

Aplicación de Control de Puerto Lógicos



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

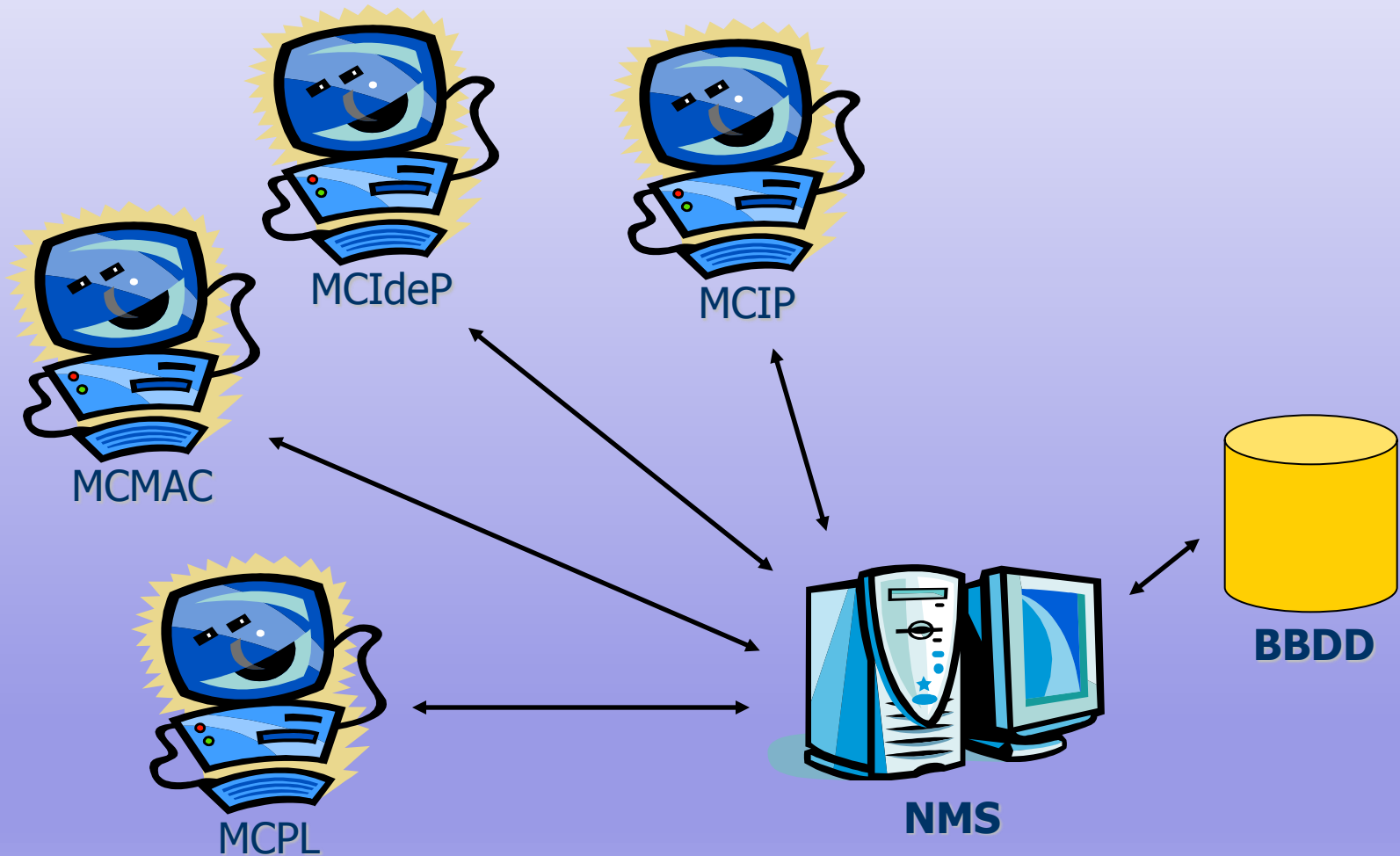
Proyecto Global

¿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)

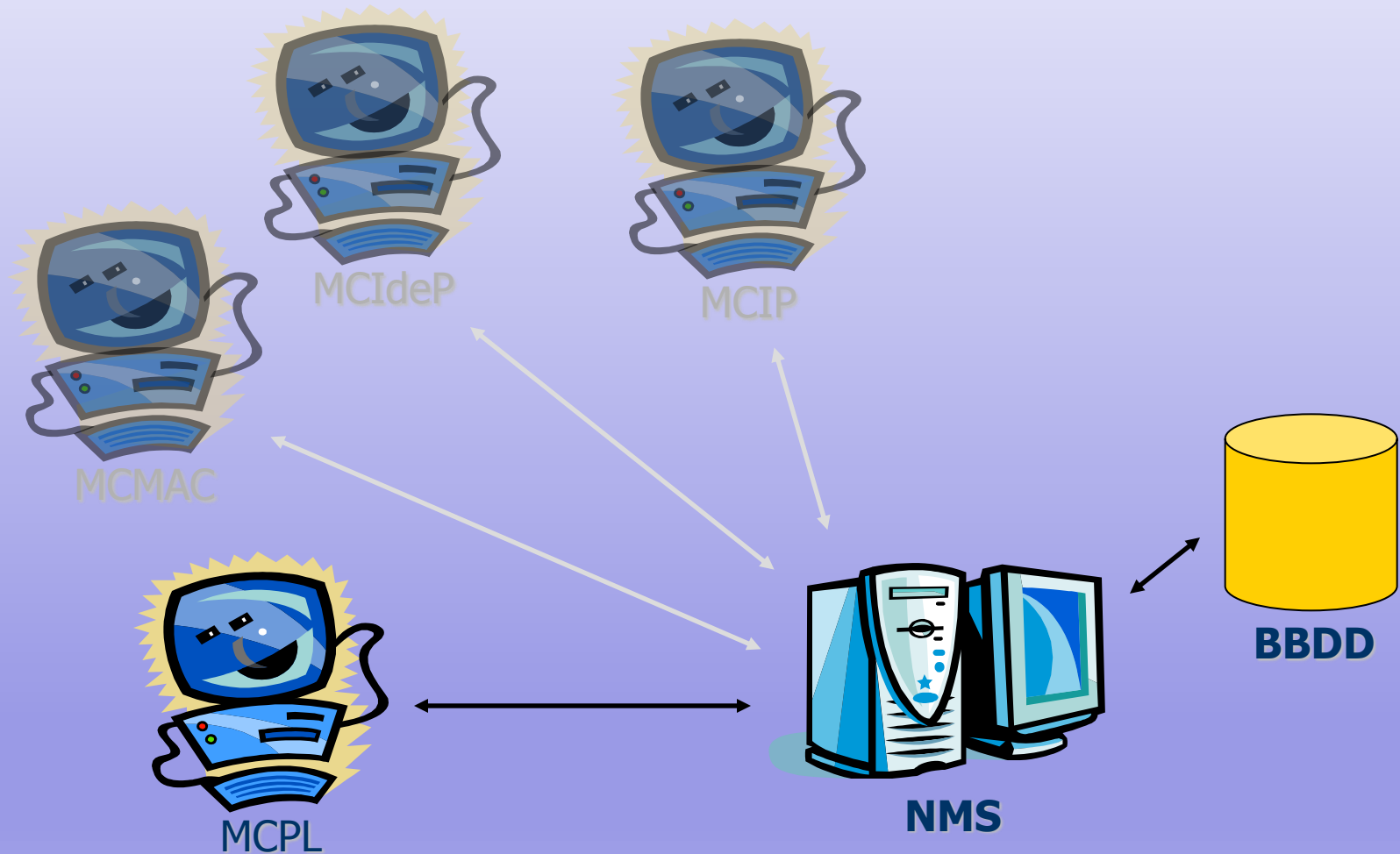
Proyecto Global

El esquema



Proyecto Global

Nuestra parte del esquema



Aplicación de Puertos Lógicos

Problemática: Puerto NO Deseado

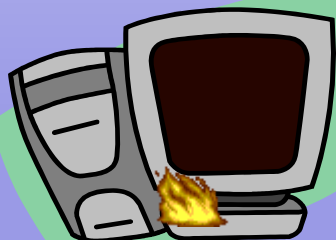
**Puertos TCP
Abiertos**

WWW: 80

FTP: 21

POP3: 110

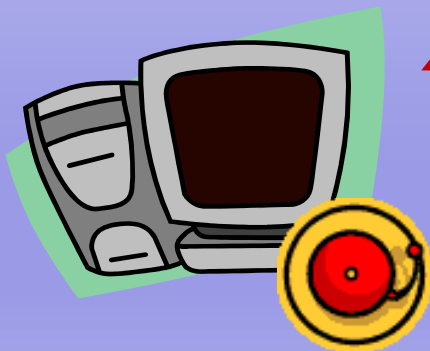
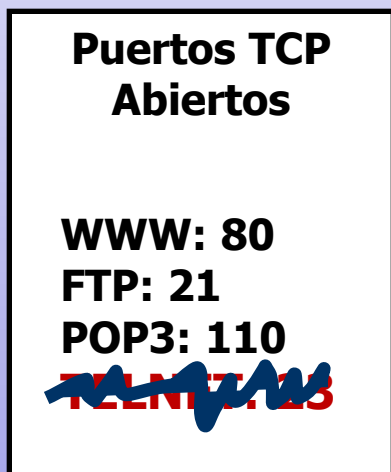
TELNET: 23



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

Aplicación de Puertos Lógicos

Problemática: Puerto NO Deseado



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

Aplicación de Puertos Lógicos

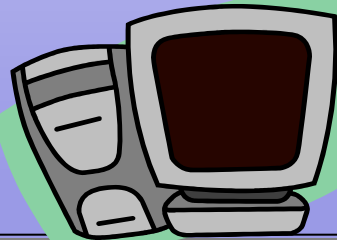
Problemática: Cae uno de Nuestros Puertos

**Puertos TCP
Abiertos**

WWW: 80

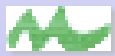
FTP: 21

POP3: 110

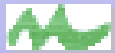


Aplicación de Puertos Lógicos

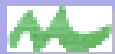
¿Existen Soluciones?



