Routing Security

Daniel Karrenberg

RIPE NCC

<daniel.karrenberg@ripe.net>

Who is talking: Daniel Karrenberg

- 1980s: helped build Internet in Europe
  - EUnet, Ebone, IXes, ...
  - RIPE

- 1990s: helped build RIPE NCC
  - 1st CEO: 1992-2000

- 2000s: Chief Scientist & Public Service
  - Trustee of the Internet Society: IETF, ...
  - Interests: Internet measurements, stability, trust & identity in the Internet, ...

Who is talking: Daniel Karrenberg

- RIPE NCC

  - started in 1992

  - first Regional Internet Registry (RIR)

  - Association of 7000+ ISPs

  - 70+ countries in "Europe & surrounding areas"

  - operational coordination

  - number resource distribution

  - trusted source of data

  - Motto: Neutrality & Expertise
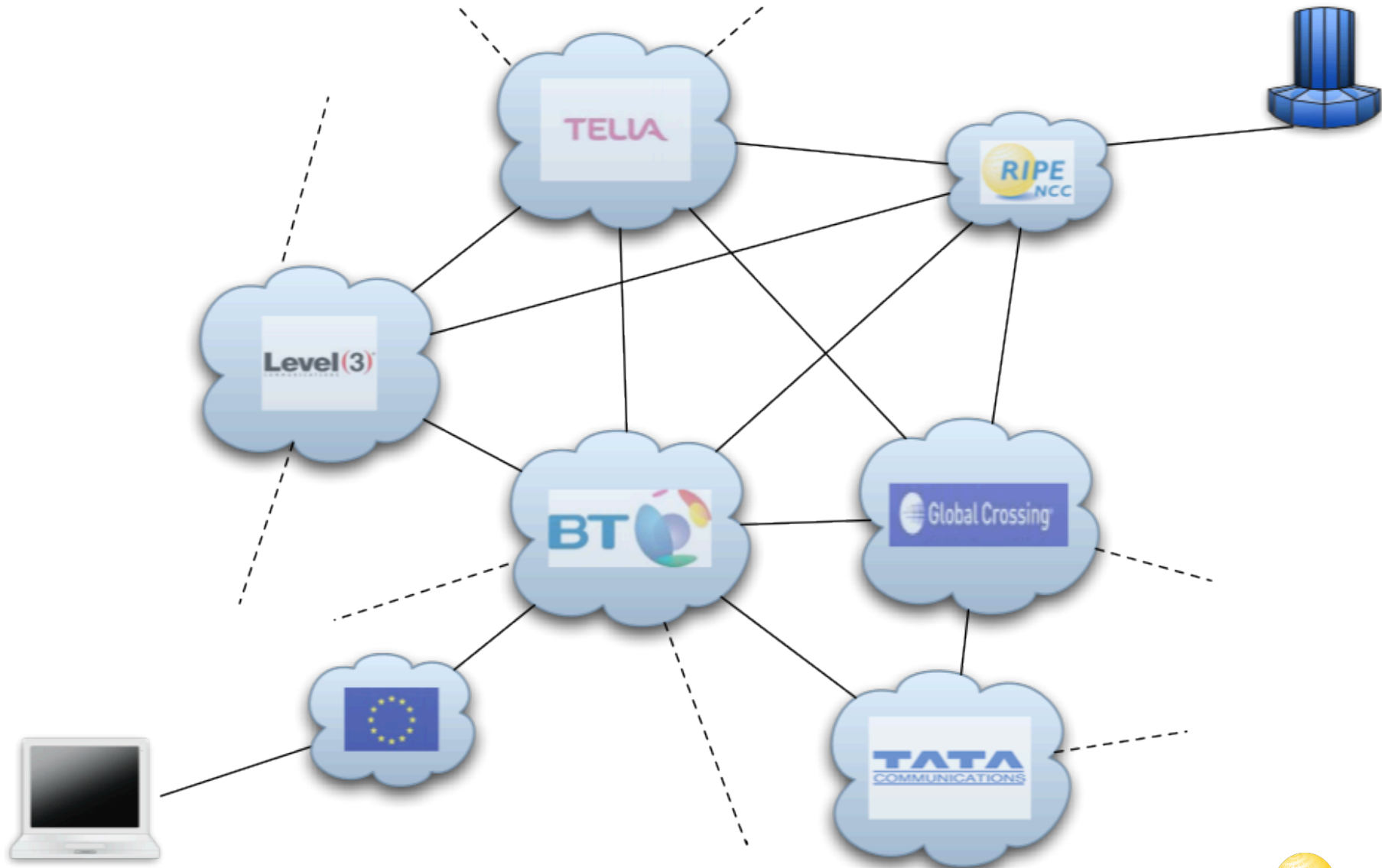
  - **not a lobby group!**

Outline

- Internet Routing
  - How it works
  - What makes it work in practice
  - What can go wrong today

