Oggetto: Tutorial sulla configurazione di base dello switch Catalyst 2900XL

By: Gianrico Fichera, ITESYS srl, http://www.itesys.it

Redatto da: Gianrico Fichera

Configurazione di base degli switch Cisco

In questo documento trattero' della configurazione di base degli switch Cisco IOS-based. Il modello preso in esame e' un Catalyst 2900XL ma i concetti introdotti possono essere applicati con successo a molti altri switch Cisco della stessa fascia. Il sistema operativo presente e' un IOS 12.0(5)2XU.

Start-up

Ecco la sequenza di boot e la configurazione di fabbrica del prodotto preso in esame:

```
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:c2900XL-c3h2s-mz-120.5.2-
XU.bin"...###################################################################
file "flash:c2900XL-c3h2s-mz-120.5.2-XU.bin" uncompressed and installed, entry point:
0x3000
executing...
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU, MAINTENANCE
INTERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 17-Jul-00 17:35 by ayounes
Image text-base: 0x00003000, data-base: 0x00301F3C

Initializing C2900XL flash...
...done Initializing C2900XL flash.
cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes
of memory.
Processor board ID FOC0520Y0KB, with hardware revision 0x01
Last reset from power-on
Processor is running Enterprise Edition Software
Motherboard revision number: C0
Model number: WS-C2924-XL-EN
System serial number: FOC0520Y0KB
C2900XL INIT: Complete
00:00:28: %SYS-5-RESTART: System restarted –
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU, MAINTENANCE
INTERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 17-Jul-00 17:35 by ayounes
— System Configuration Dialog —
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started.
```

```
Switch#sh run
Building configuration...
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!!
ip subnet-zero
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
... snip ...
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface VLAN1
no ip directed-broadcast
no ip route-cache
!
!
line con 0
transport input none
stopbits 1
line vty 5 15
!
end
```

Configurazione delle password

Nell'assegnazione delle password si utilizzano gli stessi comandi conosciuti per i router. Per l'accesso in modalita' privilegiata:

```
Switch(config)#enable secret cisco
```

Per l'accesso da telnet e' necessario l'impostazione della password sulle linee di terminale virtuale:

```
Switch(config)#line vty 0 4
              password cisco
              Login
```

Amministrazione remota

Notate la configurazione di default delle VLAN nello switch:

```
mioswitch#sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12,
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500      -      -        -    -        -   1002   1003
1002 fddi  101002     1500      -      -        -    -        -      1   1003
1003 tr    101003     1500   1005      0        -    -      srb      1   1002
1004 fdnet 101004     1500      -      -        1  ibm        -      0      0
1005 trnet 101005     1500      -      -        1  ibm        -      0      0
```

Tutte le porte sono nella VLAN1. Il 2900XL e' uno switch layer2 pertanto non e' in grado di fare routing. La configurazione layer 3 si limita all'assegnazione di un indirizzo ip e di un gateway che ne consentono l'amministrazione da remoto, tramite telnet, http o

CiscoWorks. L'amministrazione e' possibile dagli apparati presenti nella VLAN1, la vlan di default, che per questo si chiama anche 'vlan di management'. In questo esempio assegnamo allo switch l'IP 192.168.30.6/24 e gateway 192.168.30.1:

```
mioswitch(config)#int vlan1
mioswitch(config-if)#ip address 192.168.30.6   255.255.255.0
mioswitch(config)#ip default-gateway   192.168.30.1
```

E' possibile cambiare la VLAN di management ove necessario. Creiamo una nuova VLAN, la due, configuriamo l'indirizzo ip e il gioco e' fatto. E' possibile una sola VLAN di management.

```
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN2
 ip address 192.168.30.6 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
```

Adesso lo switch e' amministrabile da tutte le postazioni nella VLAN1 e anche al di fuori della LAN, se il gateway e' nella VLAN1. Il Catalyst 2900 e' dotato di server web ed e' configurabile nelle sue funzionalita' di base tramite browser quale Netscape Communicator o Internet Explorer. Per quest'ultima opzione e' necessario attivare il server web come segue:

```
mioswitch(config)#ip http server
```

L'accesso web e' protetto da nome utente e password. Lasciare il campo username in bianco se nella configurazione non sono stati definiti degli utenti. Utilizzare la password di enable. L'accesso web andrebbe protetto definendo gli indirizzi ip delle postazioni di management ed impedendone la gestione a tutti gli altri. A tale scopo si puo' utilizzare un'access-list tramite il comando "ip http access-class":

```
mioswitch(config)#ip http access-class ?
  <1-99>  Access list number
```