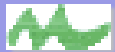
Netstat



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$ cllscsuid-??
bash-2.04$ export cllscsuid
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 SpectroCMMS. Please read the accompanying CLI user
documentation before using the create, destroy, or update commands.

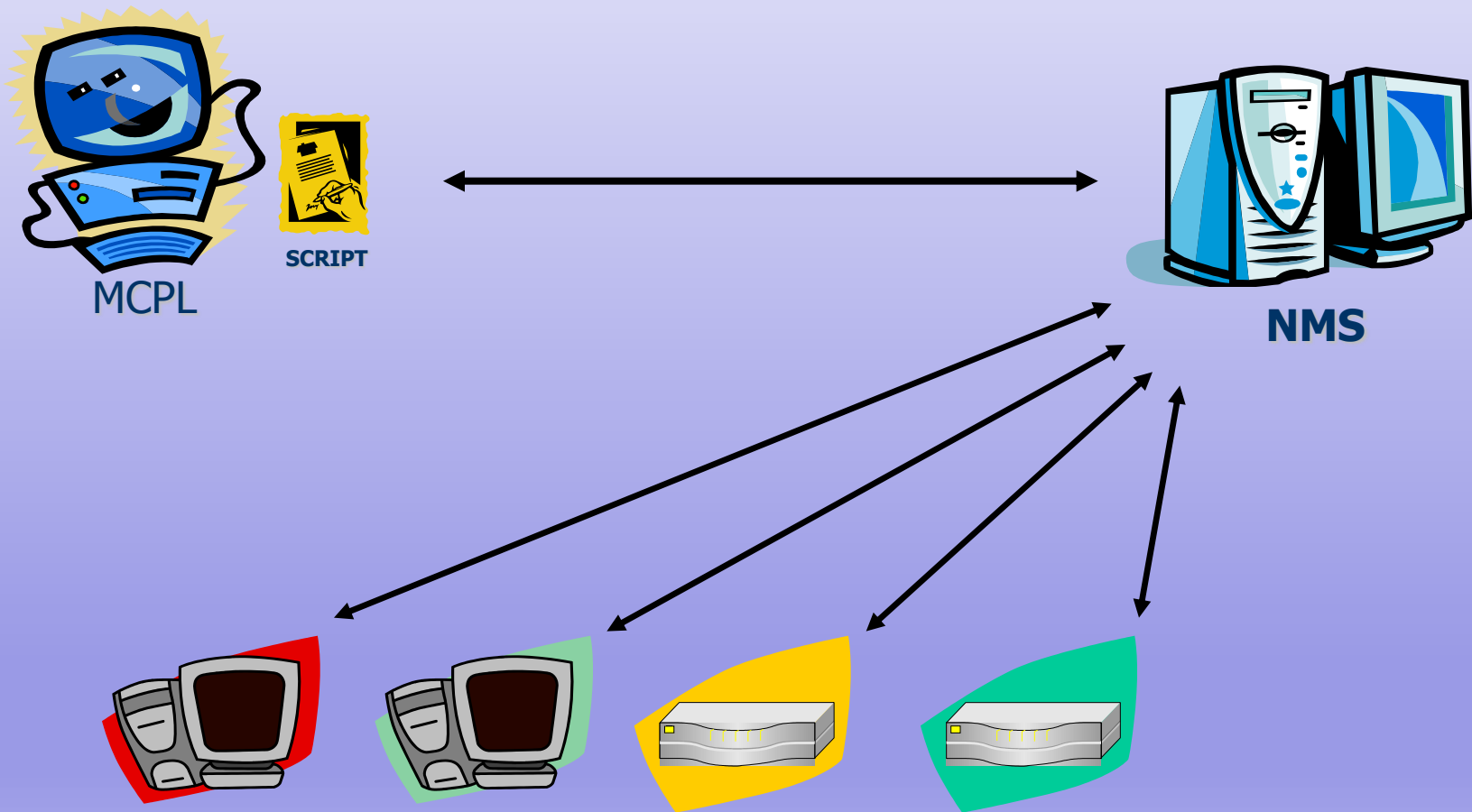
bash-2.04$ show
c:\win32app\SPECTRUM\cmmsch\show.exe: usage:
show [model|infr-low|model-handle|high|model-handle|infr-model-type-handle|
      |landscape|
      |landscape-handle|
      |infr-low|infr-high|infr|infr-name|infr-name|iflags|U|I|D|M|U|H|
      |landscape-handle|
      |relations|landscape-handle| | | | |
      |associations|infr-model-handle|
      |parents|infr-relations|infr-model-handle|
      |children|infr-relations|infr-model-handle|
      |attributes|infr|infr-attribute_id|infr-instance_id|next|...|
      |infr-low|infr-high|infr|infr-name|infr-name|
      |infr-model-handle|
      |infr-model-type-handle|infr-low|infr-high|infr|
      |infr-name|infr-name|iflags|E|S|U|E|I|G|O|M|D|P|L|
      |landscape-handle|
      |alarm|infr|infr|infr-model-handle|infr-landscape-handle|
      |events|infr|infr|infr-model-handle|
      |infr-model-handle|infr-landscape-handle|
      |inheritance|infr-model-type-handle|infr-landscape-handle|
      |rules|infr-relations|infr-landscape-handle|
      |enumerations|infr-attribute_id|infr-model-type-handle|
      |infr-landscape-handle|
      |watch|infr-model-handle|

