RoSe-T, una verifica automatica delle azioni MANRS per gli operatori di rete

Antonio Prado

Il problema

- Il BGP è il protocollo di *routing* interdominio di Internet
- È vulnerabile a errori e abusi (*hijack*, *leakage*, instabilità)
- La sicurezza del *routing* è ancora basata sulla fiducia

I protocolli di routing

Interior Gateway Protocol (IGP)

- **RIP** (Routing Information Protocol)
- **OSPF** (Open Shortest Path First)
- **EIGRP** (Enhanced Interior Gateway Routing Protocol)

Exterior Gateway Protocol (EGP)

- **BGP** (Border Gateway Protocol)

iBGP
dentro un AS

eBGP
tra AS diversi

Cos'è il Sistema Autonomo

Un Sistema Autonomo (*Autonomous System*, AS) è costituito da un gruppo di uno o più prefissi IP gestito da un operatore di rete che ha una politica di instradamento UNICA e CHIARAMENTE DEFINITA. [RFC 1930]

Obiettivo della ricerca

- Rafforzare la sicurezza del BGP
- Automatizzare la verifica delle azioni MANRS
- Supportare operatori di rete nella conformità MANRS

Le azioni MANRS

1. Impedire la propagazione di instradamenti errati
2. Bloccare traffico con IP falsificati
3. Collaborare con altri operatori
4. Documentare pubblicamente le *policy* di *routing*

Soluzioni esistenti e limiti

- Strumenti di monitoraggio: non verificano configurazioni
- Verifica formale: complessa e poco scalabile
- Mancano strumenti automatici per operatori di piccole-medie dimensioni

Strumenti per verifica configurazioni BGP

Bagpipe
FVR
C-BGP

Batfish
Minesweeper
Plankton

Pybatfish

How do I get started?

If you haven't already installed Batfish, follow the instructions listed in the batfish github repository to do so.

Install Pybatfish

We highly recommend that you install Pybatfish in a Python 3 virtual environment. Details on how to set one up can be found here. Once your virtual environment is setup and activated, upgrade pip and then install pybatfish.

```
python3 -m pip install --upgrade pip
python3 -m pip install --upgrade pybatfish
```

Now, you are ready to evaluate your own network with Batfish. We encourage you to use Jupyter notebooks as your starting point, but you can use other methods that you are a comfortable with, e.g., an IDE like PyCharm or an interactive Python shell. If you choose to use Jupyter notebooks as your starting point, you need to install Jupyter in your virtual environment. Jupyter documentation can be found here - but the commands below will get you going.

```
python3 -m pip install jupyter
jupyter notebook
```

Our notebooks provide a quick start guide for different use cases. Beyond that, the complete documentation is available on readthedocs.

Pybatfish documentation

Complete documentation of pybatfish APIs is here.

Analisi dei dati

Fonti dei dati

Storici: MRT file (*route collection raw data*)

Tempo reale: RIS *live*

RIS live


```
// Received at 19:22:23 (4.27 second delay)
{
    "timestamp": 1654968139.28,
    "peer": "37.49.237.228",
    "peer_asn": "39533",
    "id": "21-29086-17615121",
    "host": "rrc21",
    "type": "UPDATE",
    "path": [39533, 6762, 17557, 23674],
    "community": [[0, 39533], [6762, 1], [6762, 30], [6762, 40], [6762, 13930],
[39533, 49666], [65205, 6762]],
    "origin": "igp",
    "announcements": [
        {
            "next_hop": "37.49.237.228",
            "prefixes": [
                "206.84.140.0/24"
            ]
        }
    ]
}
```

```
// Received at 19:22:23 (4.28 second delay)
{
    "timestamp": 1654968139.27,
    "peer": "37.49.237.228",
    "peer_asn": "39533",
    "id": "21-29086-17615097",
    "host": "rrc21",
    "type": "UPDATE",
    "path": [39533, 6939, 37662, 327708, 327708, 327708, 36926, 37075, 37020],
    "community": [[0, 39533], [39533, 49666], [64512, 11], [64512, 21], [65205,
61968]],
    "origin": "igp",
    "announcements": [
        {
```

Analisi dei dati

Strumenti per analisi

bgpdump

bgpstream

pbgpsuite

bgpstream su RIS live

```
U|A|1654969577.050000|ris-live|rrc01|||57695|2001:7f8:4::e15f:1|2804:658c:12::/48|2
001:7f8:4::e15f:1|57695 60068 174 6762 264409 267942 269499|269499|174:21100 174:22
012 57695:13000 60068:203 60068:2006 60068:2016 60068:7046||
U|A|1654969576.110000|ris-live|rrc12|||47692|80.81.194.100|130.137.118.0/24|80.81.1
94.100|47692 6453 6453 6453 6453 6453 1299 16509 8987|8987|47692:30000 47692:30120|
|
U|A|1654969577.110000|ris-live|rrc12|||47692|80.81.194.100|179.127.68.0/23|80.81.19
4.100|47692 3356 2914 13786 28263 28287|28287|2914:410 2914:1009 2914:2000 2914:300
0 3356:3 3356:22 3356:86 3356:575 3356:666 3356:901 3356:2013 13786:110 13786:4602
13786:64011 28263:21871 28263:21891 28263:31721 28263:31811 28263:51701 28263:51711
 28263:51721 28263:51731 28263:61800 32934:10012 47692:30000 47692:30120 64055:6500
3 64355:65001||
U|A|1654969577.110000|ris-live|rrc12|||49697|80.81.195.241|130.137.79.0/24|80.81.19
5.241|49697 41047 50629 174 16509|16509|174:21001 174:22013 41047:4006 49697:2500 5
0629:180 50629:304 50629:1000 50629:10001 50629:10102 50629:10205||
U|A|1654969577.110000|ris-live|rrc12|||47692|2001:7f8::ba4c:0:1|2404:2280:147::/48|
2001:7f8::ba4c:0:1|47692 3356 6453 7713 21859 21859 21859 21859 24429|24429|3
356:3 3356:22 3356:86 3356:575 3356:601 3356:666 3356:901 3356:2013 47692:30001 476
92:30121||
U|A|1654969575.960000|ris-live|rrc25|||47787|193.107.13.3|130.137.118.0/24|193.107.
13.3|47787 1299 16509 8987|8987|1299:35000 47787:1010 47787:3120 47787:10000 47787:
10030||
U|A|1654969575.960000|ris-live|rrc25|||3214|2a03:d9c0:c0de:c0de::1|2a02:2698:a004::
/46|2a03:d9c0:c0de:c0de::1|3214 50629 12389 9049 49874|49874|3214:3601 50629:200 50
629:403 50629:1000 50629:10001 50629:10105 50629:10209||
U|A|1654969575.960000|ris-live|rrc25|||3214|185.255.53.202|189.124.80.0/21|185.255.
53.202|3214 3356 1299 13786 28263 28287|28287|3214:3301 3356:2 3356:86 3356:501 335
6:666 3356:901 3356:2065||
U|A|1654969575.960000|ris-live|rrc25|||3214|185.255.53.202|189.124.88.0/21|185.255.
53.202|3214 3356 1299 13786 28263 28287|28287|3214:3301 3356:2 3356:86 3356:501 335
6:666 3356:901 3356:2065||
U|S|1654969576.040000|ris-live|rrc12|||9031|80.81.195.204||||||IDLE
U|A|1654969576.050000|ris-live|rrc12|||35598|80.81.193.247|130.137.118.0/24|80.81.1
93.247|35598 1299 16509 8987|8987|1299:35000 35598:200 35598:205||
U|A|1654969577.050000|ris-live|rrc12|||35598|80.81.193.247|130.137.108.0/24|80.81.1
93.247|35598 3356 8732 6762 6453 16509|16509|6762:30 6762:13370 8732:1010 8732:1011
 35598:200 35598:204||
U|A|1654969575.970000|ris-live|rrc01|||36924|5.57.81.76|67.211.53.0/24|5.57.81.76|3
6924 35280 6453 3356 26405|26405|6453:86 6453:1000 6453:1100 6453:1103 35280:20 352
80:1020 35280:2040 35280:3080 35280:10000 35280:10020||
U|A|1654969575.980000|ris-live|rrc01|||62167|2001:7f8:4::f2d7:1|2a0e:97c6:83::/48|2
001:7f8:4::f2d7:1|62167 3356 2914 20473|20473|||
U|A|1654969575.980000|ris-live|rrc01|||62167|2001:7f8:4::f2d7:1|2a10:cc42:173c::/48
|2001:7f8:4::f2d7:1|62167 3356 2914 20473|20473|||
```