- Risk Mitigation
  - Routing Hygiene
  - Resource certification & checks
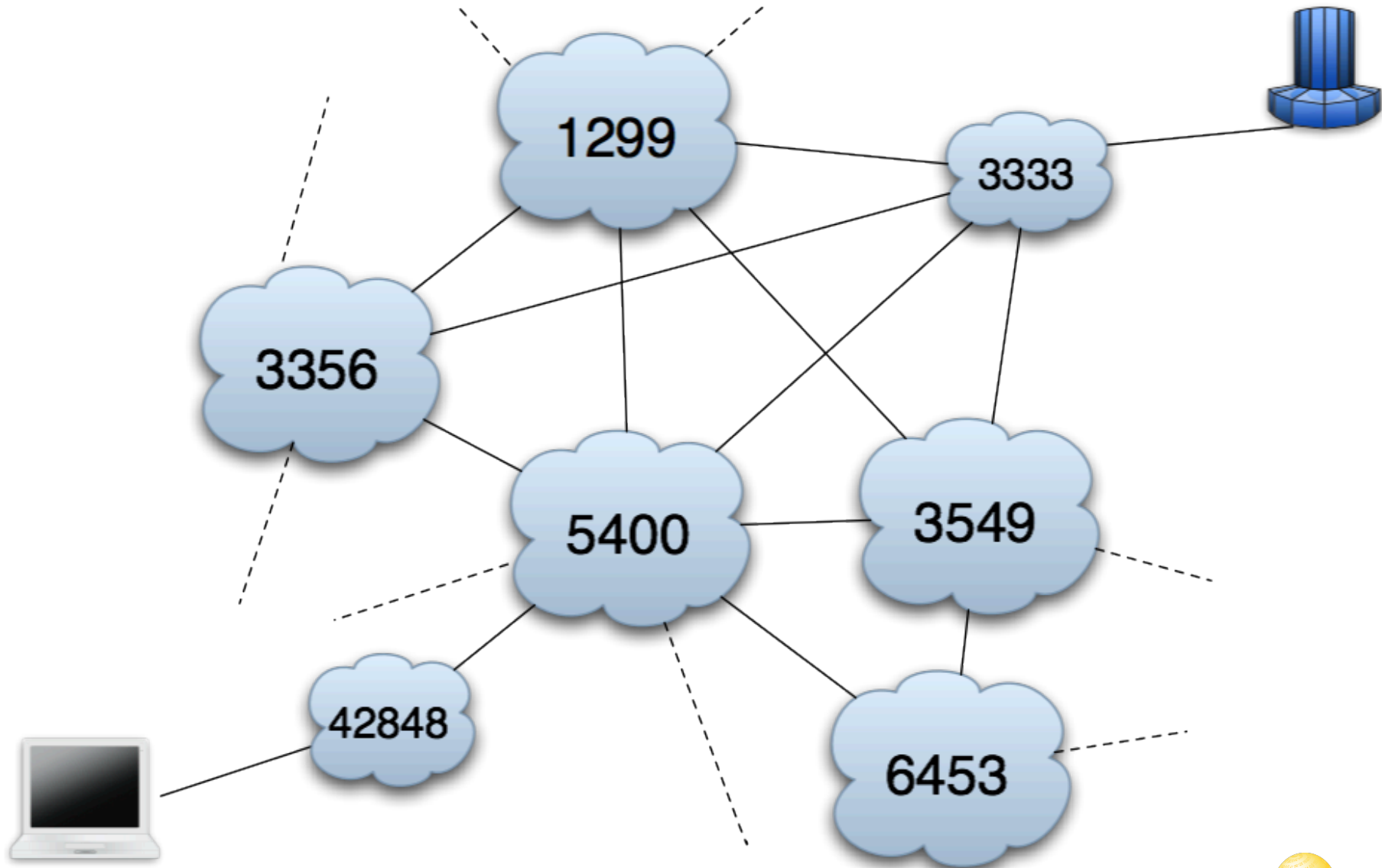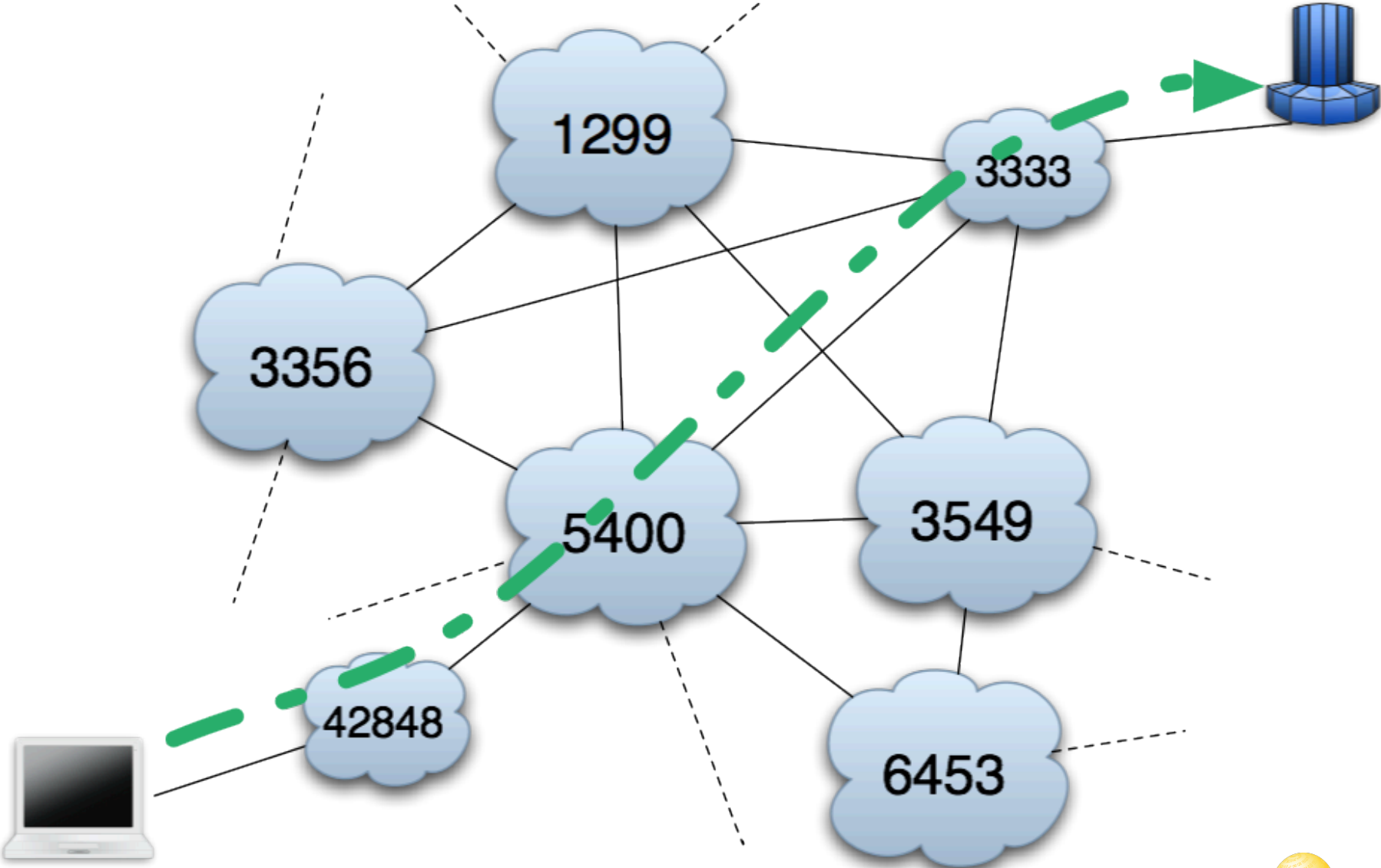 - Obstacles

