RIPE 87
Rome, Italy
27 Nov - 1 Dec 2023

ROSE-T: Making MANRS Compliance Simple (And Automatic!)

Mariano Scazzariello [*], Antonio Prado [†], Tommaso Caiazzi [‡],

[*] KTH Royal Institute of Technology, Sweden
[†] "G. D'Annunzio" University, Italy [‡] Roma Tre University, Italy

Why is Routing Security Crucial Nowadays?

Cyber Threats

Business Continuity

Sensitive Data

Why is Routing Security Crucial Nowadays?

Cyber Threats

Business Continuity

Sensitive Data

MANRS

MANRS Guidelines For Network Operators

Coordination

Network operators maintain globally accessible up-to-date contact information

Global Information

Network operators must publicly document their routing policies, ASNs and prefixes

Anti-Spoofing

Prevent packets with spoofed source IP address from entering or leaving the network

Filtering

Prevent propagation of incorrect routing information

MANRS Guidelines For Network Operators

Coordination

Network operators maintain globally accessible up-to-date contact information

Global Validation

Network operators must publicly document their routing policies, ASNs and prefixes

How Can a Network Operator Ensure the MANRS Compliance?

Anti-Spoofing

Prevent packets with spoofed source IP address from entering or leaving the network

Filtering

Prevent propagation of incorrect routing information

How Can a Network Operator Ensure the MANRS Compliance?

Coordination **Global Validation** **Anti-Spoofing** **Filtering**

⚠ No tool to automatically verify MANRS compliance!

Operators have to check their configurations and routing policies **manually** or with **minimal aid**

⬇

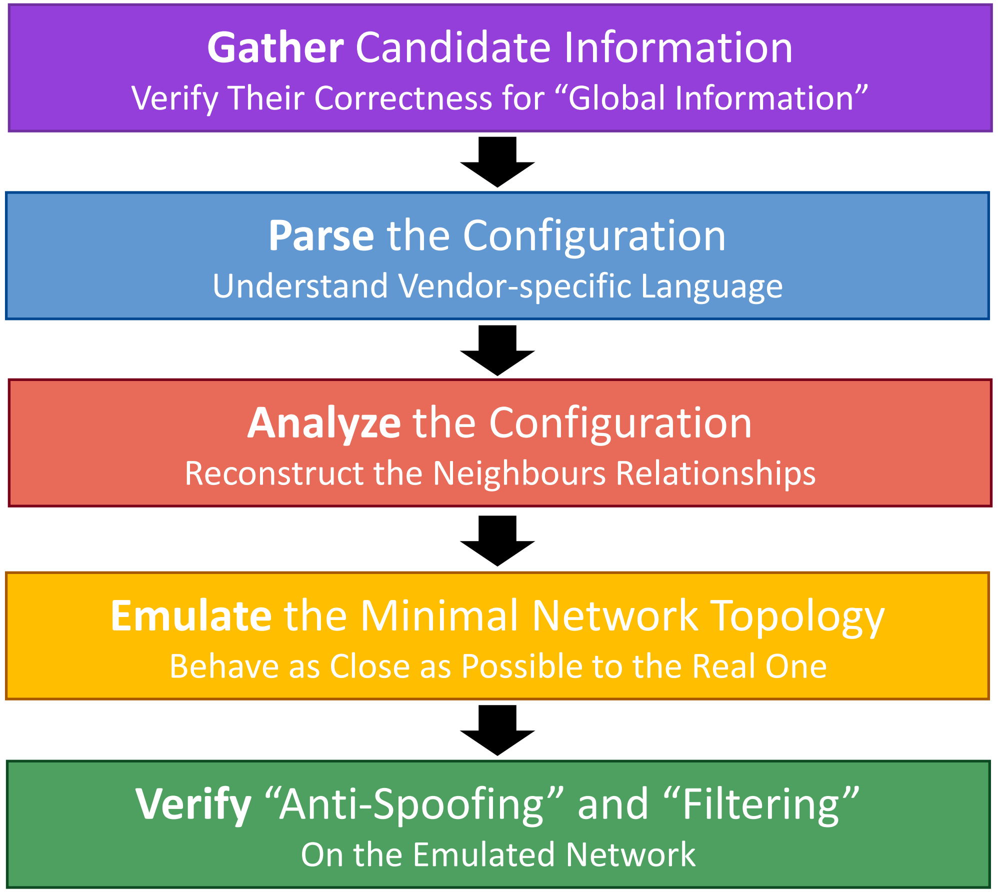
Limited **reproducibility** of the process

⬇

Not an easy task!

ROSE-T: ROuting SEcurity Tool

- The first **open-source** tool to automatically verify MANRS compliance
- **Trust No One** approach
  - Run ROSE-T locally to perform the self-assessment of the configuration



Gather Candidate Information
Verify Their Correctness for “Global Information”

