HOW TO

Configurazione SNMP

SIEMENS

Contents

Configurazione SNMP

Il seguente tutorial vi permetterà di configurare e gestire, via SNMP, gli scalance W.
L'obiettivo non sarà quello di un minuzioso elenco delle molteplici variabili e funzioni presenti nel MIB del dispositivo ma mostrarvi, attraverso alcuni esempi, la struttura che dovrete utilizzare per sfruttare al meglio le potenzialità del protocollo SNMP.

Nel caso specifico vedremo come:
1. come attivare/disattivare la scheda WiFi.
2. come attivare/disattivare la porta Et. di uno scalance X managed.
3. come cambiare il canale Tx di un access point.

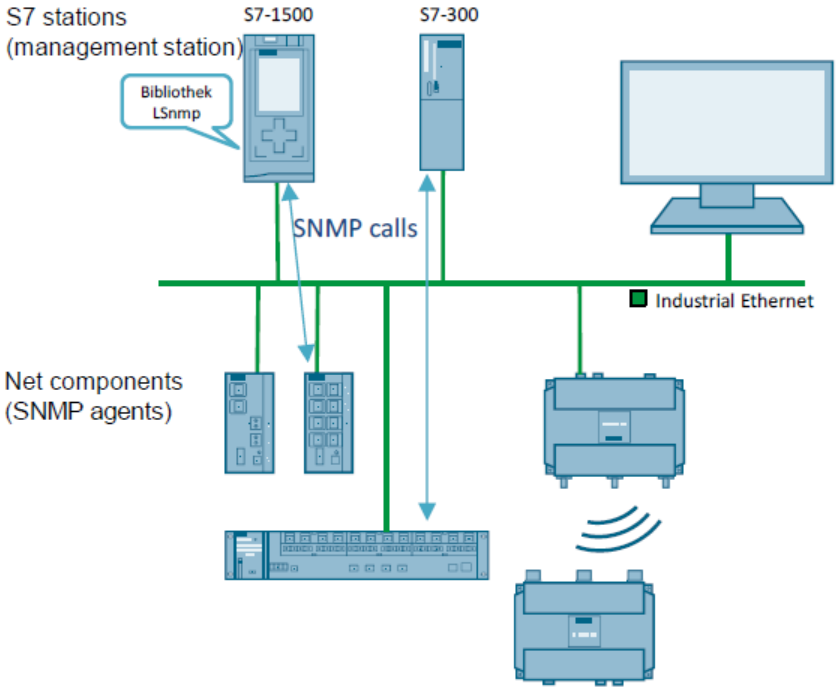
Nota importante: Se non siete interessati a leggere le nozioni base del protocollo SNMP e volete iniziare fin da subito a configurare il PLC, iniziate la lettura dalla sezione dedicata all'esempio applicativo

Come funziona il protocollo SNMP?

La funzione principale del protocollo SNMP è quella di rendere possibile una supervisione ed una gestione centralizzata di tutti i componenti di una rete.

I compiti fondamentali di questo protocollo sono:

1. monitoraggio dei componenti di rete (informazioni sulla rete/configurazione/stato, dati statistici, ecc.)
2. il controllo e la configurazione dei componenti di rete.



Il protocollo SNMP si basa fondamentalmente sui seguenti componenti:

1. SNMP Manager
2. Agent SNMP
3. Management Information Database, definito anche Management Information Base (MIB).

Un manager SMNP ha la responsabilità di attivare comunicazione e di inviare le interrogazioni ai dispositivi di rete dotati di agent SNMP.
Nel nostro caso la CPU veste il ruolo di manager SNMP.
Al Manager sono affidati i seguenti compiti:

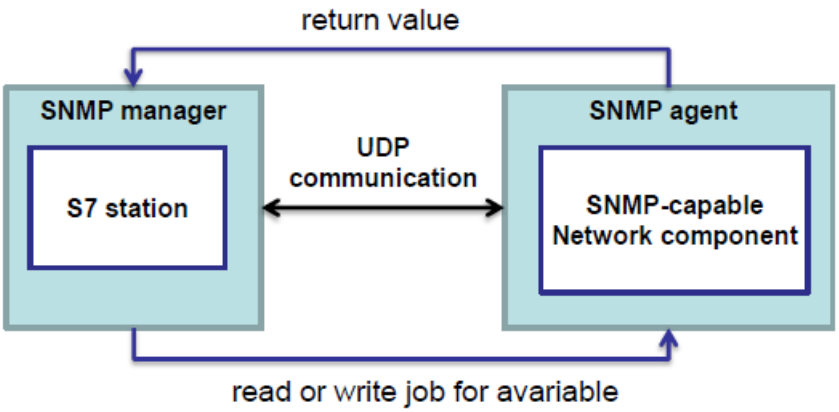
1. Interroga gli agent (funzione GET, GET NEXT, ecc.)
2. Imposta le variabili negli agent (funzione SET)
3. Riconosce gli eventi asincroni provenienti dagli agenti (funzione TRAP)

L'agent è un programma incorporato in un qualsiasi dispositivo di rete che supporta il protocollo SNMP. Abilitando l'agent, si consente al programma di popolare il database MIB (Management Information Base) con delle informazioni specifiche di quel prodotto. Queste informazioni sono rense disponibili all'SNMP Manager, quando questo invia all'agent uno dei comandi sopra elencato (GET, SET, GET NEXT, ecc.).
I compiti dell'agent SNMP sono:

1. Archiviare e recuperare le informazioni di gestione, come definite nel MIB.
2. Segnalare un evento al manager (TRAP).

.

Riassumendo la descrizione fatta fin ora del protocollo SNMP in uno schema, possiamo rappresentare la relazione manager/agent SMNP in questo modo:



Entrando nel merito della comunicazione tra manager ed agent, in questo esempio applicativo vedremo come utilizzare quattro possibili tipologie di richieste. In elenco i dettagli:

GET-request:
le GET-request sono messaggi standard utilizzati per richiamare una determinata serie di dati sul dispositivo di rete desiderato.

GET NEXT-request:
questo formato di messaggio è necessario quando sono richieste una serie di dati (es. dati raccolti in tabelle)

GETBULK-request:
l'applicazione manager può inviare una GETBULK-request (solo con vers. SNMPv2), per richiedere un numero definito di dati con un'unica request. Una sorta d'invio multiplo di diverse richieste GET NEXT.

SET-request:
le SET-request permettono al manager di modificare una o diverse serie di dati del dispositivo di rete.
Esempi: attiva/disattiva scheda wifi o una specifica porta di uno switch.

Trap SNMP:
il trap SNMP è un messaggio dell'agent che viene inviato al manager station senza richiesta.
L'agent agisce indipendentemente dal manger e attiva l'invio del TRAP solo su una serie di specifici eventi imprevisti.
Esempi: Fault di una porta, interferenza WiFi, ecc.

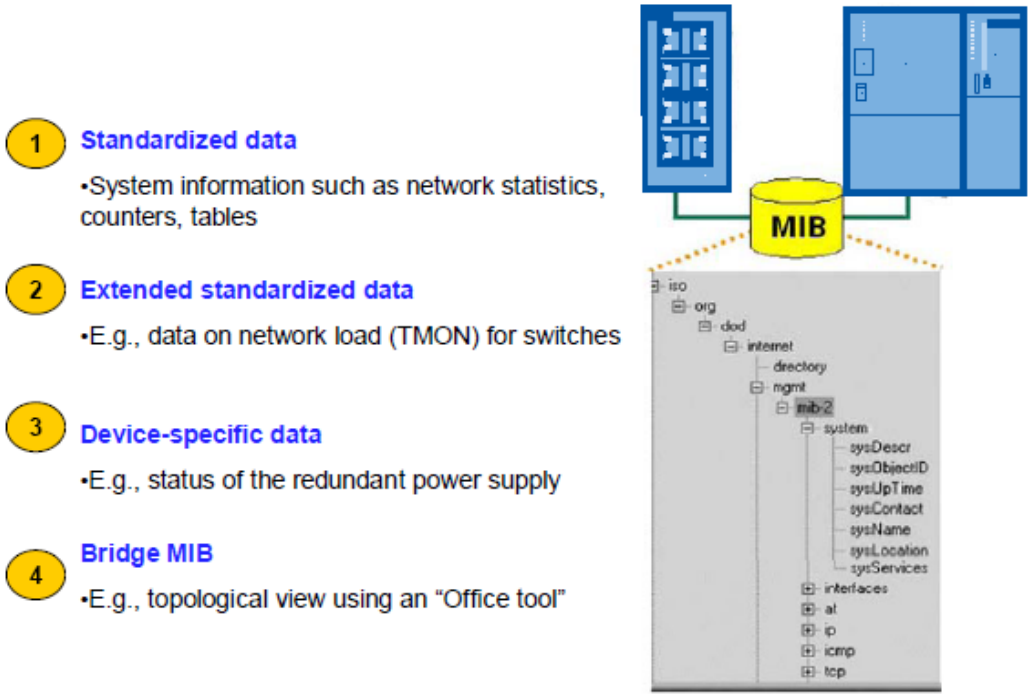
Qui sotto una tabella, estratta dal manuale, che riassume quando appena descritto:

Function	Description	SNMP version
SnmpGet	Request of a SNMP variable from a SNMP agent (get request command).	SNMPv1
SnmpSet	Changing a SNMP variable of a SNMP agent (set request command).	SNMPv1
SnmpGetNext	Expanding the get request; Enables an automatic execution and request of the following objects within an OID subtree.	SNMPv1
SnmpGetBulk	Expanding the GetNext request; Makes the request of large data volumes of a SNMP agent with only one response frame possible.	SNMPv2
SwitchIO	Includes the functions "SnmpGet" and "SnmpSet" for switching the digital output of an IWLAN client.	SNMPv1

MIB file

Il MIB (Management Information Base) è una struttura di dati standardizzata composta da diverse variabili che rappresentano i parametri (in solo lettura o lettura e scrittura) caratteristici di uno specifico dispositivo. In realtà il MIB è stato oggetto ad un tentativo di standardizzazione per permette al manager di gestire, in una rete eterogenea, di monitorare componenti di diversi produttori.

