



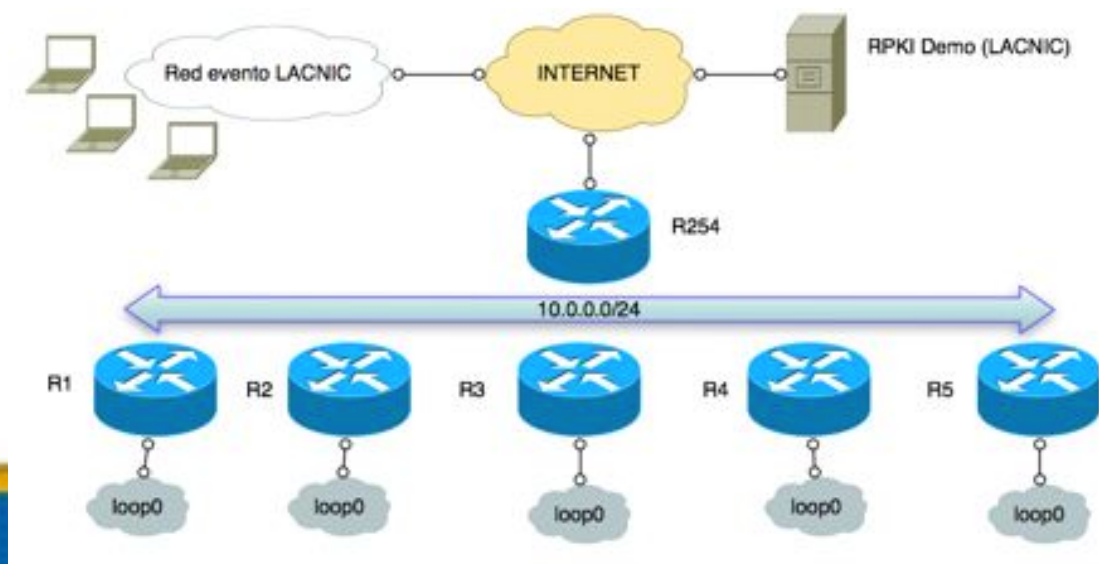
Configuración de enrutadores Cisco con validación de origen (RPKI)

