Computational Complexity of the routing assessment process

Cedric Llorens & Denis Valois &
Alexandre Gibouin & Yannick Le Teignier

2003 IEEE International Workshop
on Information Assurance

A Network Provider problem

• A large number of **devices** implementing **different functionalities,** with their respective **security policy** (e.g. core backbone, provider edge, customer edge, VLAN switch, etc.).

• Configuration management: the problem of inherent complexity versus **the problem of scale:**

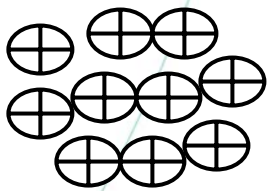
- TRIPWIRE approach: Does this device configuration has been changed?
- Scanner approach: Does this device configuration has a security weakness?
- Our approach: Does this device implements the intended features?

• **On-line versus off-line** configuration checking.

TELECOM PARIS
école nationale supérieure des télécommunications

&equant

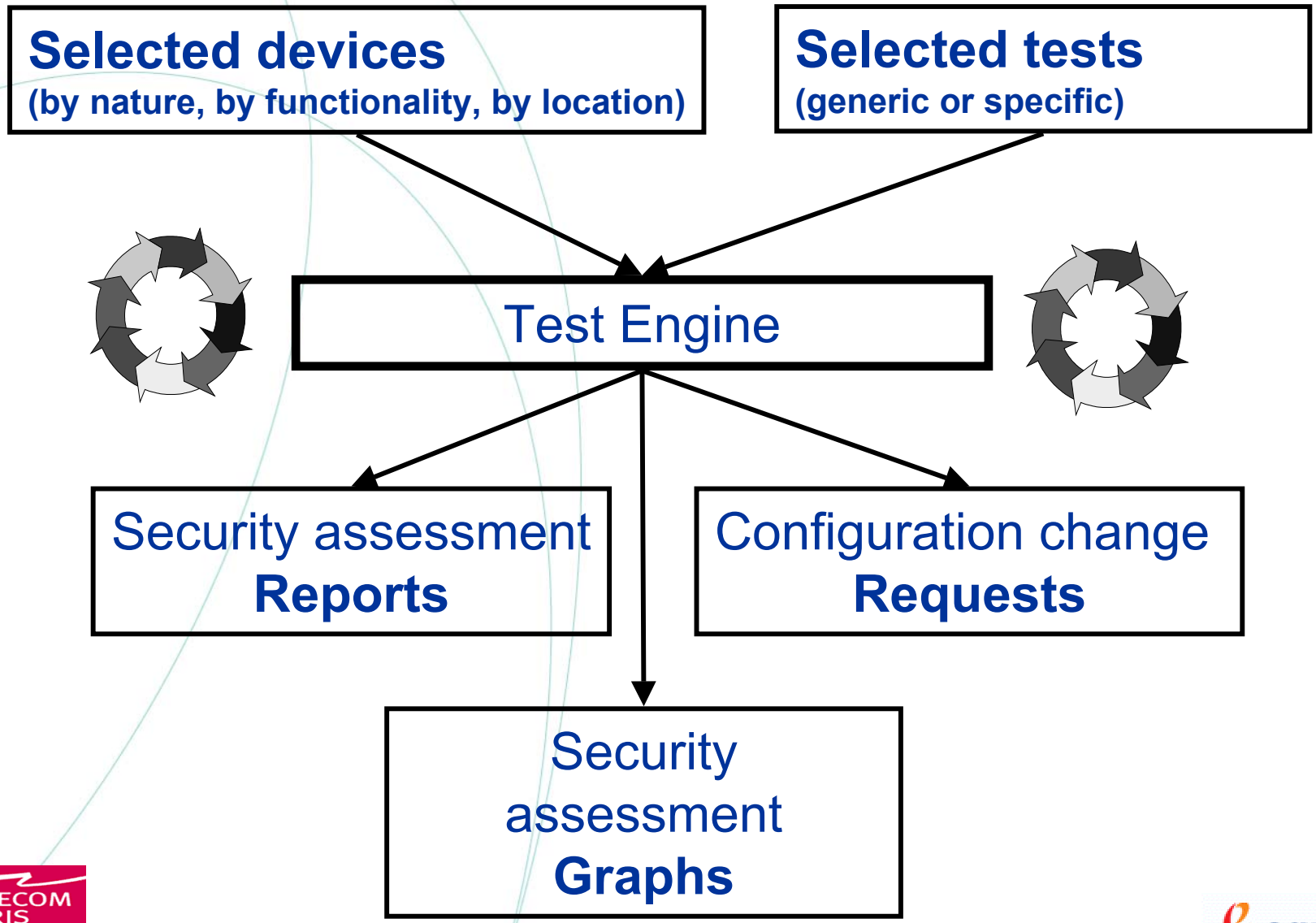
High-level model - Logical security attributes