Ovviamente ci sono molti casi in cui il MIB deve, necessariamente, riportare delle variabili proprie di un dispositivo, non condivisibili con altri apparati.
Per ovviare a questa carenza ogni costruttore, se necessario, è tenuto a fornire il file MIB del proprio prodotto. Vi troverete spesso a dovere gestire le cosiddette "private MIB".



Le variabili inserite nel database MIB sono indicizzate attraverso un codice, chiamato OID (Object Identifier).
Riassumendo.
Immaginate il MIB come costituito da diverse tabelle, organizzate come una serie di directory in una struttura da albero.
I MIB raggruppano diversi tipi di proprietà o variabili del vostro dispositivo ed ogni proprietà/variabile è identificata da un numero o una stringa univoci.
Nel ricercare una variabile o proprietà specifica, potete utilizzare o il numero identificativo (OID) o la stringa. Questi indici sono intercambiabili tra loro ed indipendenti.

Visto nella sua completezza, l’OID è la combinazione di una serie di numeri che identificano:

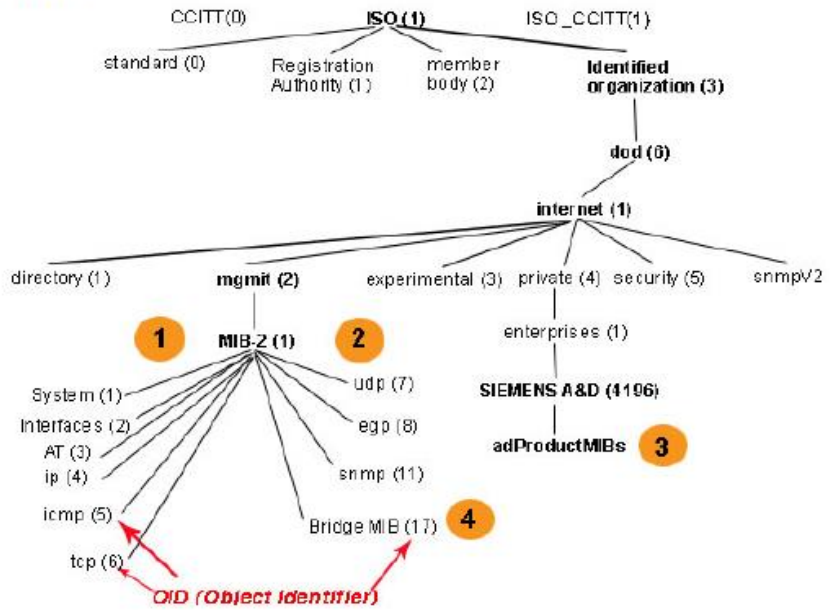
1. il MIB di appartenenza
2. dal codice che identifica il tipo di device
3. dall’identificativo della variabile/proprietà che si vuole leggere o sovrascrivere

Un esempio di OID potrebbe essere il seguente:

1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3.

The figure below shows the structure of the standard MIB (MIB-2):

Figure 3-3

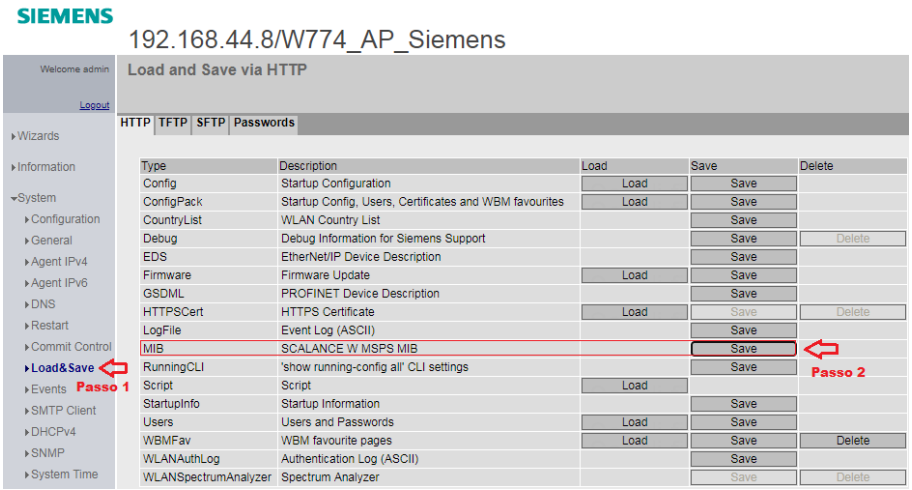


MIB Browser: Applicativo per navigare nei file MIB

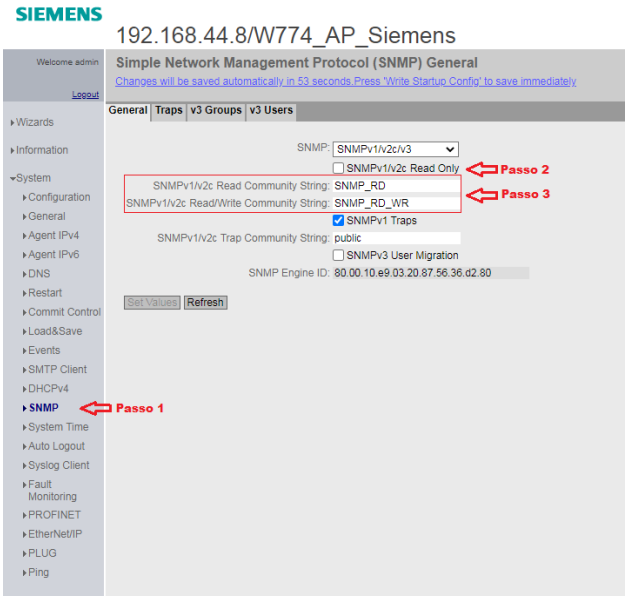
Avrete intuito che navigare all'interno di un MIB potrebbe, soprattutto all'inizio, lasciare disorientati.
Per facilitare l'accesso a queste strutture, ci sono dei software gratuiti che vi posso facilitare l'interazione con questo tipo di file.

Siemens fornisce, su tutta la famiglia Scalance, i propri file MIB.
Il modo più rapido di entrare in possesso di questi file è eseguire il download direttamente dall'interfaccia web del dispositivo.

Dovrete, quindi, dalla pagina web accedere al link SYSTEM→LOAD&SAVE ed eseguire il download del file MIB.



Mantenete la pagina web aperta e configurate le impostazioni SNMP del vostro Scalance.
Indipendentemente dal prodotto troverete le impostazioni SNMP li troverete al seguente link:
SYSTEM→SNMP

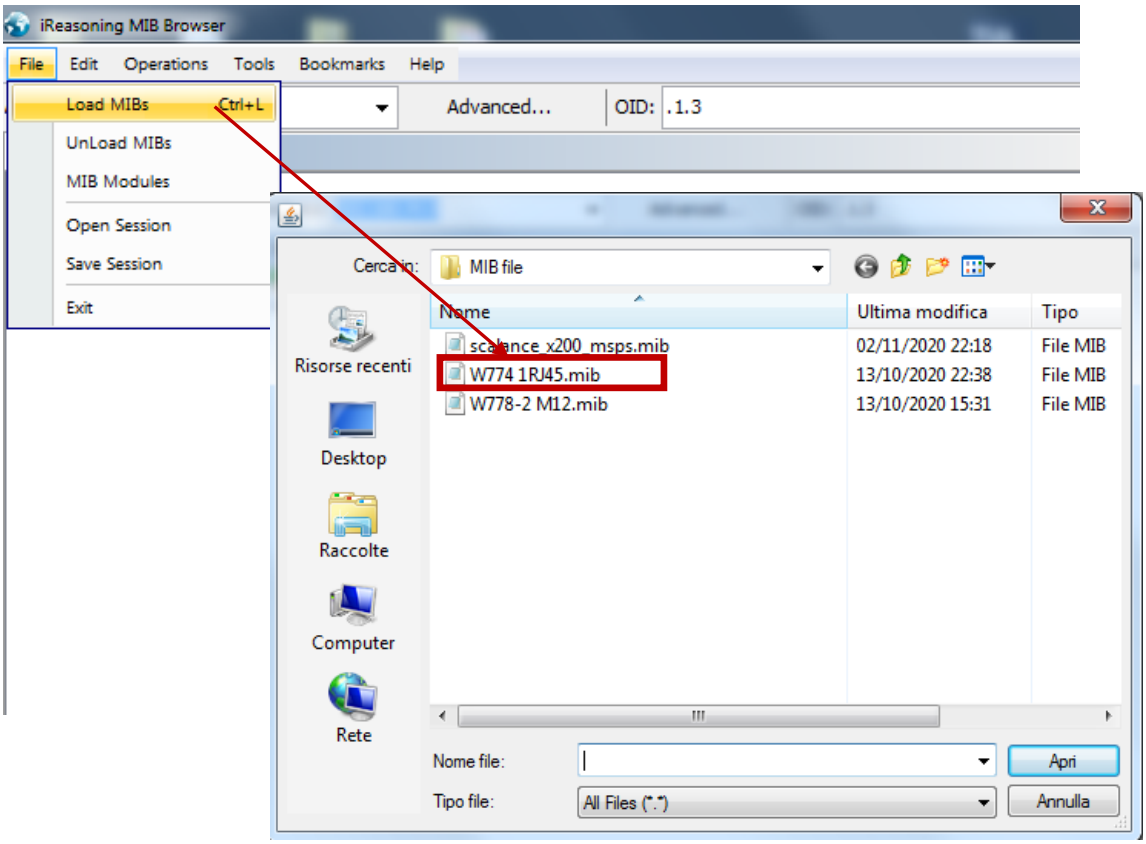


Vi consiglierei, per una questione di sicurezza, di modificare i valori di default dei parametri community string READ e READ/WRITE (passo 3 nell'immagine qui sopra).

