



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

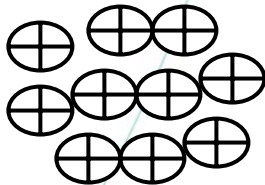
- A large number of **devices** implementing **different functionalities**, with their respective **security policy** (e.g. core backbone, provider edge, customer edge, VLAN switch, etc.).
- Configuration management: the problem of inherent complexity versus **the problem of scale**:
 - TRIPWIRE approach: 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.

High-level model - Logical security attributes

Entities



A router



A set of routers
= a network

Attributes

Basic security attributes (ex no ip-source, no ip finger, etc.)

Complex security attributes (ex ACL consistency and redundancy, etc.)

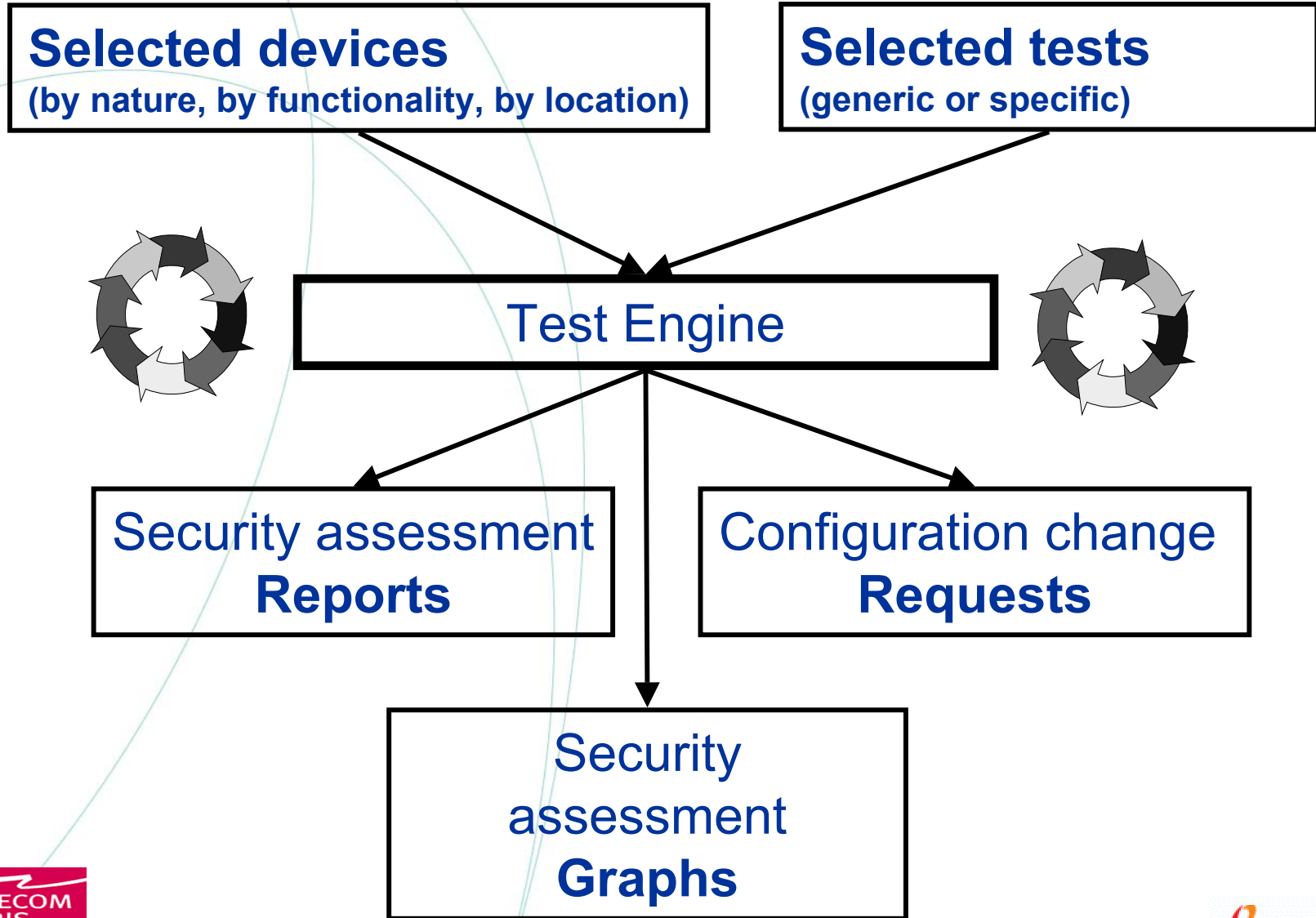
Basic security attributes (ex unique ip address range, etc.)