Astrazione e formalizzazione

Clausole di Horn e Prolog

Studio delle relazioni tra i sistemi autonomi per la realizzazione di uno strumento automatico in grado di verificare se quanto dichiarato dagli operatori trovi riscontro su Internet

Paradigma per la verifica

Mutually Agreed Norms for Routing Security

Is a global initiative that helps reduce the most common routing threats

MANRS

RoSe-T, uno strumento che

Riceve la configurazione di un *border router* (BGP speaking)

Analizza la configurazione così da comprendere: *vendor*, *transit*, *peer*, *customer*

Confronta i dati pubblicati sugli IRR con quanto presente nella configurazione

Restituisce segnali di OK, KO, WARNING, INFO

Costruisce automaticamente un ambiente emulato

Esegue molteplici test per provare la conformità alle azioni MANRS (anti-spoofing e BGP filtering)

Una riflessione sul metodo

Massima astrazione: prendi una *routing policy* (in RPSLng) e verifica se è conforme alle azioni MANRS

1

Astrazione: prendi una configurazione, leggi le parole, studia la sintassi, comprendi il senso e verifica se è conforme alle azioni MANRS

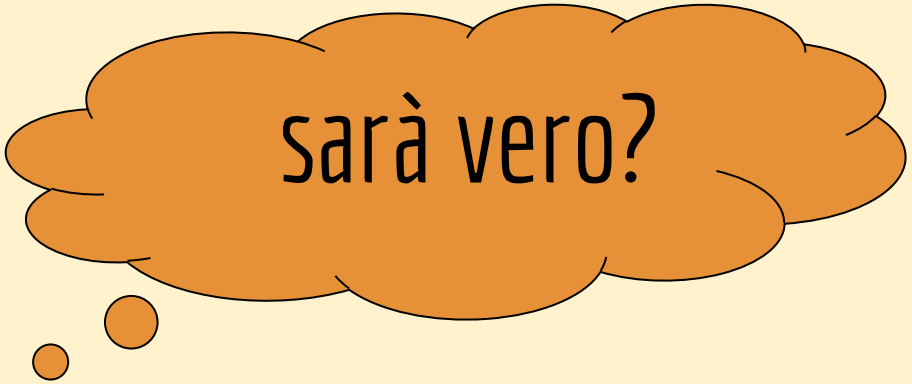
2

Emulazione: prendi una configurazione, applicala a un *router* e verifica se è conforme alle azioni MANRS

3

1 Massima astrazione

```
aut-num:        AS59715
as-name:        SBTAP-AS
org:            ORG-CdSB1-RIPE
mp-import:      afi ipv4.unicast from AS12874 accept any
mp-import:      afi ipv6.unicast from AS12874 accept any
mp-import:      afi ipv4.unicast from AS6762 accept any
mp-import:      afi ipv6.unicast from AS6762 accept any
mp-import:      afi ipv4.unicast from AS112 accept AS112
mp-import:      afi ipv6.unicast from AS112 accept AS112
mp-export:      afi ipv4.unicast to AS12874 announce AS-SBTAP
mp-export:      afi ipv6.unicast to AS12874 announce AS-SBTAP
mp-export:      afi ipv4.unicast to AS6762 announce AS-SBTAP
mp-export:      afi ipv6.unicast to AS6762 announce AS-SBTAP
mp-export:      afi ipv4.unicast to AS112 announce any
mp-export:      afi ipv6.unicast to AS112 announce any
admin-c:        SBT21-RIPE
tech-c:         SBT20-RIPE
tech-c:         AP7729-RIPE
status:         ASSIGNED
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         SBTAP-MNT
created:        2012-10-04T12:53:46Z
last-modified:  2022-10-24T14:18:26Z
source:         RIPE
```



1 Massima astrazione

```
afi ipv4.unicast from AS12874 accept any
afi ipv6.unicast from AS12874 accept any
afi ipv4.unicast from AS6762 accept any
afi ipv6.unicast from AS6762 accept any
afi ipv4.unicast from AS112 accept AS112
afi ipv6.unicast from AS112 accept AS112
afi ipv4.unicast to AS12874 announce AS-SBTAP
afi ipv6.unicast to AS12874 announce AS-SBTAP
afi ipv4.unicast to AS6762 announce AS-SBTAP
afi ipv6.unicast to AS6762 announce AS-SBTAP
afi ipv4.unicast to AS112 announce any
afi ipv6.unicast to AS112 announce any
```

è vero! ma...

```
V*   185.5.200.0/22    194.85.40.15          0          0 3267 1299 12874 59715 i
V*                     193.0.0.56                       0 3333 6762 59715 i
V*                     12.0.1.63                        0 7018 6762 59715 i
V*                     212.66.96.126                    0 20912 12874 59715 i
```

dov'è l'AS112?

2 Astrazione


```
set protocols bgp group NLNOG_V6 type external
set protocols bgp group NLNOG_V6 multihop ttl 30
set protocols bgp group NLNOG_V6 local-address 2a02:cdc5:9715:0:185:5:200:255
set protocols bgp group NLNOG_V6 import DENY_ALL_PREFIX
set protocols bgp group NLNOG_V6 family inet6 unicast
set protocols bgp group NLNOG_V6 export ALLOW_BGP_PREFIX
set protocols bgp group NLNOG_V6 peer-as 199036
set protocols bgp group NLNOG_V6 neighbor 2001:7b8:62b:1:0:d4ff:fe72:7848
```

2 Astrazione

```
INFO - Parsing peerings IPv4 addresses.
INFO - status: ASSIGNED
INFO - .... no task information
INFO - status: TERMINATEDNORMALLY
INFO - .... 2023-04-15 21:20:35.375000+02:00 Begin job.
WARNING - Peering with AS65332 is in reserved range 64000-131071.
WARNING - Peering with AS59715 is a iBGP peering.
WARNING - Peering with AS65332 is in reserved range 64000-131071.
WARNING - Peering with AS59715 is a iBGP peering.
WARNING - Peering with AS59715 is a iBGP peering.
WARNING - Peering with AS64496 is in reserved range 64000-131071.
WARNING - Peering with AS59715 is a iBGP peering.
WARNING - Peering with AS64496 is in reserved range 64000-131071.
INFO - status: ASSIGNED
INFO - .... no task information
INFO - status: TERMINATEDNORMALLY
INFO - .... 2023-04-15 21:20:35.520000+02:00 Begin job.
INFO - Configuration format is 'FLAT_JUNIPER', loading vendor configuration...
INFO - Inferring IPv6 interface addresses.
INFO - Inferring IPv6 routes.
INFO - Inferring IPv6 BGP peerings.
WARNING - Peering with AS65332 is in reserved range 64000-131071.
WARNING - Peering with AS64496 is in reserved range 64000-131071.
```