bash-2.04$ disconnect
disconnect: successful from ss - connected for 0 hours, 0 minutes
bash-2.04$
```



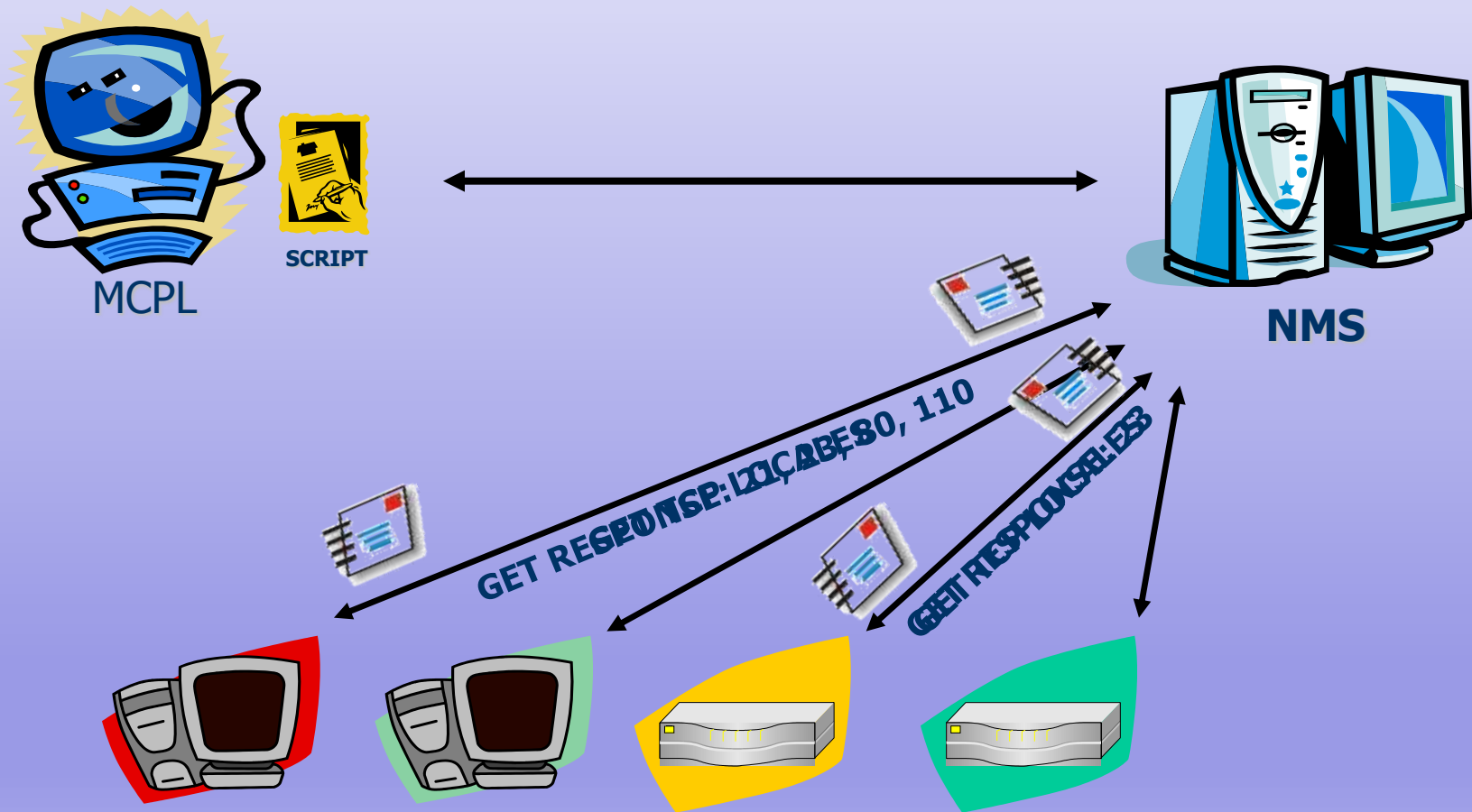
Aplicación de Puertos Lógicos

¿Cómo funciona?



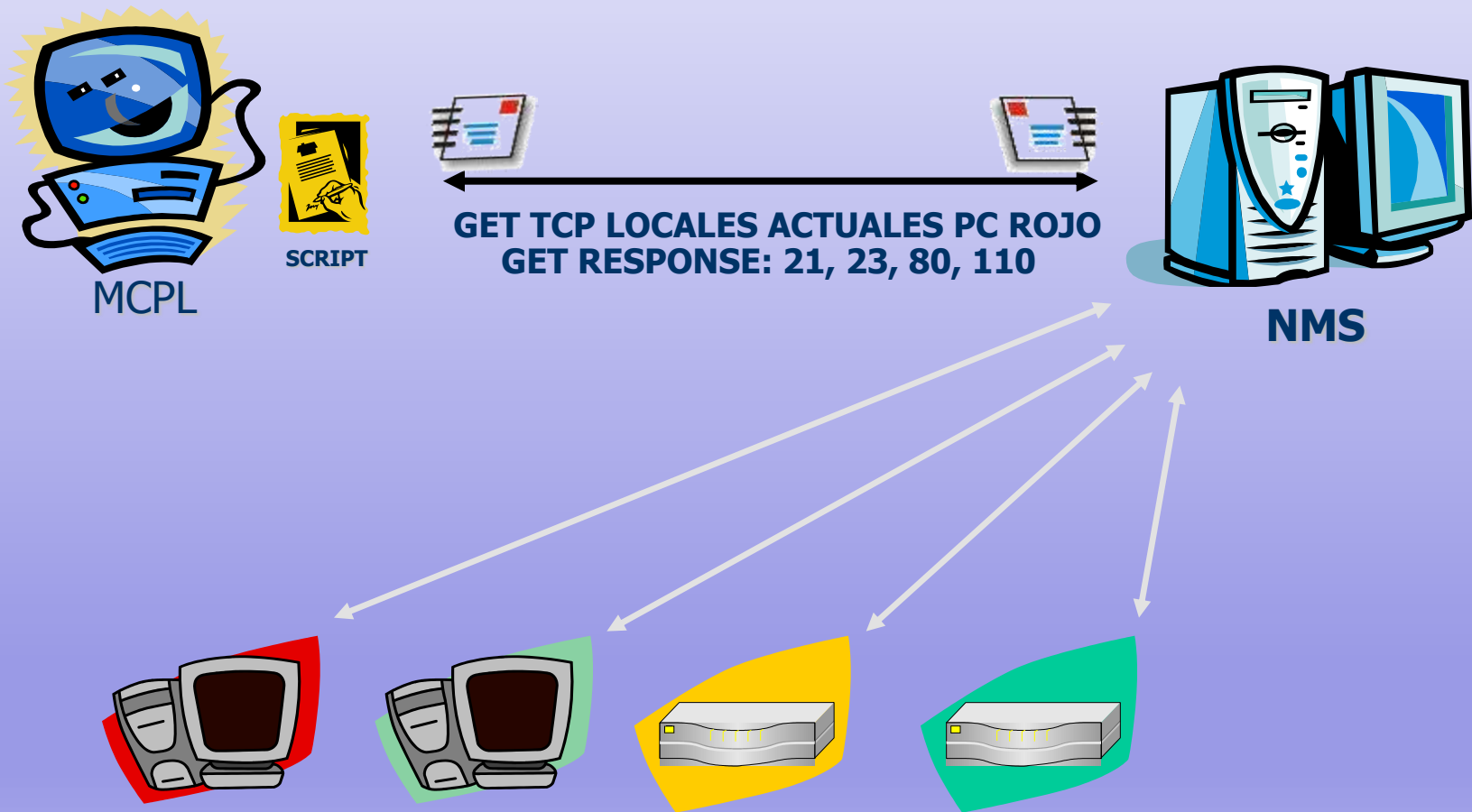
Aplicación de Puertos Lógicos

¿Cómo funciona?



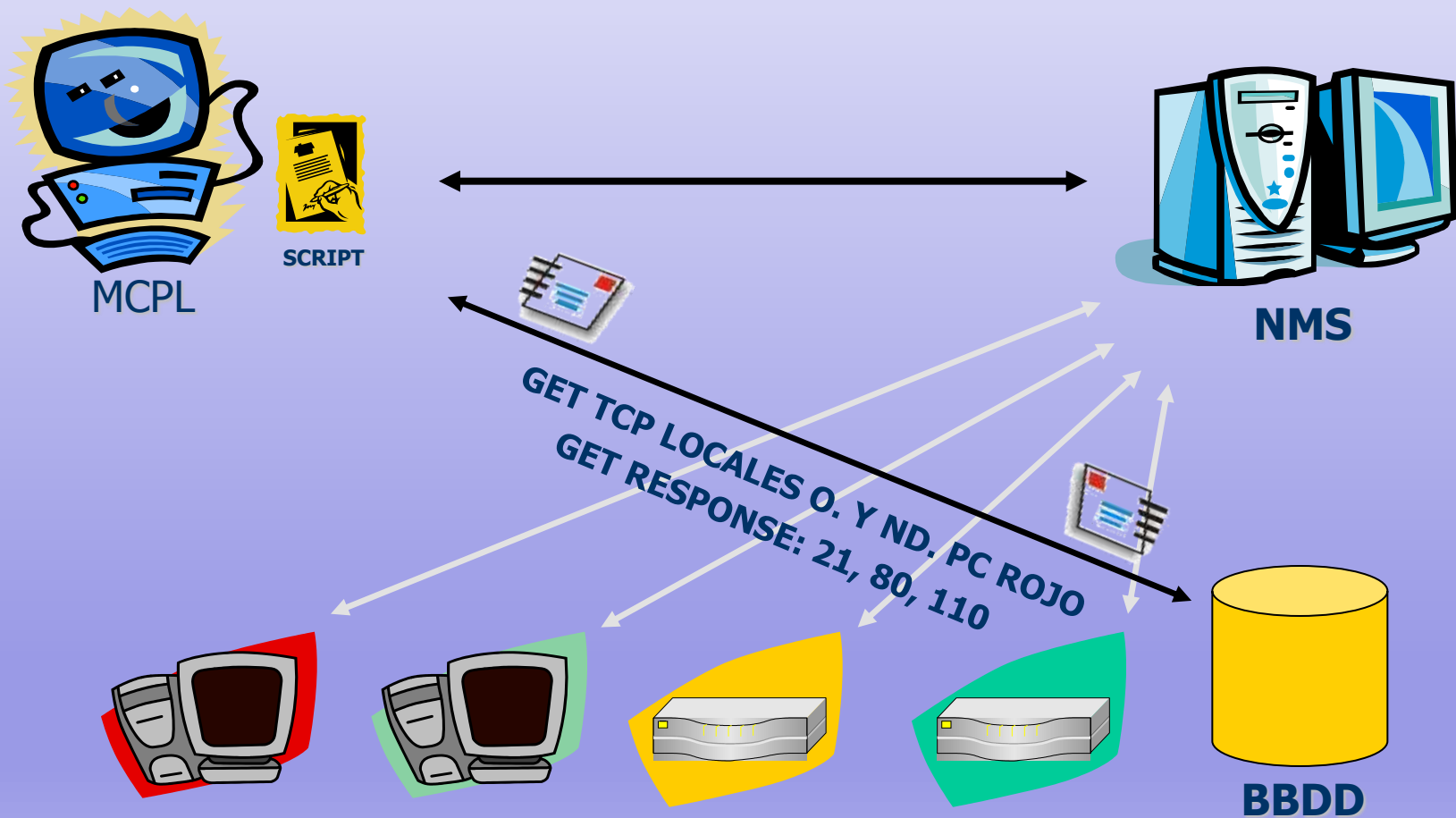
Aplicación de Puertos Lógicos

¿Cómo funciona?



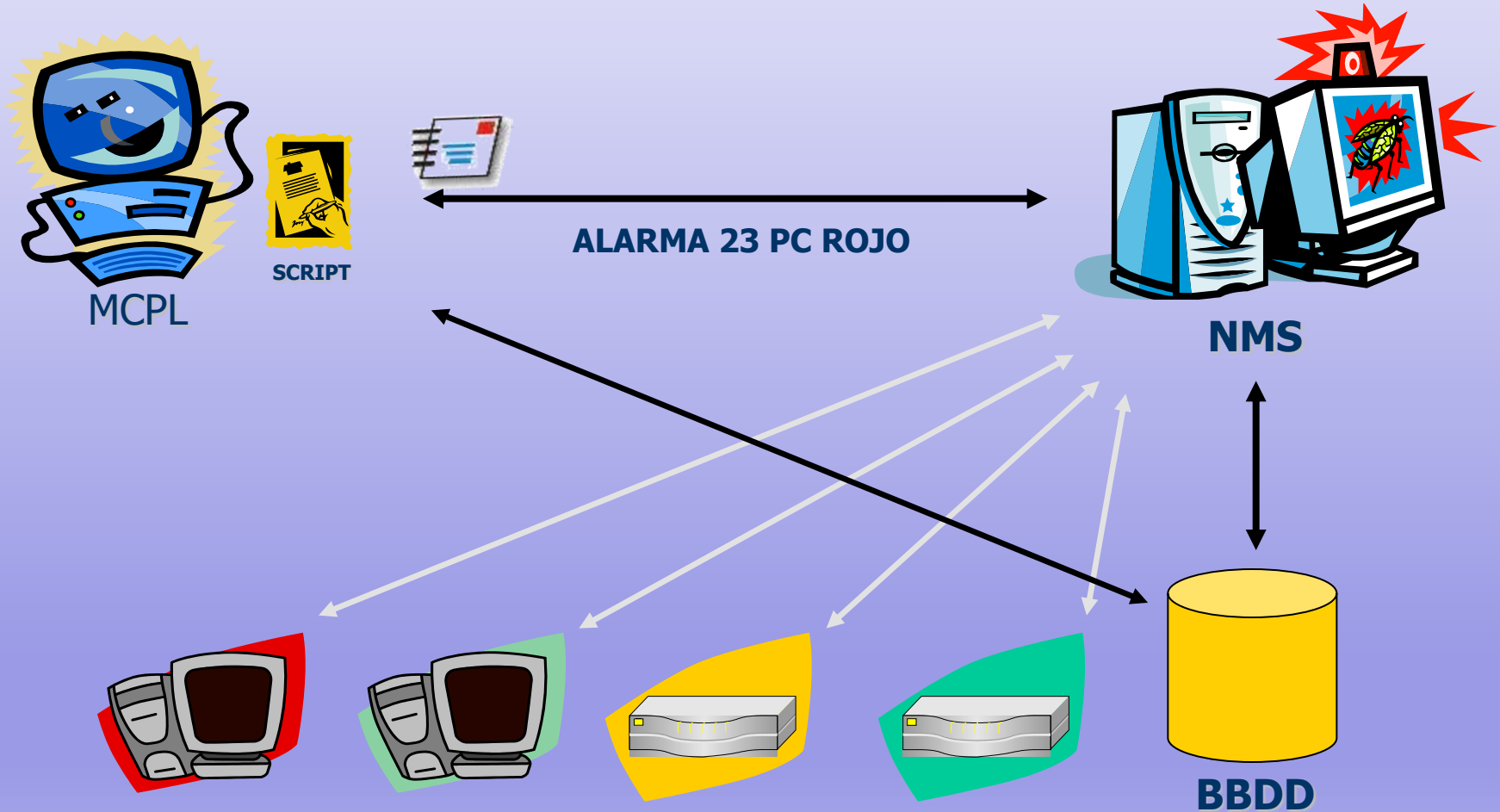
Aplicación de Puertos Lógicos

¿Cómo funciona?



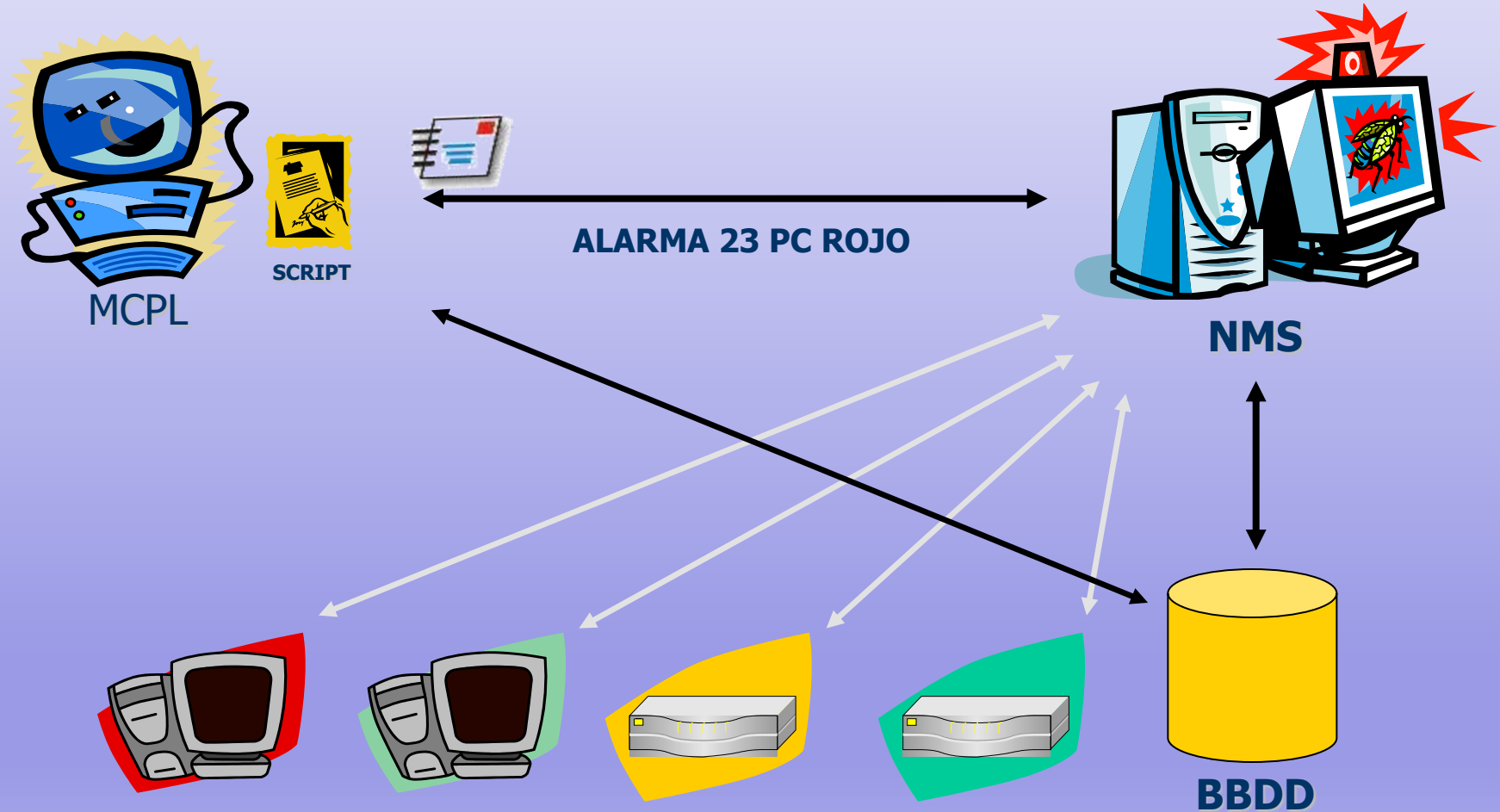
Aplicación de Puertos Lógicos

¿Cómo funciona?



Aplicación de Puertos Lógicos

¿Cómo funciona?



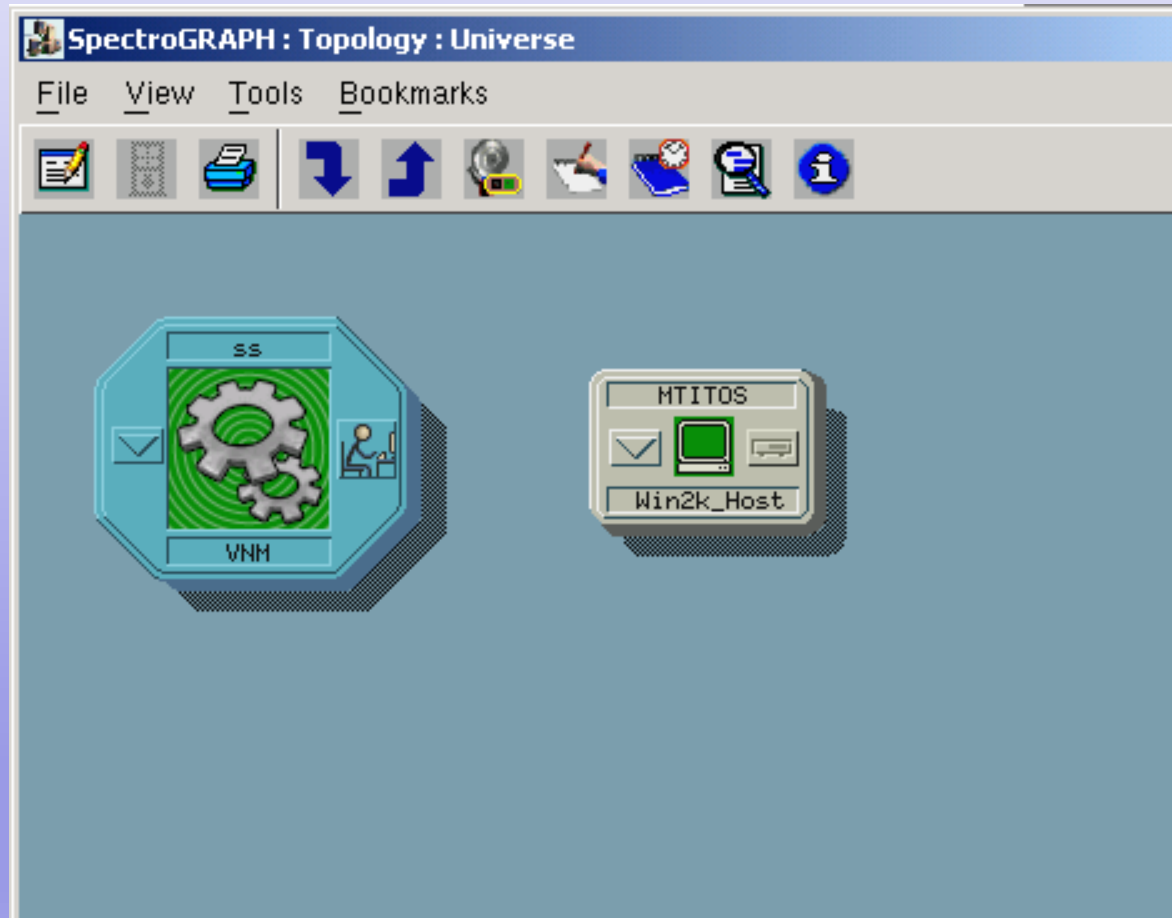
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



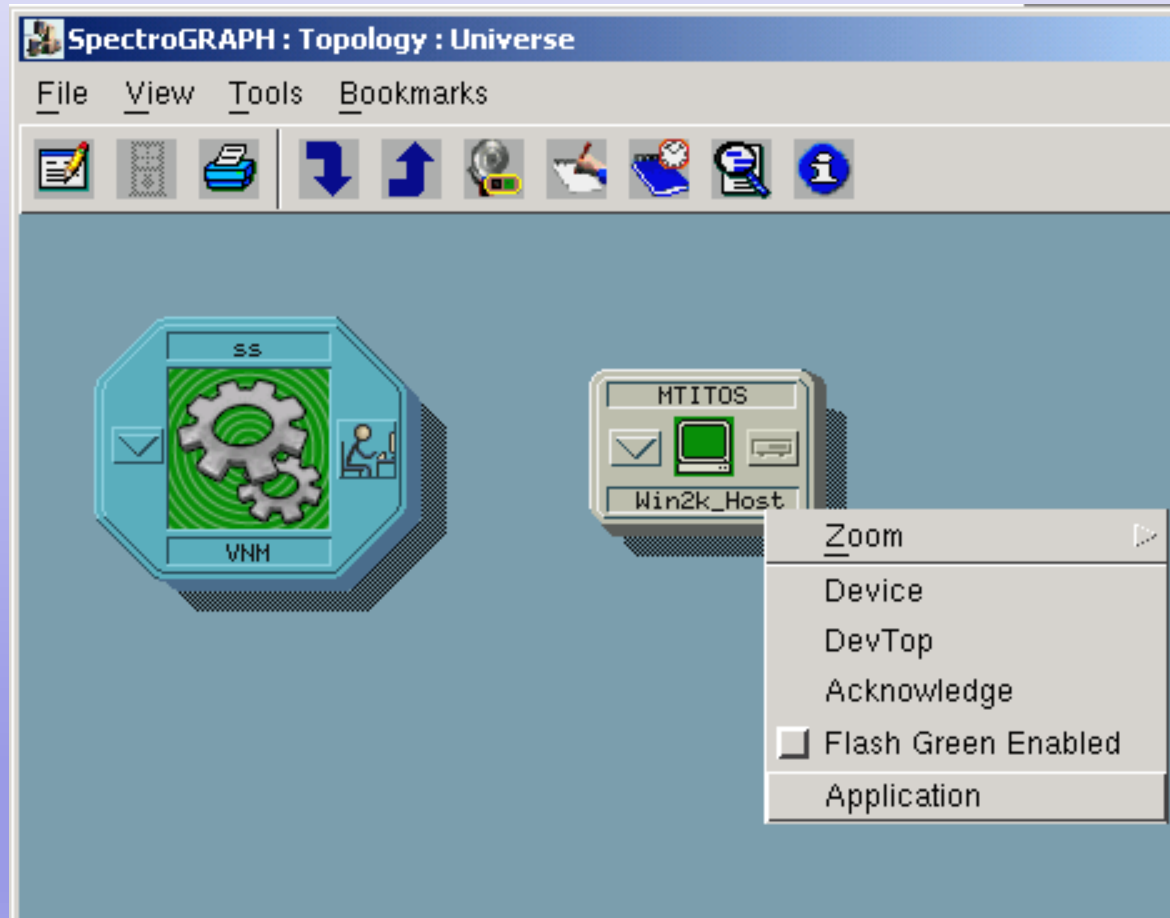
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



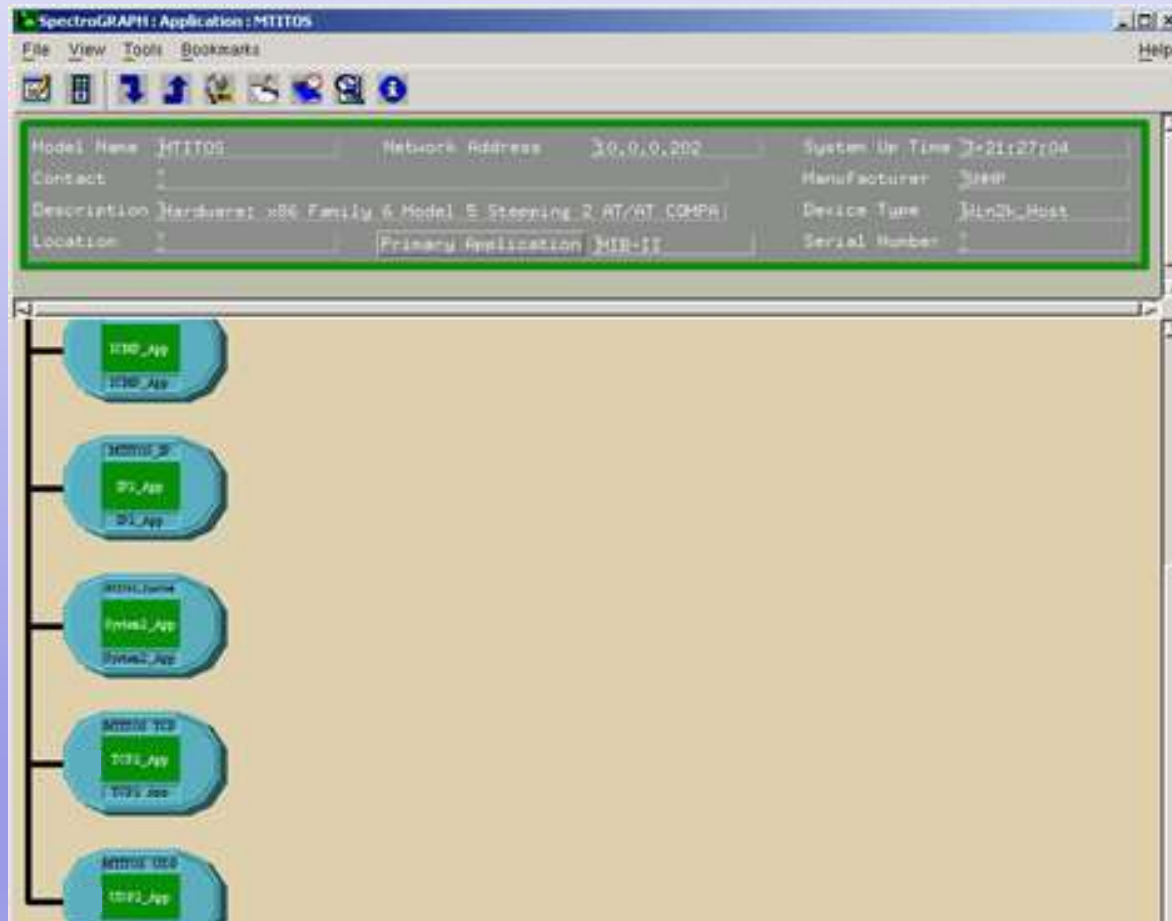
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



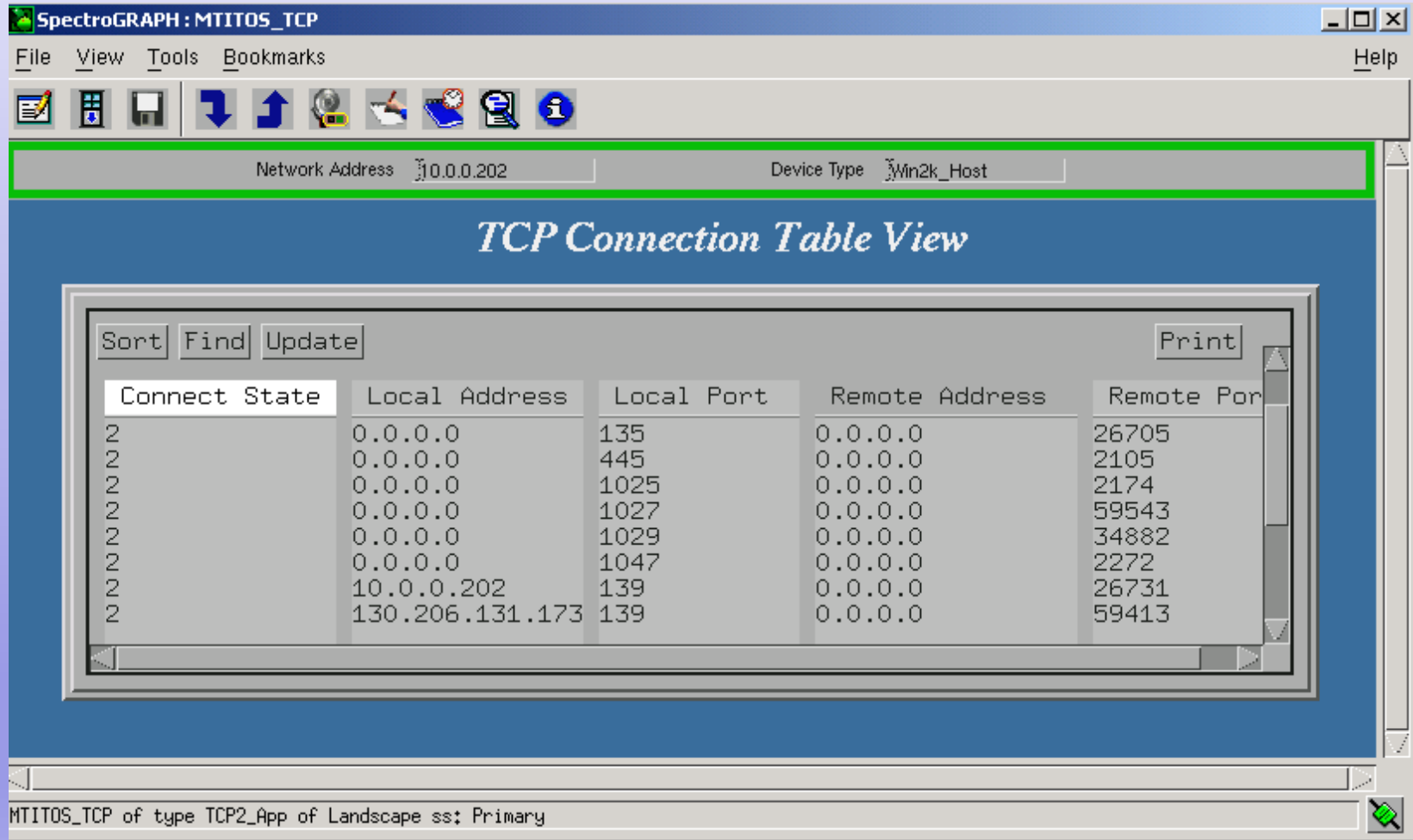
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



