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

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

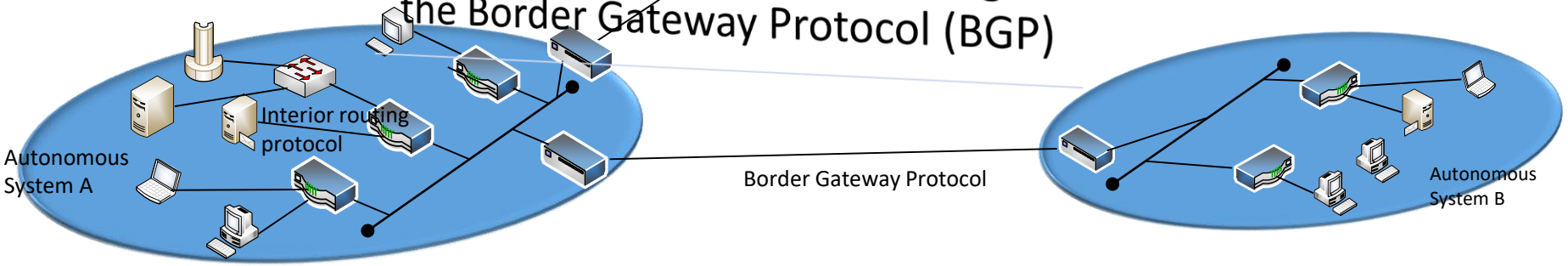
A short introduction on the backbone

Autonomous Systems (AS)

the internet is made of Autonomous Systems

each AS may have its own routing language (protocol)

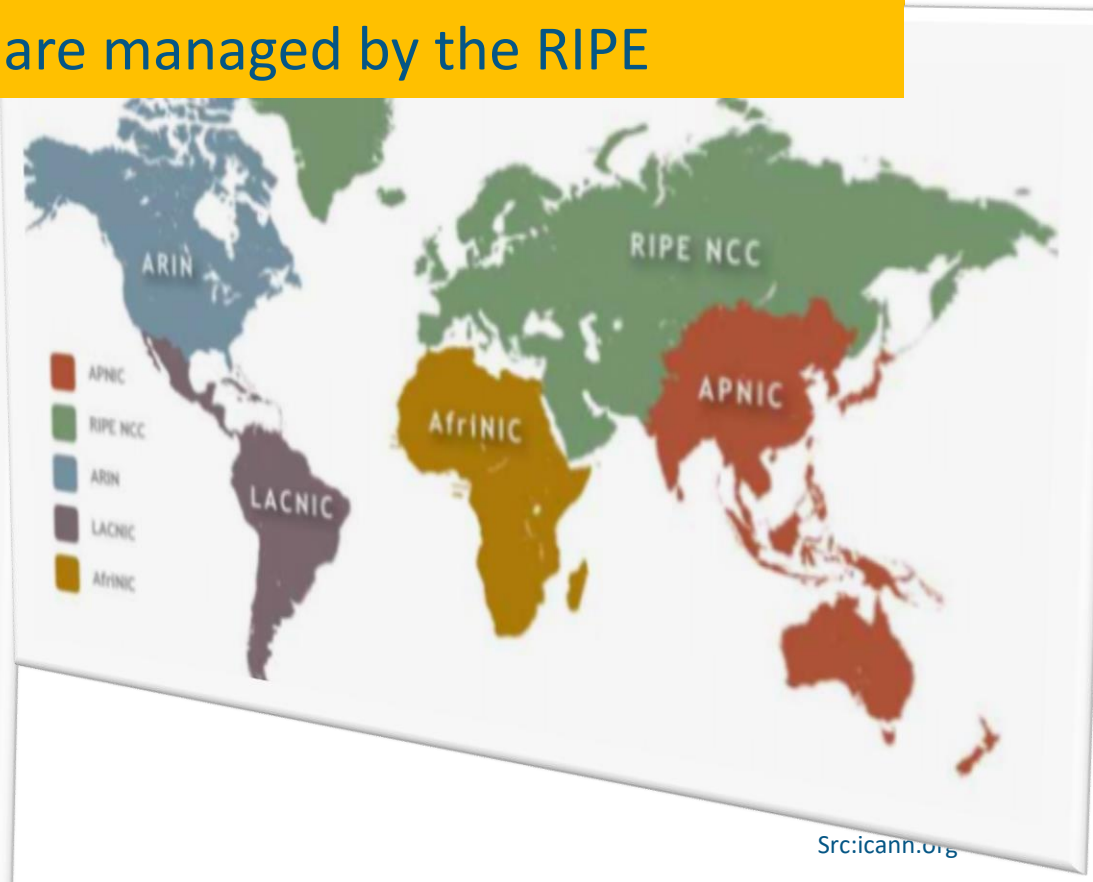
At the border of each AS, there is a need to have a common language: the Border Gateway Protocol (BGP)



