

رادصإلا، (BSS) ةيساسألا تامدخلا ةعومجم LAN ةكبش يف مكحتلا ةدحو ىلع 802.11 AireOS ماظنل (WLC) ةيكلساللا

تايوتحمللا

[ةمدقمللا](#)

[ةيساسأ تامولعم](#)

[\(DMS\) هجومللا ددعتمللا ثبلا ةمدخ](#)

[BSS لومخ ةرتفل ىصقألا دحللا](#)

[BSS لاقتنا ةرادا](#)

[بلط](#)

[هيف بوغرملا ريغ لمحللا ديصر بلط](#)

[هيف بوغرملا ريغ نسحمللا لاوتجلا بلط](#)

[\(نرم يكلسال نييعت\) FRA لوصوللا ةطقن ىلا ليمعلا هيجوت](#)

[كيش و ككفت](#)

[BSS لاقتنا ةرادا ةباجتسا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[ةكبش لىطيطختلا مسرلا](#)

[تانويوكتلا](#)

[\(DMS\) هجومللا ددعتمللا ثبلا ةمدخ](#)

[BSS لومخلا ةرتفل ىصقألا دحللا ةرادا](#)

[BSS لاقتنا ةرادا](#)

[ةحصللا نم ققحتلا](#)

[SSID معد](#)

[ءالمعللا معد](#)

[ءاطخألا حيحصت ليمع طاشن](#)

[DMS تانوكماب دوزم ليمع](#)

[لليمعلل BSS لاقتنا ةينكما](#)

[ءجارملا](#)

ةمدقمللا

(مكحت زاغ lan يكلسال) WLC ىلع 802.11v لوكوتورب نم معدلا ةقيثو اذف فصيفي

ةيساسأ تامولعم

ءابرهكلا يسندنهم دهعم) IEEE ةيكلساللا ةكبشلا ةرادا ىلا 802.11v رايعم ريشي (8 ليدعتلا) 802.11 رايعملل اقفو (تايونورت كللالاو

عم تامولعمل لدا بت (ةيكللساللة كبشلة اراد) WNM معدت يتل تا طحمل اعيطتست م.هئادأ نيسحت لجا نم (نيكللساللة اعلمعلاو لوصول طاقن) ضعبل اهضعب

هذه WNM تامدخ يلعأ و 8.1 رادصل AireOS WLC معدي

- (DMS) هجومل ددعتمل ثبللة مدخ
- (ةيساساللة تامدخاللة وومجم) BSS ل لومخاللة ةرتفل يصولال دخاللة اراد
- BSS لاقتناللة اراد