Entities	Attributes	Metrics
 A router	Basic security attributes (ex no ip-source, no ip finger, etc.)	
	Complex security attributes (ex ACL consistency and redundancy, etc.)	
 A set of routers = a network	Basic security attributes (ex unique ip address range, etc.)	
	Complex security attributes (ex network routing topology rules, MPLS/VPN perimeter, etc.)	

TELECOM PARIS
école nationale supérieure des télécommunications

equant

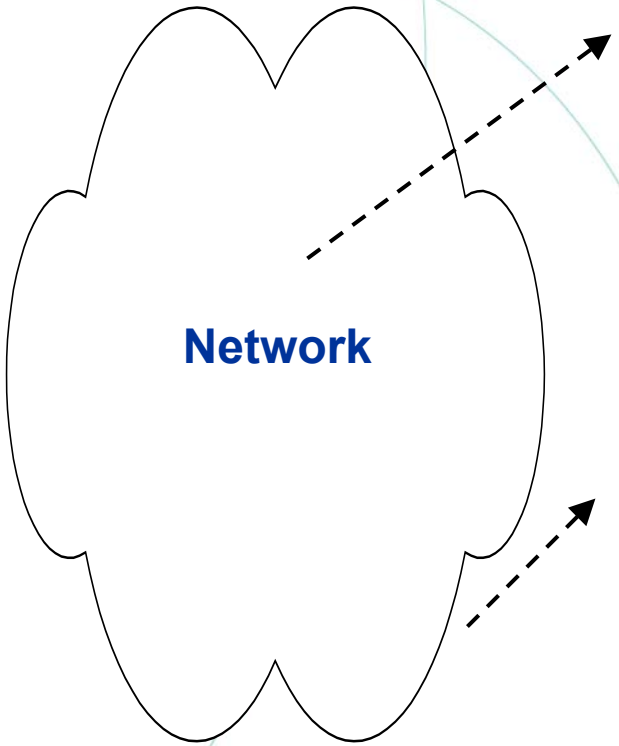
High-level model - Reverse engineering



TELECOM PARIS
école nationale supérieure des télécommunications

equant

Backbone network routing protocols



IGP (internal gateway protocol)

-> RIP, IS-IS, OSPF

- Fast convergence
- Fast failure detection
- Number of IP prefixes advertised limited
- Internal backbone ip address range use only

EGP (external gateway protocol)

-> EGP, BGPv4

- Flexible
- Scalable
- High Number of IP prefixes advertised (>100.000)
- Customer ip address range

TELECOM PARIS
école nationale supérieure des télécommunications

equant

Backbone network routing security policy

- **IGP (internal gateway protocol) / IS-IS**
  - Password security policy
  - Administrative distance security policy
  - Topology security policy

- **EGP (external gateway protocol) / BGPv4**
  - Password security policy
  - Topology security policy
  - Connections security policy

