F-TICKS: la forma de tener los logs que queremos y necesitamos en eduroam

José Manuel Macías Luna
jmanuel.macias@rediris.es

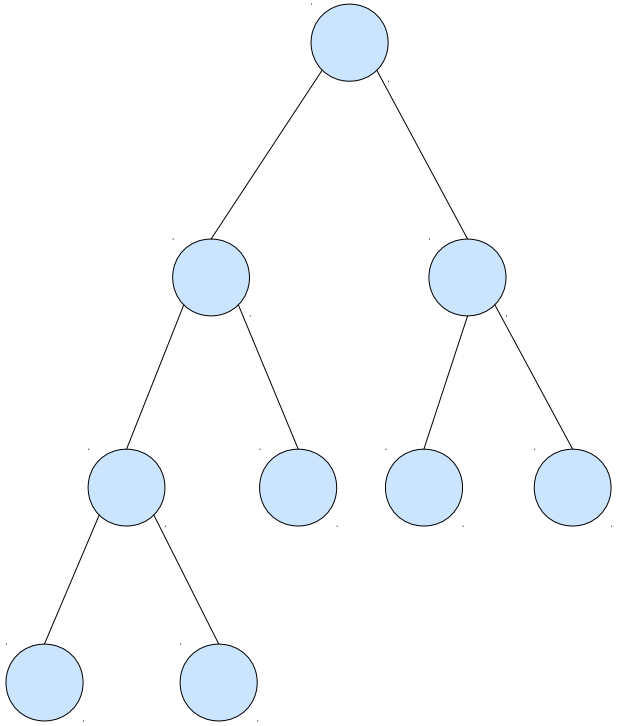
Cuenca, 5 de octubre de 2011

La necesidad...

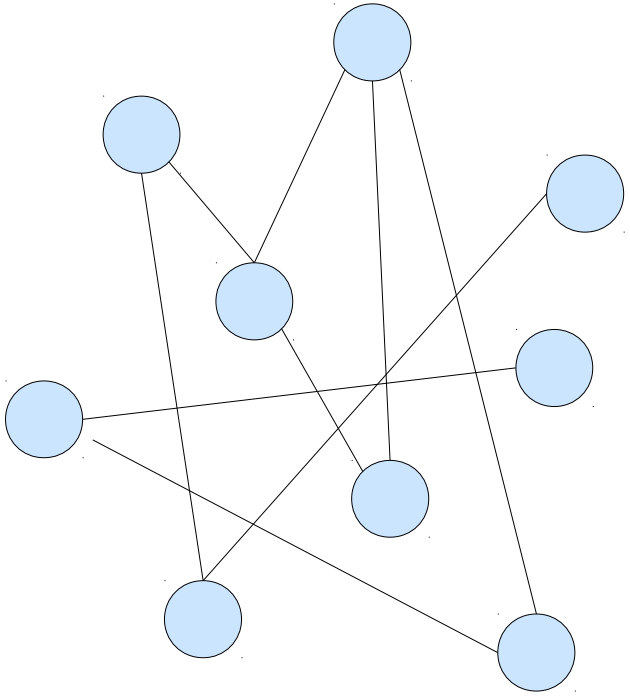
- Preguntas que se pretende contestar
  - ¿cuantos usuarios hacen roaming en eduroam?
  - ¿qué problemas pueden identificarse en el roaming a nivel internacional? ¿o nacional? ¿o incluso local?
  - ¿cuantas veces se conecta/reconecta un usuario a lo largo de un día y a qué horas?
  - ¿cuales son los hábitos *locales* de roaming?
  - ¿qué dispositivos utilizan los usuarios para conectarse?
  - ...es más; cuando entre en funcionamiento RadSec:
    - ¿cómo se recolectará información si no hay proxies intermedios?
    - ¿cómo podría depurarse de una manera más sencilla para los administradores?