Complex security attributes (ex network routing topology rules, MPLS/VPN perimeter, etc.)

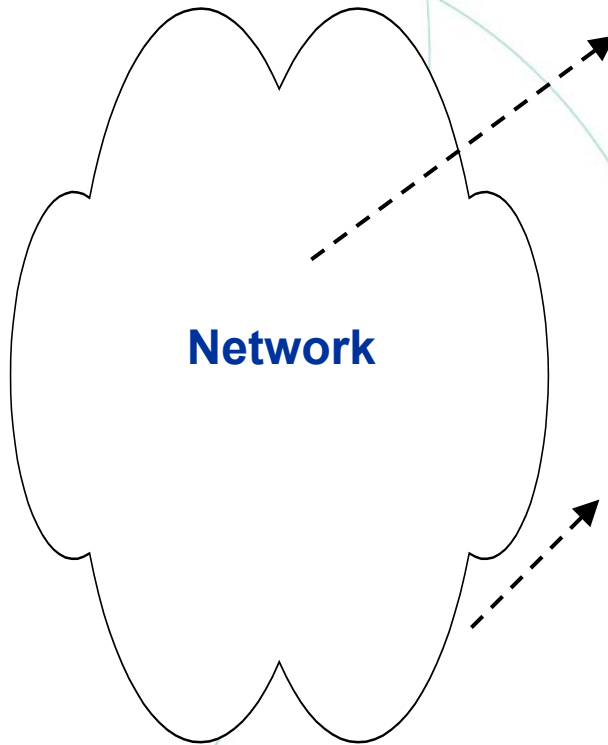
Metrics



High-level model - Reverse engineering



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

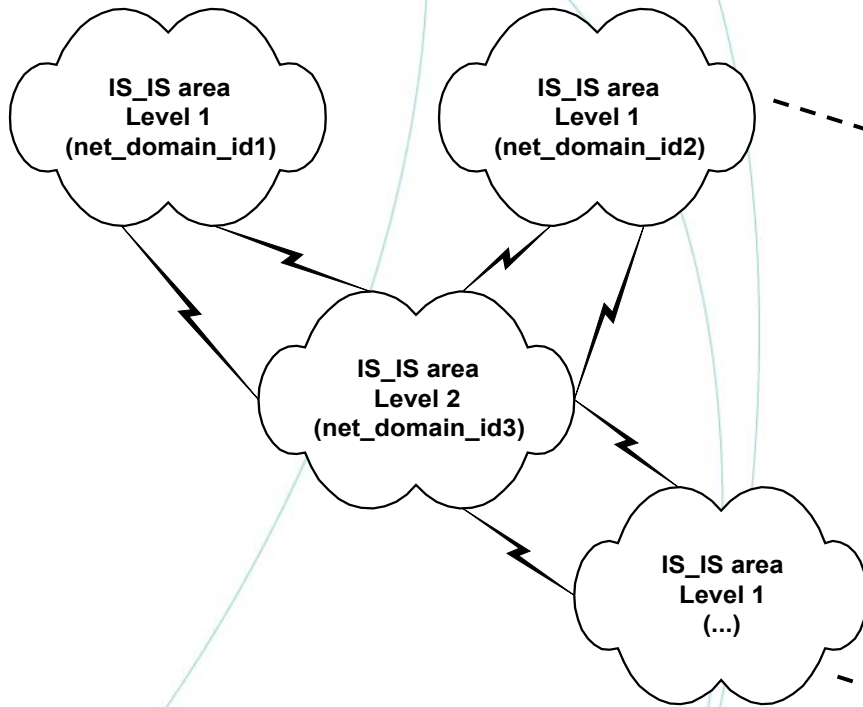
Backbone network routing security policy