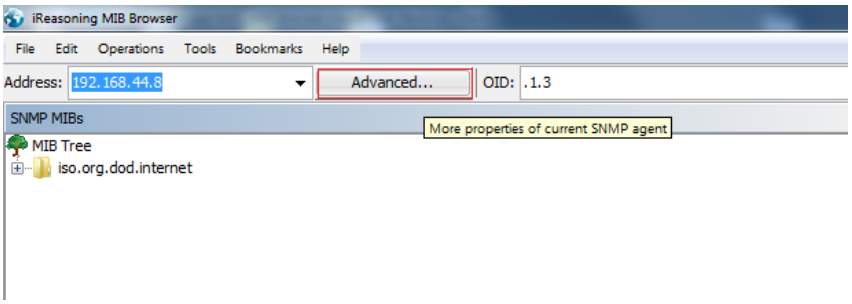
Prendente nota di questi valori, serviranno successivamente per accedere alle variabili del MIB.
Per visualizzare la struttura del file MIB, dovete scaricare un MIB-Browser.
Ci sono diversi software gratuiti che potete scaricare da internet.

Per questo tutorial ho scelto il seguente:
http://www.ireasoning.com/mibbrowser.shtml

Avviate il MIB Browser ed importate il file MIB del dispositivo scalance.
In questo primo caso, ho importato il file di un W774-1 RJ45, un access point da interno quadro.

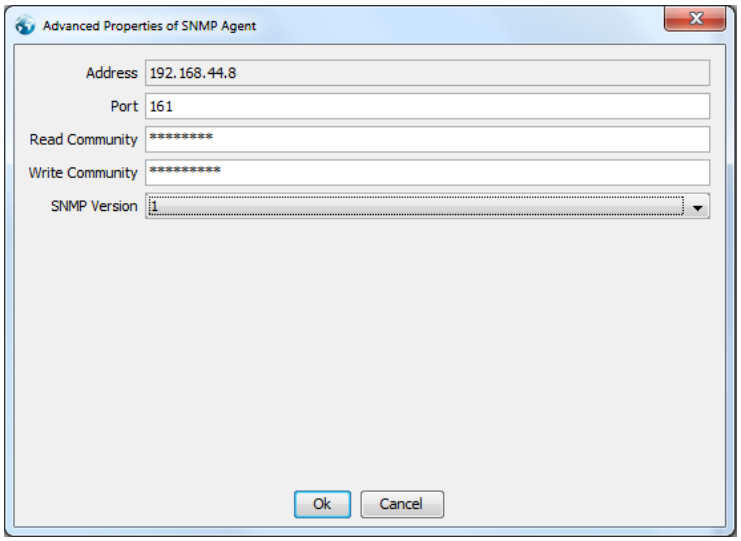


Inserite l'indirizzo IP del dispositivo e premete il pulsante ADVANCED

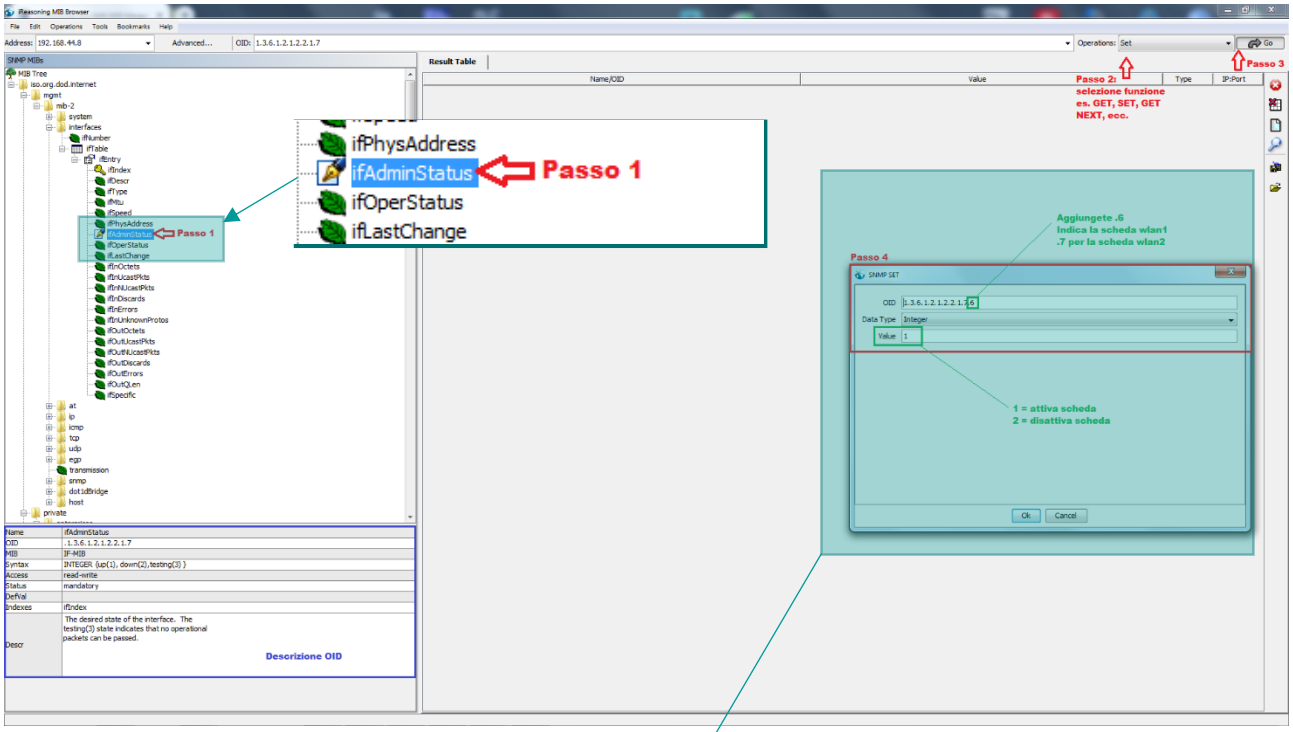


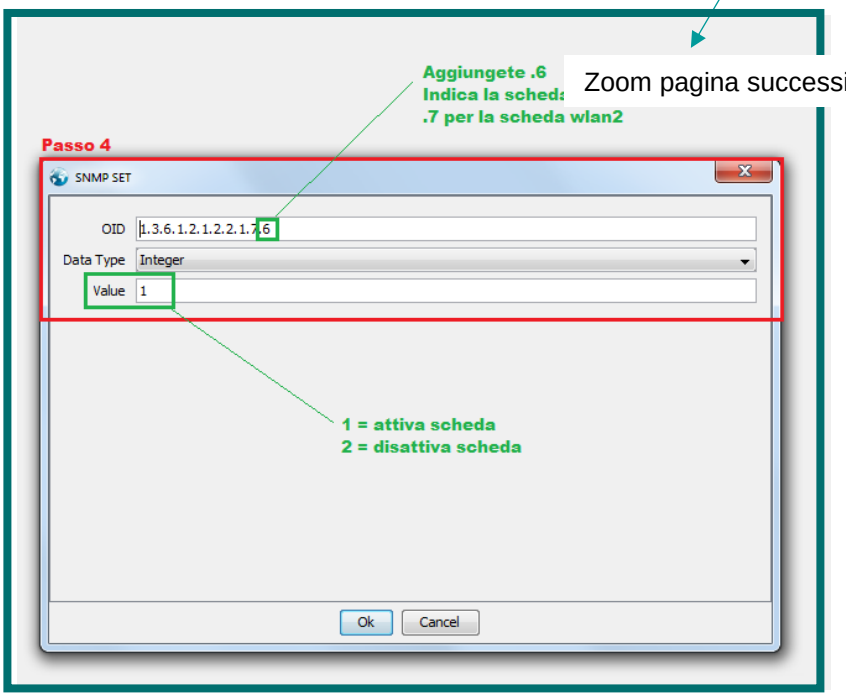
Inserite i valori dichiarati come community nello scalance.
In questo caso specifico:

READ COMMUNITY: SNMP_RD
WRITE COMMUNITY: SNMP_RD_WR



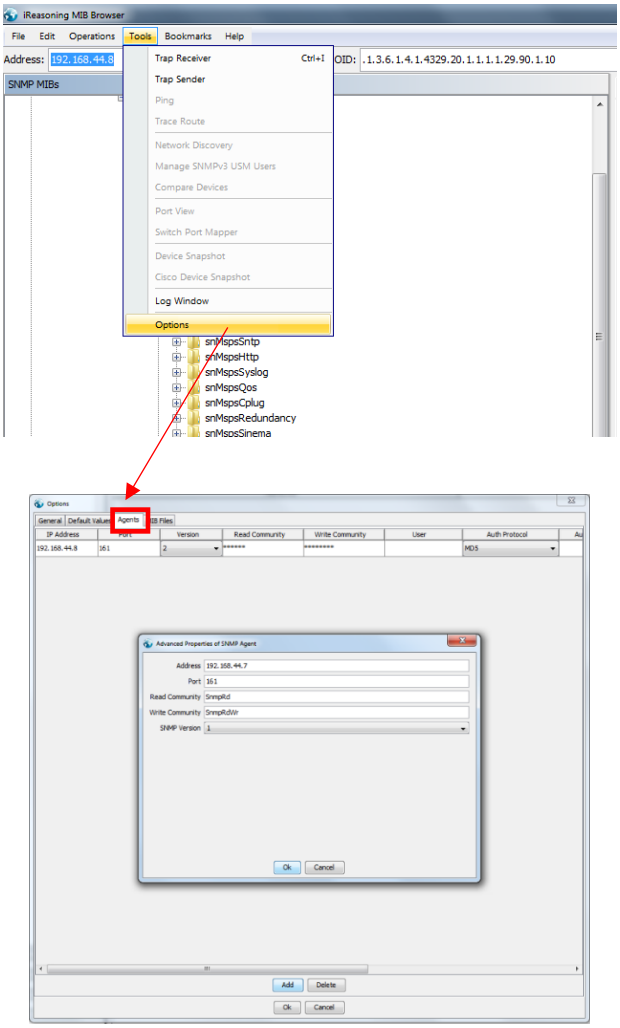
Al termine premete OK.
Questo software oltre a darvi la possibilità di navigare all'interno della struttura MIB, vi permette di poter utilizzare le richieste previste dal protocollo SNMP (GET; SET; GET NEXT; ecc.).
Un ottimo banco prova per capire la sintassi dei comandi e verificarne il funzionamento, prima di utilizzare il progetto TIA portal.
Proviamo, per esempio, a gestire l'attivazione della scheda WiFi dello scalance W.
Seguite le indicazioni riporta qui sotto:



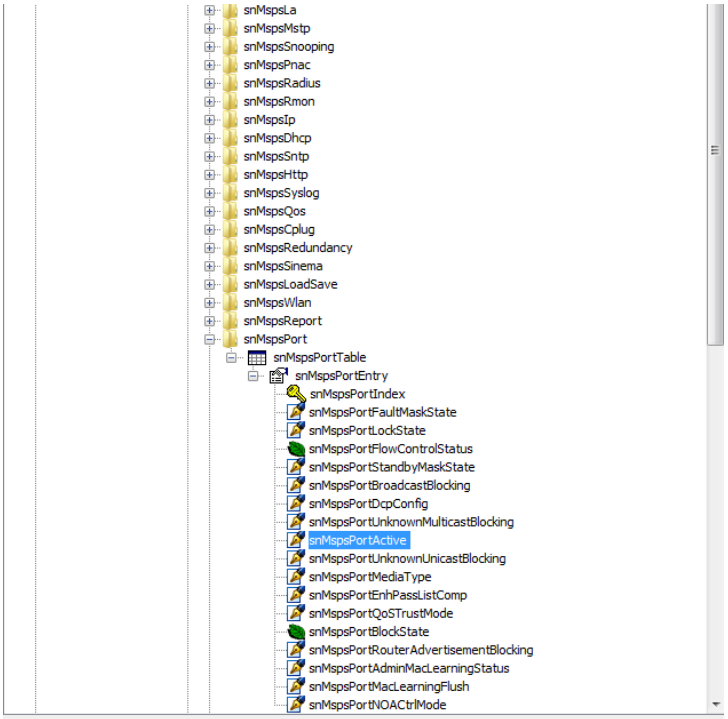


Premete ok.
Vi apparirà un messaggio di conferma.
Tuttavia, la scheda WiFi non si attiverà o, viceversa, non si disattiverà immediatamente.
Il comando viene recepito immediatamente dal dispositivo ma i tempi di reboot della scheda WiFi, richiederanno indicativamente tra i 15 ed i 20 secondi.

Per concludere inizializziamo una seconda connessione.
Inseriamo uno Scalance X e proviamo ad utilizzare lo stesso comando per attivare o meno una porta di uno switch.

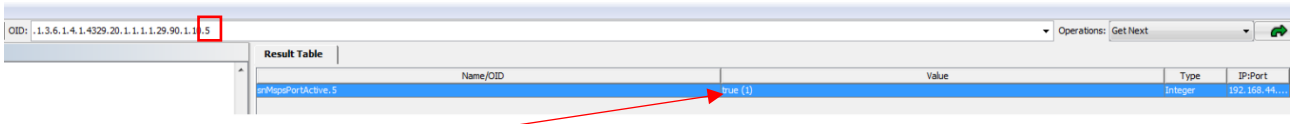


Inserite l'indirizzo IP del dispositivo ed i valori associati alle variabili 'COMMUNITY' che, in questo caso, ho mantenuto identiche a quelli definiti per lo Scalance W.
Importate, ovviamente, anche il file MIB dello switch.
Un consiglio che posso darvi è quello di disinstallare il MIB dello scalance W (barra dei menù: File→Unload MIB) ed installare quello relativo allo Scalance (barra dei menù: File→Load MIB).
In questo modo la struttura del MIB-Browser rimarrà più ordinata.



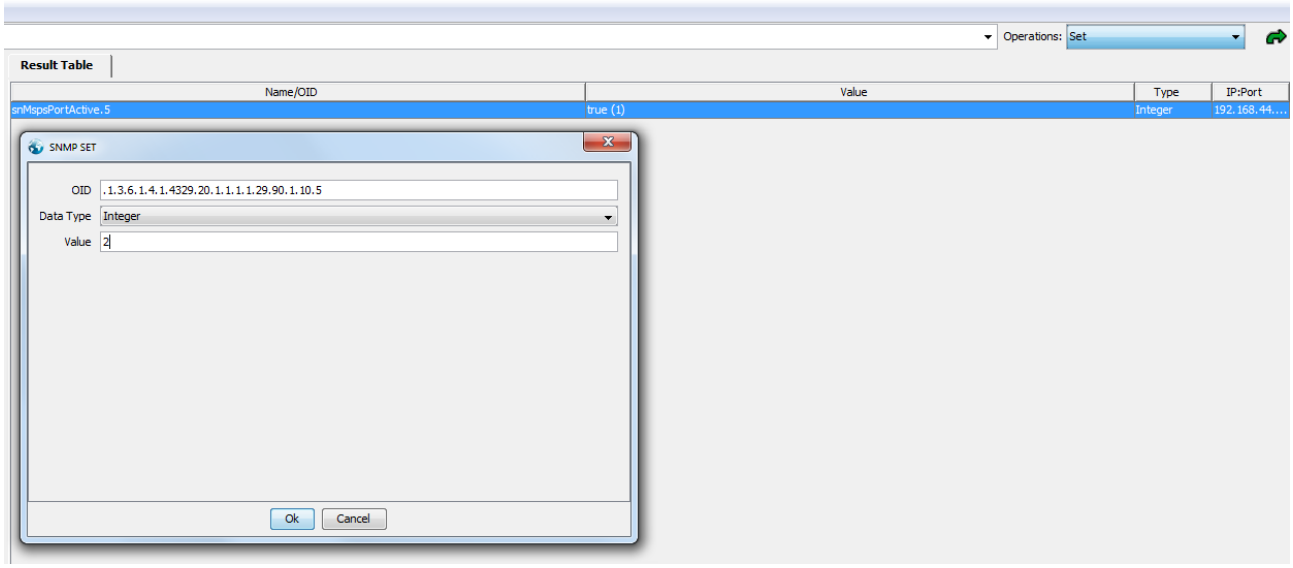
Name	snMspsPortActive
OID	.1.3.6.1.4.1.4329.20.1.1.1.29.90.1.10
MIB	SN-MSPS-SCW-MIB
Syntax	TruthValue (INTEGER) {true(1), false(2) }
Access	read-write
Status	current
DefVal	
Indexes	snMspsPortIndex
Descr	Setting this object to false(2) forces link down on this ports and its connected devices.

Aggiungete al termine del OID il numero di porta che volete gestire (es. la porta numero 5).
Richiediamo lo stato attuale.

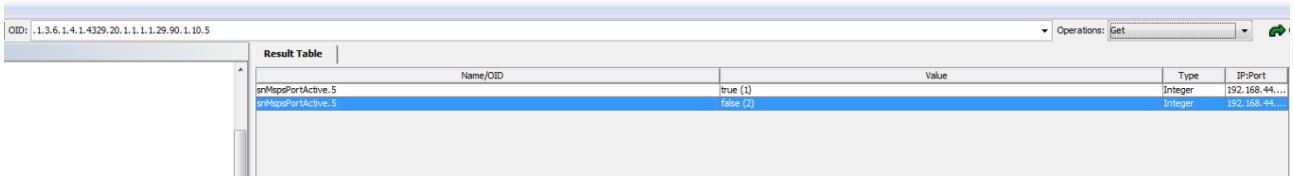


La porta risulta attiva.

Richiamiamo la funzione SET e disattiviamo la porta numero 5 (valore 2).



Una veloce verifica che il comando è stato eseguito correttamente, attraverso la funzione 'GET'.



Come configurare lo scalance W

Riprendo quando già indicato nel capitolo precedente a beneficio di chi è passato direttamente a questo punto.
Per configurare lo Scalance, indipendentemente dalla serie, dovete accedere al web server del vostro dispositivo e accedere al seguente link:

SYSTEM→SNMP

Nota relativa al passo 3.
Vi consiglierei, per una questione di sicurezza, di modificare i valori di default dei parametri community string READ, READ/WRITE e se utilizzerete TRAP anche il valore della rispettiva community

Qui sotto trovate una tabella che riassume, nelle varie revisioni del protocollo SNMP, i livelli di sicurezza adottati di volta, in volta:

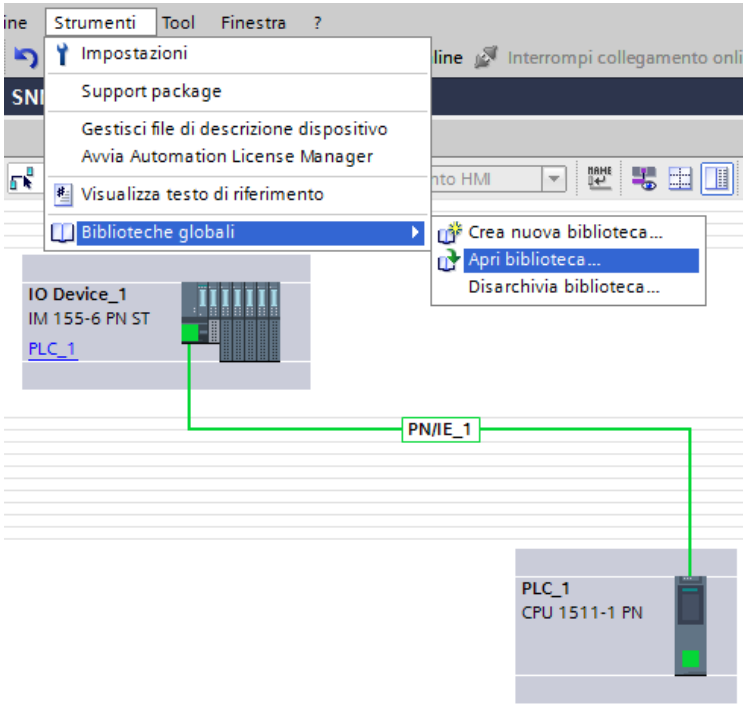
SNMP v1	Sicurezza basata su community
SNMP v2c	Sicurezza basata su community
SNMP v2u	Sicurezza basata sugli utenti
SNMP v2	Sicurezza basata sulla parte
SNMP v3	Sicurezza basata sugli utenti