capisce sessioni BGP

capisce Juniper

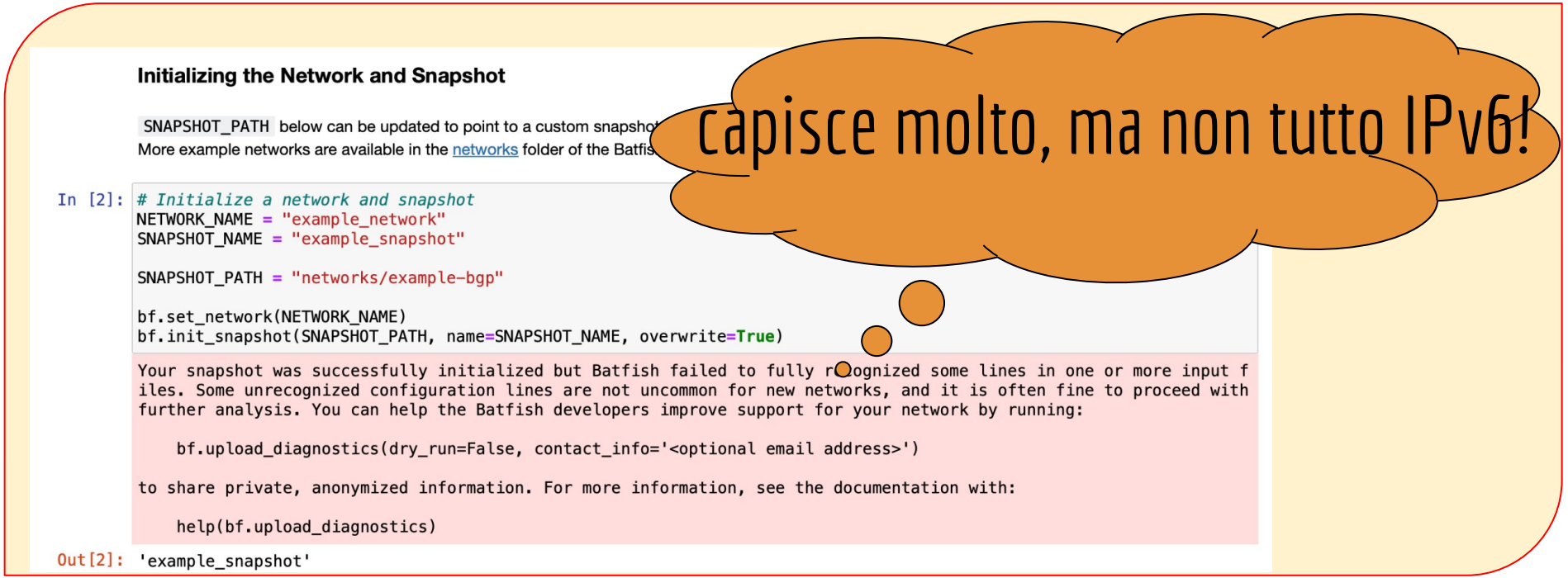
2 Astrazione

```
- Interface 'xe-0/1/0' remapped into 'ge-0/0/1.0'.
- Interface 'xe-0/1/0.0' remapped into 'ge-0/0/1.0'.
- Interface 'xe-0/1/1' remapped into 'ge-0/0/2.0'.
- Interface 'xe-0/1/1.100' remapped into 'ge-0/0/2.100'.
- Interface 'xe-0/1/1.169' remapped into 'ge-0/0/2.169'.
- Interface 'xe-0/1/2' remapped into 'ge-0/0/3.0'.
- Interface 'xe-0/1/2.0' remapped into 'ge-0/0/3.0'.
- Interface 'xe-0/1/3' remapped into 'ge-0/0/4.0'.
- Resulting interfaces are:
-    • lo0 with addresses: []
-    • lo0.0 with addresses: []
-    • ge-0/0/1.0 with addresses: []
-    • ge-0/0/1.0 with addresses: [IPv4Interface('185.5.200.255/2
54/64'), IPv6Interface('2a02:cdc6:3074::/64'), IPv6Interface('2a0
-    • ge-0/0/2.0 with addresses: []
-    • ge-0/0/2.100 with addresses: [IPv4Interface('185.5.202.2/24'),
-    • ge-0/0/2.169 with addresses: [IPv4Interface('169.254.63.74/24'
-    • ge-0/0/3.0 with addresses: []
-    • ge-0/0/3.0 with addresses: [IPv4Interface('89.221.32.157/31'),
-    • ge-0/0/4.0 with addresses: []
```

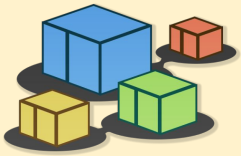
capisce le interfacce

e le mappa con IP

2 Astrazione



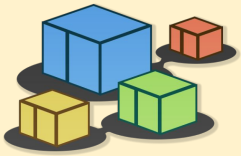
3 Emulazione



Kathará

Kathará is an open source container-based network emulation system for showing interactive demos/lessons, testing production networks in a sandbox environment, or developing new network protocols

3 Emulazione



Chiediamo a kathara di prendere tutto ciò che viene digerito dal *parser* e di creare uno scenario, cioè una piccola Internet con tutti gli elementi essenziali della configurazione:

- *peer*
- *transit*
- *customer*

3 Emulazione

Kathará

```
- Creating Kathara network scenario from configuration...
- Created device under test with name `as_59715`.
- Searching peering device with name `as_112`.
- Device `as_112` not found, creating...
- Device `as_112` created and directly connect
- Searching peering device with name `as_
- Device `as_112` already created.
- Searching peering device with name `as_67
- Device `as_6762` not found, creating...
- Last connected `as_59715` iface idx=2, next peering if idx=4.
- Created dummy collision domain for `as_59715` on idx
- Device `as_6762` created and directly connected with device `as_59715` on
- Peering with AS6762 is provider, add client.
- Added client `as_6762_client` on collision domain `AAAD`.
- Searching peering device with name `as_6762`.
- Device `as_6762` already created.
- Added client `as_59715_client` on iface idx=5 on collision domain `AAAE`.
```