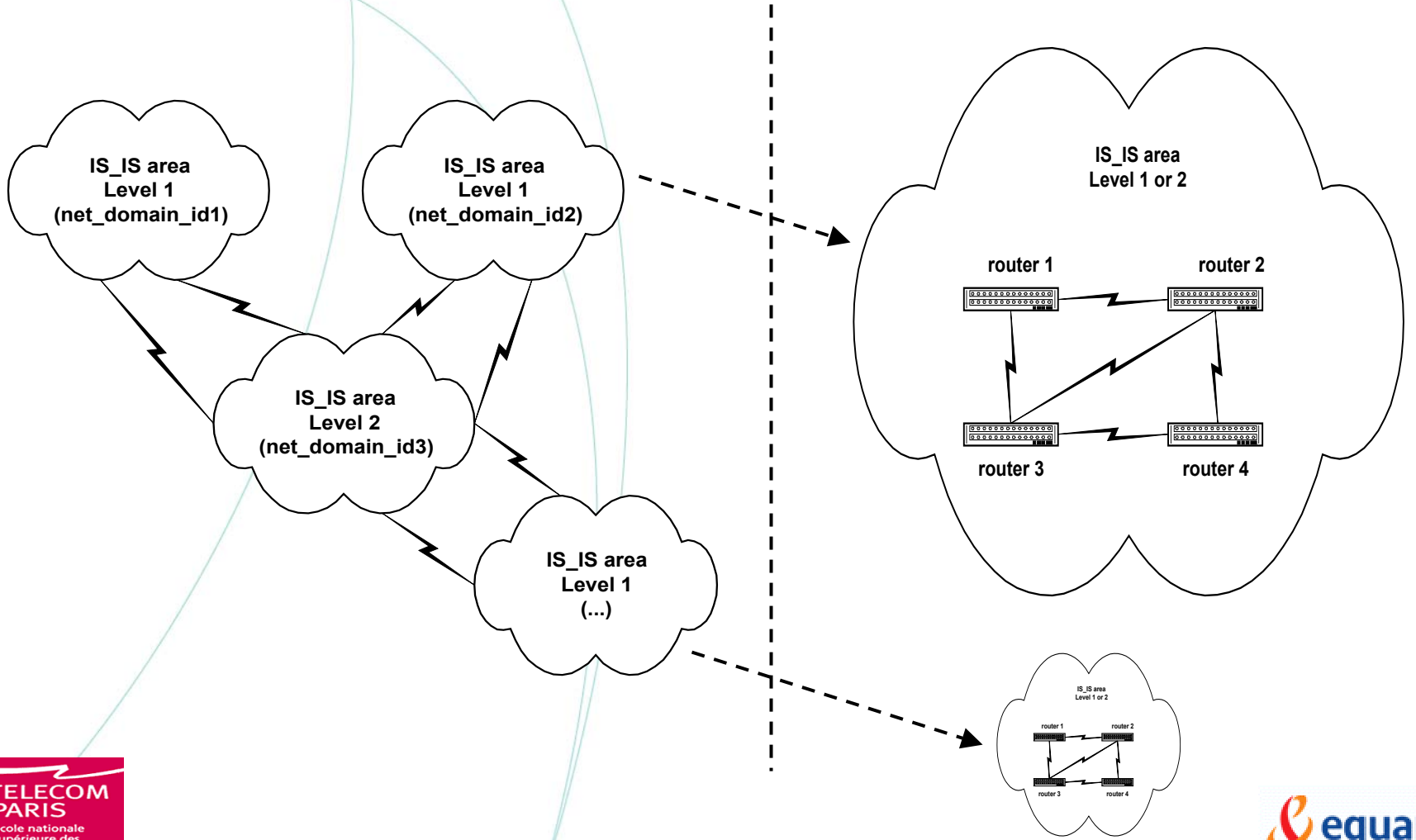
TELECOM PARIS
école nationale supérieure des télécommunications