The screenshot shows the SpectroGRAPH: MTITOS_TCP application window. The title bar reads "SpectroGRAPH : MTITOS_TCP". The menu bar includes "File", "View", "Tools", "Bookmarks", and "Help". The toolbar contains icons for file operations and network functions. Below the toolbar, there are input fields for "Network Address" (set to "10.0.0.202") and "Device Type" (set to "Win2k_Host"). The main display area is titled "TCP Connection Table View" and contains a table of active TCP connections. The table has columns for "Connect State", "Local Address", "Local Port", "Remote Address", and "Remote Port". The table is sorted by "Connect State" and shows 10 connections. A "Print" button is located in the top right corner of the table area. The status bar at the bottom indicates "MTITOS_TCP of type TCP2_App of Landscape ss: Primary".

Connect State	Local Address	Local Port	Remote Address	Remote Port
2	0.0.0.0	135	0.0.0.0	26705
2	0.0.0.0	445	0.0.0.0	2105
2	0.0.0.0	1025	0.0.0.0	2174
2	0.0.0.0	1027	0.0.0.0	59543
2	0.0.0.0	1029	0.0.0.0	34882
2	0.0.0.0	1047	0.0.0.0	2272
2	10.0.0.202	139	0.0.0.0	26731
2	130.206.131.173	139	0.0.0.0	59413

Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



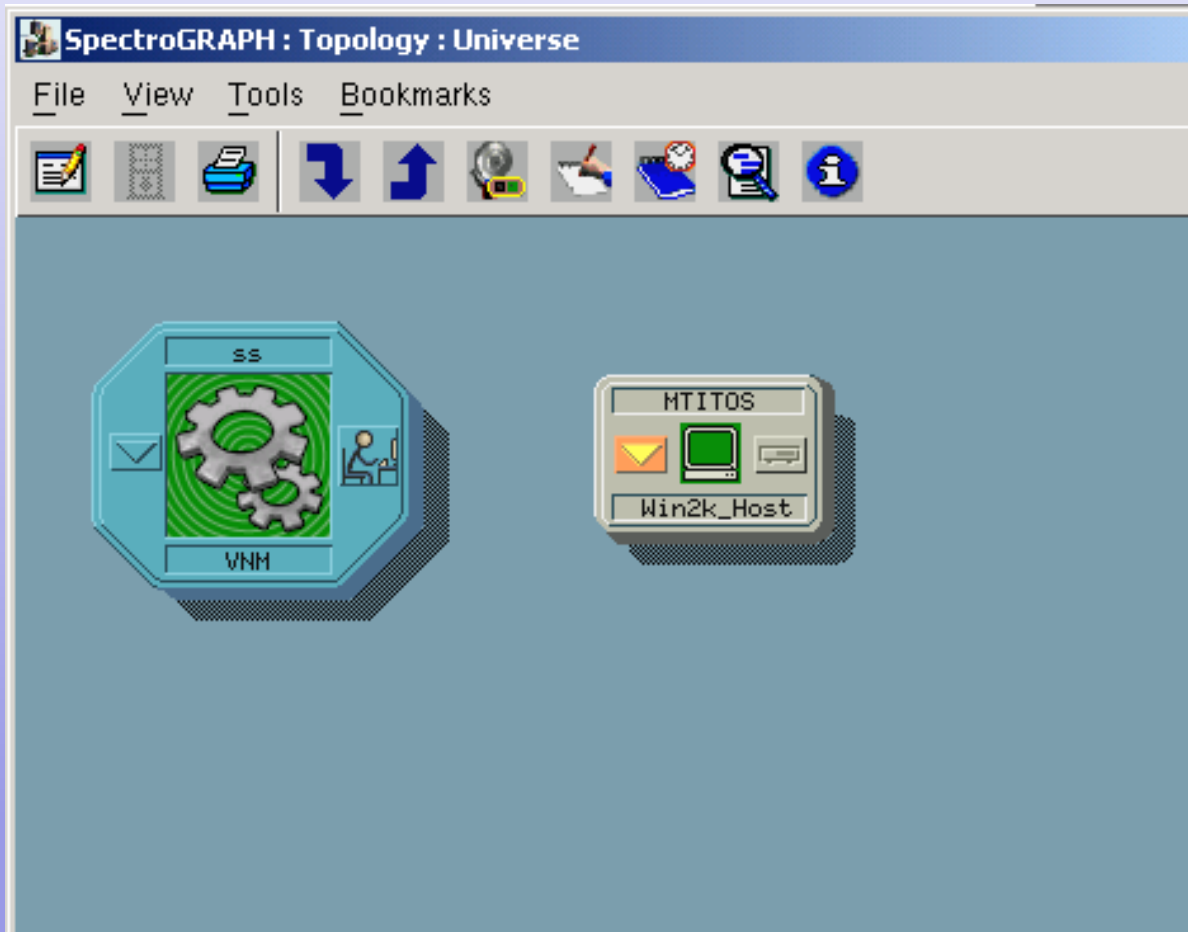
Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?



Aplicación de Puertos Lógicos

¿Qué hemos desarrollado?




The screenshot shows a web-based application titled "TCP Ports Configuration". At the top, there are two input fields: "Model_Name" with the value "MTITOS_TCP" and "Device Type" with the value "Win2k_Host". The main content area has a blue background and contains several sections:

- Ejecutar Script:** A button labeled "AHORA".
- Script en Modo Bucle:** Two buttons labeled "Activar" and "Desactivar". Below them, a status indicator shows "Ahora está" followed by a dropdown menu currently set to "Desactivado".
- Nextscan:** A text input field containing the date and time "13/10/2003-10:49:12".
