Configurazione del multicast wireless sui WLC serie 5760 e 3850

Sommario

Introduzione

In questo documento viene descritto come configurare il multicast wireless sui Cisco serie 5760 e 3850 Wireless LAN Controller (WLC), che supportano sia il *multicast con unicast* che il *multicast con* meccanismi di consegna *multicast*.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dell'implementazione multicast sui Cisco serie 5760 e 3850 WLC.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5760 WLC
- Cisco serie 3850 WLC
- Cisco serie 3602 Access Point (AP).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Completare questa procedura per abilitare il multicast sulle piattaforme NWGC (Next-Generation Wiring Closet):

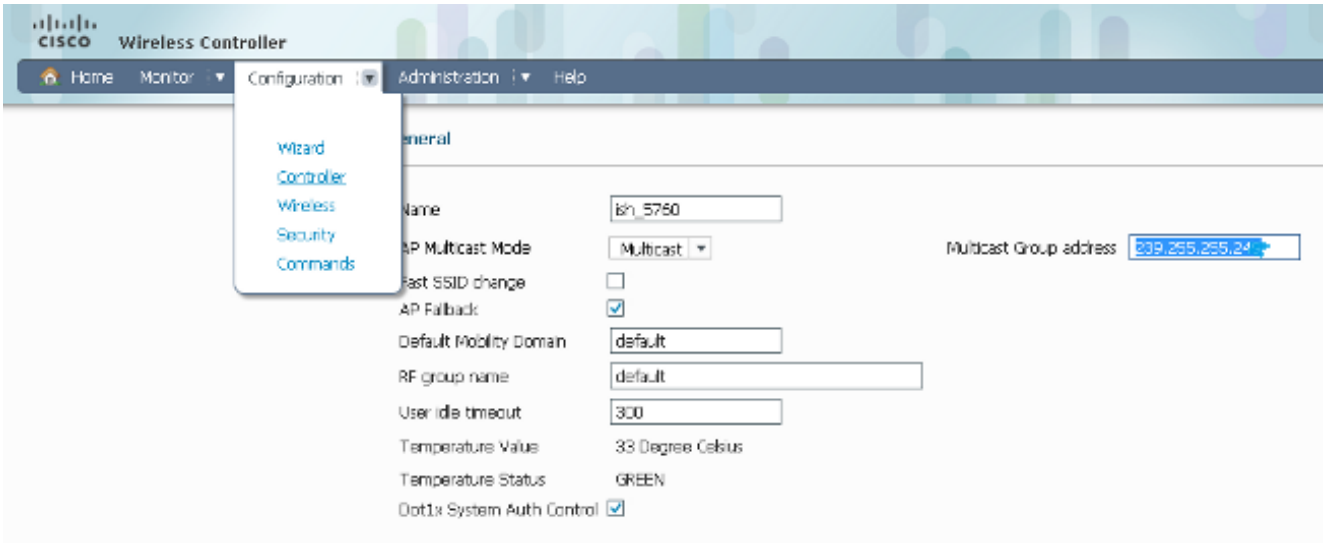
1. Immettere il comando **wireless multicast** per abilitare il multicast sul controller:

   ```
   ish_5760(config)#wireless multicast
   ```

   Nota: Per impostazione predefinita, questo comando abilita il *multicast con* meccanismo di recapito *unicast*.
2. Se è necessario modificare il meccanismo di recapito in *multicast con multicast*, immettere questo comando:

   ```
   ish_5760(config)#ap capwap multicast 239.255.255.250
   ```

   Nota: Questo comando configura il gruppo multicast a cui si uniscono tutti i punti di accesso wireless (CAPWAP) Control and Provisioning of Wireless Access Point (CAPWAP). Lo switch viene ottimizzato in modo da inviare un messaggio CAPWAP multicast che raggiunge tutti i punti di accesso. Questo processo è diverso quando si utilizza la modalità unicast, in quanto lo switch deve inviare messaggi unicast a tutti i CAPWAP. Ciò consente di ridurre al minimo il carico di sistema sul controller.Facoltativamente, è possibile selezionare **Configuration > Controller** dalla GUI per configurare queste informazioni, come mostrato di seguito:



3. Immettere questi comandi per abilitare lo snooping IGMP (Internet Group Management Protocol) sul controller (abilitato per impostazione predefinita):

   ```
   ip igmp snooping

   ip igmp snooping querier
   ```

   Nota: Il comando **ip igmp snooping querier** configura il controller in modo che controlli periodicamente se un client è ancora in ascolto del traffico multicast.

