

BSS (Basic Service Set) 802.11v sur AireOS WLC

Contenu

[Introduction](#)

[Informations générales](#)

[Service de multidiffusion dirigée \(DMS\) :](#)

[Période d'inactivité BSS max. :](#)

[Gestion de la transition BSS](#)

[Demande sollicitée](#)

[Demande d'équilibrage de charge non sollicitée](#)

[Demande d'itinérance optimisée non sollicitée](#)

[Piloter le client sur l'AP FRA \(affectation radio flexible\)](#)

[Imminent de dissociation](#)

[Réponse de gestion de la transition BSS](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Service de multidiffusion dirigée \(DMS\)](#)

[Gestion de la période d'inactivité BSS max.](#)

[Gestion de la transition BSS](#)

[Vérification](#)

[Prise en charge SSID](#)

[Assistance client](#)

[Déboguer l'activité du client](#)

[Client doté de fonctionnalités DMS](#)

[Possibilité de transition BSS client](#)

[Références](#)

Introduction

Ce document décrit la prise en charge du protocole 802.11v sur un WLC (contrôleur de réseau local sans fil).

Informations générales

802.11v fait référence à l'IEEE (Institute of Electrical and Electronics Engineers) 802.11 Wireless Network Management (Amendement 8).

Les stations qui prennent en charge WNM (Wireless Network Management) peuvent échanger

des informations entre elles (points d'accès et clients sans fil) afin d'améliorer leurs performances.

AireOS WLC version 8.1 ou ultérieure prend en charge ces services WNM :

- Service de multidiffusion dirigée (DMS)
- BSS (Basic Service Set) Gestion des périodes d'inactivité max.
- Gestion de la transition BSS

Service de multidiffusion dirigée (DMS) :

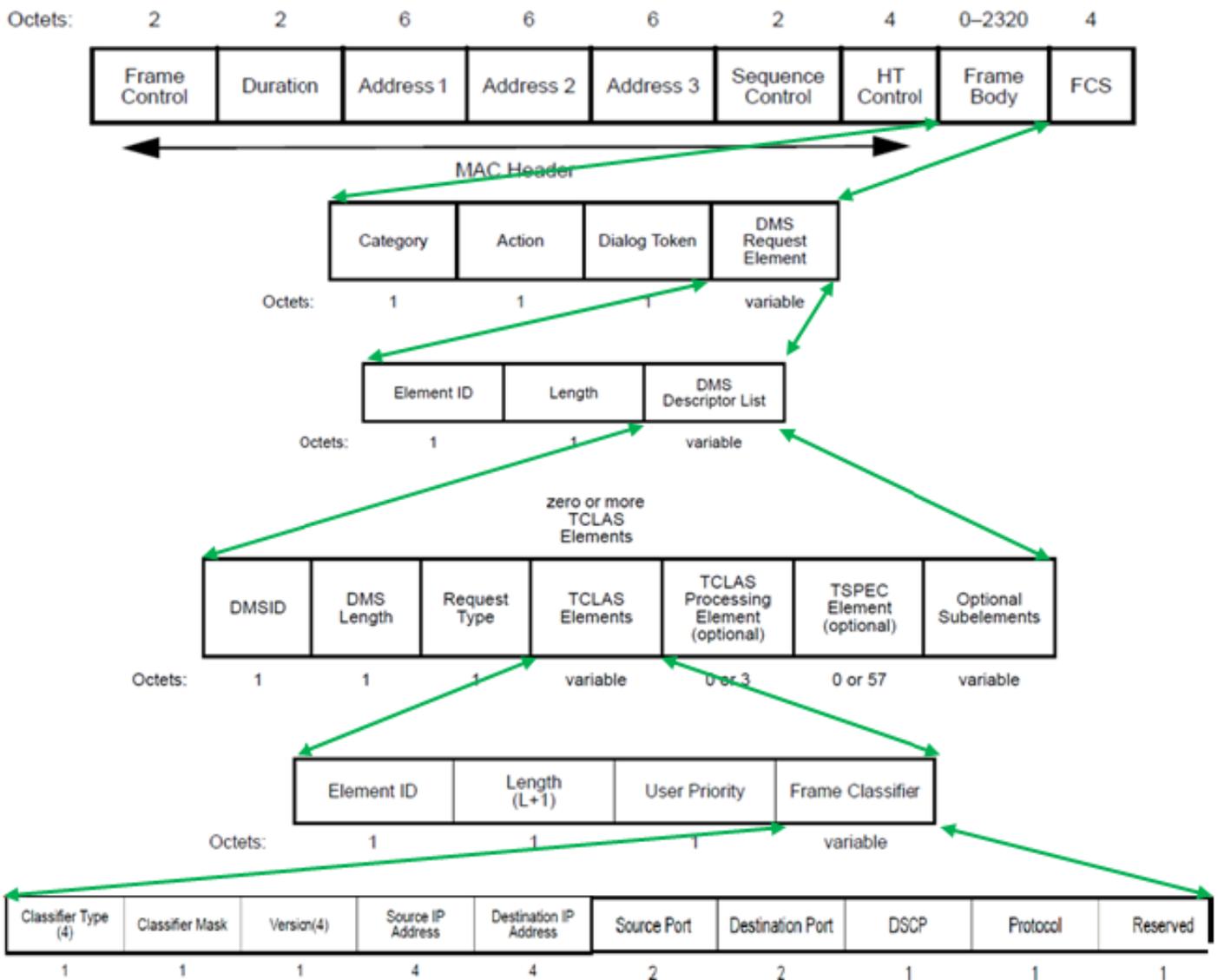
Les clients qui prennent en charge DMS peuvent demander à l'AP (point d'accès) d'envoyer un flux de multidiffusion en monodiffusion, comme une fonction de flux de support dynamique.

Pour plus d'informations sur le flux multimédia : [Guide de déploiement de VideoStream](#)

Sans DMS, un client doit réveiller chaque intervalle DTIM pour recevoir le trafic de multidiffusion. Avec DMS, l'AP (point d'accès) met en mémoire tampon le trafic de multidiffusion pour certains clients, lorsque le client se réveille, il envoie une trame de monodiffusion afin de demander ce trafic. Il permet au client de dormir plus longtemps et d'économiser l'énergie de la batterie. Les trames de multidiffusion sont transmises en monodiffusion sur l'air, envoyées à un débit de données supérieur à celui auquel elles auraient été utilisées sans DMS.

Les clients sans fil peuvent envoyer une trame Add de type requête DMS afin de demander au point d'accès d'envoyer en monodiffusion le trafic d'un ou plusieurs flux de multidiffusion spécifiques.

Trame de gestion - Type de demande DMS



Il existe trois types de demande DMS :

Description Valeur du type de demande

Ajouter	0
Supprimer	1
Modifier	2
Réservé	3-255

La demande DMS-Add inclut un descripteur DMS.

Dans la liste des descripteurs DMS se trouve l'élément TCLAS, qui spécifie le flux de trafic de multidiffusion que le client sans fil demande d'obtenir en monodiffusion. TCLAS spécifie l'adresse IP source/de destination, le port source/de destination en plus des autres champs.

Le point d'accès envoie ces flux de trafic en monodiffusion au client sans fil et continue également d'envoyer ces flux en multidiffusion à tout autre client du réseau qui ne prend pas en charge DMS.

Dans une trame de requête DMS, il peut également y avoir un élément TSPEC (facultatif), dans lequel le client sans fil peut définir les exigences et les caractéristiques de QoS d'un flux de trafic.

Note: TSPEC non pris en charge

Dans cet exemple, le client a envoyé une requête DMS (trame de gestion, code de catégorie 10 : WNM, code d'action 23 : Requête DMS, pour le flux de multidiffusion IPv4 sur le groupe 224.0.0.251, UDP (Protocole 17), port de destination 9 (dans ce document, Wireshark n'est pas en mesure de décoder complètement une requête DMS).

3... Apple 58:95:0a CiscoInc 7d:d9:10 802.11 DMS Request[Malformed Packet]

Frame 34853: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0

Radiotap Header v0, Length 18

802.11 radio information

IEEE 802.11 Action, Flags:C

IEEE 802.11 wireless LAN management frame

- Fixed parameters
 - Category code: WNM (10)
 - Action code: DMS Request (23)
- Tagged parameters (27 bytes)
- [Malformed Packet: IEEE 802.11]

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11011010	00000101
0010	00000000	00000000	11010000	00000000	00111010	00000001	01111100	00001110: . .
0018	11001110	01111101	11011001	00010000	10100100	11110001	11101000	01011000	.}.....X
0020	10010101	00001010	01111100	00001110	11001110	01111101	11011001	00010000	.. .}..
0028	11110000	11011101	Category	Action	Dial.Token	Element-ID	Length	DMS IDC..
0030	DMS Length	Req- Type	Ele-ID-TCLAS	Length (L+1)	User Priority	Classif.Type	Classif.Mask	Version (4)U.
0038	Source IP address				Destination IP address			
0040	Source Port		Destination Port		DSCP	Protocol	00000000	00111111?
0048	11001100	01010000	10111000						.P.

3... Apple 58:95:0a CiscoInc 7d:d9:10 802.11 DMS Request[Malformed Packet]

Frame 34853: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0

Radiotap Header v0, Length 18

802.11 radio information

IEEE 802.11 Action, Flags:C

IEEE 802.11 wireless LAN management frame

- Fixed parameters
 - Category code: WNM (10)
 - Action code: DMS Request (23)
- Tagged parameters (27 bytes)
- [Malformed Packet: IEEE 802.11]

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11011010	00000101
0010	00000000	00000000	11010000	00000000	00111010	00000001	01111100	00001110: . .
0018	11001110	01111101	11011001	00010000	10100100	11110001	11101000	01011000	.}.....X
0020	10010101	00001010	01111100	00001110	11001110	01111101	11011001	00010000	.. .}..
0028	11110000	11011101	00001010	00010111	00000101	01100011	00011000	00000000c..
0030	00010110	00000000	00001110	00010011	00000000	00000100	01010101	00000100U.
0038	00000000	00000000	00000000	00000000	11100000	00000000	00000000	11111011
0040	00000000	00000000	00000000	00001001	00000000	00010001	00000000	00111111?
0048	11001100	01010000	10111000						.P.