- Frecscan:** A text input field containing the number "40", followed by the label "(min)".

On the right side of the interface, there are two buttons: "Cambiar Puertos Originales" and "Cambiar Puertos No Deseados".

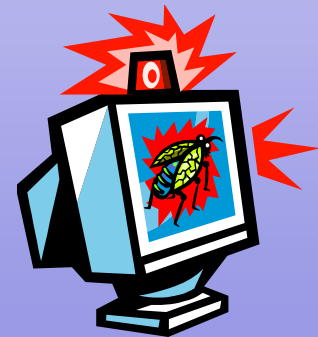
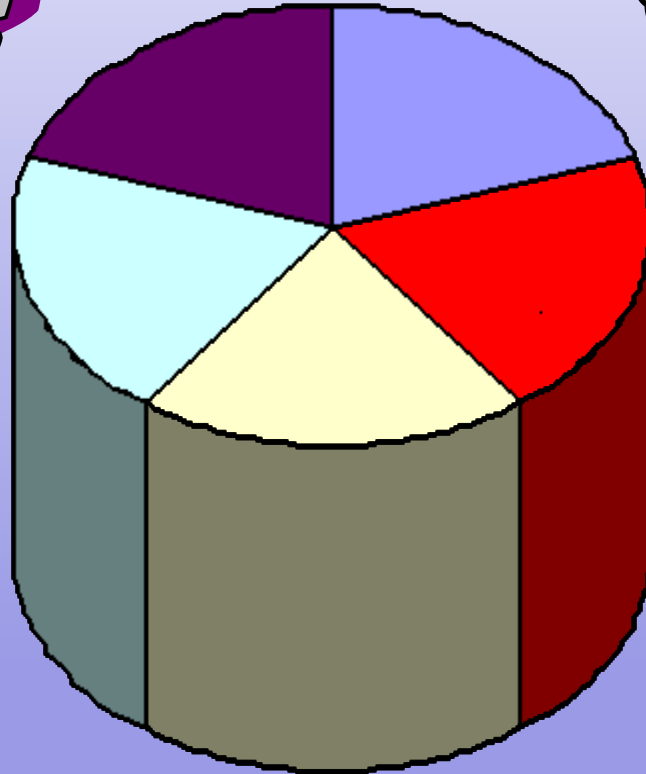
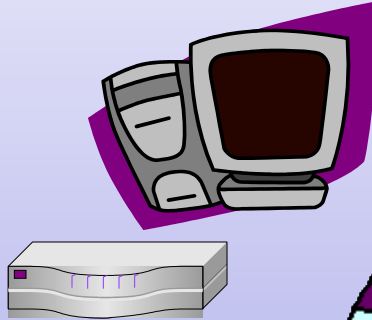
Base de Datos

El Diseño

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

Base de Datos

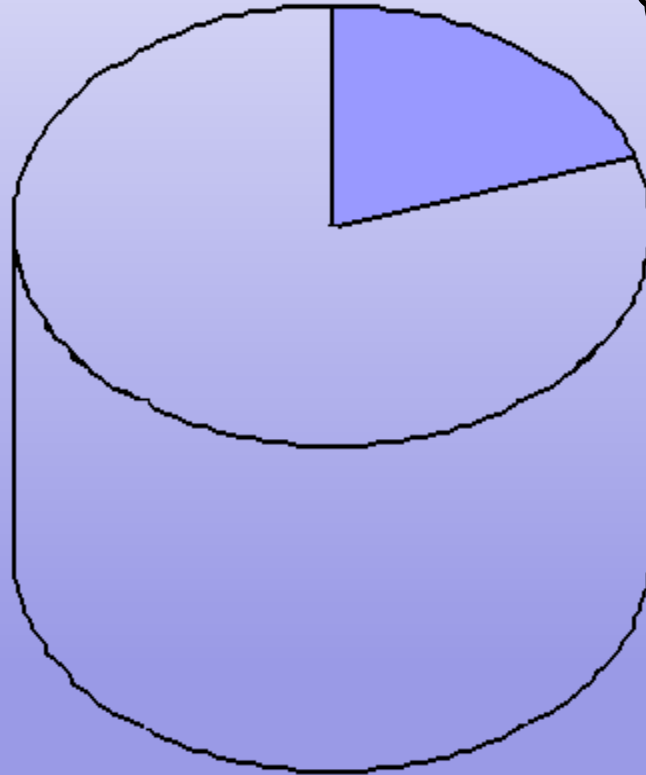
La Aplicación



@IP

Base de Datos

Usuarios



Base de Datos

Usuarios

Detalle Usuario

CODIGO

D.N.I.

NOMBRE

APELLIDOS

EMAIL

TELÉFONO

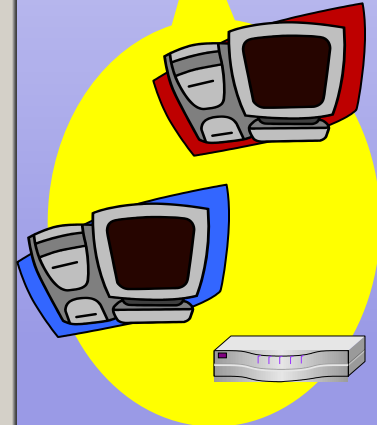
DEPARTAMENTO

DISPOSITIVOS

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

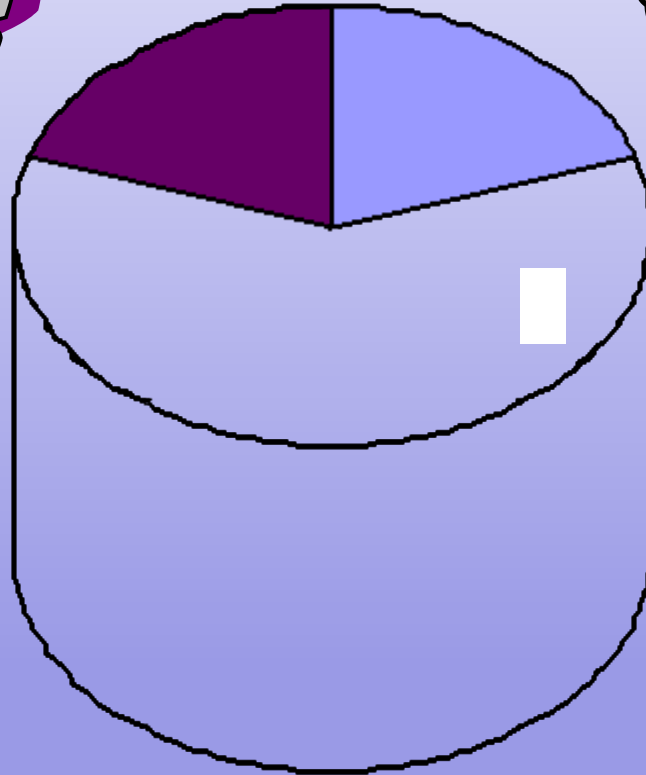
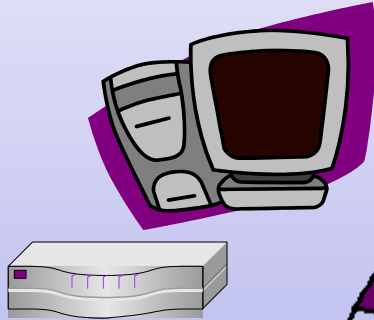
**DATOS
PERSONALES**



**DISPOSITIVOS
ASIGNADOS**

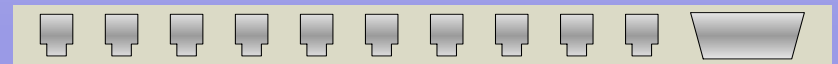
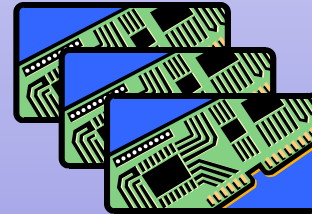