I file html del server web sono nella flash dello switch:

```
mioswitch#dir
Directory of flash:/

  2  -rwx     1645810   Jul 18 2000 01:26:29  c2900XL-c3h2s-mz-120.5.2-XU.bin
  3  -rwx      105970   Jul 18 2000 01:26:29  c2900XL-diag-mz-120.5.2-XU
  4  drwx        6784   Jul 18 2000 01:26:30  html
111  -rwx        1296   Mar 01 1993 00:48:59  config.text
112  -rwx         272   Jan 01 1970 00:00:26  env_vars

3612672 bytes total (834560 bytes free)
mioswitch#dir html
Directory of flash:/html/

  5  drwx           0   Jul 18 2000 01:26:29  Snmp
  6  -rwx         656   Jul 18 2000 01:26:29  ClusterBuilder.html.gz
  7  -rwx         613   Jul 18 2000 01:26:29  ClusterManager.html.gz
  8  -rwx        1413   Jul 18 2000 01:26:29  Graph.html.gz
  9  -rwx         211   Jul 18 2000 01:26:29  back.html.gz
 10  -rwx         253   Jul 18 2000 01:26:29  basiccfg.html.gz
 11  -rwx         636   Jul 18 2000 01:26:29  switchmgr.html.gz
 12  -rwx         185   Jul 18 2000 01:26:29  blank.html.gz
 13  -rwx         989   Jul 18 2000 01:26:29  cluster.html.gz
 14  -rwx         250   Jul 18 2000 01:26:29  menu.html.gz
 15  -rwx         347   Jul 18 2000 01:26:29  port.html.gz
 16  -rwx         331   Jul 18 2000 01:26:29  cv.html.gz
 17  -rwx         860   Jul 18 2000 01:26:29  popup.html.gz
 18  -rwx         343   Jul 18 2000 01:26:29  Detective.html.gz
 19  -rwx         787   Jul 18 2000 01:26:29  DrawGraph.html.gz
 20  -rwx         803   Jul 18 2000 01:26:29  GraphFrame.html.gz
... snip ...
```

Per l'amministrazione remota tramite snmp si utilizza il comando "snmp-server". Questo e' utile quando si utilizzano applicazioni per l'amministrazione o il monitoraggio da remoto come mrtg o CiscoWorks. Notate le password di sola lettura (RO) e di lettura/scrittura (RW) rispettivamente 'cisco' e cisco2':

```
snmp-server community cisco RO
snmp-server community cisco2 RW
snmp-server community pluto view v1default RO
snmp-server location catania
snmp-server contact gianrico
snmp-server host 192.168.30.45 trap pluto  tty config
```

Parametri di base: duplex e speed

Ad ogni porta e' associata una interfaccia di tipo FastEthernet. Lo stato di tale interfaccia si mostra col comando: 'show interface fasteth0/N' dove N e' il numero di porta dello switch:

```
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0006.2874.4041 (bia 0006.2874.4041)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Auto-duplex (Full), Auto Speed (100), 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 5000 bits/sec, 10 packets/sec
  5 minute output rate 98000 bits/sec, 17 packets/sec
     4674 packets input, 383089 bytes
     Received 229 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 8 multicast
     0 input packets with dribble condition detected
     7451 packets output, 5149573 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Configuriamo velocita' e duplex per la porta 1. Di default le porte hanno abilitata l'autonegoziazione ovvero il riconoscimento automatico della velocita' della Ethernet e del duplex.
Ecco come si forza rispettivamente il duplex e la velocita':

```
mioswitch(config)#int fast0/1
mioswitch(config-if)#description --- router gateway internet ---
mioswitch(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation

mioswitch(config-if)#duplex auto
mioswitch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration

mioswitch(config-if)#speed auto
```

Assegnazione delle VLAN alle porte

L'assegnazione di una porta in una VLAN si effettua col comando 'switchport'. La VLAN viene creata automaticamente con l'assegnazione della stessa ad una porta. Nell'esempio a seguire associamo la VLAN numero due alle porte 1 e 2 dello switch:

```
interface FastEthernet0/1
 description --- router gateway internet ---
 switchport access vlan 2
!
interface FastEthernet0/2
 switchport access vlan 2
```

In questo secondo esempio creiamo una terza VLAN, la numero 10. Ecco il risultato:

```
mioswitch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
mioswitch(config)#int fast0/15
mioswitch(config-if)#switch access vlan 10
mioswitch#sh vlan brief
VLAN Name                             Status    Ports
---- -------------------              ----------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                                Fa0/7, Fa0/8, Fa0/10, Fa0/11,
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/16,
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    VLAN0002                                 active    Fa0/1, Fa0/2, Fa0/9
10   VLAN0010                                 active    Fa0/15
1002 fddi-default                             active
1003 token-ring-default                       active
1004 fddinet-default                          active
1005 trnet-default                            active
```

Spanning-Tree

Lo spanning-tree e' abilitato di default. Nelle LAN senza la presenza di loop puo' anche essere disabilitato. Nelle LAN con loop e' indispensabile. In ogni caso conviene disabilitarlo sulle porte non collegate ad altri switch in quanto queste non possono generare loop. In quest'ultimo caso la porta iniziera' il forwarding dei pacchetti da subito invece di necessitare di circa 30 secondi dovuti alla presenza di STP. Se l'argomento non e' chiaro consiglio la lettura del tutorial sullo Spanning-Tree.

Per disabilitare STP si utilizza il comando '`spanning-tree portfast`'.
Nell'esempio a seguire utilizziamo il comando "debug spantree event" per analizzare il portfast:

```
Ecco cosa succede col portfast disattivo sulla fastethernet 0/20:

mioswitch#debug spantree event
Spanning Tree event debugging is on
mioswitch#debug spantree tree
Spanning Tree BPDU debugging is on
mioswitch#
01:28:08: ST: FastEthernet0/20 vlan 1 -> listening
01:28:08: %LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to up
01:28:08: The port state changed due to the interface up/down on interface
FastE
thernet0/20
01:28:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20,
chan
ged state to up
01:28:23: port = 0, old = 0, new = 0
01:28:23: ST: FastEthernet0/20 vlan 1 -> learning
01:28:38: port = 0, old = 0, new = 0
01:28:38: ST: FastEthernet0/20 vlan 1 -> forwarding
Ecco cosa succede col portfast attivo sulla fastethernet 0/2:
01:29:45: ST: FastEthernet0/2 vlan 2 ->jump to forwarding from blocking
01:29:45: port = 0, old = 0, new = 0
01:29:45: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
01:29:45: The port state changed due to the interface up/down on interface
FastE
thernet0/2
01:29:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
chang
ed state to up
interface FastEthernet0/1
 description --- router gateway internet ---
 switchport access vlan 2
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 2
 spanning-tree portfast
```

Se lo switch e' l'unico della rete o se gli switch hanno una topologia priva di loop e' possibile disabilitare lo STP per tutte le porte. Poiche' il tipo di STP e' PVST (ovvero vi e' una istanza per VLAN) ecco l'esempio per disattivarlo nella VLAN numero 10:

```
!
no spanning-tree vlan 10
ip subnet-zero
!
```

Fare molta attenzione quando si disabilita lo Spanning-Tree. Accertarsi che la topologia lo consenta.

Sicurezza

La sicurezza sulle porte consente la protezione della rete da intrusioni provenienti dalla LAN stessa piu' che dall'esterno. Le intrusioni provenienti dall'esterno di una LAN si gestiscono tramite firewall.

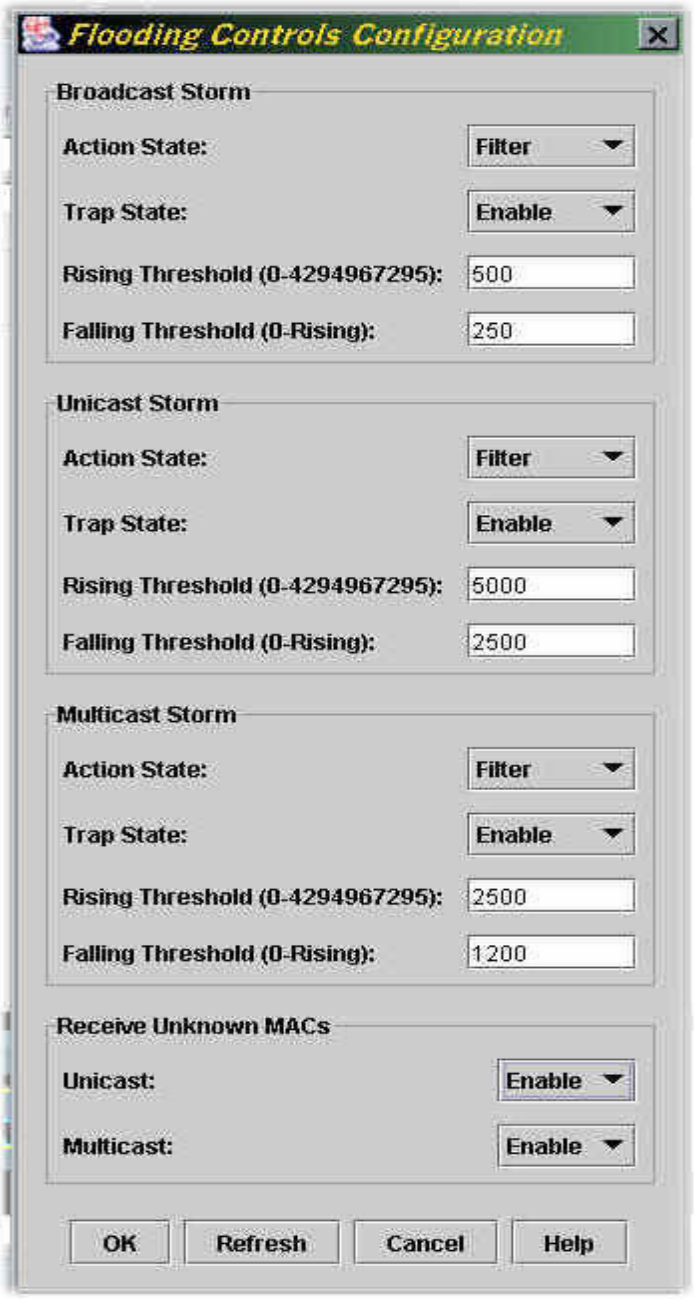
Supponiamo per esempio di gestire la LAN dell'Universita' di Scienze dell'Informazione di Pennyville. Senza che nessuno ci avverta vi sono continui inserimenti di HUB nella LAN e la reale topologia della rete sfugge ormai al nostro controllo. Questo e' da evitare. Per correre ai ripari forziamo lo switch a mappare un solo MAC su ogni porta che dev'essere collegata ad un PC. Se si viola la regola la porta si disattiva automaticamente:

```
mioswitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
mioswitch(config)#int fast0/20
mioswitch(config-if)#port security action ?
  shutdown  shut down the port from which security violation is de-
tected
  trap      send snmp trap for security violaiton

mioswitch(config-if)#port security ?
  action         action to take for security violation
  max-mac-count  maximum mac address count
  <cr>

Current configuration:
!
interface FastEthernet0/20
 port security max-mac-count 1
 port security action shutdown
end
```

Come passo successivo proteggiamo lo switch dal flooding di traffico dovuto, ad esempio, da un attacco DDoS, o da un componente di rete malfunzionante. Nel caso in cui i pacchetti per secondo superano una soglia viene inviata una segnalazione tramite trap snmp. La segnalazione avviene sia nel caso di traffico unicast che multicast o broadcast. Ecco un esempio di configurazione realizzata tramite la comoda interfaccia web in dotazione:

```
interface FastEthernet0/13
 port storm-control filter
 port storm-control trap
 port storm-control broadcast action filter
 port storm-control broadcast trap
 port storm-control multicast action filter
 port storm-control multicast trap
 port storm-control unicast action filter
 port storm-control unicast trap
```

Nell'immagine che segue si possono interpretare i valori (qui sono quelli di default) relativi a questo esempio. I valori sono espressi in termini di pacchetti per secondo (vai a pagina successiva).


Flooding Controls Configuration
Broadcast Storm
Action State:
Filter
Trap State:
Enable
Rising Threshold (0-4294967295):
500
Falling Threshold (0-Rising):
250
Unicast Storm
Action State:
Filter
Trap State:
Enable
Rising Threshold (0-4294967295):
5000
Falling Threshold (0-Rising):
2500
Multicast Storm
Action State:
Filter
Trap State:
Enable
Rising Threshold (0-4294967295):
2500
Falling Threshold (0-Rising):
1200
Receive Unknown MACs
Unicast:
Enable
Multicast:
Enable
OK
Refresh
Cancel
Help

Risoluzione dei problemi e SPAN

Se la rete non si comporta come dovrebbe e vogliamo monitorare esattamente tutti i frame in transito in una porta possiamo utilizzare lo "span". Si tratta di duplicare il traffico di una porta su una seconda, libera, cioe' non collegata fisicamente cosi' da porter agganciare il nostro strumento di monitoring, normalmente uno sniffer.
Le due porte devono essere nella stessa VLAN. Ecco come duplicare il traffico della Fast0/4 sulla 0/3.

```
interface FastEthernet0/3
 port monitor FastEthernet0/4
!
```

Per chi usa i telefoni IP

Anche se non e' un argomento di base ecco, per chi utilizza nella propria rete i telefoni IP, come gestire la seconda VLAN, riservata al traffico voce, su una stessa porta.

```
IPphone collegato alla fasteth0/18 con VLAN 10. Traffico
dati nella stessa interfaccia nella VLAN di
default:
interface FastEthernet0/18
 switchport priority default 0
 switchport voice vlan 10        <---- traffico voce va qui
!
mioswitch(config-if)#switchport priority default ?
  <0-7>  Priority for untagged frames (7 is highest)
```

```
In questo secondo tipo di configurazione, tutto il traffico
va nella vlan nativa:
mioswitch(config-if)#switchport voice vlan ?
  <1-4094>  Vlan for voice traffic
  dot1p     Priority tagged on PVID
  none      Don't tell telephone about voice vlan
  untagged  Untagged on PVID

mioswitch(config-if)#switchport voice vlan dot1p
```

Etherchannel

Per Etherchannel si intende la possibilita' di raggruppare piu' porte al fine di creare un unico flusso di dati di maggior capacita'. Un uso tipico e' per il collegamento tra switch. Raggruppare piu' porte a 100mbps, per esempio, puo' voler dire avere un canale dati di 200, 300 o piu' mbps, ideale per una dorsale collegante piu' switch. Se non si hanno a disposizione porte gigaethernet e gli switch sono tutti 10/100 e' una buona soluzione per LAN di piccole dimensioni. Naturalmente ai due capi dell'Etherchannel gli switch devono essere configurati allo stesso modo. Ecco nell'esempio come raggruppare tre porte, dalla 0/10 alla 0/12 e creare il gruppo 1, che rappresenta l'Etherchannel:

```
interface FastEthernet0/10
 port group 1
!
interface FastEthernet0/11
 port group 1
!
interface FastEthernet0/12
 port group 1
!
```

Trunk

Per trunking si intende la possibilita' di far transitare piu' VLAN sullo stesso canale fisico. Cio' accade nelle reti con piu' VLAN con collegamenti inter-switch. Laddove vi sono piu' switch e si usano le VLAN e' pressocche' indispensabile usare i trunk nei collegamenti inter-switch altrimenti si dovrebbe riservare una dorsale per ogni VLAN. Vi sono due protocolli che gestiscono l'incapsulamento delle VLAN sullo stesso canale fisico: ISL e 802.1q. Il primo e' proprietario Cisco, il secondo standard. Ecco la porta 0/22 configurata con trunk 802.1q:

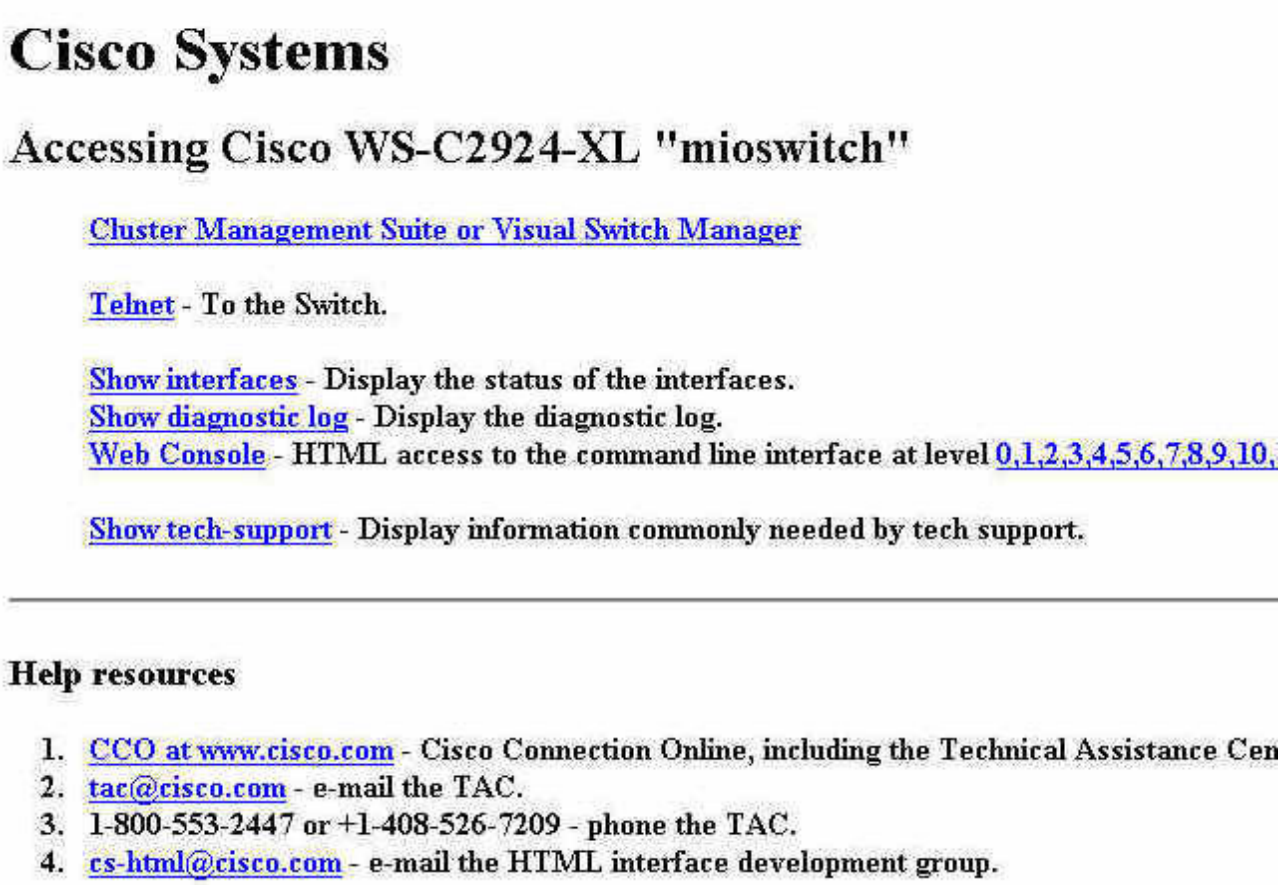
```
mioswitch#sh run int fast0/22
Building configuration...

Current configuration:
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

Configurazione da interfaccia WEB

Le funzionalita' di base dello switch possono essere configurate da web. Cio' e' molto utile per creare una configurazione iniziale con rapidita' e lasciare solo ad un uso successivo l'interfaccia caratteri. Abbiamo gia' spiegato come configurare lo switch per consentirne l'amministrazione da web. Lo switch in oggetto ha ip 192.168.30.6. Ecco una galleria d’immagini che possono aiutare ad accedere da web allo switch:

Galleria d'immagini:

Immagine 1: http://192.168.30.6



Cisco Systems

Accessing Cisco WS-C2924-XL "mioswitch"

Cluster Management Suite or Visual Switch Manager

Telnet - To the Switch.

Show interfaces - Display the status of the interfaces.
Show diagnostic log - Display the diagnostic log.
Web Console - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,

Show tech-support - Display information commonly needed by tech support.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Cen
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Immagine 2: Accesso alla Web Console (e' in Java)