- Discussion
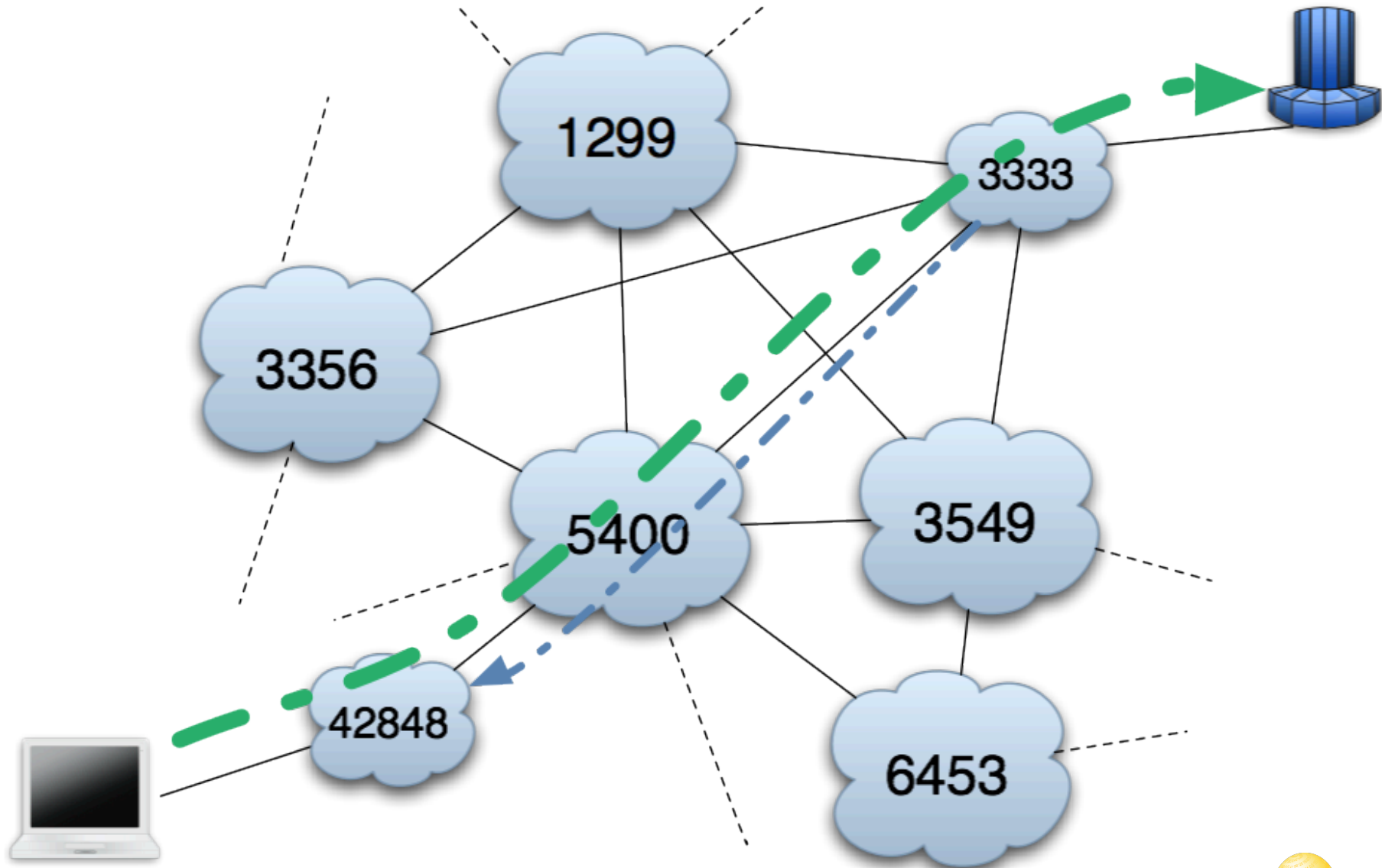
The Internet
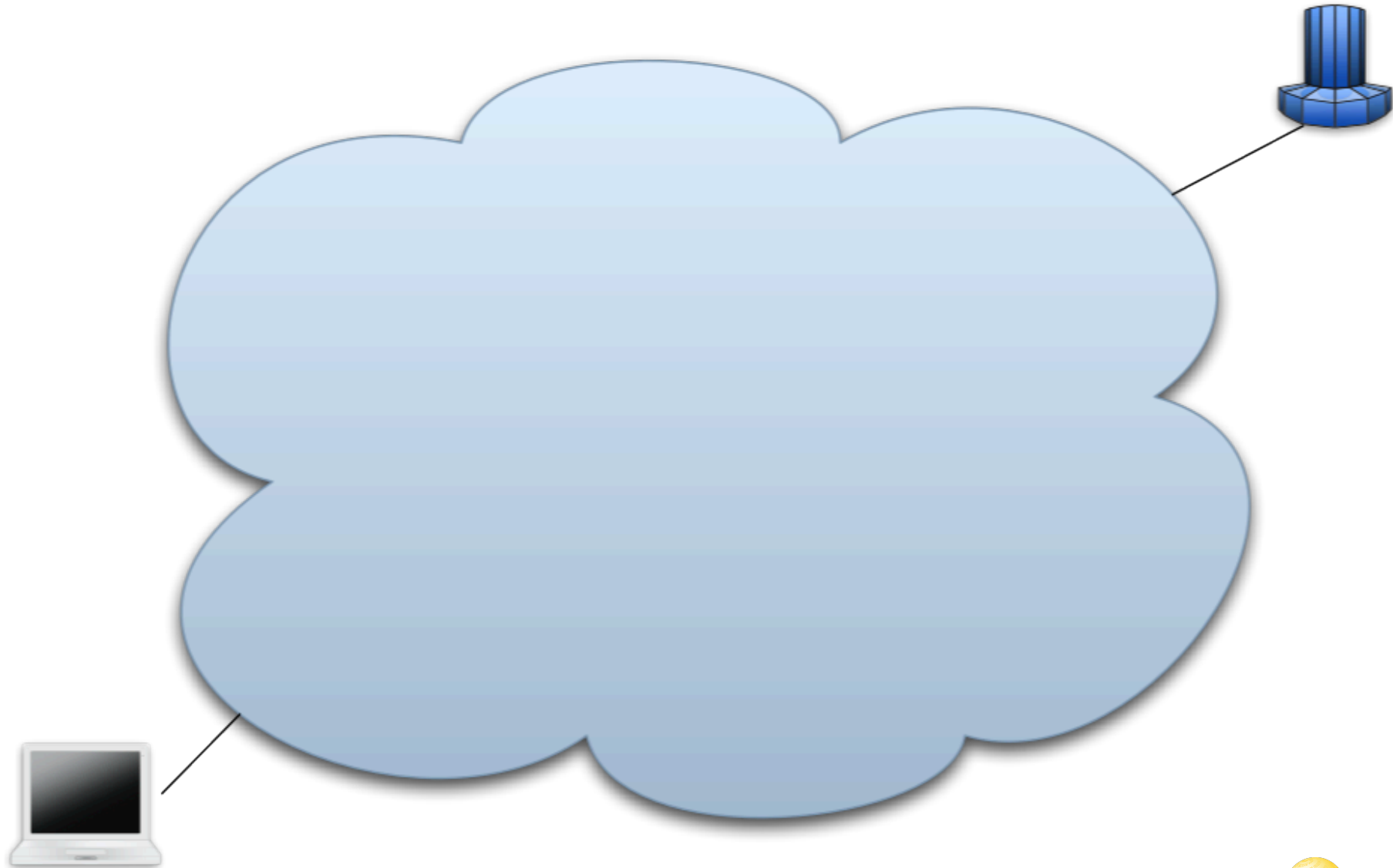
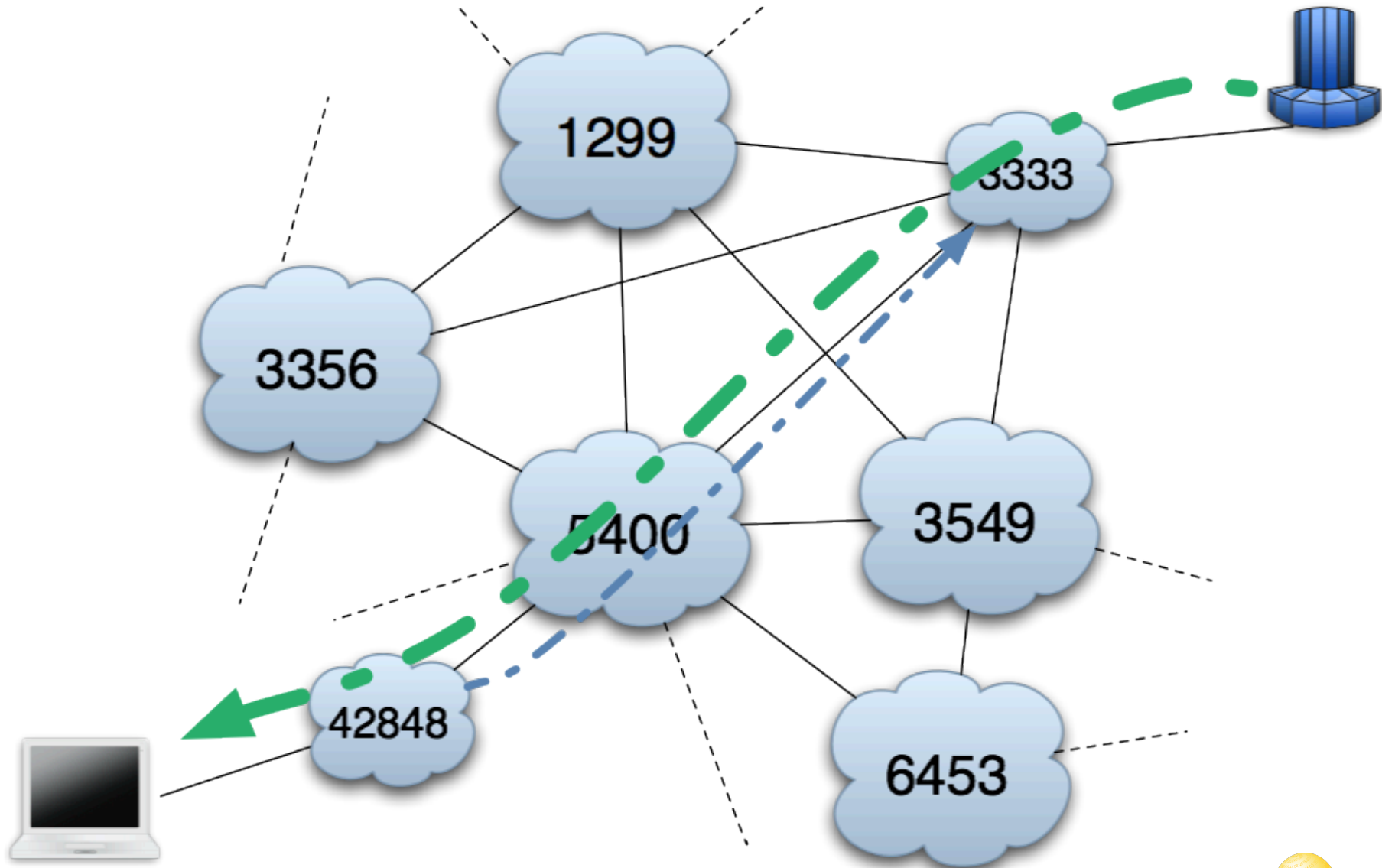# Part(s) of the Internet

