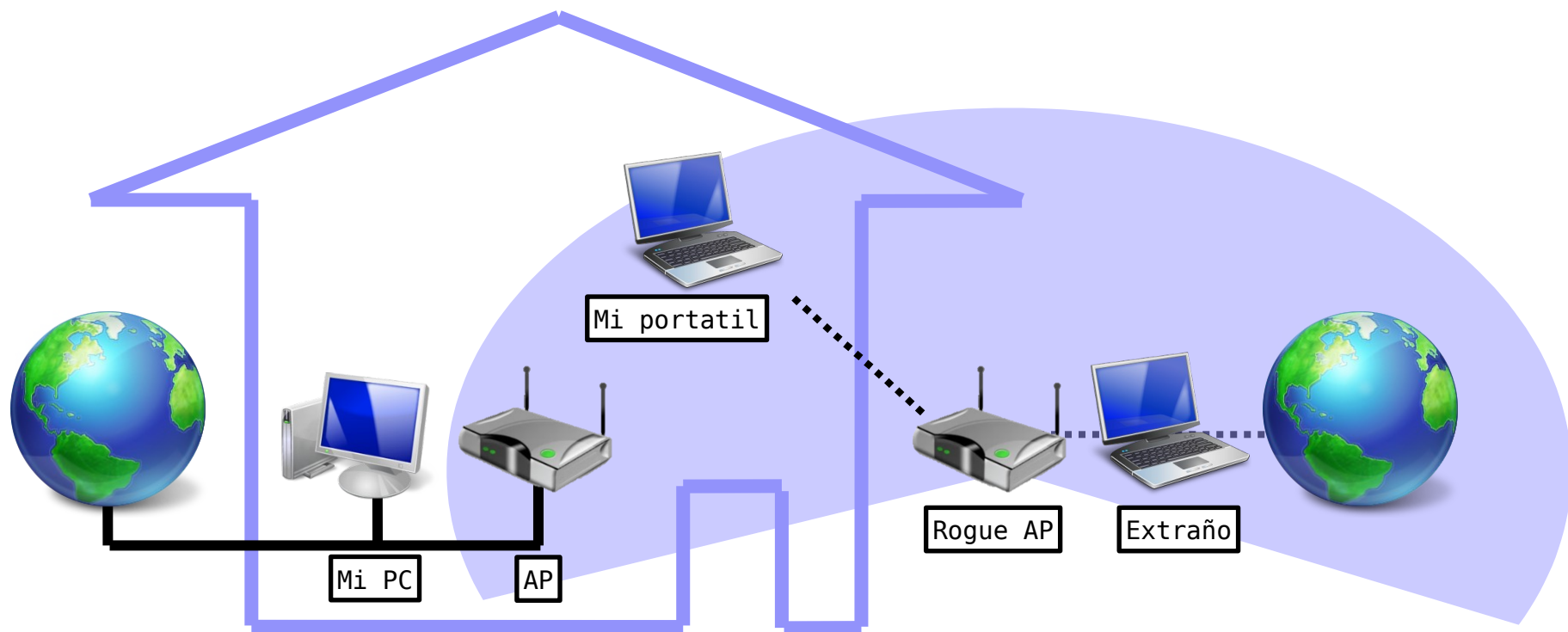


Detección de puntos de acceso falsos en redes WiFi



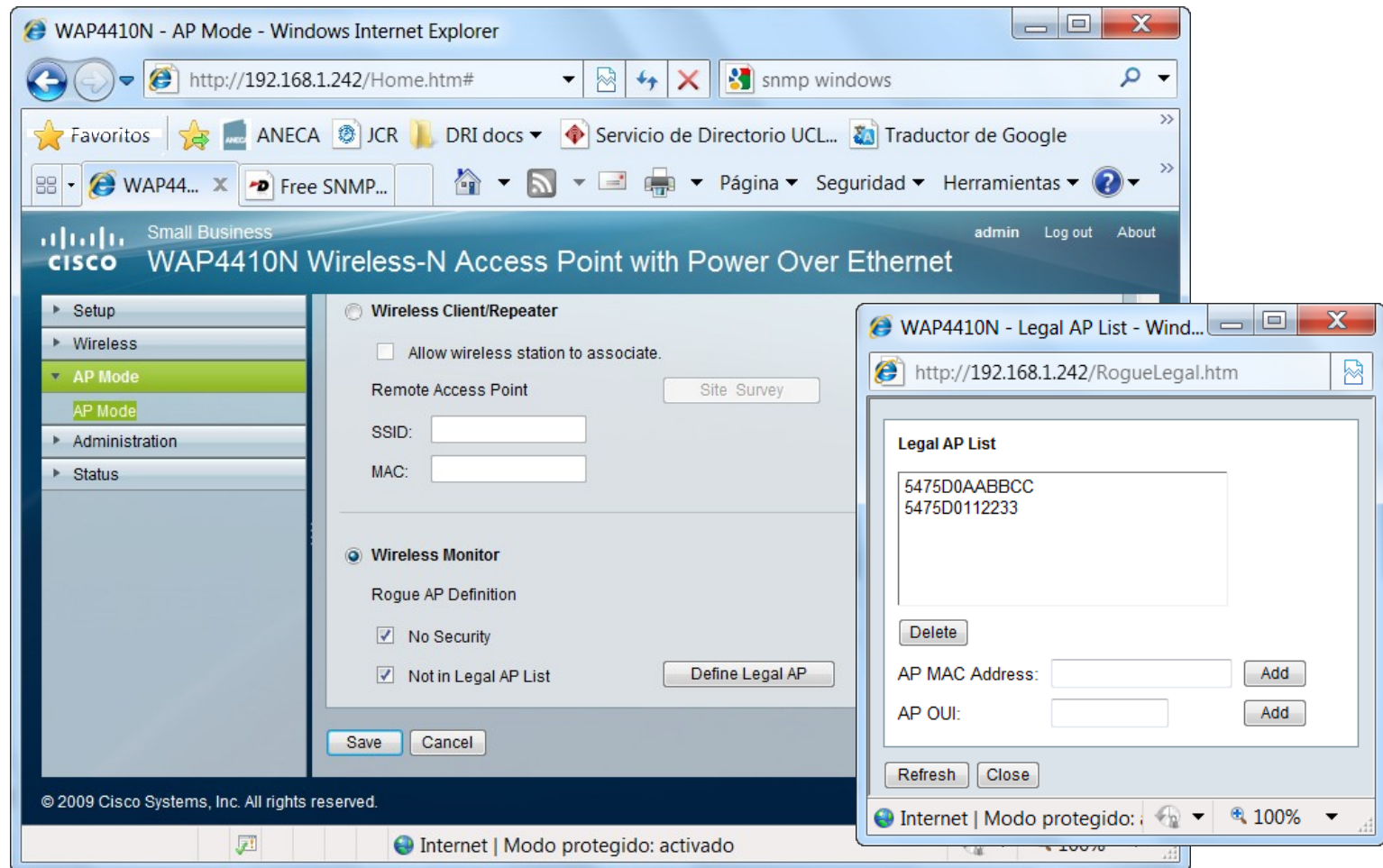
Protección contra falso AP

¿Qué es un AP falso?



Protección contra falso AP

AP monitor – Configuración



Protección contra falso AP

AP monitor – Log de eventos

Small Business
cisco WAP4410N Wireless-N Access Point with Power Over Ethernet

Setup
Wireless
AP Mode
Administration
Management
Log
Diagnostics
Factory Default
Firmware Upgrade
Reboot
Configuration Management
Status

Log

Email Alert
E-Mail Alert: ☐ Enabled ☒ Disabled
SMTP Server:
E-Mail Address for Logs:
Log Queue Length: entries
Log Time Threshold: seconds

Syslog Notification
Syslog Notification ☐ Enabled ☒ Disabled
Syslog Server IP Address: . . .

Log
☒ Unauthorized Login Attempt ☒ Authorized Login
☒ System Error Messages ☒ Configuration Changes

© 2009 Cisco Systems, Inc. All rights reserved.

