

Wireless Network

Esercitazioni

Alessandro Villani
avillani@science.unitn.it

Installazione di un Access Point CISCO 350

Access Point: Cisco 350

- ▣ Access Point Cisco Serie 350
- ▣ Configurabili via seriale:
 - Cavo null-modem
 - Baud Rate: 9600
 - Parity: none
 - Data bit: 8
 - Stop bit: 1
 - Flow Control: none
 - Default passwd: vuota
 - Line feed con Carriage Returns

Access Point: Boot

```
Testing DRAM...
DRAM OK
DRAM OK
Power-on reset.
Copyright 1996-2000 Cisco Systems, Inc.
Copyright 1984-2000 Wind River Systems, Inc.
System ID: 00409651F303
Motherboard: MPC855 50MHz, 8192KB FLASH, 16384KB DRAM, Revision B0
Bootstrap Ver. 1.09: FLASH, CRC 710B6415 (OK)
Initialization: OK
Memory Bank      total      used      left
DRAM             16738168      0 16738168
Config           524288       116  524172
FLASH           7733248    1440032  6293216
Memory Bank:File      address      size  encoding type  flags
a) Config:AP Installation Key  FE020000      64  none  Key  0000
b) Config:VAR Installation Key FE020040      52  none  Key  0000
c) FLASH :EnterpriseAP Sys 12.00 FE0A0000    1142188 gzip  Exec  0801
d) FLASH :EnterpriseAP Web 12.00 FE1B6DAC    137972  .tar.gz Web  0000
e) FLASH :Inflate Ver. c10 FE1D69A0     7556  gzip  Ddrdr  0800
f) FLASH :AMC FMC21A FPGA 0.14 FE1DA624     37380  none  FPGA  0000
g) FLASH :340 Series FWare 05.02B FE1E3828     57412  .tar.gz Data  0000
h) FLASH :PC4800 Firmware 05.02B FE1F186C     57408  .tar.gz Data  0000
i) FLASH :AP Installation Key FE1FF8AC      64  none  Key  0000
j) FLASH :VAR Installation Key FE1FF8EC      52  none  Key  0000
Inflating "EnterpriseAP Sys 12.00"...
312748 bytes OK
Loaded driver for device "fec0", ifIndex=1.
Loaded driver for device "awc0", ifIndex=2.
Configured device "fec0" as IP address "10.0.0.1", network mask 0xfffffff0.
Attaching network interface lo0... done.
```

Access Point: Configurare via CLI

□ L'interfaccia testuale simula quella WEB

```
AP350-51f303      Express Setup      Uptime: 00:02:05
System [Name      ] [AP350-51f303      ]
[Terminal Type   ] [teletype         ]
MAC Address      : 00:40:96:51:f3:03
Config. Server [Protocol ] [DHCP             ]
IP [Address       ] [10.0.0.1         ]
IP [Subnet Mask   ] [255.255.255.0   ]
Default [Gateway  ] [255.255.255.255 ]
[Service Set ID (SSID) ] [tunamini        ]
[Role in Radio Network ] [Repeater Access Point ]
[Optimize Radio Network Por ] [Throughput] [Hw Radio]
[Ensure Compatibility With: ] [2Mb/sec Clients] [_]
[non-Aironet 802.11] [_]
[Security Setup]
[SNMP Admin. Community ] [                  ]
[Apply] [OK] [Cancel] [Restore Defaults]
[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
(Auto Apply On) :Top, :Up, *R, *(Auto Apply On) :Top, :Up, *R, -, <ENTER>, or [Link
Text]:
```

Access Point: Configurazione

- Gli AP Cisco hanno di default l'IP 10.0.0.1
- È quindi possibile raggiungerli anche via rete utilizzando un cross oppure uno switch/hub e mettendosi nella stessa sottorete
- Col software allegato c'è anche un tool per trovare gli AP installati

Access Point: Modifica IP Address

- Per assegnare un IP, utilizzando la CLI:

```
Pr n → Protocol none  
Ad 192.168.91.124 → Address 192.168.91.124  
G 192.168.91.1 → Gateway 192.168.91.1
```

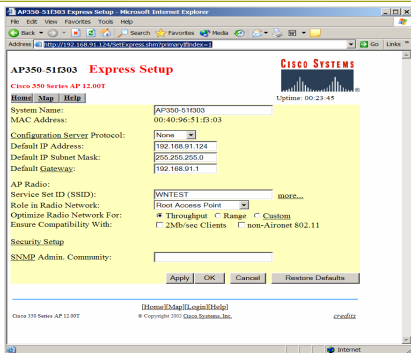
- Per assegnare l'SSID:

```
Ser → Service Set ID (SSID) WNTEST  
Ro Ro → Role in Radio Network Root Access Point
```

- Per salvare la configurazione:

```
Ap → Apply  
Ad 192.168.91.124 → Address 192.168.91.124  
G 192.168.91.1 → Gateway 192.168.91.1
```

Access Point: Interfaccia WEB

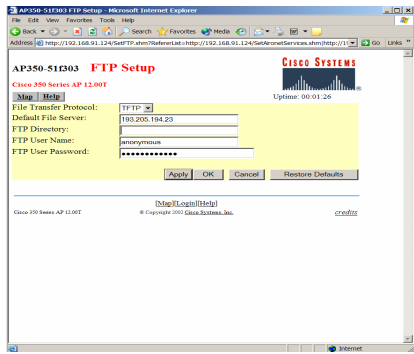


Access Point: Aggiornare il Firmware

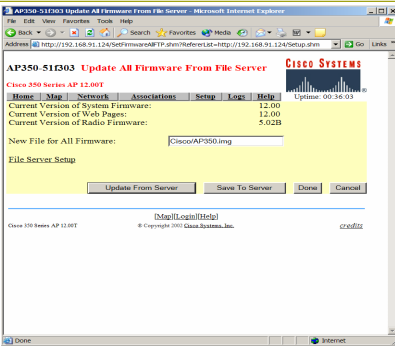
- Il firmware è disponibile all'indirizzo:
<http://www.cisco.com/public/sw-center/sw-wireless3.shtml>