Parse the Configuration
Understand Vendor-specific Language

Analyze the Configuration
Reconstruct the Neighbours Relationships

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network

ROSE-T – Step-by-Step

Gather

Parse

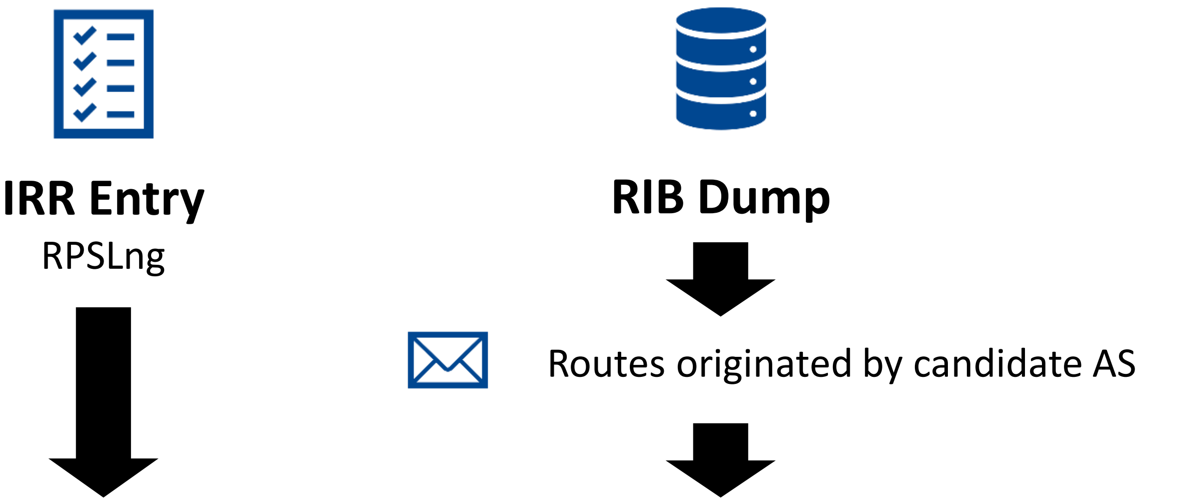
Analyze

Emulate

Verify

ROSE-T – Step-by-Step

Gather Candidate Information
Verify Their Correctness for “Global Information”



IRR Entry
RPSLng

RIB Dump

Routes originated by candidate AS

✓ Verify that the networks announced to transits are in the IRR Entry

✓ Verify that the networks in the IRR Entry are announced to transits

Parse

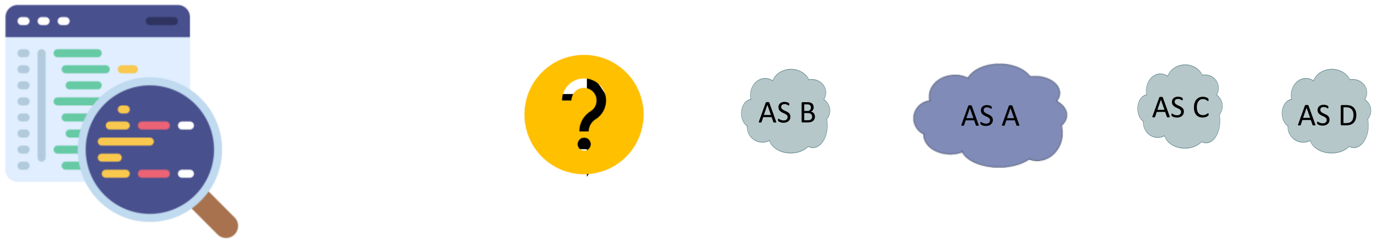
Analyze

Emulate

Verify

ROSE-T – Step-by-Step

Parse the Configuration
Understand Vendor-specific Language



Vendor-specific Configuration

Agnostic Format

Gather

Analyze

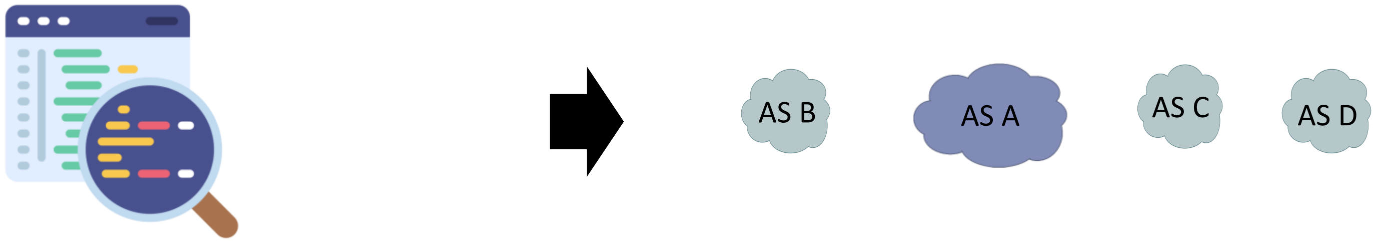
Emulate

Verify

Exploit what Batfish does best: **parsing vendor configurations**

ROSE-T – Step-by-Step

Parse the Configuration
Understand Vendor-specific Language



Vendor-specific Configuration

Agnostic Format

Exploit what Batfish does best: **parsing vendor configurations**

Take Batfish's output as a foundation

Enrich it with missing information

Gather

Analyze

Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships

Agnostic Format

Gather

Parse

Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships

AS B
AS A
AS C
AS D

Agnostic Format

IRR Entry

RPSLng

? What are their relationships?

Gather

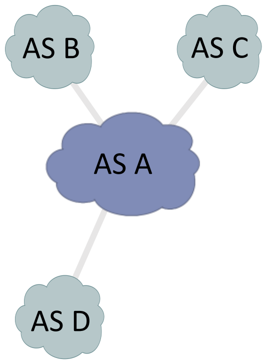
Parse

Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration
Reconstruct the Neighbours Relationships



Intermediate Representation

←

IRR Entry
RPSLng

Gather

Parse

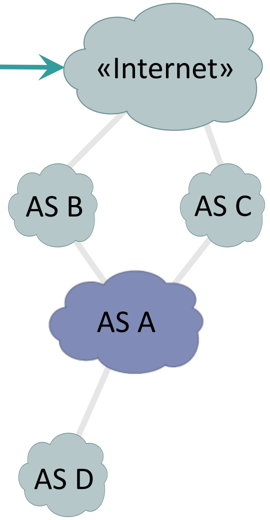
Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration
Reconstruct the Neighbours Relationships