Multicast Flow su NGWC

Questi passaggi delineano il flusso del traffico multicast sui NGWC quando viene implementata la configurazione precedente:

1. Il controller intercetta i pacchetti IGMP inviati dai client wireless.

2. Se la voce client per quella combinazione multicast *gruppo-vlan-origine* esiste, il controller aggiorna i timer IGMP.

   Se si tratta di una nuova voce, il WLC crea un MGID (Multicast Group Identifier) basato sulla tupla (source, group, VLAN), con un intervallo compreso tra 1 e 4.095 per il layer 2 (L2) o tra 4.160 e 8.191 per il layer 3 (L3).

3. Il pacchetto IGMP viene inoltrato a monte.

4. La voce MGID viene inviata all'access point insieme alle informazioni sull'associazione del client in modo che il client possa ricevere il traffico multicast.

5. In base al meccanismo di recapito (multicast con unicast/multicast), il controller inoltra il traffico all'access point in modo appropriato. **Nota:** Se il meccanismo di recapito è multicast, la crittografia DTLS (Datagram Transport Layer Security) e il contrassegno QoS (Quality of Service) non vengono applicati.
6. L'access point inoltra quindi il traffico a ciascun client, a seconda delle esigenze.

Verifica

Per verificare che la configurazione funzioni correttamente, attenersi alla seguente procedura:

1. Immettere il comando **show wireless multicast** per verificare se il multicast è stato abilitato correttamente:

```
ish_5760#show wireless multicast

Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap Multicast group Address : 239.255.255.249
AP Capwap Multicast QoS Policy Name : unknown
AP Capwap Multicast QoS Policy State : None
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled

Vlan Non-ip-mcast Broadcast MGID
--------------------------------
1 Enabled Enabled Disabled
10 Enabled Enabled Enabled
24 Enabled Enabled Enabled
25 Enabled Enabled Enabled
26 Enabled Enabled Enabled
32 Enabled Enabled Enabled
```

2. Immettere il comando **show capwap sum** per verificare le informazioni CAPWAP:

```
ish_5760#show capwap sum

Name Src Src Dest Dst Dtls MTU Xact
IP Port IP Port En
---- ----------- ---- ------------ ----- ---- ----- ---
Ca1  172.16.15.1 5247 239.10.10.11 5247  No   1449  1
Ca19 172.16.15.1 5247 172.17.1.54  52451 Yes  1380  3
```

Nota: Come mostrato nell'output, l'interfaccia **Ca1** viene usata per la modalità multicast AP. L'interfaccia Ca1 ha un valore DTLS di No, mentre l'interfaccia **Ca19** ha un valore *DTLS* di **Sì**.

3. Immettere i **dettagli show capwap** o **show capwap summary** per verificare il numero di access point che sono stati aggiunti al gruppo multicast:

```
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 2
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 1


Name APName Type PhyPortIf Mode McastIf
------ --------------------------------
Ca2 ish_3502_lw_2 data  -  multicast Ca0
Ca1 ish_ap       data  - multicast Ca0
Ca0 -     mcas - unicast     -


Name SrcIP               SrcPort     DestIP DstPort DtlsEn MTU
--- ---------------     -------     ------  ------- ------ ---
Ca2 10.105.132.138 5247 10.106.55.133   39237   No     1464
Ca1 10.105.132.138 5247 10.106.15.135   38899   No     1464
Ca0  10.105.132.138 5247  239.255.255.249 5247    No      1464


Name IfId               McastRef
---   ------------------ --------
Ca2   0x0098BA0000000041 0
Ca1   0x00BC2C800000003D 0
Ca0   0x008B53C000000001  2
```

Nota: L'ultima riga di questo output punta all'interfaccia del tunnel CAPWAP creata per il traffico multicast e **McastRef** mostra il numero di access point che sono stati uniti al gruppo. Queste informazioni sono utili quando è necessario verificare se un punto di accesso che non riceve il traffico multicast è stato aggiunto al gruppo multicast.