RFI – Facultad de Ingeniería – UDELAR

Montevideo, Uruguay

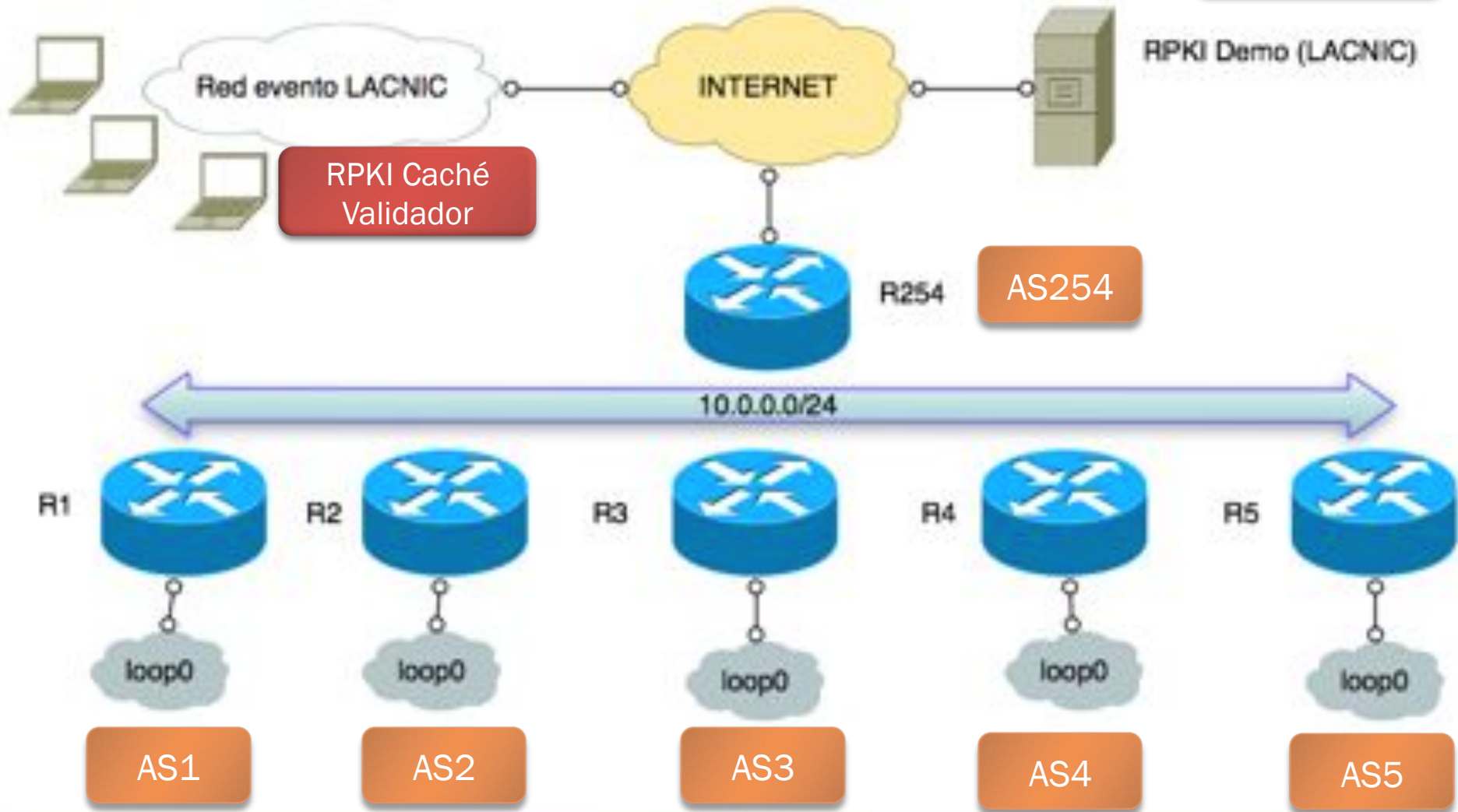
Carlos Martínez

- ▶ Vamos a simular un punto de intercambio de tráfico (IXP)
- ▶ Nos dividiremos en 6 grupos
- ▶ Cada grupo establecerá al menos una sesión BGP con el router central
- ▶ Los que gusten pueden establecer peerings entre grupos



Testbed de RPKI

Hosted
RPKI





Actores en el Testbed

- ▶ **Sistemas autónomos**
 - ▶ “Usuarios”
 - ▶ AS 1 al AS 5
 - ▶ “Router central”
 - ▶ AS 254
- ▶ **Routers**
 - ▶ R1 (AS 1) al R5 (AS 5)
- ▶ **LAN de Interconexión**
 - ▶ 10.0.0.0/24
 - ▶ R1: 10.0.0.1/24 ... R5: 10.0.0.5/24
 - ▶ R254: 10.0.0.254/24



Actores en el Testbed (ii)

- ▶ Cada router tiene asignado para 'sus' clientes una red / 16:
 - ▶ R1: 10.1.0.0/16
 - ▶ R5: 10.5.0.0/16
- ▶ Cada usuario de un router debera anunciar rutas a los vecinos, y configurar peerings con los vecinos



Configuración de interfaces Loopback

```
!  
interface loopback 10  
  no shutdown  
  ip address 10.1.0.1/24  
  description Red 1 del grupo 1  
!
```

```
!  
interface loopback 11  
  no shutdown  
  ip address 10.1.1.1/24  
  description Red 2 del grupo 1  
!
```

```
!  
router bgp 1  
  bgp log-neighbor-changes  
  bgp rpki cache a.b.c.d port-number P refresh-  
time 10  
  network 10.1.0.0/24  
  neighbor 10.0.0.254 remote-as 254  
  neighbor 10.0.0.254 soft-reconfiguration inbound  
  neighbor 10.0.0.2 remote-as 2  
  neighbor 10.0.0.2 soft-reconfiguration inbound  
!  
!
```



AS 20 – Recursos y ROAs

Logout

Certificado Ativo CA

Mudar Chave | Revocar Certificado | Atualização Certificado | Descarregar Cert. DER | Descarregar Cert. PEM

Sujeito	CN=Id15G2sbRdGLFDF-E-wvVHX-B
Emissor	CN=Th4EsbmLbJvM1nziQ7L903mhdY
Válido Desde	12/05/2011 16:01:14
Válido Até	19/05/2012 12:00:00
Recursos	Ver
Nro Série	37418
SIA	rsync://repository-demo-vm/tpk/demo/hoes rsync://repository-demo-vm/tpk/demo/hoes 91dab1bf756b/Id15G2sbRdGLFDF-E-wvV
AIA	rsync://repository-demo-vm/tpk/demo/hoes
Distribuição	rsync://repository-demo-vm/tpk/demo/hoes

