Aplicación de Control de Puerto Lógicos

Índice

- Proyecto Global
  - ¿Qué queremos conseguir?
  - Esquema Global de Funcionamiento
- Aplicación de Puertos Lógicos TCP/UDP
  - Problemática
  - Cómo funciona
  - Qué hemos desarrollado
- Base de Datos
  - Diseño
  - Aplicación
- Conclusiones

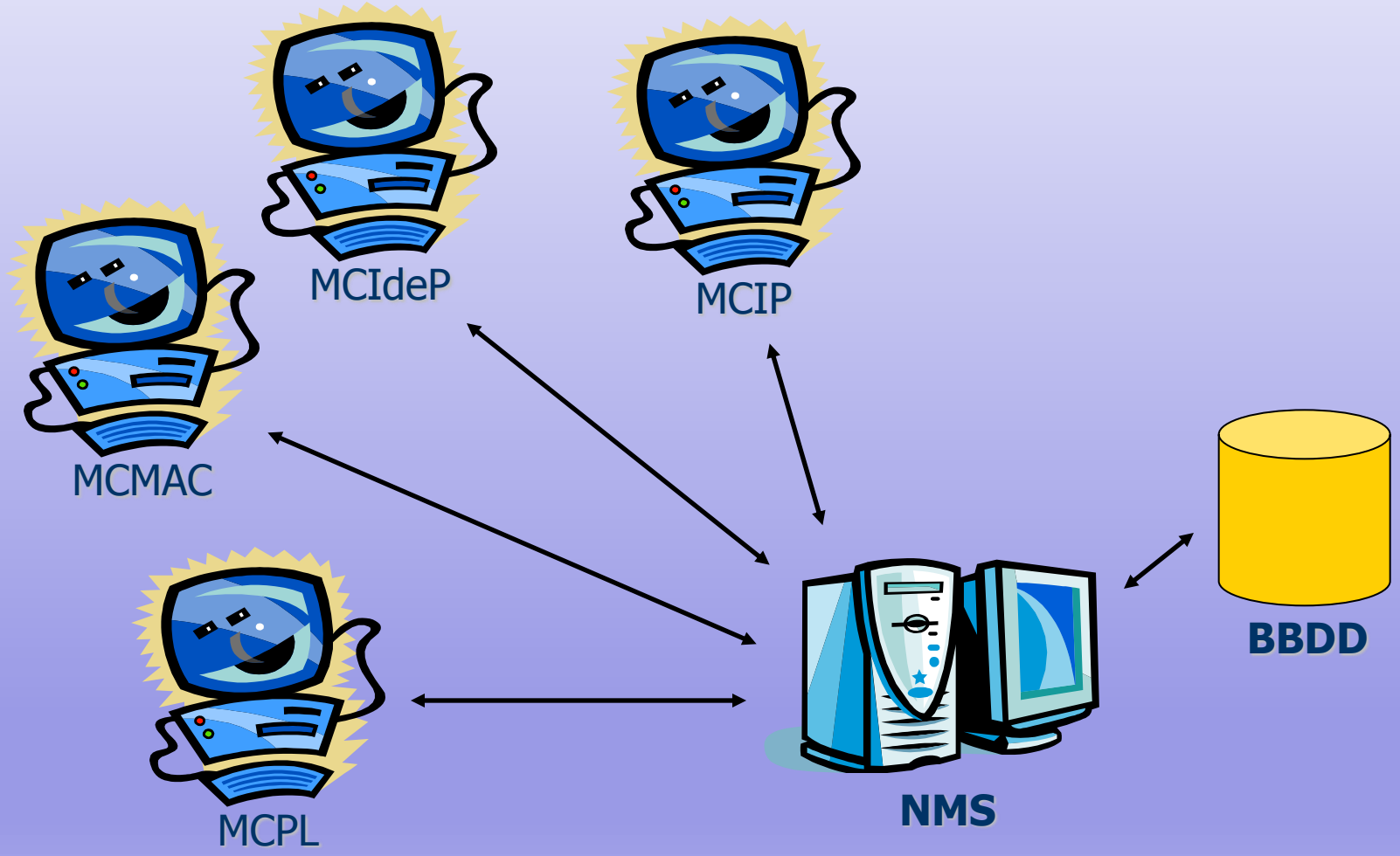
Proyecto Global

¿Qué queremos conseguir?

- Control de inactividad de los puertos (MCIdeP)
- Control por dirección MAC (MCMAC)
- Control por dirección IP (MCIP)
- Control de puertos lógicos TCP y UDP (MCPL)
- Repositorio centralizado de la información de Red (BBDD)

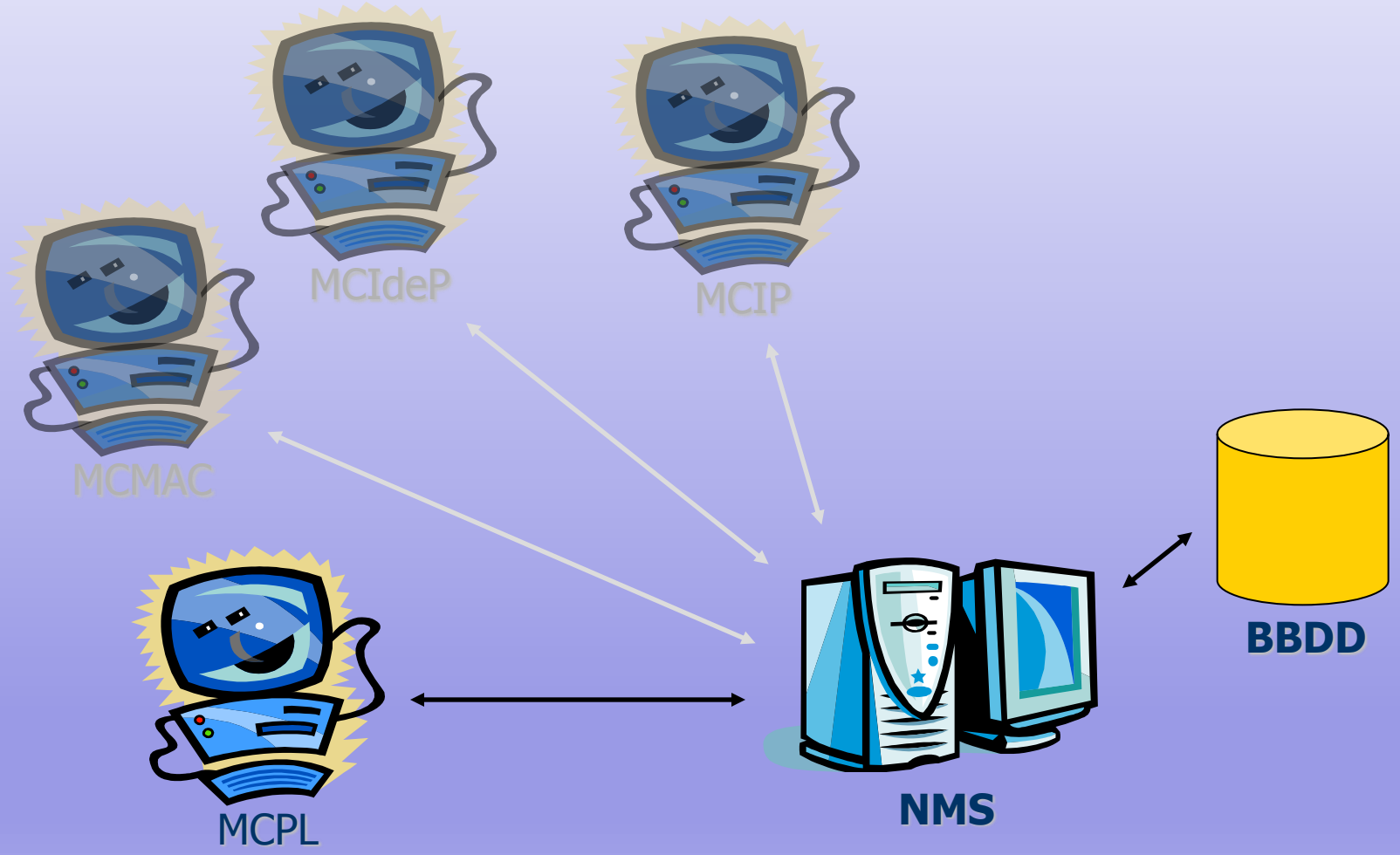
Proyecto Global

El esquema



Proyecto Global

Nuestra parte del esquema

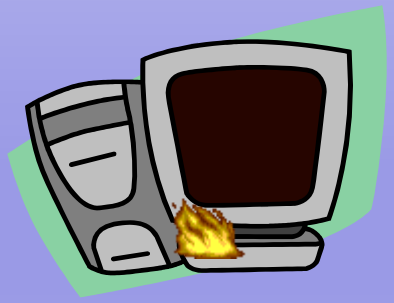


Aplicación de Puertos Lógicos

Problemática: Puerto NO Deseado

Puertos TCP Abiertos

WWW: 80
FTP: 21
POP3: 110
TELNET: 23



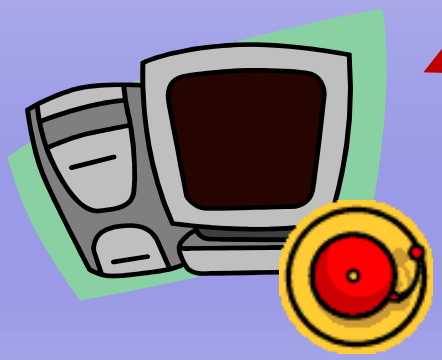
Usan Apache como servidor web…
Y esta versión tiene una vulnerabilidad…
¡Controlaré el equipo!

Aplicación de Puertos Lógicos

Problemática: Puerto NO Deseado

Puertos TCP Abiertos

WWW: 80
FTP: 21
POP3: 110
~~**TELNET: 23**~~



Usan Apache como servidor web…
Y esta versión tiene una vulnerabilidad…
¡Controlaré el equipo!

Aplicación de Puertos Lógicos

Problemática: Cae uno de Nuestros Puertos

Puertos TCP Abiertos

WWW: 80
FTP: 21
POP3: 110

Aplicación de Puertos Lógicos

¿Existen Soluciones?

- Netstat
- TCP-Wrapper
- Firewalls Personales
- Escáneres de puertos

Aplicación de Puertos Lógicos

Tipos de puertos

Puertos TCP Abiertos

WWW: 80
FTP: 21
POP3: 110

ORIGINALES o CONOCIDOS:
CONTROLADOS

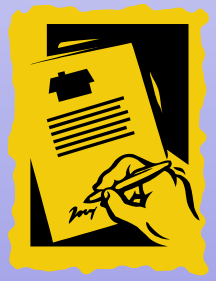
Puerto TCP Abierto

TELNET: 23

NO DESEADOS:
NO CONTROLADOS

Aplicación de Puertos Lógicos

¿Cómo funciona?



SCRIPT

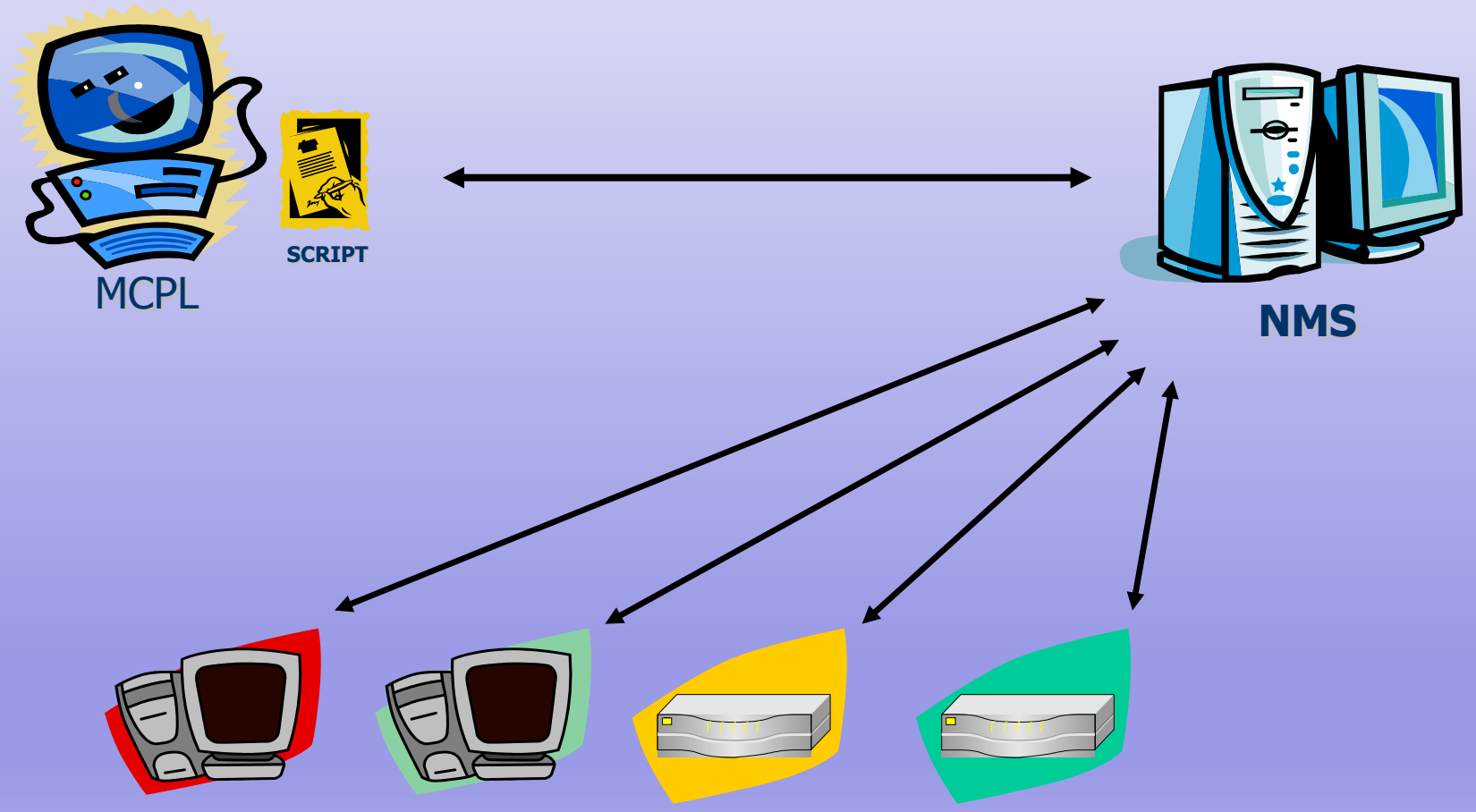
```
bash-2.04$ clisessid=$$
bash-2.04$ export clisessid
bash-2.04$ connect ss
connect: successful ss
current landscape is 0x700000

WARNING:  CLI is a powerful tool that allows a user to make changes
directly to the SPECTRUM knowledge-base without the error checking
provided by SpectroGRAPH.  Please read the accompanying CLI user
documentation before using the create, destroy, or update commands.

bash-2.04$ show
c:\win32app\SPECTRUM\vnmsh\show.exe: usage:
show    models [nhr=low_model_handle-high_model_handle] [mth=model_type_handle]
                        [mname=model_name] [lh=landscape_handle] |
        landscapes |
        types [mthr=low_mth-high_mth] [mtname mt_name] [flags U:I:D:M:U:R]
                        [lh=landscape_handle] |
        relations [lh=landscape_handle] |
        associations [mh=model_handle] |
        parents [rel=relation] [mh=model_handle] |
        children [rel=relation] [mh=model_handle] |
        attributes [-a] [attr=attribute_id[,iid=instance_id][,next1...]
                        [attrr=low_attr-high_attr] [attrname=attr_name]]
                        [mh=model_handle] |
        attributes mth=model_type_handle [attrr=low_attr-high_attr]
                        [attrname=attr_name] [flags=E:R:W:S:T:C:O:M:D:P:L]
                        [lh=landscape_handle] |
        alarms [-a] [-x] [mh=model_handle][lh=landscape_handle] |
        events [-x] [-s | -n no_events ]
                        [mh=model_handle:lh=landscape_handle] |
        inheritance mth=model_type_handle [lh=landscape_handle] |
        rules rel=relation [lh=landscape_handle] |
        enumerations [attr=attribute_id] [mth=model_type_handle]
                        [lh=landscape_handle] |
        watch [mh=model_handle]
bash-2.04$ disconnect
disconnect: successful from ss - connected for 0 hours, 0 minutes
bash-2.04$
```