(DMS): هجومل ددعتمل ثبللة مدخ

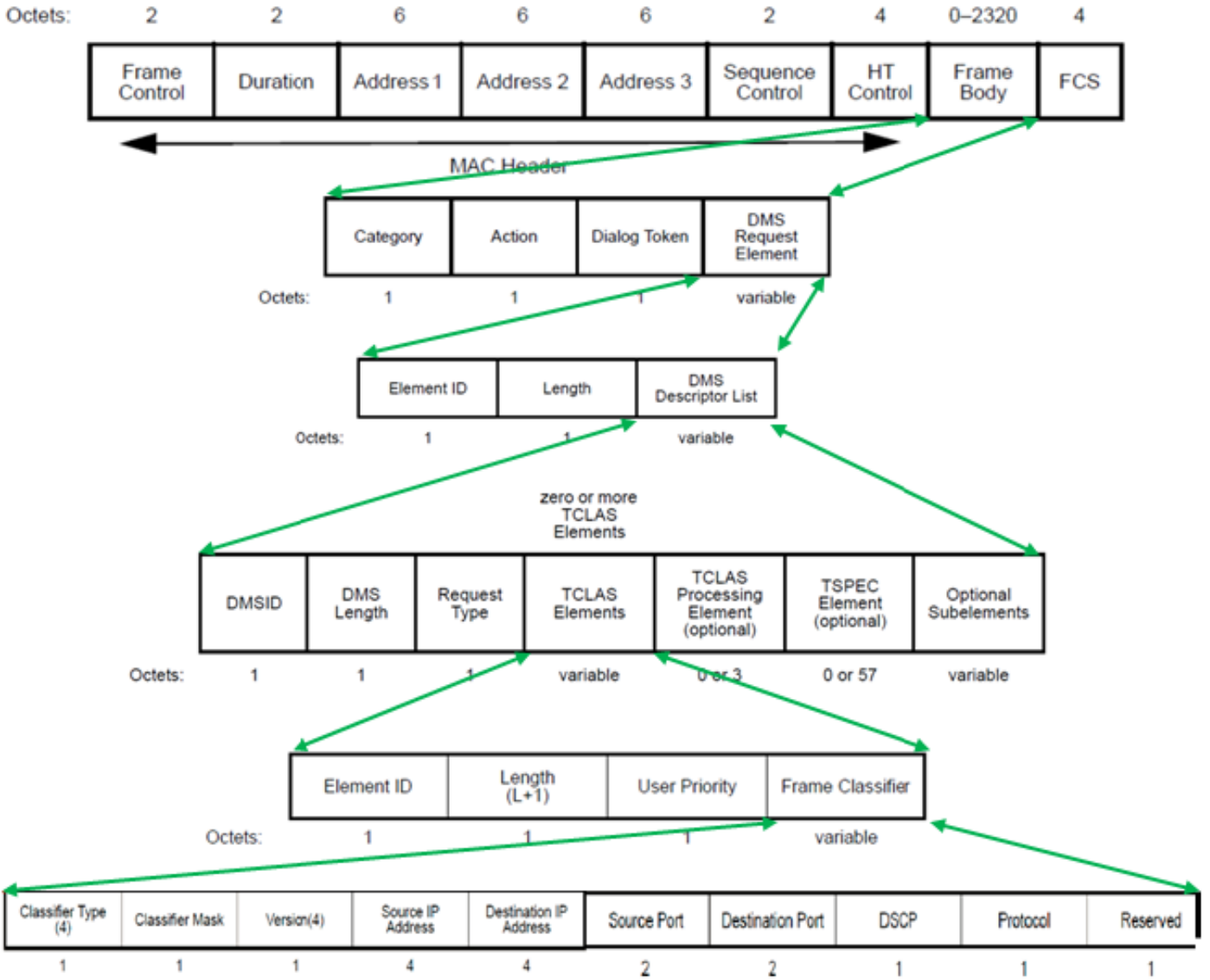
ددعتم قفد لاسرال (AP) لوصوللة طقن يلا اوبلطي نأ DMS نومعدي نيذلال اعلمعلل نكمي ةيكللمانيذ طئاسو قفدت ةفيظو لثم ،يداحأ ثبك ثبلل

طئاسولا قفدتل تامولعملال نم ديزمل [VideoStream رشن ليلا](#)

ثبلل رورم ةكرح يقلتل DTIM لصالل كهيبنت ليمعلا يلع بجي ،DMS مادختسإ نودب ،نيعم ليمعل ددعتملال ثبلل رورم ةكرح (Access Point) لوصوللة طقن نخت ،DMS عم .ددعتملال وهف .هذه رورملا ةكرح بلطل يداخالل ثبلل ارادللسرت اهناف ،هيبنتلاب ليمعلا موقمي امذنع ددعتملال ثبلل تارادللسرا متي .ةيراطبللة قاط رفويو لوطأ ةدمل مونلاب ليمعلا لجمسي م ادختسإ م تيس ناكل يذلال لدعملال نم يلعأ تانايب لدعبل اهلاسررا متي ،اوهال ربع يداخالل ثبك DMS نودب هيف

لوصوللة طقن ةبللامل "DMS بلط عون ةفاضإ" رادللسرال نيكللساللة اعلمعلل نكمي يداخالل كشب ةددحملال ددعتملال ثبلل تاقفدت نم رثكأ وادحاو قفدت تانايب رورم ةكرح لاسراب

DMS بلط عون - ةراداللا رادل



DMS: بلط نم عاوناً ةثالث كانه

بلطال عون ةميقي فصولا

ةفاضل	0
ةلازل	1
رپيغت	2
يظفتم	3-255

DMS فصولا ةفاضل-بلط نم مضتي

يذلا ددتم لث بل رورم ةكرح قفدت ددحي يذلا، TCLAS رصنع دجوي، DMS فصولا ةمئاق لخد ةهوجل/ردصم لل IP ناونع TCLAS ددحي. يذاح ثبكه لعل لوصحلل يكل لسلاللا ليمعلا هبلطي يرخا لوقح بناج يلا ةهوجل/ردصم ل ذفنم.