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

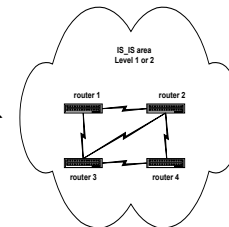
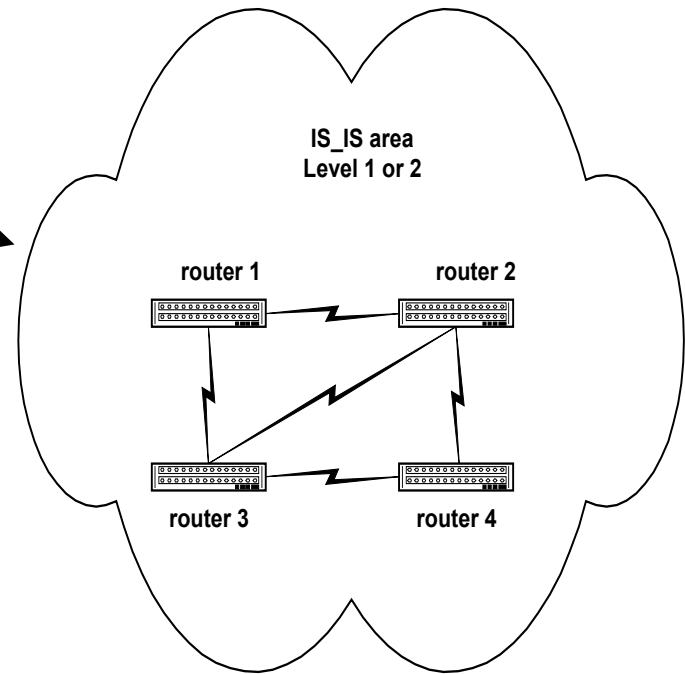
- **EGP (external gateway protocol) / BGPv4**
 - Password security policy
 - Topology security policy
 - Connections security policy