Governance

IP addresses distribution is also geographical:

All european addresses are managed by the RIPE



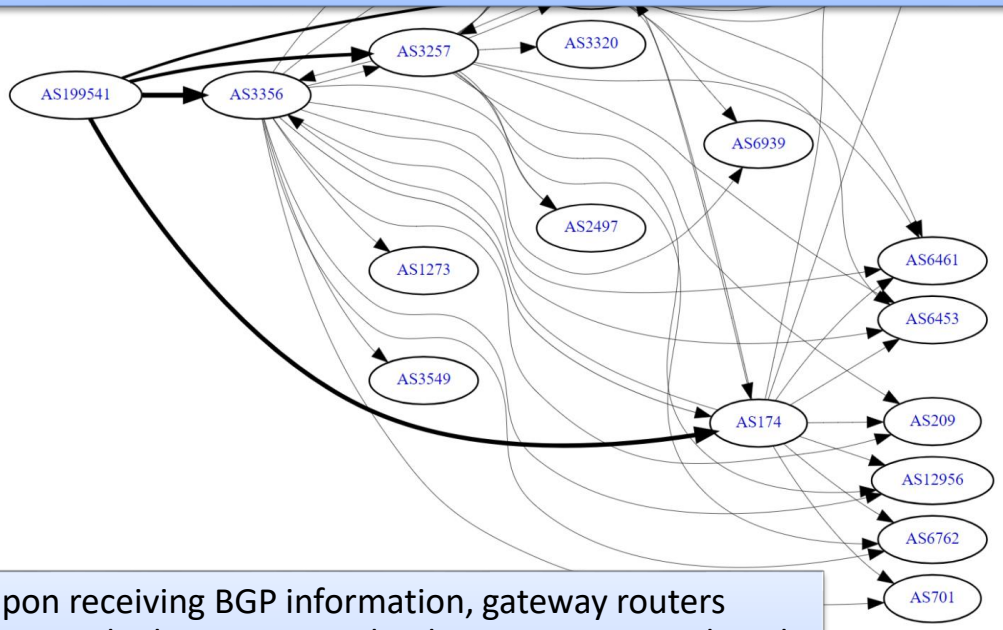
Src:icann.org

How addresses are made accessible worldwide?

AS199541 IPv4 Route Propagation

Border Gateway Protocol (BGP)

- BGP allows an AS to tell the others how to reach its networks (and vice versa).
- **Huge** address tables are frequently exchanged to maintain the internet global mapping.




```
Length: 53
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 25
Path attributes
  Path Attribut - ORIGIN: IGP
    Flags: 0x40: 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 Attribut - AS_PATH: 1
    Flags: 0x40: 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 Attribut - NEXT_HOP: 192.168.12.1
  Path Attribut - 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)
```

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.

What can possibly go wrong?

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

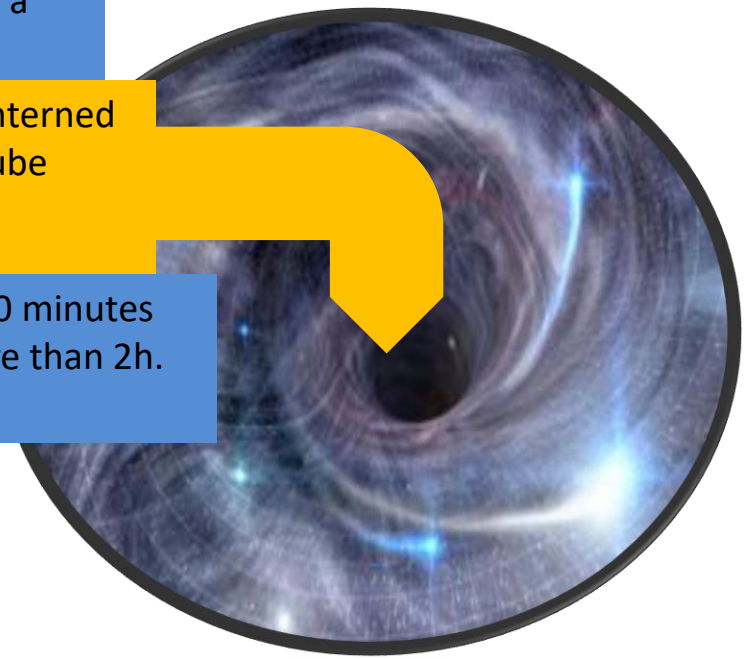
February 2008, Pakistanis gov decide to block access to youtube to its nationals because of offensive videos.