عباتتو يكل لسلاللا ليمعلا يلا يذاح ثبكه هذه رورم ل ةكرح تاقفدت لوصولا ةطقن لسرت DMS مدي ال ةكبلشال يفرخا ليمعلا يلا ددتم ثبكه تاقفدت لال كلت لاسرا اضيا.

ليمعلا ل نكمي شيح، (يراي تخا) TSPEC رصنع كانه نوكي نا نكمي، DMS بلط راطا لخد رورم ل ةكرح قفدت لاهصئاصخو ةمدخل ةدوج تابلطتم ديدحت يكل لسلاللا.

TSPEC معد متي ال: ةظالم

بطل 23: ءارجإلإا زمر ،WNM: 10 ةئفلا زمر ،ةرادإلا راطا) DMS بطل ليمعلا لسرا ،لاثلما اذف ذفنم ،(17 لوكوتوربال) UDP ،224.0.0.251 ةومجملا يف IPv4 ددعتملا ثبال قفدتل ،DMS (لمالكلا بطل ريفشت كف wireshark ل نكمي ال دنتمسلا اذف يف) 9 ةهوللا

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.

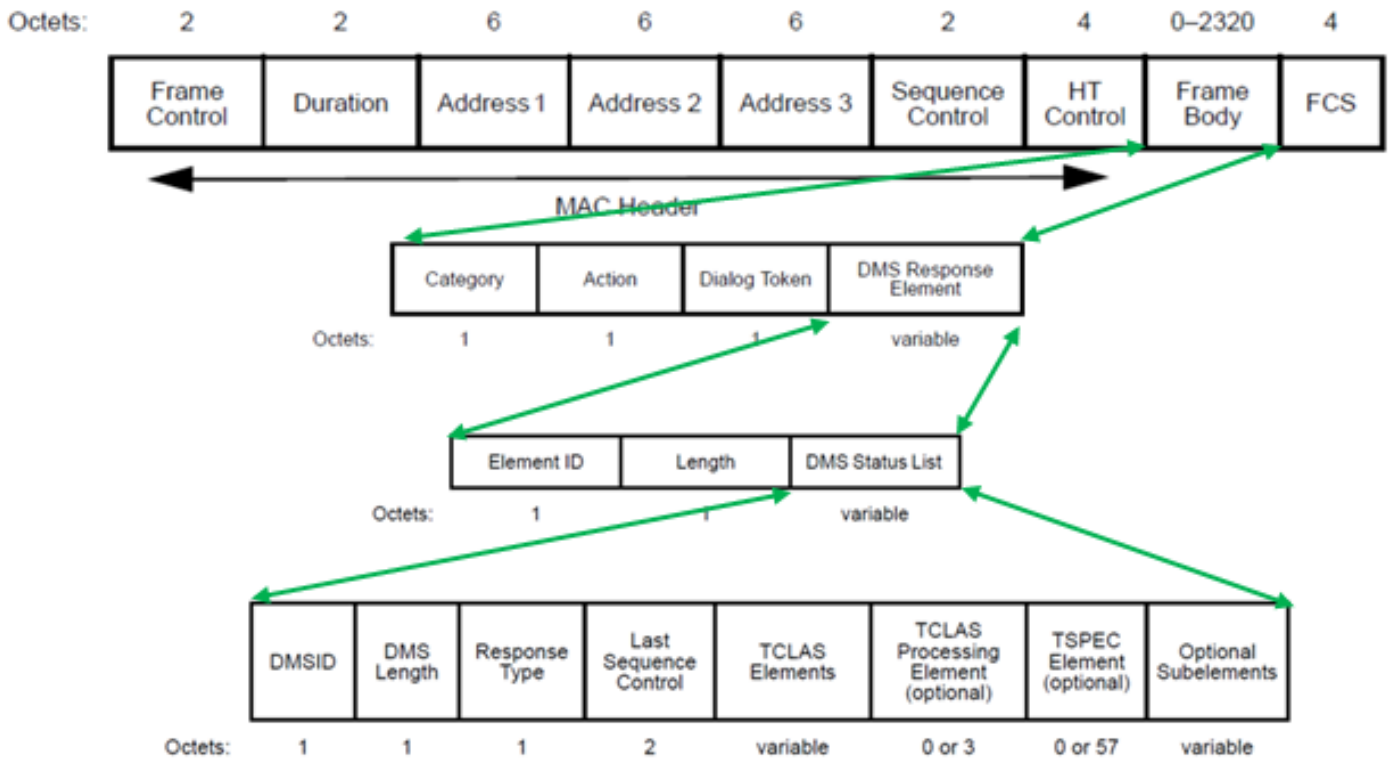
نأ نكمي يتلاو ،DMS ةباجتسا مادختساب DMS بطل يلع ةباجلاب لوصولا ةطقن موقت DMS. ضفر-ةباجتسا وأ DMS لوبق-ةباجتسا نوكت