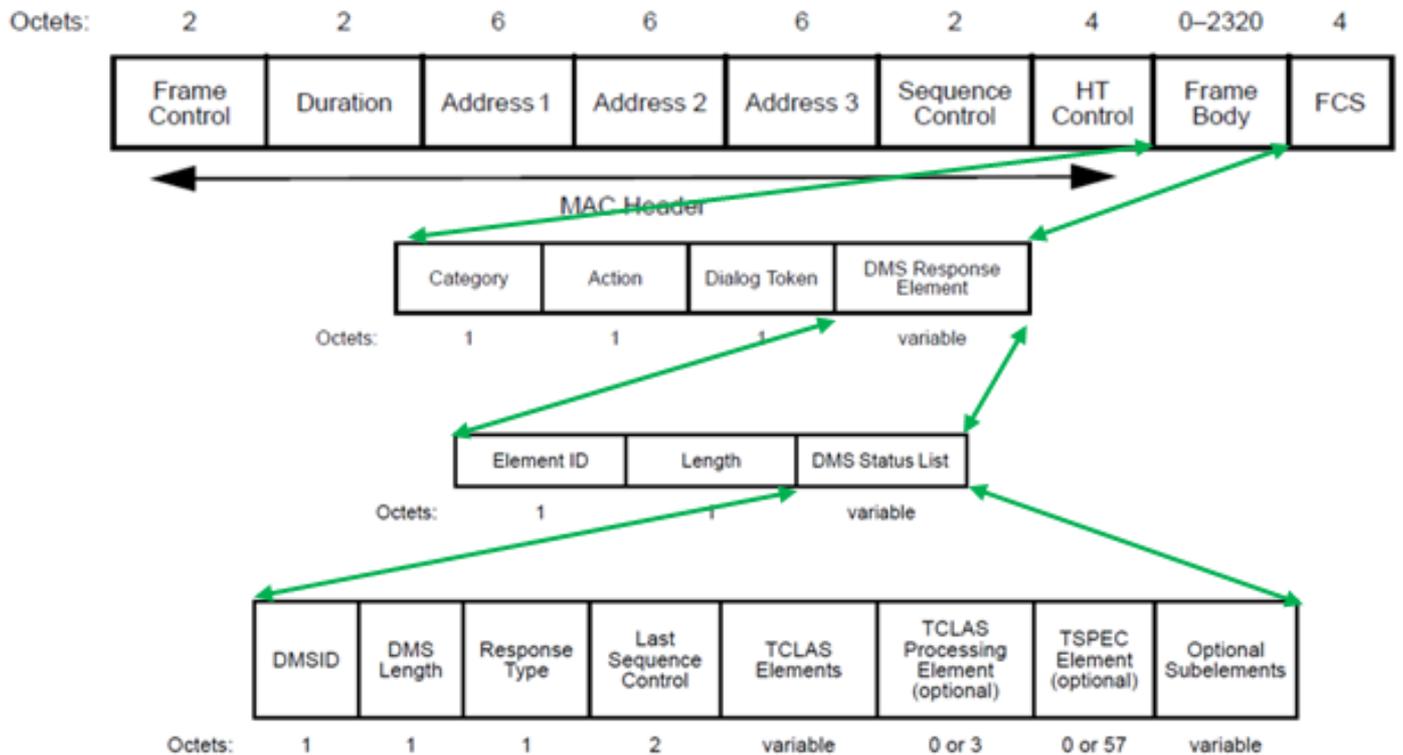
Le point d'accès répond à la demande DMS avec une réponse DMS, qui peut être une réponse DMS-Accepter ou Réponse DMS-Refuser.

Si l'AP envoie une réponse DMS-Accepter, il attribue également un DMSID à ce flux de communication.

Le client sans fil peut utiliser le changement de type de requête DMS pour modifier un DMSID existant, par exemple pour demander un TSPEC différent pour un flux de trafic.

Note: La modification DMS n'est pas prise en charge

Trame de gestion - Type de réponse DMS



Il existe trois types de réponse DMS :

Valeur du champ Description

0	Accept (accepter)
1	Refusé
2	Terminer
3-255	Réservé

Dans cet exemple, le point d'accès a envoyé un accusé de réception de réponse DMS et il attribue un ID DMS 1 à la demande DMS envoyée par le client.

3... CiscoInc 7d:d9:10 Apple 58:95:0a 802.11 DMS Response[Malformed Packet]

```

+ Frame 34855: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters
    - Category code: WNM (10)
    - Action code: DMS Response (24)
  + Tagged parameters (8 bytes)
  + [Malformed Packet: IEEE 802.11]

```

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11010101	00000101
0010	00000000	00000000	11010000	00000000	11011010	00000000	10100100	11110001
0018	11101000	01011000	10010101	00001010	01111100	00001110	11001110	01111101	.X.. ..}
0020	11011001	00010000	01111100	00001110	11001110	01111101	11011001	00010000}..
0028	01110000	01000000	Category	Action	Dial.Token	Element-ID	Length	DMS ID	p@...d..
0030	DMS Length	Resp- Type	Last Sequence Control	10011100	00101011	10011110	00000011+..	

3... CiscoInc 7d:d9:10 Apple 58:95:0a 802.11 DMS Response[Malformed Packet]

```

+ Frame 34855: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters
    - Category code: WNM (10)
    - Action code: DMS Response (24)
  + Tagged parameters (8 bytes)
  + [Malformed Packet: IEEE 802.11]

```

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11010101	00000101
0010	00000000	00000000	11010000	00000000	11011010	00000000	10100100	11110001
0018	11101000	01011000	10010101	00001010	01111100	00001110	11001110	01111101	.X.. ..}
0020	11011001	00010000	01111100	00001110	11001110	01111101	11011001	00010000}..
0028	01110000	01000000	00001010	00011000	00000101	01100100	00000101	00000001	p@...d..
0030	00000011	00000000	11111111	11111111	10011100	00101011	10011110	00000011+..

Après cela, s'il y a un paquet avec le groupe de destination 224.0.0.251 sur le port 9, il est envoyé à l'air en tant que multidiffusion et il est également mis en mémoire tampon sur l'AP jusqu'à ce que le client qui a envoyé la requête DMS soit éveillé soit disponible pour le recevoir en tant que monodiffusion.

Voici un exemple de destination de paquet vers le groupe 224.0.0.251 sur le port 9 envoyé en tant que multidiffusion régulière. Notez que l'adresse MAC du destinataire et de la destination fait référence au groupe de multidiffusion.

```
+ Radiotap Header v0, Length 18
+ 802.11 radio information
- IEEE 802.11 Data, Flags: .....F.C
  Type/Subtype: Data (0x0020)
+ Frame Control Field: 0x0802
  000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: IPv4mcast fb (01:00:5e:00:00:fb)
  Destination address: IPv4mcast_fb (01:00:5e:00:00:fb)
  Transmitter address: CiscoInc_7d:d9:10 (7c:0e:ce:7d:d9:10)
  Source address: IntelCor_7c:30:58 (e4:b3:18:7c:30:58)
  BSS Id: CiscoInc_7d:d9:10 (7c:0e:ce:7d:d9:10)
  STA address: IPv4mcast_fb (01:00:5e:00:00:fb)
  .... .... 0000 = Fragment number: 0
  0110 0000 0010 .... = Sequence number: 1538
  Frame check sequence: 0xb8fad31e [correct]
  [FCS Status: Good]
+ Logical-Link Control
+ Internet Protocol Version 4, Src: 172.16.0.51, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 59887, Dst Port: 9
  Source Port: 59887
  Destination Port: 9
  Length: 110
  Checksum: 0x6288 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 124]
```

Voici un exemple de trame envoyée en monodiffusion au client qui a envoyé la requête DMS. Ici, l'adresse de destination et de réception est l'adresse MAC du client et non l'adresse MAC de multidiffusion. Le paquet de multidiffusion est également envoyé en tant qu'AMSDU.

```
⊕ Radiotap Header v0, Length 21
⊕ 802.11 radio information
⊖ IEEE 802.11 QoS Data, Flags: .....F.C
  ... Type/Subtype: QoS Data (0x0028)
  ⊕ Frame Control Field: 0x8802
  ... 000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Apple 58:95:0a (a4:f1:e8:58:95:0a)
  Destination address: Apple 58:95:0a (a4:f1:e8:58:95:0a)
  ... Transmitter address: CiscoInc_7d:d9:10 (7c:0e:ce:7d:d9:10)
  ... Source address: IntelCor_7c:30:58 (e4:b3:18:7c:30:58)
  ... BSS Id: CiscoInc_7d:d9:10 (7c:0e:ce:7d:d9:10)
  ... STA address: Apple_58:95:0a (a4:f1:e8:58:95:0a)
  ... .... 0000 = Fragment number: 0
  ... 0000 0001 0000 .... = Sequence number: 16
  ... Frame check sequence: 0x174f6716 [correct]
  ... [FCS Status: Good]
  ⊕ Qos Control: 0x0083
⊖ IEEE 802.11 Aggregate MSDU
  ⊖ A-MSDU Subframe #1
  ... Destination address: IPv4mcast_00 (01:00:5e:00:00:00)
  ... Source address: IntelCor_7c:30:58 (e4:b3:18:7c:30:58)
  ... A-MSDU Length: 138
  ⊕ Logical-Link Control
  ⊕ Internet Protocol Version 4, Src: 172.16.0.51, Dst: 224.0.0.251
  ⊖ User Datagram Protocol, Src Port: 59887, Dst Port: 9
  ... Source Port: 59887
  ... Destination Port: 9
  ... Length: 110
  ... Checksum: 0x6288 [unverified]
  ... [Checksum Status: Unverified]
  ... [Stream index: 124]
```

Une fois qu'un client sans fil ne veut plus recevoir un flux de multidiffusion en tant que monodiffusion, il peut envoyer une nouvelle demande DMS pour fermer ce flux, il utilise l'ID DMS qui a été attribué auparavant par l'AP. Il s'agit d'une requête DMS - Type de suppression (1)