La necesidad... (II)

Modelo jerárquico actual de eduroam



Modelo basado en descubrimiento de pares a través de DNS (a.k.a. DNSROAM)



La necesidad... (III)

```
Tue Oct  4 11:44:32 2011
        Packet-Type = Access-Request
        User-Name = "anonymous@organizacion.es"
        Framed-MTU = 1400
        Called-Station-Id = "0016.46f9.03c0"
        Calling-Station-Id = "7cc5.3798.1111"
        Service-Type = Login-User
        Message-Authenticator = 0x9ef245b0cfe7cc2a2a502b2eaed18d24
        EAP-Message = 0x020100160163617 26c6f7340726564697269732e6573
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 10767
        NAS-IP-Address = 130.206.x.x
        NAS-Identifier = "APIDXXX"
```

```
Tue Oct  4 11:44:48 2011
        Packet-Type = Access-Accept
        User-Name = "usuario@organizacion.es"
        MS-MPPE-Recv-Key = 0xa3d929220b38dde55bcf3aa1de9b9e5cfb554df008cdf953b9f7b046be556878
        MS-MPPE-Send-Key = 0x214c08d7e78ce51827534c9fcb0364792324c323291aee4212d32bc610dc16ab
        EAP-Message = 0x03060004
        Message-Authenticator = 0xd8b8c6fdd18a1634b50e0cb255bde08c
```

Resumiendo...

- La infraestructura ha alcanzado gran complejidad, con muchos puntos intermedios donde puede haber fallos
  - En ocasiones hay que implicar a todos los puntos intermedios para la depuración de un problema
  - Diversidad de formatos de logs (freeradius, radiator, IAS, Microsoft, CISCO,…)
- Por otro lado, calcular cuantos usuarios usan eduroam, y estudiar hábitos de conexión se pone difícil...
  - ...más posible a nivel local, si bien no existe una receta que sirva para todo el mundo
    - ...se quedan atrás datos de *roaming local*
- Finalmente, RadSec cambiará además el modelo actual de eduroam

La solución...

- F-TICKS es una propuesta que aparece dentro de GN3
- Es tan sencillo como un formato común de “logs” (f-ticks)
- Fácil de implementar en los sabores de proxies más habituales (freeradius y radiator)
  - ...pero también podéis usarlo vosotros
- Inicialmente con la idea de generar estadísticas intra-federación que puedan ser recopiladas en un determinado servidor central
- Para el transporte de la información se utiliza SYSLOG/UDP
- Se usa una cadena de texto estandarizada para contener la información imprescindible

Sintaxis

- Información básica:

```
F-TICKS/eduroam/1.0
    #REALM=%R#VISCOUNTRY=ES#CSI=%{Calling-Station-Id}#RESULT=OK#
```

dominio | país | MAC | resultado

- Información extendida:

```
F-TICKS/eduroam/1.0
     #REALM=%R#VISCOUNTRY=ES#CSI=%{Calling-Station-Id}#RESULT=OK#VISINST=FOO#
```

Institución visitada

- En clave Syslog se ve así:

```
user.info<14>: Oct  4 17:24:03 francio.rediris.es radiusd:
   F-TICKS/eduroam/1.0#REALM=rediris.es#VISINST=ETLR
                      #VISCOUNTRY=ES#CSI=0026828dafab#RESULT=OK#
```

Receta 1

- Receta para freeradius (fichero radiusd.conf):

```
modules {
        # stats via f_ticks
        linelog f_ticks {
                filename = syslog
                format = ""
                reference = "f_ticks.%{%{proxy-reply:Packet-Type}:-format}"
                f_ticks {
                        Access-Accept = "F-TICKS/eduroam/1.0#REALM=%
{Realm}#VISINST=%{Client-Shortname}#VISCOUNTRY=ES#CSI=%{Calling-Station-
Id}#RESULT=OK#"
                        Access-Reject = "F-TICKS/eduroam/1.0#REALM=%
{Realm}#VISINST=%{Client-Shortname}#VISCOUNTRY=ES#CSI=%{Calling-Station-
Id}#RESULT=FAIL#"
                }

        }
…
}
```

```
post-auth {
        auth_log
        f_ticks
        Post-Auth-Type REJECT {
                auth_log
                f_ticks
        }
}
```

Receta 2

- Receta para radiator (fichero radius.cfg):

```
<AuthLog SYSLOG>
        Identifier TICKS
        LogSuccess 1
        LogFailure 1
        LogSock udp
        LogHost 198.51.100.253
        SuccessFormat F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=%{eduroam-SP-
Country}#VISINST=%{Operator-Name}#CSI=%{Calling-Station-Id}#RESULT=OK#
        FailureFormat F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=%{eduroam-SP-
Country}#VISINST=%{Operator-Name}#CSI=%{Calling-Station-Id}#RESULT=FAIL#
</AuthLog>
```

Estado actual...