Come utilizzare l’esempio applicativo

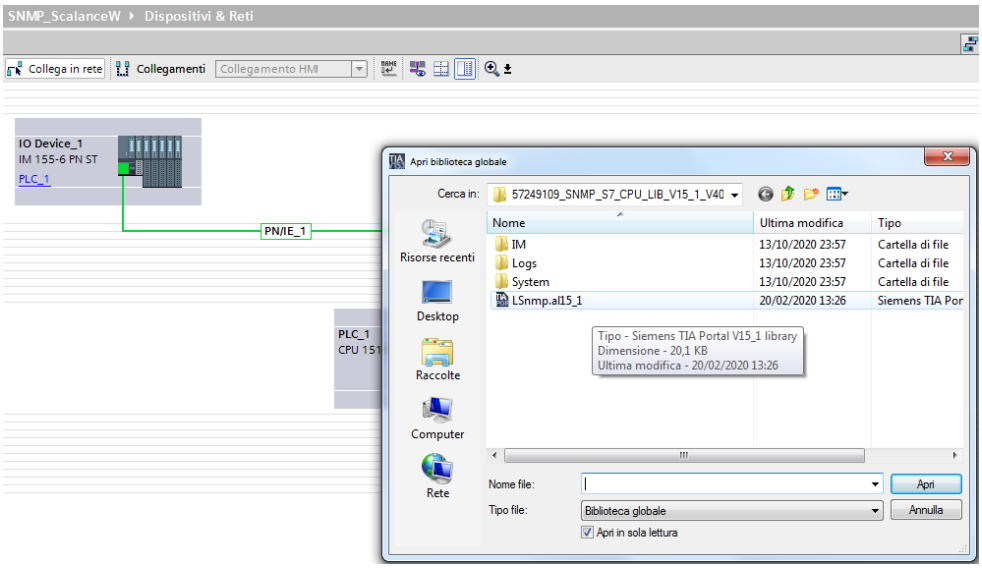
Dovete, innanzitutto, scaricare dal sito Industry Online Support l’esempio applicativo:

https://support.industry.siemens.com/cs/gb/en/view/57249109

Inserite i blocchi dell’esempio applicativo, nel vostro progetto.
Aprite il menù ‘strumenti’, ‘biblioteche globali’ e selezionate la voce ‘apri biblioteca’.

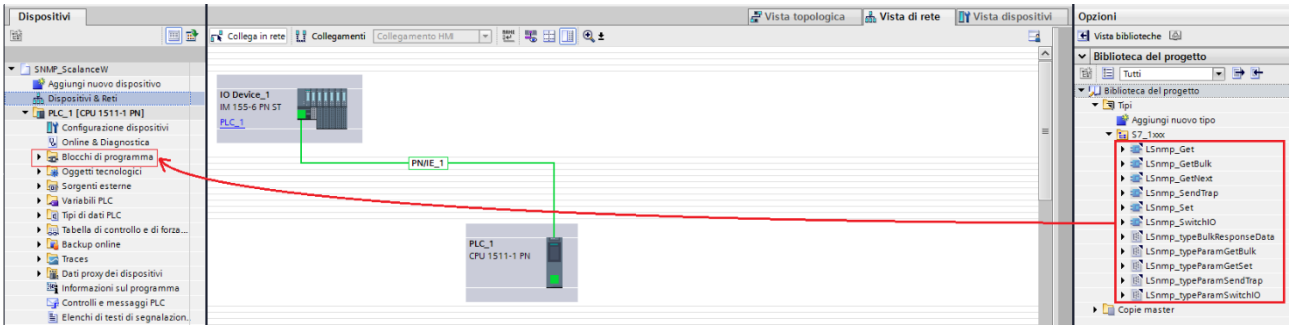


Selezionate la directory dove avete salvato l’esempio applicativo e selezionate il file ‘Lsnmp.al15_1’



Attendente che il TIA Portal termini di caricare la biblioteca dei blocchi.

Selezionate tutta la libreria ed importatela all’interno del vostro progetto.



La libreria di funzioni è costituita dai seguenti blocchi:

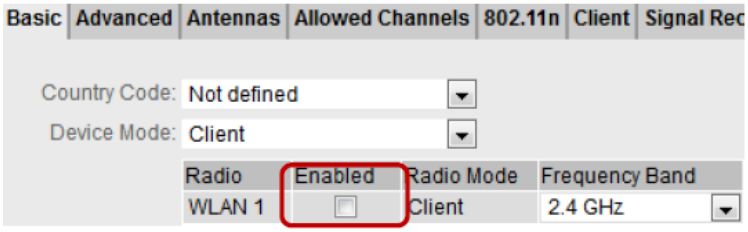
SnmpGet	FB_Block	SET_GET_Blocks
SnmpGetBulk	FB_Block	SET_GET_Blocks
SnmpGetNext	FB_Block	SET_GET_Blocks
SnmpSet	FB_Block	SET_GET_Blocks
SnmpGetParam	DB	SET_GET_Blocks
SnmpSetParam	DB	SET_GET_Blocks
SnmpGetBulkParam	DB	SET_GET_Blocks
typeParamGetSet	UDT	SET_GET_Blocks
typeParamGetBulk	UDT	SET_GET_Blocks
typeParamGetBulkResponseData	UDT	SET_GET_Blocks
SwitchIO	FB_Block	SWITCH_IO_FB
SwitchIOParam	DB	SWITCH_IO_FB
typeParamSwitchIO	UDT	SWITCH_IO_FB

In questa prima versione, vedremo nel dettaglio i blocchi SnmpGet e Set, applicati ad uno scalance W ed un X.

Breve premessa in merito alla costruzione del valore OID dei dispositivi wireless.
Come già detto, l'identificativo OID serve per puntare in lettura o scrittura una particolare variabile della struttura MIB.
Con gli scalance W dovete inserire un ulteriore valore, al termine del OID, che identifica la scheda WiFi "destinataria" del comando.
Analogamente la medesima considerazione, dovrete farla anche per gli switch della famiglia Scalance X.
In questo caso, ovviamente, il numero che andrete ad inserire al termine del "codice" OID, deve identificare la porta dello switch.

Riprendo quando già descritto nel capitolo dedicato al MIB Browser.
Il codice OID per agire sull'attivazione o meno della sceda WiFi è il seguente: '1.3.6.1.2.1.2.2.1.7'

Questo OID agisce come il parametro 'Enable' della pagina web. Link: Interface→WLAN



Come appena detto, questo codice non è sufficiente per gestire la scheda wifi.
Dovete inserire, alla fine del codice OID, uno di questi valori a seconda di quale scheda o SSID volete disabilitare:

- WLAN 1: number 6
- WLAN 2: number 7
- VAP 1.1 – VAP 1.8: numbers 10-17
- VAP 2.1 – VAP 2.8: numbers 30-37
- VAP 1.1 – VAP 1.8: numbers 70-77
- VAP 2.1 – VAP 2.8: numbers 90-97

Quindi il seguente OID agirà sulla prima scheda WiFi:

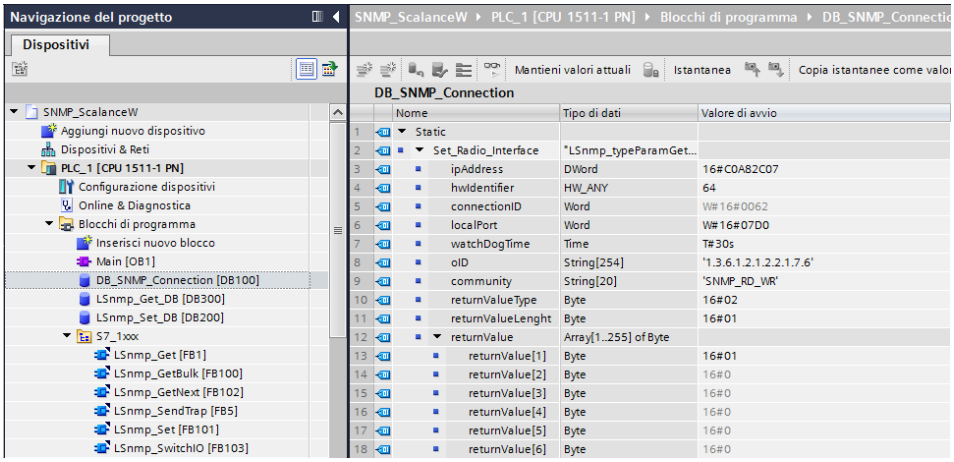
1.3.6.1.2.1.2.2.1.7.6

Questo è solo "l'indirizzo" di destinazione del comando.
Se state agendo in lettura (es. comando GET) avete finito; non servono altre informazioni affinché il comando vada a buon fine.
Se state eseguendo una scrittura dovrete dichiarare, attraverso un valore numerico, che tipo di azione volete portare a termine.
Nel caso specifico dovrete impostare il valore ad 1 o 2:

Integer	Meaning
1	enable
2	disable

Ricordatevi che in questo caso specifico il valore da trasmette come comando è numerico ma, ci sono altri casi dove la variabile può assumere un altro tipo come: string, counter, time, ecc.