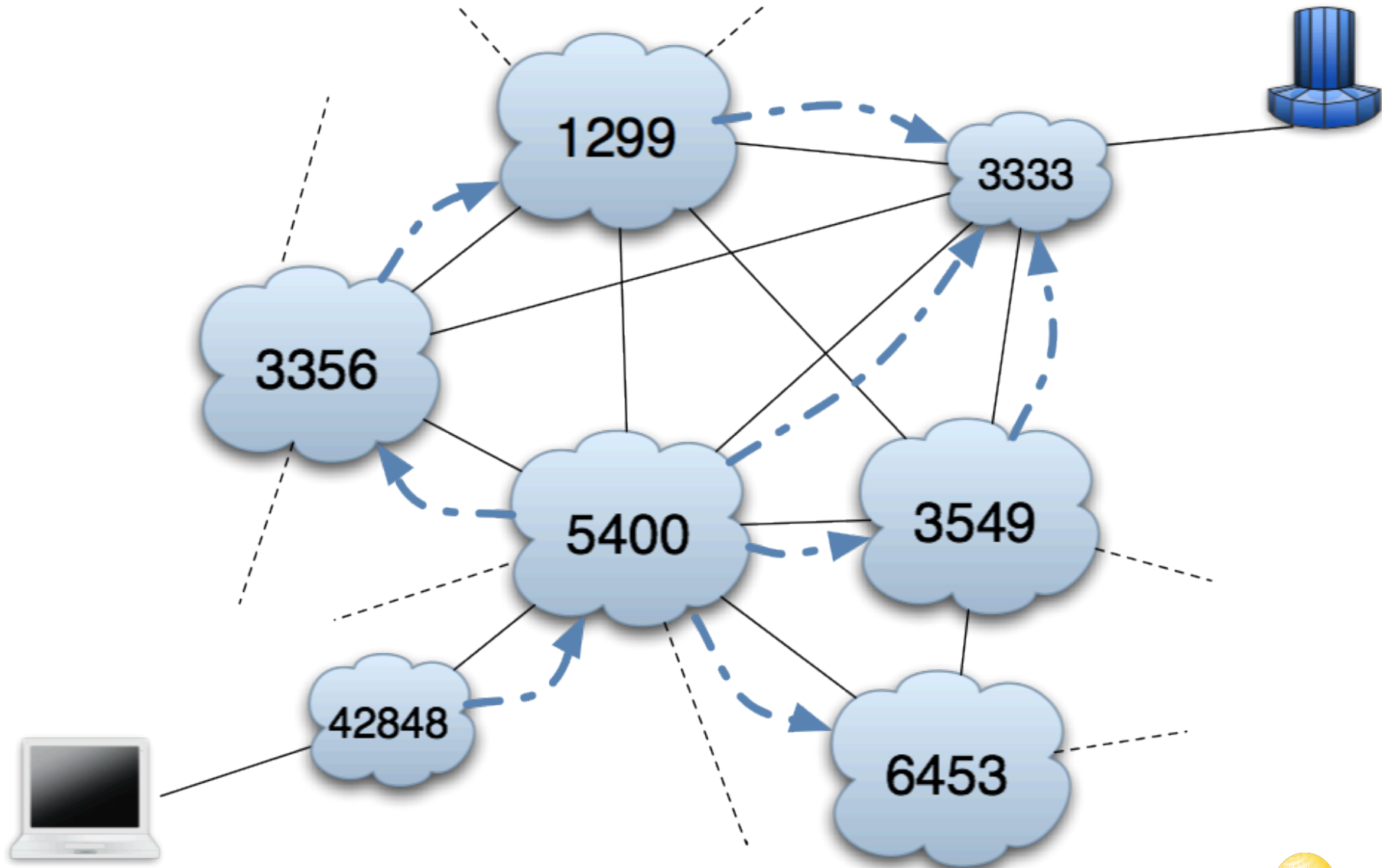# "Autonomous Systems"

Packet Flow

Routing Information Flow (BGP)

Both Directions are Needed

Choice and Redundancy

Questions?

What makes it work

Transit "Upstream"

Transit "Upstream"

"Peer"

Our AS

"Peer"

Customer "Downstream"

Customer "Downstream"
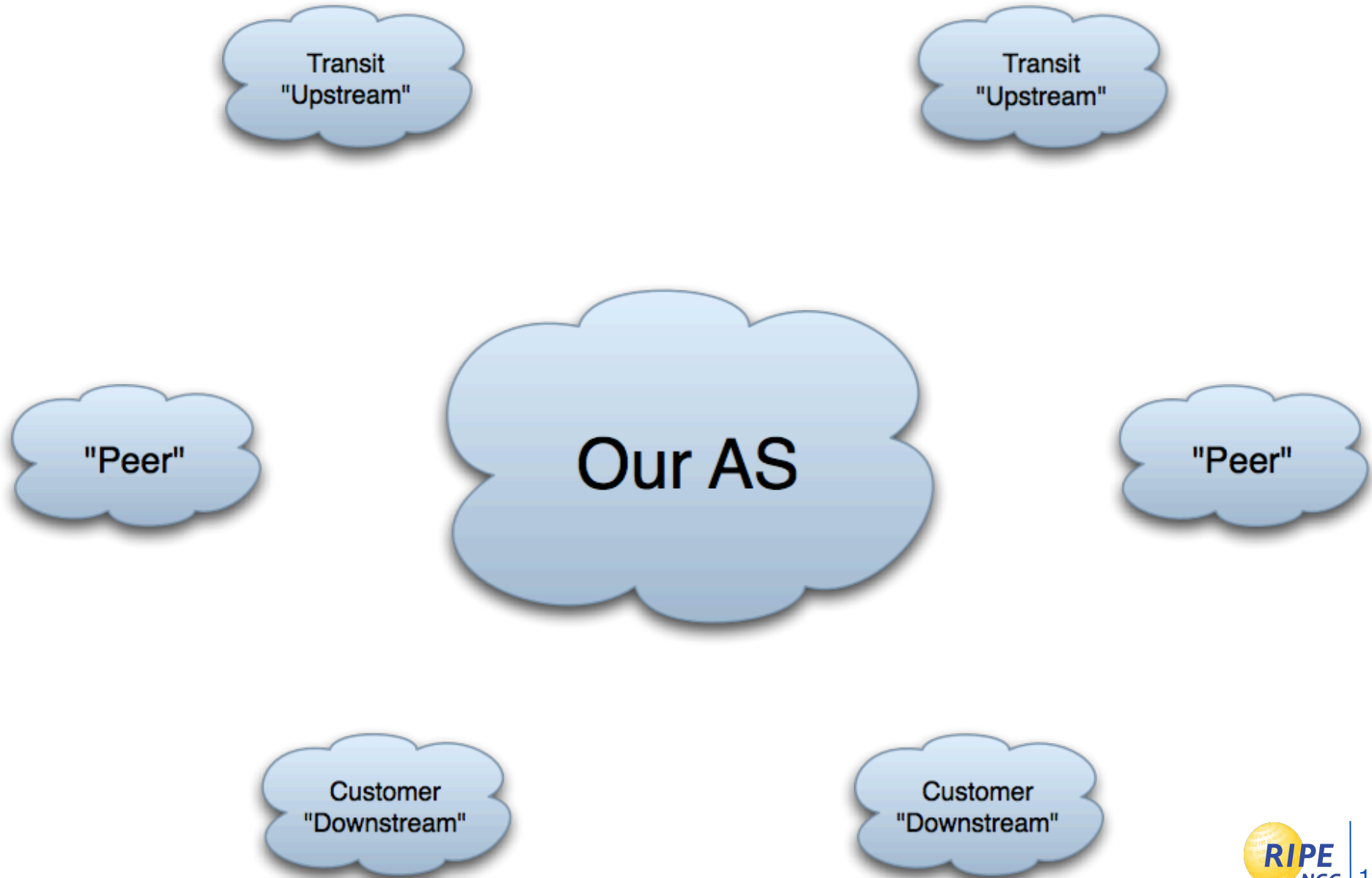
Business Relationships