DMSID نبيعتب اضيا موقت اهناف ،DMS response-Accept لسرت لوصولا ةطقن تناك اذا اذف لاصلتالا قفدتل

دوجوم DMSID لي دعتل يكلساللا ليمعلا ةطساوب DMS بلط عون ريغت مادختسا نكمي رورملا ةكرح قفدتل فلتخم TSPEC بلطل لاثملا لابس عل

موعدم ريغ DMS ريغت :ةظحالم

DMS ةباجتسا عون - ةرادلا راطا



DMS ةباجتسا نم عاوناً ةثالث كانه

فصولا لقحلا ةميق

- 0 لوبق
- 1 نركنأ
- 2 ءاهنإ
- 3-255 يظفتم

فرعم نييعتب تماق امك DMS Response-Accept لاسراب لوصولا ةطقن تماق ،لاثملا اذه يف ليمعلا ةطساوب هلاسرإ مت يذلا DMS بلطل 1 مقر DMS

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+..

إلى اهلا سراً متي، 9 ذفنملا إلى 224.0.0.251 هجولا عومجم عم مزح كانه تناك اذا لك ذعب
 يذلا ليمعلا حبصي يتح لوصولاً عطقن إلى اضيأ اتقوم اهنيزخت متي ودعتم شبك عاول
 يداحأ شبك اهلابقتسال اجاتم عطقني علاحي في DMS بلط لسراً

نأ ظحال multicast يداعك لسري 9 عانيم إلى 224.0.0.251 عومجم نأ عيأ طبر نم لاثم اذه
 ددعتملا شبكلا عومجم إلى ريشي هجولا ولبقتسملاب صاخلا MAC ناونع

```

+ Radiotap Header v0, Length 18
+ 802.11 radio information
- IEEE 802.11 Data, Flags: .....F.C
  Type/Subtype: Data (0x0020)
+ Frame Control Field: 0x0802
  .... 0000 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]

```

هذه الصورة تظهر تفاصيل حزمة شبكة. الحزمة هي من نوع IEEE 802.11 Data، وتحتوي على حقل تحكم إطار (Frame Control Field) وبيانات بروتوكول الإنترنت (Internet Protocol Version 4) وبيانات بروتوكول المستخدم (User Datagram Protocol).

المتلقي (Receiver address) والوجهة (Destination address) هما نفس العنونة: IPv4mcast_fb (01:00:5e:00:00:fb). المرسل (Transmitter address) هو CiscoInc_7d:d9:10 (7c:0e:ce:7d:d9:10). المصدر (Source address) هو IntelCor_7c:30:58 (e4:b3:18:7c:30:58).

البيانات هي من نوع Internet Protocol Version 4، مع عنوان المصدر (Src) 172.16.0.51 وعنوان الوجهة (Dst) 224.0.0.251. البروتوكول المستخدم (User Datagram Protocol) له رقم منفذ المصدر (Src Port) 59887 ورقم منفذ الوجهة (Dst Port) 9.

