
BGP,OT,2471,Iles de la Guadeloupe,-,Outage affected 15 prefixes, bgpstream.com/event/113143



**bgpstream** @bgpstream · 6h
BGP,OT,2471,Iles de la Guadeloupe,-,Outage affected 15 prefixes, bgpstream.com/event/113139

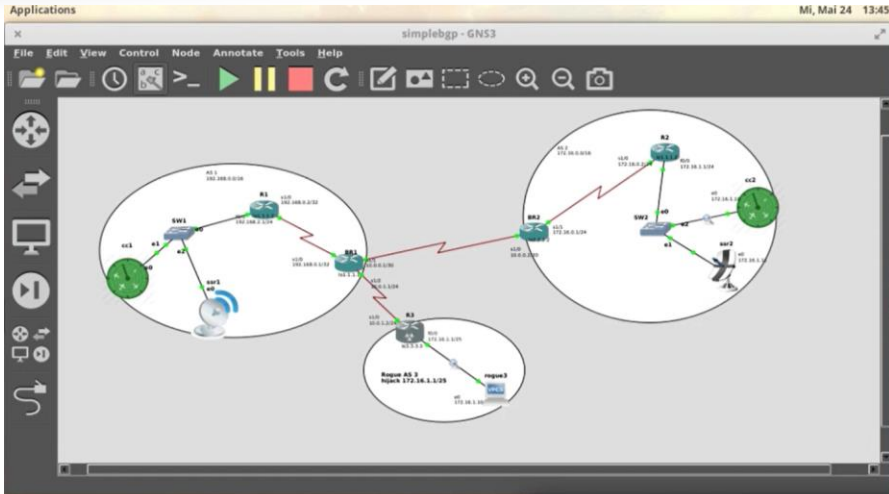


**bgpstream** @bgpstream · 6h
BGP,OT,27895,Necle S.A.,-,Outage affected 36 prefixes,

Bgpstream capture 09/11/2017



Difficulty



*Standard input (cc2 Ethernet0 to SW2 Ethernet1)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
89	126.185120	172.16.1.10	192.168.2.10	ICMP	98	Echo (ping) reply
90	127.274417	192.168.2.10	172.16.1.10	ICMP	98	Echo (ping) request
91	127.274569	172.16.1.10	192.168.2.10	ICMP	98	Echo (ping) reply
92	128.349829	192.168.2.10	172.16.1.10	ICMP	98	Echo (ping) request
93	128.350846	172.16.1.10	192.168.2.10	ICMP	98	Echo (ping) reply
94	129.434960	192.168.2.10	172.16.1.10	ICMP	98	Echo (ping) request
95	129.435163	172.16.1.10	192.168.2.10	ICMP	98	Echo (ping) reply
97	130.506314	192.168.2.10	172.16.1.10	ICMP	98	Echo (ping) request
98	130.506781	172.16.1.10	192.168.2.10	ICMP	98	Echo (ping) reply

Frame 20: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: ca:04:11:dc:00:08 (ca:04:11:dc:00:08), Dst: Private_66:68:00 (00:50:79:66:68:00)

Internet Protocol Version 4, Src: 192.168.2.10, Dst: 172.16.1.10

Internet Control Message Protocol

0000 00 50 79 66 68 00 ca 04 11 dc 00 08 00 00 45 00 .Pyfh.....E.
0010 00 54 72 2e 00 00 3c 01 9c ae c0 a8 02 0a ac 10 .Tr...<.....
0020 01 0a 08 00 ef 04 30 72 00 05 08 09 0a 00 0c 0d0f.....
0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ..!*%&'()*+,-./0123456789;<=>?
0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d
0060 3e 3f

Internet Control Message Protocol: Protocol Packets: 98 · Displayed: 74 (75.5%) · Profile: Default

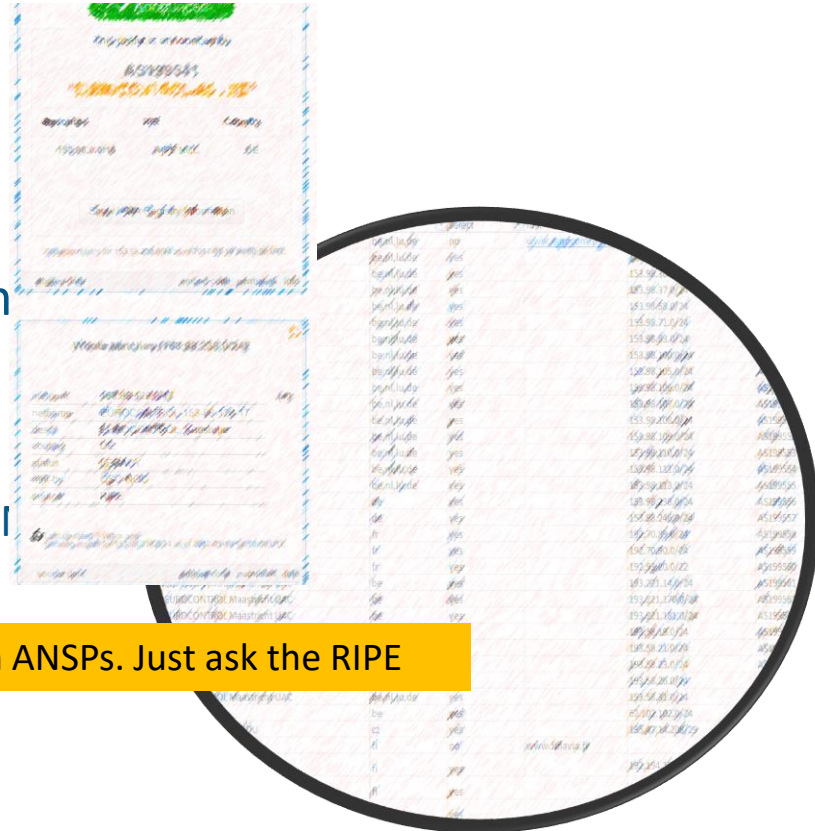
No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