Dummy OTT connected to all providers



Intermediate Representation

IRR Entry
RPSLng

Gather

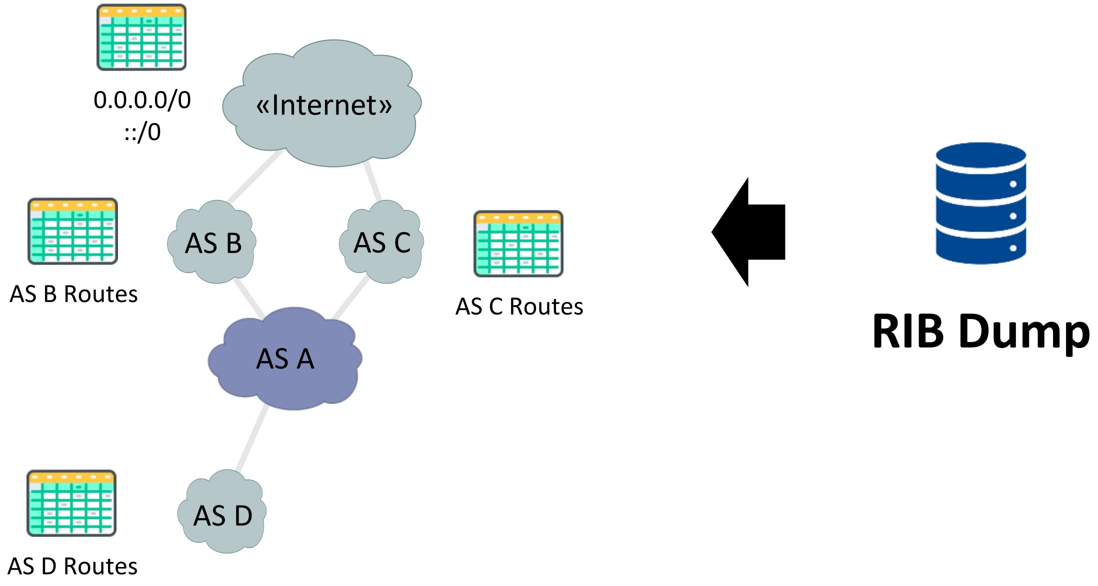
Parse

Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration
Reconstruct the Neighbours Relationships



Intermediate Representation

Gather

Parse

Emulate

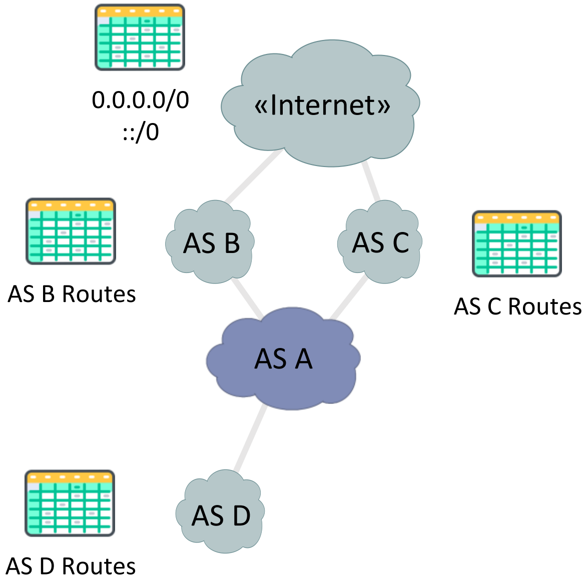
Verify

✓ ROSE-T also supports multi-hop peerings!