49165 133.314820 Apple 58:95:0a CiscoInc 7d:d9:10 802.11 DMS Request

- Frame 49165: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Radiotap Header v0, Length 18
- 802.11 radio information
- IEEE 802.11 Action, Flags:C
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters
 - Category code: WNM (10)
 - Action code: DMS Request (23)
 - Tagged parameters (6 bytes)

```

0000  00000000 00000000 00010010 00000000 00101110 01001000 00000000 00000000  ....H..
0008  00010000 00000010 10000101 00001001 10100000 00000000 11011101 00000101  ....
0010  00000000 00000000 11010000 00000000 00111010 00000001 01111100 00001110  ....|.
0018  11001110 01111101 11011001 00010000 10100100 11110001 11101000 01011000  .}....X
0020  10010101 00001010 01111100 00001110 11001110 01111101 11011001 00010000  ..|...}..
0028  11110000 11100001 00001010 00010111 00000110 01100011 00000011 00000001  ....C..
0030  00000001 00000001 11010110 10111000 00111001 00110100 00000000 00000000  ..94

```

49165 133.314820 Apple 58:95:0a CiscoInc 7d:d9:10 802.11 DMS Request

- Frame 49165: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Radiotap Header v0, Length 18
- 802.11 radio information
- IEEE 802.11 Action, Flags:C
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters
 - Category code: WNM (10)
 - Action code: DMS Request (23)
 - Tagged parameters (6 bytes)

```

0000  00000000 00000000 00010010 00000000 00101110 01001000 00000000 00000000  ....H..
0008  00010000 00000010 10000101 00001001 10100000 00000000 11011101 00000101  ....
0010  00000000 00000000 11010000 00000000 00111010 00000001 01111100 00001110  ....|.
0018  11001110 01111101 11011001 00010000 10100100 11110001 11101000 01011000  .}....X
0020  10010101 00001010 01111100 00001110 11001110 01111101 11011001 00010000  ..|...}..
0028  11110000 11100001 00001010 00010111 00000110 01100011 00000011 00000001  ....C..
0030  00000001 00000001 11010110 10111000 00111001 00110100 00000000 00000000  ..94

```

Et le point d'accès confirme cette terminaison avec une terminaison de type de réponse DMS (2)

49170 133.317305 CiscoInc 7d:d9:... Apple 58:95:0a 802.11 DMS Response

```

+ Frame 49170: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters
    - Category code: WNM (10)
    - Action code: DMS Response (24)
  + Tagged parameters (8 bytes)

```

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11010101	00000101
0010	00000000	00000000	11010000	00000000	11011010	00000000	10100100	11110001
0018	11101000	01011000	10010101	00001010	01111100	00001110	11001110	01111101	.X.. ..}
0020	11011001	00010000	01111100	00001110	11001110	01111101	11011001	00010000}..
0028	01100000	01100000	Category	Action	DialToken	Element-ID	Length	DMS ID	..d..
0030	DMS Length	Resp-Type	Last Sequence Control	00111010	10011010	00010001	00000100:...

49170 133.317305 CiscoInc 7d:d9:... Apple 58:95:0a 802.11 DMS Response

```

+ Frame 49170: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters
    - Category code: WNM (10)
    - Action code: DMS Response (24)
  + Tagged parameters (8 bytes)

```

0000	00000000	00000000	00010010	00000000	00101110	01001000	00000000	00000000H..
0008	00010000	00000010	10000101	00001001	10100000	00000000	11010101	00000101
0010	00000000	00000000	11010000	00000000	11011010	00000000	10100100	11110001
0018	11101000	01011000	10010101	00001010	01111100	00001110	11001110	01111101	.X.. ..}
0020	11011001	00010000	01111100	00001110	11001110	01111101	11011001	00010000}..
0028	01100000	01100000	00001010	00011000	00000110	01100100	00000101	00000001	..d..
0030	00000011	00000010	11111111	11111111	00111010	10011010	00010001	00000100	...:...

Période d'inactivité BSS max. :

Lorsqu'un point d'accès ne reçoit plus de trames d'un client sans fil pendant une certaine période, il suppose que le client a quitté le réseau et qu'il le dissocie. La période d'inactivité BSS Max est la durée pendant laquelle un point d'accès peut garder un client associé sans avoir à recevoir de trame (le client peut rester en veille). Cette valeur est communiquée au client sans fil via la trame de réponse d'association et de réassociation. Cela permet aux clients de rester en veille plus longtemps et d'économiser l'énergie de la batterie.

La période d'inactivité BSS Max apparaît uniquement dans les trames de réponse association-réponse ou réassociation

```
802.11 radio information
IEEE 802.11 Association Response, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
  Tagged parameters (153 bytes)
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Extended Capabilities (4 octets)
    Tag: BSS Max Idle Period
      Tag Number: BSS Max Idle Period (90)
      Tag length: 3
      BSS Max Idle Period (1000 TUs): 400
      .... .0 = BSS Max Idle Period Options: Protected Keep-Alive Required: 0
    Tag: Vendor Specific: Microsot: WMM/WME: Parameter Element
    Tag: QoS Map Set
```

La période d'inactivité maximale BSS est spécifiée en unités de 1 000 TU (unités de temps).
Chaque unité de temps est égale à 1,024 millisecondes

Délai d'inactivité = 1,024 x BSS Période d'inactivité max. = X secondes

Dans l'exemple de trame :

Délai d'inactivité = 1,024 x 405 = 414,72 secondes

Si le bit Protected Keep-alive Required est défini sur 1, cela signifie que le client sans fil doit envoyer une trame protégée RSN au point d'accès afin de réinitialiser le compteur d'inactivité. Si elle est définie sur 0, comme dans cet exemple, le client sans fil peut envoyer n'importe quel type de trame (protégée ou non protégée) pour réinitialiser le compteur d'inactivité au niveau de l'AP.

Gestion de la transition BSS

La demande de gestion de la transition BSS 802.11v est une suggestion adressée au client. Le client peut décider lui-même de suivre ou non la suggestion. La dissociation d'un client peut être forcée si la fonction Disassociation-imminent est activée. Il dissocie le client après un certain temps si le client ne se réassocie pas à l'un des points d'accès suggérés.

La transition BSS 802.11v est appliquée à ces quatre scénarios :

Demande sollicitée

Le client sans fil envoie une requête de gestion de la transition BSS 802.11v avant qu'ils ne se déplacent pour trouver une meilleure option de réassociation des points d'accès.

Exemple de requête de gestion de la transition BSS 802.11v

```

1093 2.515163 CiscoInc 3a:0f:... CiscoInc 7d:d9:10 802.11 BSS Transition Management Query
-----
+ Frame 1093: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  + Fixed parameters
  + Tagged parameters (2 bytes)
-----
0000 00000000 00000000 00010010 00000000 00101110 01001000 00000000 00000000 .....H..
0008 00010000 00000010 10000101 00001001 10100000 00000000 11101011 00000101 .....
0010 00000000 00000000 11010000 00000000 00111010 00000001 01111100 00001110 .....|.
0018 11001110 01111101 11011001 00010000 11000100 01111101 01001111 00111010 .}...}0:
0020 00001111 01011100 01111100 00001110 11001110 01111101 11011001 00010000 .\|...}..
0028 11100000 11110010 00001010 00000110 00000110 00000110 00010001 10001001 .....1.
0030 01110101 01001111                                     u0

```

```

1093 2.515163 CiscoInc 3a:0f:... CiscoInc 7d:d9:10 802.11 BSS Transition Management Query
-----
+ Frame 1093: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0
+ Radiotap Header v0, Length 18
+ 802.11 radio information
+ IEEE 802.11 Action, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  + Fixed parameters
  + Tagged parameters (2 bytes)
-----
0000 00000000 00000000 00010010 00000000 00101110 01001000 00000000 00000000 .....H..
0008 00010000 00000010 10000101 00001001 10100000 00000000 11101011 00000101 .....
0010 00000000 00000000 11010000 00000000 00111010 00000001 01111100 00001110 .....|.
0018 11001110 01111101 11011001 00010000 11000100 01111101 01001111 00111010 .}...}0:
0020 00001111 01011100 01111100 00001110 11001110 01111101 11011001 00010000 .\|...}..
0028 11100000 11110010 00001010 00000110 00000110 00010001 00010001 10001001 .....1.
0030 01110101 01001111                                     u0

```

QReason signifie Motif de requête de transition BSS, qui est la raison pour laquelle le client demande la liste des points d'accès candidats. Dans cet exemple, le client a envoyé une raison 16, qui correspond à Faible RSSI. Pour obtenir la liste complète des raisons de la requête de transition, consultez le tableau 8-138 de la norme IEEE 802.11-2012.

Une fois que la radio a reçu cette trame, elle répond avec une demande de gestion de transition BSS afin de fournir la liste des candidats AP.

```

1098 2.522295 CiscoInc 7d:d9:... CiscoInc 3a:0f:5c 802.11 BSS Transition Management Request
-----
Frame 1098: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 Action, Flags: .....C
IEEE 802.11 wireless LAN management frame
- Fixed parameters
  . Category code: WNM (10)
  . Action code: BSS Transition Management Request (7)
  . Dialog token: 0x06
  . ... ..1 = Preferred Candidate List Included: 1
  . ... ..0 = Abridged: 0
  . ... .1.. = Disassociation Imminent: 1
  . ... 0... = BSS Termination Included: 0
  . ...0 ... = ESS Disassociation Imminent: 0
  . Disassociation Timer: 1953
  . Validity Interval: 200
  . BSS Transition Candidate List Entries: 344300c88b262cd0e702000000060700000000000000000...

```

Demande d'équilibrage de charge non sollicité

Lorsque la fonctionnalité d'équilibrage de charge + transition BSS du WLC est activée, le point d'accès n'envoie plus de trame de déauthentification à un client sans fil lorsqu'il est lourdement chargé, il envoie une demande de gestion de transition BSS afin de suggérer au client sans fil un autre point d'accès moins chargé.

Pour plus d'informations sur la fonctionnalité de équilibrage de charge : [Configuration de l'équilibrage de charge agressif](#)

Demande d'itinérance optimisée non sollicitée

Lorsque WLC a optimisé l'itinérance + transition BSS activée, l'AP n'envoie plus de trame de déauthentification à un client sans fil lorsque le client ne répond pas au RSSI minimum (ou à tout autre paramètre lié à l'itinérance optimisée), il envoie une gestion de transition BSS afin de suggérer au client sans fil un meilleur AP.

Pour plus d'informations sur la fonctionnalité d'itinérance optimisée : [Itinérance optimisée Cisco](#)

Piloter le client sur l'AP FRA (affectation radio flexible)

Si un client se connecte à une cellule moins optimale dans un point d'accès FRA, le point d'accès envoie une requête de gestion de transition BSS 802.11v à ce client.