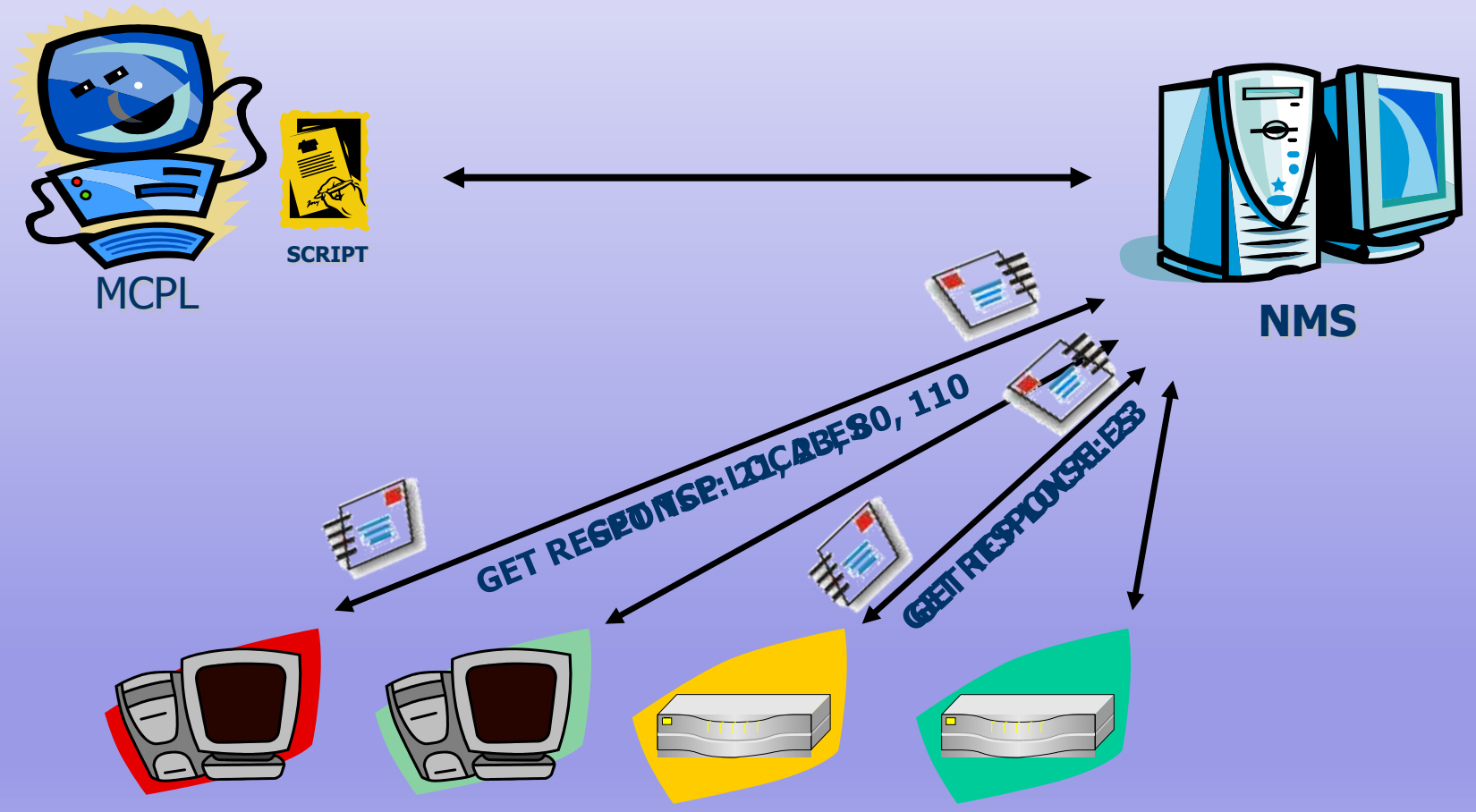
Aplicación de Puertos Lógicos

¿Cómo funciona?



Aplicación de Puertos Lógicos

¿Cómo funciona?

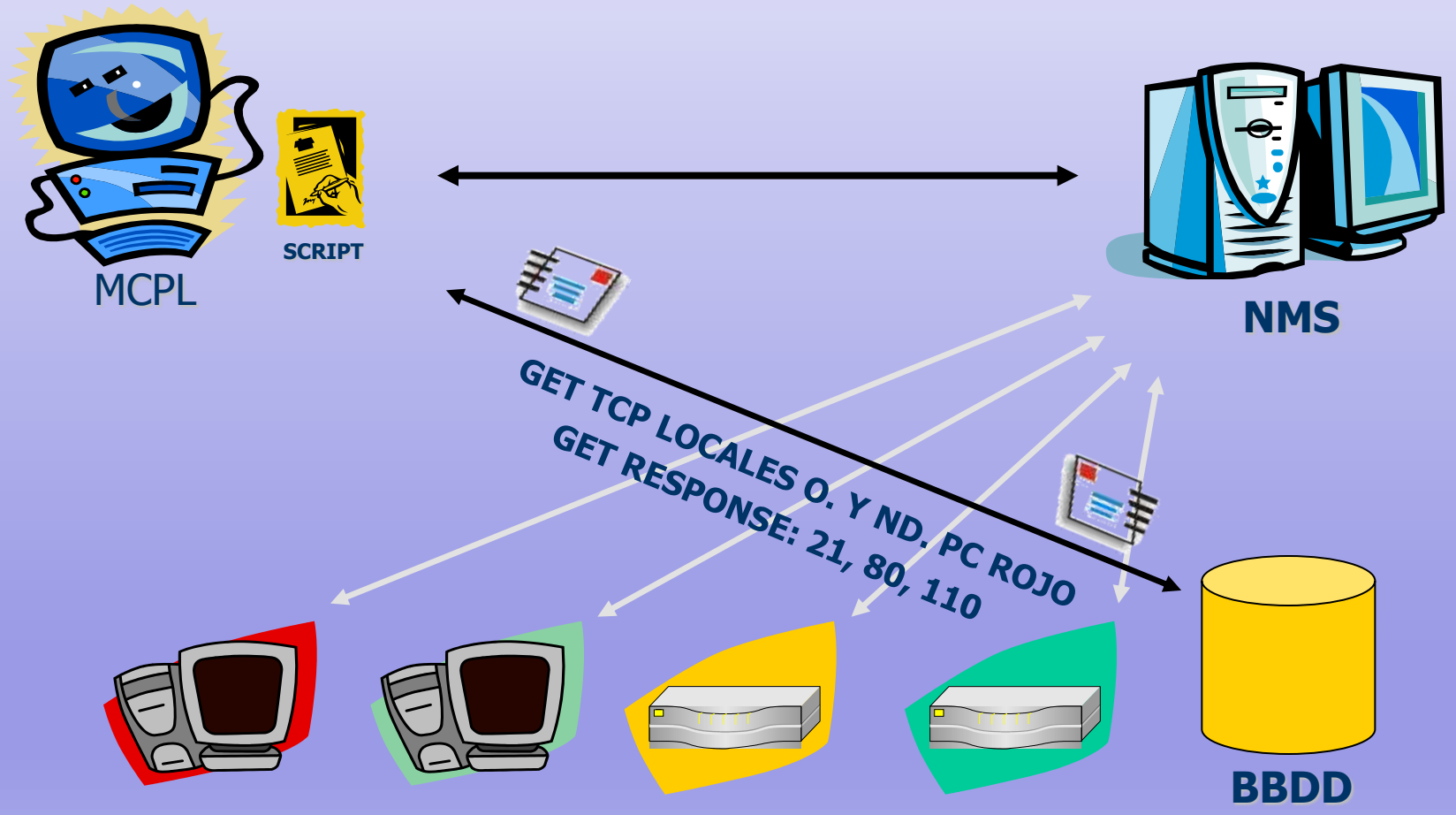


Aplicación de Puertos Lógicos

¿Cómo funciona?

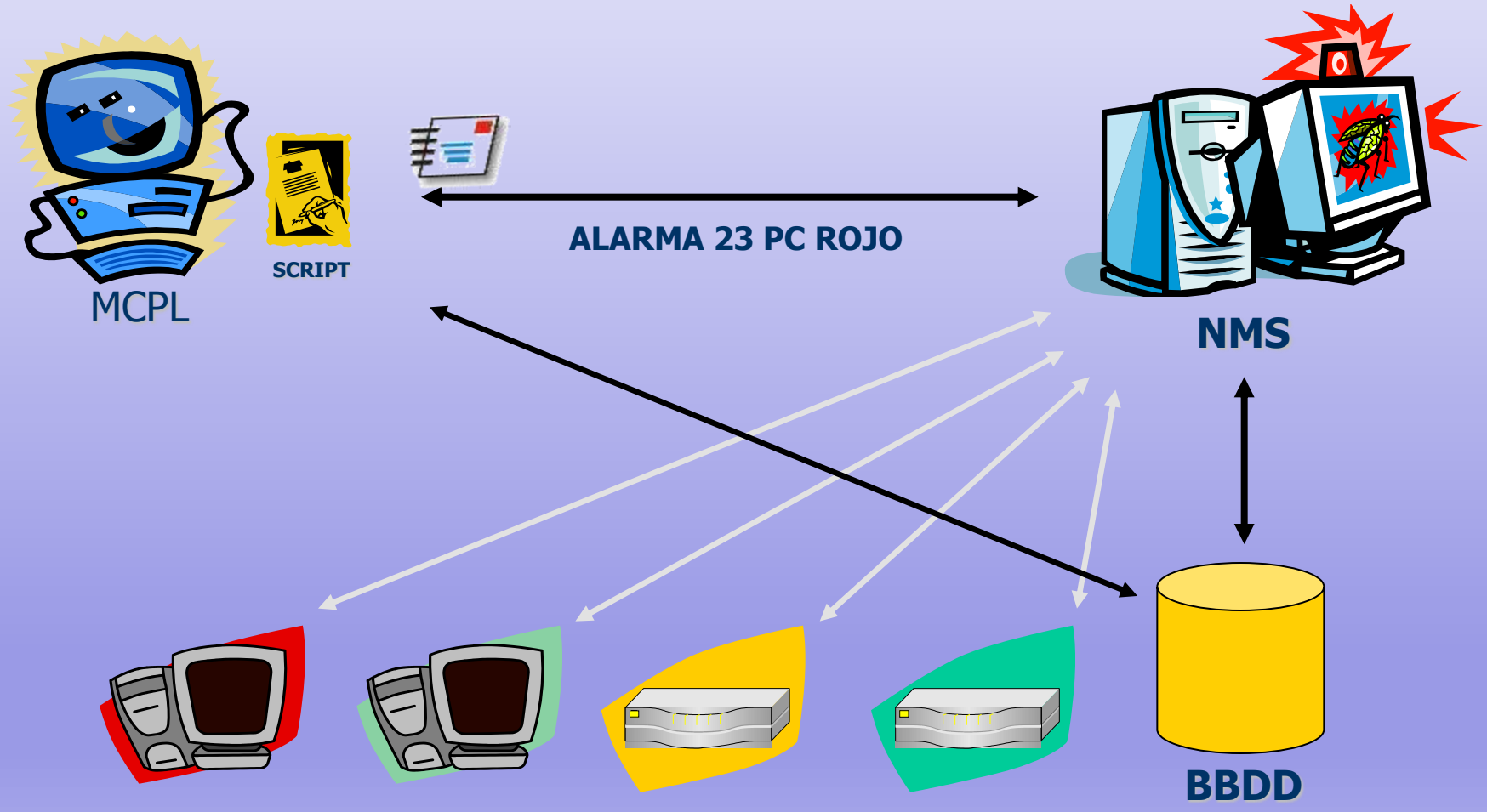
Aplicación de Puertos Lógicos

¿Cómo funciona?



