La nueva red interna de la BUS

Claudio J. Arjona
con la colaboración de Francisco Sánchez

Jornada de Buenas Prácticas. 18 de Diciembre, 2017

UNIVERSIDAD DE SEVILLA
VICERRECTORADO DE INVESTIGACIÓN

UNIVERSIDAD D SEVILLA
Biblioteca

Indice

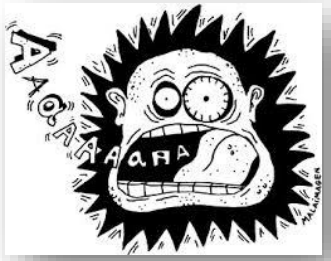
0

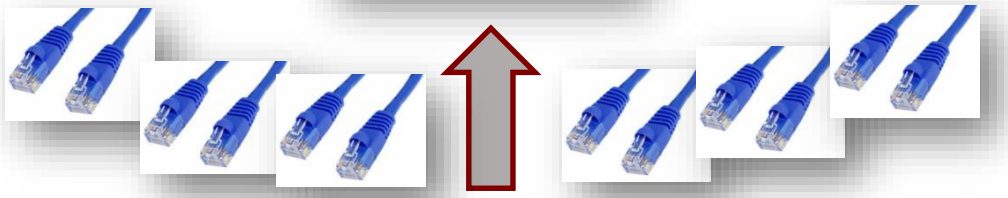
Razones del cambio

Causas mayores

Falta de direcciones IP públicas

Petición de devolución al SIC/US de la subred 150.214.216.*





Solicitud de nuevos puntos de conexión a red por parte de las bibliotecas: más personal y nuevos equipos conectables, como la impresoras multifunción

Razones del cambio

1

Seguridad Informática

Intentos de acceso continuos

Observar hora y usuario : root – misma IP atacante

```
14 09:53:03 localhost sshd[39715]: Failed password for root from 218.65.30.40 port 7290 ssh2
14 09:53:03 localhost sshd[39715]: error: maximum authentication attempts exceeded for root from 218.65.30.40 port 7290 ssh2 [preauth]
14 09:53:03 localhost sshd[39715]: Disconnecting: Too many authentication failures [preauth]
14 09:53:03 localhost sshd[39715]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=218.65.30.40  user=root
14 09:53:03 localhost sshd[39715]: PAM service(sshd) ignoring max retries; 6 > 3
14 09:53:07 localhost sshd[39765]: reverse mapping checking getaddrinfo for 40.30.65.218.broad.xy.jx.dynamic.163data.com.cn [218.65.30.40] failed - POSSIBLE BR
-IN ATTEMPT!
14 09:53:07 localhost sshd[39765]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=218.65.30.40  user=root
14 09:53:07 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:09 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:10 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:12 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:13 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:15 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:16 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:18 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:19 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:21 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:22 localhost sshd[39765]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:24 localhost sshd[39765]: Failed password for root from 218.65.30.40 port 10260 ssh2
14 09:53:24 localhost sshd[39765]: error: maximum authentication attempts exceeded for root from 218.65.30.40 port 10260 ssh2 [preauth]
14 09:53:24 localhost sshd[39765]: Disconnecting: Too many authentication failures [preauth]
14 09:53:24 localhost sshd[39765]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=218.65.30.40  user=root
14 09:53:24 localhost sshd[39765]: PAM service(sshd) ignoring max retries; 6 > 3
14 09:53:27 localhost sshd[39769]: reverse mapping checking getaddrinfo for 40.30.65.218.broad.xy.jx.dynamic.163data.com.cn [218.65.30.40] failed - POSSIBLE BR
-IN ATTEMPT!
14 09:53:28 localhost sshd[39769]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=218.65.30.40  user=root
14 09:53:28 localhost sshd[39769]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:30 localhost sshd[39769]: Failed password for root from 218.65.30.40 port 53802 ssh2
14 09:53:31 localhost sshd[39769]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
14 09:53:33 localhost sshd[39769]: Failed password for root from 218.65.30.40 port 53802 ssh2
```