ROSE-T – Step-by-Step

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Intermediate Representation

Gather

Parse

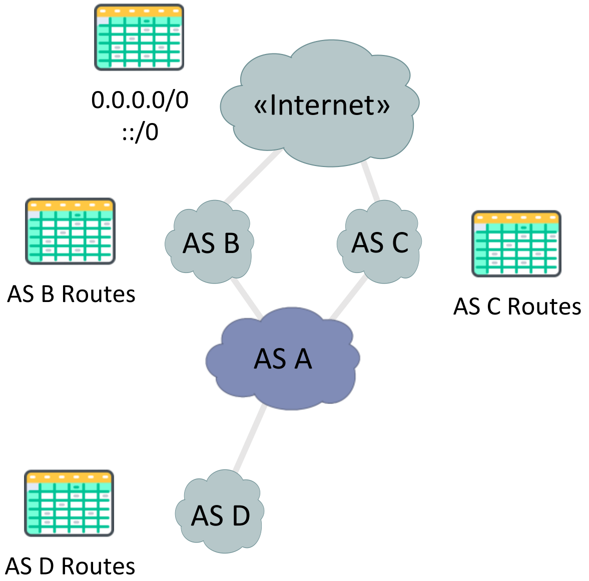
Analyze

Verify

ROSE-T – Step-by-Step

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Intermediate Representation

Kathará

Gather

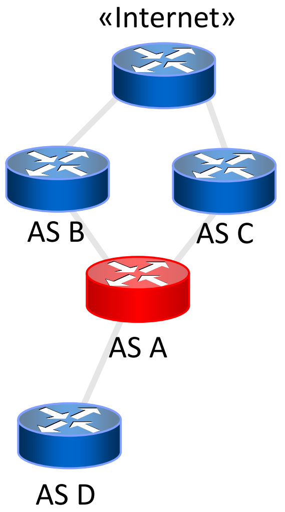
Parse

Analyze

Verify

ROSE-T – Step-by-Step

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Runnable Network Scenario

← Kathará

Gather

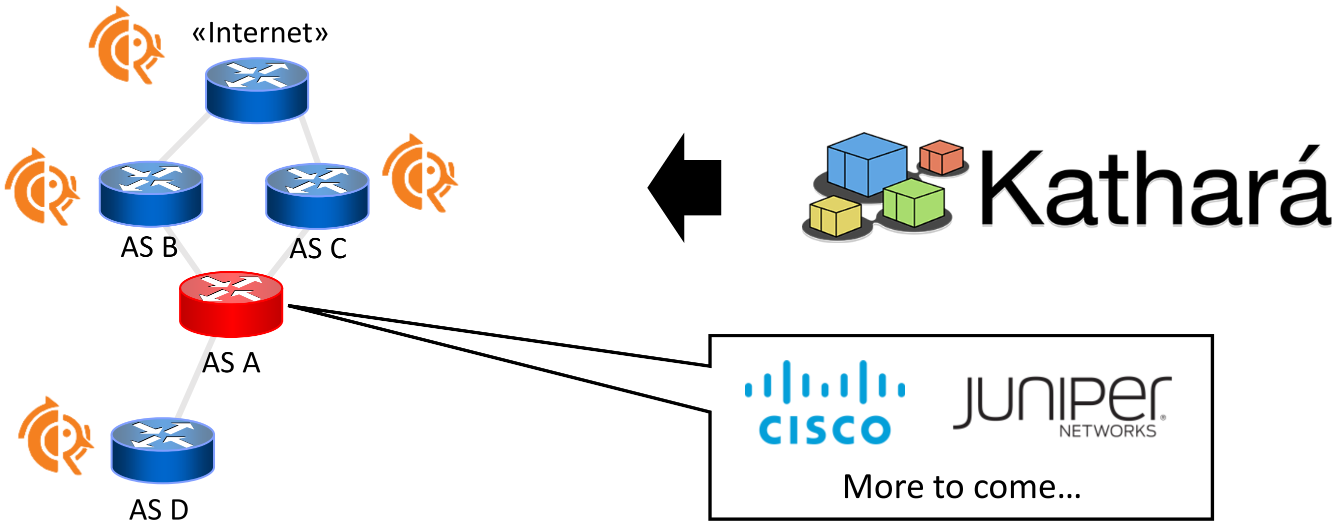
Parse

Analyze

Verify

ROSE-T – Step-by-Step

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Runnable Network Scenario

Vendor Container

Gather

Parse

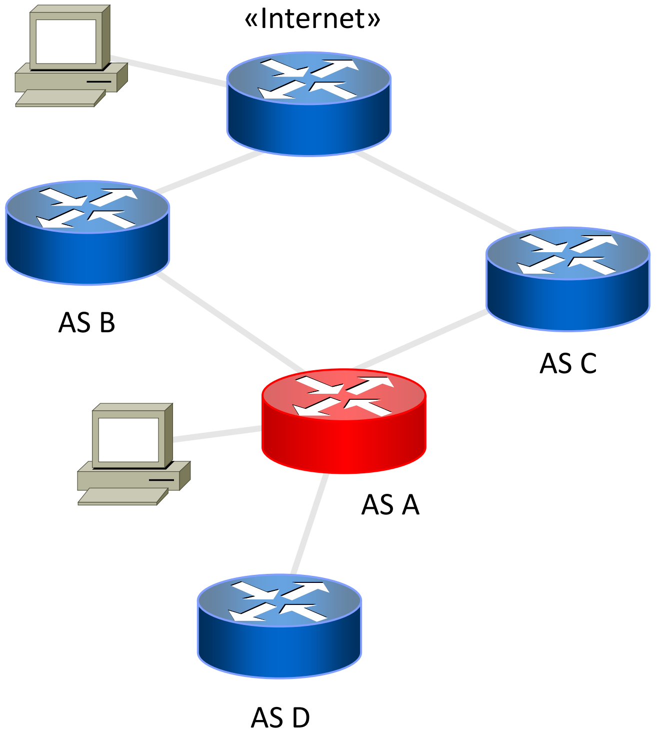
Analyze

Verify

✓ ROSE-T can easily be extended to support other vendors

ROSE-T – Step-by-Step

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Gather

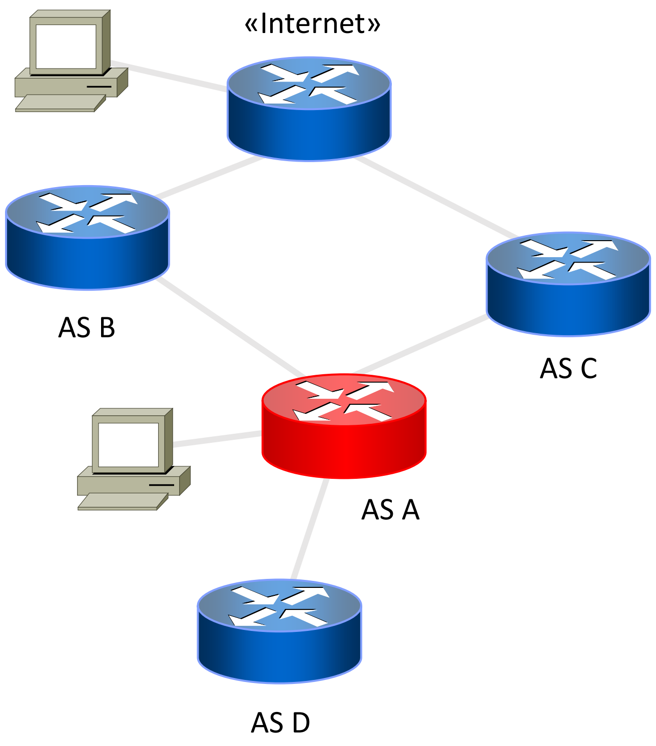
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

Gather

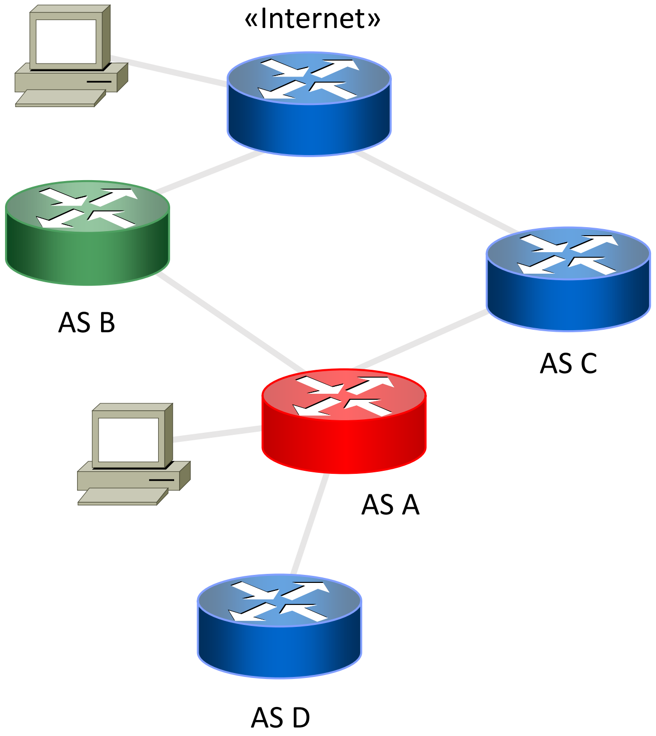
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