Transmission Paths
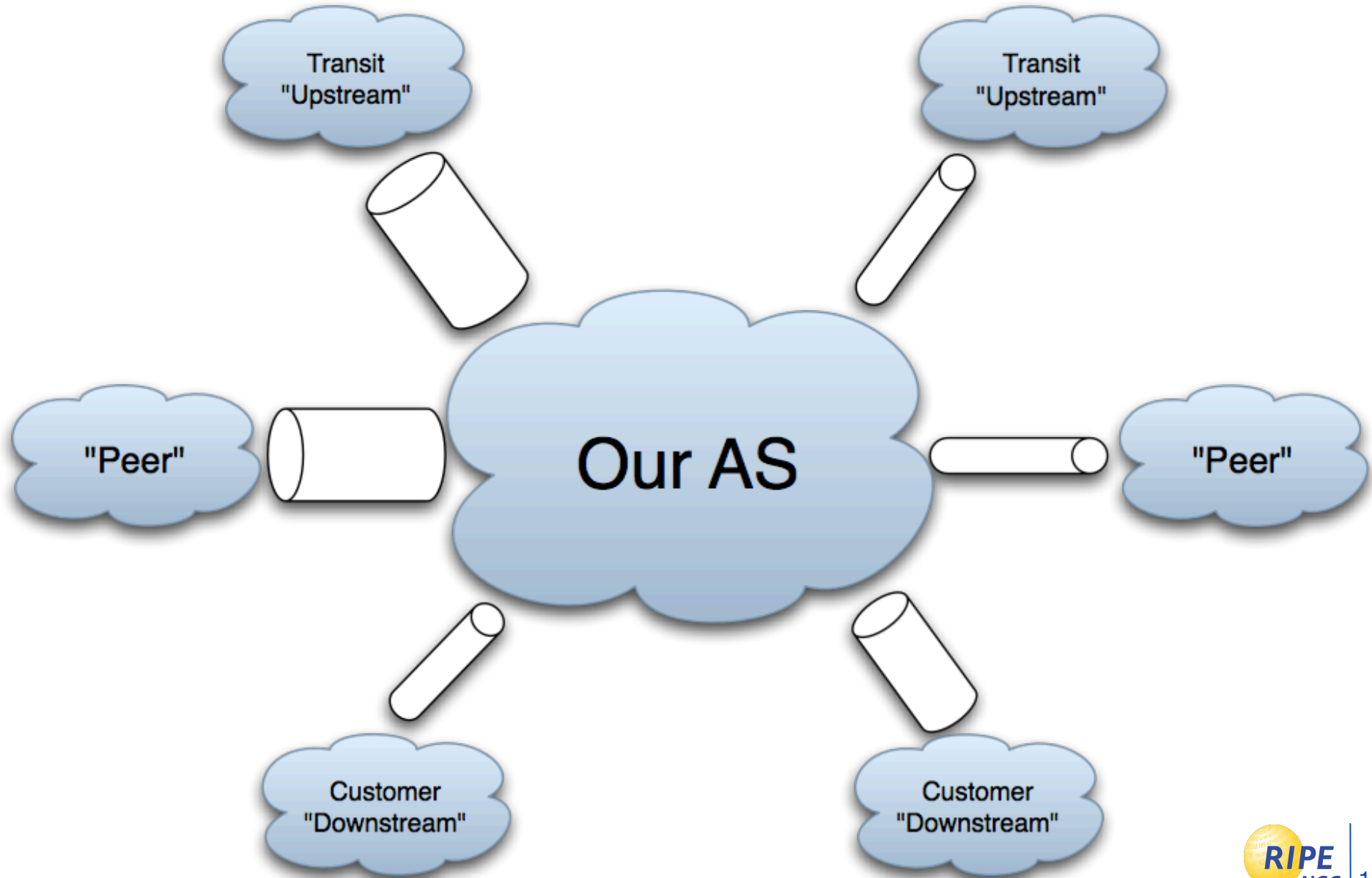
Routing Engineering
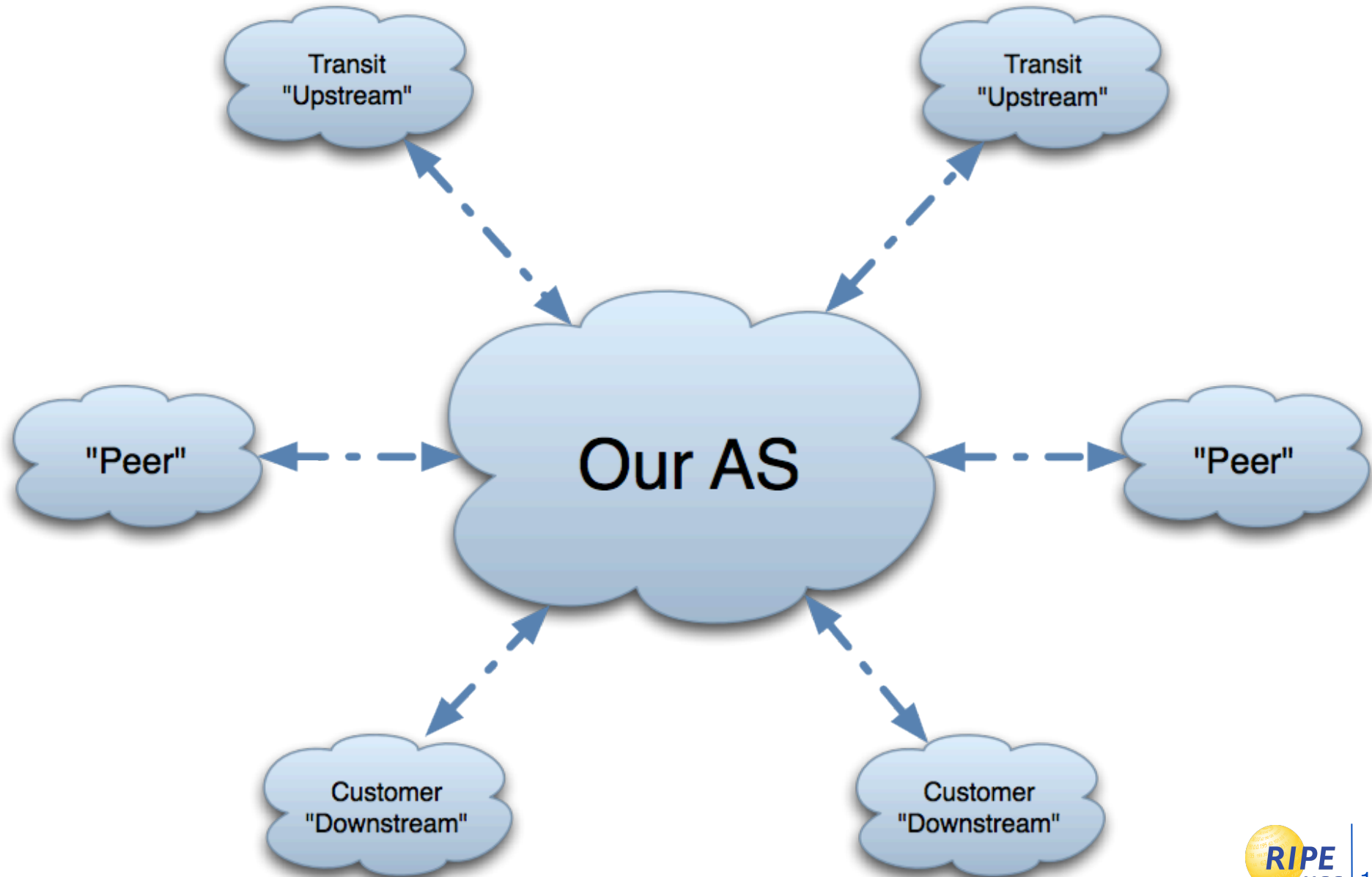
Routing Engineering Methods

- Inbound Traffic
  - Selectively announce routes.
  - Very little control over preferences by other ASes.

- Outbound Traffic
  - Decide which of the known routes to use.