Immagine 3: Se non avete la Java Virtual Machine scaricatela dal sito Sun

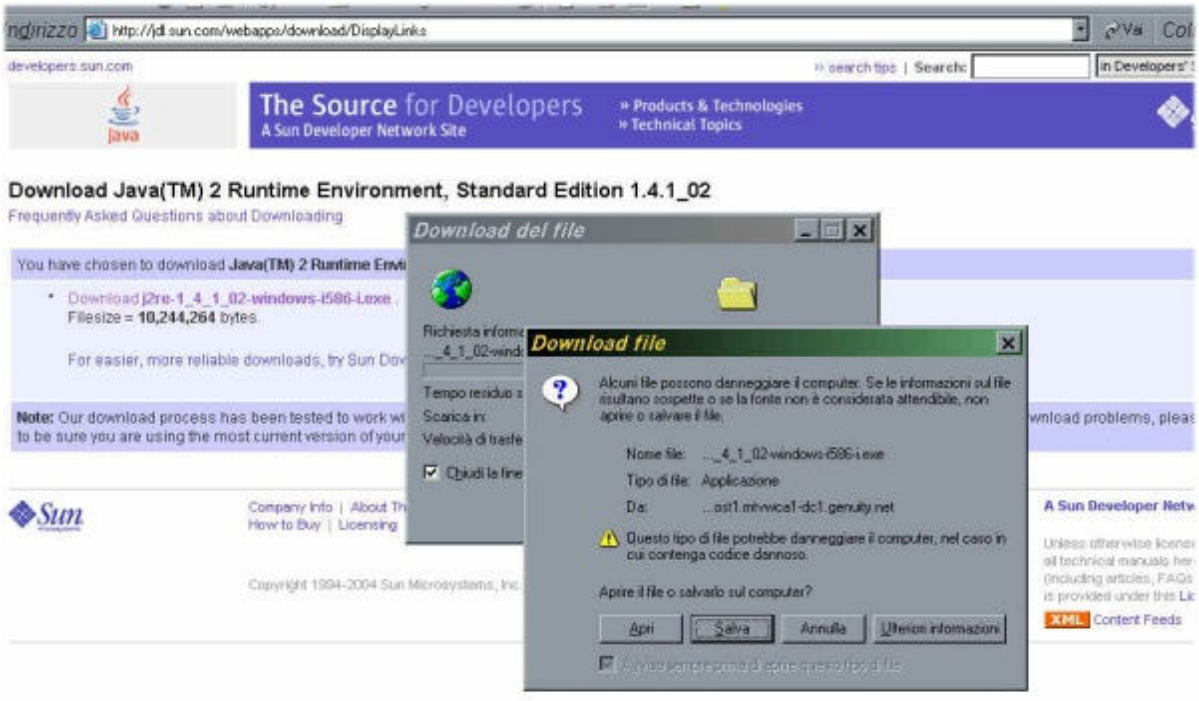


Immagine 4: Richiesta di username e password (leggi l'articolo)