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

In Feb 2013, several global traffic redirection to Belarusian ISP GlobalOneBel taking place almost every day during several months. Victims were

- Major financial institutions,
- governments,
- network service providers.

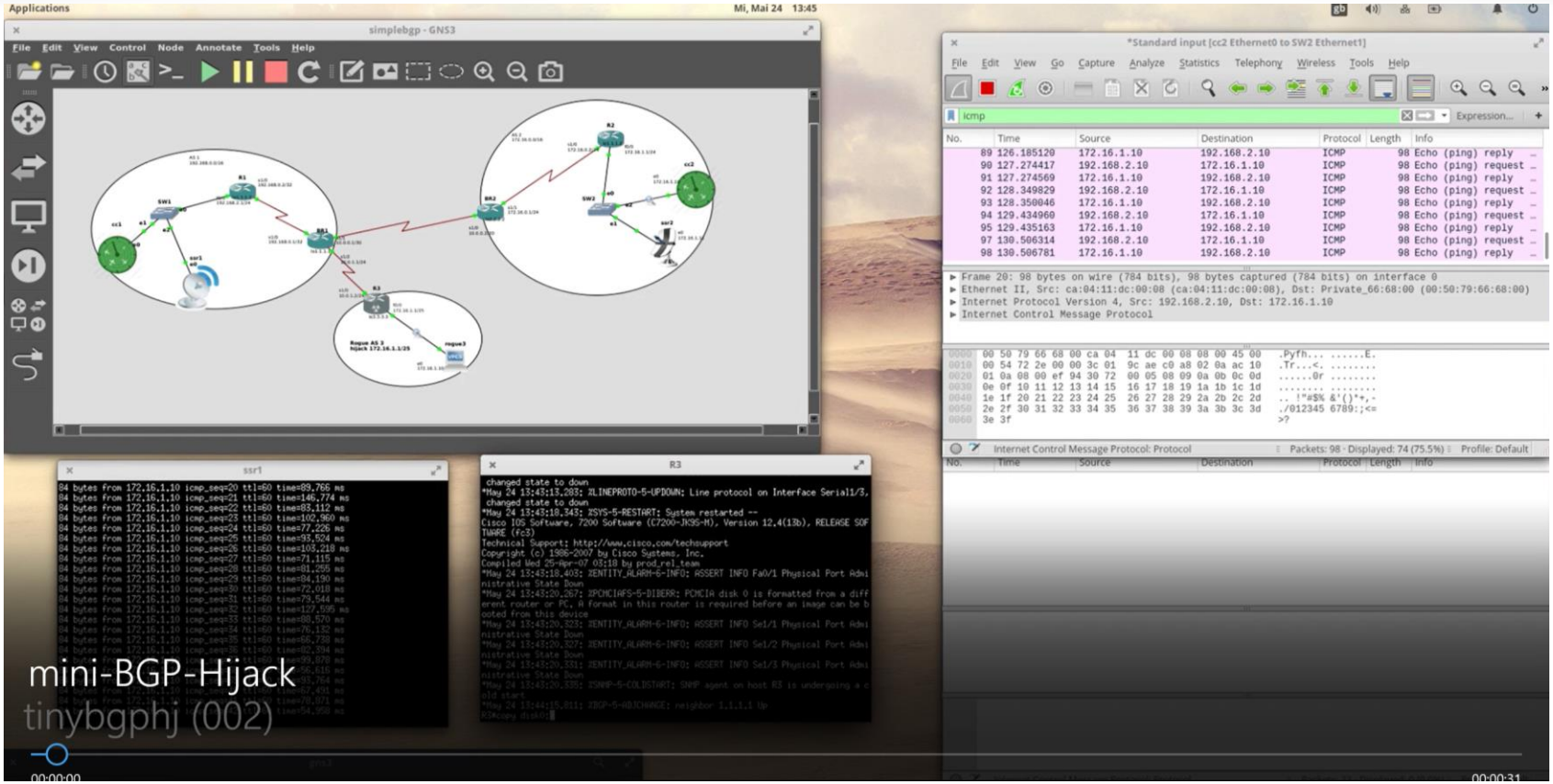
Affected countries

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