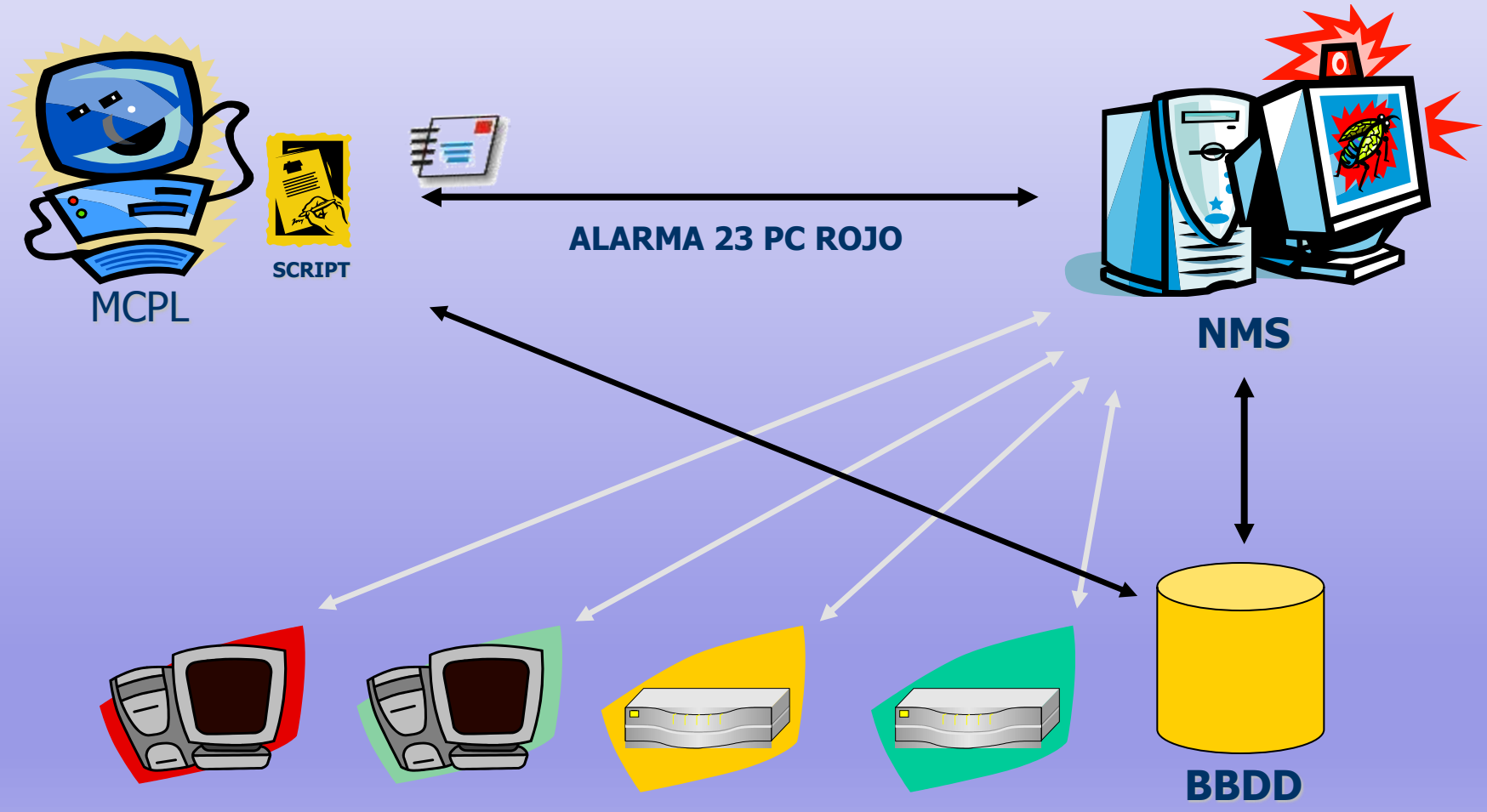
Aplicación de Puertos Lógicos

¿Cómo funciona?



Aplicación de Puertos Lógicos

¿Cómo funciona?

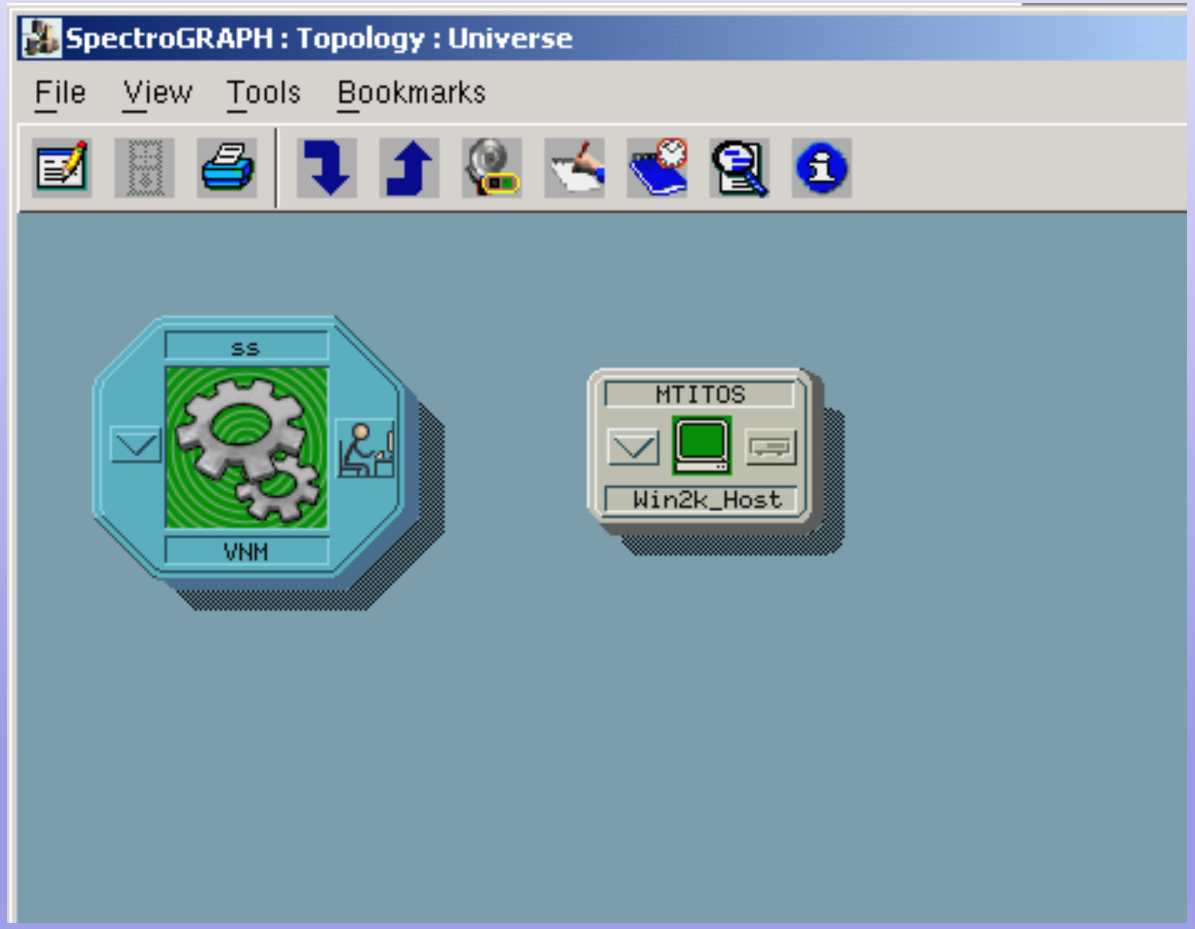


Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?

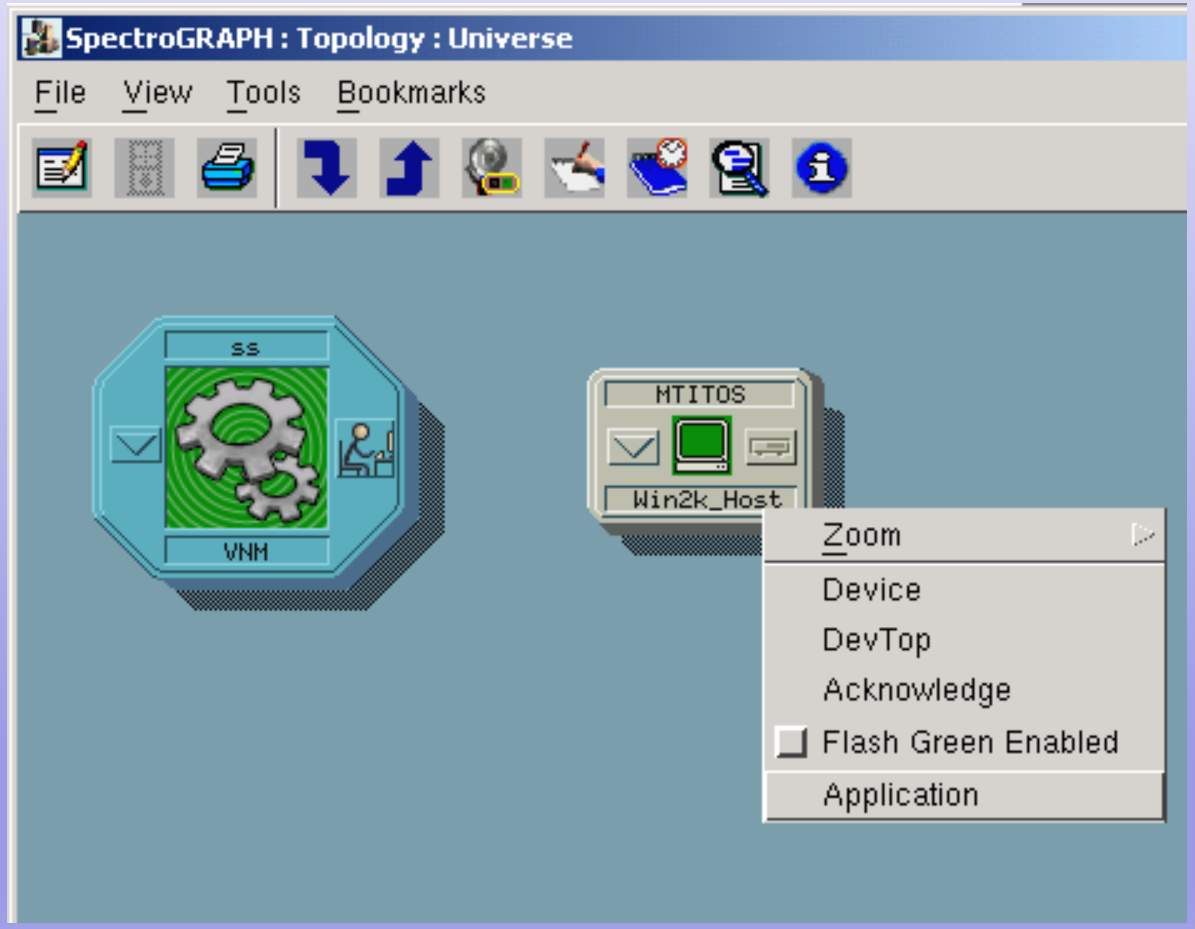
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



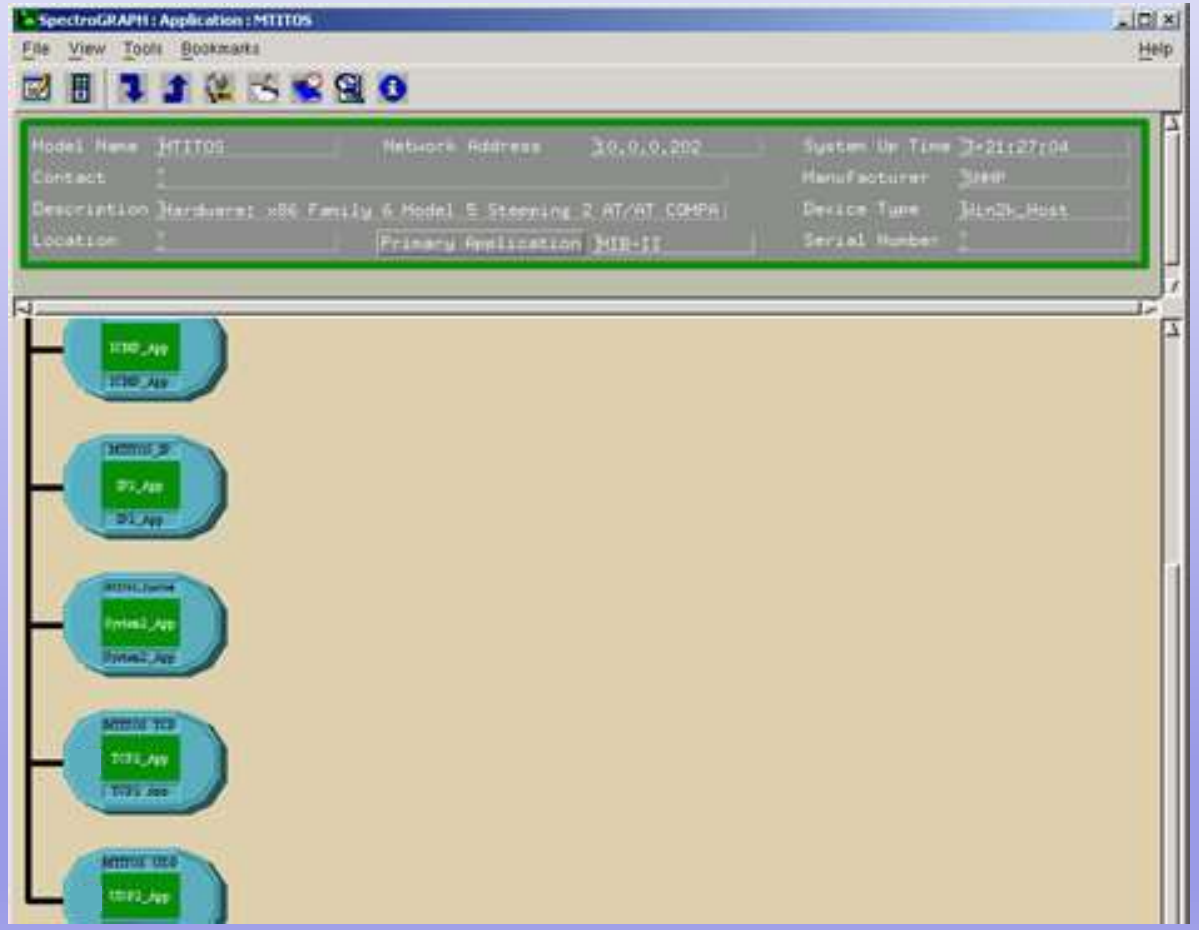
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