mini-BGP-Hijack
tinybgphj (002)



Implications for European Aviation

- EU ANSPs live in either
 - their own Autonomous System
 - DFS, SNA-F, Avinor, Austrocontrol...
 - The Eurocontrol Autonomous System
 - Be, Ne, Lux...
 - Commercial AS
 - ENAV (Telecom IT), Sweden ATM (TELIA)



It takes less of an hour to list all AS and prefixes of all European ANSPs. Just ask the RIPE

[Login](#)[RIPE Database \(Whois\)](#)[Website](#)[Manage IPs and ASNs](#) >[Analyse](#) >[Participate](#) >[Get Support](#) >[Publications](#) >[About Us](#) >

You are here: [Home](#) > [Manage IPs and ASNs](#) > [RIPE Database](#) > [Webupdates](#)

[Resources](#) >[RIPE Database](#) ▾[Query the RIPE Database](#)[Full Text Search](#)[Syncupdates](#)[Create an Object](#)

RIPE Database Text Search

This service allows searches over the full text of the RIPE Database object data.

The search is done on object text without regard for any relationships. Multiple search terms should be separated with a space.

[+ Advanced Search](#)

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

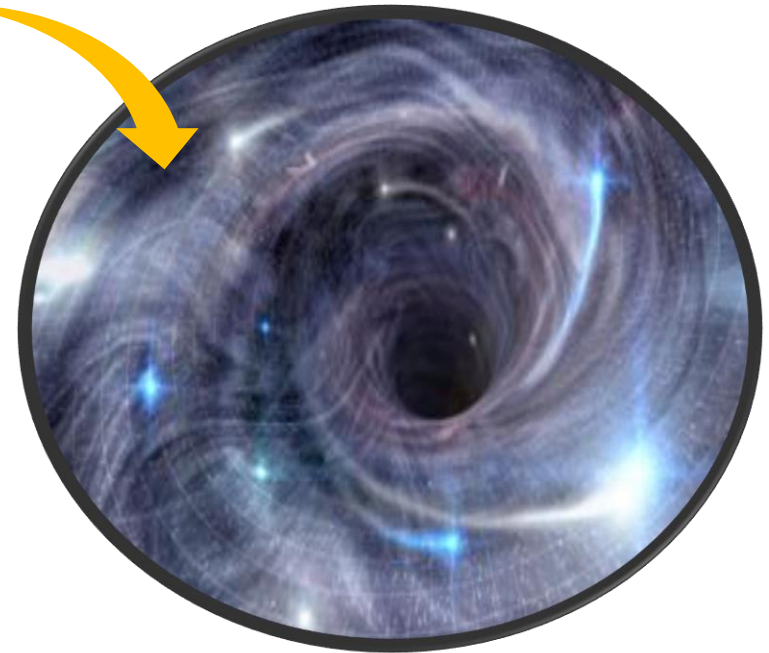
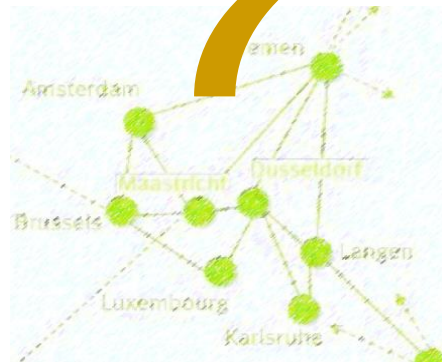
RIPE Database Software Version 1.90



[Home](#) | [Sitemap](#) | [Contact Us](#) | [Service Announcements](#) | [Privacy Statement](#) | [Legal](#) | [Cookies](#) | [Copyright Statement](#) | [Terms of Service](#)



reroute all or most of European ANSPs prefixes into a black hole for several hours

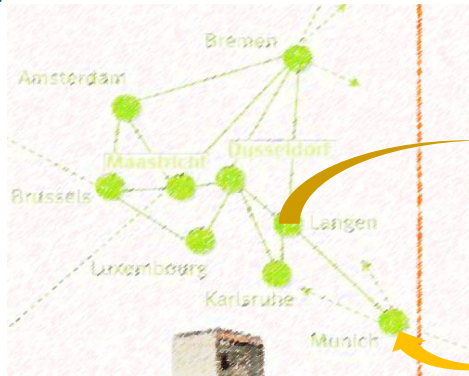




Weird idea 2



highjack routes from ANSP X. Try to figure out when radar surveillance UDP/ASTERIX messages are present and if found play with them...