Attack frequency

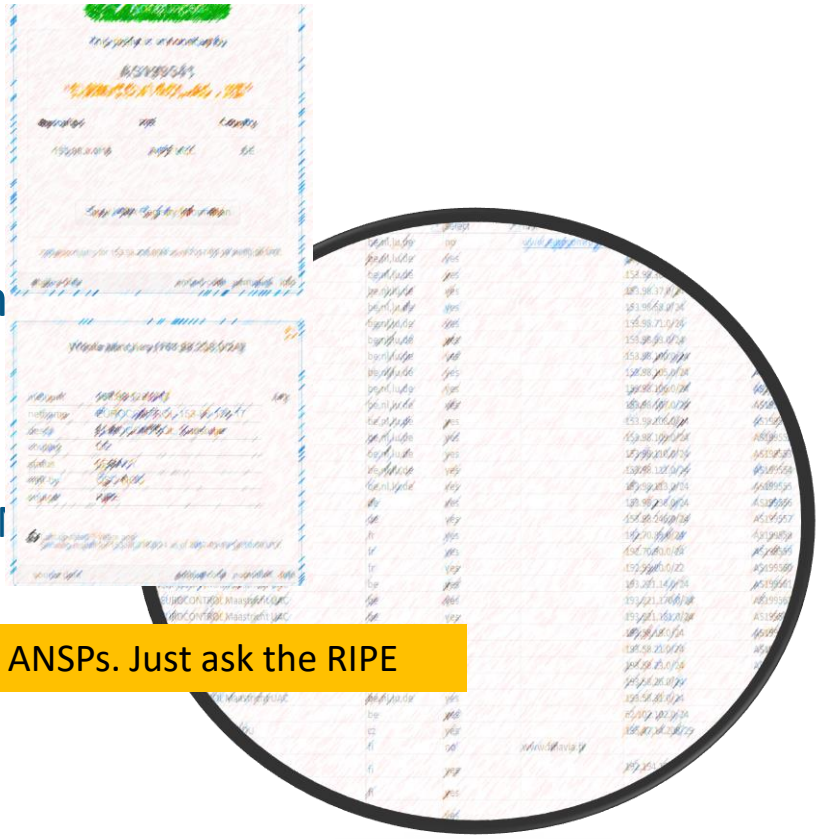
Bgpstream capture 09/11/2017

Difficulty

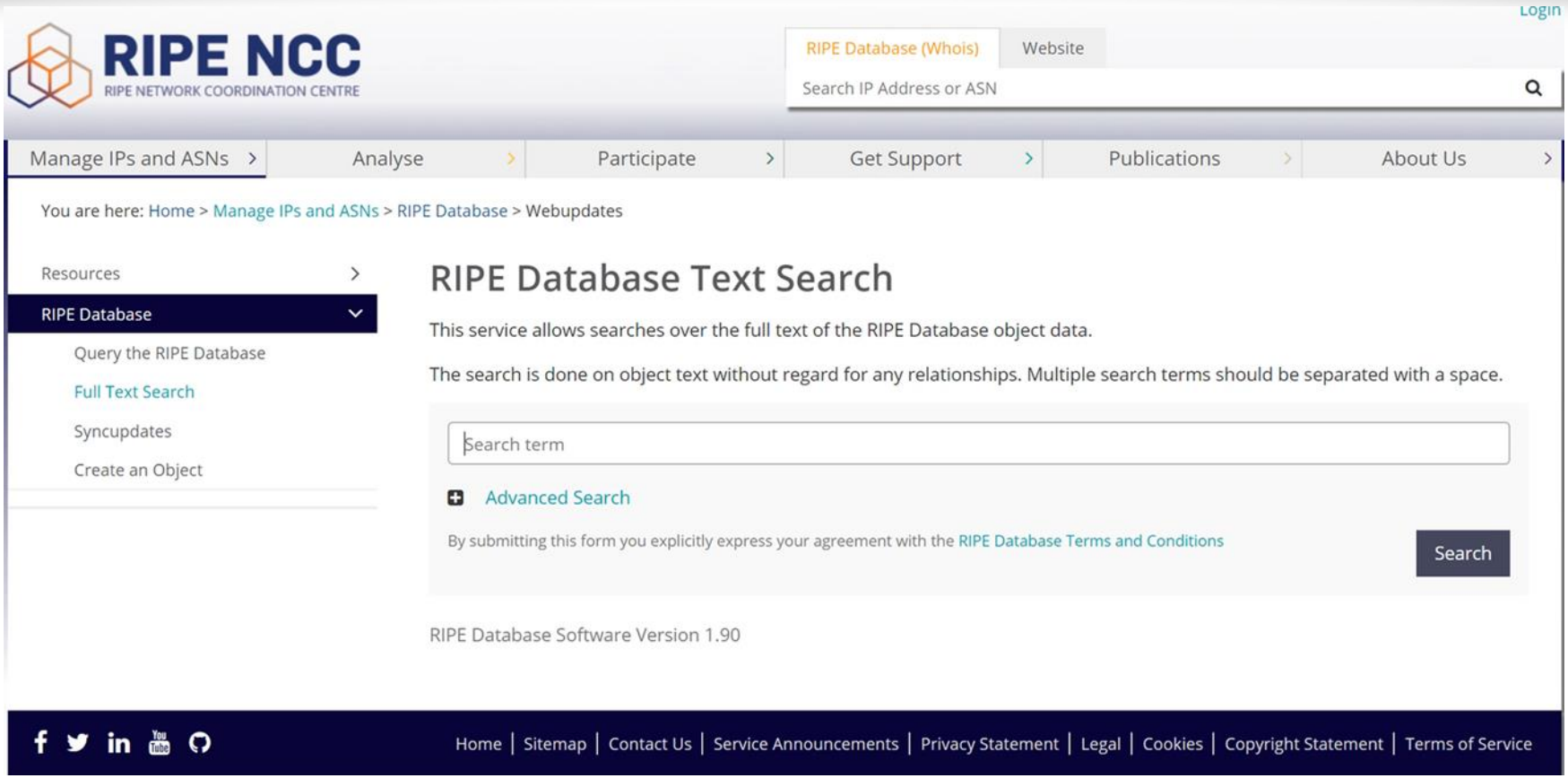


Implications for European Aviation

- 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 (TELIAI

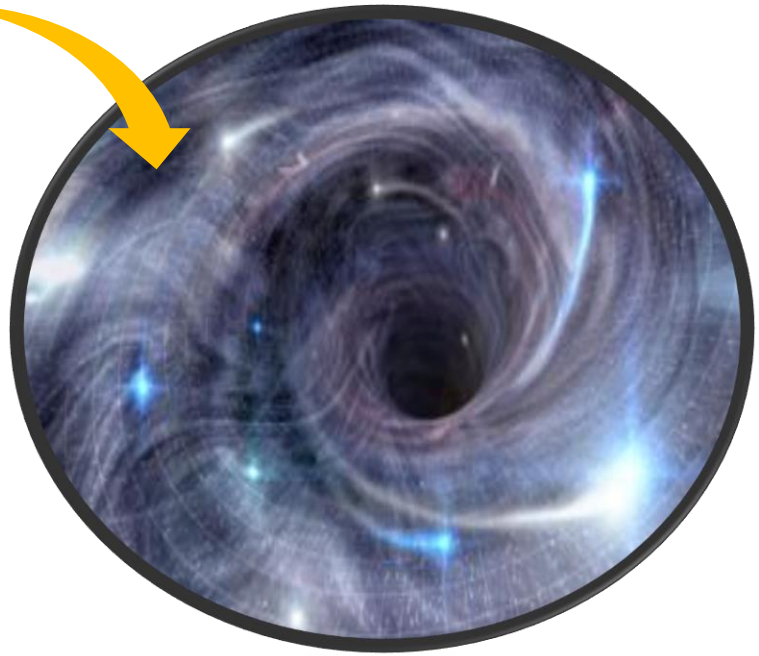


It takes less of an hour to list all AS and prefixes of all European ANSPs. Just ask the RIPE


RIPE NCC
RIPE NETWORK COORDINATION CENTRE
Login
RIPE Database (Whois)
Website
Search IP Address or ASN
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.
Search term
Advanced Search
By submitting this form you explicitly express your agreement with the RIPE Database Terms and Conditions
Search
RIPE Database Software Version 1.90
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