Gather

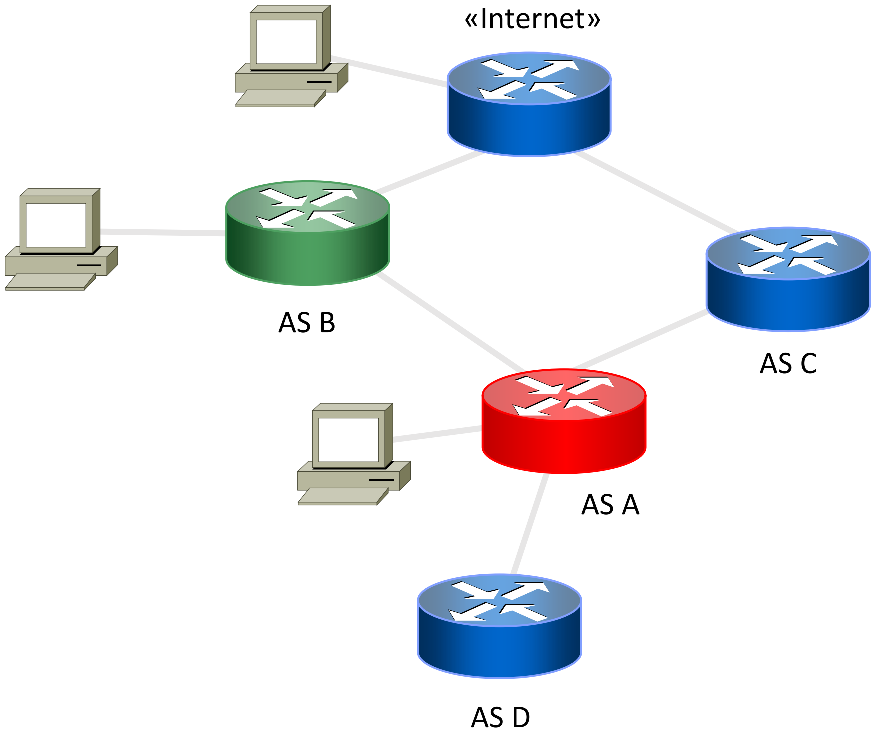
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client

Gather

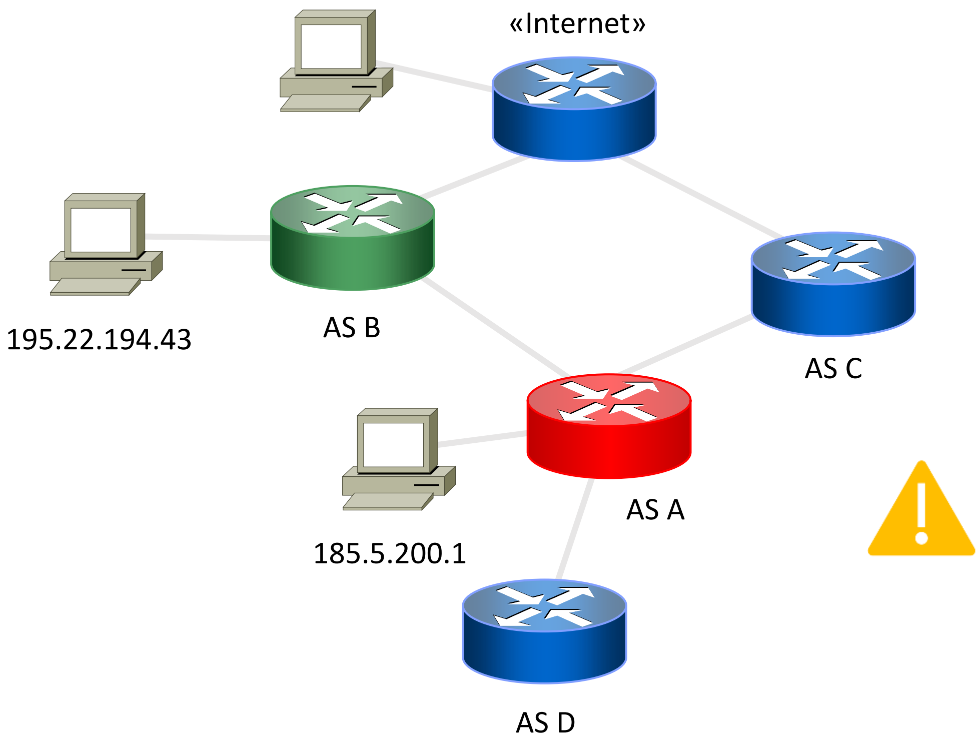
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client

⚠ Carefully choose subnets that are correctly announced and reachable

Gather

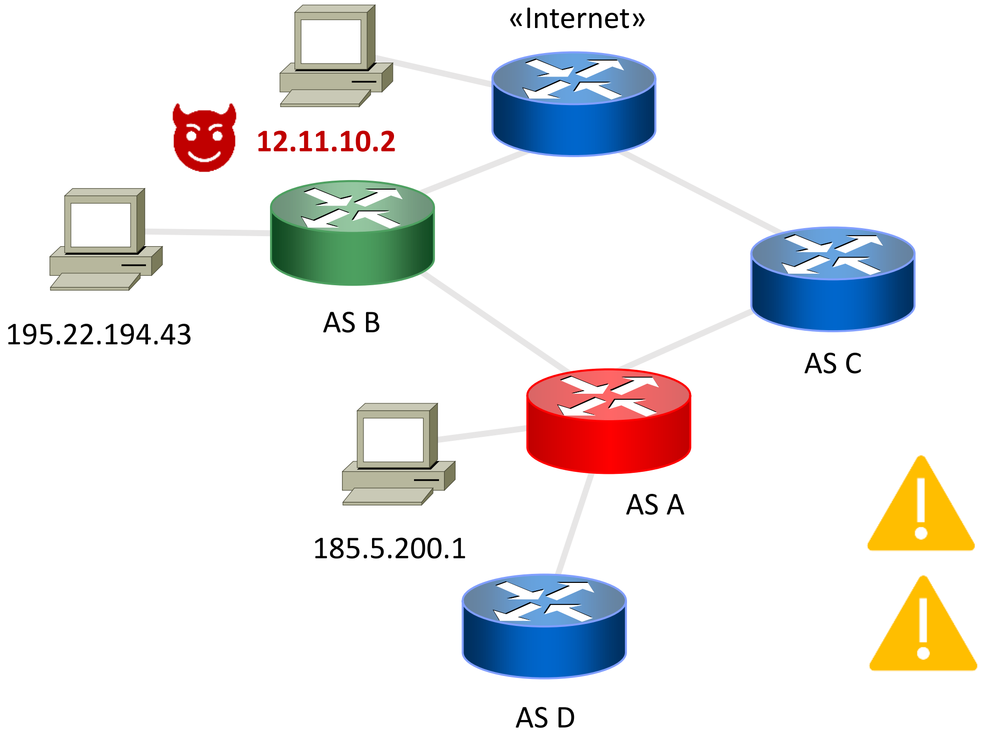
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client