equant

Computation of the IGP routing graph

Topology level 1

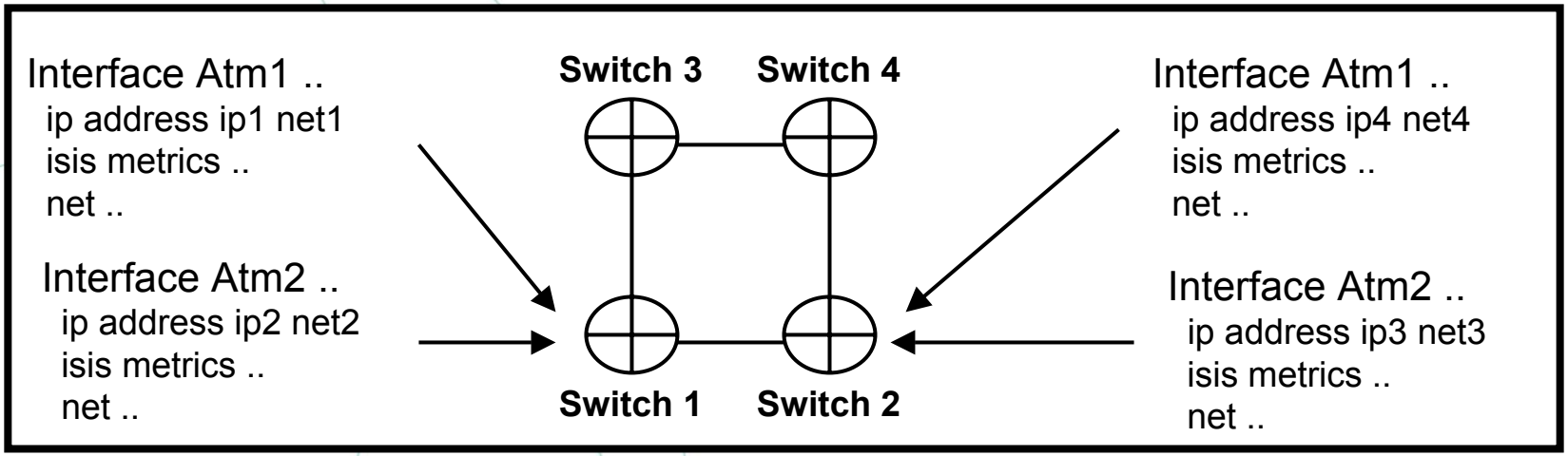
Topology level 2

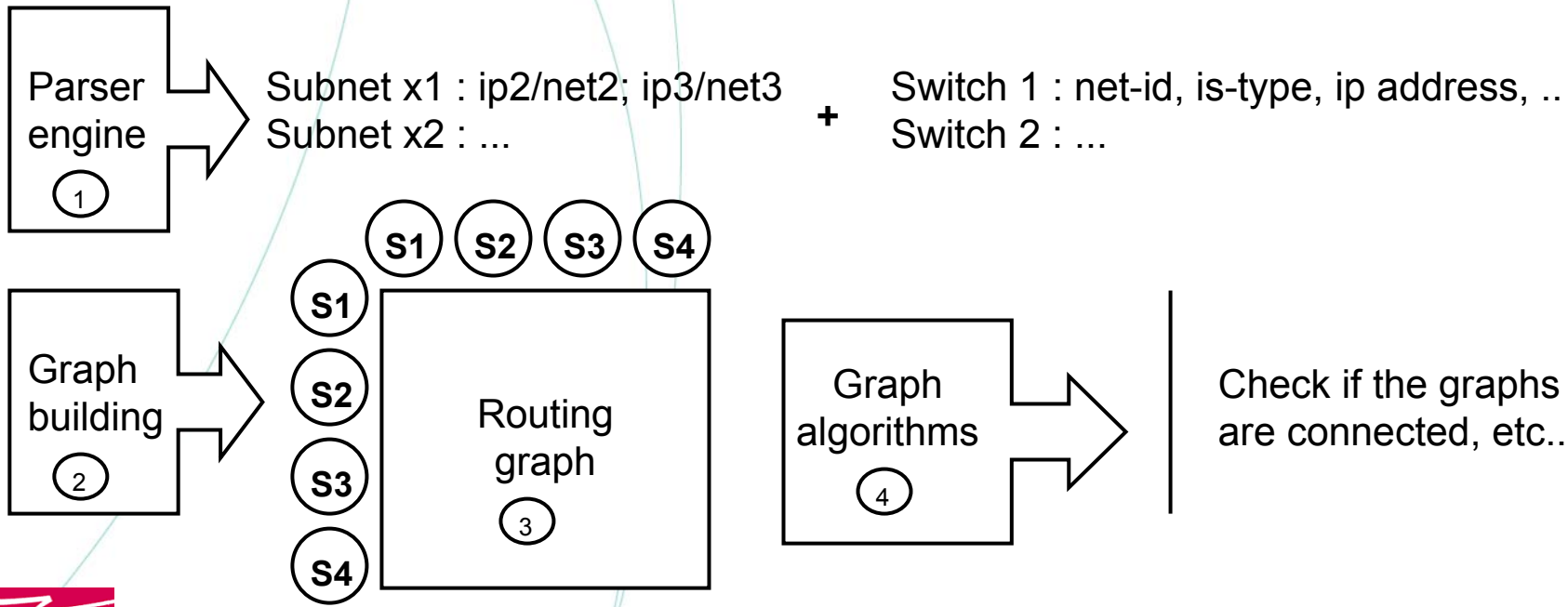


TELECOM PARIS
école nationale supérieure des télécommunications

equant

Computation of the IGP routing graph





TELECOM PARIS
école nationale supérieure des télécommunications

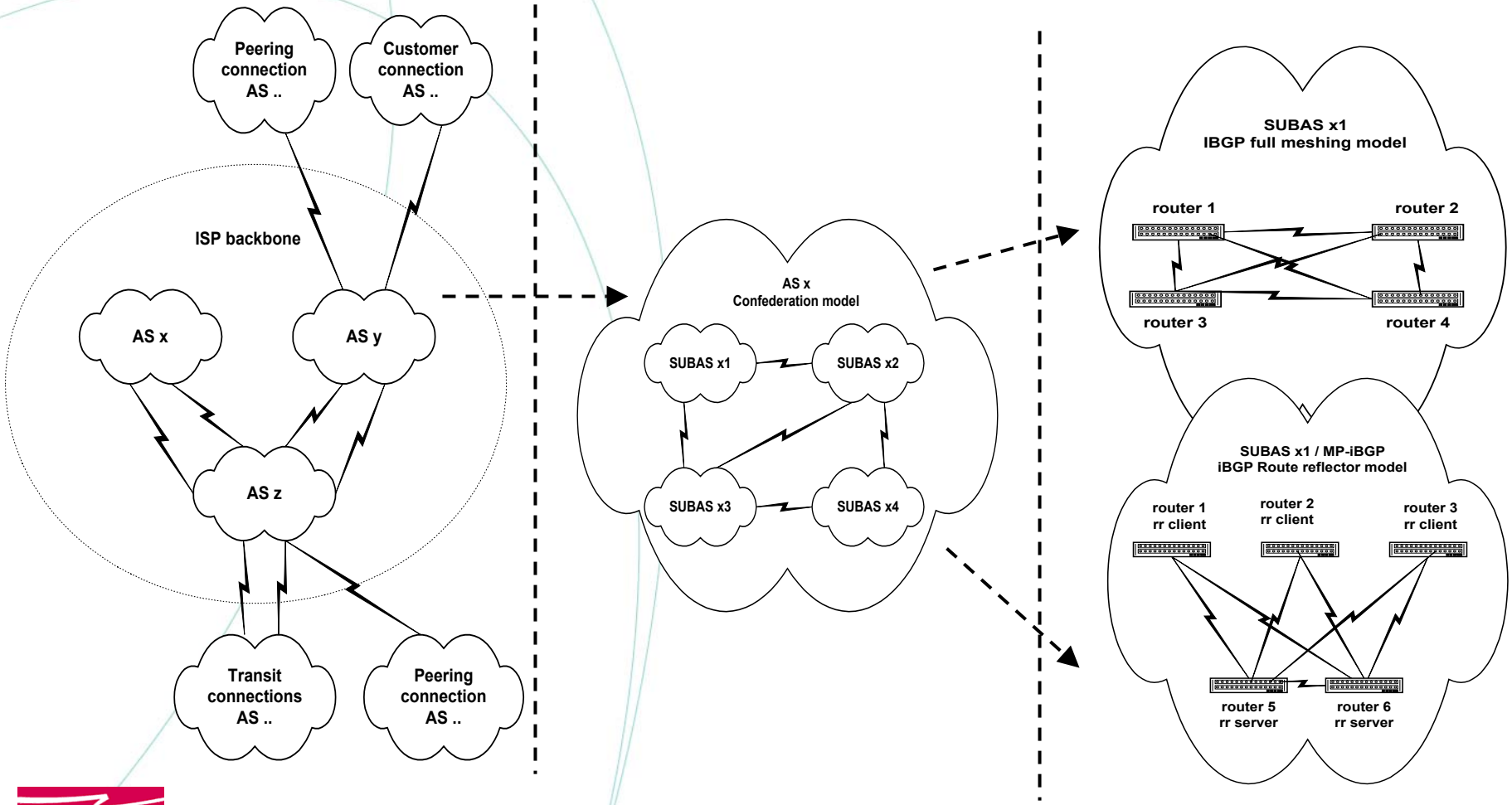
&equant