WAP4410N - Log View - Windows Internet Explorer

http://192.168.1.242/log_data.htm

Log

Jan	1	00:13:53	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:14:14	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:14:35	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:14:56	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:15:17	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:15:38	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:15:59	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:16:20	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:16:41	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:17:02	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:17:23	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:17:44	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:18:05	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:18:26	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:18:47	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:19:08	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:19:29	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:19:50	syslog:	5475D0B31169	Rogue AP[Illegal]
Jan	1	00:20:12	syslog:	5475D0B31169	Rogue AP[Illegal]

Internet | Modo protegido: activado 100%

Protección contra falso AP

AP monitor – Traps SNMP

Small Business WAP4410N Wireless-N Access Point with Power Over Ethernet

- ▶ Setup
- ▶ Wireless
- ▶ AP Mode
- ▼ Administration
 - Management
 - Log
 - Diagnostics
 - Factory Default
 - Firmware Upgrade
 - Reboot
 - Configuration Management
- ▶ Status

SNMP

SNMP v1 & v2: ☒ Enabled ☐ Disabled

Contact: DRILab242

Device Name: WAP4410N

Location: Albacete

Get Community : public

Set Community: public

SNMP Trap-Community: public

SNMP Trusted Host: ☐ Any IP Address

☒ 192 . 168 . 1 . 11 ~ 12

SNMP Trap-Destination: 192 . 168 . 1 . 12

Save

Cancel

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**.

Identification

In the Contact field, enter contact information for the AP. In the Device Name field, enter the name of the AP. In the Location field, specify the area or location where the AP resides.

Get Community

Enter the name of your Get community.

Set Community

Enter the name of your Set community.

SNMP Trusted Host

If you want to be able to access the AP from any IP address, select **Any IP Address**. If you want to specify an IP address or range of IP addresses, then select the second option and complete the fields provided.

SNMP Trap-Community

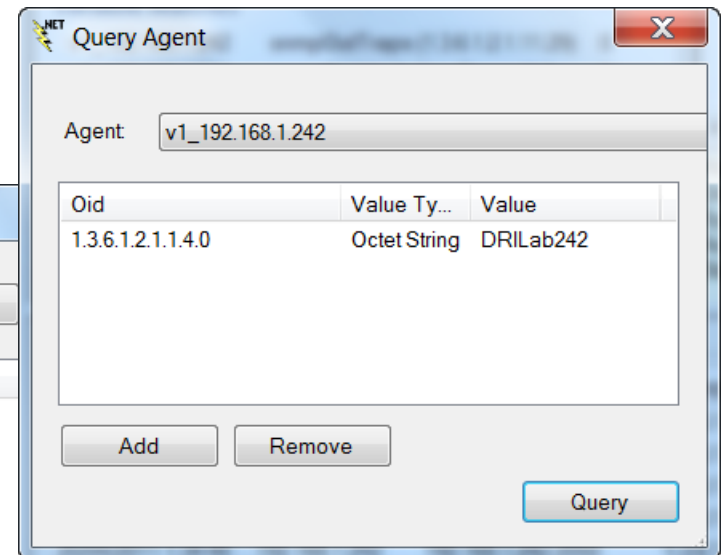
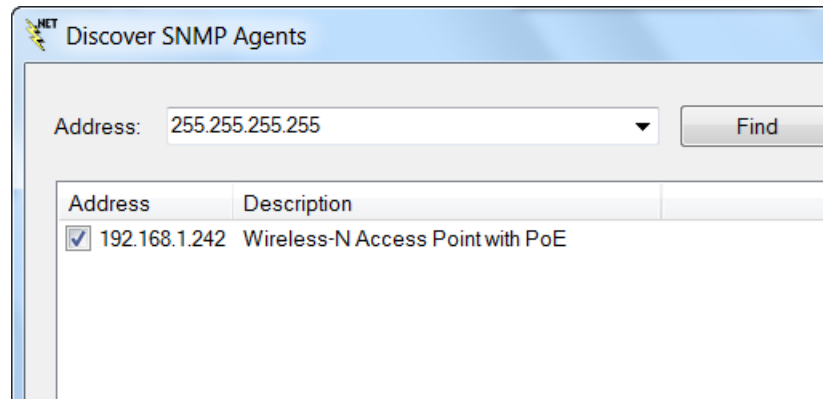
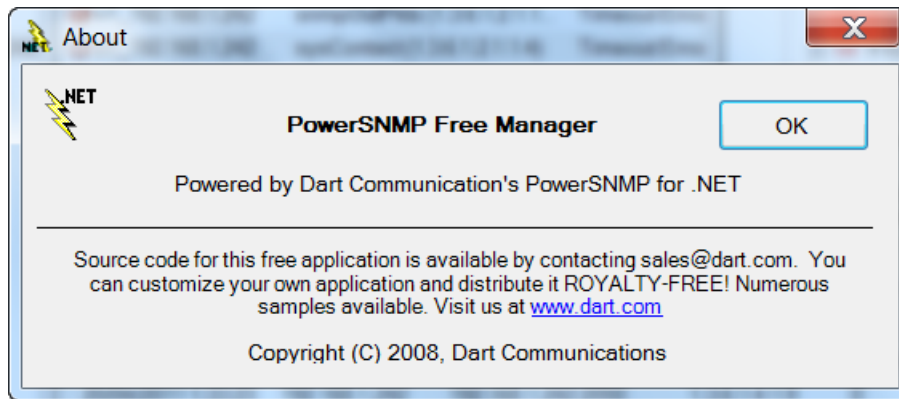
Enter the name of your Trap community.