Computation of the IGP routing graph

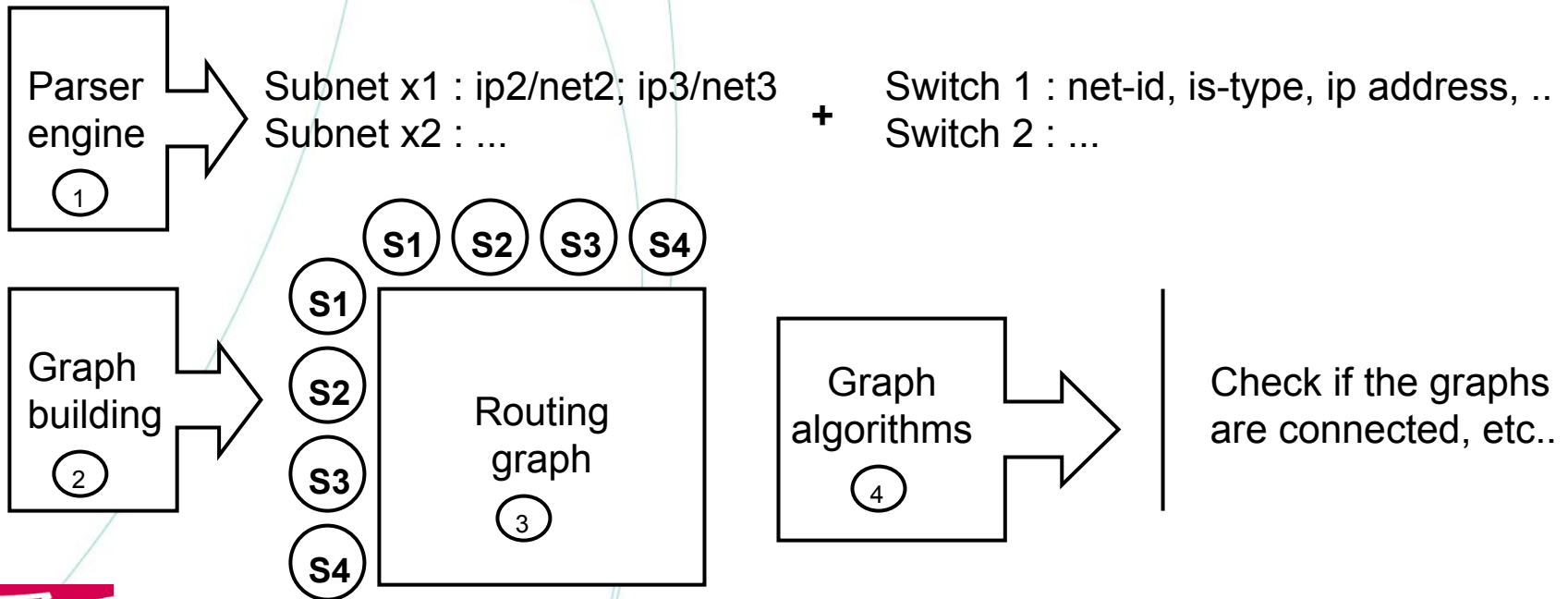
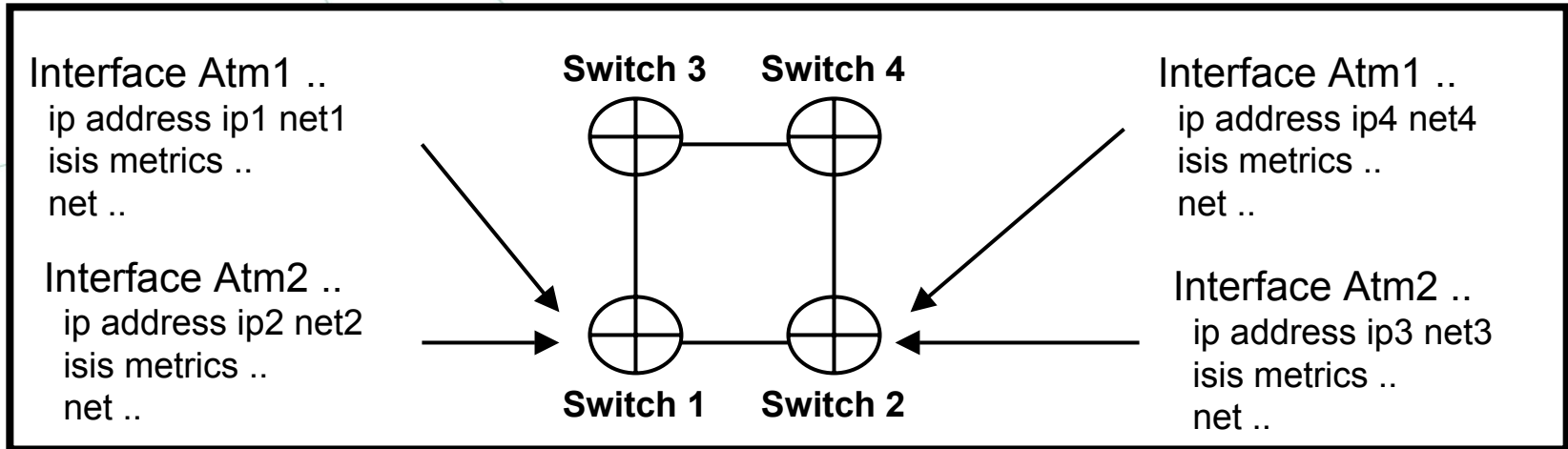
Topology level 1