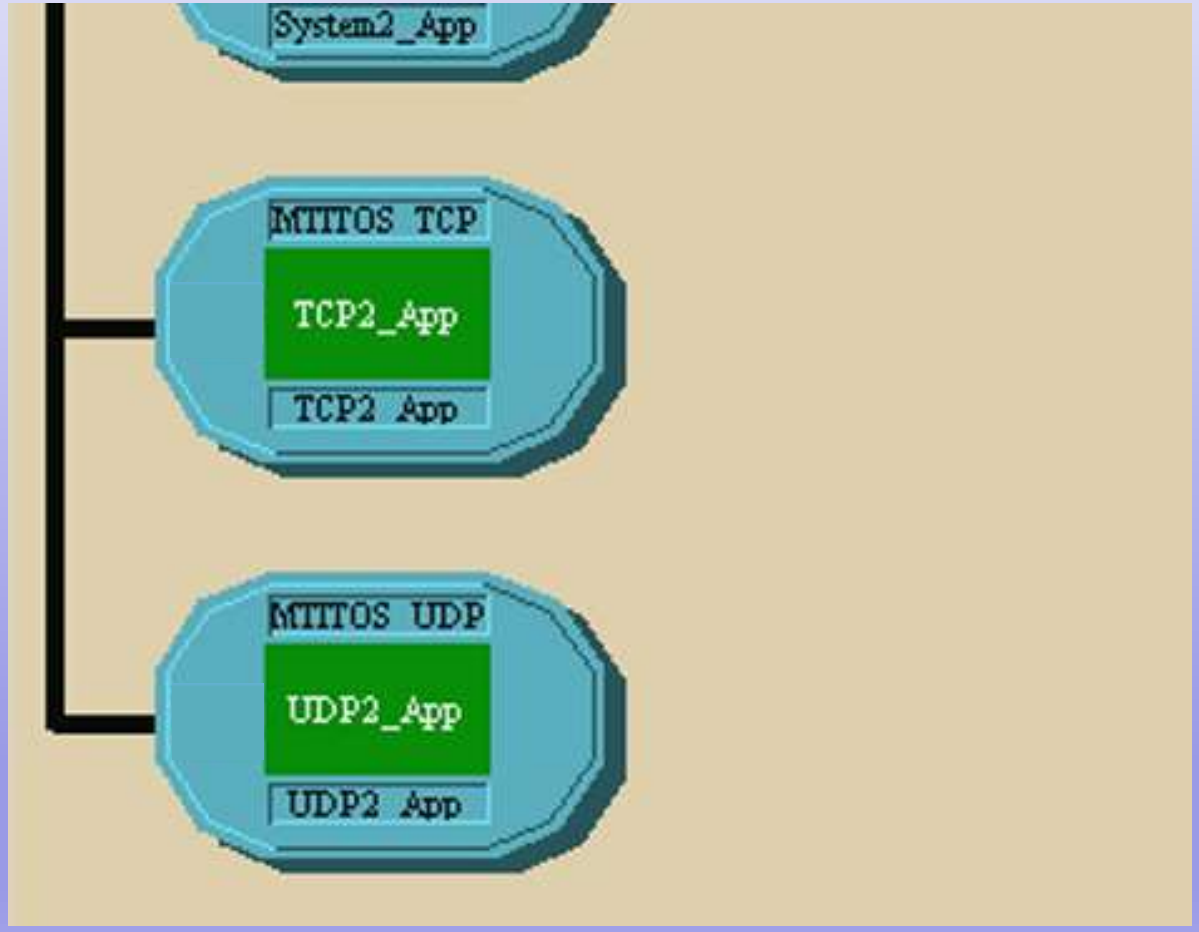
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



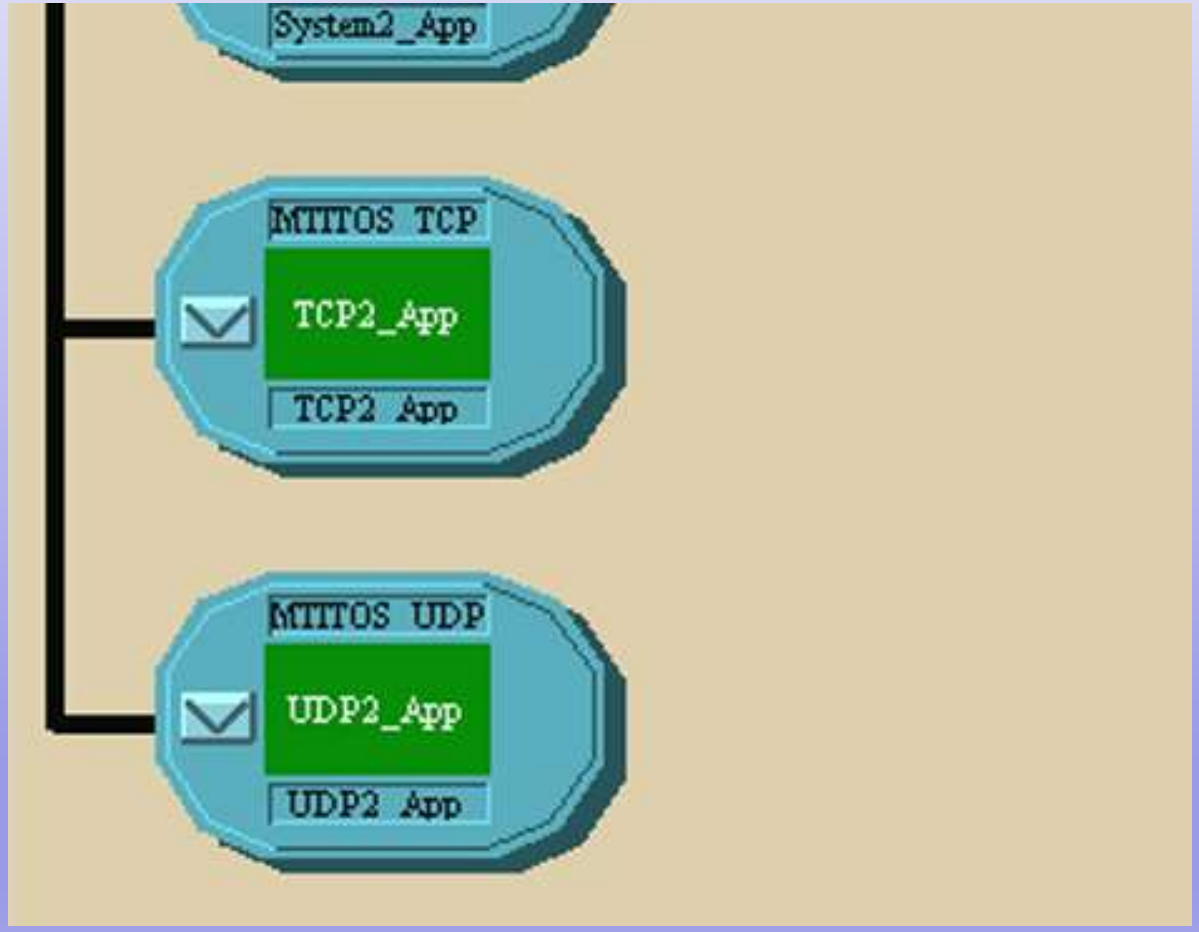
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



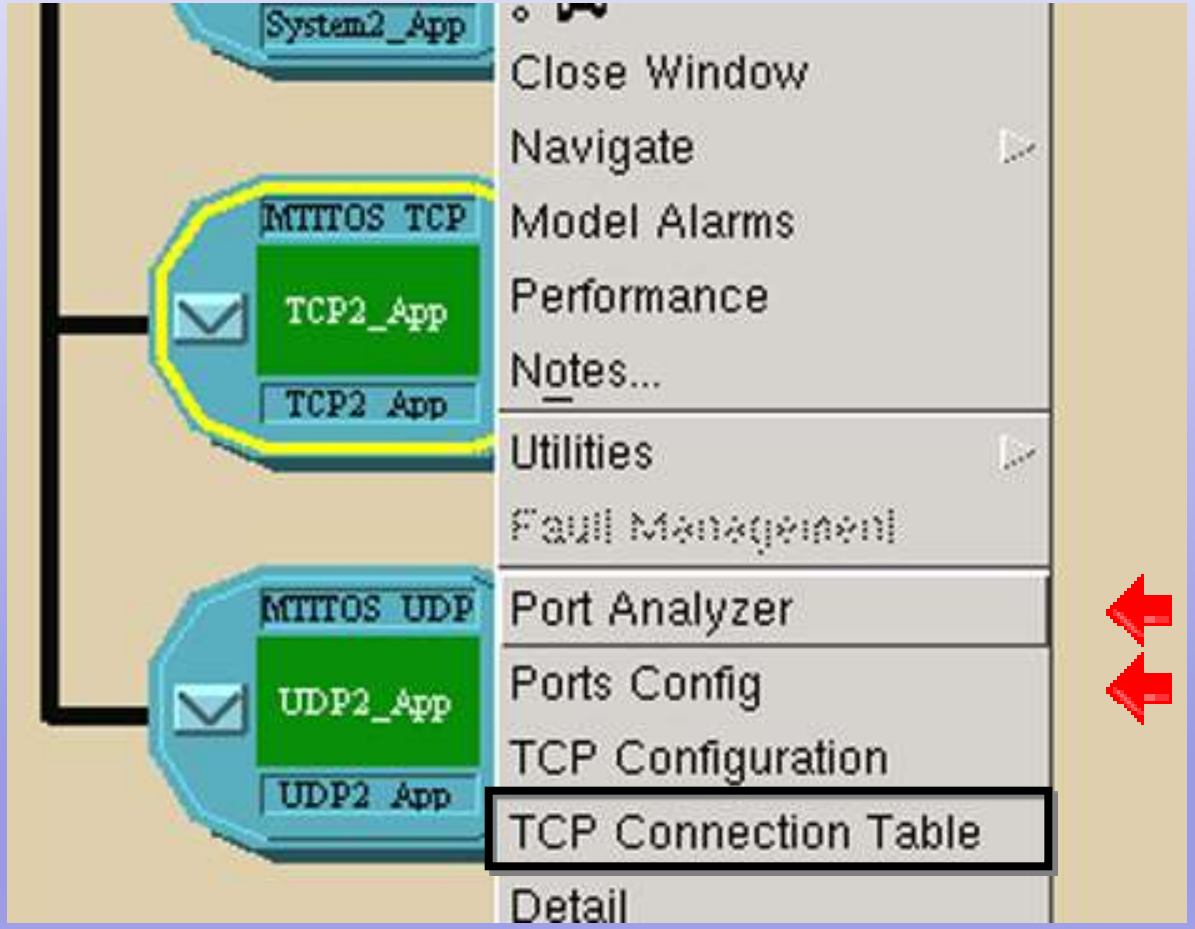
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



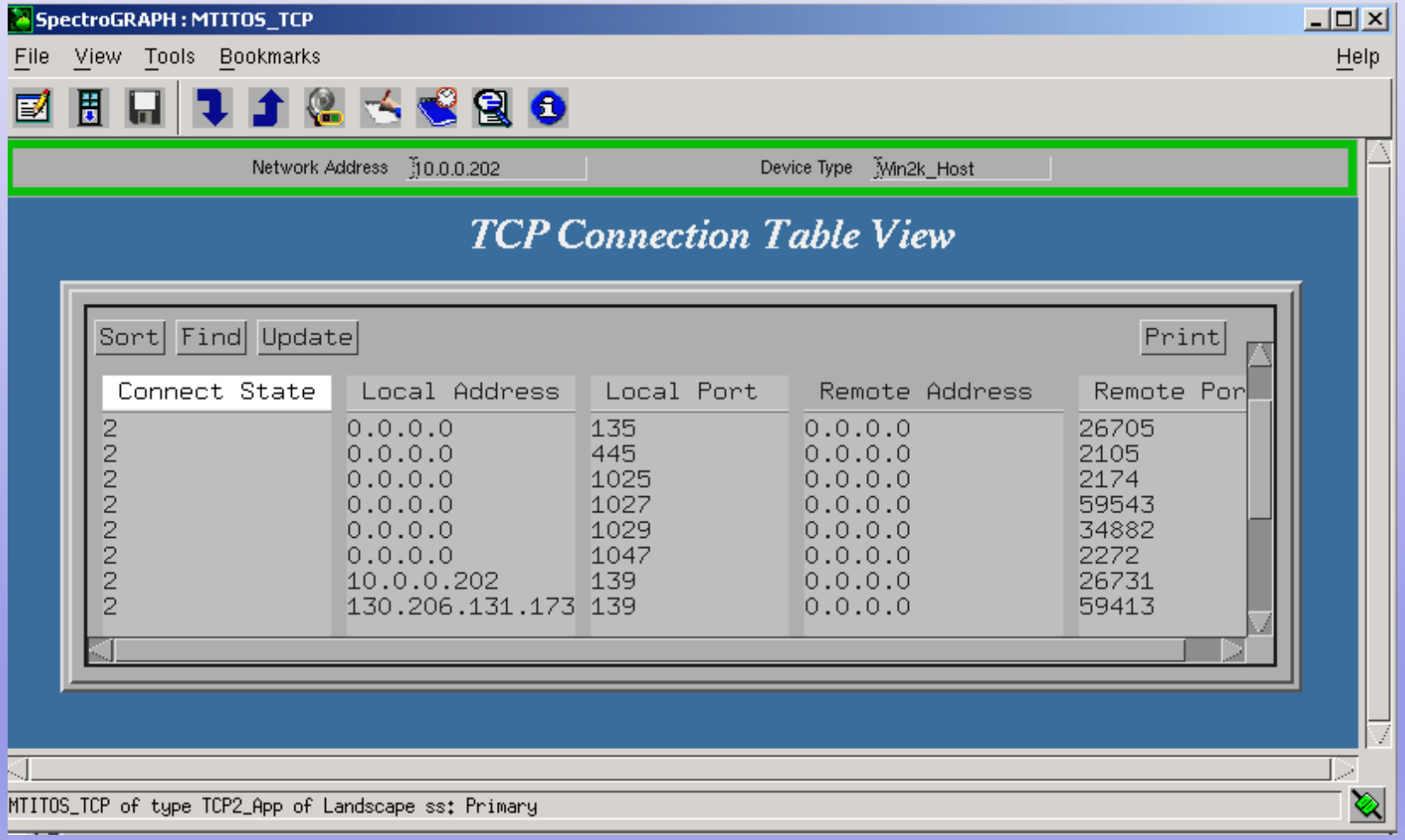
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