SNMP Trap-Destination

Enter the destination IP Address.

Protección contra falso AP

Configuración de gestor SNMP



Protección contra falso AP

Configuración de gestor SNMP

The screenshot displays the PowerSNMP Free Manager application window. The interface is divided into several sections:

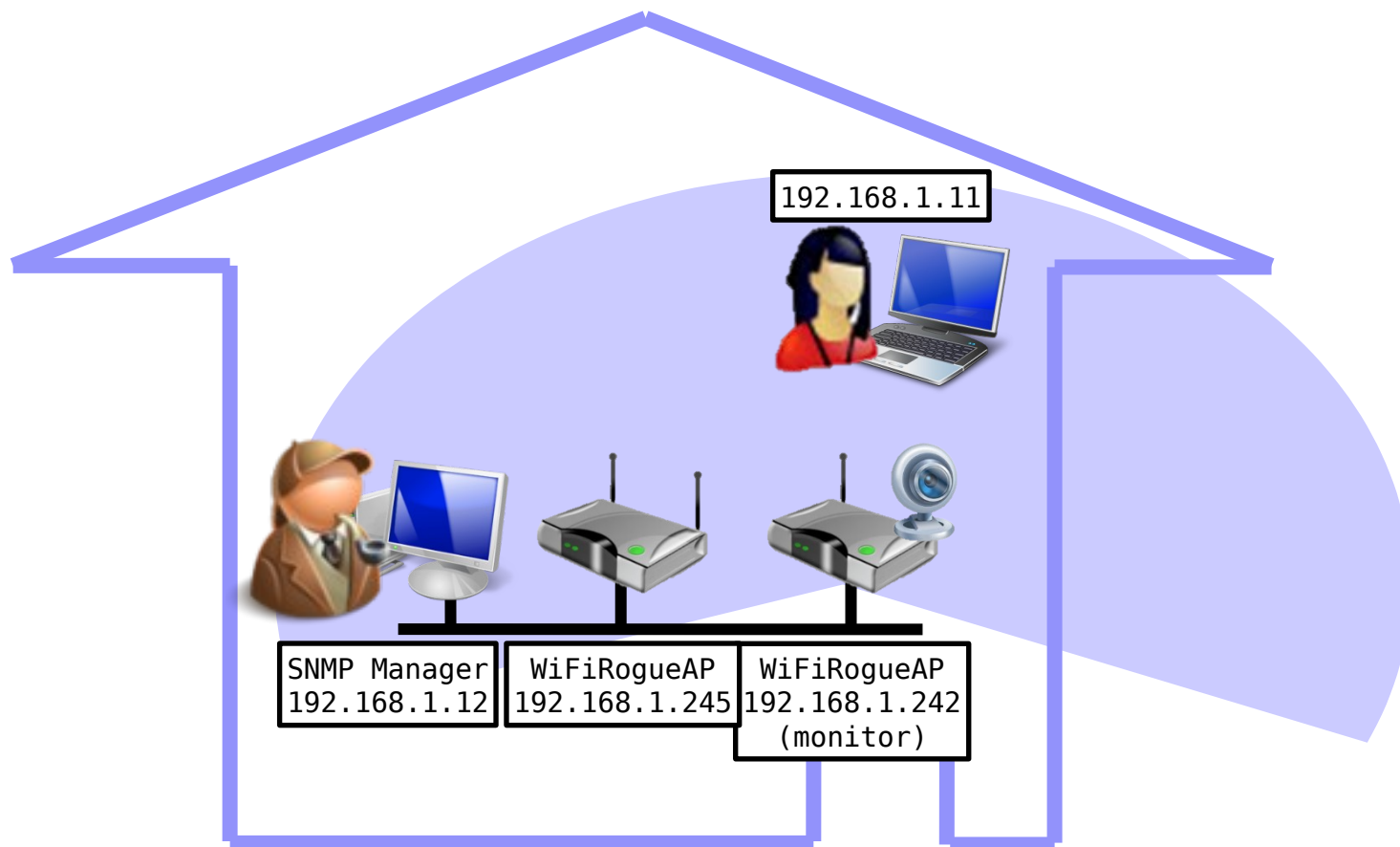
- Left Panel (Tree View):** Shows a hierarchy of discovered devices. Under 'Discovered Devices', there are 'Network Nodes' and 'SNMP Agents'. Under 'SNMP Agents', there are folders for 'SNMPv1', 'SNMPv2', and 'SNMPv3'. The 'SNMPv1' folder is expanded, showing a specific agent 'v1_192.168.1.242'.
- Top Panel (Table):** Titled 'Variable Watches', it lists the values of various MIB variables for the selected agent. The table has three columns: 'Agent Address', 'Variable (Oid)', and 'Value'.
- Right Panel (Tree View):** Shows a list of MIB objects for the selected agent. The objects are: 5 sysName, 6 sysLocation (highlighted with a yellow background), 7 sysServices, 8 sysORLastChange, 9 sysORTable, and 2 interfaces. Below this list, the details for the selected 'sysLocation' object are shown: Name: sysLocation, Oid: 1.3.6.1.2.1.1.6, Syntax: OctetString (SIZE (0..255)), Access: ReadWrite, Status: Mandatory.