Topology level 2

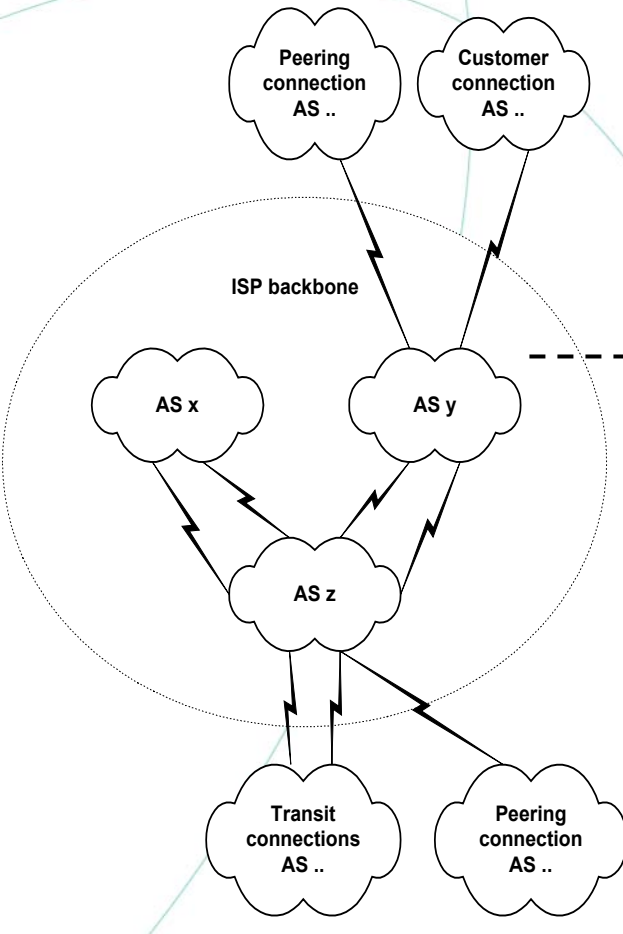


Computation of the IGP routing graph

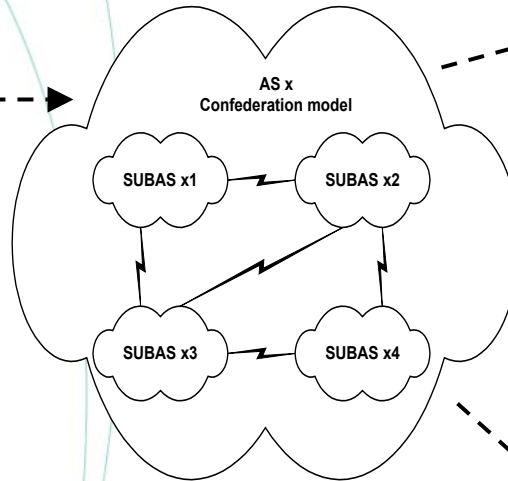


Computation of the EGP routing graph

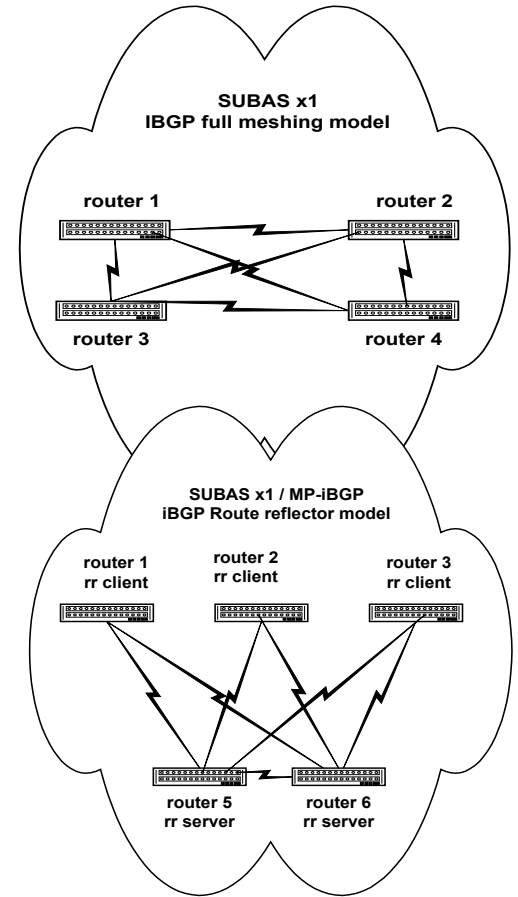
Topology level 1



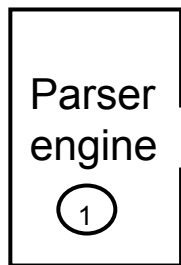
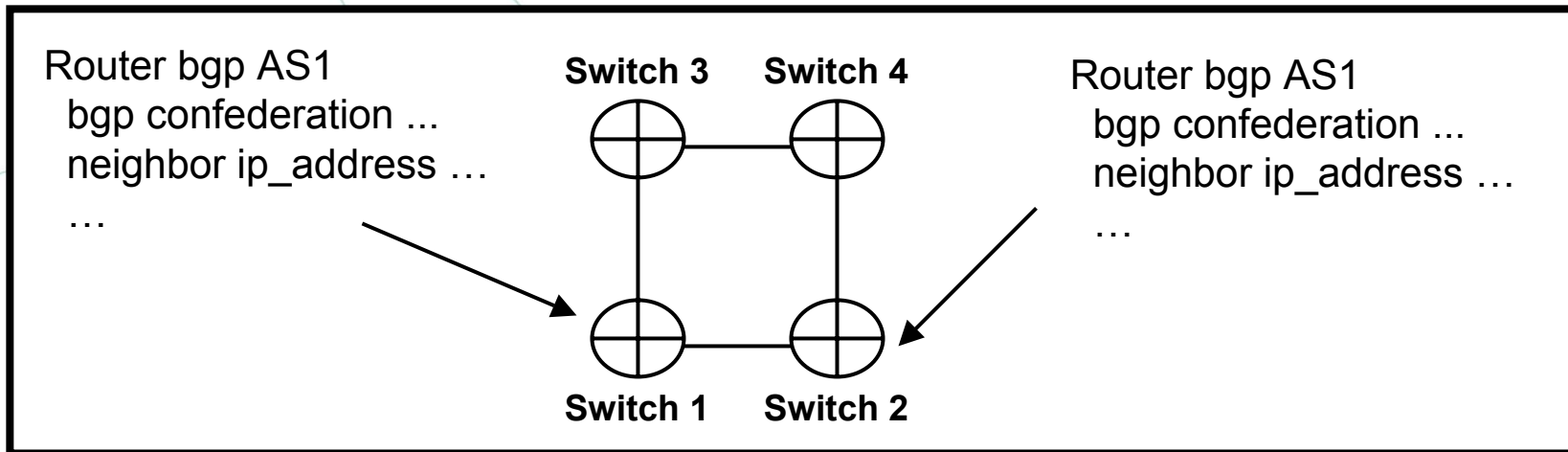
Topology level 2



Topology level 3

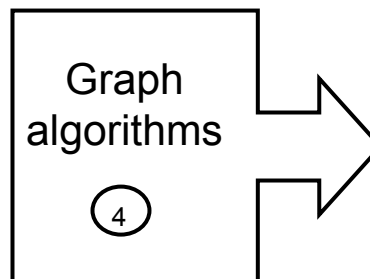
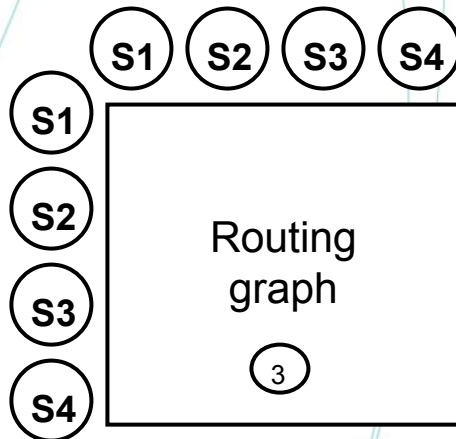
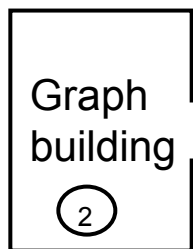


Computation of the EGP routing graph



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

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



Check if the graphs
are connected, etc..

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.

Tool Scope of Usage

The screenshot displays the Config Checker application window. The interface is divided into several sections:

- Left Panel:** Contains status indicators (Status Counter, Status Buttons, Active Profile) and a list of profiles.
- Main Window:** Displays configuration details for 'interface Serial1/1/0.9 point-to-point'. The configuration includes commands like 'ip address', 'ip access-group', 'no ip redirects', and 'no ip proxy-arp'. A callout bubble labeled 'Config Window' points to this area.
- Bottom Panel:** Shows a list of errors and warnings. Each entry includes a status icon (red X or yellow triangle), a severity level, and a comment. A callout bubble labeled 'Check Result Window' points to this area.

Key elements and callouts:

- Status Counter:** Shows 1 error, 129 warnings, 133 errors, 1 info, and 0 status buttons.
- Status Buttons:** A callout bubble states: "Status Buttons are used to hide/show related check results".
- Active Profile:** A callout bubble points to the profile selection area.
- Check Result Window:** A callout bubble points to the error log, which contains messages such as "access-list [redacted] is not defined but applied in line: 3117 (ip access-group [redacted])".

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*)

Questions ?

cedric.llorens@equant.com

denis.valois@equant.com

yannick.leteignier@equant.com

alexandre.gibouin@equant.com