Per aggiornare il firmware si utilizza un server tftp (Trivial File Transfer Protocol)

Access Point: Aggiornare il Firmware



Access Point: Aggiornare il Firmware



Access Point: Modifica IP Address

- Su questi AP si possono configurare:
 - Chiavi WEP da 40 e da 128 bit
 - La potenza trasmittiva (da 1mW a 50mW)
 - Quale antenna utilizzare in ricezione ed in trasmissione
 - Quali velocità sono richieste (basic), quali sono per unicast (yes), quali non utilizzate (no)
 - Fino a 16 SSID (utilizzando le VLAN)

Access Point: Modifica IP Address

- ▣ Altre configurazioni importanti:
 - Creare l'utente con diritti di amministrazione
 - Configurare un server con syslog o SNMP
 - Abilitare un server radius per il controllo dei MAC address
 - Abilitare un server 802.1x

Autenticazione del MAC
su radius

Analisi pacchetti: ethereal

- ▣ Dump pacchetti utilizzando ethereal
- ▣ Si possono analizzare tutti i pacchetti oppure una selezione opportuna

Autenticazione Radius

```
Frame 1 (107 bytes on wire, 107 bytes captured)
Arrival Time: May 6, 2004 12:50:30.924943000
Time delta from previous packet: 0.000000000 seconds
Time since reference or first frame: 0.000000000 seconds
Frame Number: 1
Packet Length: 107 bytes
Capture Length: 107 bytes
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.23 (172.31.194.23), Dst Addr:
radius.science.unin.it (192.168.194.168)
User Datagram Protocol, Src Port: 6001 (6001), Dst Port: radius (1812)
Source port: 6001 (6001)
Destination port: radius (1812)
Length: 73
Checksum: 0x644d (correct)
Radius Protocol
Code: Access Request (1)
Packet identifier: 0xbc (188)
Length: 65
Authenticator
Attribute value pairs
  t:User Name(1) 1:15, Value:"00028a-clf100"
  t:User Password(3) 1:38, Value:"XXXXXXXX\000\000\000\000\000\000\000"
  t:NAS IP Address(4) 1:6, Value:172.31.194.23
  t:NAS Port(5) 1:6, Value:0
```

Autorizzazione Radius

```
Frame 2 (62 bytes on wire, 62 bytes captured)
Arrival Time: May 6, 2004 12:50:30.938469000
Time delta from previous packet: 0.003526000 seconds
Time since reference or first frame: 0.003526000 seconds
Frame Number: 2
Packet Length: 62 bytes
Capture Length: 62 bytes
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: radius.science.unin.it (192.168.194.168), Dst Addr:
172.31.194.23 (172.31.194.23)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 6001 (6001)
Source port: radius (1812)
Destination port: 6001 (6001)
Length: 28
Checksum: 0x2b1a (correct)
Radius Protocol
Code: Access Accept (2)
Packet identifier: 0xbc (188)
Length: 20
Authenticator
```

Richiesta Accounting Radius

```
Frame 3 (132 bytes on wire, 132 bytes captured)
Arrival Time: May 6, 2004 12:50:30.931190000
Time delta from previous packet: 0.002721000 seconds
Time since reference or first frame: 0.006247000 seconds
Frame Number: 3
Packet Length: 132 bytes
Capture Length: 132 bytes
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.23 (172.31.194.23), Dst Addr:
radius.science.unin.it (192.168.194.168)
User Datagram Protocol, Src Port: 6002 (6002), Dst Port: radius-acct (1813)
Source port: 6002 (6002)
Destination port: radius-acct (1813)
Length: 98
Checksum: 0xbbd9 (correct)
Radius Protocol
Code: Accounting Request (4)
Packet identifier: 0xbd (189)
Length: 90
Authenticator
Attribute value pairs
  t:User Name(1) 1:15, Value:"00028a-clf100"
  t:Acct Session ID(44) 1:15, Value:"00028a-clf100"
  t:NAS identifier(32) 1:10, Value:"Amsys-13"
  t:NAS IP Address(4) 1:6, Value:172.31.194.23
  t:NAS Port(5) 1:6, Value:2
  t:NAS Port Type(61) 1:6, Value:Wireless IEEE 802.11(19)
  t:Acct Authentic(45) 1:6, Value:Radius(1)
  t:Acct Status Type(40) 1:6, Value:Start(1)
```

Ok Accounting Radius

```
Frame 4 (62 bytes on wire, 62 bytes captured)
  Arrival Time: May  6, 2004 12:50:30.938601000
  Time delta from previous packet: 0.004411000 seconds
  Time since reference or first frame: 0.010658000 seconds
  Frame Number: 4
  Packet Length: 62 bytes
  Capture Length: 62 bytes
  Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
  Internet Protocol, Src Addr: radius.science.unistn.it (192.168.194.168), Dst Addr:
  172.31.194.23 (172.31.194.23)
  User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: 6002 (6002)
  Source port: radius-acct (1813)
  Destination port: 6002 (6002)
  Length: 28
  Checksum: 0xdd76 (correct)
  Radius Protocol
  Code: Accounting Response (5)
  Packet identifier: 0xbd (189)
  Length: 20
  Authenticator
```