- Bottom Panel (Table):** Titled 'Traps', it shows a list of received traps. The table has six columns: 'Time', 'Sender', 'Originator', 'Enterprise', 'Specific Trap', and 'Generic Trap'.

Agent Address	Variable (Oid)	Value
v1_192.168.1.242	snmpOutPkts (1.3.6.1.2.1.1...	3912
v1_192.168.1.242	sysContact (1.3.6.1.2.1.1.4)	DRILab242
v1_192.168.1.242	sysName (1.3.6.1.2.1.1.5)	WAP4410N
v1_192.168.1.242	sysLocation (1.3.6.1.2.1.1.6)	Albacete

Time	Sender	Originator	Enterprise	Specific Trap	Generic Trap
20/04/2011 1:33:23	192.168.1.242	192.168.1.242:2050	1.3.6.1.4.1.9	0	0
20/04/2011 1:33:44	192.168.1.242	192.168.1.242:2050	1.3.6.1.4.1.9	0	0
20/04/2011 1:34:05	192.168.1.242	192.168.1.242:2050	1.3.6.1.4.1.9	0	0
20/04/2011 1:34:27	192.168.1.242	192.168.1.242:2050	1.3.6.1.4.1.9	0	0
20/04/2011 1:34:48	192.168.1.242	192.168.1.242:2050	1.3.6.1.4.1.9	0	0

Protección contra falso AP

Montaje a realizar



Protección contra falso AP

Montaje a realizar