Immaginate, per esempio, di voler modificare l'identificativo SSID della vostra rete o volerne dichiarare uno nuovo.
Avrete bisogno di una variabile stringa, per poter agire in tal senso.
Inserite, ora, una DB nel vostro progetto e richiamante al suo interno la UDT: 'typeParamGetSet'



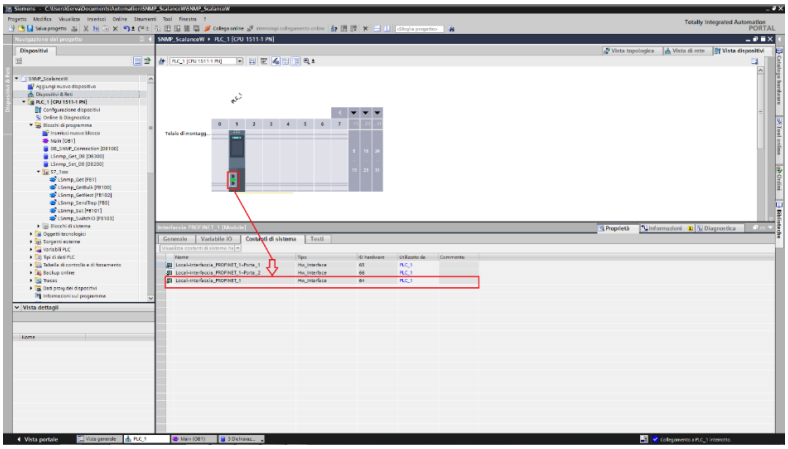
Qui sotto, vedete nel dettaglio la descrizione di ogni parametro di questa DB.

Parameters	Description
ipAddress	IP address of the network components; The IP address must be coded as a hexadecimal value, e.g. 16#AC = 172.
hwIdentifier	Hardware identification of the PROFINET interface for the S7-1500/S7-1200 CPU; **Note:** S7-300/S7-400 CPUs deviceID >> is the local_device_id of the S7-300/S7-400 CPU (see \4\)
connectionID	The SNMP block connection ID required for setting up the UDP access point; **Note:** If you want to plan further open communication connections in addition to the UDP connection, you must select the respective different connection IDs (value range: W#16#0001 to W#16#0FFF).
localPort	The local port number of the UDP connection; If you want to plan further open communication connections in addition to the UDP connection, you must select the respective different local port numbers.
watchDogTime	Monitoring time of the processes; Default value:=4 s
oID	Object identifier of the SNMP variable to be retrieved in SNMP format **(for example, 1.3.6.1.2.1.1.4.0")**; The OID object can be found in the general (RFC1213: MIB II) or in the private MIB file of the device (see \3\)
community	In most cases, "public" is chosen as the community name for read access and "private" for write access. This value must match the community name chosen in the project planning for the network component (see section 3).
returnValueType	Data type of SNMP variable: 02: Integer, 04: String, 41: Counter, 43: Timeticks During the Read access ("LSnmp_Get," "LSnmp_GetNext"), values of SNMP variable type are automatically determined and entered here. For the Write access ("LSnmp_Set"), the type of SNMP variable must be programmed.
returnValueLength	Length of the SNMP variable; During the Read access ("LSnmp_Get," "LSnmp_GetNext"), the length of the SNMP variable is automatically determined and entered here. For the Write access ("LSnmp_Set"), the length of the SNMP variable must be programmed.
returnValue	ARRAY OF BYTE: The array length is limited to 255 bytes. During the Read access ("LSnmp_Get", "LSnmp_GetNext"), the response data of the SNMP variable is entered here. For the Write access ("LSnmp_Set"), the data witch which the SNMP variable should be described must be entered here.

Brevemente, ho compilato la DB in questo modo:

1. IPaddress. L'indirizzo del mio scalance in hex (192.168.44.7 → C0.A8.2C.07)
2. HW ID. Identificativo della scheda della cpu.

Per rilevare questo valore dovete aprire le proprietà della cpu.



Nel mio caso il valore assunto dal HW ID della cpu è 64.
Potete lasciare i parametri 'connectionID', 'localPort' e 'watchDogTime' ai valori di default.

Come OID inserire l'identificativo della variabile.
Il parametro 'Community' deve essere concorde con i valori inseriti nella pagina web degli Scalance (pagina SNMP).

ReturnValueType: dichiarate il tipo (integer, string, ecc.).

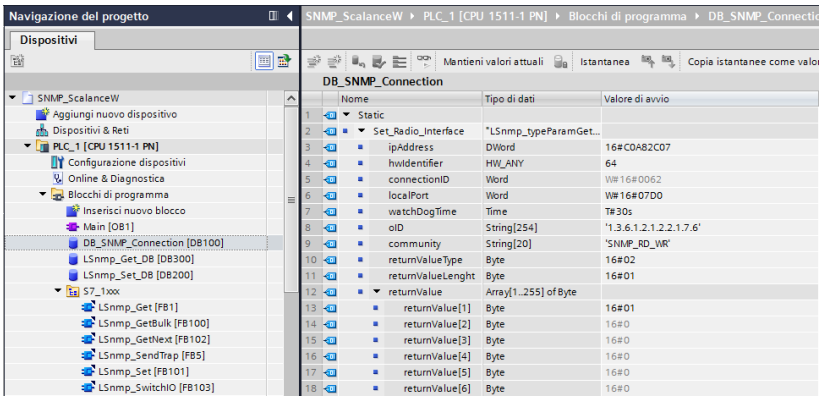
ReturnValueLength: dichiarate quanti byte, dall'array 'returnValue', sono validi per il vostro comando.

ReturnValue. È un array in cui dovete dichiarare il valore da scrivere nella variabile MIB.

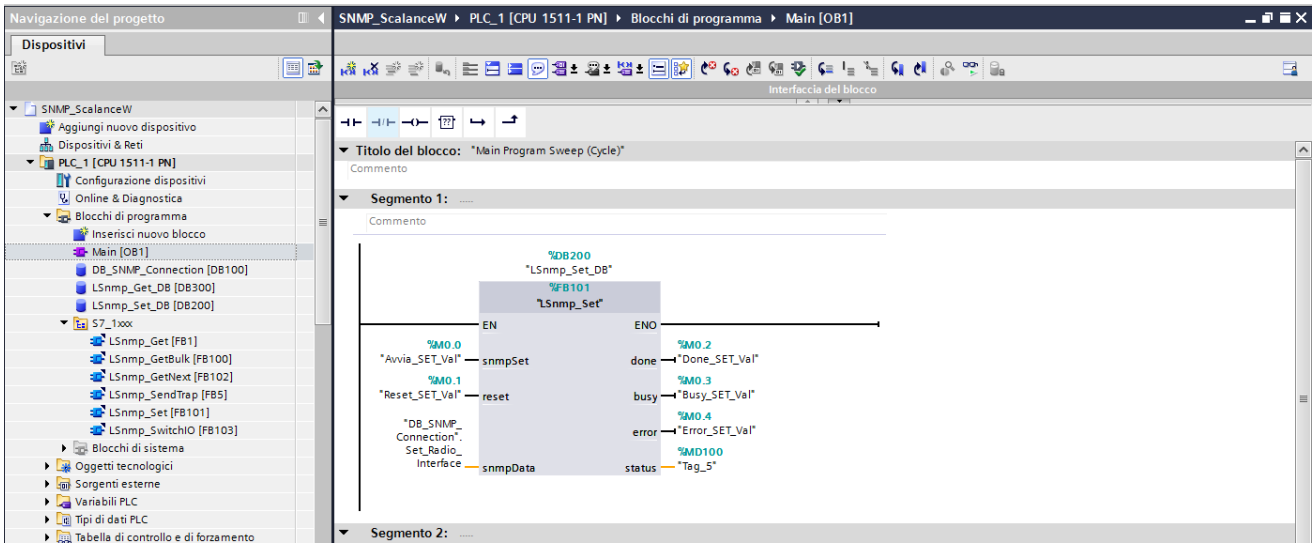
Esempio.
Voglio attivare la scheda WiFi.
Il valore da scrivere nella variabile è 01.
Quindi scriverò 01 nel primo byte dell'array 'return value'.

È un valore di tipo intero. Quindi come 'returnValueType' dichiareremo il valore 02 (=integer).

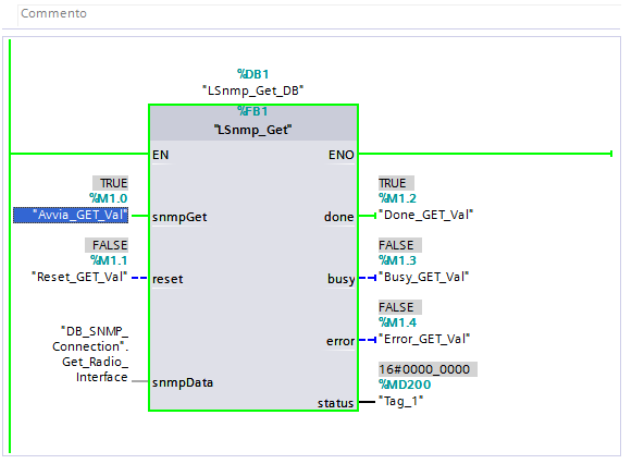
Infine, devo dichiarare quanti bye considerare validi dell'arreay 'return value'.
Come 'ReturnValueLength', in questo caso, dichiarerò 01.