- En fase de piloto a nivel europeo
  - 19 federaciones aportando ticks
- "recetas" para ponerlo en funcionamiento para freeradius, radiator y pronto en radsecproxy
- 1 servidor central para toda Europa recolectando datos
  - Estudiando escalabilidad/redundancia
- Discutiendo cuestiones relacionadas con privacidad
- Discutiéndose la escalabilidad de cara a eduroam global y a incluir información de uso local
- Viendo su posible uso en depuración de problemas
  - Inclusión de información sobre el tipo de autenticación, por ejemplo
- Estudiando su posible uso para otros sistemas distribuidos

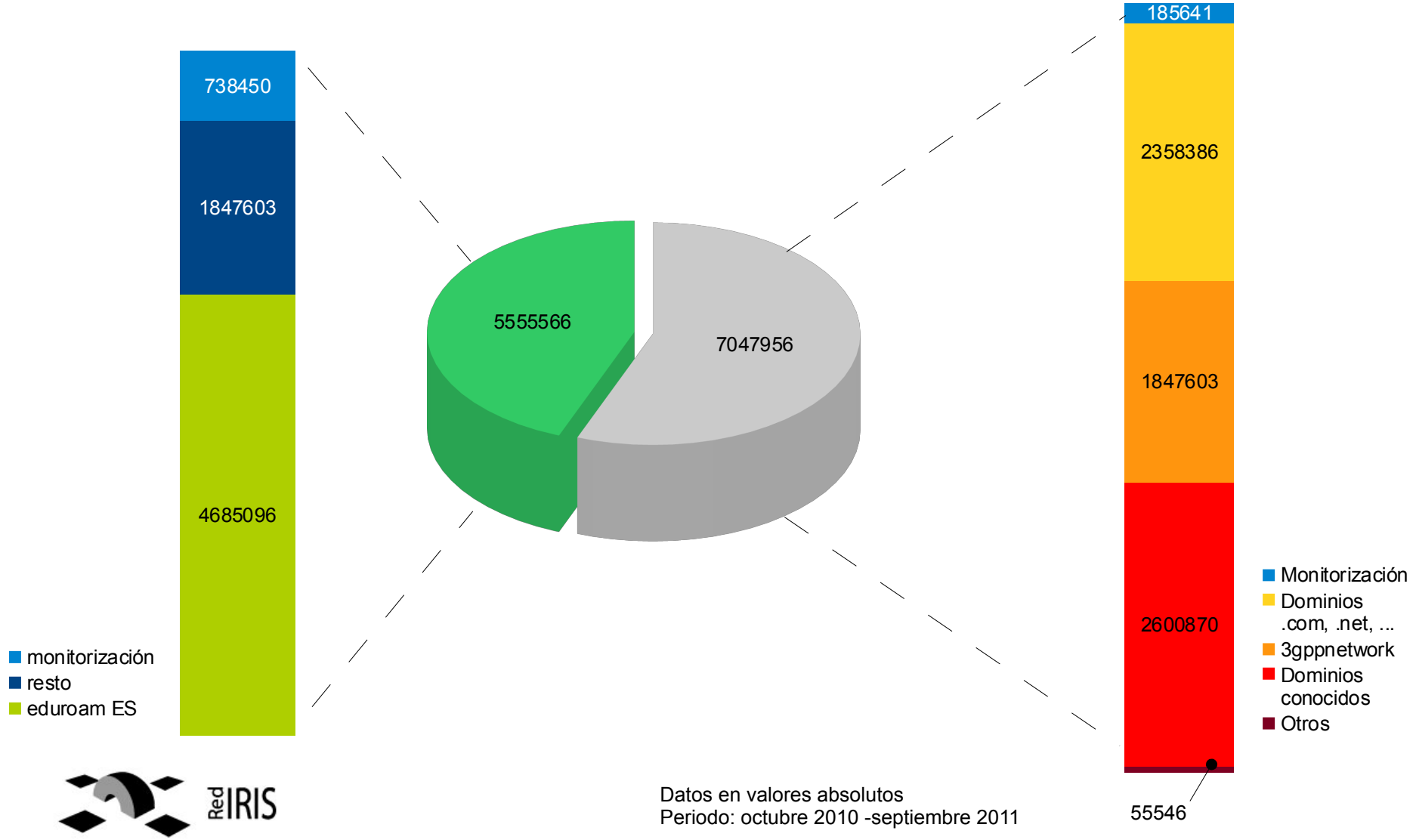
Privacidad...