creazione dello scenario

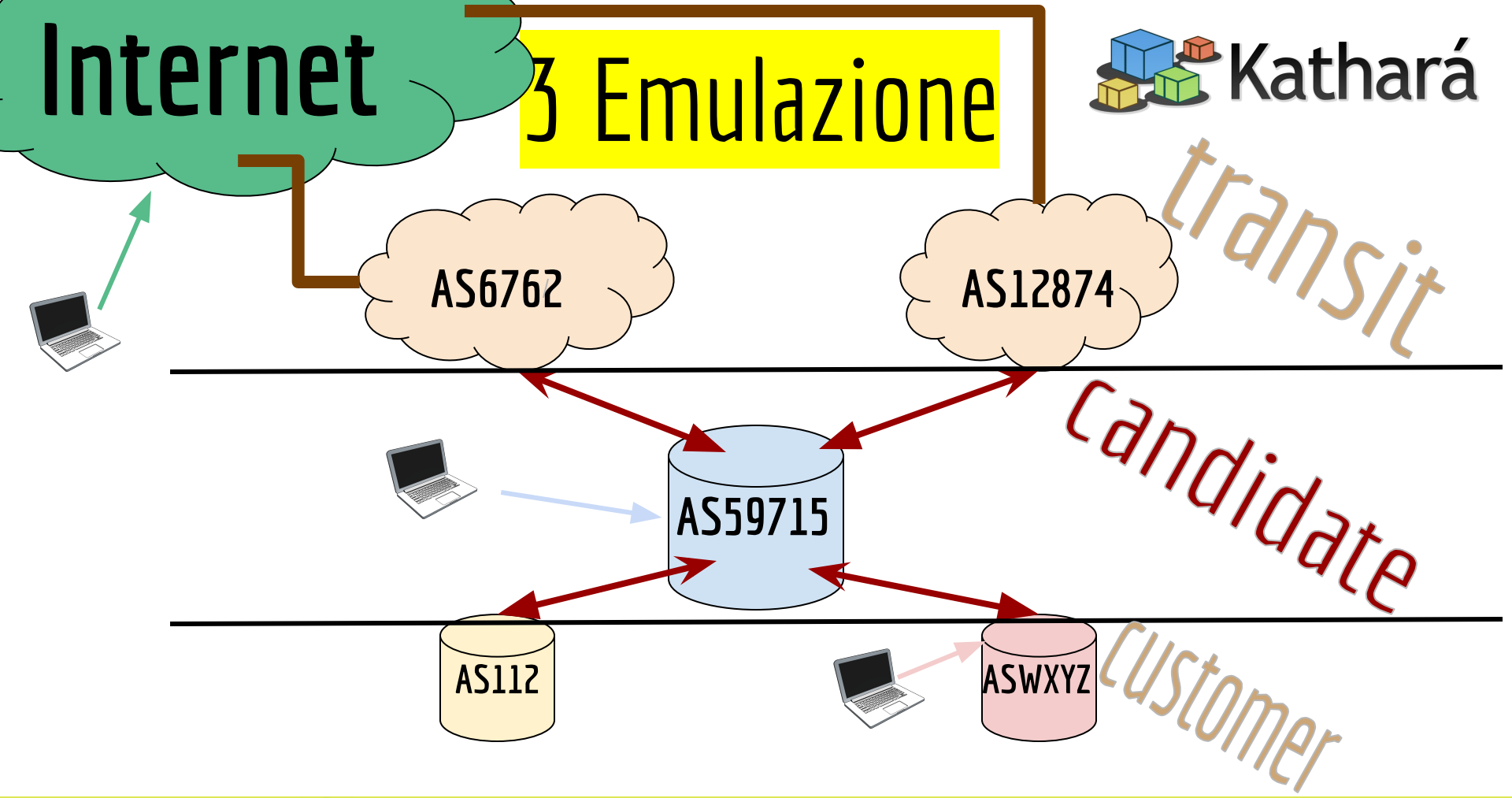
3 Emulazione

Kathará

configurazione delle sessioni BGP

```
- Configuring BGP in peering device `as_112`...
- Adding neighbor to `as_112` on interface IP=185.5.201.241 toward
- Adding neighbor to `as_112` on interface IP=2a02:cdc5:9715:0:185
- Configuring BGP in peering device `as_6762`...
- Adding neighbor to `as_6762` on interface IP=89.221.32.156 towar
- Adding neighbor to `as_6762` on interface IP=2001:41a8:60:2::79
- AS6762 is a provider, announcing 0.0.0.0/0 on IPv4...
- AS6762 is a provider, announcing ::/0 on IPv6...
```

3 Emulazione



```
vrnetlab@vr-vmx> show configuration | display set
set version 18.2R1.9
set system login user vrnetlab uid 2000
set system login user vrnetlab class super-user
set system login user vrnetlab authentication encrypted-password "$6$EW.Wa.FU$02rXc6GKbIU/7XtLk86fzom6wFmQP1W87YbJQTeHLFGNySmeX1/gLG07Igylv.EeqZ6Xi0b7pC.DZLUcPHQwp1"
set system root-authentication encrypted-password "$6$ZV/KaRqY$VHz3zZJQEJGxCWFXbhU4SQOc6ukC.AkJ..uLdbq97PSCKREOXtyjVMppgDWeKdOQDfDaYRfWK/NkZsgrHHraA1"
set system host-name vr-vmx
set system management-instance
set system services ssh
set system services extension-service request-response grpc clear-text port 57400
set system services extension-service request-response grpc max-connections 4
set system services netconf ssh
set system services netconf rfc-compliant
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set chassis fpc 0 pic 0 number-of-ports 96
set interfaces ge-0/0/1 description DOWNLINK-HUAWEI-10G-WAN
set interfaces ge-0/0/1 unit 0 family inet address 185.5.203.254/24
set interfaces ge-0/0/1 unit 0 family inet address 185.5.201.201/23
set interfaces ge-0/0/1 unit 0 family inet address 185.5.200.255/23
set interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc5:9715:0:185:5:200:255/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc5:9715:0:185:5:203:254/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc6:3074::/64
deactivate interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc6:3074::/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc6:3074:0:185:5:200:255/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2a02:cdc6:3074:0:185:5:203:254/64
set interfaces ge-0/0/2 description DOWNLINK-HUAWEI-10G-ASPTP
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 100 vlan-id 100
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 preferred
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 virtual-address 185.5.202.254
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 priority 150
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 advertise-interval 1
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 accept-data
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 authentication-type simple
set interfaces ge-0/0/2 unit 100 family inet address 185.5.202.2/24 vrrp-group 10 authentication-key "$9$QcnWnCuRhr8xdp0yKv87NUjHmT3n/Atu1jHTF3/O0hSrevLwYo"
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 primary
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 vrrp-inet6-group 10 virtual-inet6-address 2a02:cdc5:9715:a000:185:5:202:254
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 vrrp-inet6-group 10 virtual-link-local-address fe80::185:5:202:254
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 vrrp-inet6-group 10 priority 150
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 vrrp-inet6-group 10 preempt
set interfaces ge-0/0/2 unit 100 family inet6 address 2a02:cdc5:9715:a000:185:5:202:2/64 vrrp-inet6-group 10 accept-data
set interfaces ge-0/0/2 unit 169 vlan-id 169
set interfaces ge-0/0/2 unit 169 family inet rpf-check mode loose
set interfaces ge-0/0/2 unit 169 family inet address 169.254.63.74/24
set interfaces ge-0/0/2 unit 169 family inet6 rpf-check mode loose
set interfaces ge-0/0/2 unit 169 family inet6 address 2a02:cdc5:9715:169:169:254:63:074/64
set interfaces ge-0/0/3 description DOWNLINK-HUAWEI-10G-WAN-TRANSIT
set interfaces ge-0/0/3 unit 0 family inet rpf-check mode loose
set interfaces ge-0/0/3 unit 0 family inet filter input FW_SBTAP_IPV4_IN
set interfaces ge-0/0/3 unit 0 family inet filter output FW_SBTAP_IPV4_OUT
set interfaces ge-0/0/3 unit 0 family inet address 89.221.32.157/31
set interfaces ge-0/0/3 unit 0 family inet6 rpf-check mode loose
set interfaces ge-0/0/3 unit 0 family inet6 filter input FW_SBTAP_IPV6_IN
set interfaces ge-0/0/3 unit 0 family inet6 filter output FW_SBTAP_IPV6_OUT
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:41a8:60:2::7a/126
set interfaces fxp0 unit 0 family inet address 10.0.0.15/24
set forwarding-options rpf-loose-mode-discard family inet
set forwarding-options rpf-loose-mode-discard family inet6
set routing-options options syslog level debug
set routing-options rib inet6.0 static route 100::/128 discard
set routing-options rib inet6.0 static route 100::/128 retain
set routing-options rib inet6.0 static route 100::/128 install
---(more 8%)---
```

Kathará

configurazione del candidato caricata nel JunOS su kathara

3 Emulazione

sessioni BGP del JunOS su kathara

```
vrnetlab@vr-vmx> show bgp summary
Groups: 18 Peers: 23 Down peers: 19
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                       1          1          0          0          0          0
inet6.0
                       1          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Received/Accepted/Damped...
38.229.6.20           65332          0          0       0       0          59 Active
38.229.46.20          65332          0          0       0       0          59 Active
38.229.240.100        64496          0          0       0       0          59 Active
38.229.244.100        64496          0          0       0       0          59 Active
64.79.149.244        397601          0          0       0       0          59 Active
89.221.32.156          6762          4          3       0       0          22 1/1/1/0              0/0/0/0
169.254.63.100        59715          0          0       0       0          59 Connect
169.254.63.101        59715          0          0       0       0          59 Connect
178.248.237.29       197068          0          0       0       0          59 Active
185.5.200.243         59715          0          0       0       0          59 Connect
185.5.201.241           112          2          2       0       0          22 0/0/0/0              0/0/0/0
185.5.202.131         59715          0          0       0       0          59 Connect
212.114.120.72       199036          0          0       0       0          59 Connect
2001:7b8:62b:1:0:d4ff:fe72:7848      199036          0          0       0          59 Active
2001:1898:2400:3000:8000::105        397601          0          0       0          59 Active
2001:41a8:60:2::79     6762          4          3       0       0           5 Establ
  inet6.0: 1/1/1/0
2604:8800:60:240::100     64496          0          0       0       0          59 Active
2604:8800:240::100        64496          0          0       0       0          59 Active
2620:0:6b0:8000::20       65332          0          0       0       0          59 Active
2620:0:6b0:ff00::20       65332          0          0       0       0          59 Connect
2a02:cdc5:9715:0:185:5:201:241          112          2          2       0          8 Establ
  inet6.0: 0/0/0/0
2a02:cdc5:9715:169:169:254:63:100       59715          0          0       0       0          59 Connect
2a02:cdc5:9715:169:169:254:63:101       59715          0          0       0       0          59 Connect
```