Razones del cambio

1

Seguridad Informática

Intentos de acceso continuos

Observar hora y usuarios

Varias IPs atacantes

Razones del cambio

1

Seguridad Informática

Intentos de acceso continuos

Observar hora y usuarios

Varias IPs atacantes

```
Apr 6 08:57:49 | faild password user root | 181.112.28.254 | exec |
Apr 6 09:08:01 | warning no id | 113.108.21.16
Apr 6 09:44:59 | warning no id | 202.170.80.40
Apr 6 10:04:24 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:25 | warning no id | 93.185.115.133
Apr 6 10:04:27 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:29 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:32 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:34 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:37 | warning invalid user admin | 186.130.69.38
Apr 6 10:04:37 | to many auth fail | 186.130.69.38 | exec | /sbin/ipt
Apr 6 10:45:45 | warning invalid user usuario | 190.173.156.188
Apr 6 10:45:47 | warning invalid user usuario | 190.173.156.188
Apr 6 10:45:49 | warning invalid user usuario | 190.173.156.188
Apr 6 10:45:51 | warning invalid user usuario | 190.173.156.188
Apr 6 10:45:53 | warning invalid user usuario | 190.173.156.188
```

Seguridad Informática

Intentos de acceso continuos

Observar hora y usuarios

Una IP atacante con lista de usuarios

```
13:03:14 app-1 sshd[25253]: pam_unix(sshd:auth): check pass; user unknown
13:03:14 app-1 sshd[25253]: pam_unix(sshd:auth): authentication failure; l
13:03:16 app-1 sshd[25253]: Failed password for invalid user temp from 8.1
13:03:16 app-1 sshd[25255]: Invalid user carla from 8.12.45.242
13:03:16 app-1 sshd[25255]: pam_unix(sshd:auth): check pass; user unknown
13:03:16 app-1 sshd[25255]: pam_unix(sshd:auth): authentication failure; l
13:03:18 app-1 sshd[25255]: Failed password for invalid user carla from 8.
13:03:18 app-1 sshd[25257]: Invalid user laura from 8.12.45.242
13:03:18 app-1 sshd[25257]: pam_unix(sshd:auth): check pass; user unknown
13:03:18 app-1 sshd[25257]: pam_unix(sshd:auth): authentication failure; l
13:03:20 app-1 sshd[25257]: Failed password for invalid user laura from 8.
13:03:21 app-1 sshd[25259]: Invalid user joana from 8.12.45.242
13:03:21 app-1 sshd[25259]: pam_unix(sshd:auth): check pass; user unknown
13:03:21 app-1 sshd[25259]: pam_unix(sshd:auth): authentication failure; l
13:03:23 app-1 sshd[25259]: Failed password for invalid user joana from 8.
13:03:23 app-1 sshd[25261]: Invalid user isabel from 8.12.45.242
13:03:23 app-1 sshd[25261]: pam_unix(sshd:auth): check pass; user unknown
13:03:23 app-1 sshd[25261]: pam_unix(sshd:auth): authentication failure; l
13:03:25 app-1 sshd[25261]: Failed password for invalid user isabel from 8
13:03:25 app-1 sshd[25263]: Invalid user antonio from 8.12.45.242
13:03:25 app-1 sshd[25263]: pam_unix(sshd:auth): check pass; user unknown
13:03:25 app-1 sshd[25263]: pam_unix(sshd:auth): authentication failure; l
13:03:26 app-1 sshd[25263]: Failed password for invalid user antonio from
13:03:27 app-1 sshd[25265]: Invalid user david from 8.12.45.242
13:03:27 app-1 sshd[25265]: pam_unix(sshd:auth): check pass; user unknown
```

Proteger las impresoras de red

PROTEGER A LAS IMPRESORAS:
CUALQUIERA PODÍA IMPRIMIR DESDE EL "MUNDO MUNDIAL"

Un segundo paso:
Que cada uno solo vea las impresoras que debe usar para impedir cruce de documentos entre bibliotecas → firewall local (problema con el correo electrónico desde la impresora)

Razones del cambio

1

No delegar la seguridad

No se pretende volver loco al personal con tareas y responsabilidades complejas

¿Quién sabe activar y parametrizar el firewall de Windows?