- Hay quien considera la MAC (CSI) como un dato de carácter privado
  - Si se puede relacionar con un usuario, se puede trazar dónde estuvo ese usuario
  - ...pero esa información ya queda almacenada en proxies intermedios y en la institución visitada
- Otros piensan que tampoco debería 'darse a conocer' la institución visitada por sus usuarios (VISINST)
  - Este dato no siempre puede conocerse en la actualidad, pero en ocasiones sí (la IP del NAS si es pública, por ejemplo)
- Estos datos ahora mismo viajan “en claro” (SYSLOG)
- Sin embargo...
  - Las MACs pueden no enviarse, ser ofuscadas (o sólo enviarse el prefijo)
  - La institución visitada puede omitirse también
  - El canal puede cifrarse (rsyslog)

1 año de f-ticks...

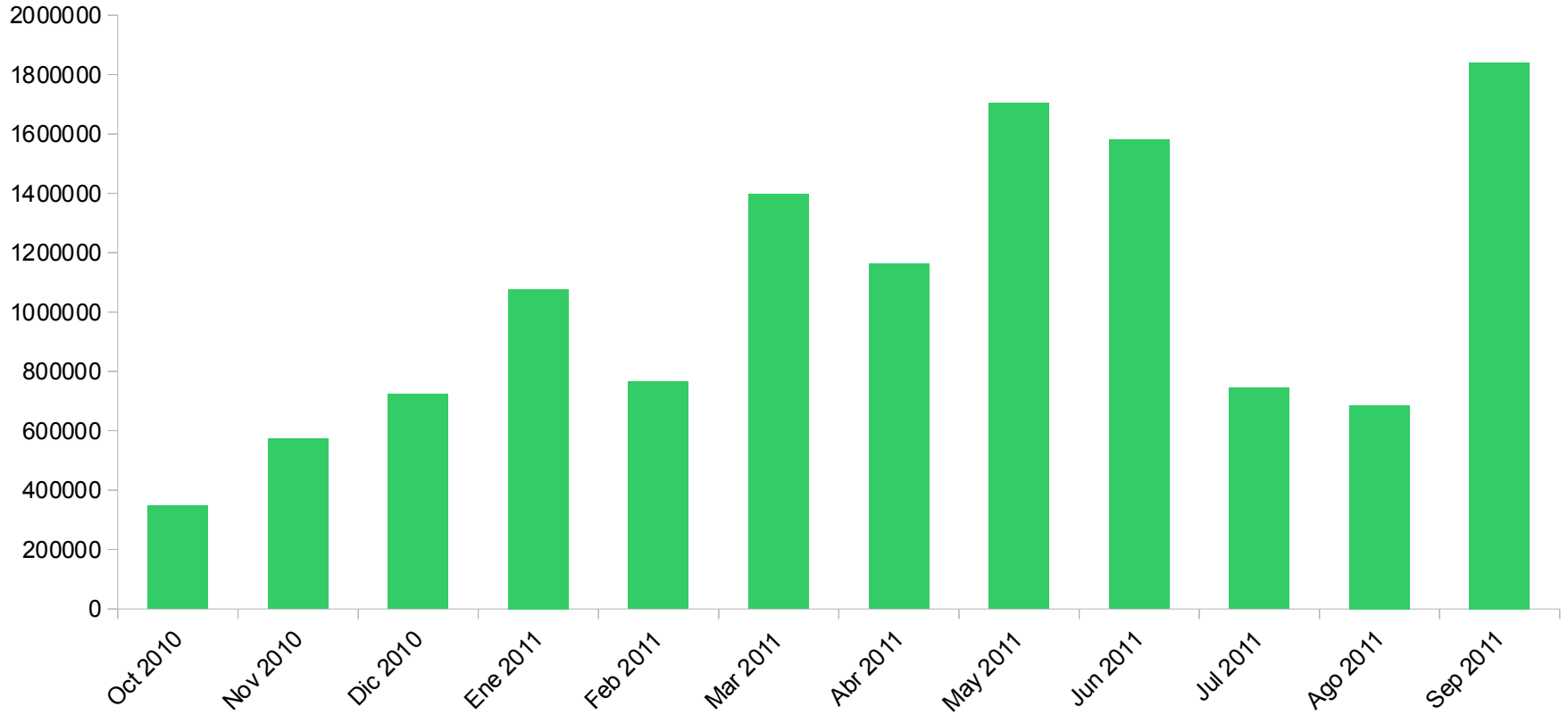
- Analizamos datos de los proxies de RedIRIS
  - Datos entre octubre 2010-septiembre 2011
  - 12 603 523 intentos de autenticación
  - Aprox 3 GB de información en crudo (texto)
  - No analizados datos de los proxies regionales
  - Tampoco hay datos dentro de una organización
- Para roamings internacionales (no sólo ES)
  - Resumen últimos 3 meses sólo
  - Sólo la información de los países participando en la actual fase de piloto
    - AT, BE, BG, CH, CZ, DE, DK, ES, FI, HR, IE, IT, LU, NL, PL, PT, RS, SK, UK