Lorsqu'un point d'accès qui prend en charge FRA (comme 2800 ou 3800) utilise seulement 5 GHz, il y a deux cellules (micro et macro). Si un client se connecte à la macro-cellule mais que la micro-cellule est plus optimale (basée sur RSSI), alors le point d'accès envoie une demande de gestion de transition BSS 802.11v au client afin de suggérer de déplacer la micro-cellule et vice versa.

Cette fonctionnalité est disponible depuis la version 8.2.110.0.

Pour plus d'informations sur FRA : [FRA \(Flexible Radio Assignment\) et Radios redondantes](#)

Imminent de dissociation

Dans une demande de gestion de transition BSS, vous pouvez ajouter un champ Disassociation Imminent. Cette fonction est de dissocier le client après un certain temps si le client ne se réassocie pas à un autre AP.

Lorsque la demande d'itinérance optimisée non sollicitée est déclenchée, le point d'accès envoie une demande de gestion de transition BSS au client et attend une certaine période (durée configurée sous Optimized Roaming Disassociation Timer), si le client ne se dirige pas vers un meilleur point d'accès dans cette période, alors le point d'accès termine la disassociation du client.

Lorsque la demande d'équilibrage de charge non sollicité est déclenchée, le point d'accès envoie une demande de gestion de transition BSS au client et attend une certaine période (durée configurée sous Disassociation Timer), si le client ne se déplace pas vers un point d'accès moins encombré dans cette période, alors le point d'accès termine la disassociation du client.

Exemple de trame de gestion de la transition BSS avec Disassociation imminente activée :

```
802.11 radio information
IEEE 802.11 Action, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Request (7)
    Dialog token: 0x01
    ....1 = Preferred Candidate List Included: 1
    ....0 = Abridged: 0
    ....1.. = Disassociation Imminent: 1
    ....0... = BSS Termination Included: 0
    ...0 .... = ESS Disassociation Imminent: 0
    Disassociation Timer: 200
    Validity Interval: 200
    BSS Transition Candidate List Entries: 341054a274ede004e7020000000b070301ffdd1d0040960c...
```

Réponse de gestion de la transition BSS

Une fois qu'un client sans fil a reçu une demande de gestion de transition BSS, il peut ou ne peut pas envoyer de réponse de gestion de transition BSS. Si le client passe à un autre AP, il l'envoie avec le code d'état Accepter, mais s'il prévoit de rester sur le même AP pour plusieurs raisons, il l'envoie avec le code d'état Rejeter plus le motif de rejet.

Exemple de trame de réponse de gestion de la transition BSS

```
60272 12:16:06.114913 Apple_58:95:0a CiscoInc_e8:32:70 BSS Transition Management Response
Frame 60272: 51 bytes on wire (408 bits), 51 bytes captured (408 bits) on interface 0
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 Action, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Response (8)
    Dialog token: 0x0c
    BSS Transition Status Code: 1
    BSS Termination Delay: 0
```

Dans cet exemple, le client sans fil rejette la liste des candidats AP et ne se déplace pas vers un autre AP. Le code d'état 1 indique la raison pour laquelle le client quitte le ESS. Pour obtenir la liste complète des définitions de code d'état, consultez le tableau 8-253 de la norme IEEE 802.11-2012.

Conditions préalables

Conditions requises

Pour tirer parti des fonctionnalités 802.11v d'un réseau local sans fil, il est nécessaire d'avoir des clients sans fil prenant en charge la norme 802.11v.

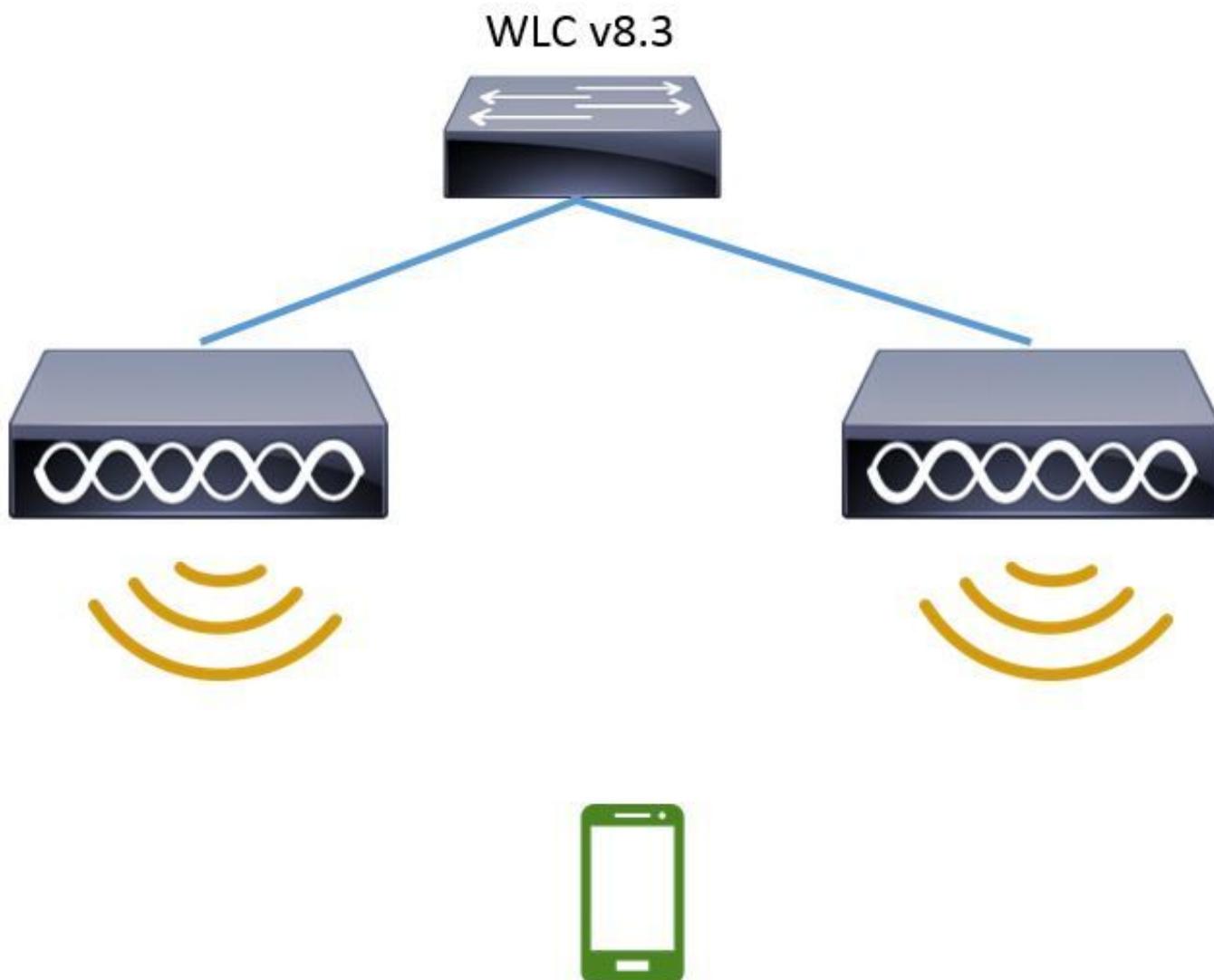
Components Used

WLC v8.3

Ipod Touch 6e génération v10.1.1

Configuration

Diagramme du réseau



Configurations

Service de multidiffusion dirigée (DMS)

Configuration sur WLAN pour activer DMS :

Configuration CLI :

```
> config wlan disable <wlan-id>  
> config wlan dms enable <wlan-id>  
> config wlan enable <wlan-id>
```

Configuration de l'interface utilisateur graphique (disponible à partir de la version 8.3)

Étape 1. Accédez à **WLANs > Wlan-ID** et cliquez sur WLAN pour activer DMS.

WLANs

WLANs

Current Filter: None [Change Filter] [Clear Filter]

<input type="checkbox"/>	WLAN ID	Type	Profile Name
<input type="checkbox"/>	6	WLAN	phone-open
<input type="checkbox"/>	7	WLAN	11v

Étape 2. Accédez à **Advanced > 11v BSS Transition Support** et activez le service de multidiffusion dirigée

WLANs > Edit '11v'

General Security QoS Policy-Mapping **Advanced**

FlexConnect Local Switching Enabled

FlexConnect Local Auth Enabled

Learn Client IP Address Enabled

Wlan based Central Switching Enabled

Central DHCP Processing Enabled

Override DNS Enabled

NAT-PAT Enabled

Central Assoc Enabled

11k

Assisted Roaming Prediction Optimization Enabled

Neighbor List Enabled

Neighbor List Dual Band Enabled

Denial Maximum Count

Prediction Minimum Count

HTTP Profiling

Universal AP Admin Support

Universal AP Admin

11v BSS Transition Support

BSS Transition

Disassociation Imminent

Disassociation Timer(0 to 3000 TBTT)

Optimized Roaming Disassociation Timer(0 to 40 TBTT)

BSS Max Idle Service

Directed Multicast Service

mDNS

mDNS Snooping Enabled

mDNS Profile

Gestion de la période d'inactivité BSS max.