- Inputs
  - Cost
  - Transmission Capacity
  - Load
  - Routing State

Routing Engineering Principles
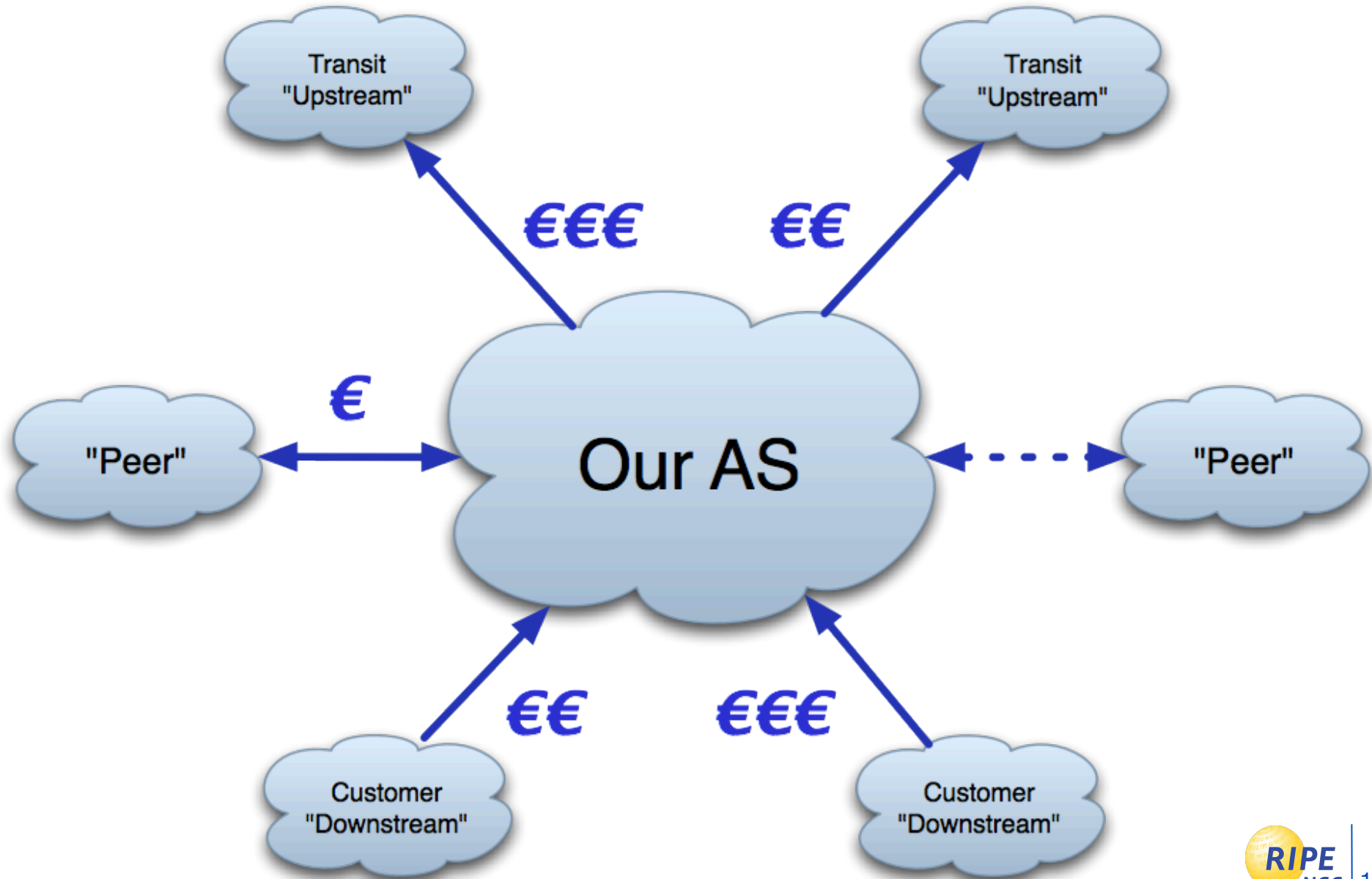
- **Autonomous Decisions by each AS**

- Local tools

- Local strategies

- Local knowlege

- Business advantages

- **Autonomous Decisions by each AS**

- (One of the reasons for rapid growth of the
  Internet)

Questions?

What can go wrong

- Misconfiguration
  - Announcing too many routes (unitentional transit)
  - Originating wrong routes

- Malicious Actions
  - Originating wrong routes (hijacking)

Hijacking
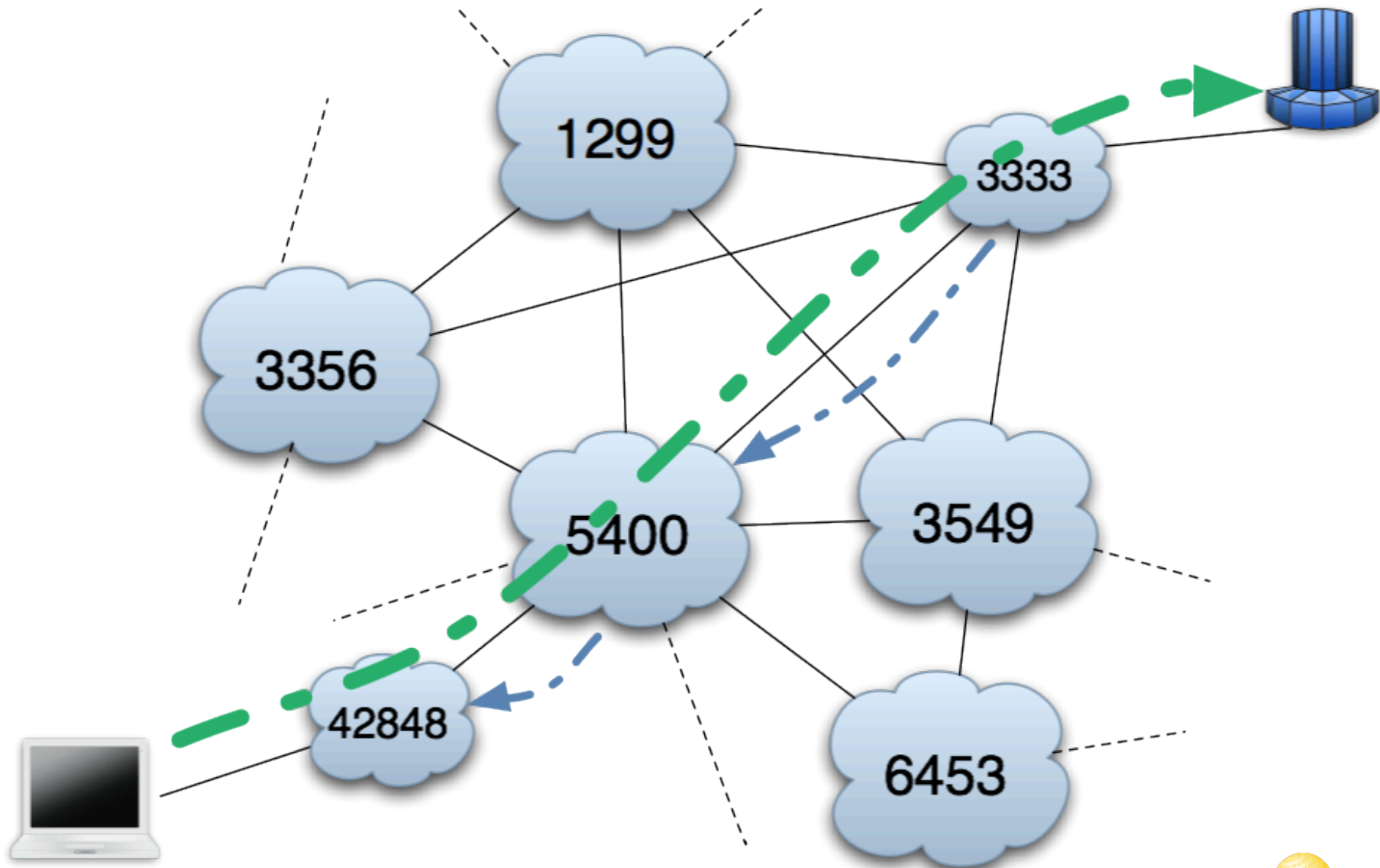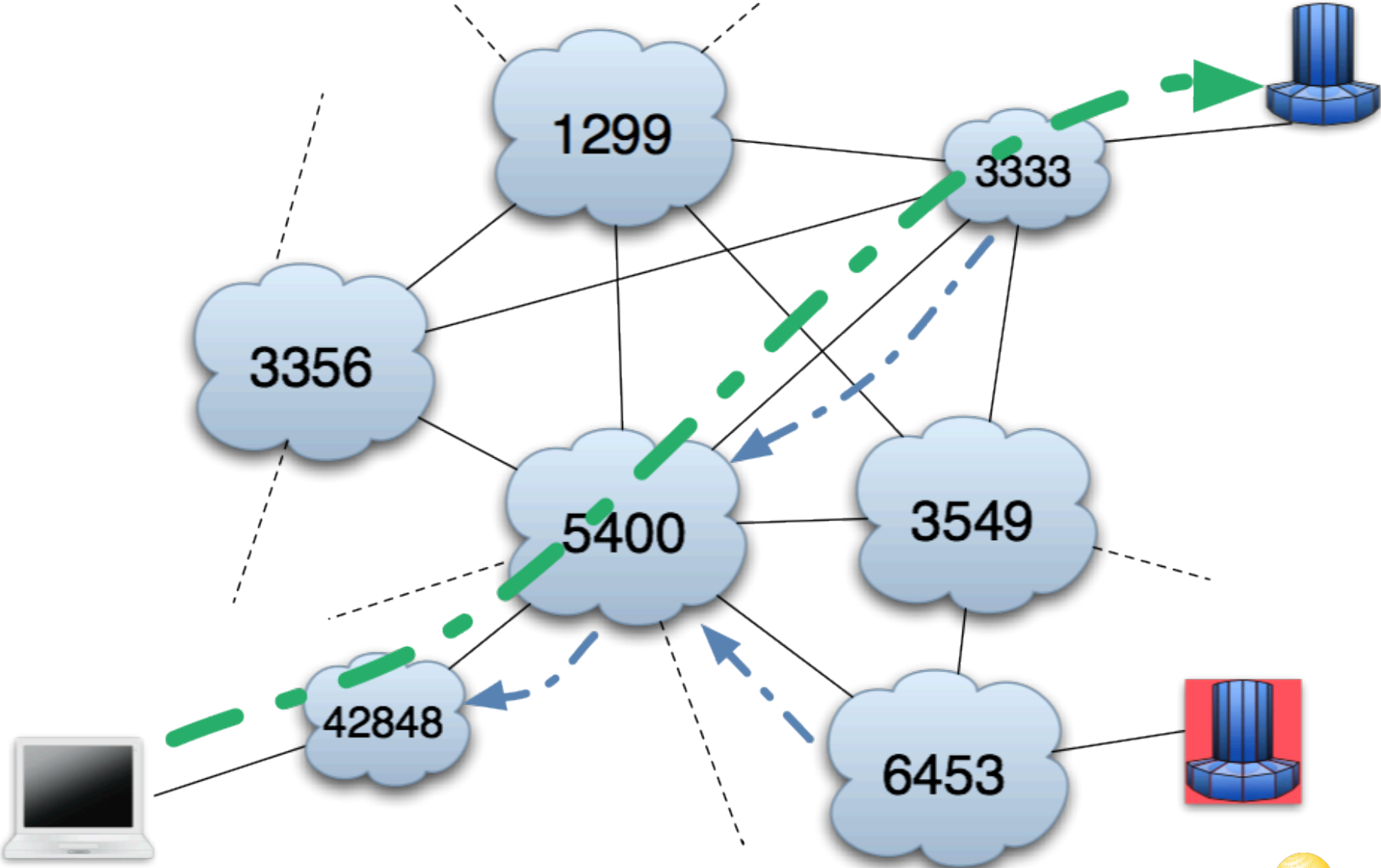
Hijacking