3 Emulazione

router FRR su kathara per emulazione transit

```
as_6762# sh bgp summary

IPv4 Unicast Summary:
BGP router identifier 89.221.32.156, local AS number 6762 vrf-id 0
BGP table version 4
RIB entries 4, using 768 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt
89.221.32.157   4      59715         4         5        0    0    0 00:00:21            3        4

Total number of neighbors 1

IPv6 Unicast Summary:
BGP router identifier 89.221.32.156, local AS number 6762 vrf-id 0
BGP table version 3
RIB entries 3, using 576 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor         V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt
2001:41a8:60:2::7a 4      59715         4         5        0    0    0 00:00:03            2        3

Total number of neighbors 1
as_6762#
```

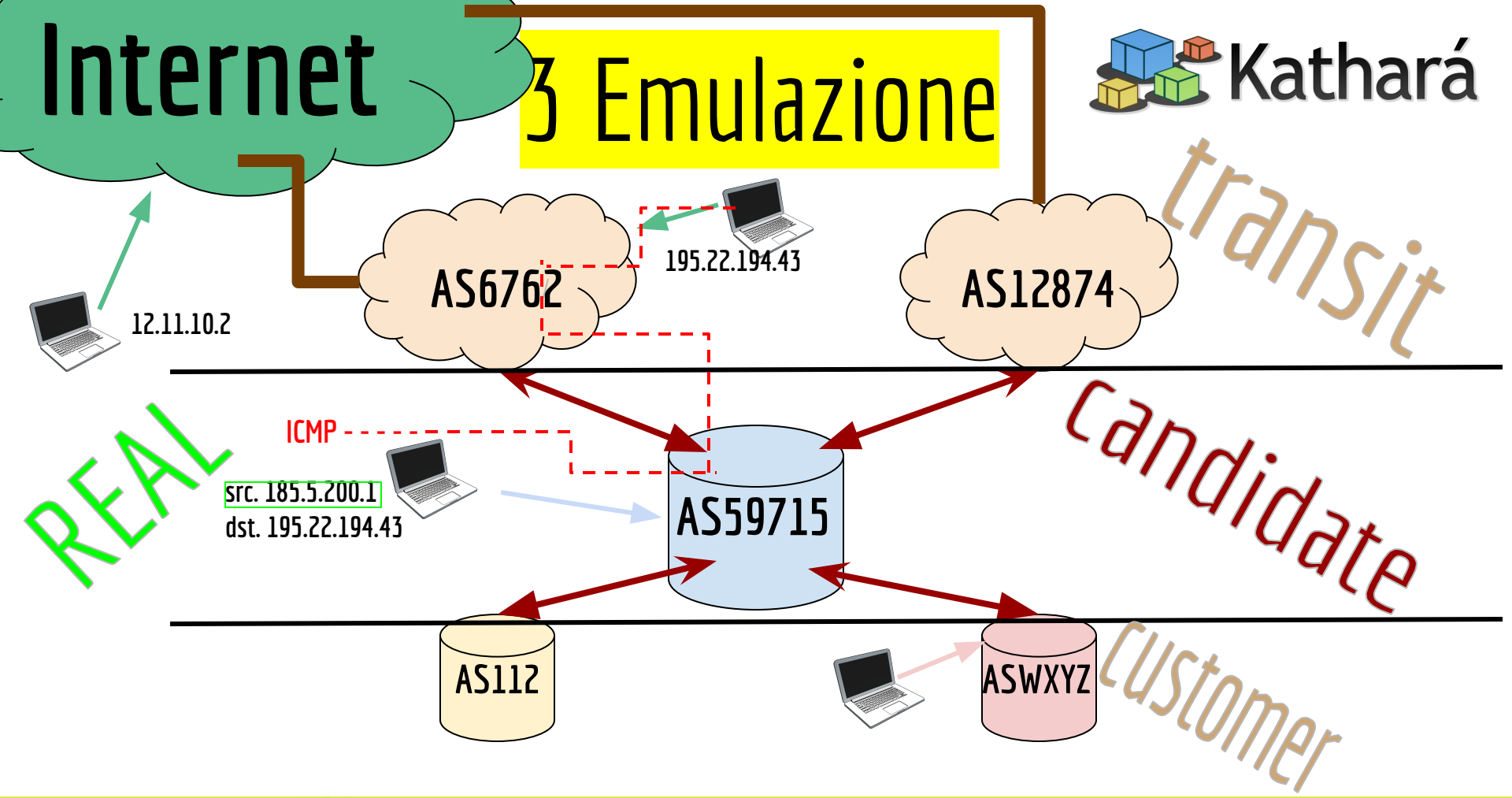

MANRS

ACTION 2 for network operators

Blocking traffic from spoofed IP addresses: an operator should implement a system that enables Source Address Validation for its own network and its customers. It is then necessary to include anti-spoofing filters to prevent packets with an incorrect source IP address from entering or leaving the network.