Acciones realizadas

2

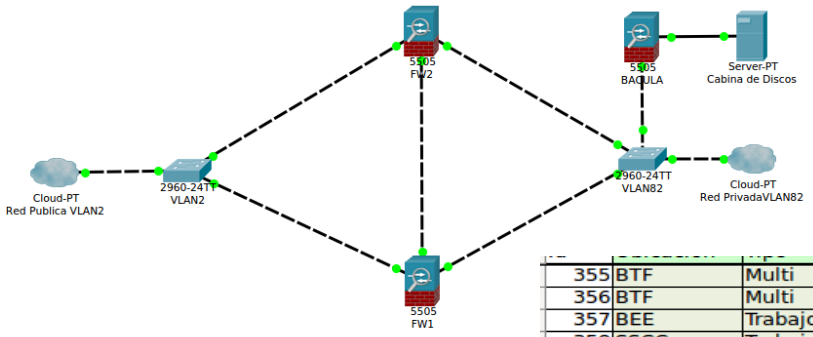
Inversiones en hardware

- **Dos servidores como firewall**
- **Un conmutador para comunicaciones**
- **Un rack en el SIC**

Acciones realizadas

2

Diseño e implementación



- Software libre
- Colaboración del Dpto. de Telemática de Teleco de Cartuja
- Becario especializado, alumno de Teleco
- Coordinación de Javier Escudero

Recogida de datos

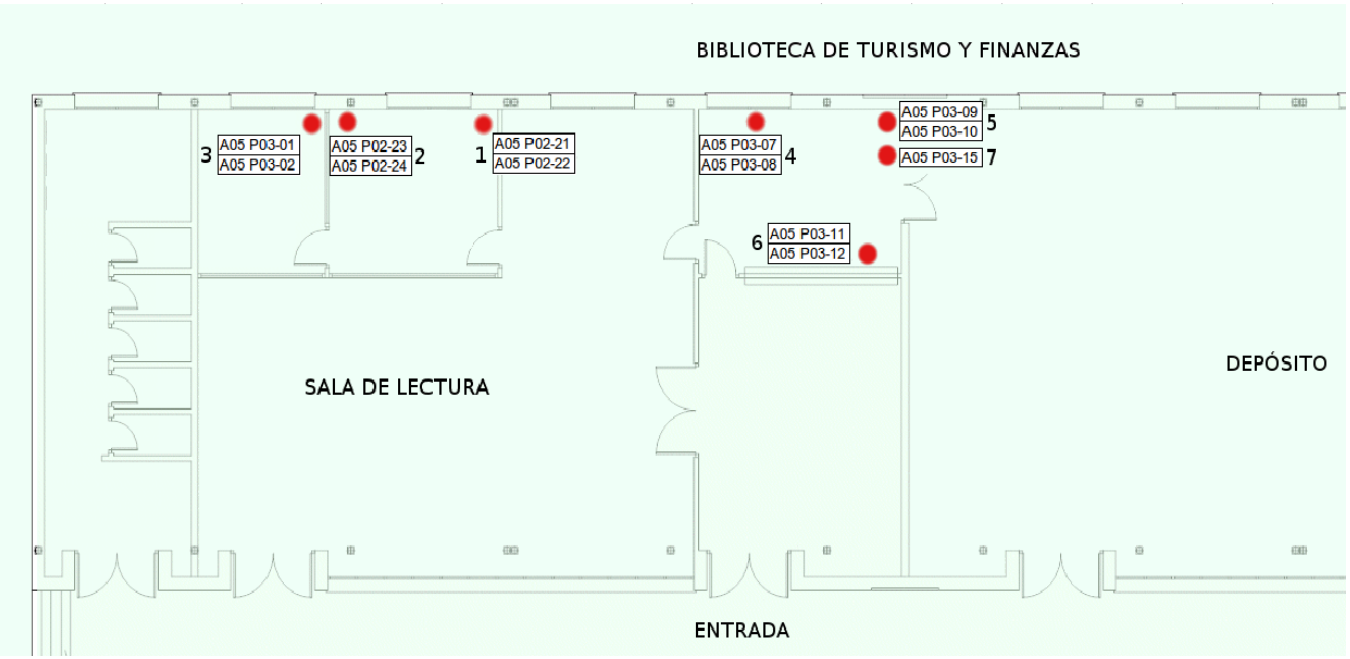
Becarios de informática
Bibliotecarios, TABs y TEBs
Coordinación de Paco Sánchez