الحزمة لها طول (Length) 110 بايت، وحقول التحقق من صحة (Checksum) غير مؤكدة (unverified).

```
⊕ 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]
```

لاسرا هنكمي، يداحاً شبك ددعتم لال شبلل قفدي قلت نع يكلسالال ليمع ال فقوت درجم ب
لبق نم هنييعت مت يذال DMS فرعم مدختسي هناف، قفدتال اذه قالغال ديچ DMS بلط
(1) عون ةلازا - DMS بلط هناف لوصول ةطقن ةطساوب

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
  
```

DMS (2) ةباجتسا عون ءانإ عم ءانإلا اذه لوصولا ةطقن دكؤتو

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

BSS لومخ ڦرتفل ىصقأال دحل

هنا، نقولنا نم ڦنڦم ڦرتفل ىكلسال لڦم نم تاراطا لوصولا ڦطقن لڦقتسڦ ال امدنع تقولا رادقم The BSS Max Idle Period ب دصقڦ اهلصڦو ڦكبشال كرت لڦمعلنا نأ ضررتڦي راطا ڦا ڦقلت ىل اءءال نود نرتقملا لڦمعلاب ظافءال هڦ لوصولا ڦطقنل نكمڦ ڦذلا نم ڦمڦقلا هذب ىكلسال لڦمعلال مالءم تڦ (نوكسال عضو ڦى قڦڦ نأ لڦمعلل نكمڦ) تقول نڦمئان اءاب ال مءلل حمسڦ اذو. نارتقالا ڦءاعا نارتقالا ڦءاءتسا راطا لالء ڦر راطابلا ڦقاط رڦفوتو لوطأ.

نارتقالا ڦءاعا و نارتقالا ڦءاءتسا تاراطا ڦى طقف BSS Max لومخ ڦرتف رهظت

```

+ 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

```

يُراح دحو و 1000 غلبت يتال تادحول في BSS لومخ ةرتفل يصقألا دحل ديحت متي ةينات يللم 1.024 يواست ةينمز ةدحو لك. (ةينمزلا تادحول) (TU) ةيناطيرب

$$\text{ةينات } x = \text{لومخلا ةرتفل يصقألا دحل BSS} \times 1.024 = \text{لومخلا ةلهم}$$

لثمل راطا في

$$\text{ةينات } 414.72 = 1.024 \times 405 = \text{لومخلا ةلهم}$$

بجي هنأ ينعي اذهف، 1 يلل ةيمحمل "ةبولطملا ةايحلا يلل ةظفاحملا" تب ةدحو نييحت مت اذا تقؤملا طبض ةداعإل لوصول ةطقن يلل RSN ب يمحمل راطا لاسرا يكلساللا ليمعلا يلل نم عون ي لاسرا يكلساللا ليمعلا نكمي، لثملا اذه لثم 0 يلل هطبض ةلاح في. لمخال لوصول ةطقن في لمخال تقؤملا طبض ةداعإل (ةيمحمل ريغ وأ ةيمحمل) تاراطال

BSS لاقتنا ةراد

عيطتسي. ليمعلا يلل اهجوم اجاتقا 802.11v راي عمل اقفو BSS لاقتنا ةراد بلط دعي في ليمع نارقتا ءاغلا لضر نكمي. ال ما جارتقالا عابتاب ءاوس صاخلا هراق ذاختا ليمعلا دعي مل اذا تقولا نم ةرتف دعب ليمعلا نع لصفيو. ءاغلال ةكيشو ةفيظو نيكت ةلاح ةحرتقمل لوصول طاقن دحأب نارقتقالا ليمعلا

ة: ب رال تاهوي رانيسلا هذه يلل BSS 802. 11v راي عمل اقفو لاقتنا ةلهم عقي ببط متي

بلط

رايخ لجا نم هلاوجت لبق BSS 802.11v لاقتنا ةراد مالعتسا يكلساللا ليمعلا لسري اهب نارقتقالا ةداعإل لوصول طاقنل لصفأ

BSS 802.11v لاقتنا ةراد مالعتسا يلل لثم

```

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 00001110 00001110 00010001 00110001 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 00001110 00001110 00010001 00110001 10001001 .....1.
0030 01110101 01001111 u0

```

ةحشرم ال AP ةمئاق ل ليمع ال بلط ببس وهو ،BSS ل اقاتنا مالعتسا ببس QReason ينعى
 دلع لوصحلل .ةضفخنم ال RSSI عم قفاوتي وهو ،16 اببس ليمع ال لسرا ،لاثم ال اذه يف
 IEEE 802.11-2012 نم 8-138 لودجل عجار يلاققان ال مالعتسال اببسا ةلماك ةمئاق

ةمئاق ريفوتل BSS ل اقاتنا ةرادا بلط عم ببس يمتسي ،راطال اذه وي دارل لبقتسي نأ دعب
 AP يحشرم