3 Emulazione

Kathará

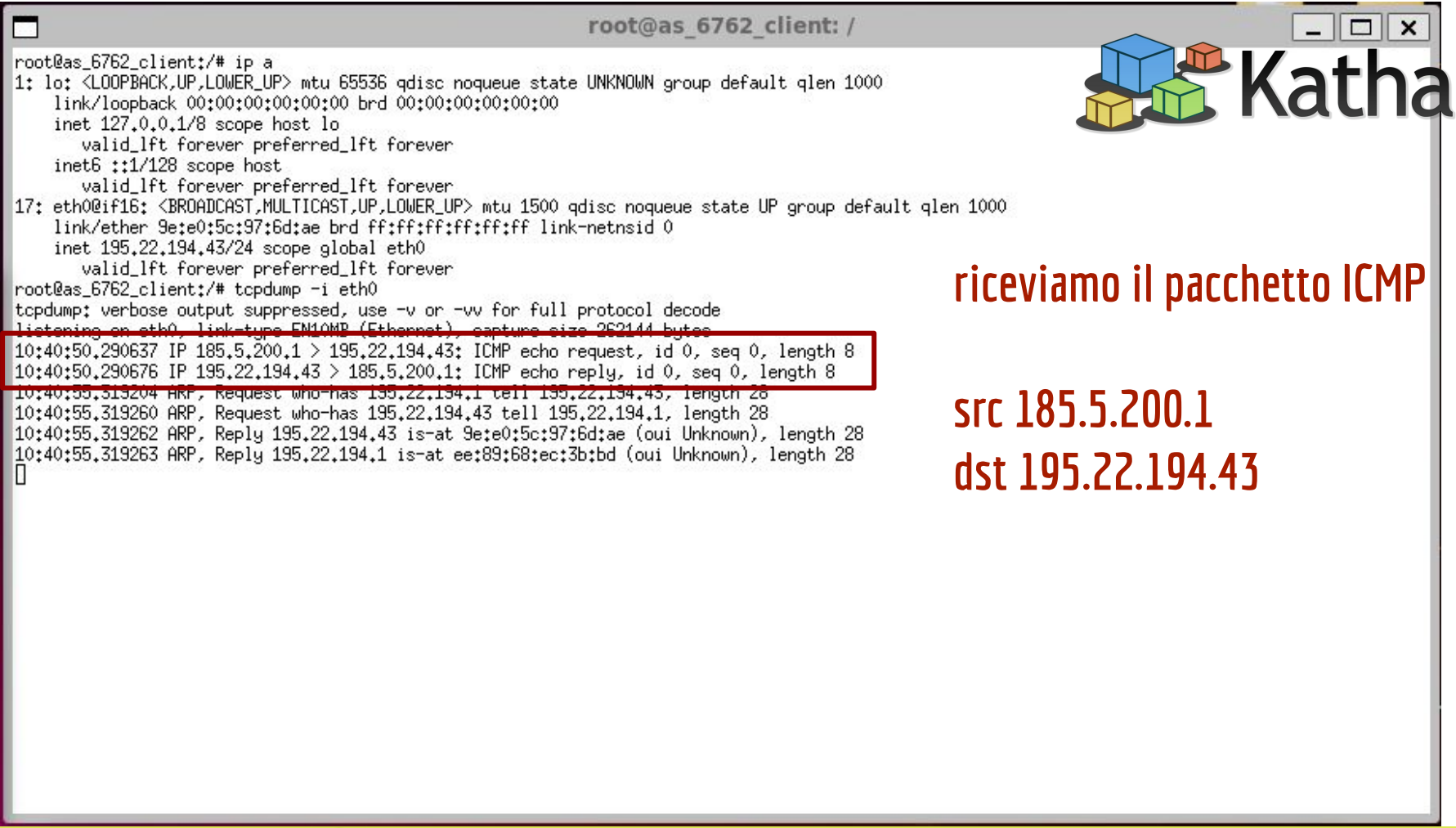


Kathará

inviamo un pacchetto ICMP

src 185.5.200.1

dst 195.22.194.43



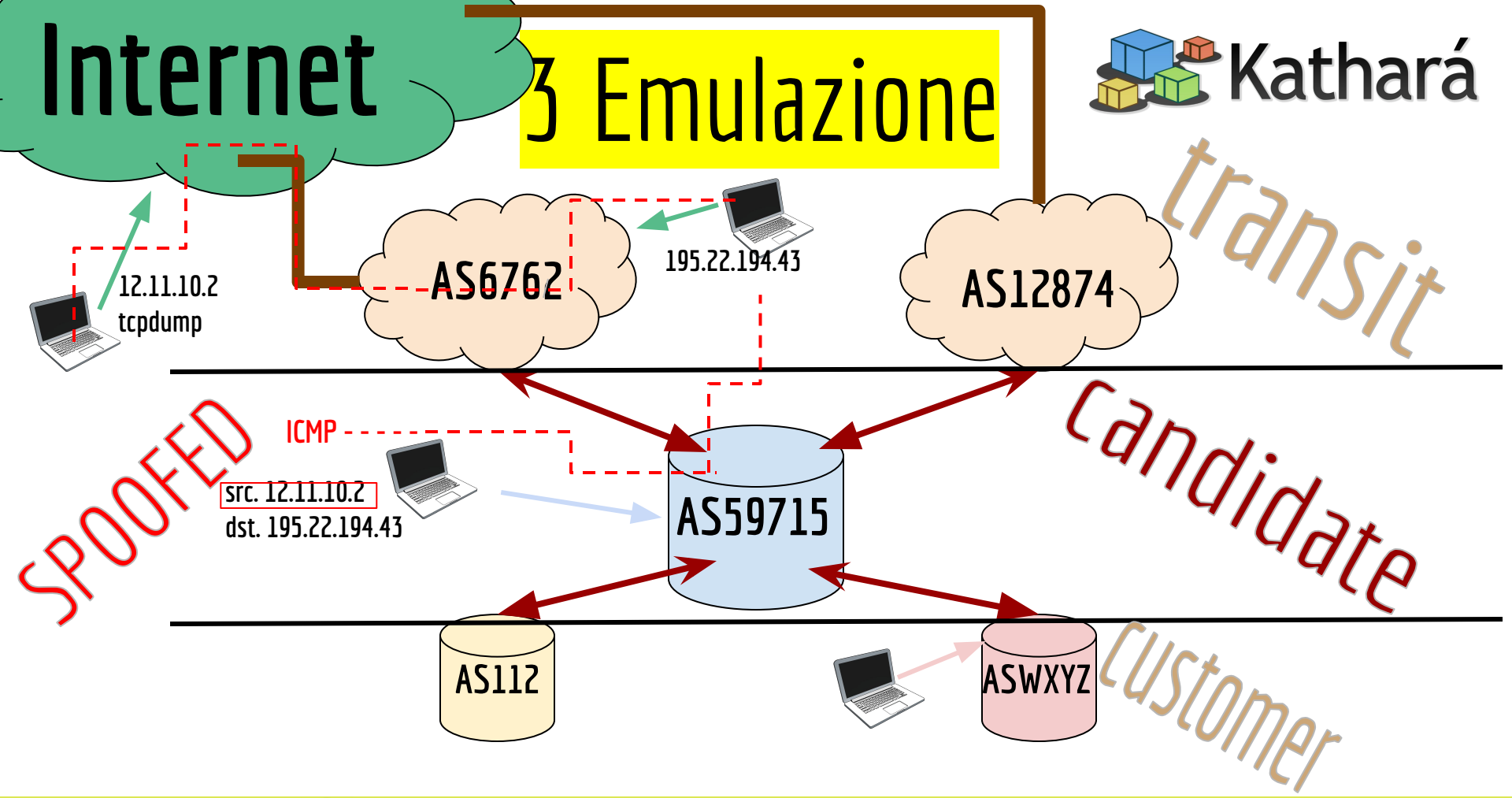
Kathará

riceviamo il pacchetto ICMP

src 185.5.200.1