⚠ Carefully choose subnets that are correctly announced and reachable

⚠ Select a non-overlapping network for the "Internet" host

Gather

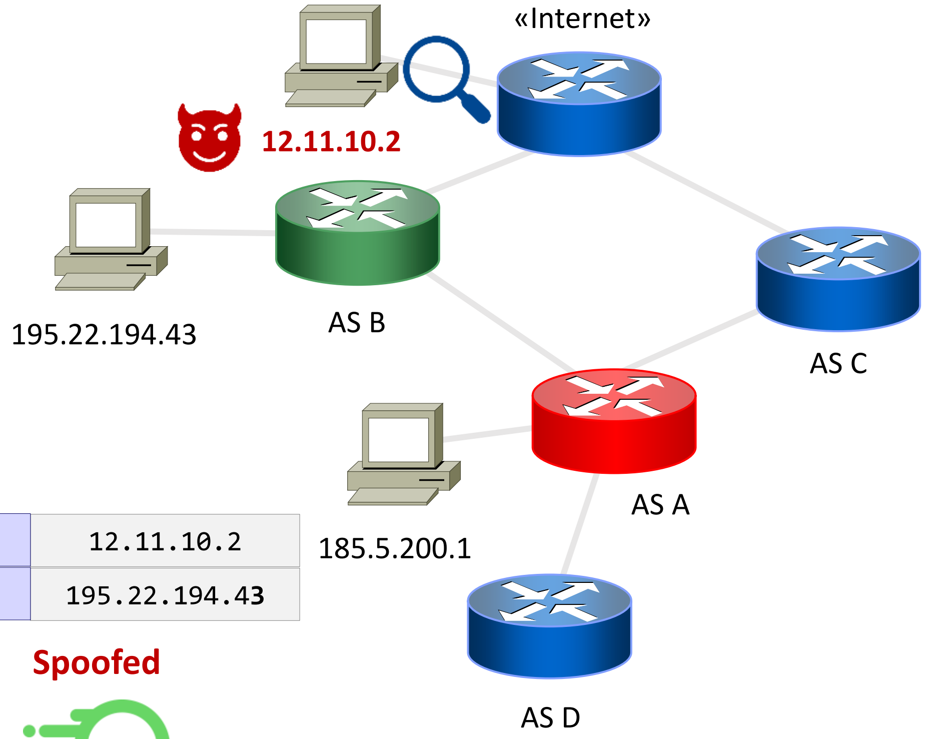
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

scapy

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

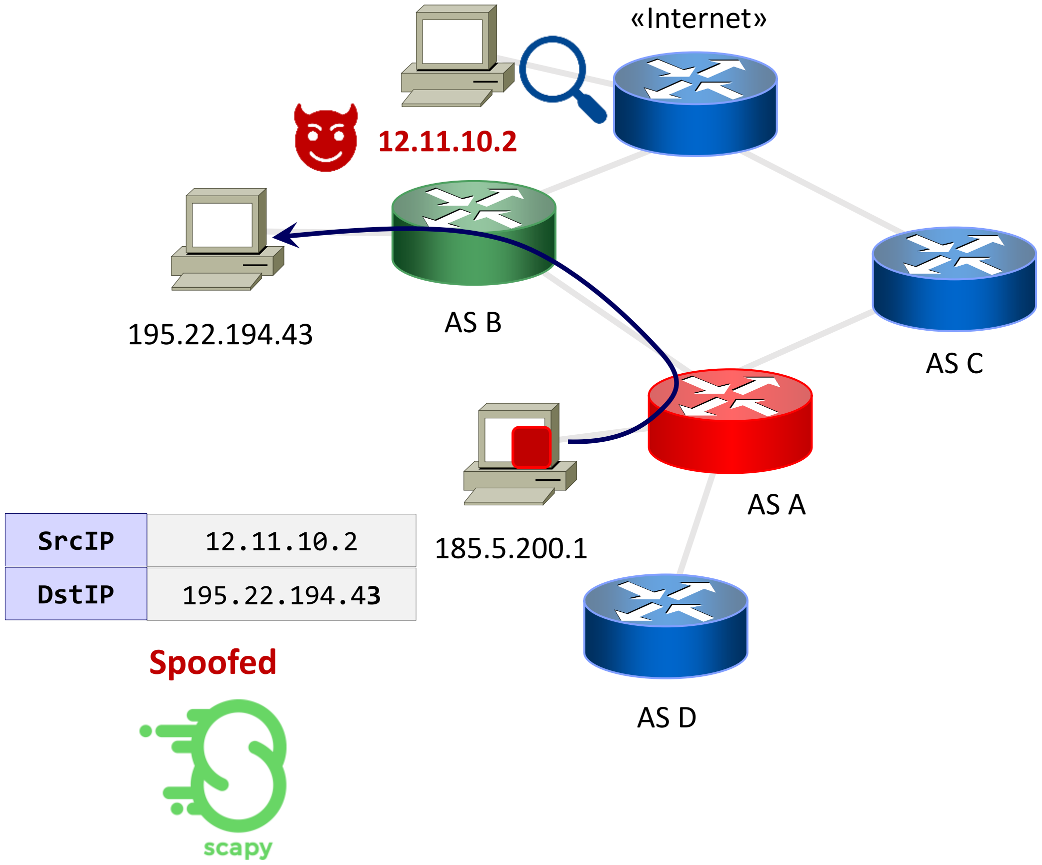
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