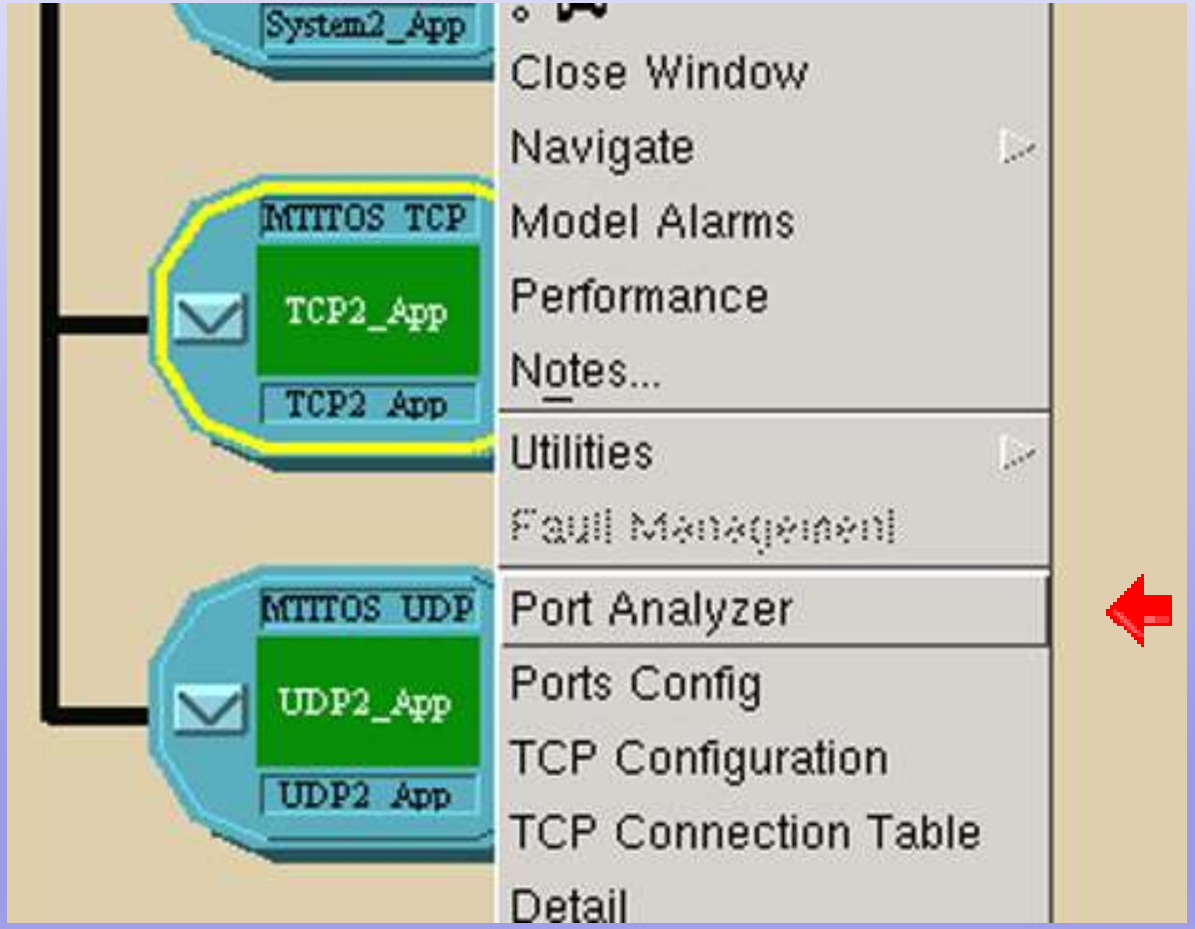
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?

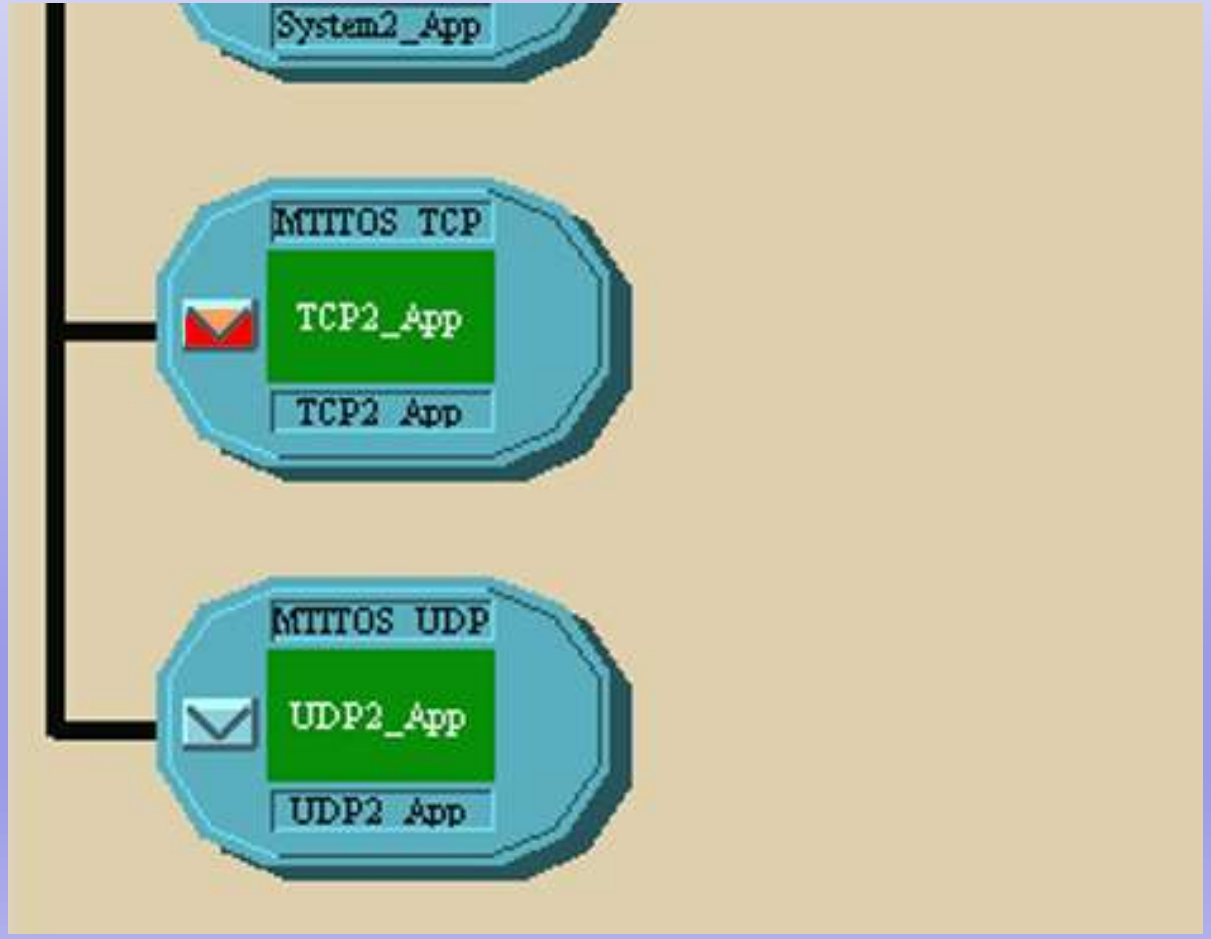


Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?

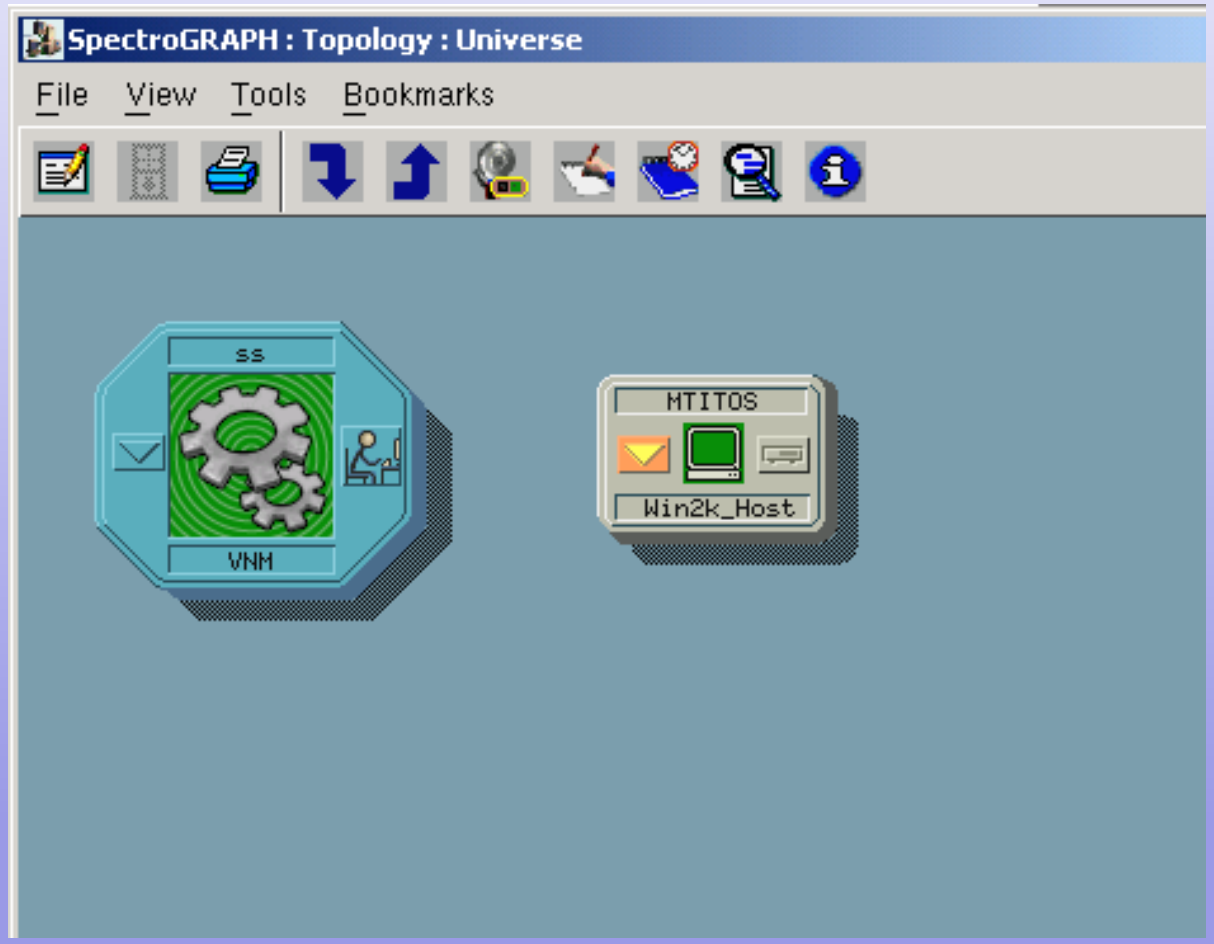
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



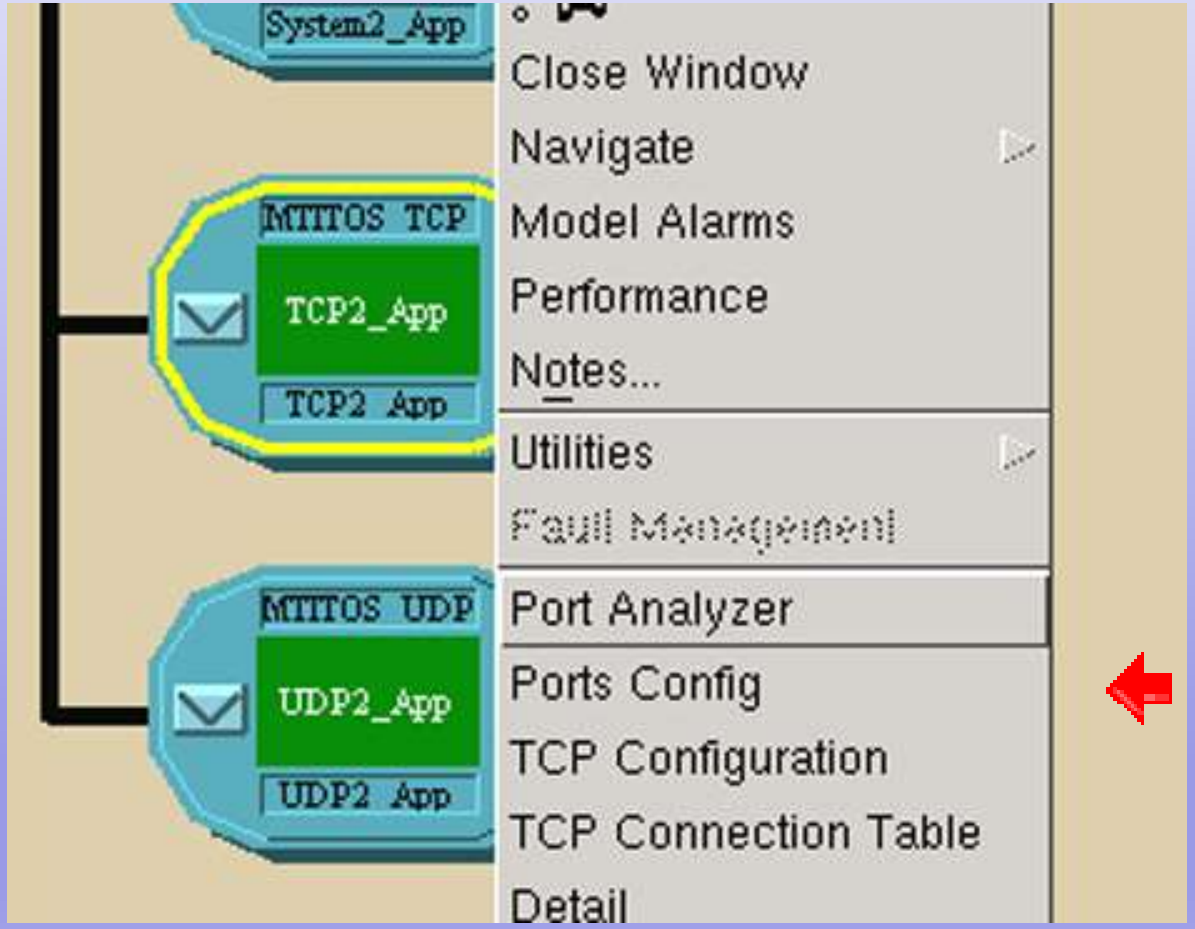
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?