dst 195.22.194.43

3 Emulazione

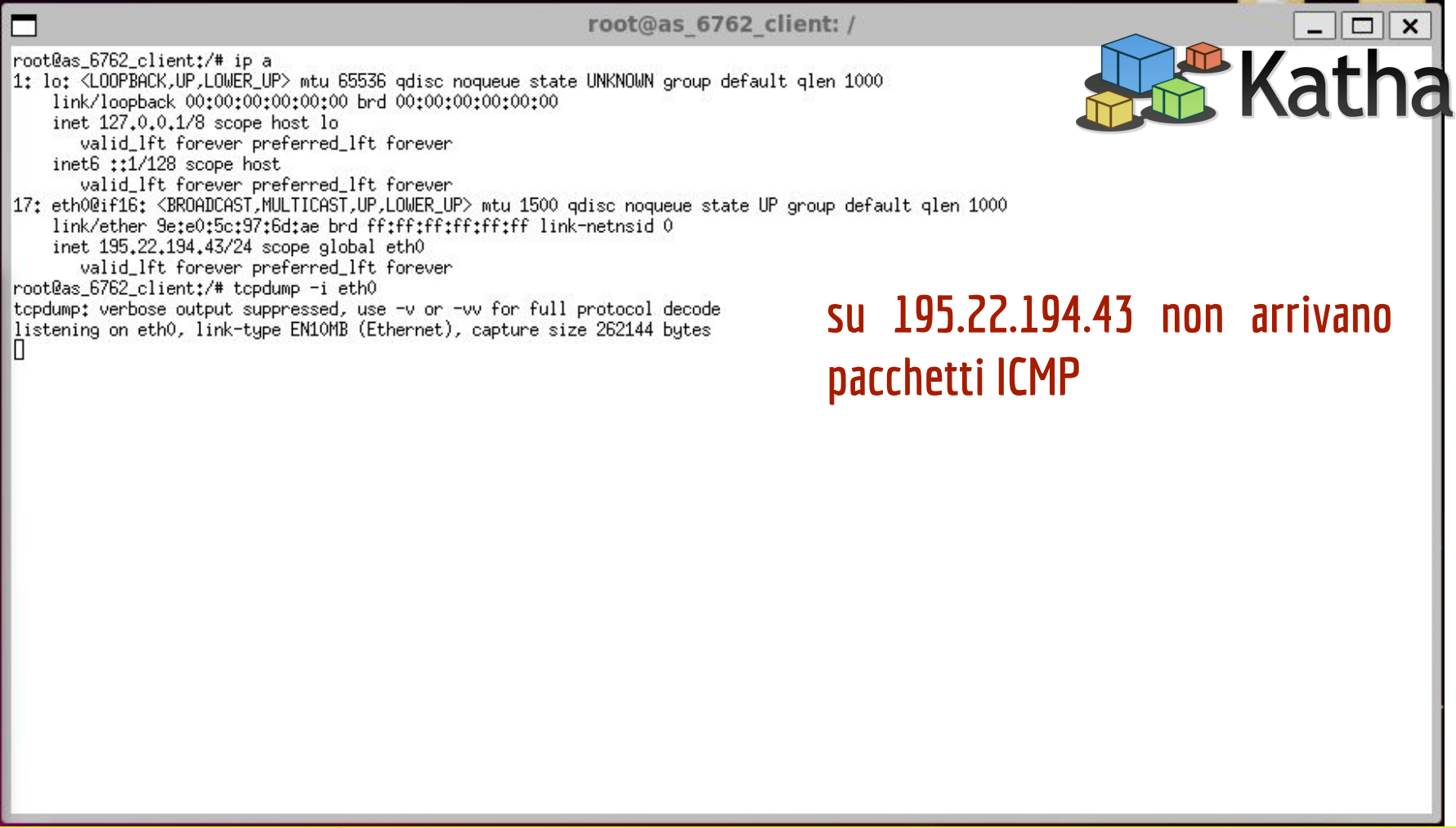


Kathará

inviamo un pacchetto ICMP

src 12.11.10.2

dst 195.22.194.43



Kathará

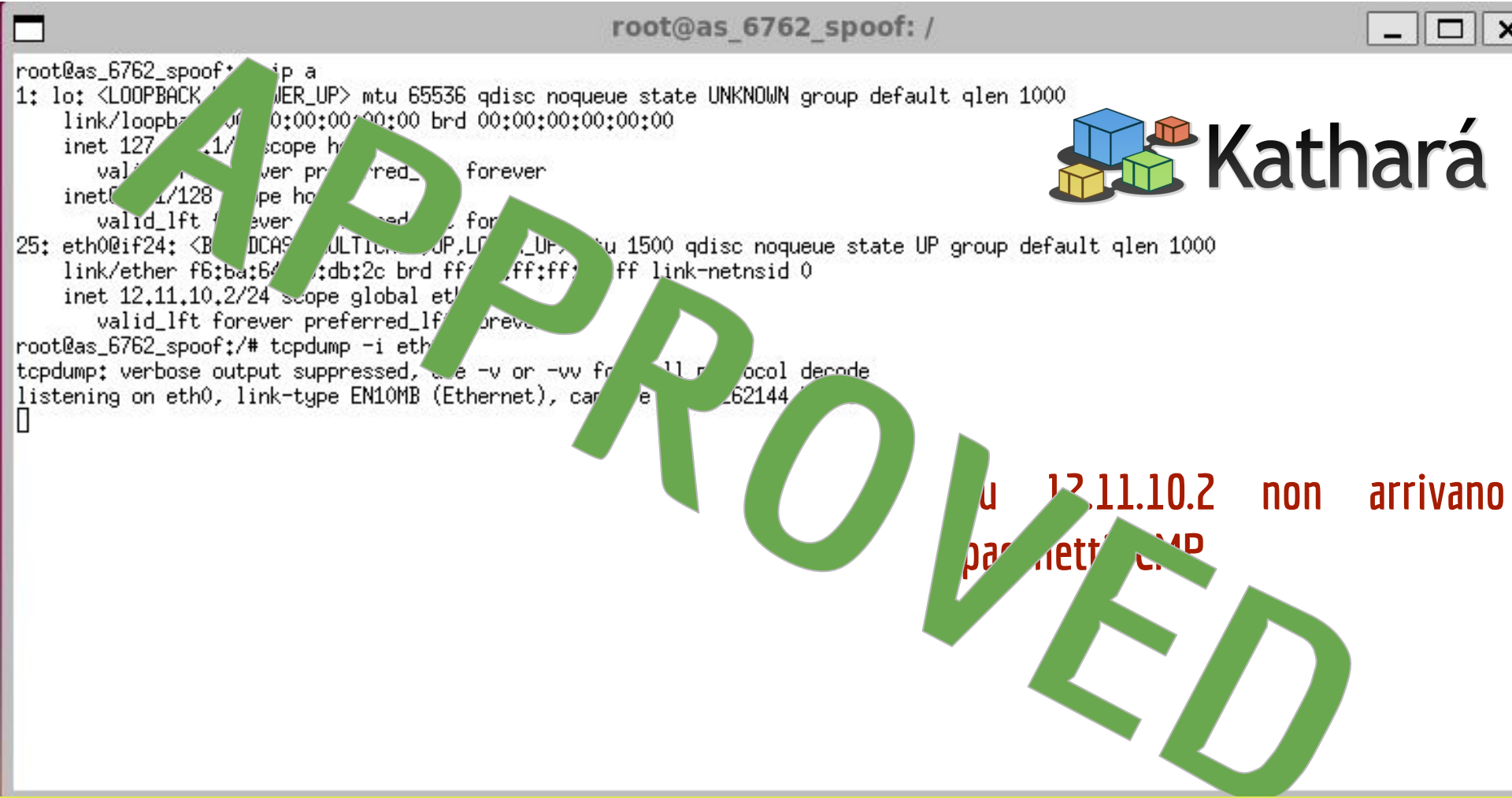
su 195.22.194.43 non arrivano pacchetti ICMP