Configuration sur WLAN pour activer la gestion de la période d'inactivité maximale BSS :

Configuration CLI :

```
> config wlan disable <wlan-id>
> config wlan bssmaxidle enable <wlan-id>
> config wlan usertimeout <seconds> <wlan-id>
> config wlan enable <wlan-id>
```

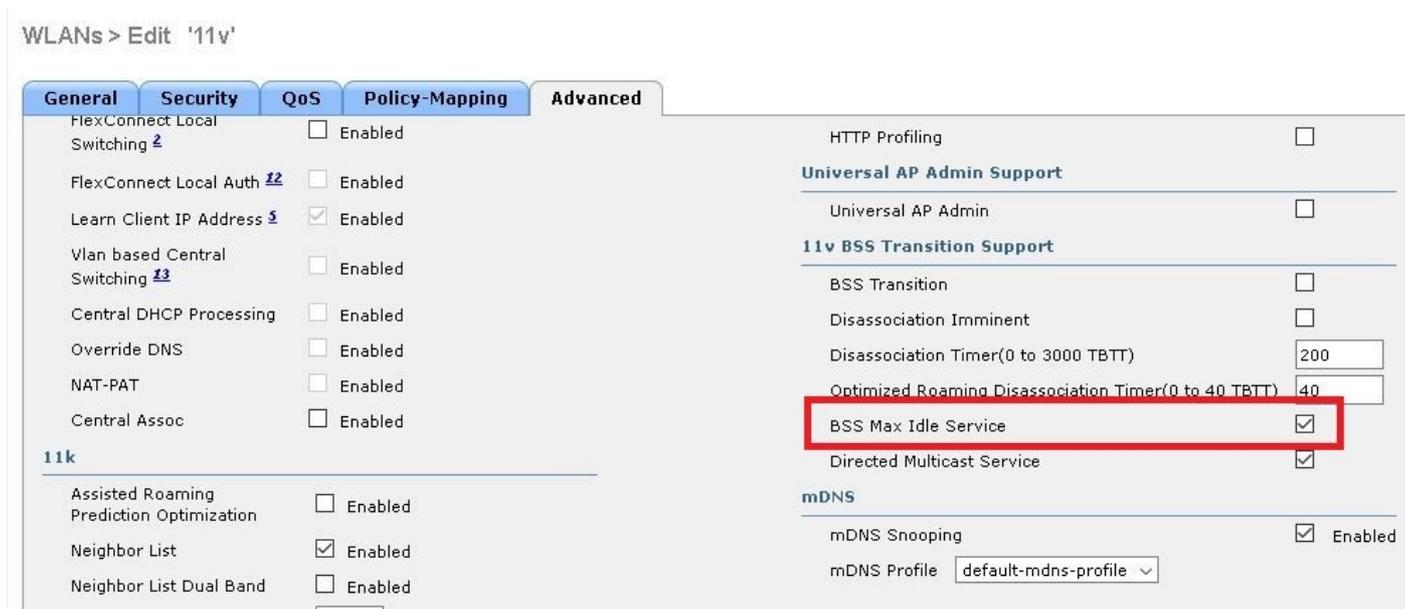
<seconds> Client Idle timeout(in seconds) on this WLAN. Range 0,15-100000 secs. 0 in order to disable

Configuration de l'interface utilisateur graphique :

Étape 1. Accédez à **WLANs > WLAN-ID** et cliquez sur WLAN pour définir la période d'inactivité BSS Max.



Étape 2. Accédez à **Advanced > 11v BSS Transition Support** et activez **BSS Max Idle Service**.



Note: Cette interface utilisateur graphique est présentée dans la version 8.3. Pour les versions précédentes, utilisez la commande **config wlan bssmaxidle enable <wlan-id>**

Étape 3. Accédez à **Advanced > Client User Idle timeout** et définissez la valeur de délai en secondes.

WLANs > Edit '11v'

General	Security	QoS	Policy-Mapping	Advanced
Static IP Forwarding ==		<input type="checkbox"/> Enabled		
Wi-Fi Direct Clients Policy		<input type="text" value="Disabled"/>		
Maximum Allowed Clients Per AP Radio		<input type="text" value="200"/>		
Clear HotSpot Configuration		<input type="checkbox"/> Enabled		
Client user idle timeout(15-100000)		<input checked="" type="checkbox"/>	<input type="text" value="400"/>	Timeout Value (secs)
Client user idle threshold (0-10000000)		<input type="text" value="0"/>	Bytes	
Radius NAI-Realm		<input type="checkbox"/>		
11ac MU-MIMO		<input checked="" type="checkbox"/>		
Off Channel Scanning Defer				
Scan Defer Priority		0 1 2 3 4 5 6 7		
		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>		
Scan Defer Time(msecs)		<input type="text" value="100"/>		
FlexConnect				

Gestion de la transition BSS

Configuration sur WLAN pour activer la gestion de la transition BSS :

Note: Si seule la transition BSS est activée, la seule façon pour les points d'accès d'envoyer des trames de demande de gestion de transition BSS est si un client sans fil envoie une trame de requête de gestion de transition BSS.

Note: Pour que les AP envoient une demande de gestion de transition BSS lorsqu'ils sont lourdement chargés, il est nécessaire d'activer la transition BSS + l'équilibrage de charge.

Note: Pour que les points d'accès envoient une demande de gestion de transition BSS lorsqu'un client sans fil n'a pas le meilleur RSSI, il est nécessaire d'activer la transition BSS + l'itinérance optimisée.

Demande sollicitée

Configuration CLI :

```
> config wlan disable <wlan-id>
> config wlan bss-transition enable <wlan-id>
> config wlan enable <wlan-id>
```

Configuration de l'interface utilisateur graphique :

Étape 1. Accédez à **WLANs > WLAN ID > Advanced** et activez **BSS Transition**.

WLANs > Edit '11v'

The screenshot shows the 'Advanced' configuration tab for a WLAN. The 'BSS Transition' option under the '11v BSS Transition Support' section is checked and highlighted with a red box. Other options include 'Universal AP Admin Support', 'Disassociation Imminent', 'Disassociation Timer', 'Optimized Roaming Disassociation Timer', 'BSS Max Idle Service', and 'Directed Multicast Service'. The 'mDNS' section is also visible with 'mDNS Snooping' checked and 'mDNS Profile' set to 'default-mdns-profile'.

Section	Option	Value / Status
General	FlexConnect Local Switching	<input type="checkbox"/> Enabled
	FlexConnect Local Auth	<input type="checkbox"/> Enabled
	Learn Client IP Address	<input checked="" type="checkbox"/> Enabled
	Vlan based Central Switching	<input type="checkbox"/> Enabled
	Central DHCP Processing	<input type="checkbox"/> Enabled
	Override DNS	<input type="checkbox"/> Enabled
	NAT-PAT	<input type="checkbox"/> Enabled
	Central Assoc	<input type="checkbox"/> Enabled
	11k	Assisted Roaming Prediction Optimization
Neighbor List		<input checked="" type="checkbox"/> Enabled
Neighbor List Dual Band		<input type="checkbox"/> Enabled
Denial Maximum Count		2
Prediction Minimum Count		2
Advanced	HTTP Profiling	<input type="checkbox"/>
	Universal AP Admin Support	
	Universal AP Admin	<input type="checkbox"/>
	11v BSS Transition Support	
	BSS Transition	<input checked="" type="checkbox"/>
	Disassociation Imminent	<input type="checkbox"/>
	Disassociation Timer(0 to 3000 TBTT)	200
	Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
	BSS Max Idle Service	<input checked="" type="checkbox"/>
	Directed Multicast Service	<input checked="" type="checkbox"/>
mDNS		
mDNS Snooping	<input checked="" type="checkbox"/> Enabled	
mDNS Profile	default-mdns-profile	

Demande d'équilibrage de charge non sollicité

Configuration CLI :

```
> config wlan disable <wlan-id>
> config wlan bss-transition enable <wlan-id>
> config wlan load-balance allow enable <wlan-id>
> config wlan enable <wlan-id>
```

Configuration de l'interface utilisateur graphique :

Étape 1. Accédez à **WLANs > WLAN ID > Advanced** et activez **BSS Transition** et **Client Load Balancing**.

WLANs > Edit '11v'

General	Security	QoS	Policy-Mapping	Advanced
FlexConnect Local Switching 2	<input type="checkbox"/>	Enabled		HTTP Profiling <input type="checkbox"/>
FlexConnect Local Auth 22	<input type="checkbox"/>	Enabled		Universal AP Admin Support
Learn Client IP Address 1	<input checked="" type="checkbox"/>	Enabled		Universal AP Admin <input type="checkbox"/>
Vlan based Central Switching 23	<input type="checkbox"/>	Enabled		11v BSS Transition Support
Central DHCP Processing	<input type="checkbox"/>	Enabled		BSS Transition <input checked="" type="checkbox"/>
Override DNS	<input type="checkbox"/>	Enabled		Disassociation Imminent <input type="checkbox"/>
NAT-PAT	<input type="checkbox"/>	Enabled		Disassociation Timer(0 to 3000 TBTT) <input type="text" value="200"/>
Central Assoc	<input type="checkbox"/>	Enabled		Optimized Roaming Disassociation Timer(0 to 40 TBTT) <input type="text" value="40"/>
11k				
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		BSS Max Idle Service <input checked="" type="checkbox"/>
Neighbor List	<input checked="" type="checkbox"/>	Enabled		Directed Multicast Service <input checked="" type="checkbox"/>
Neighbor List Dual Band	<input type="checkbox"/>	Enabled		mDNS
Denial Maximum Count <input type="text" value="2"/>				mDNS Snooping <input checked="" type="checkbox"/> Enabled
Prediction Minimum Count <input type="text" value="2"/>				mDNS Profile <input type="text" value="default-mdns-profile"/>

WLANs > Edit '11v'

General	Security	QoS	Policy-Mapping	Advanced
Layer2 Acl	<input type="text" value="None"/>			Management Frame Protection (MFP)
URL ACL	<input type="text" value="None"/>			MFP Client Protection 2 <input type="text" value="Optional"/>
P2P Blocking Action	<input type="text" value="Disabled"/>			DTIM Period (in beacon intervals)
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled	<input type="text" value="60"/>	Timeout Value (secs)	802.11a/n (1 - 255) <input type="text" value="1"/>
Maximum Allowed Clients 4	<input type="text" value="0"/>			802.11b/g/n (1 - 255) <input type="text" value="1"/>
Static IP Tunneling 21	<input type="checkbox"/> Enabled			NAC
Wi-Fi Direct Clients Policy	<input type="text" value="Disabled"/>			NAC State <input type="text" value="None"/>
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>			Load Balancing and Band Select
Clear HotSpot Configuration	<input type="checkbox"/> Enabled			Client Load Balancing <input checked="" type="checkbox"/>
Client user idle timeout(15-100000)	<input checked="" type="checkbox"/>	<input type="text" value="400"/>	Timeout Value (secs)	Client Band Select <input type="checkbox"/>
Client user idle threshold (0-100000000)	<input type="text" value="0"/>		Bytes	Passive Client
Radius NAI-Realm	<input type="checkbox"/>			Passive Client <input type="checkbox"/>
				Voice
				Media Session Snooping <input type="checkbox"/>

Demande d'itinérance optimisée non sollicitée

Configuration CLI :

```
> config wlan disable <wlan-id>
> config wlan bss-transition enable <wlan-id>
> config wlan chd <wlan-id> enable
> config wlan enable <wlan-id>
> config advanced { 802.11a | 802.11b } optimized-roaming enable
```

Configuration de l'interface utilisateur graphique :

Étape 1. Accédez à **WLANs > WLAN ID > Advanced** et activez **BSS Transition and Coverage Hole Detection**.