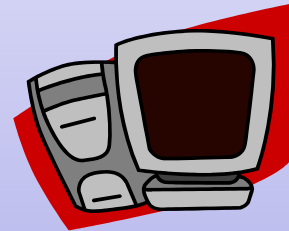
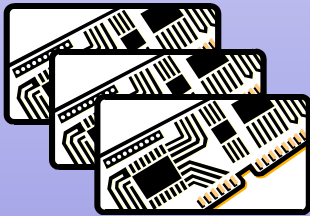
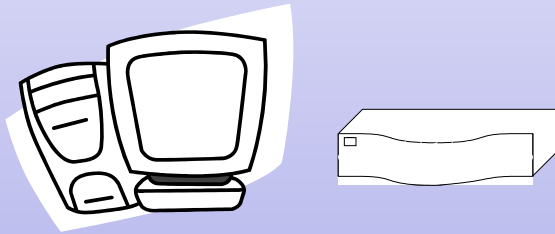
Base de Datos

Dispositivos



Base de Datos

Dispositivos



Base de Datos

Dispositivos

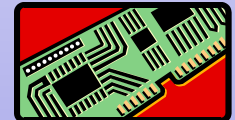
Gestión de Puertos

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

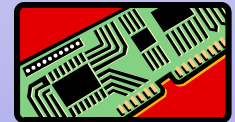
Detalle Dispositivo

GENERAL | INTERFACES | INCIDENCIAS

INTERFAZ

INTERFAZ	VLAN	CONECTA A	
		DISPOSITIVO	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			

10.0.0.13



VLAN

Base de Datos

Dispositivos

Detalle Dispositivo

GENERAL | INTERFACES | **INCIDENCIAS**

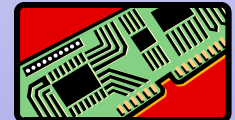
INCIDENCIAS

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

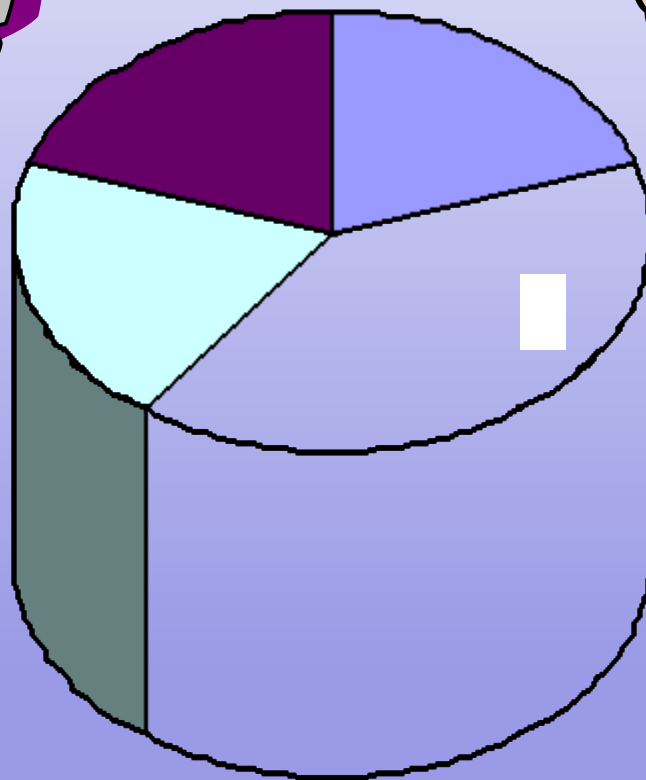
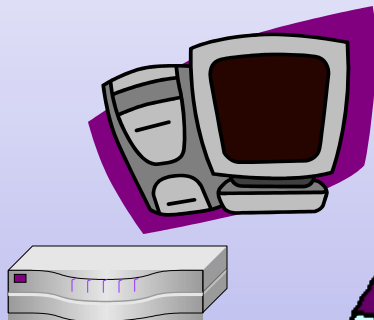


10.0.0.13



Base de Datos

Conexiones



Base de Datos

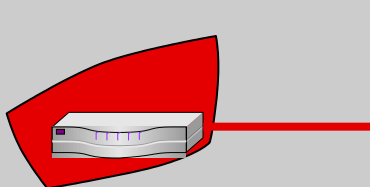
Conexiones

Detalle Dispositivo

GENERAL | INTERFACES | INCIDENCIAS