Computation of the EGP routing graph

Topology level 1

Topology level 2

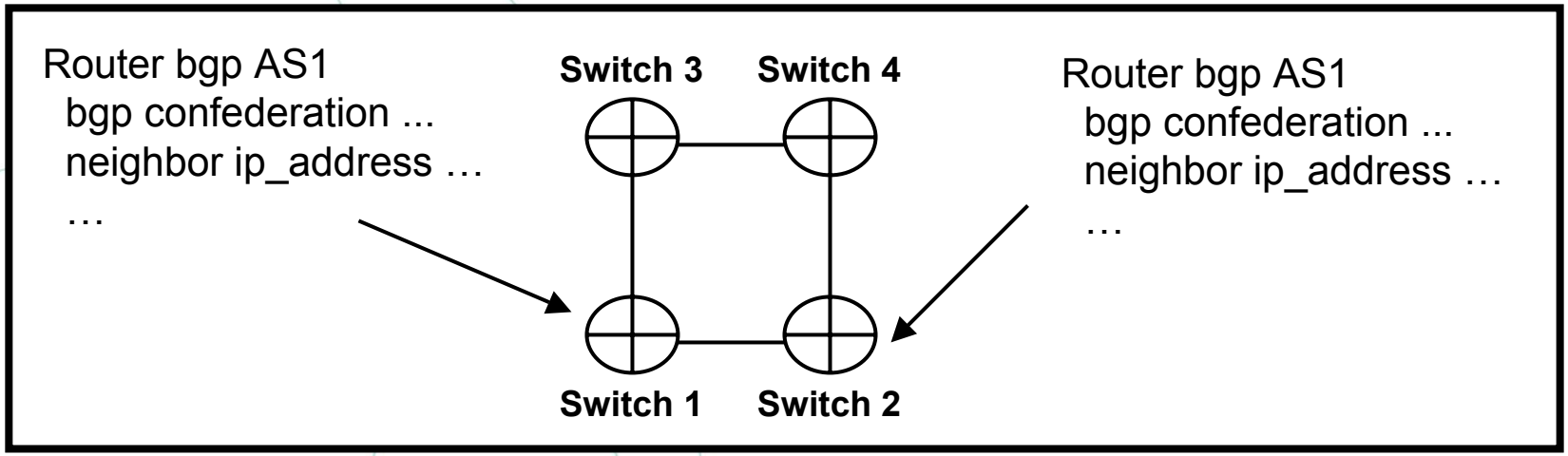
Topology level 3



TELECOM PARIS
école nationale supérieure des télécommunications

equant

Computation of the EGP routing graph



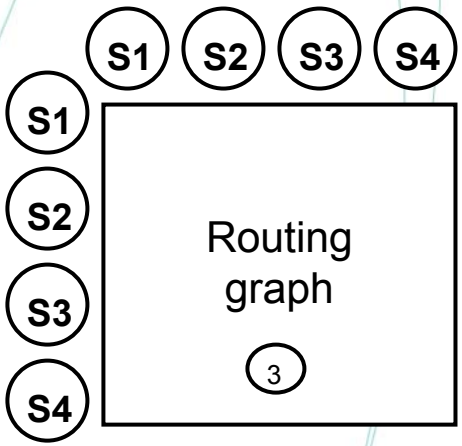
Parser engine (1)

Switch 1 : AS(id), Confederation(id), Neighbor(ip)
Switch 1 : AS(id), Confederation(id), Neighbor(ip)
...

+

Switch 1 : ip address
Switch 2 : ip address
...

Graph building (2)



Graph algorithms (4)

Check if the graphs are connected, etc..

TELECOM PARIS
école nationale supérieure des télécommunications

equant

Tool Scope of Usage

- **Regular backbone assessments** (automated).

- **Diagnostic help** (ad-hoc test); e.g. recently used for the SNMP bug (parsing of thousand router configurations).