Recursos

- AS2003
- 10.2.0.0/16
- 127.2.0.0/16
- 127.17.0.0/16
- 2001:db8:2::/48



Listar ROAs

Nome	Válido Desde	Válido Até	ASN de Origen	Recursos IPs	
roa-usr-nro1	12/05/2011 00:00:00	19/05/2012 00:00:00	AS20	10.2.0.0/16	Descargar Editar Revocar Validar

<< < > >>

Editar ROA

Nome

Válido Desde 

Válido Até 

ASN de Origen

Prefixo/Comprimento 

Comprimento Máximo: 

10.2.0.0/16 20 

R1#sh ip route

```
10.0.0.0/8 is variably subnetted, 4 subnets, 4 masks
B      10.2.0.0/17 [20/0] via 192.168.0.2, 00:24:28
B      10.2.224.0/19 [20/0] via 192.168.0.2, 00:24:28
B      10.20.0.0/16 [20/0] via 192.168.0.2, 00:24:28
B      10.20.0.0/21 [20/0] via 192.168.0.6, 00:24:28
192.168.0.0/24 is variably subnetted, 4 subnets, 2 masks
C      192.168.0.0/30 is directly connected, Serial2/1
L      192.168.0.1/32 is directly connected, Serial2/1
C      192.168.0.4/30 is directly connected, Serial2/0
L      192.168.0.5/32 is directly connected, Serial2/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, Ethernet1/0
L      192.168.10.1/32 is directly connected, Ethernet1/0
B      192.168.20.0/24 [20/0] via 192.168.0.2, 00:24:28
B      192.168.66.0/24 [20/0] via 192.168.0.6, 00:24:28
```

```
R1#sh ip bgp 10.2.224.0
BGP routing table entry for 10.2.224.0/19,
version 4
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    3          4
Refresh Epoch 1
20, (received & used)
  192.168.0.2 from 192.168.0.2 (10.20.0.1)
    Origin incomplete, metric 0, localpref 100,
valid, external, best
    path 65716730 RPKI State valid
```

```
R1#sh ip bgp 10.2.192.0
BGP routing table entry for 10.2.192.0/19,
version 3
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  66, (received & used)
    192.168.0.6 from 192.168.0.6 (10.20.0.1)
      Origin incomplete, metric 0, localpref 100,
valid, external
    path 65716774 RPKI State invalid
```

```
R1#sh ip bgp 10.2.160.0
BGP routing table entry for 10.2.160.0/21,
version 12
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    3          4
  Refresh Epoch 1
  20, (received & used)
    192.168.0.2 from 192.168.0.2 (10.20.0.1)
      Origin incomplete, metric 0, localpref 100,
valid, external, best
      path 65716598 RPKI State not found
```

```
R1#sh ip bgp rpki-neighbors
```

```
BGP SOVC neighbor is 192.168.10.10/32000  
connected to port 32000
```

```
Flags 0, Refresh time is 5, Serial number is 1  
InQ has 0 messages, OutQ has 0 messages,  
formatted msg 402
```

```
Session IO flags 3, Session flags 1
```

```
Neighbor Statistics:
```

```
Nets Processed 2
```

```
Connection state is ESTAB, I/O status: 1, unread  
input bytes: 0
```

```
Minimum incoming TTL 0, Outgoing TTL 255
```

```
Local host: 192.168.10.1, Local port: 15722
```

```
Foreign host: 192.168.10.10, Foreign port: 32000
```



Visualizando la tabla de RPKI

```
R1#sh ip bgp rpki-table
```

```
2 BGP sovc network entries using 176 bytes of memory
```

```
2 BGP sovc record entries using 40 bytes of memory
```

Network	Maxlen	Origin-AS	Source	Neighbor
10.0.0.0/16	20	10	0	192.168.10.10/320
10.2.0.0/16	20	20	0	192.168.10.10/320



Comentarios finales

- ▶ Las configuraciones completas de los routers así como los scripts que sincronizan el repositorio están publicamente disponibles
- ▶ Estaremos durante toda la semana disponibles para ayudarles a crear vuestros certificados y ROAs
- ▶ También estaremos disponibles para consultas técnicas relacionadas con RPKI



¡Muchas gracias!

carlos_@_lacnic.net