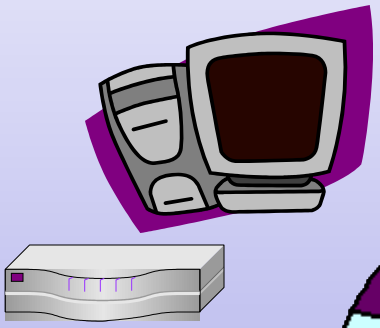
Base de Datos

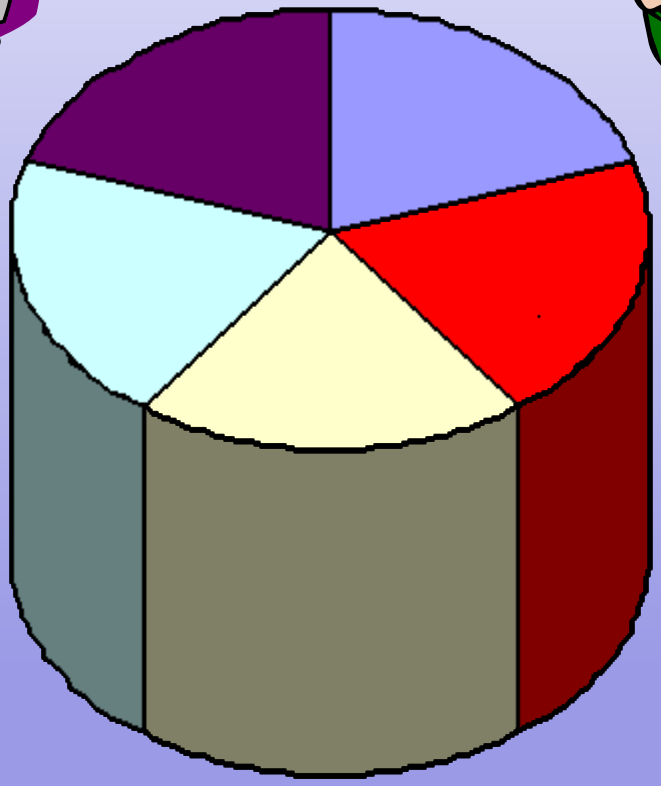
El Diseño

- Repositorio Centralizado de los Datos de Red
- Información Estática vs. Dinámica
- Actualización Automática de los Datos

Base de Datos

La Aplicación

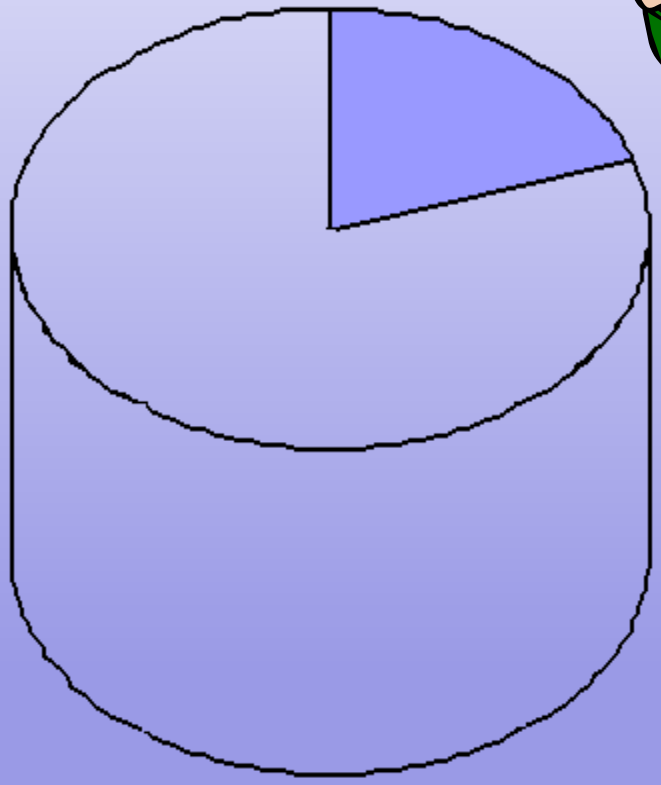




@IP

Base de Datos

Usuarios



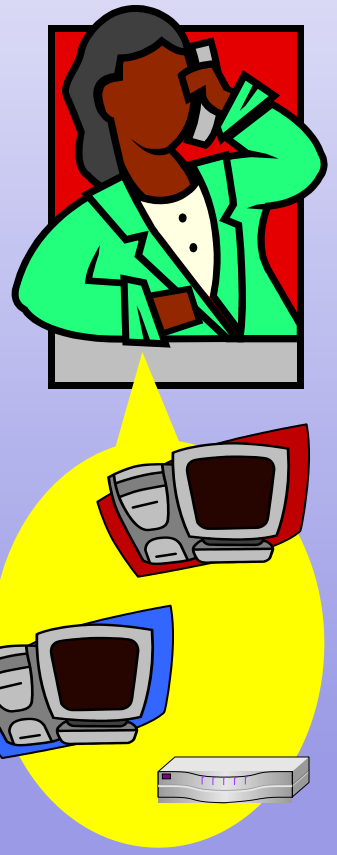
Base de Datos

Usuarios

Detalle Usuario

CODIGO	4
D.N.I.	87654321
NOMBRE	MARGALIDA
APELLIDOS	BUADES
	PUIGSERVER
EMAIL	margalida.buades@uib.es
TELÉFONO	971173000
DEPARTAMENTO	BIO BIOLOGIA

DATOS PERSONALES



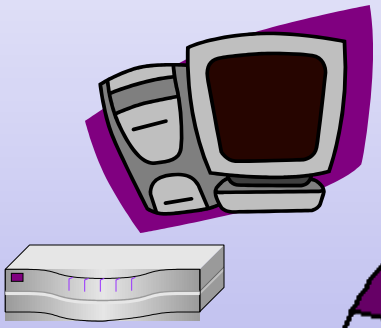
CÓDIGO	NOMBRE	MODELO	ALTA	BAJA	LAST	DESCRIPCIÓN
6	PC_5	SATELLITE	28/10/2003		28/10/2003	
3	PC_3	SATELLITE	28/10/2003		28/10/2003	
36	VH24_MO1	VH24	29/10/2003		29/10/2003	

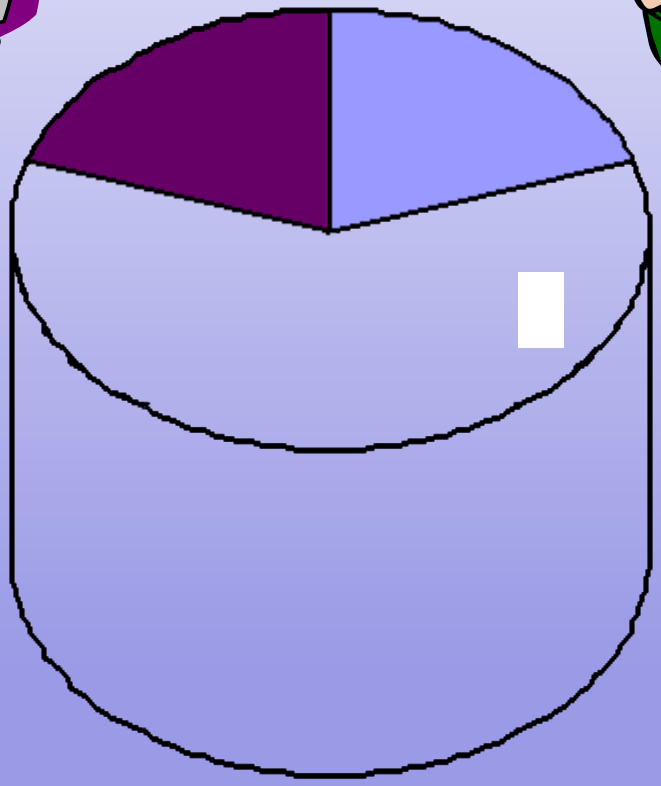
CERRAR

DISPOSITIVOS ASIGNADOS

Base de Datos

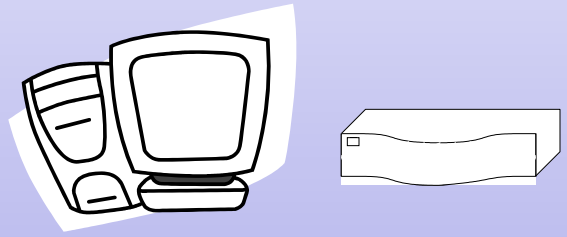
Dispositivos

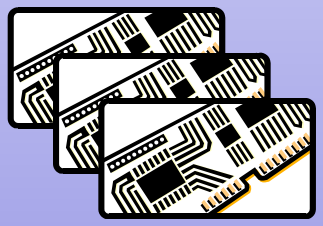


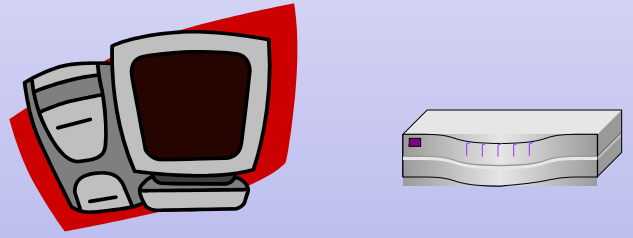


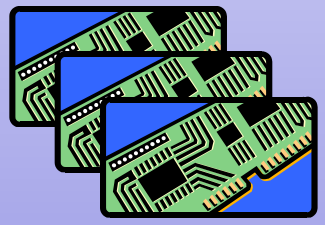
Base de Datos

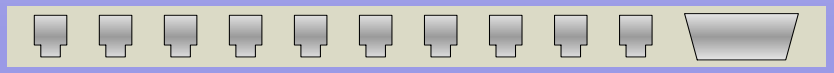
Dispositivos











Base de Datos

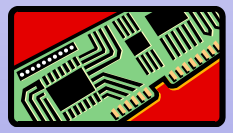
Dispositivos

Gestión de Puertos

CÓDIGO	@MAC	@IP				NOMBRE	MODELO
12	12:12:56:56:23:45	192	168	182	15	VH24_AT2	VH24

PUERTO	DESCRIPCIÓN	FECHA ALTA
80	WEB	12/07/2002
21	FTP	23/07/2002
20	FTP	23/07/2004
443	HTTPS	07/11/2003

10.0.0.13



Base de Datos

Dispositivos

Detalle Dispositivo

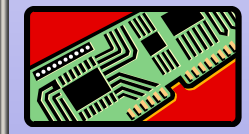
GENERAL | INTERFACES | INCIDENCIAS

INTERFAZ

INTERFAZ	VLAN	CONECTA A DISPOSITIVO	CONECTA A INTERFAZ
1	BLAU	22:22:34:12:12:34	1
2	BLAU		
3	BLAU	33:33:33:33:33:33	1
4	BLAU		
5	BLAU		
6	BLAU		
7	VERM		
8	BLAU		
9	BLAU		
10			
11			
13			
14			
15			
16			
17			

VLAN

10.0.0.13



Base de Datos

Dispositivos

Detalle Dispositivo

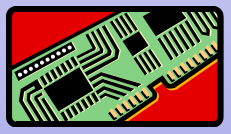
GENERAL | INTERFACES | INCIDENCIAS

INCIDENCIAS

CÓDIGO	TIPO	FECHA ALTA	PROBLEMÁTICA	FECHA SOLUCIÓN
5	IP DUPL	12/04/2002	CONFLICTO DE IP	15/04/2002
10	PLO OBERT	31/10/2003		31/10/2003
11	PLO OBERT	31/10/2003		31/10/2003