ORDEN
CONSTANCIA
LIMPIEZA

355	BTF	Multi	1605	00:25:36:36:A4:B8		192.168.197.105
356	BTF	Multi	1605	28:80:23:CD:84:19		192.168.197.106
357	BEE	Trabajo	701	00:15:B7:33:27:6A		192.168.196.135
358	SSCC	Trabajo	1801	B4:B5:2F:B9:4C:52		192.168.195.207
359	SSCC	Trabajo	1801	70:71:BC:90:16:2D		192.168.195.208
360	SSCC	Trabajo	1801	80:FA:5B:08:EA:49		192.168.195.209
361	SSCC	Trabajo	1801	68:5b:35:d3:f1:52		192.168.195.210
362	SSCC	Trabajo	1801	70:71:BC:90:4F:09		192.168.195.211
363	SSCC	Trabajo	1801	70:71:BC:90:15:CC		192.168.195.212
364	BBA	Trabajo	201	00:1E:68:60:00:4A		192.168.196.35
365						
366						
367	SSCC	Multi	1805	00:00:00:00:00:04		192.168.195.112
368						
369	SIT	Trabajo	1901	00:24:1D:3F:A6:41		192.168.199.199
370	SIT	Trabajo	1901	00:1C:C0:4F:CA:F1		192.168.199.200
371	SIT	Trabajo	1901	DC:4A:3E:51:70:07		192.168.199.201
372	SIT	Trabajo	1901	DC:4A:3E:51:0B:3B		192.168.199.202
374	SIT	Trabajo	1901	00:1C:98:01:00:62		192.168.199.203
375	SIT	Trabajo	1901	00:24:1D:70:23:48		192.168.199.204
376	SIT	Trabajo	1901	70:71:BC:93:83:71		192.168.199.205
377	SIT	Trabajo	1901	00:24:1D:3F:5C:F2		192.168.199.206
378	SIT	Trabajo	1901	70:85:C2:30:1E:96		192.168.199.207
379						
380						
381	SSCC	Trabajo	1801	00:24:1d:96:21:7b		192.168.195.213
382	SSCC	Trabajo	1801	20:25:64:4F:88:BE		192.168.195.214
383	SSCC	Trabajo	1801	B4:B5:2F:B0:2C:2B		192.168.195.215
384	SSCC	Multi	1805	38:63:BB:06:76:AF		192.168.195.113
385	SSCC	Trabajo	1801	D8:97:BA:8C:D6:19		192.168.195.216
386	SSCC	Trabajo	1801	70:71:BC:93:83:43		192.168.195.217
387	SSCC	Trabajo	1801	70:71:BC:93:85:0C		192.168.195.218

Mucho trabajo de la BUS

- Localizar planos
- Anotar rosetas e identificarlas
- Ver su VLAN
- Anotar puesto a puesto la roseta
- Creación de un EXCEL por centro
- Asignación de IP pública por centro y función



ID	EQUIPO	MAC	ROSETA	S.O.	CONTACTO	FUNCIONALIDAD
1	FTFTRAB126	00:24:1D:96:04:23	A05 P02-22	W8	VINAGRE LOBO JOSÉ MANUEL	PC_TRABAJO
2	FTFTRAB153	70:71:BC:90:11:D8	A05 P02-24	W8	Surián Ruiz Ana María	PC_TRABAJO
3	FTFTRAB125	70:71:BC:93:80:2C	A05 P03-02	W7	Clemente Castillana Rosa	PC_TRABAJO
4	FTFPREST146*	68:B5:99:C2:77:A1	A05 P03-08	W SERVER 2008	VINAGRE LOBO JOSÉ MANUEL	PC_PRESTAMO
5	FTFPREST145	38:60:77:25:73:96	A05 P03-09	W7	VINAGRE LOBO JOSÉ MANUEL	PC_PRESTAMO
5	FTFPRIN01	38:60:77:25:68:30	A05 P03-10		VINAGRE LOBO JOSÉ MANUEL	MULTIFUNCION
6			A05 P03-11			PANTALLA
6	FTFPREST144	B4:B5:2F:B0:7A:3E	A05 P03-12	W7	VINAGRE LOBO JOSÉ MANUEL	PC_PRESTAMO