4. Immettere il comando **show int capwap 0** per verificare che l'interfaccia del tunnel visualizzi l'indirizzo di destinazione come indirizzo del gruppo multicast:

```
ish_5760#show int capwap 0
Capwap0 is up, line protocol is up
Hardware is Capwap
MTU 1464 bytes, BW 10000000 Kbit/sec, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation UNKNOWN, loopback not set
Keepalive set (10 sec)
Carrier delay is 0 msec
Tunnel iifid 39217105861607425, Tunnel MTU 1464
Tunnel source 10.105.132.138:5247, destination 239.255.255.249:5247
```

5. Immettere il comando **show wireless multicast group summary** per verificare se viene creata

una voce MGID per il gruppo multicast a cui il client tenta di unirsi (nell'esempio riportato viene utilizzato **239.255.255.250**):

```
ish_5760#show wireless multicast group summary
IPv4 groups
-------------
MGID   Source   Group             Vlan
-------------------------------------
4160   0.0.0.0 239.255.255.250   32
```

6. Immettere questo comando per verificare se il client in questione è stato aggiunto alla tabella MGID:

```
ish_5760#show wireless multicast group 239.255.255.250 vlan 32
Source : 0.0.0.0
Group : 239.255.255.250
Vlan : 32
MGID : 4160


Number of Active Clients : 1
Client List
-------------


Client MAC     Client IP      Status
---------------------------------------
1410.9fef.272c 192.168.24.50 MC_ONLY
```

7. Immettere questo comando per verificare se la voce MGID è stata aggiunta all'access point per questo client:

```
ish_ap#show capwap mcast mgid id 4160
L3 MGID = 4160 WLAN bitmap = 0x0001
Slot map/tx-cnt: R0:0x0000/0 R1:0x0001/1499
Clients per Wlan
Wlan : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

!! This shows the number of clients per slot, per Service Set
Identification (SSID) on the AP.

Normal Mcast Clients R0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Normal Mcast Clients R1: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
rx pkts = 1499 drp pkts = 0
tx packets:
wlan : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
slots0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots1 : 1499 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0


Normal Mcast Clients:
Client: 1410.9fef.272c --- Qos User Priority: 0
```

Nota: Prendere in considerazione i contatori sui pacchetti ricevuti e trasmessi. Queste informazioni sono utili quando si cerca di determinare se l'access point inoltra correttamente i pacchetti al client.

8. Immettere il comando **show ip igmp snooping igmpv2-tracking** per visualizzare tutte le mappature dei gruppi multicast client. Fornisce un'istantanea dei client connessi e dei gruppi

a cui sono connessi. Di seguito è riportato un esempio di output:

```
ish_5760#show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------

Client: 192.168.24.50 Port: Ca1
Group: 239.255.255.250 Vlan: 32 Source: 0.0.0.0 blacklisted: no

!! If the client has joined more than one multicast group, all the group entries
will be shown here one after the other.


SGV to Client mappings
----------------------

Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32
Client: 192.168.24.50 Port: Ca1 Blacklisted: no

!! If there is more than one client entry, these will be shown here.
```

9. Immettere questo comando per verificare il MGID dal controller:

```
ish_5760#show ip igmp snoop wireless mgid
Total number of L2-MGIDs = 33

Total number of MCAST MGIDs = 0

Wireless multicast is Enabled in the system
Vlan bcast nonip-mcast mcast mDNS-br mgid Stdby Flags
1 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
100 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
115 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
517 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
518 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
519 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
520 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
521 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
522 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
523 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
524 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
525 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
526 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
527 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
528 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
529 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
530 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
531 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
1002 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1003 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1004 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1005 Enabled Enabled Enabled Enabled Disabled 0:0:1:0


Index MGID (S, G, V)
-----------------------------------------------------------
```

Risoluzione dei problemi

Di seguito è riportato un elenco dei comandi di **debug** che è possibile utilizzare per risolvere i problemi di configurazione del controller:

- **debug ip igmp snooping**
- **debug ip igmp snooping 239.255.255.250**
- **debug ip igmp snooping querier**
- **debug ip igmp snoop wireless ios client-tracking**
- **debug ip igmp snoop wireless ios events**
- **errore debug ip igmp snoop wireless ios**
- **dettaglio ap wireless debug ip igmp snoop**
- **errore debug ip igmp snoop wireless ap**
- **debug ip igmp snoop wireless ap event**
- **debug ip igmp snoop wireless ap message**
- **debug platform multicast**
- **errore di debug platform multicast**
- **debug platform multicast event**
- **piattaforma di debug l2m-igmp/l2m-mld/l2multicast/l3multicast**
- **errore debug l2mcast wireless ios**
- **debug l2mcast wireless ios mgid**
- **debug l2mcast wireless ios spi**

  Nota: Per evitare problemi di prestazioni, assicurarsi di utilizzare solo i comandi di **debug** multicast appropriati.