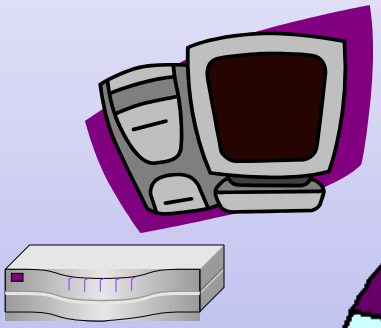
NUEVA

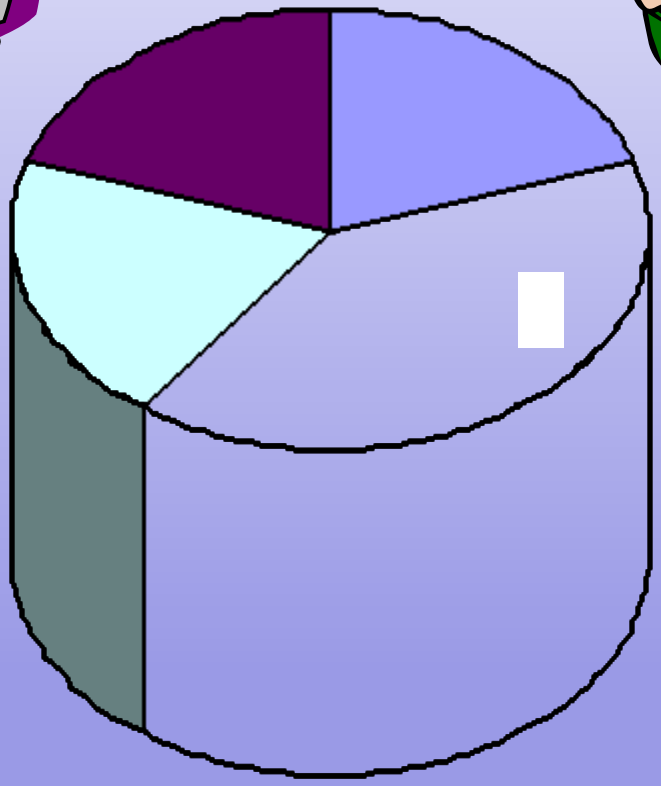
10.0.0.13



Base de Datos

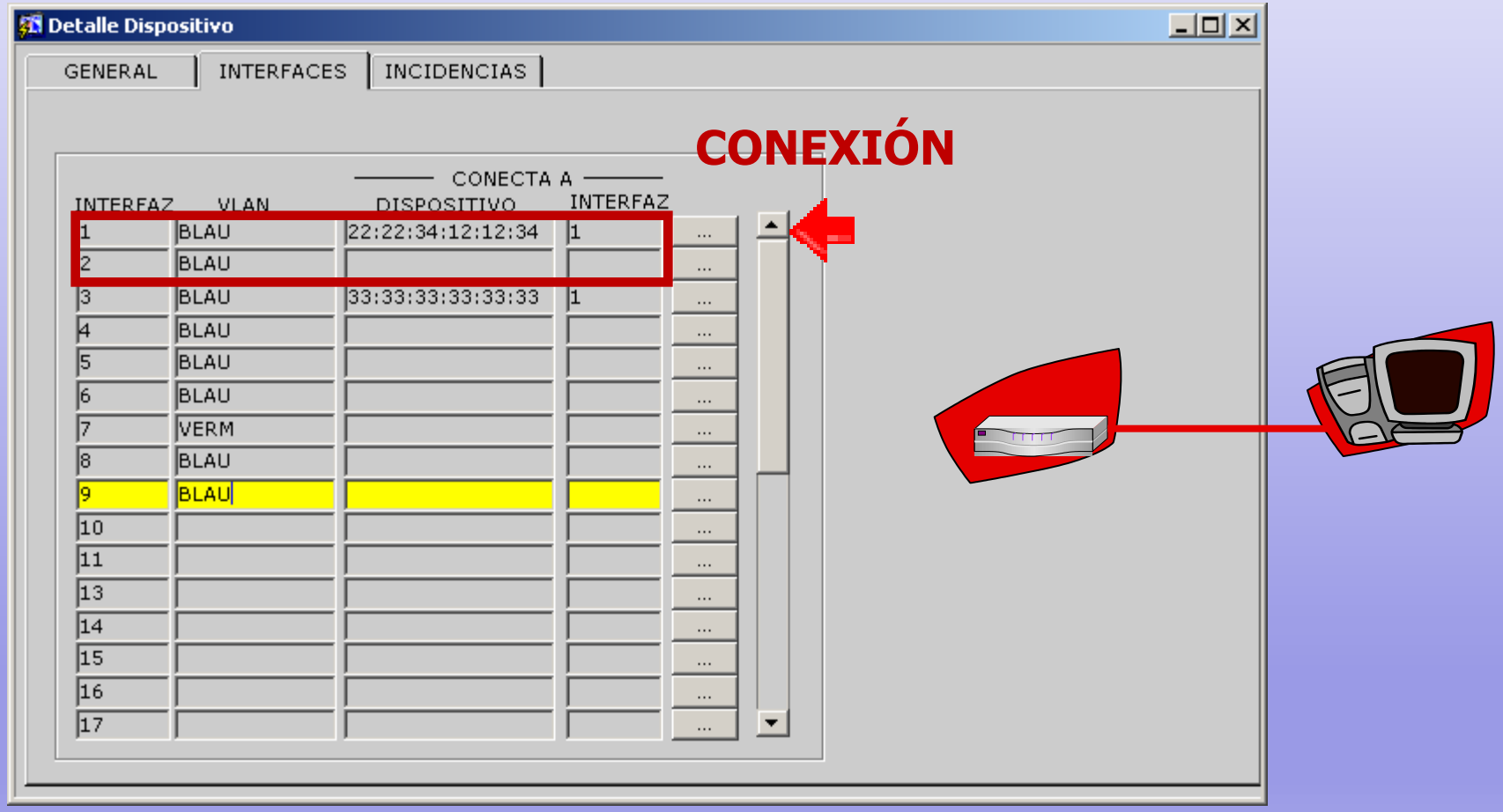
Conexiones





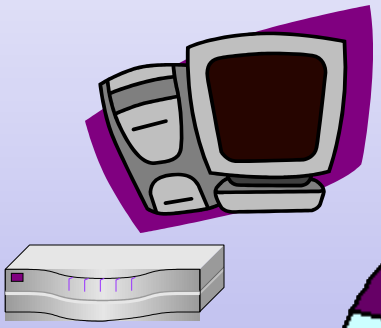
Base de Datos

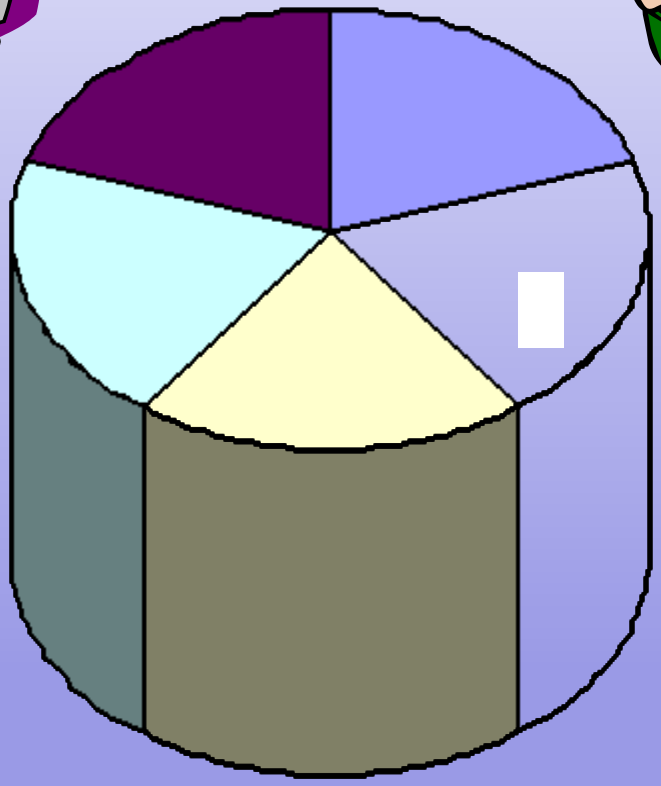
Conexiones



Base de Datos

Gestión de IPs

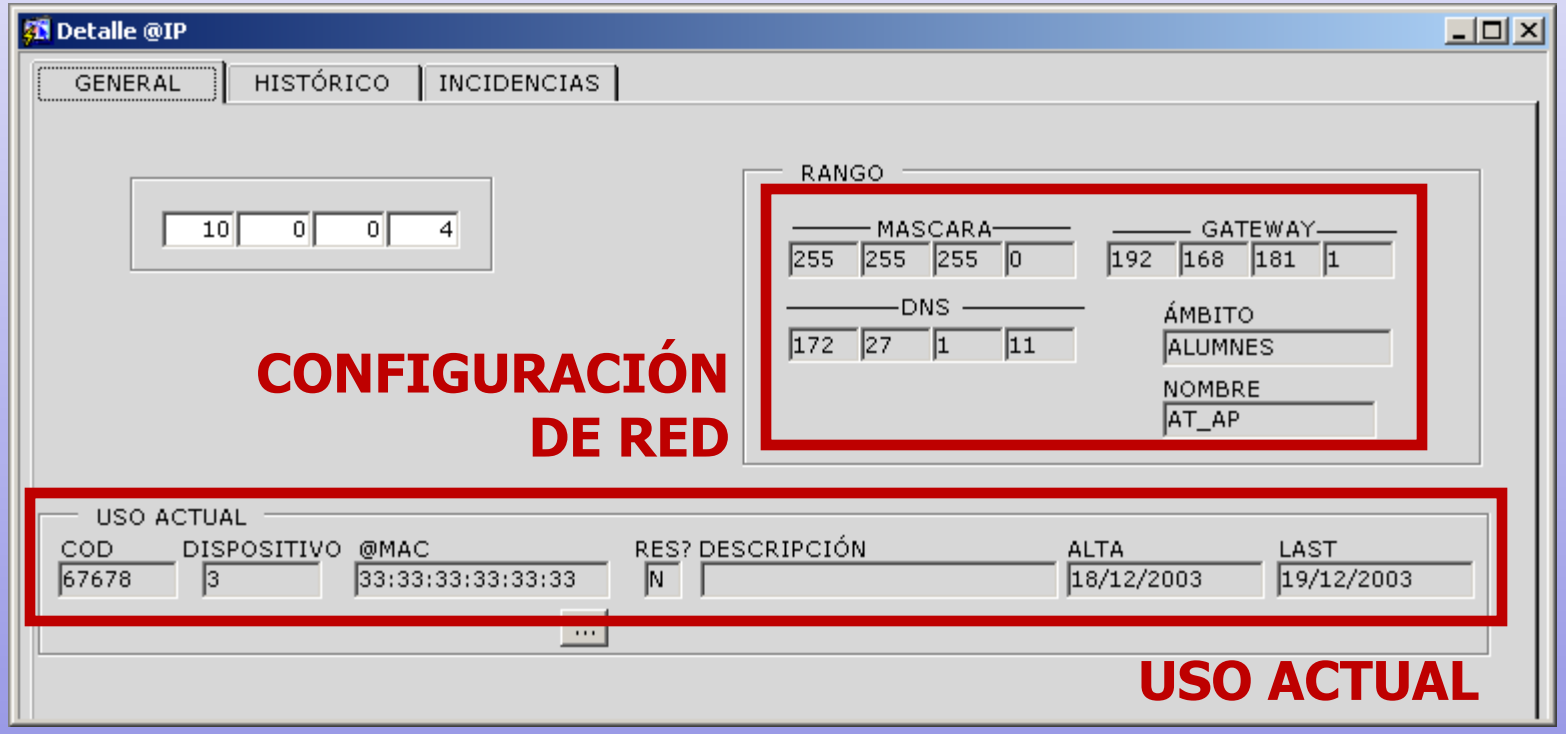




@IP

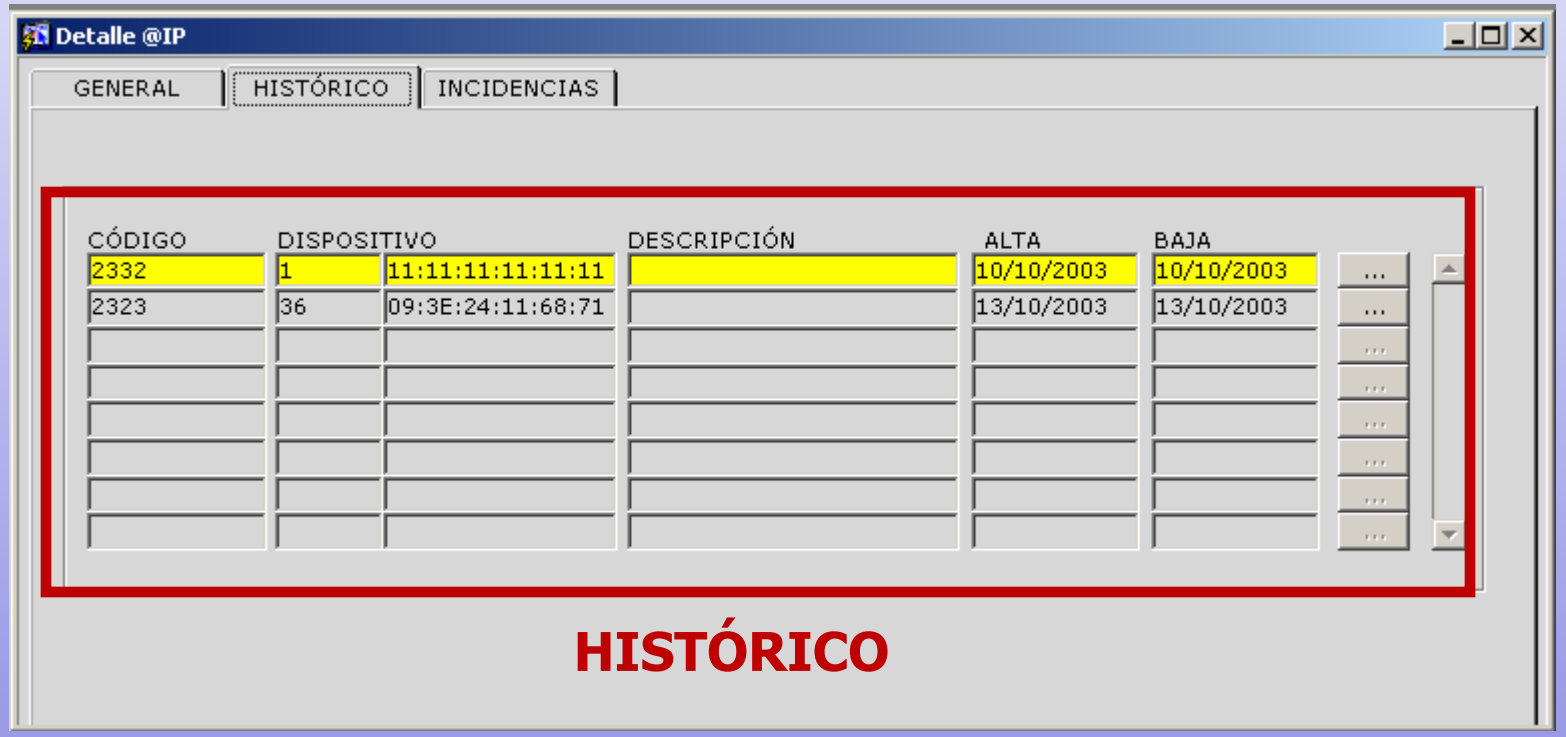
Base de Datos

Gestión de IPs



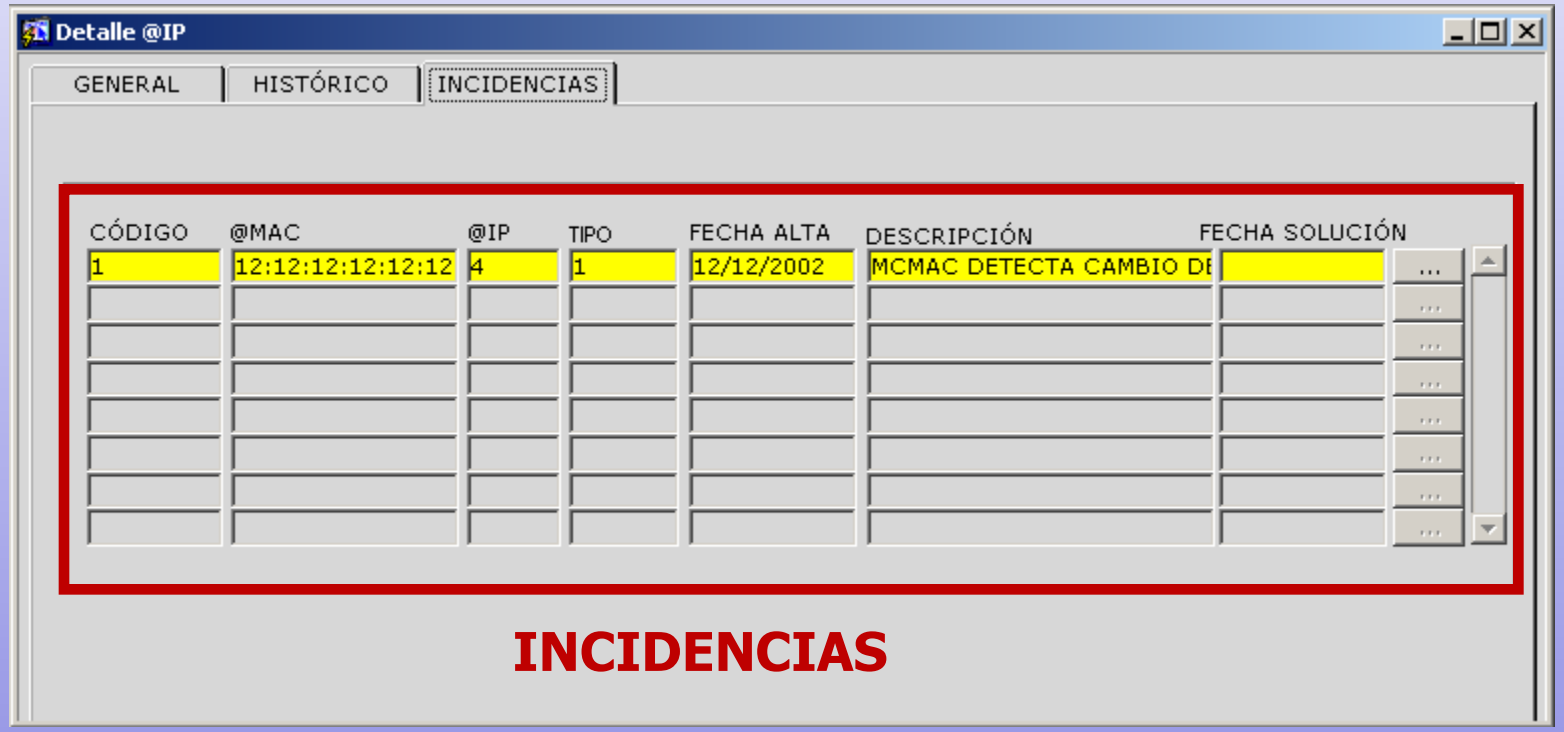
Base de Datos