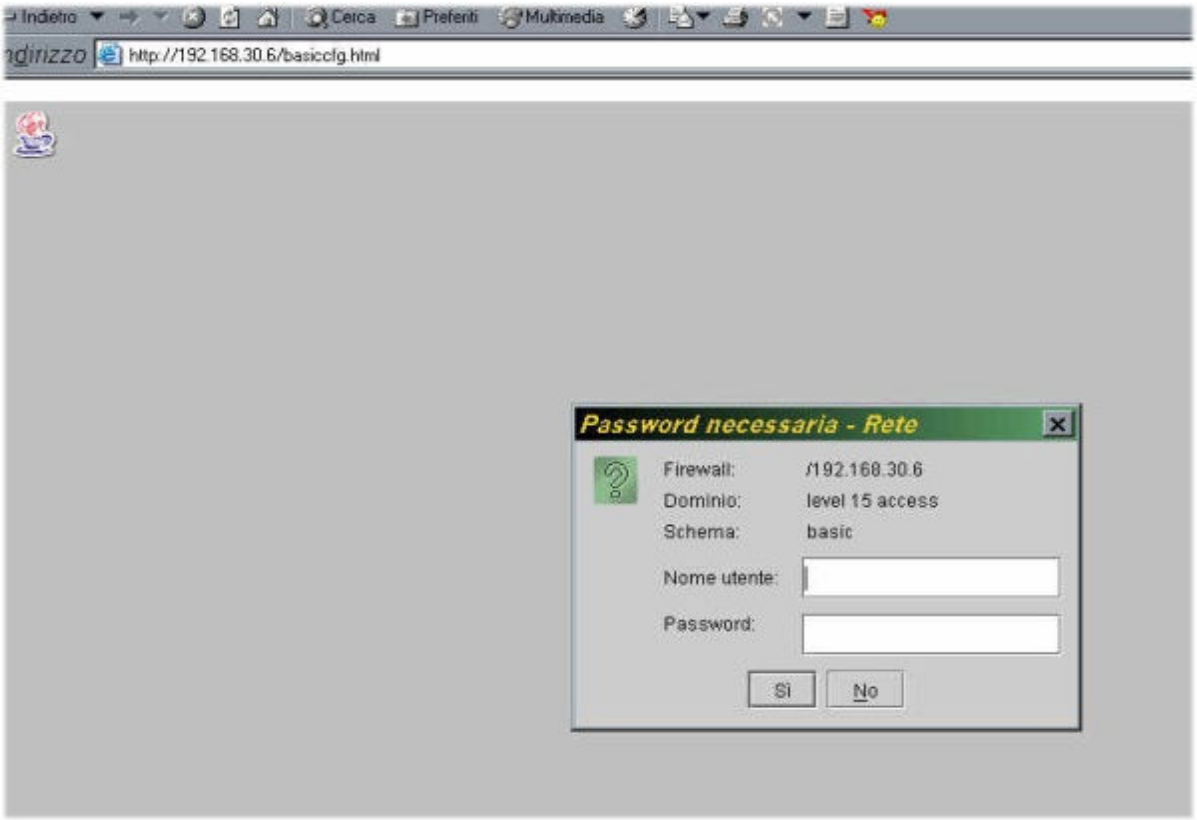


Immagine 5: schermata iniziale successiva all'accesso

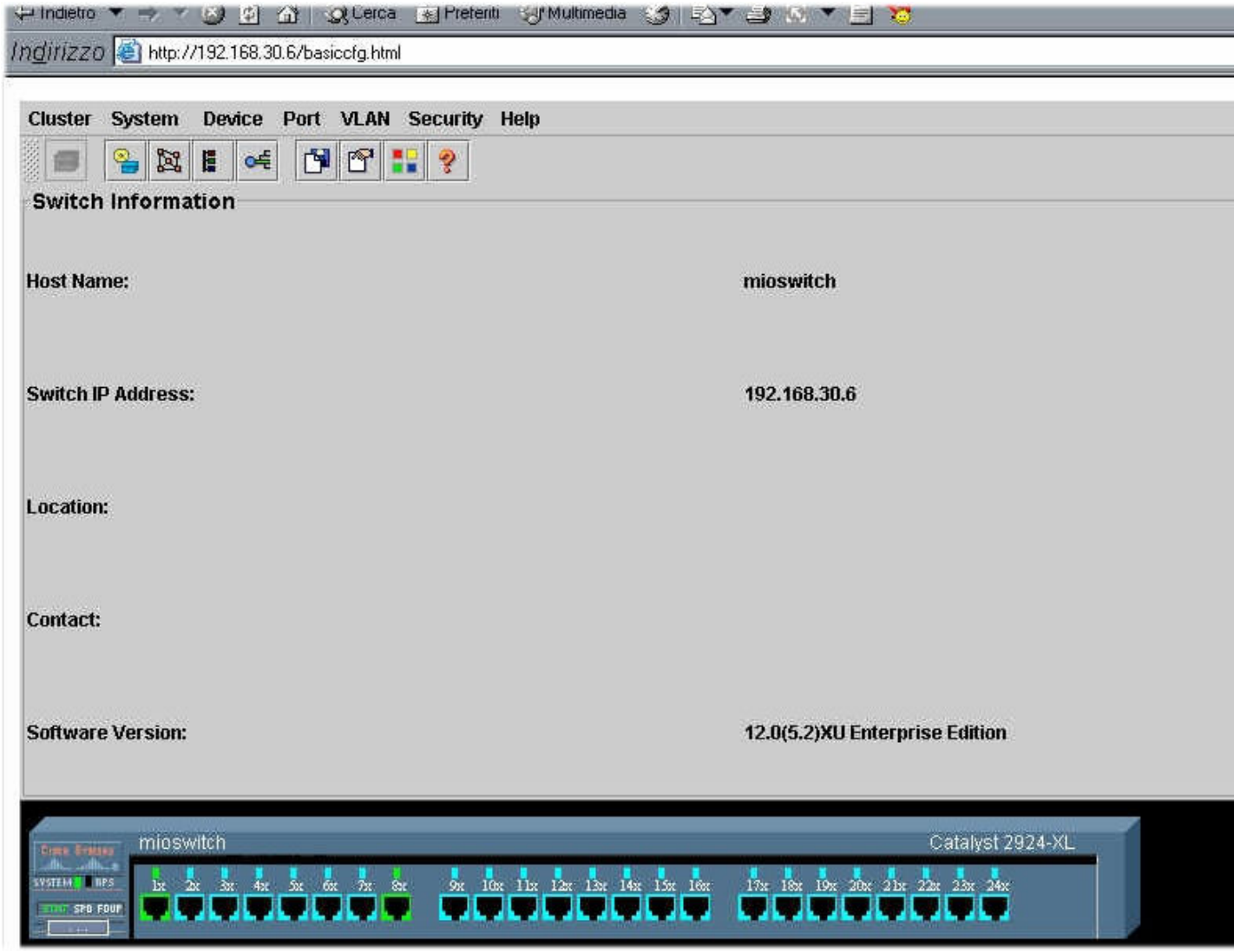


Immagine 6: Cliccando col mouse sulle porte queste si possono configurare