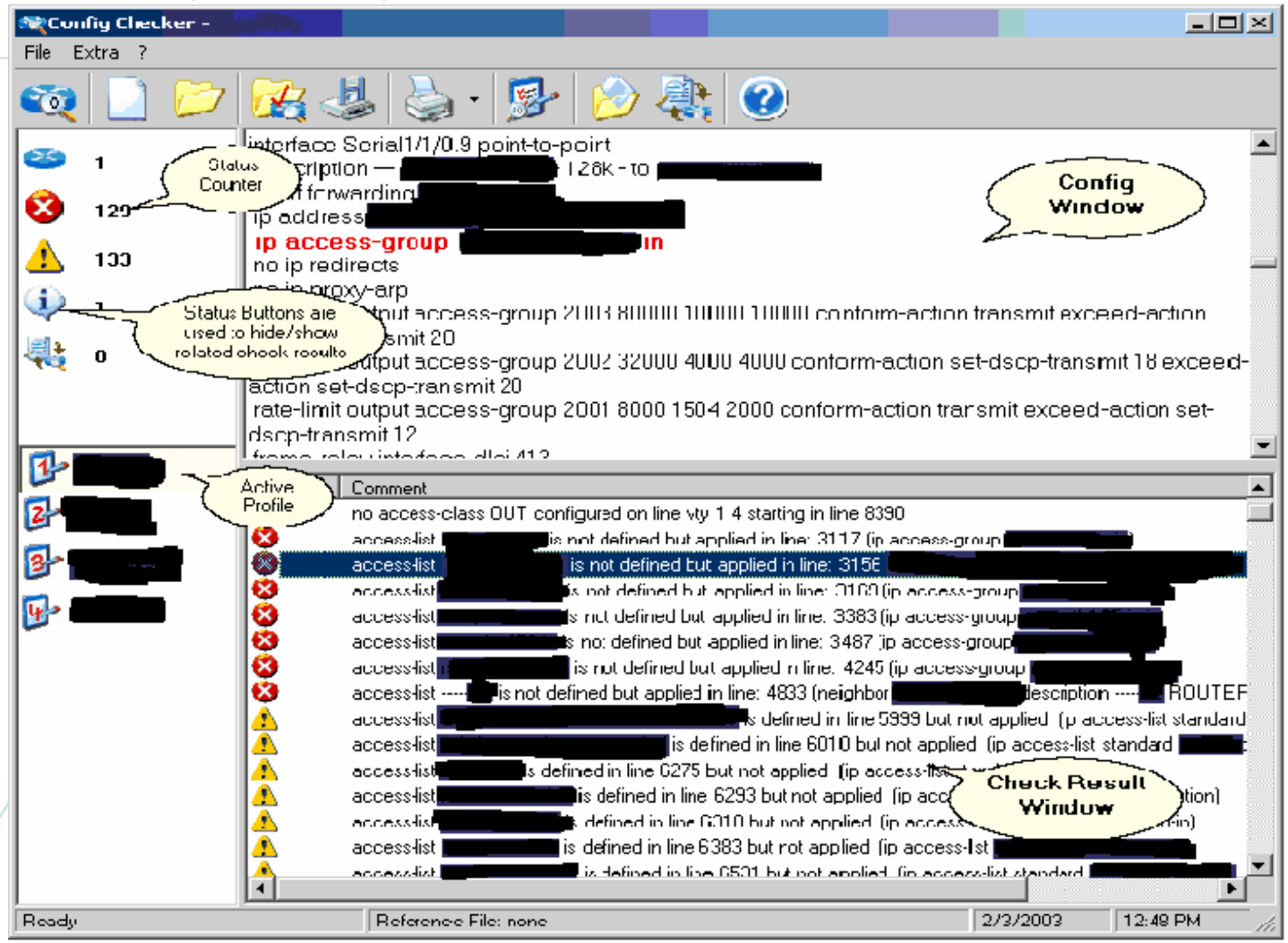
- **On demand** for any Customer VPN audit (development of a User Graphical Interface for network operational teams to lead security assessments).

- **Driven by**
  - Network Security Office.
  - Backbone and Edge network teams.

TELECOM PARIS
école nationale supérieure des télécommunications

equant

Tool Scope of Usage



TELECOM PARIS
école nationale supérieure des télécommunications

equant

Research and perspectives

Define a framework for **network logical risk measurement** taking into account the following inputs:

- **Threat:** any circumstance or event with the potential to cause harm to a network component … *(-> Probability Theory & Bayesian networks).*
- **Vulnerability:** is a logical security weakness in a network component … *(-> Network logical security metrics).*
- **Consequence:** is the impact with an exploited network component vulnerability … *(-> Analytic Hierarchy Process).*
- **Risk Model:** is the framework used to evaluate risk *(-> Probabilistic Risk Assessment method - NASA)*

TELECOM PARIS
école nationale supérieure des télécommunications

&equant

Questions ?

cedric.llorens@equant.com
denis.valois@equant.com
yannick.leteignier@equant.com
alexandre.gibouin@equant.com

TELECOM PARIS
école nationale supérieure des télécommunications

equant