Di seguito è riportato un esempio di output del comando **show debug**:

```
show debug
NG3K Wireless:
NG3K WIRELESS Error DEBUG debugging is on
L3 Multicast platform:
NGWC L3 Multicast Platform debugs debugging is on
L2M IGMP platform debug:
NGWC L2M IGMP Platform debugs debugging is on
```

```
NGWC L2M IGMP SPI debugs debugging is on
NGWC L2M IGMP Error debugs debugging is on
IP multicast:
IGMP debugging is on for 239.10.10.11
IGMP tracking:
igmpv2 tracking debugging is on
L2MC Wireless:
L2MC WIRELESS SPI EVENTS debugging is on
L2MC WIRELESS REDUNDANCY EVENTS debugging is on
L2MC WIRELESS ERROR debugging is on
IGMP Wireless:
IGMP SNOOP wireless IOS Errors debugging is on
IGMP SNOOP wireless IOS Events debugging is on

Nova Platform:
igmp/snooping/wireless/ap/event debugging is on
multicast/event debugging is on
igmp/snooping/wireless/ap/message/rx debugging is on
igmp/snooping/wireless/ap/message/tx debugging is on
wireless/log debugging is on
l2multicast/error debugging is on
igmp/snooping/wireless/ap/error debugging is on
multicast/error debugging is on
multicast debugging is on
l2multicast/event debugging is on
wireless/platform debugging is on
igmp/snooping/wireless/ap/detail debugging is on
```

Di seguito è riportato un output di esempio che mostra la creazione di MGID sul controller:

```
*Sep 7 00:12:11.029: IGMPSN: Received IGMPv2 Report for group 239.255.255.250 received
on Vlan 32, port Ca1
*Sep 7 00:12:11.029: IGMPSN: group: Received IGMPv2 report for group 239.255.255.250
from Client 192.168.24.50 received on Vlan 32, port Ca1
*Sep 7 00:12:11.029: (l2mcast_tracking_is_client_blacklisted) Client: 192.168.24.50
Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32 Port: Ca1
*Sep 7 00:12:11.029: (l2mcsn_process_report) Allocating MGID for Vlan: 32 (S,G):
:239.255.255.250
*Sep 7 00:12:11.029: (l2mcast_wireless_alloc_mcast_mgid) Vlan: 32 Source: 0.0.0.0
Group: 239.255.255.250
*Sep 7 00:12:11.030: (l2mcast_wireless_alloc_mcast_mgid) Hash entry added!
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client) Protocol: IGMPSN
Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, MGID:
4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_get_client_params) Client Addr: 192.168.24.50 Client-id:
40512055681220617 Mcast-vlan: 32(l2mcast_wireless_inform_client) Protocol: IGMPSN
Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, iifid =
0x9667C000000004 MGID: 4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_wireless_inform_client) Sent INFORM CLIENT SPI
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client)
l2mcast_wireless_inform_client passed
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: IGMP has sent the
WCM_INFORM_CLIENT with ^I client_id = 40512055681220617/8fed8000000009 ^I capwap id =
42335320837980164 ^I mac_addr = 1410.9fef.272c ^I num_entry = 1
```

Una volta creata la voce sul lato Cisco IOS®, questa viene passata al processo Wireless Control Module (WCM), che verifica prima di aggiungere la voce:

```
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: i = 0, source = 0.0.0.0 group =
239.255.255.250 client_ip = 192.168.24.50 vlan = 32, mgid = 4160 add = 1
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: in igmp_wcm_client_join_callback
source = 0.0.0.0 group = 239.255.255.250 client_ip = 192.168.24.50 vlan = 32
```

```
client_mac = 1410.9fef.272c mgid = 4160
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: apfMswtp_iifid = 9667c000000004
capwap_if_id = 9667c000000004
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: rrc_manual_mode = 0
rrc_status = 2
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: locking mgid Tree in file
bcast_process.c line 491
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: allocateL3mgid: mgid entry AVL
search key dump:
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: 00000000: 00 00 00 00 ef 01 01
01 00 08 ff ff ff ff ff ff .................^M 00000010: ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff .................^M 00000020: ff ff ..^M
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mcast_group_client_lookup:
Lookup failed for client with mac 1410.9fef.272c
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: unlocking mgid Tree in file
bcast_process.c line 624
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: spamLradSendMgidInfo: ap =
0C85.25C7.9AD0 slotId = 1, apVapId = 1, numOfMgid = 1 join = 1 isL2Mgid = 0,
mc2ucflag = 0, qos = 0
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mscbApMac = 0c85.25c7.9ad0
client_mac_addr = 1410.9fef.272c slotId = 1 vapId = 1 mgid = 4160 numOfSGs = 2,
rrc_status = 2
```