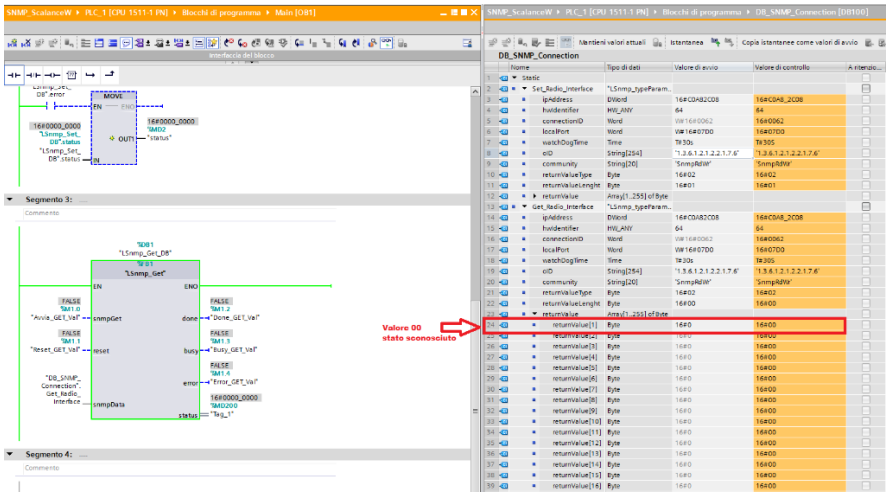
Inserite nel blocco OB1, la funzione 'LSnmp_Set' e 'LSnmp_Get'. Inserite le variabili I/O come indicato nell'immagine qui sotto:



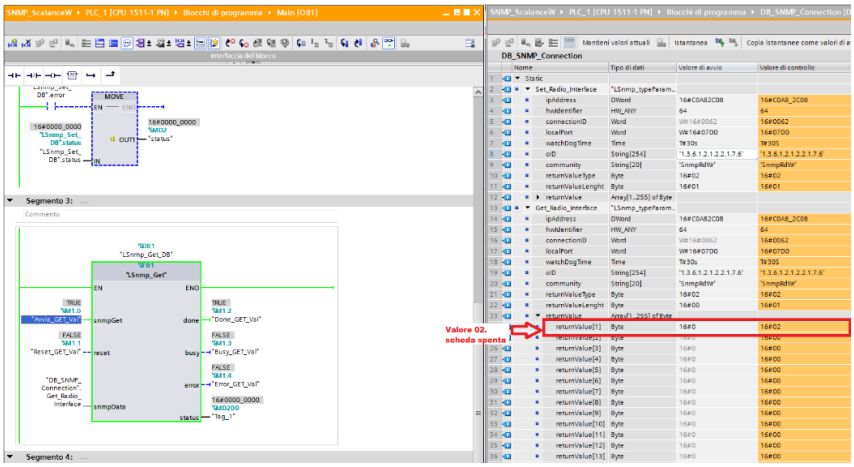
Salvate il programma e compilatelo.
Eseguite il download e andate on-line con la cpu.



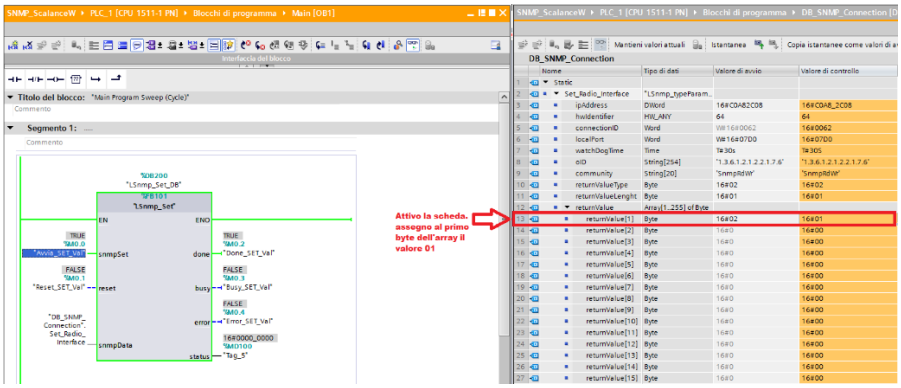
Prima di attivare o meno la scheda WiFi, potrebbe essere utile conoscere lo stato attuale.
Il valore inizialmente indicato nell'array relativo alla chiamata GET ('return value') è '00'.



Attivate la chiamata GET e verificate il valore riportato dell'array 'return value':

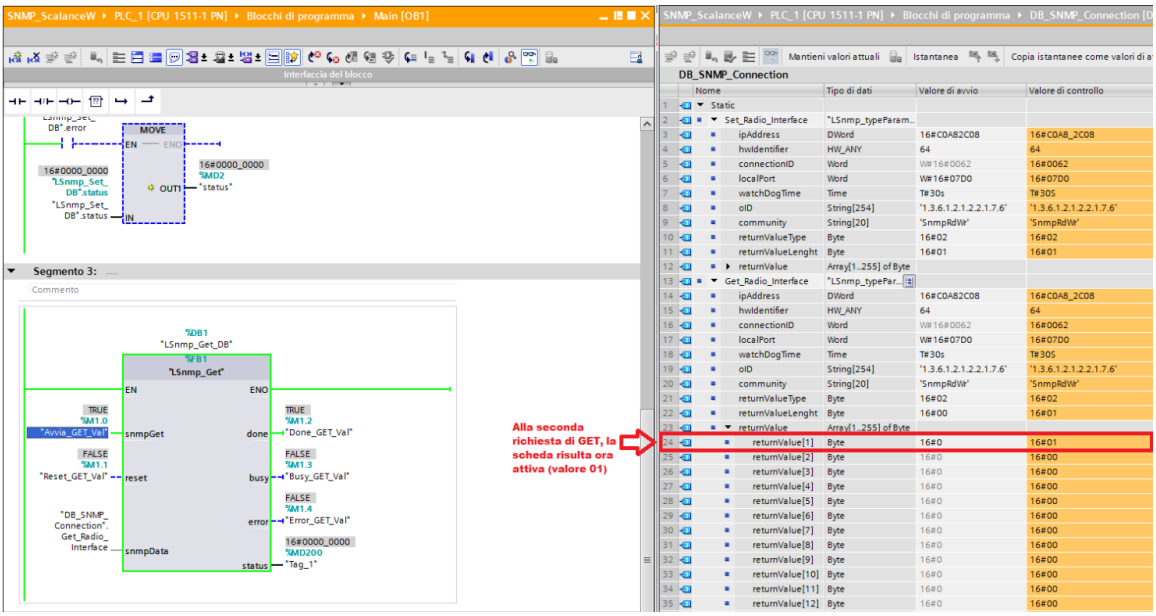


Valore 16#02.
La scheda WiFi è attualmente spenta.
Attiviamo la rete, attraverso la funzione SET.



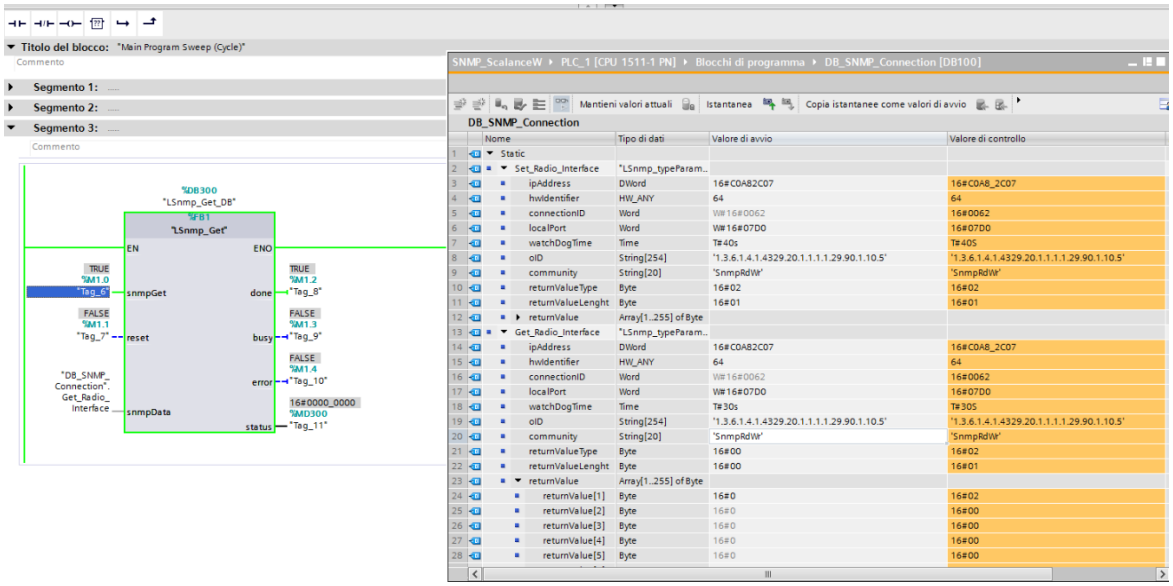
Il comando viene eseguito all'istante. Notate lo stato del bit di uscita 'DONE'.
Tuttavia, dovrete considerare i tempi di reboot del dispositivo.
Per questo motivo, l'attivazione della scheda avverrà in circa 15/20 secondi.

Per assicuraci, da remoto, che la scheda WiFi è in funzione, attiviamo una nuova richiesta GET e verifichiamo nuovamente il valore riportato nell'array 'return value'.

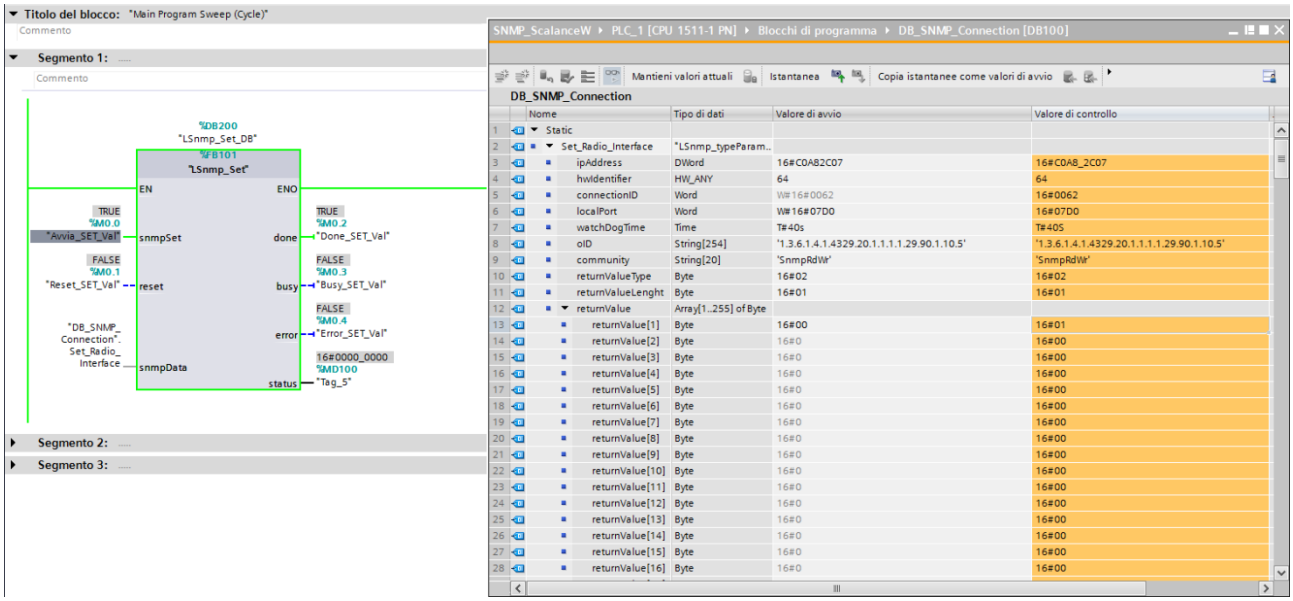


Valore 16#01.
Scheda WiFi attiva.