Gestión de IPs



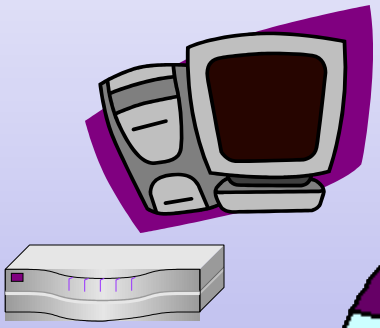
Base de Datos

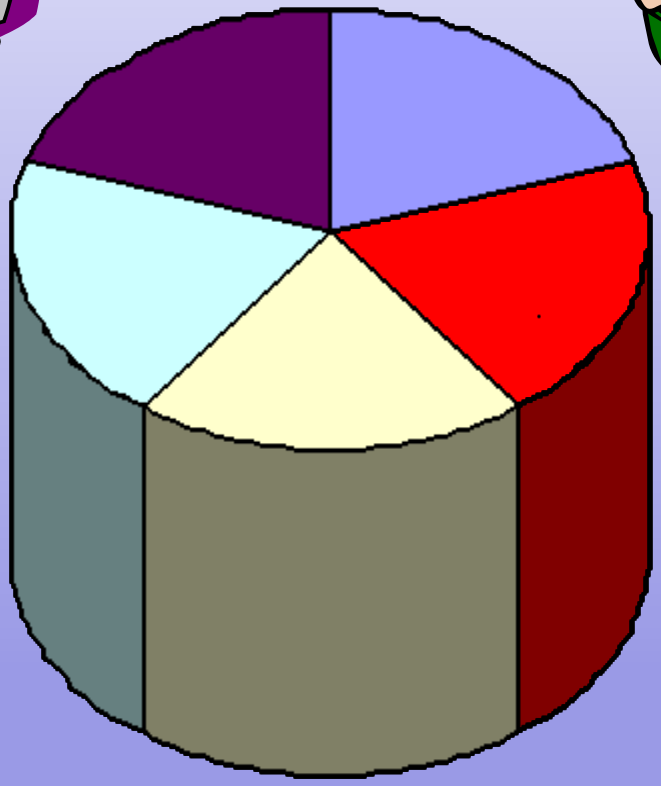
Gestión de IPs



Base de Datos

Incidencias

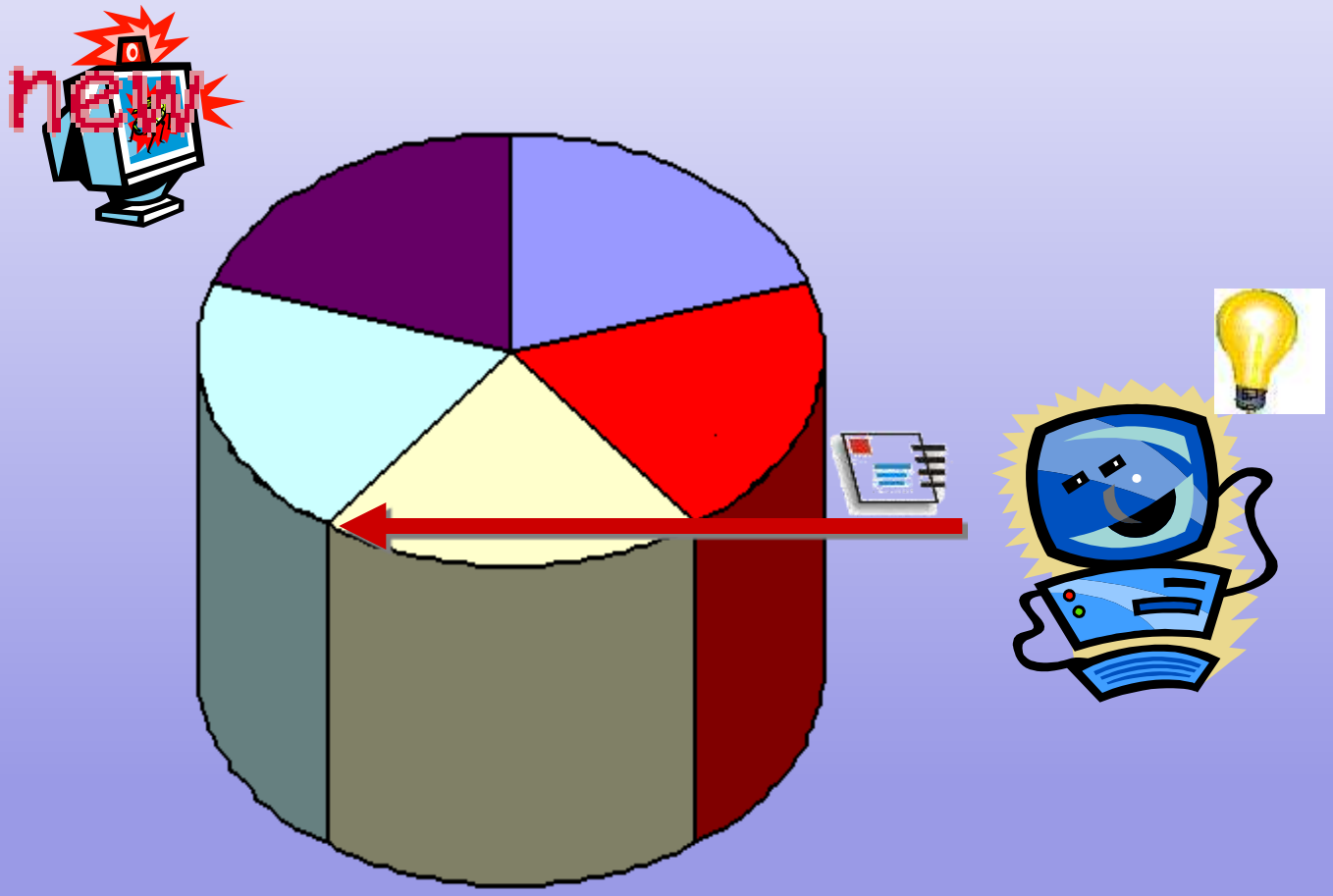




@IP

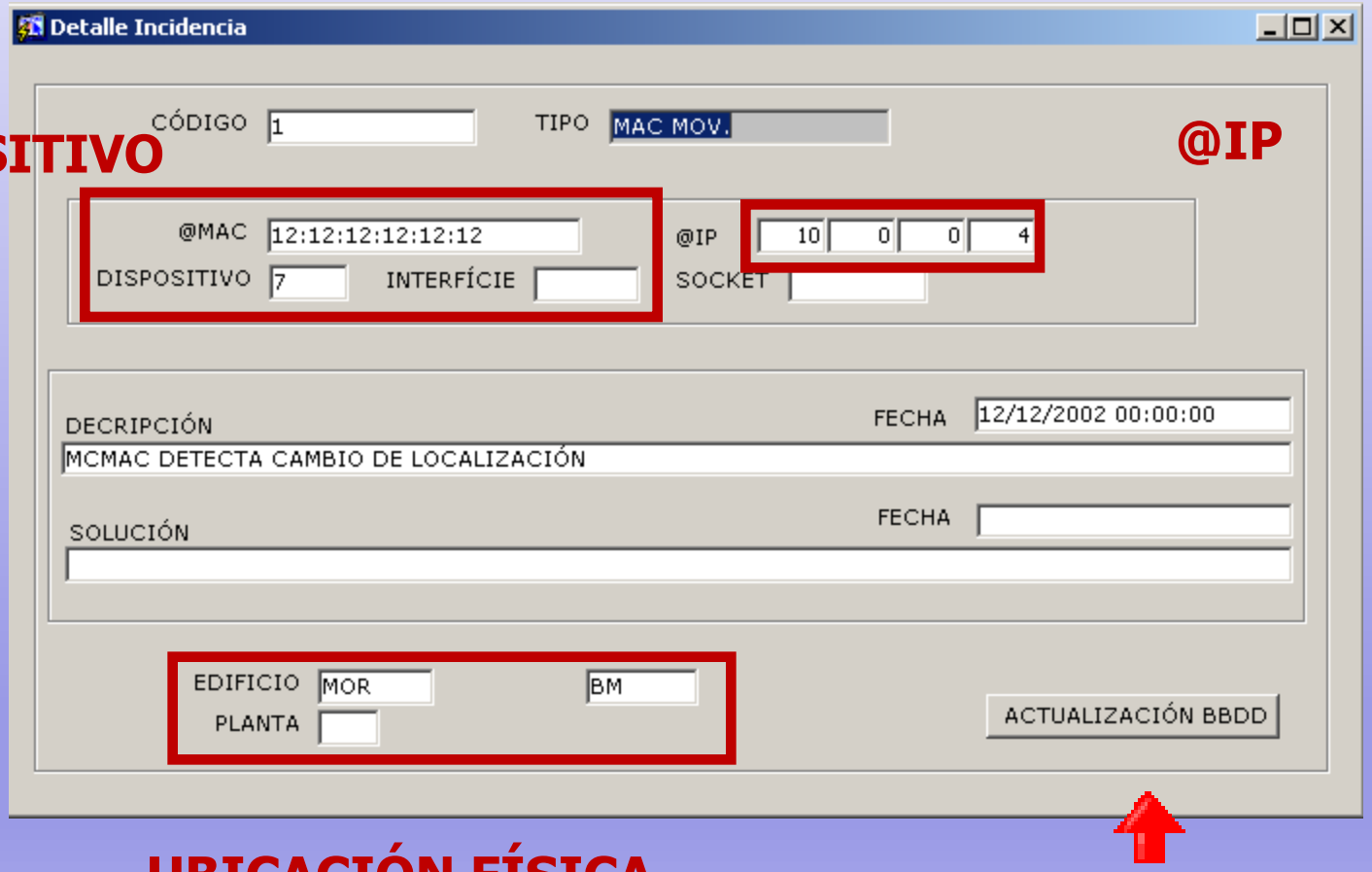
Base de Datos

Incidencias



Base de Datos

Incidencias



DISPOSITIVO

@IP

UBICACIÓN FÍSICA

Conclusiones

- Seguridad
- Fiabilidad
- Automatización
- Facilidad
- Comodidad
- Complementar la Plataforma de Gestión
- Diseño abierto a nuevas Funcionalidades