OK / FAIL



Datos en valores absolutos
Periodo: octubre 2010 -septiembre 2011

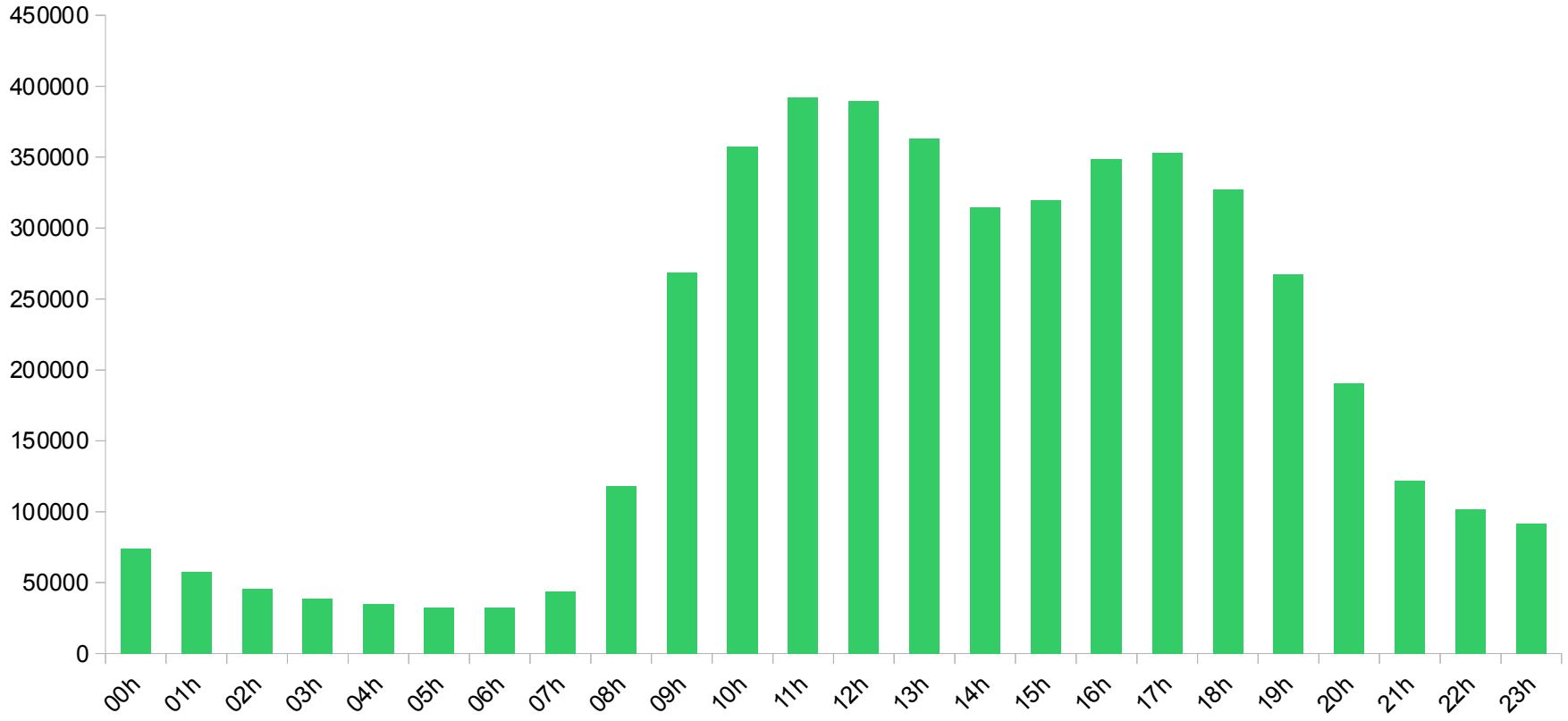
Autenticaciones satisfactorias



Red IRIS

Datos en valores absolutos
Periodo: octubre 2010 -septiembre 2011

Hora de las conexiones