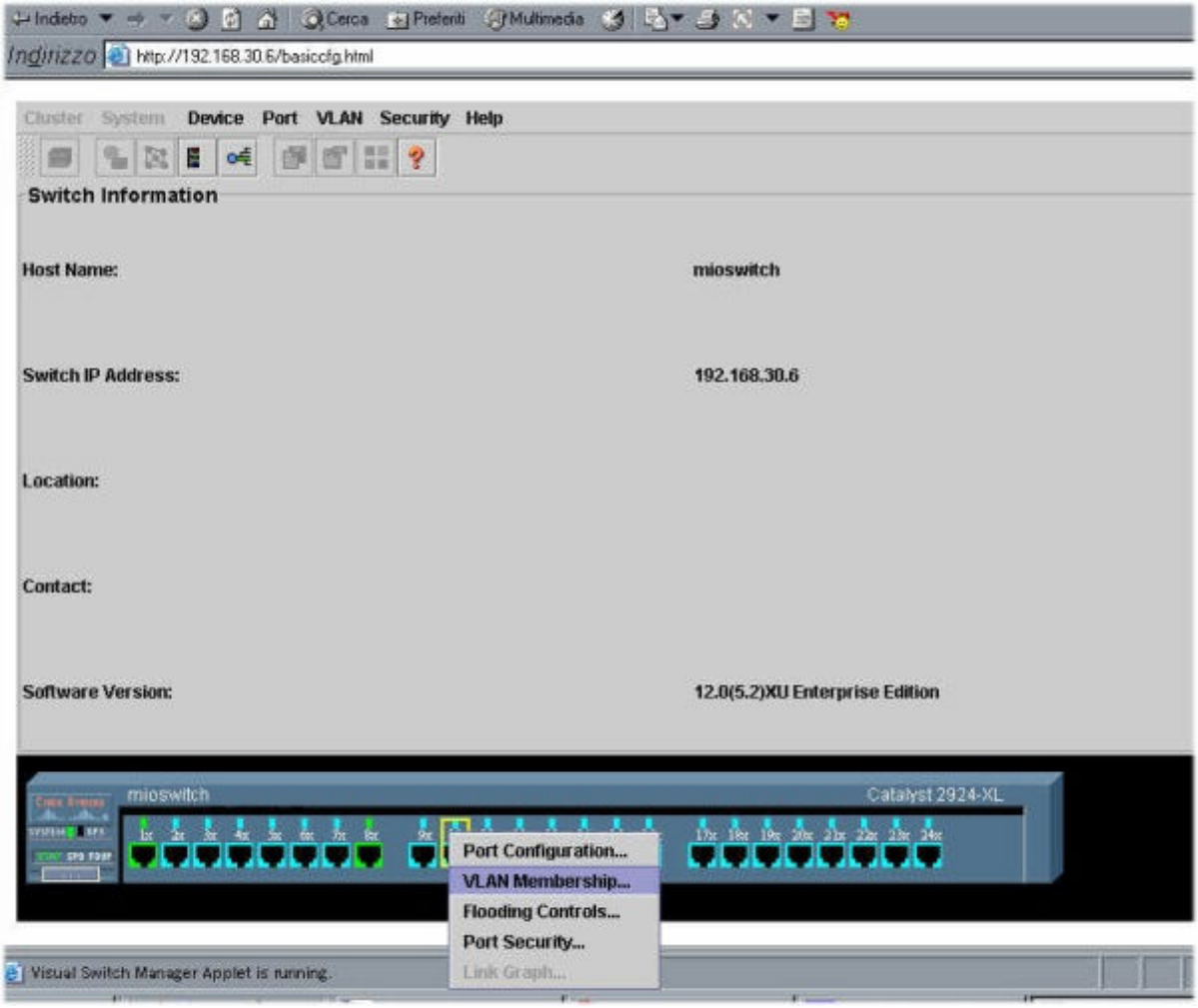


Immagine 7: Assegnazione di una VLAN ad una porta

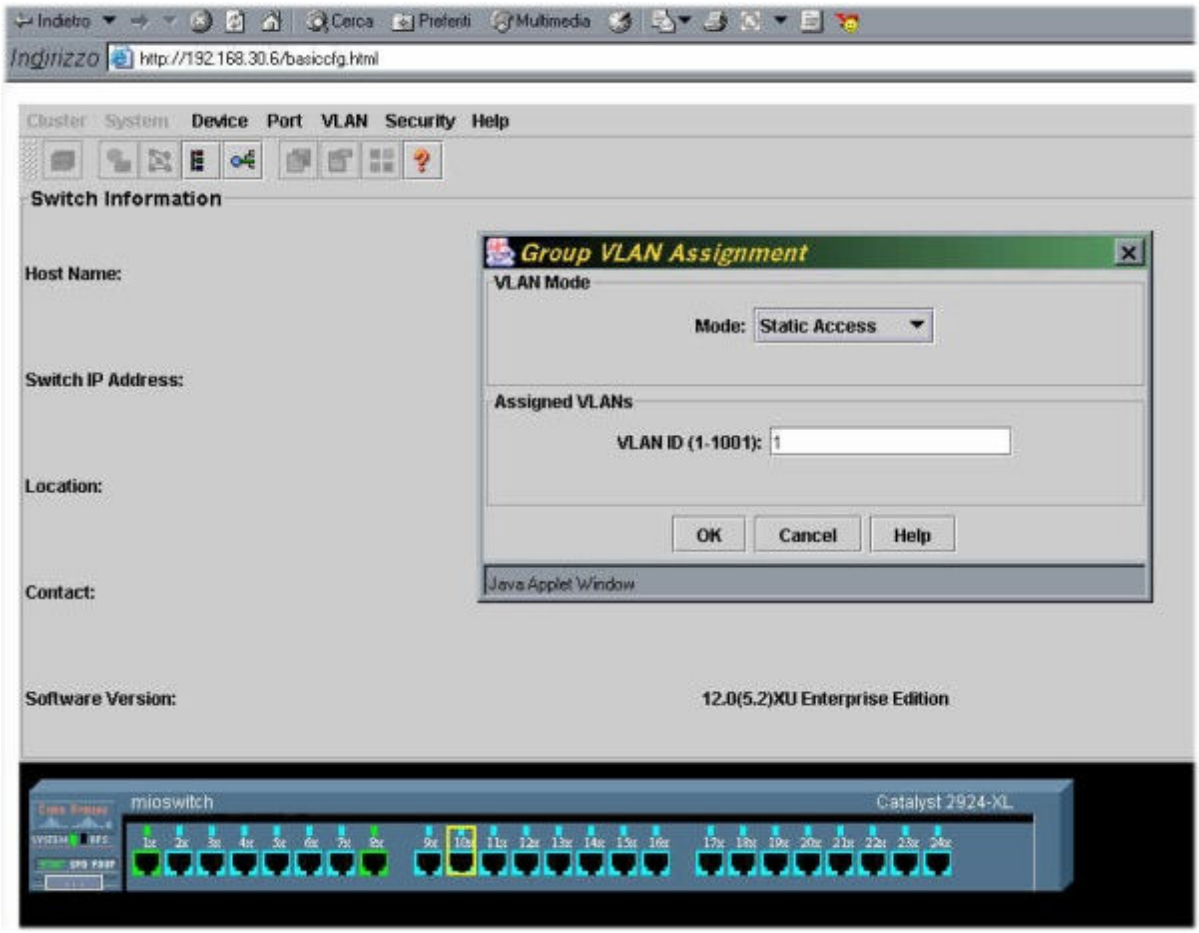


Immagine 8: Modifica della VLAN di Management