Hijacking
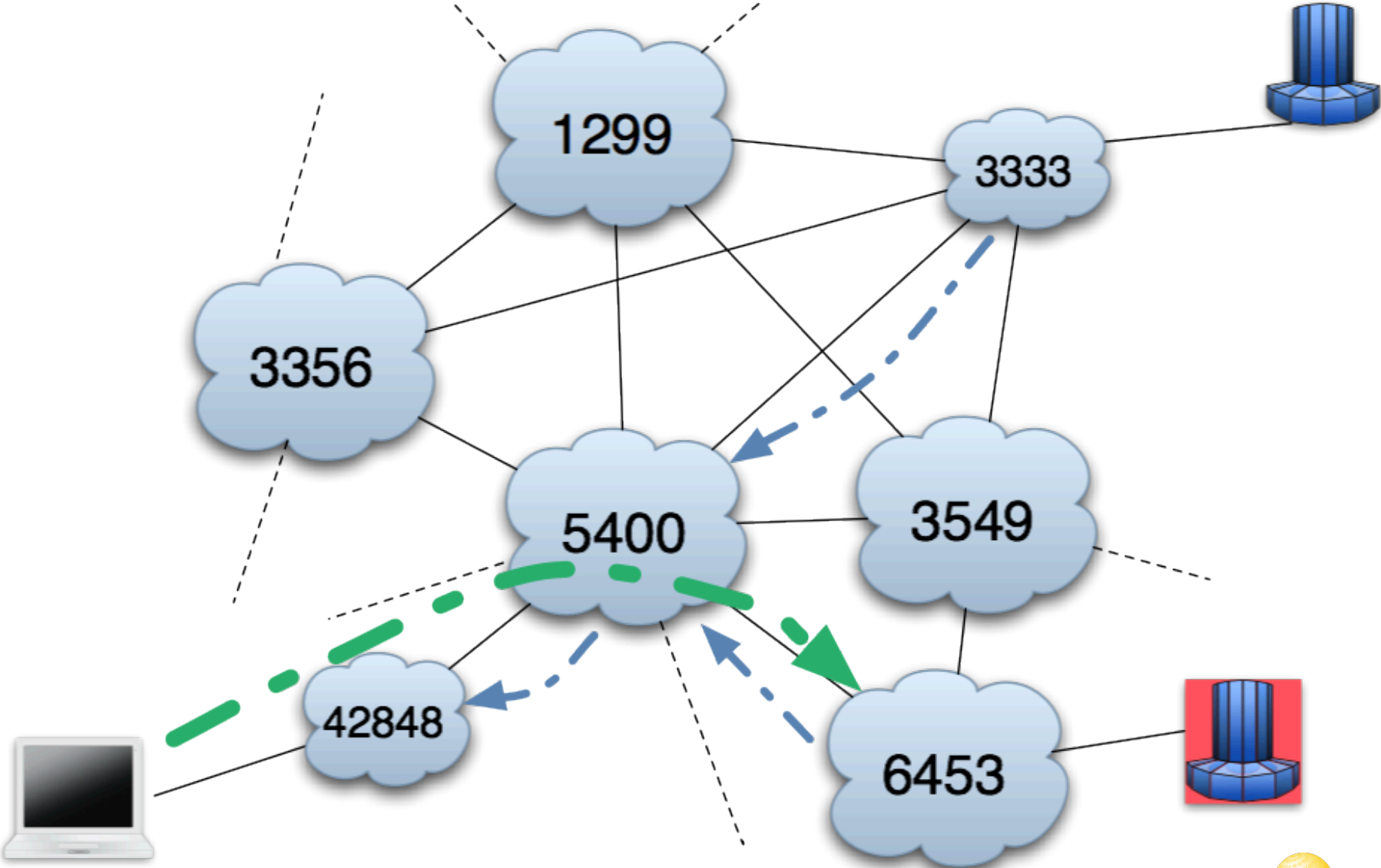
Questions?

Examples

- YouTube & Pakistan Telecom (2008)

- A number of full table exports

- Various route leaks from China (2010)

YouTube Movie

Outline

- Internet Routing
  - How it works
  - What makes it work in practice
  - What can go wrong today

- **Risk Mitigation**
  - Routing Hygiene
  - Resource certification & checks
  - Obstacles

- Public Policy Considerations

- Discussion

Routing Hygiene

- Do not accept customer routes from peers or upstreams

- Limit number of prefixes accepted per adjacent AS

- Use a routing registry
  - no global authoritative registry exists

- Use own knowledge about topology
  - topology is constantly changing
  - distruptions can cause drastic changes

Routing Hygiene

- Is applied locally / autonomously

- Has a cost

- Subservient to routing engineering
  - No obstruction
  - Maintain Autonomy

- Cooperation
  - Trust
  - Community
  - Personal Relations

Resource Certification - Motivation

- Good practice:
    - to register routes in an IRR
    - to filter routes based on IRR data

- Problem:
    - only useful if the registries are complete
    - many IRRs exist, lacking standardisation

- Result:
    - Less than half of all prefixes are registered in an IRR
    - Real world filtering is difficult and limited
    - Accidental leaks happen, route hijacking is possible

Resource Certification – Definition

"Resource certification is a reliable method for proving the association between resource holders and Internet resources."

Digital Resource Certificates

- Based on open IETF standards (sidr-wg)

- Issued by the RIPE NCC

- The certificate states that an Internet number resource has been registered by the RIPE NCC

- The certificate does not give any indication of the identity of the holder

- All further information on the resource can be found in the registry

What Certification offers

- Proof of holdership

- Secure Inter-Domain Routing
  - Route Origin Authorisation
  - Preferred certified routing