Di seguito è riportato un elenco dei comandi di **debug** che è possibile utilizzare per risolvere i problemi di configurazione dell'access point:

- **debug capwap mcast fwd**
- **debug capwap mcast query**

Di seguito è riportato un esempio di output del comando **debug**:

```
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapDecodeMgidPayload: mgidTypeStr L3 IGMP MGID
ADD,mgidType 53,mgid=4160,mgid operation=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapAddMgidEntry: slotId= 1, client_mac=
1410.9fef.272c, mgid= 4160, wlanid= 0, mc2ucflag= 0, priority= 0, downpriority= 0
L3 mgid flag = L3 IGMP MGID .
*Sep 7 06:00:38.099: CAPWAP MCAST: allocateMgidEntry: mgid = 4160,isL3Mgid=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwap_bss_mgid_enable:MGID 4160 enable -
Slot=1 WLAN=1
*Sep 7 06:00:38.099: CAPWAP MCAST: L3 IGMP MGID ADD MGID = 4160 SUCCESSFUL .!!
```

> **Nota:** Quando si aggiunge la voce MGID, l'ID VLAN viene visualizzato come **0** nell'output precedente. Tuttavia, anche se la voce viene eliminata, mostra il mapping VLAN corretto.

Di seguito è riportato un elenco di comandi **show** che è possibile analizzare ulteriormente dal controller:

- **mostra riepilogo client wireless**
- **mostra tutto il database wcdb**
- **mostra riepilogo gruppi multicast wireless**
- **show wireless multicast group <ip> vlan <id>**
- **show wireless multicast source <ip> group <ip> vlan <id>**

- **show ip igmp snooping wireless mgid**
- **show ip igmp snooping igmpv2-tracking**

Di seguito è riportato un elenco di comandi **show** che è possibile utilizzare per ulteriori analisi dall'access point:

- **show capwap mcast mgid all**
- **show capwap mcast id mgid <id>**

Considerazioni importanti

Di seguito sono riportate alcune importanti considerazioni e limitazioni relative alla configurazione descritta nel presente documento:

- Il numero di gruppi multicast a cui ogni client può restare in ascolto è limitato a 16. Dopo che il client ha inviato la richiesta di *join* con il 17° gruppo, la creazione viene eseguita sul lato Cisco IOS, ma il lato WCM invia un messaggio di *rifiuto* a Cisco IOS. Quest'ultimo elimina quindi il gruppo.
- Attualmente è supportato solo IGMP versione 2 (V2). Se un client utilizza IGMP versione 3 (V3), la creazione di MGID non viene eseguita sul controller. Per questo motivo, nell'origine, nel gruppo e nella VLAN l'indirizzo di origine è sempre **0.0.0.0**.
- Il numero di MGID L3 supportati sulla NGWC è compreso tra 4.160 e 8.191. Poiché una voce MGID è una combinazione di indirizzo multicast e VLAN, possono esistere solo 4.000 combinazioni di questo tipo. Ciò potrebbe rappresentare un limite in ambienti di grandi dimensioni.
- la funzione *Bonjour* sulle VLAN non è supportata. Infatti l'indirizzo IP 224.0.0.251 è un indirizzo multicast locale del collegamento. I Cisco serie 5760 e 3850 WLC, come qualsiasi altro switch Catalyst, non snoop gli indirizzi locali del collegamento. Per questo motivo, verrà visualizzato questo messaggio di errore:

```
IGMPSN: group: Received IGMPv2 report for group 224.0.0.251 from Client 192.168.24.94
received on Vlan 32, port Ca93 with invalid group address.
```