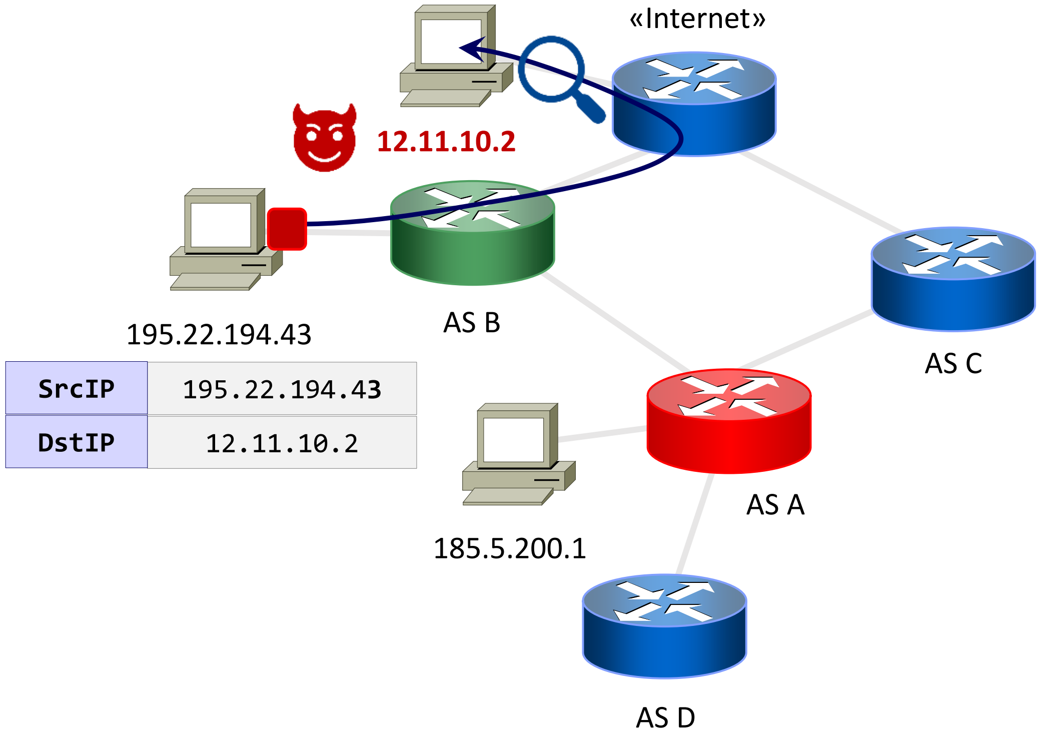
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



SrcIP	195.22.194.43
DstIP	12.11.10.2

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

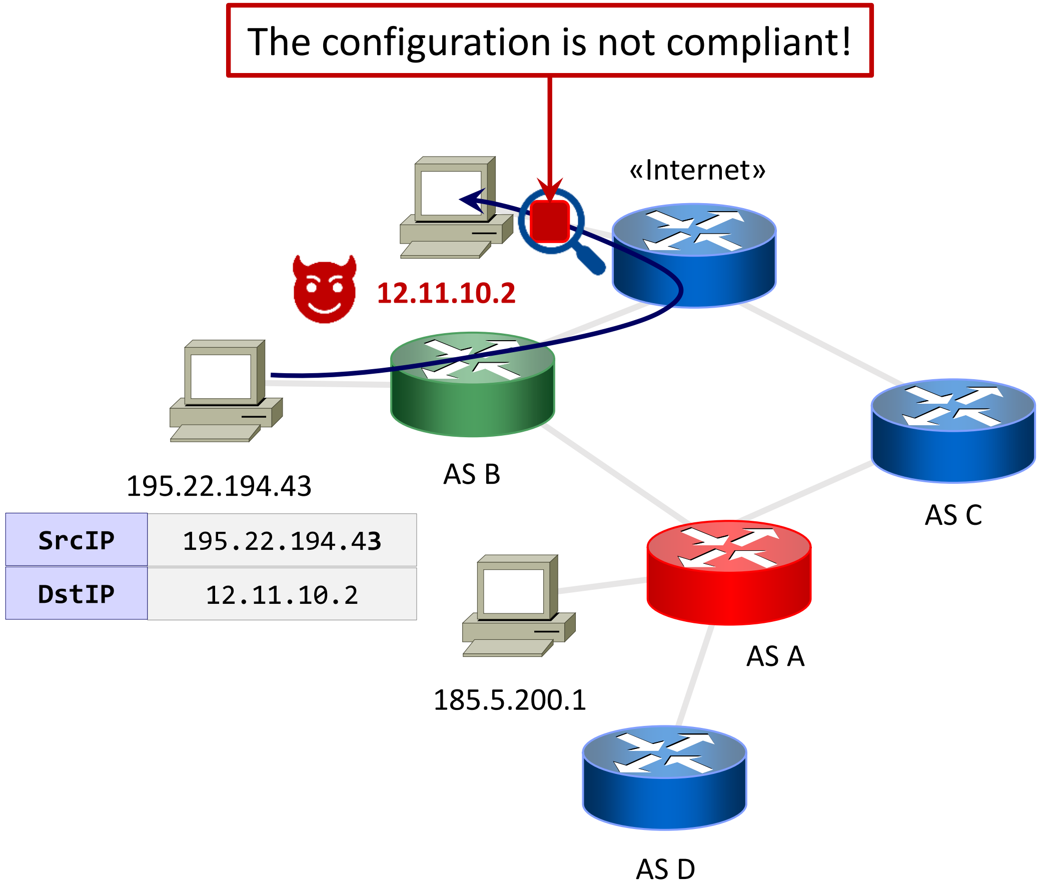
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



The configuration is not compliant!