WLANs > Edit '11v'

General	Security	QoS	Policy-Mapping	Advanced
FlexConnect Local Switching 2	<input type="checkbox"/>	Enabled		HTTP Profiling <input type="checkbox"/>
FlexConnect Local Auth 22	<input type="checkbox"/>	Enabled		Universal AP Admin Support
Learn Client IP Address 1	<input checked="" type="checkbox"/>	Enabled		Universal AP Admin <input type="checkbox"/>
Vlan based Central Switching 23	<input type="checkbox"/>	Enabled		11v BSS Transition Support
Central DHCP Processing	<input type="checkbox"/>	Enabled		BSS Transition <input checked="" type="checkbox"/>
Override DNS	<input type="checkbox"/>	Enabled		Disassociation Imminent <input type="checkbox"/>
NAT-PAT	<input type="checkbox"/>	Enabled		Disassociation Timer(0 to 3000 TBTT) <input type="text" value="200"/>
Central Assoc	<input type="checkbox"/>	Enabled		Optimized Roaming Disassociation Timer(0 to 40 TBTT) <input type="text" value="40"/>
11k				BSS Max Idle Service <input checked="" type="checkbox"/>
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		Directed Multicast Service <input checked="" type="checkbox"/>
Neighbor List	<input checked="" type="checkbox"/>	Enabled		mDNS
Neighbor List Dual Band	<input type="checkbox"/>	Enabled		mDNS Snooping <input checked="" type="checkbox"/> Enabled
Denial Maximum Count	<input type="text" value="2"/>			mDNS Profile <input type="text" value="default-mdns-profile"/>
Prediction Minimum Count	<input type="text" value="2"/>			

WLANs > Edit '11v'

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input type="checkbox"/>	Enabled		
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled		
Enable Session Timeout	<input type="checkbox"/>			
Aironet IE	<input type="checkbox"/>	Enabled		
Diagnostic Channel 18	<input type="checkbox"/>	Enabled		
Override Interface ACL	IPv4	<input type="text" value="None"/>		IPv6 <input type="text" value="None"/>
Layer2 Acl	<input type="text" value="None"/>			
URL ACL	<input type="text" value="None"/>			
P2P Blocking Action	<input type="text" value="Disabled"/>			
Client Exclusion 3	<input checked="" type="checkbox"/>	Enabled	<input type="text" value="60"/>	Timeout Value (secs)
Maximum Allowed Clients 8	<input type="text" value="0"/>			

Étape 2. Naviget to **WIRELESS > Advanced > Optimized Roaming** et enable pour les deux bandes **Optimized Roaming Mode**. Pour plus d'informations sur les paramètres d'itinérance optimisée, consultez ce document : [Guide de déploiement HDX \(High Density Experience\), version 8.0](#)

Wireless

MONITOR WLANs CONTROLLER **WIRELESS** SECURITY

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
 - Advanced**
 - RF Management
 - Flexible Radio Assignment
 - Load Balancing
 - Band Select
 - Rx Sens Threshold
 - Optimized Roaming**
 - Network Profile
 - Qos
 - Preferred Calls

Optimized Roaming

802.11 a

Optimized Roaming Mode Enable

Optimized Roaming Interval sec

Optimized Roaming Data Rate Threshold mbps

802.11 b

Optimized Roaming Mode Enable

Optimized Roaming Interval sec

Optimized Roaming Data Rate Threshold mbps

1. CHDM configuration can be done in Wireless---> RF Profile ---> Edit
 2. Disable 802.11a / 802.11b network before changing Optimized Roaming

Imminent de dissociation

Configuration CLI :

```
> config wlan disable <wlan-id>
> config wlan bss-transition enable <wlan-id>
> config wlan disassociation-imminent enable <wlan-id>
> config wlan bss-transition disassociation-imminent oproam-timer <timer-in-TBTT> <WLAN id>
> config wlan bss-transition disassociation-imminent timer <timer-in-TBTT> <WLAN id>
> config wlan enable <wlan-id>
```

Étape 1. Accédez à **WLANs > WLAN ID > Advanced**, activez **BSS Transition, Disassociation Imminent** et définissez **Disassociation Timer** et **Optimized Roaming Disassociation Timer**.

Configuration de l'interface utilisateur graphique :

General	Security	QoS	Policy-Mapping	Advanced
FlexConnect Local Switching 2	<input type="checkbox"/>	Enabled		HTTP Profiling <input type="checkbox"/>
FlexConnect Local Auth 22	<input type="checkbox"/>	Enabled		Universal AP Admin Support
Learn Client IP Address 3	<input checked="" type="checkbox"/>	Enabled		Universal AP Admin <input type="checkbox"/>
Vlan based Central Switching 13	<input type="checkbox"/>	Enabled		11v BSS Transition Support
Central DHCP Processing	<input type="checkbox"/>	Enabled		BSS Transition <input checked="" type="checkbox"/>
Override DNS	<input type="checkbox"/>	Enabled		Disassociation Imminent <input type="checkbox"/>
NAT-PAT	<input type="checkbox"/>	Enabled		Disassociation Timer(0 to 3000 TBTT) <input type="text" value="200"/>
Central Assoc	<input type="checkbox"/>	Enabled		Optimized Roaming Disassociation Timer(0 to 40 TBTT) <input type="text" value="40"/>
11k				BSS Max Idle Service <input checked="" type="checkbox"/>
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		Directed Multicast Service <input checked="" type="checkbox"/>
Neighbor List	<input checked="" type="checkbox"/>	Enabled		mDNS
Neighbor List Dual Band	<input type="checkbox"/>	Enabled		mDNS Snooping <input checked="" type="checkbox"/> Enabled
Denial Maximum Count	<input type="text" value="2"/>			mDNS Profile <input type="text" value="default-mdns-profile"/>
Prediction Minimum Count	<input type="text" value="2"/>			

General	Security	QoS	Policy-Mapping	Advanced
FlexConnect Local Switching 2	<input type="checkbox"/>	Enabled		HTTP Profiling <input type="checkbox"/>
FlexConnect Local Auth 22	<input type="checkbox"/>	Enabled		Universal AP Admin Support
Learn Client IP Address 3	<input checked="" type="checkbox"/>	Enabled		Universal AP Admin <input type="checkbox"/>
Vlan based Central Switching 13	<input type="checkbox"/>	Enabled		11v BSS Transition Support
Central DHCP Processing	<input type="checkbox"/>	Enabled		BSS Transition <input checked="" type="checkbox"/>
Override DNS	<input type="checkbox"/>	Enabled		Disassociation Imminent <input checked="" type="checkbox"/>
NAT-PAT	<input type="checkbox"/>	Enabled		Disassociation Timer(0 to 3000 TBTT) <input type="text" value="200"/>
Central Assoc	<input type="checkbox"/>	Enabled		Optimized Roaming Disassociation Timer(0 to 40 TBTT) <input type="text" value="40"/>
11k				BSS Max Idle Service <input checked="" type="checkbox"/>
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		Directed Multicast Service <input checked="" type="checkbox"/>
				mDNS

Note: Les minuteurs sont spécifiés dans les unités TBTT (Target Beacon Transmission Time), qui est l'intervalle entre chaque balise. Par défaut, chaque balise est envoyée toutes les 100 ms, donc par défaut 1 TBTT = 100 ms. Minuteurs = X TBTT/10 = x secondes.

Vérification

Ces images montrent la prise en charge du WLAN (Wireless Local Area Network) et des clients sans fil pour les différents services 802.11v.

Prise en charge SSID

- DMS

```

> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
< IEEE 802.11 Wireless LAN management frame
  < Fixed parameters (12 bytes)
    Timestamp: 0x0000002a95f28006
    Beacon Interval: 0.104448 [Seconds]
  > Capabilities Information: 0x1011
  < Tagged parameters (267 bytes)
    > Tag: SSID parameter set: tst-80211v
    > Tag: Supported Rates 12(B), 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: Country Information: Country Code US, Environment Any
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
    > Tag: HT Information (802.11n D1.10)
  < Tag: Extended Capabilities (8 octets)
    Tag Number: Extended Capabilities (127)
    Tag length: 8
    > Extended Capabilities: 0x00 (octet 1)
    > Extended Capabilities: 0x10 (octet 2)
    > Extended Capabilities: 0x00 (octet 3)
  < Extended Capabilities: 0x04 (octet 4)
    .... ..0 = Channel Usage: Not supported
    .... ..0. = SSID List: Not supported
    .... .1.. = DMS: Supported
    .... 0... = UTC TSF Offset: Not supported
    ...0 .... = Peer U-APSD Buffer STA Support: Not supported
    ..0. .... = TDLS Peer PSM Support: Not supported
    .0.. .... = TDLS channel switching: Not supported
    0... .... = Interworking: Not supported
    > Extended Capabilities: 0x01 (octet 5)
    > Extended Capabilities: 0x40 (octet 6)
    > Extended Capabilities: 0x00 (octet 7)
    > Extended Capabilities: 0x40 (octet 8)
  > Tag: Cisco CCX1 CKIP + Device Name
  > Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x03
  > Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
  < Tag: VHT Operation (IEEE Std 802.11ac/D3.1)

```

- Gestion de la transition BSS

```
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
  Tagged parameters (231 bytes)
    Tag: SSID parameter set: tst-11v
    Tag: Supported Rates 11(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 11
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: Country Information: Country Code MX, Environment Any
    Tag: QBSS Load Element 802.11e CCA Version
    Tag: Power Constraint: 3
    Tag: ERP Information
    Tag: HT Capabilities (802.11n D1.10)
    Tag: RSN Information
    Tag: HT Information (802.11n D1.10)
    Tag: RM Enabled Capabilities (5 octets)
    Tag: Extended Capabilities (6 octets)
      Tag Number: Extended Capabilities (127)
      Tag length: 6
      Extended Capabilities: 0x00 (octet 1)
      Extended Capabilities: 0x10 (octet 2)
      Extended Capabilities: 0x08 (octet 3)
        .... 0 = TFS: Not supported
        .... 0. = WNM-Sleep Mode: Not supported
        ..0. = TIM Broadcast: Not supported
        ... 1... = BSS Transition: Supported
        ...0 .... = QoS Traffic Capability: Not supported
        ..0. .... = AC Station Count: Not supported
        .0.. .... = Multiple BSSID: Not supported
        0... .... = Timing Measurement: Not supported
      Extended Capabilities: 0x00 (octet 4)
      Extended Capabilities: 0x01 (octet 5)
      Extended Capabilities: 0x40 (octet 6)
    Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x02
      Tag Number: Vendor Specific (150)
```