Per concludere la parte dedicata all'utilizzo dei blocchi, vediamo come eseguire la stessa funzione con uno Scalance X. Riportiamo il valore OID, già sperimentato attraverso il MIB Browser.
Non aggiungerò ulteriori commenti all'esecuzione di questa prova. Effettuo prima un 'GET' per conoscere lo stato della porta (la numero 5).



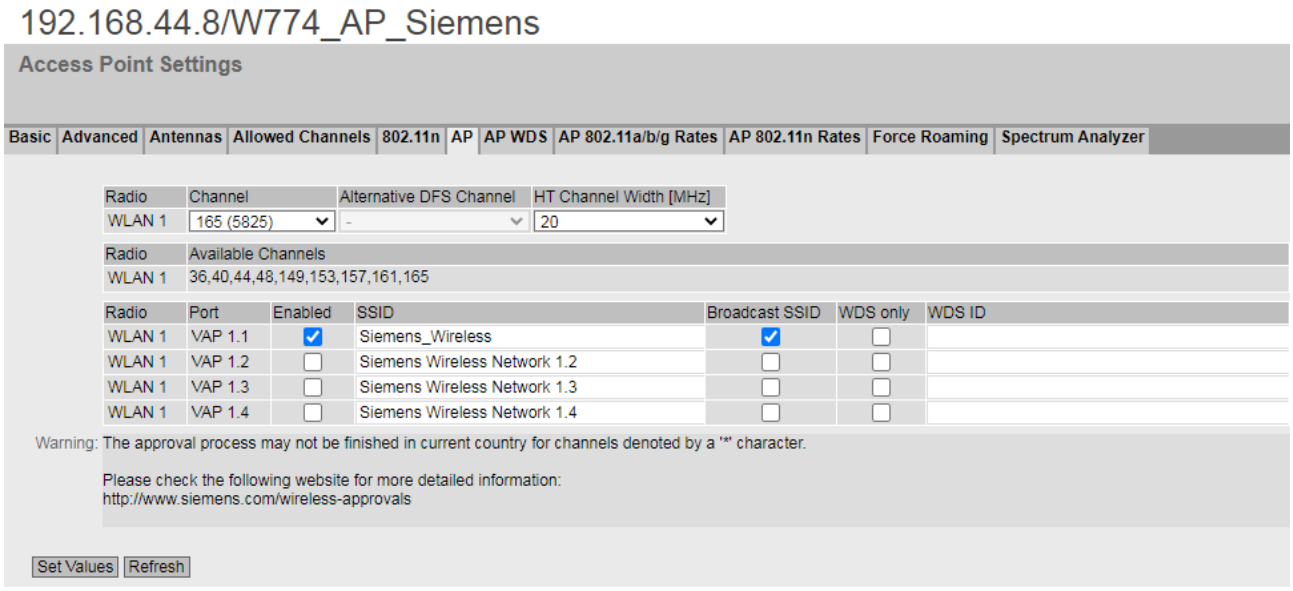
Concludo con un comado di 'SET' per riattivare la porta.



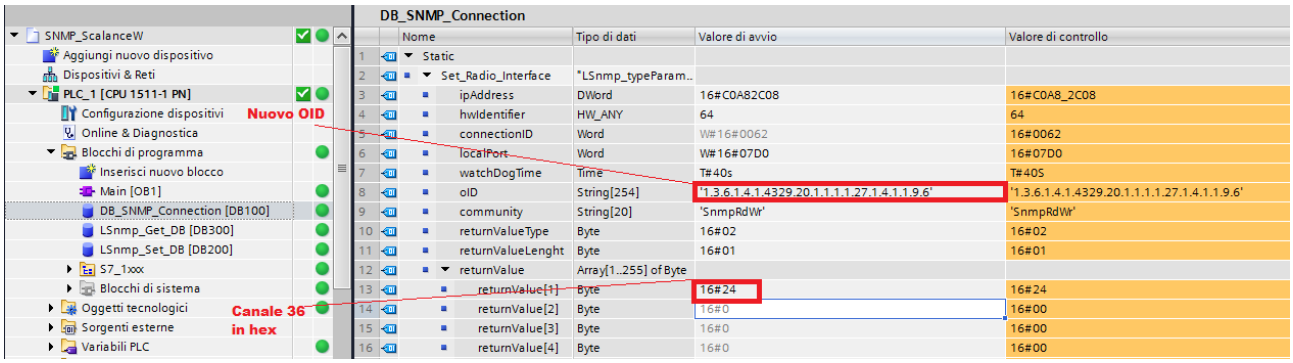
Esempio. Come cambiare il canale Tx dell'access point via SNMP.

Vedremo come cambiare il canale di trasmissione di un access point.

Verifichiamo, prima di tutto, il canale attualmente impiegato dall'access point.
In questo caso il canale 165.

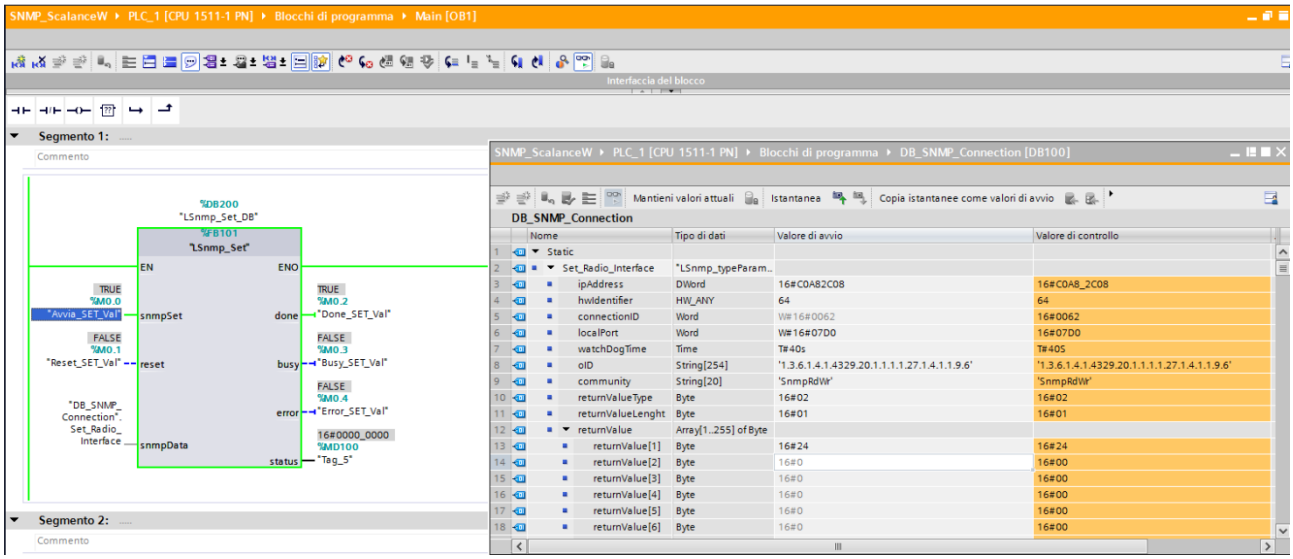


L'identificativo OID per gestire il cambio di canale è il seguente:
1.3.6.1.4.1.4329.20.1.1.1.27.1.4.1.1.9.6

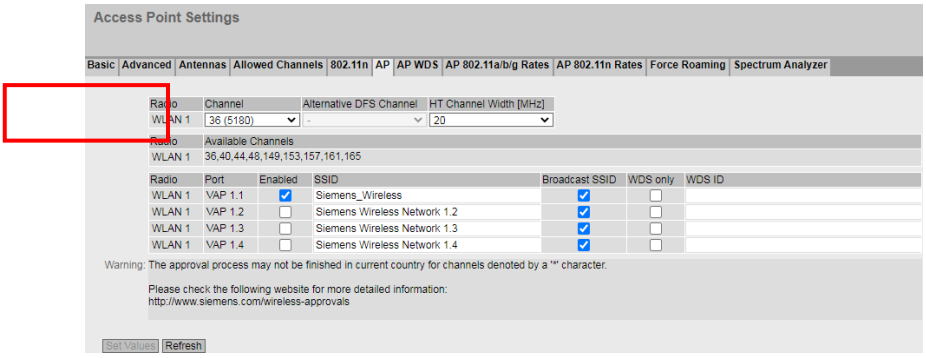


Vi ricordo che al termine del codice OID dovete inserire l'identificativo della scheda WiFi.
Nell'array 'return value' dovete inserire, nel primo byte, il valore in hex del canale che volete cambiare.
Esempio: voglio attivare il canale 36, in hex 24.

Eseguo il blocco 'LSnmp_SET'



A 'DONE' attivo, ritornate alla pagina web del dispositivo ed aggiornatela (F5).
Noterete che il nuovo canale di trasmissione dell'access point è, come richiesto, il 36.



Congratulazioni avete eseguito il vostro primo comando via SNMP.

Avete terminato.

Con riserva di modifiche e salvo errori.
Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.
Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.