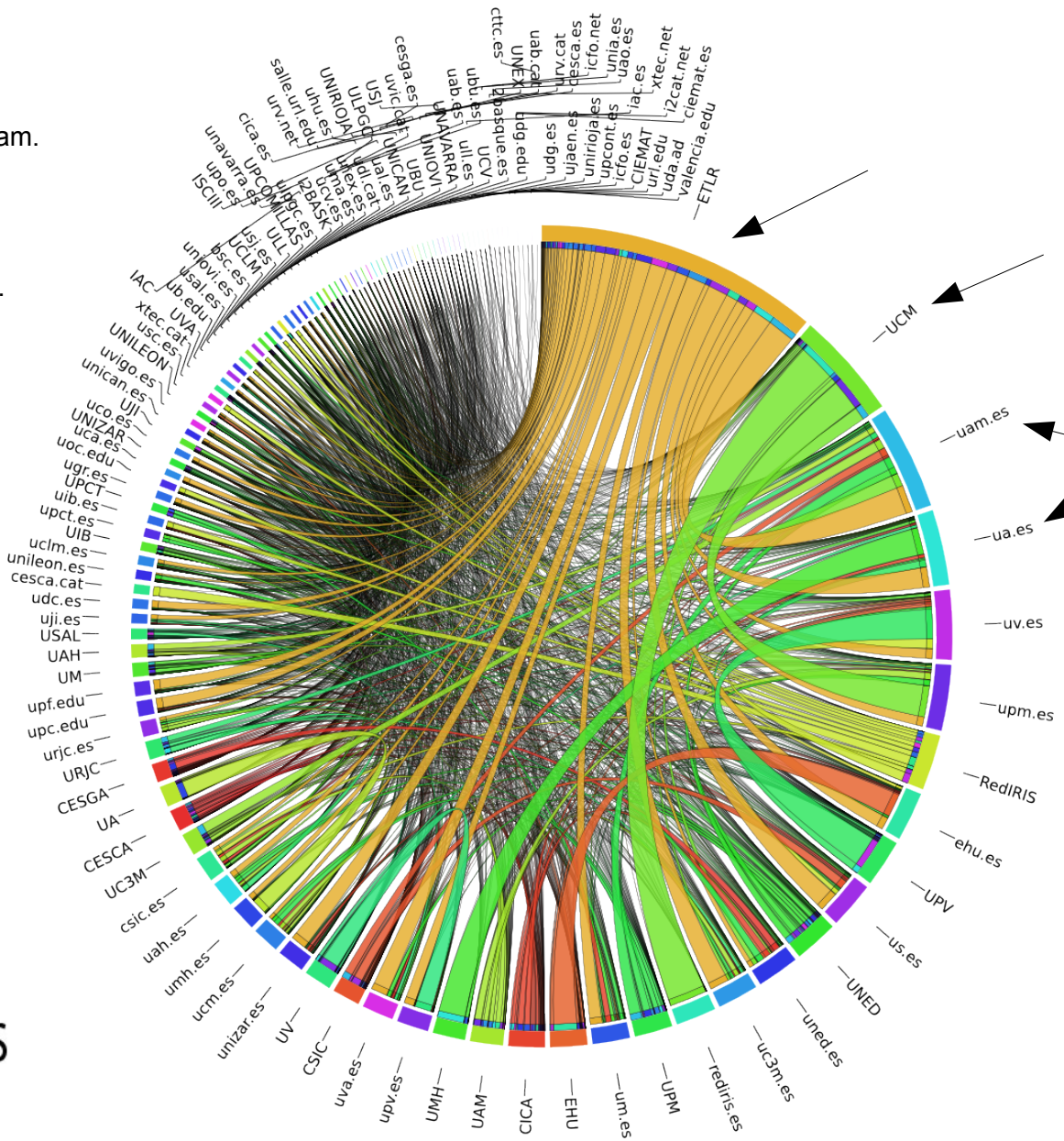


Datos en valores absolutos
Periodo: octubre 2010 -septiembre 2011

Roaming eduroam ES

Roaming a y desde dominios españoles y desde resto de eduroam. No se incluyen datos bajo los proxies regionales y CSIC