root@as_6762_spoof: /

```
root@as_6762_spoof:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
25: eth0@if24: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f6:6a:64:c9:db:2c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 12.11.10.2/24 scope global eth0
       valid_lft forever preferred_lft forever
root@as_6762_spoof:/# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Kathará

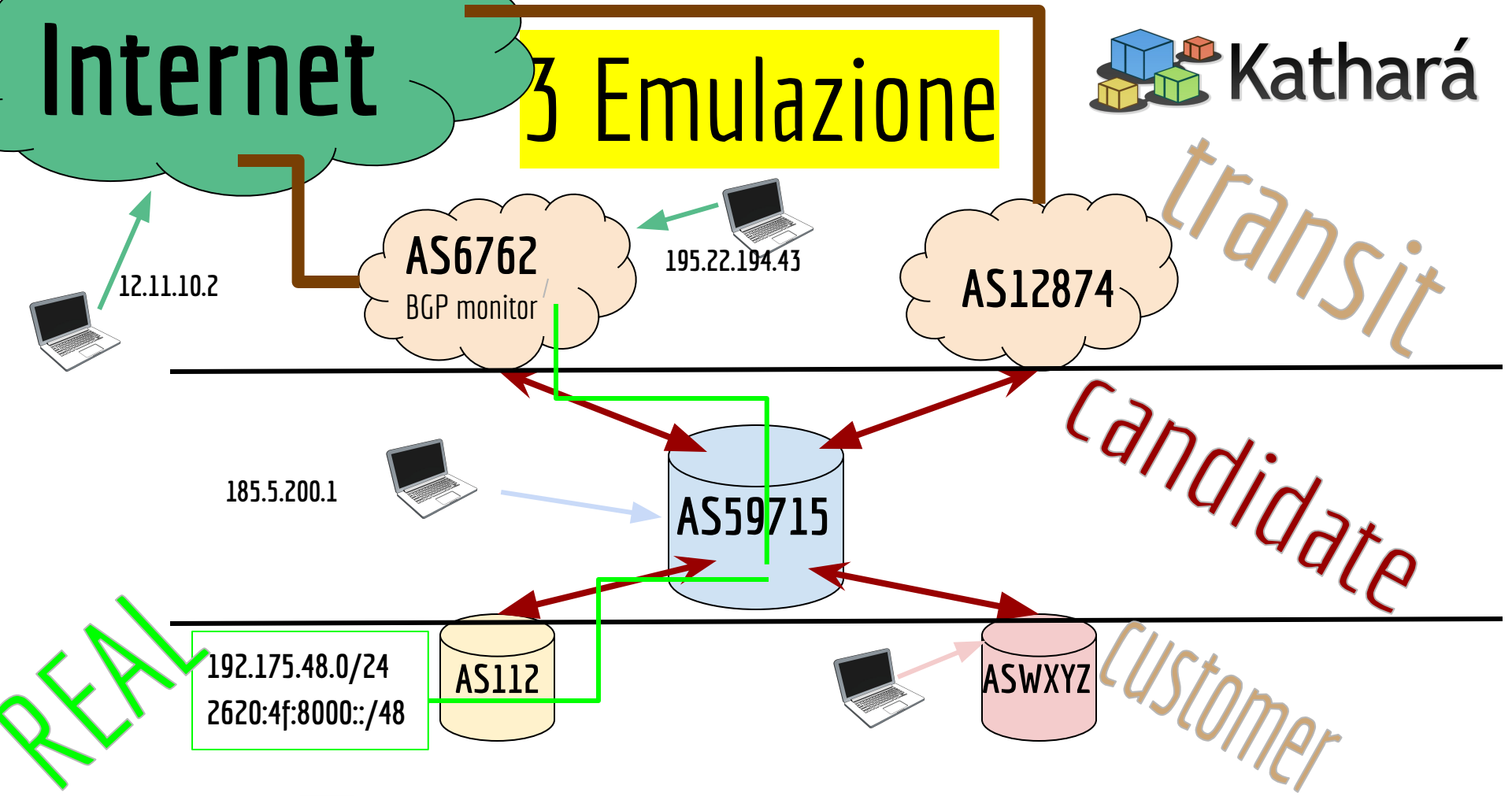
su 12.11.10.2 non arrivano pacchetti ICMP


root@as_6762_spoof: /
root@as_6762_spoof:/# ip a
1: lo: <LOOPBACK
link/loopb
inet 127
forever
inet
valid_lft
25: eth0@if24: <B
1500 qdisc noqueue state UP group default qlen 1000
link/ether f6:ba:6
link-netnsid 0
inet 12.11.10.2/24 scope global et
valid_lft forever preferred_lf
root@as_6762_spoof:/# tcpdump -i eth
tcpdump: verbose output suppressed,
-v or -vv fr
ocol decode
listening on eth0, link-type EN10MB (Ethernet), ca
62144
Kathará
APPROVED
non arrivano

MANRS

ACTION 1 for network operators

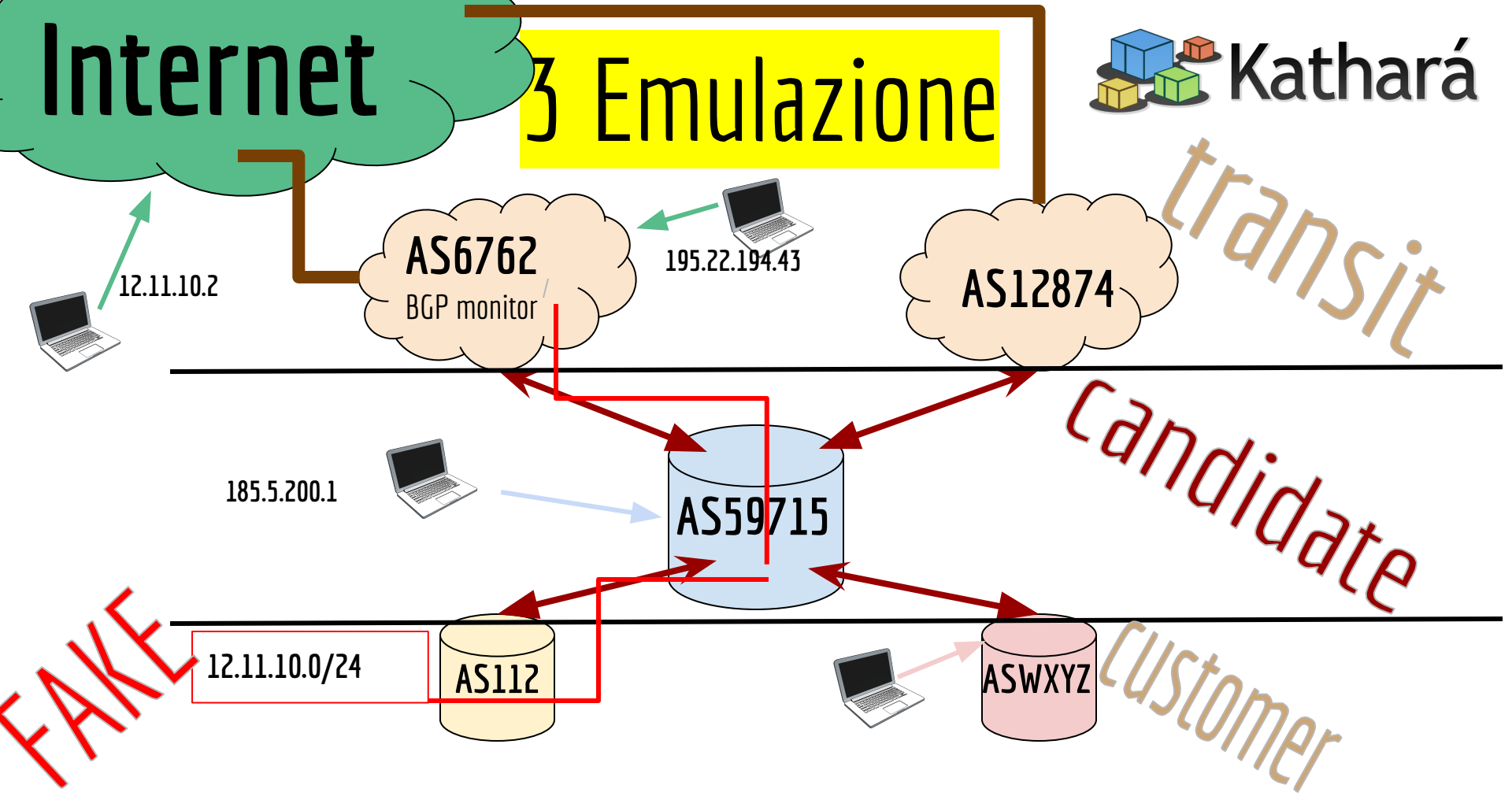
Preventing the propagation of incorrect routing information: it is necessary to implement a system on the basis of which an operator announces to adjacent networks only and exclusively its own prefixes and those of its customers. Likewise, the operator must verify that the prefixes announced by its customers are really their own.


Internet
3 Emulazione
Kathará
AS6762
BGP monitor
12.11.10.2
195.22.194.43
AS12874
transit
185.5.200.1
AS59715
candidate
REAL
192.175.48.0/24
2620:4f:8000::/48
AS112
ASWXYZ
customer

Internet

3 Emulazione

Kathará



Conclusione e sviluppi futuri

- RoSe-T riduce i rischi del *routing* BGP
- Favorisce l'adozione di pratiche sicure
- Prossimi passi: supporto altre azioni e monitoraggio *live*