- Resource transfers

- Validation is the added value!
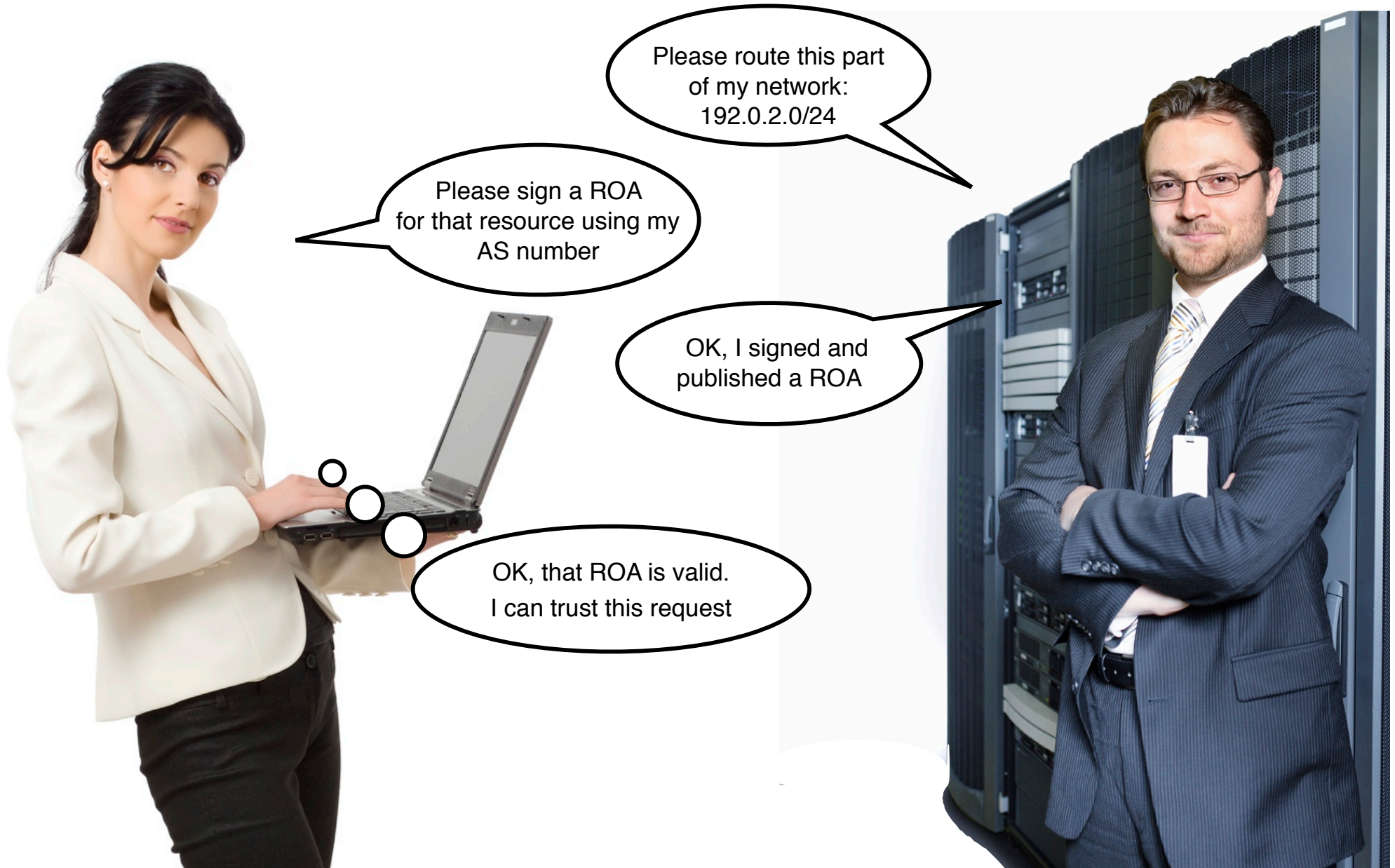
Proof of holdership

Certificate of Holdership

- Public Key

- Resources

- Signature

Route Origin Authorisation (ROA)

R.O.A. Specification

- IP Prefixes

- AS Numbers

- Signature

Automated Provisioning using ROAs

Who Controls Routing?

- Certificates do not create additional powers for the Regional Internet Registries

- Certificates reflect the resource registration status
  - no registration → no certificate
  - the reverse is not true!

- Routing decisions are made by network operators!

4 out of 5 Regional Internet
Registries have RPKI in production
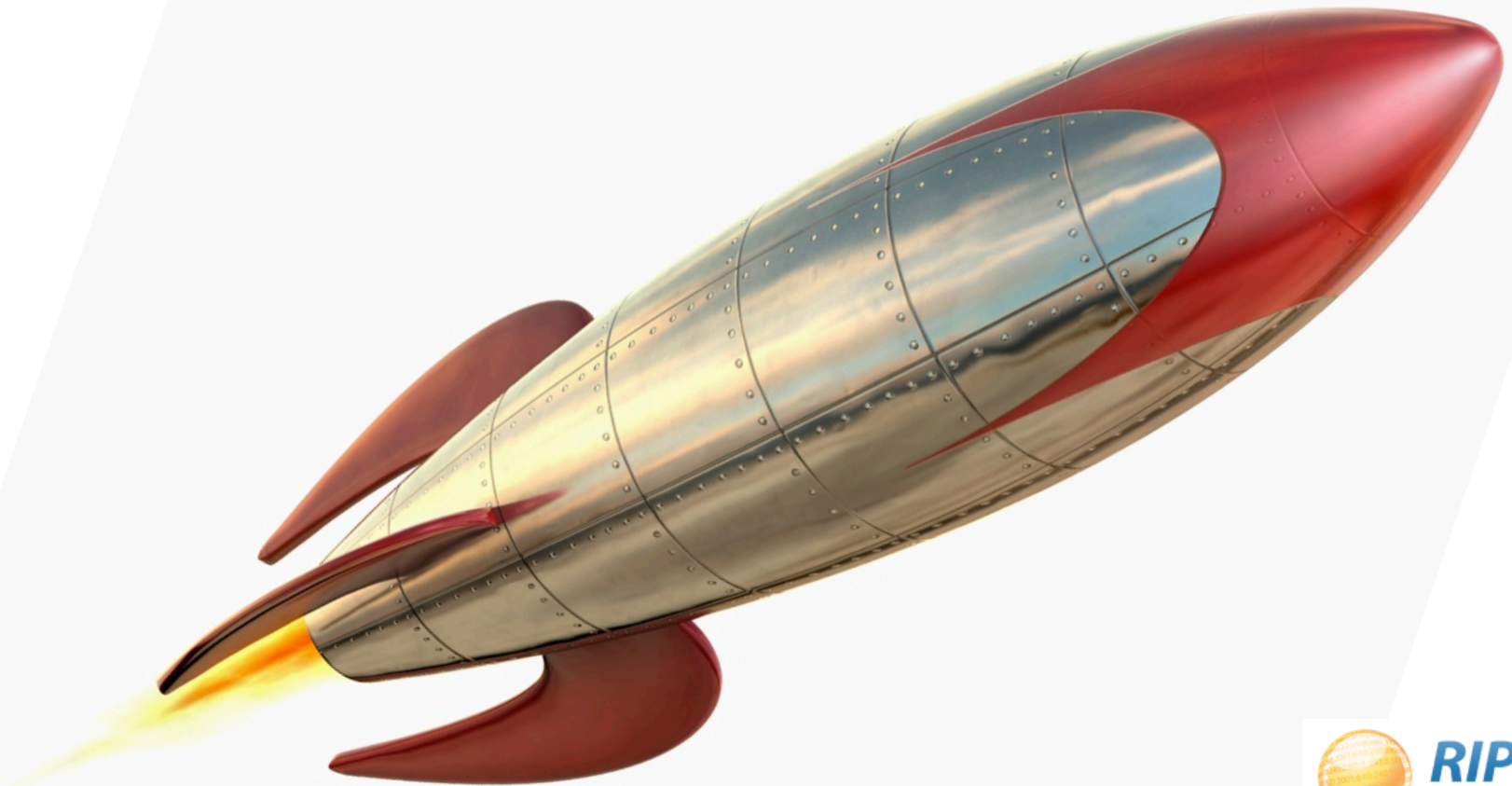
Obstacles

- **Fear of loosing autonomy**

- Cost

- Low threat perception

- Fear of loosing business advantage

- **Fear of loosing autonomy**

Questions?

My Messages Today

- Routing security needs to be improved
  - Accidents do happen … sometimes
  - Hijackings do happen … sometimes

- The sky is not falling
  - It does not happen all the time
  - It does not affect large areas of the Internet

My Messages Today

- Industry is addressing the problems
  - Local measures taken autonomously
  - RPKI being deployed by RIRs
  - RPKI based routing tools being developed
  - RPKI based routing protocols being studied in IETF

Outline

- Internet Routing
  - How it works
  - What makes it work in practice
  - What can go wrong today

- Risk Mitigation
  - Routing Hygiene
  - Resource certification & checks
  - Obstacles

- **Discussion**

The End!

Край

Y Diwedd

Fí

Finis

Соңы

ՎերՋ

النهاية

Liðugt

Ende

Finvezh

Кінець

Konec

Ënn

Fund

پایان

Kraj

Son

Kpaj

Lõpp

Beigas

Vége

An Críoch

הסוף

Endir

Fine

Sfârşit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Fim

Amaia

Loppu

Tmiem

Koniec