Ingeniería Informática

UBICACIÓN	EQUIPO	MAC	ROSETA	FUNCIONALIDAD
1	EIIPREST086	20:25:64:4F:88:C0	A8 P7-02	PC_PRESTAMO
3	EIIPREST076	E0:69:95:F4:3D:2D	A8 P7-06	PC_PRESTAMO
4	EIITRAB084	E0:69:95:F4:33:46	A8 P7-08	PC_TRABAJO
5	EIITRAB083	E0:69:95:F4:52:7B	A8 P7-10	PC_TRABAJO
6	EIITRAB068	70:71:BC:93:83:32	A8 P7-12	PC_PRESTAMO
8	EIITRAB082	B4:B5:2F:B0:7A:0F	A8 P7-16	PC_TRABAJO
9	EIIPRIN071	28:80:23:CE:13:F5	A8 P7-22	MULTIFUNCION

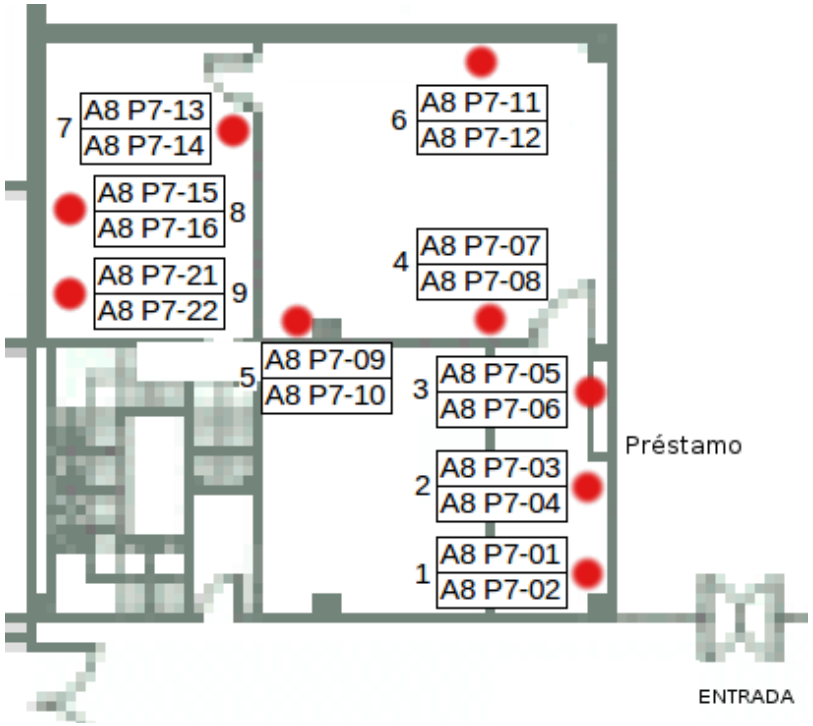


Foto actual

Logros

Usamos ¼ de las IPs públicas

Devolvimos las 150.214.216.*

Reasignamos las IPs restantes: 150.214.182.*

Por cada IP pública tenemos varias IPs privadas

Es un modelo para otras secciones de la Administración de la US

Impresoras sin IP externa → no accesibles desde fuera de la BUS

Muchas IPs privadas sobrantes

- **Asignadas por centro**
- **Cada centro tiene sus IPs libres**

IPs públicas sobrantes, para nuevos proyectos, aplicaciones y servidores

Foto actual

3

CUIDADO!!!