SrcIP	195.22.194.43
DstIP	12.11.10.2

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

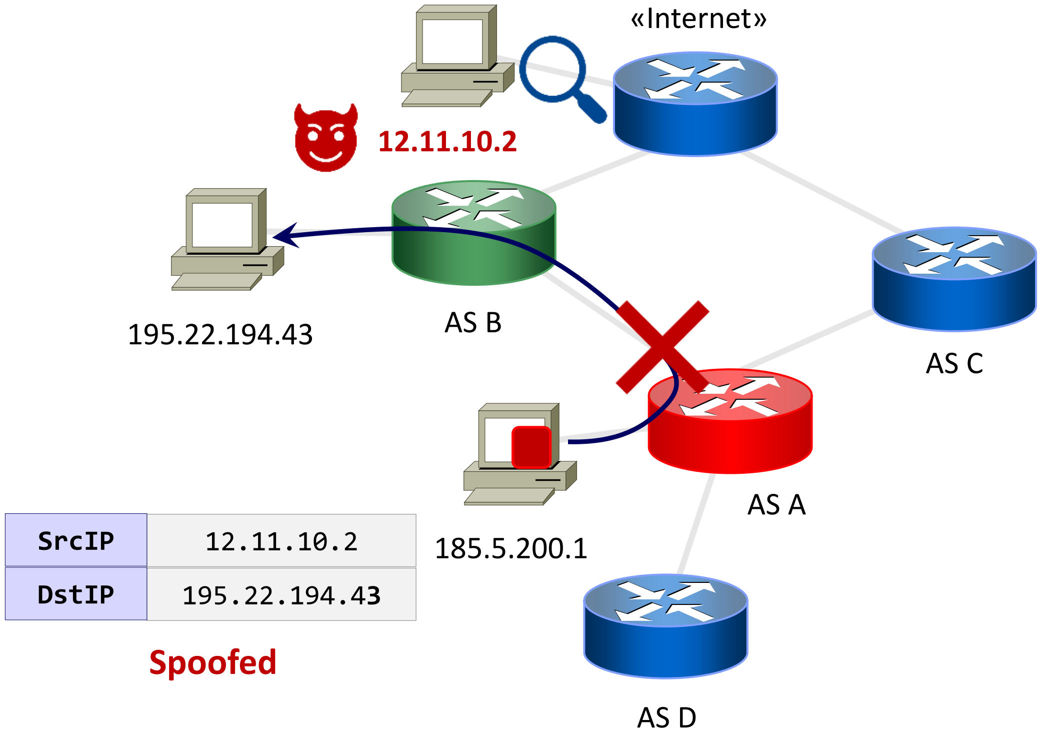
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

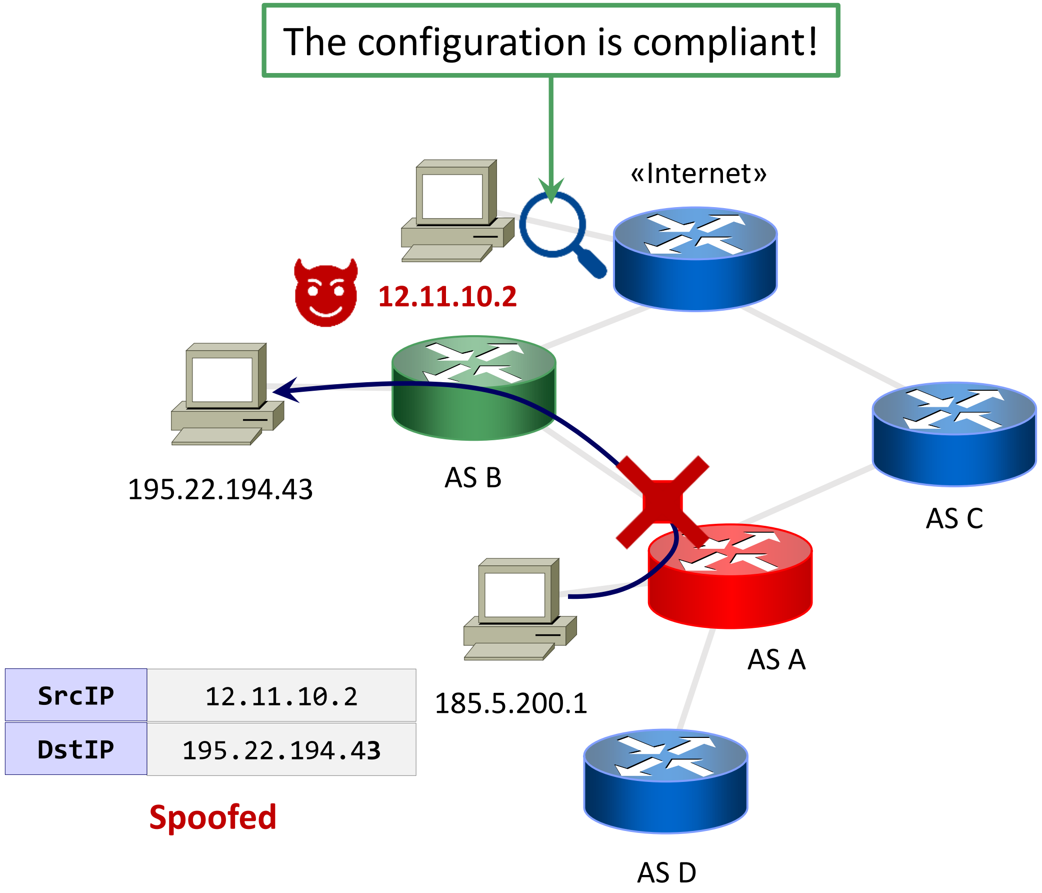
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

Analyze

Emulate

Conclusions

The **ROSE-T** tool:

- Implements the **first tool** to **automatically** verify MANRS compliance
- Allows network operators to test their configurations without relying on **manual and error-prone** procedures
- **Reduces the time** for MANRS adoption that would lead to a **more secure** global routing infrastructure

Future Work

- Extend verification to multiple routers

- Currently, ROSE-T implements the verification of Network Operators Actions
  - Expand the support to IXPs and CDNs Verification

- ROSE-T aims to verify networks beyond MANRS…
  - Verify RPKI deployments
  - Additional features (*e.g.,* ASPA validation)

- Release a verifiable code to certify MANRS compliance

Contacts

Mariano Scazzariello

KTH Royal Institute of Technology

Antonio Prado

“G. D’Annunzio” University

Tommaso Caiazzi

Roma Tre University

Contribute!