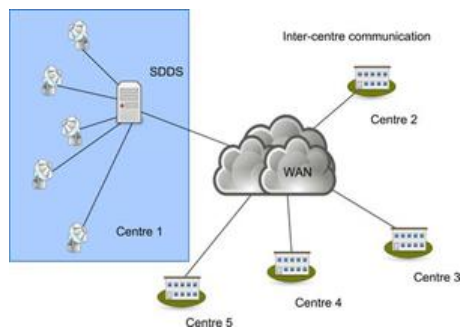
Add/Remove/change plots?



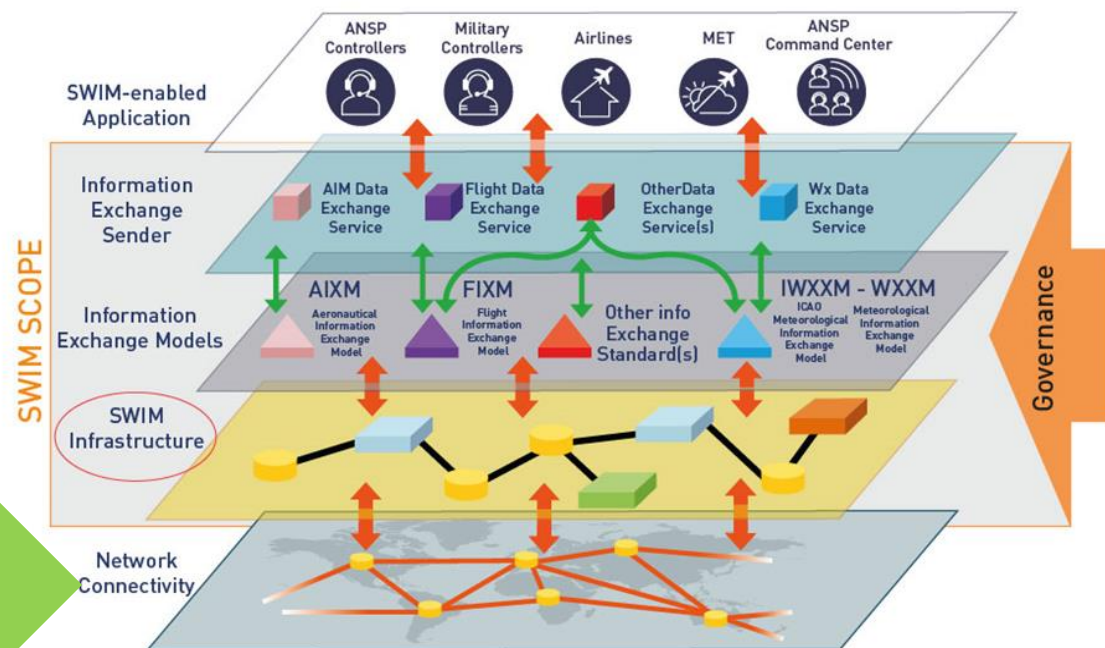
```
ASTERIX PROTOCOL
BLOCK Cat 1
  ASTERIX CATEGORY: Monoradar Target Reports (1)
  Block length: 47
  RECORD : 1
  RECORD : 2
    FSPEC Asterix: 0x0000f7a4
    System Area Code: 8
    System Identification code: 226
    Target Report Descriptor: 0xa8
    Track number: 126
    Position in Polar Coordinates: 0x4c2bb35b rho= 76,00 NM, theta= 252,00 deg
    Calculated Track Velocity in Polar Representation: Ground speed= 358,16 kt
    .... 1111 1000 1110 = Mode-3/A Code: 7616
    ..00 0101 1100 1000 = Flight Level (*25ft): 1480 = 370 FL (x100ft)
    0000 010 - Radar Plot Characteristics: 2
```



PENS, SDDS and SWIM



Internet « governance »





Conclusion

➤ Some solutions exist

➤ prefix filtering

- Reversed incentive (you protect the rest of the internet, not you)

➤ RPKI (validation of the origin)

- Centralized authority...

➤ BGPSec (validation of the Path)

- Online cryptography (need updated hardware)
- Effective when all AS of a path implement BGPSec (who starts?)

<https://www.internetsociety.org/deploy360/start/>



EASA
European Aviation Safety Agency

Questions?

Your safety is our mission.

An agency of the European Union