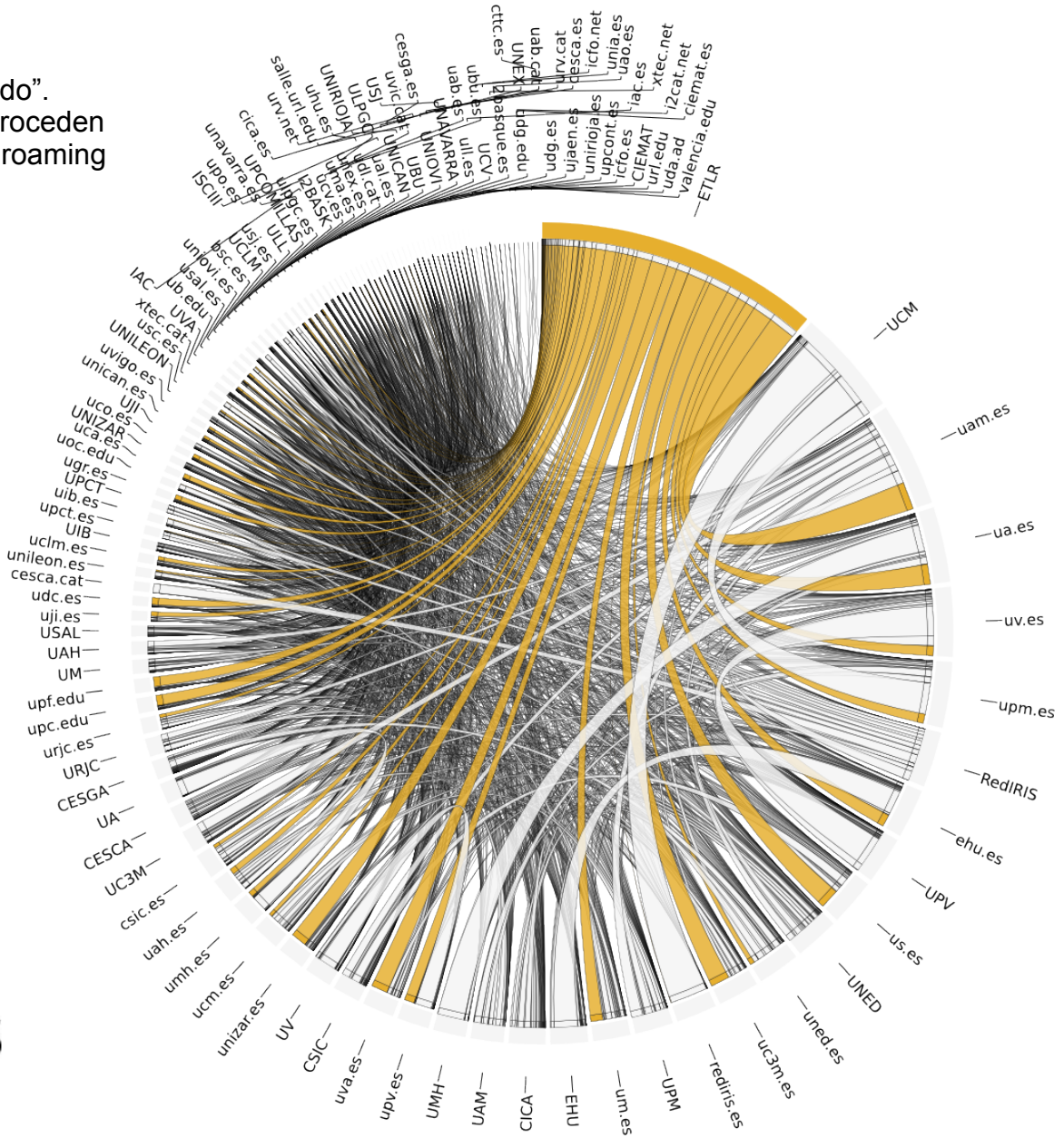
oct. 2010 – sep. 2011.



Roaming eduroam ES

“españoles por el mundo”. Dominios de los que proceden los usuarios haciendo roaming en el extranjero

oct. 2010 – sep. 2011



Roaming eduroam EU

“europeos por Europa”. Dominios de los que proceden los usuarios haciendo roaming en el extranjero y visitas a los países en el piloto. Se omiten datos de roaming intrafederación.