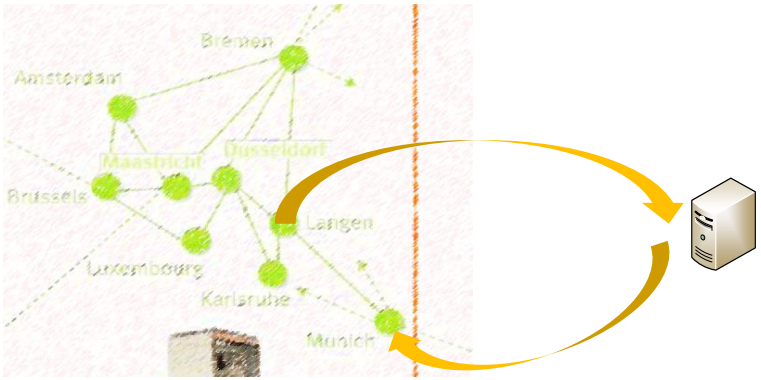
Weird idea 1

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…

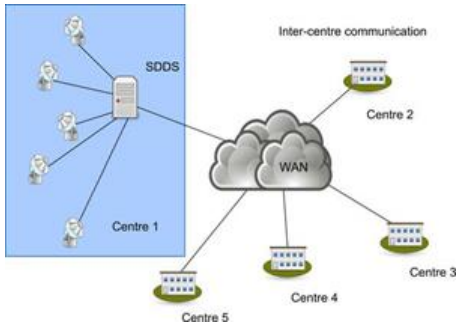


Add/Remove/change plots?

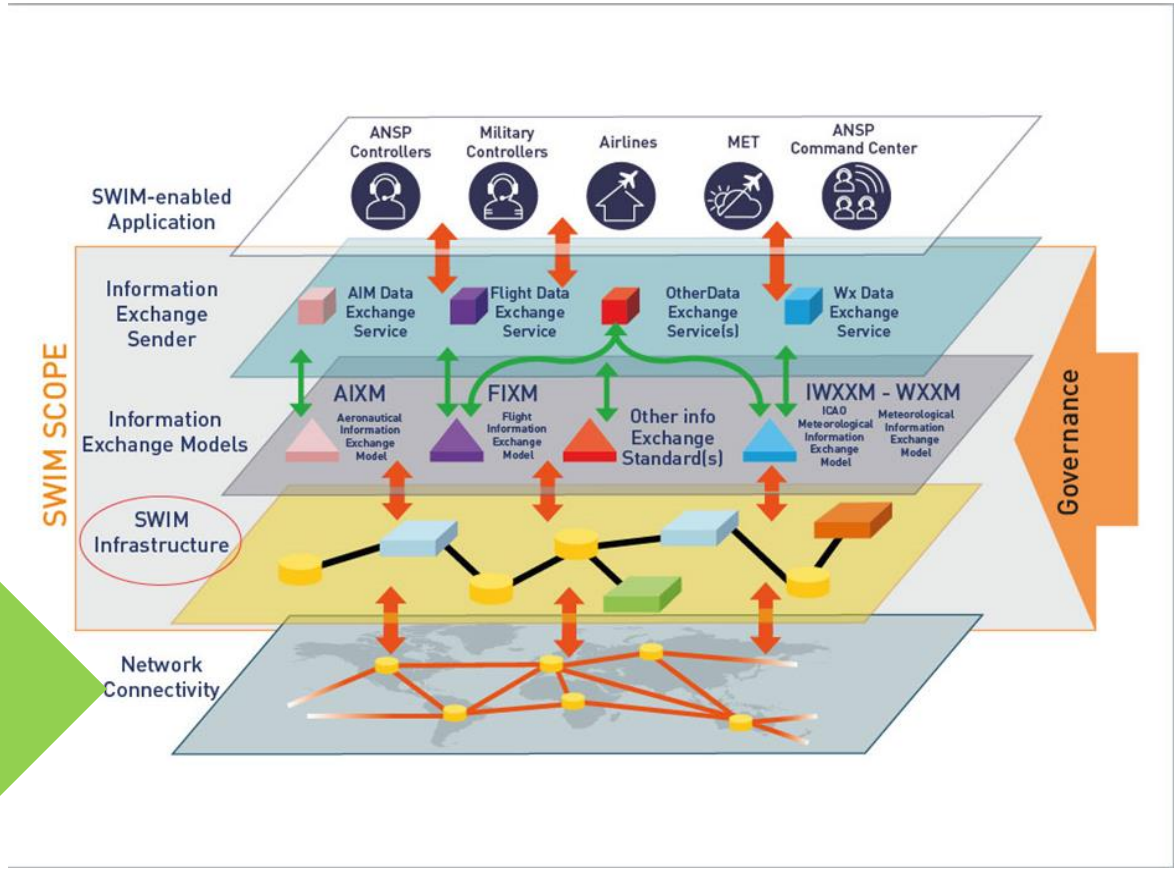
WIRESHARK

```
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