Assistance client

- DMS

```
802.11 radio information
IEEE 802.11 Association Request, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters (4 bytes)
    Capabilities Information: 0x1011
    Listen Interval: 0x0014
  Tagged parameters (144 bytes)
    Tag: SSID parameter set: tst-80211v
    Tag: Supported Rates 12(B), 18, 24, 36, 48, 54, [Mbit/sec]
    Tag: Power Capability Min: 3, Max :22
    Tag: Supported Channels
    Tag: RSN Information
    Tag: HT Capabilities (802.11n D1.10)
  Extended Capabilities (4 octets)
    Tag Number: Extended Capabilities (127)
    Tag length: 4
    Extended Capabilities: 0x00 (octet 1)
    Extended Capabilities: 0x00 (octet 2)
    Extended Capabilities: 0x00 (octet 3)
  Extended Capabilities: 0x04 (octet 4)
    ....0 = Channel Usage: Not supported
    ....0 = SSID List: Not supported
    ... .1.. = DNS: Supported
    ....0... = UTC TSF Offset: Not supported
    ...0 .... = Peer U-APSD Buffer STA Support: Not supported
    ..0. .... = TDLS Peer PSM Support: Not supported
    .0.. .... = TDLS channel switching: Not supported
    0... .... = Interworking: Not supported
  Tag: Vendor Specific: Broadcom
  Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
  Tag: Vendor Specific: Microsof: WMM/WME: Information Element
```

- Gestion de la transition BSS

```

+ IEEE 802.11 Association Request, Flags: .....C
- IEEE 802.11 Wireless LAN management frame
  + Fixed parameters (4 bytes)
  - Tagged parameters (140 bytes)
    + Tag: SSID parameter set: tst-11v
    + Tag: Supported Rates 11(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
    + Tag: Power Capability Min: 5, Max :24
    + Tag: Supported Channels
    + Tag: RSN Information
    + Tag: HT Capabilities (802.11n D1.10)
    - Tag: Extended Capabilities (3 octets)
      Tag Number: Extended Capabilities (127)
      Tag length: 3
      + Extended Capabilities: 0x00 (octet 1)
      + Extended Capabilities: 0x00 (octet 2)
      - Extended Capabilities: 0x08 (octet 3)
        .... 0 = TFS: Not supported
        .... 0 = WMM-Sleep Mode: Not supported
        .... 0 = TIM Broadcast: Not supported
        .... 1... = BSS Transition: Supported
        .... 0... = QoS Traffic Capability: Not supported
        ..0. .... = AC Station Count: Not supported
        .0.. .... = Multiple BSSID: Not supported
        0... .... = Timing Measurement: Not supported
    + Tag: RM Enabled Capabilities (5 octets)
    + Tag: Vendor Specific: Broadcom
    + Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    + Tag: Vendor Specific: Microsof: WMM/WME: Information Element
  
```

Débuguer l'activité du client

Afin de surveiller l'activité du client 11v, ces commandes sont disponibles.

```

> debug client <mac-add-of-client>
> debug mac addr <mac-add-of-client>
> debug 11v all enable
  
```

Client doté de fonctionnalités DMS

Le client est compatible 11v

```

*apfMsConnTask_0: Nov 01 22:55:27.577: a4:f1:e8:58:95:0a Association received from mobile on
BSSID 7c:0e:ce:7d:d9:10 AP AP-3700-1
*apfMsConnTask_0: Nov 01 22:55:27.577: a4:f1:e8:58:95:0a Client is 11v BSS Transition capable
Le client envoie une requête DMS pour le port udp 9 du groupe 224.0.0.251 et le point d'accès
envoie le DMS accepter
  
```

```

*apfMsConnTask_0: Nov 01 22:56:43.928: a4:f1:e8:58:95:0a Got action frame from this client.
*apfMsConnTask_0: Nov 01 22:56:43.928: a4:f1:e8:58:95:0a Received a 11v Action Frame with code
[23] from mobile station
*apfMsConnTask_0: Nov 01 22:56:43.928: Received 80211v_DMS_REQ Action Frame
*apfMsConnTask_0: Nov 01 22:56:43.928: WLAN-id : 1 | vap_ip : 1
*apfMsConnTask_0: Nov 01 22:56:43.928: a4:f1:e8:58:95:0a Posting msg of type:
  
```

```

APF_80211v_MSG_DMS_REQ for STA and LRAD:7c:0e:ce:7d:d9:10,slot:0, len:26
*apfMsConnTask_0: Nov 01 22:56:43.928: 11v g_msgQueue = 0x2b415828,          osapiMessageSend
rc = 0
*apf80211vTask: Nov 01 22:56:43.929: Tclas found:
*apf80211vTask: Nov 01 22:56:43.929: [
*apf80211vTask: Nov 01 22:56:43.929: Version = 4,
*apf80211vTask: Nov 01 22:56:43.929: Destination IP = 224.0.0.251,
*apf80211vTask: Nov 01 22:56:43.929: Destination Port = 9,
*apf80211vTask: Nov 01 22:56:43.929: Protocol = 17,
*apf80211vTask: Nov 01 22:56:43.929: ]
*apf80211vTask: Nov 01 22:56:43.929: a4:f1:e8:58:95:0a New client requesting DMS for this Tclas
*apf80211vTask: Nov 01 22:56:43.929: DMS Request IE processed: State: DMS_REQ_ADD_ACCEPTED
*apf80211vTask: Nov 01 22:56:43.929: DMS Response IE created.
*apf80211vTask: Nov 01 22:56:43.929: Element ID: 100, Length: 5
*apf80211vTask: Nov 01 22:56:43.929: DMS ID: 1, DMS Length: 3, Response Type: DMS_RESP_ACCEPT,
Last Sequence Control: 65535
*apf80211vTask: Nov 01 22:56:43.929: dmsRequestState = DMS_REQ_ADD_ACCEPTED
*apf80211vTask: Nov 01 22:56:43.929: a4:f1:e8:58:95:0a apf80211vSendPacketToMs: 802.11v Action
Frame sent successfully to wlc
*apf80211vTask: Nov 01 22:56:43.929: apf80211vDmsDB_AddSTA: New DMS Client: a4:f1:e8:58:95:0a
created and added under DMS ID: 1
*apf80211vTask: Nov 01 22:56:43.929: a4:f1:e8:58:95:0a apfPostDmsClientRequestMsg: posting
capwap for ms lradmac7c:0e:ce:7d:d9:10
*apf80211vTask: Nov 01 22:56:43.929: 11v g_msgQueue = 0x2b415828,          osapiMessageSend rc
= 0
*apf80211vTask: Nov 01 22:56:43.929: a4:f1:e8:58:95:0a apf80211vHandleDmsMsgSend: send capwap
for STA lradmac 7c:0e:ce:7d:d9:10

```

À partir du point d'accès où le client est connecté

```
AP# debug dot11 dot11v all
```

```

*Nov  1 22:51:04.323: DOT11v: Inside DMS ADD Operation
*Nov  1 22:51:04.323: DOT11v: TCLAS found in DMS DB
*Nov  1 22:51:04.323: DOT11v: New client detected
*Nov  1 22:51:04.323: DOT11v: Ref Cnt: 1
*Nov  1 22:51:04.323: DOT11v: Client A4:F1:E8:58:95:0A added to DMS DB Entry
*Nov  1 22:51:04.323: DOT11v: DMS Add Operation Succeeded
*Nov  1 22:51:04.323: Received and decoded a DMS client request payload SUCCESSFULLY

```

Ensuite, le client est ajouté à la base de données DMS sur le réseau local sans fil. Tous les clients qui envoient une demande DMS-Add pour la même chaîne de multidiffusion sont répertoriés sous le même ID DMS.

```
> show wlan 1
```

```

WLAN Identifier..... 1
Profile Name..... 11v
Network Name (SSID)..... 11v
Status..... Enabled
.
.
.
Number of active DMS Clients..... 1
DMS ID Client MAC Addresses
1 a4:f1:e8:58:95:0a

```

La base de données DMS est stockée dans l'AP où ce client est connecté :

```
AP# show controllers dot11Radio { 0 | 1 } | beg Global DMS
```

Global DMS - requests:2 uc:130 drop:0
DMS enabled on WLAN(s): 11v
11v

DMS database:
Entry 1: mask=0x55 version=4 dstIp=0xE00000FB srcIp=0x00000000 dstPort=9 srcPort=0 dcsp=0
protocol=17
{Client, SSID}: {08:74:02:77:13:45, 11v}, {A4:F1:E8:58:95:0A, 11v},

Une fois que le client sans fil ferme le flux DMS, il envoie une requête DMS Remove

```
*apfMsConnTask_0: Nov 01 22:57:33.990: a4:f1:e8:58:95:0a Got action frame from this client.
*apfMsConnTask_0: Nov 01 22:57:33.990: a4:f1:e8:58:95:0a Received a 11v Action Frame with code
[23] from mobile station
*apfMsConnTask_0: Nov 01 22:57:33.990: Received 80211v_DMS_REQ Action Frame
*apfMsConnTask_0: Nov 01 22:57:33.990: WLAN-id : 1 | vap_ip : 1
*apfMsConnTask_0: Nov 01 22:57:33.990: a4:f1:e8:58:95:0a Posting msg of type:
APF_80211v_MSG_DMS_REQ for STA and LRAD:7c:0e:ce:7d:d9:10,slot:0, len:5
*apfMsConnTask_0: Nov 01 22:57:33.990: 11v g_msgQueue = 0x2b415828, osapiMessageSend
rc = 0
*apf80211vTask: Nov 01 22:57:33.991: DMS Request IE processed: State: DMS_REQ_DEL_ACCEPTED
*apf80211vTask: Nov 01 22:57:33.991: DMS Response IE created.
*apf80211vTask: Nov 01 22:57:33.991: Element ID: 100, Length: 5
*apf80211vTask: Nov 01 22:57:33.991: DMS ID: 1, DMS Length: 3, Response Type:
DMS_RESP_TERMINATE, Last Sequence Control: 65535
*apf80211vTask: Nov 01 22:57:33.991: dmsRequestState = DMS_REQ_DEL_ACCEPTED
*apf80211vTask: Nov 01 22:57:33.991: a4:f1:e8:58:95:0a apf80211vSendPacketToMs: 802.11v Action
Frame sent successfully to wlc
*apf80211vTask: Nov 01 22:57:33.991: STA: a4:f1:e8:58:95:0a has dequeued and deleted from the
DMS Entry with ID: 1
*apf80211vTask: Nov 01 22:57:33.991: apf80211vDmsDB_DeleteSTA: STA: a4:f1:e8:58:95:0a deleted
successfully under DMS ID: 1
*apf80211vTask: Nov 01 22:57:33.991: a4:f1:e8:58:95:0a apfPostDmsClientRequestMsg: posting
capwap for ms lrادمac7c:0e:ce:7d:d9:10
*apf80211vTask: Nov 01 22:57:33.991: 11v g_msgQueue = 0x2b415828, osapiMessageSend rc
= 0
```