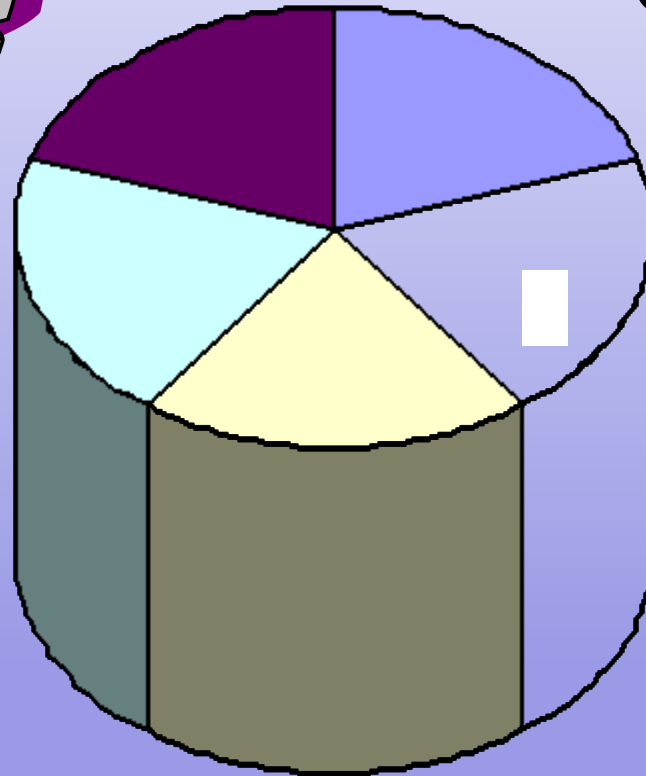
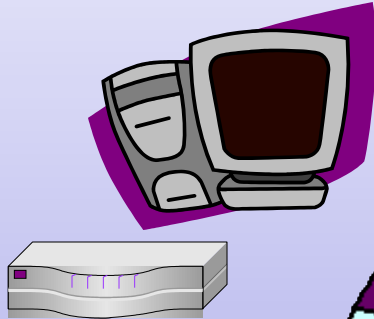
CONEXIÓN

INTERFAZ	VLAN	CONECTA A DISPOSITIVO	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			



Base de Datos

Gestión de IPs



@IP

Base de Datos

Gestión de IPs

CONFIGURACIÓN DE RED

USO ACTUAL

COD	DISPOSITIVO	@MAC	RES?	DESCRIPCIÓN	ALTA	LAST
67678	3	33:33:33:33:33:33	N		18/12/2003	19/12/2003

Gestión de IPs

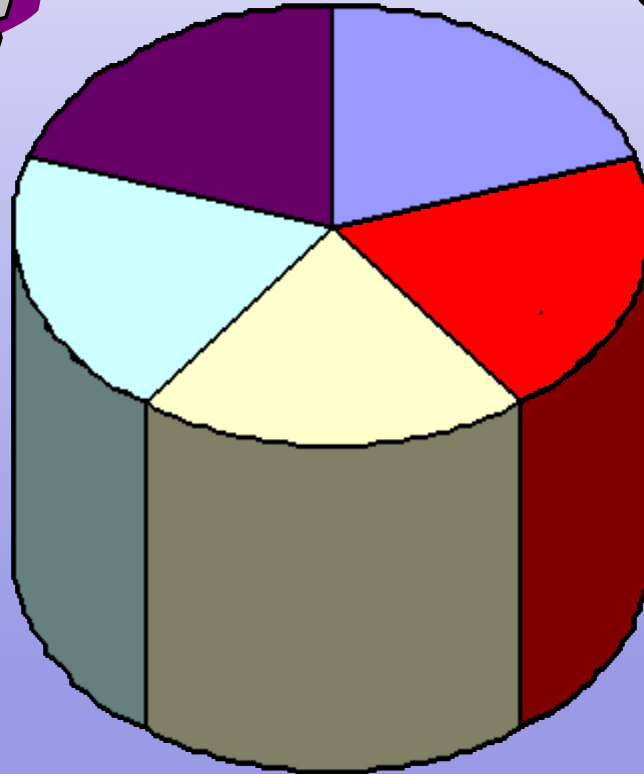
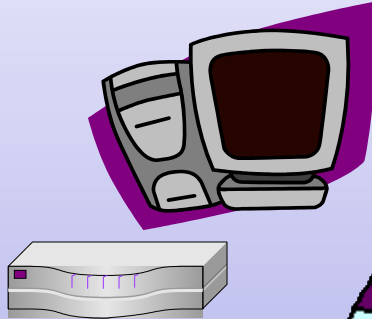
[illegible]

Gestión de IPs

[illegible]

Base de Datos

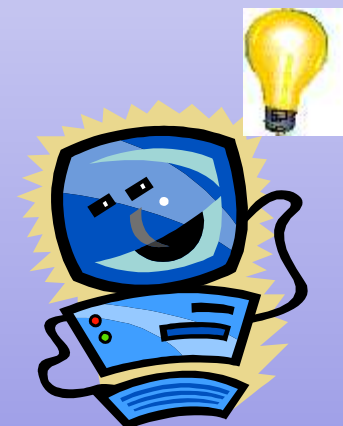
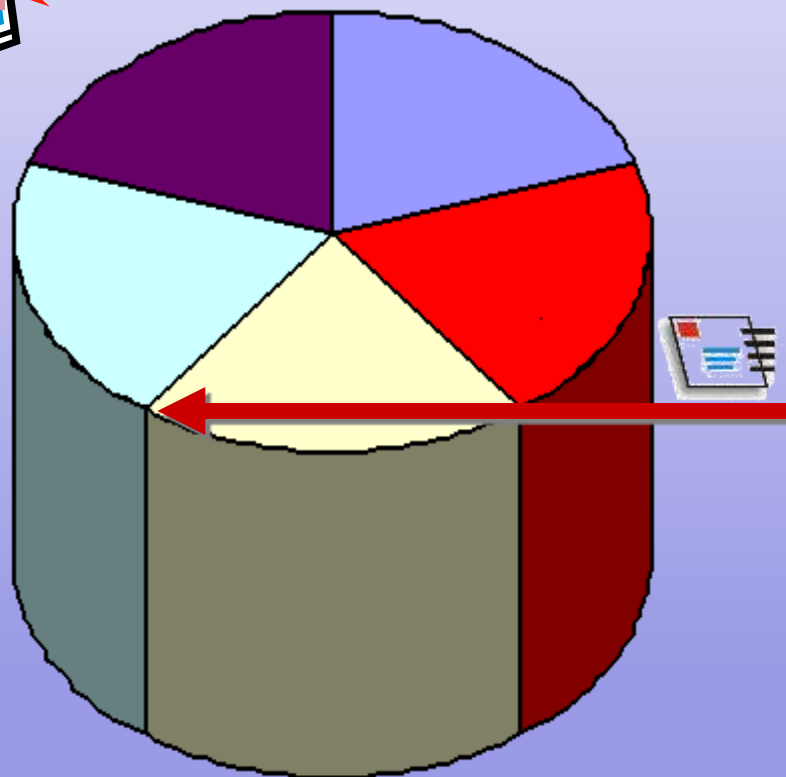
Incidencias



@IP

Base de Datos

Incidencias



Base de Datos

Incidencias

DISPOSITIVO

Detalle Incidencia

CÓDIGO TIPO

@IP

@MAC @IP

DISPOSITIVO INTERFICIE

SOCKET

DESCRIPCIÓN FECHA

SOLUCIÓN FECHA

EDIFICIO








PLANTA

ACTUALIZACIÓN BBDD

UBICACIÓN FÍSICA



Conclusiones

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