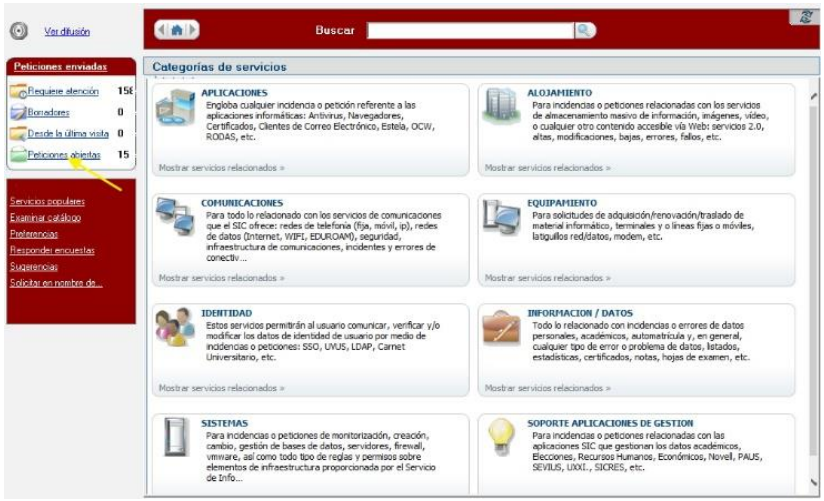
Las cosas SOLO FUNCIONAN en las rosetas de la VLAN82

NO REUSAR LA 182

Cada centro tiene un conjunto de IPs para MOSTRADOR, otro para TRABAJO y otro para las MULTIFUNCIONES

SOS

La IP antigua de un PC o impresora ahora es la IP de TODOS LOS PCs de trabajo de la biblioteca de un centro, por ejemplo.



IP de acceso a recursos electrónicos: IP pública
IP del ordenador: privada y FIJA
Para el SOS: el PC pide red por DHCP
Problemas de red NO físicos: Sección I&T

Procedimientos

Sustitución de ordenador, placa base

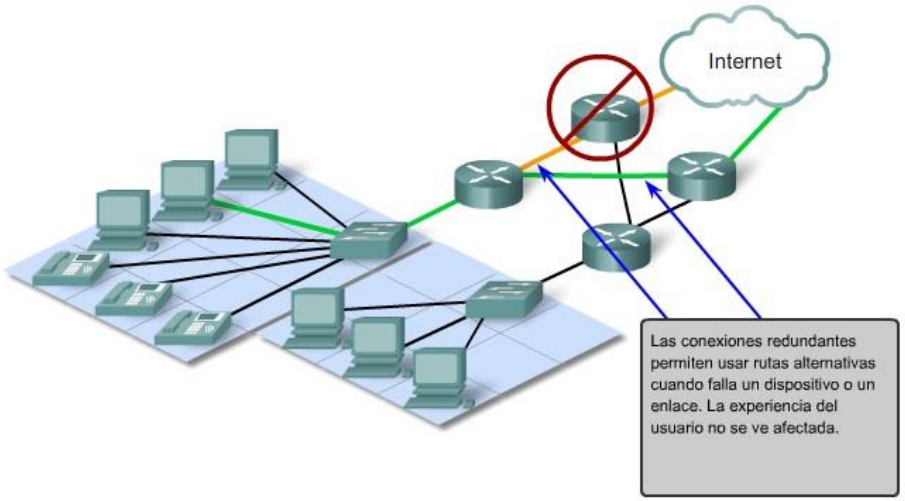
- Usar la misma roseta
- Mandarnos la nueva MAC
- Si se necesita nueva roseta:
  - Usar una de VLAN82
  - Solicitar paso de VLAN2 a VLAN 82
  - Si la roseta es de PC de consulta en sala, solicitar paso a VLAN82

Poner nuevo ordenador o portátil de trabajo

- Solicitud previa de paso de roseta a VLAN82
- La MAC debemos tenerla nosotros

Acciones pendientes

Volver a reasignar IPs públicas



Tolerancia fallos

ENVIAR INFORMACIÓN DEFINITIVA A LAS BIBLIOTECAS

Tolerancia a fallas

Asignar IPs públicas a su cometido real

Pasar resto de rosetas de mostrador y trabajo a VLAN82

(hay rosetas no conectadas)

Muchas gracias por vuestra atención

Claudio J. Arjona
Paco Sánchez Avellaneda
Javier Escudero
Manuel Barea
Becarios
Jesús Bocanegra
Yago Fernández
Adrián Camacho

Agradecimientos
Profesores del
Departamento de
Ingeniería Telemática
Rafael Estepa
Germán Madinabeitia
Y a la ***Fundación AICIA***

UNIVERSIDAD DE SEVILLA

UNIVERSIDAD D SEVILLA
Biblioteca