À partir du point d'accès

```
*Nov 1 22:57:33.167: DOT11v: Removing client A4:F1:E8:58:95:0A from DMS DB Entry
*Nov 1 22:57:33.167: DOT11v: DMS DB Delete Operation Succeeded
*Nov 1 22:57:33.167: Received and decoded a DMS client request payload SUCCESSFULLY
```

Possibilité de transition BSS client

Le client est compatible 11v

```
*apfMsConnTask_3: Apr 12 10:46:36.239: 08:74:02:77:13:45 Association received from mobile on
BSSID f0:7f:06:e8:32:76 AP AP-3700
*apfMsConnTask_3: Apr 12 10:46:36.239: 08:74:02:77:13:45 Client is 11v BSS Transition capable
```

Le client envoie une requête de gestion de la transition BSS

```
*apfMsConnTask_1: Nov 14 05:40:32.857: c4:7d:4f:3a:0f:5c Got action frame from this client.
*apfMsConnTask_1: Nov 14 05:40:32.858: c4:7d:4f:3a:0f:5c Received a 11v Action Frame with code
[6] from mobile station
*apfMsConnTask_1: Nov 14 05:40:32.858: Received 80211v_BSS_TRANS_QUERY Action Frame
*apfMsConnTask_1: Nov 14 05:40:32.859: WLAN-id : 1 | vap_ip : 1
*apfMsConnTask_1: Nov 14 05:40:32.859: c4:7d:4f:3a:0f:5c Posting msg of type:
```

APF_80211v_MSG_BSS_TRANS_QUERY for STA and Lrad:00:c8:8b:26:2c:d0,slot:0, len:1

```
*apf80211vTask: Nov 14 05:40:32.860: Session URL is not NULL
*apf80211vTask: Nov 14 05:40:32.860: Disassociation Imminent is 1
*apf80211vTask: Nov 14 05:40:32.860: Disassociation Timer is 200
*apf80211vTask: Nov 14 05:40:32.860: Building BSS Transition Request Frame
*apf80211vTask: Nov 14 05:40:32.860: Adding Neighbor List Subelement
*apfMsConnTask_1: Nov 14 05:40:32.861: 11v g_msgQueue = 0x2b415828,          osapiMessageSend
rc = 0
*apf80211vTask: Nov 14 05:40:32.861: Location Info: 0,0,0 for BSSID: 7c:0e:ce:7d:d9:10
*apf80211vTask: Nov 14 05:40:32.861: Data Length of BSS Transition Request Frame: 73
*apf80211vTask: Nov 14 05:40:32.862: apf80211vHandleBSSTransQuery: lradMacAddr:
00:c8:8b:26:2c:d0 rscb parent MAC ADDR: 00:c8:8b:26:2c:d0 rscb mac address: 00:00:00:00:00:00
*apf80211vTask: Nov 14 05:40:32.862: 11v Action Frame sent:
*apf80211vTask: Nov 14 05:40:32.863: c4:7d:4f:3a:0f:5c apf80211vSendPacketToMs: 802.11v Action
Frame sent successfully to wlc
*apf80211vTask: Nov 14 05:40:32.863: Successfully sent BSS Transition Request Action Frame to
STA: c4:7d:4f:3a:0f:5c
```

Comme le Wlan a activé Disassociation Imminent, le client est dissocié après la fin du compteur Disassociation

```
*apf80211vTask: Nov 14 05:40:32.863: c4:7d:4f:3a:0f:5c Setting Session Timeout to 20 sec -
starting session timer for the mobile
*apf80211vTask: Nov 14 05:40:32.863: c4:7d:4f:3a:0f:5c Disassociate client in 20 seconds
*osapiBsnTimer: Nov 14 05:40:52.768: c4:7d:4f:3a:0f:5c Authentication session timer expired:
mark mobile for immediate deletion
*osapiBsnTimer: Nov 14 05:40:52.768: c4:7d:4f:3a:0f:5c apfMsSessionExpireCallback (apf_ms.c:707)
Expiring Mobile!
*apfReceiveTask: Nov 14 05:40:52.769: apfMsExpireMobileStation: Delete Immediately
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c apfMsExpireMobileStation (apf_ms.c:7521)
Changing state for mobile c4:7d:4f:3a:0f:5c on AP 00:c8:8b:26:2c:d0 from Associated to
Disassociated
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c apfSendDisAssocMsgDebug
(apf_80211.c:3541) Changing state for mobile c4:7d:4f:3a:0f:5c on AP 00:c8:8b:26:2c:d0 from
Disassociated to Disassociated
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c Sent Disassociate to mobile on AP
00:c8:8b:26:2c:d0-0 (reason 1, caller apf_ms.c:7614)
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c Sent Deauthenticate to mobile on BSSID
00:c8:8b:26:2c:d0 slot 0(caller apf_ms.c:7616)
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c Setting active key cache index 8 ---> 8
*apfReceiveTask: Nov 14 05:40:52.769: c4:7d:4f:3a:0f:5c Deleting the PMK cache when de-
authenticating the client.
*apfReceiveTask: Nov 14 05:40:52.769: Sent Deauthenticate to STA: c4:7d:4f:3a:0f:5c on BSSID:
00:c8:8b:26:2c:d0, slotId: 0, vapId: 1
```

Le point d'accès envoie une trame de gestion de la transition BSS en raison de l'équilibrage de charge

```
*apfMsConnTask_3: Apr 12 10:47:18.785: 08:74:02:77:13:45 11v BSS Transition Request is posted to
11v queue.
*apf80211vTask: Apr 12 10:47:18.789: Session URL is not NULL
*apf80211vTask: Apr 12 10:47:18.789: Disassociation Imminent is 1
*apf80211vTask: Apr 12 10:47:18.789: Disassociation Timer is 200
*apf80211vTask: Apr 12 10:47:18.789: Building BSS Transition Request Frame
*apf80211vTask: Apr 12 10:47:18.789: Adding Neighbor List Subelement
*apf80211vTask: Apr 12 10:47:18.789: Data Length of BSS Transition Request Frame: 22
*apf80211vTask: Apr 12 10:47:18.789: apf80211vHandleBSSTransQuery: lradMacAddr:
f0:7f:06:e8:32:70 rscb parent MAC ADDR: f0:7f:06:e8:32:70 rscb mac address: 00:00:00:00:00:00
*apf80211vTask: Apr 12 10:47:18.789: 11v Action Frame sent:
*apf80211vTask: Apr 12 10:47:18.790: 08:74:02:77:13:45 apf80211vSendPacketToMs: 802.11v Action
Frame sent successfully to wlc
```

*apf80211vTask: Apr 12 10:47:18.790: **Successfully sent BSS Transition Request Action Frame to STA: 08:74:02:77:13:45**

Le point d'accès envoie une trame de gestion de transition BSS en raison de l'itinérance optimisée

```
*apfMsConnTask_0: Nov 04 04:58:55.320: a4:f1:e8:58:95:0a Posting msg of type:
APF_80211v_MSG_BSS_TRANS_QUERY for STA and LRAD:7c:0e:ce:7d:d9:10,slot:0, len:0
*apfMsConnTask_0: Nov 04 04:58:55.320: 11v g_msgQueue = 0x2b415828,          osapiMessageSend
rc = 0
*apfMsConnTask_0: Nov 04 04:58:55.320: a4:f1:e8:58:95:0a 11v BSS Transition Request is posted to
11v queue.
*apf80211vTask: Nov 04 04:58:55.321: Session URL is not NULL
*apf80211vTask: Nov 04 04:58:55.321: Disassociation Imminent is 1
*apf80211vTask: Nov 04 04:58:55.321: Disassociation Timer is 40
*apf80211vTask: Nov 04 04:58:55.321: Building BSS Transition Request Frame
*apf80211vTask: Nov 04 04:58:55.321: Adding Neighbor List Subelement
*apf80211vTask: Nov 04 04:58:55.321: No Neighbor Candidate found :Resetting Candidate Included
List
*apf80211vTask: Nov 04 04:58:55.321: Data Length of BSS Transition Request Frame: 4
*apf80211vTask: Nov 04 04:58:55.321: apf80211vHandleBSSTransQuery: lradMacAddr:
7c:0e:ce:7d:d9:10 rscb parent MAC ADDR: 7c:0e:ce:7d:d9:10 rscb mac address: 00:00:00:00:00:00
*apf80211vTask: Nov 04 04:58:55.322: 11v Action Frame sent:
*apf80211vTask: Nov 04 04:58:55.322: a4:f1:e8:58:95:0a apf80211vSendPacketToMs: 802.11v Action
Frame sent successfully to wlc
*apf80211vTask: Nov 04 04:58:55.322: Successfully sent BSS Transition Request Action Frame to
STA: a4:f1:e8:58:95:0a
*apf80211vTask: Nov 04 04:58:55.322: a4:f1:e8:58:95:0a Setting Session Timeout to 4 sec -
starting session timer for the mobile
*apf80211vTask: Nov 04 04:58:55.322: a4:f1:e8:58:95:0a Disassociate client in 4 seconds
```

Références

[Chapitre : Itinérance de transition rapide 802.11r, 802.11k, 802.11v et 802.11w](#)

Norme IEEE pour les technologies de l'information — Télécommunications et échange d'informations entre les systèmes Réseaux locaux et métropolitains — Exigences spécifiques - Partie 11 : Contrôle d'accès moyen LAN sans fil
Spécifications (MAC) et PHY (Physical Layer)