```

1098 2.522295 CiscoInc 7d:d9:... CiscoInc 3a:0t: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...

```

هيف بوغرم ال ريغ لمحلل ديصر بلط

م لوصولا ةطقن نإف ،BSS ل اقاتنا نيكتم + لامحال ةنزاوم ةزيم ل ع WLC يوتحي ام دنع

اهنإف ،ريبك لكش ب ةلمحم نوكي امدنع يكلسال ليمع ىلإ ةقداصم ءاغلإ راطلإ لسرت دعت
لليمحت لقا ىرخأ لوصو ةطقن يكلسال ليمع حارتقا لجأ نم BSS لاقنتنا ةرادا بلط لسرت

[ةيوقلا لامحالآ ةنزاوم نيوكت](#) :لامحالآ ةنزاوم ةزيم لوح تامولعمل نم ديزم

هيف بوغرملا ريغ نسحملا لواجتلا بلط

نيسحتب ماق دق (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع نوكي امدنع
ءاغلإ راطلإ لسرت دعت مل لوصول ةطقن نإف ،BSS لوكتورب ربع لاقنتنالا نيكمت + لواجتلا
يا وأ) RSSI لوكتورب نم ىندالآ دحلاب ليمعلا يف ال امدنع يكلسال ليمع ىلإ ةقداصم
ةطقن حارتقا لجأ نم BSS لاقنتنا ةرادا لسرت اهنإف ،(نسحملا لواجتلاب ةطبرت رم ىرخأ ةملمع
يكلساللا ليمعلا لصف لوصول.

[نسحملا لواجتلا Cisco](#) :نسحملا لواجتلا ةزيم لوح تامولعمل نم ديزم

(نرم يكلسال نييعت) FRA لوصول ةطقن ىلإ ليمعلا هيحوت

ةرادا بلط لوصول ةطقن لسرت ،FRA لوصول ةطقن لخاد ةيلاثم لقا ةيلخب ليمع لصتا اذا
لليمعلا اذه ىلإ BSS 802.11v لاقنتنا

زتره ايج 5 (3800 وأ 2800 لثم) ءارمحل تحت ةعشالآ معدت يتلا لوصول طاقن مدختست امدنع
ةيلخلاب لصتيا ءالمعلا دحأ ناك اذا .(ةريبك ىرخأ ةقيد ةيلخ) ناتيلخ كانه ،طقف
بلط لوصول ةطقن لسرتف ،(RSSI ىلإ ادانتسا) لصفالآ يه ةقيد ةيلخ نكلو ةريبكلا
ححص سكة لاول ةقيدلا ةيلخلا لقن حارتقال ليمعلا ىلإ BSS 802.11v لاقنتنا ةرادا

8.2.110.0 رادصإلا ذنم ةزيملا هذه رفوت

[تالاصتالآ او \(FRA\) ةنرملا ةيكلساللا تالاصتالآ](#) :FRA ةينقت لوح تامولعمل نم ديزم
[ةنرملا ةيكلساللا](#)

كيشو ككفت

ةفيظولا هذه نم ضرغلأ .كيشو نارتقا ءاغلإ لقح ةفاضلآ نكمي ،BSS لاقنتنا ةرادا بلط يف
ةطقن نارتقالا ءداعب ليمعلا مقوي مل اذا تقولا نم ةرتف دعب ليمعلا نارتقا ءاغلإ وه
ىرخأ لوصول.

بلط لوصول ةطقن لسرت ،هيف بوغرملا ريغ نسحملا لواجتلا بلط ليغشت متي امدنع
نارتقا ءاغلإ" تقوم نمض نوكملا تقولا) ةنيعم ةرتف رطنتو ليمعلا ىلإ BSS لاقنتنا ةرادا
ةرتفلا كلت لالخال لوصول ةطقن ىلإ لواجتلاب ليمعلا مقوي مل اذا ،("نسحملا لواجتلا
لليمعلا نارتقا ءاغلإ لوصول ةطقن لمكت مث ،ةينمزالا

لاقنتنا ةرادا بلط لوصول ةطقن لسرت ،"هيف بوغرملا ريغ لمحل ديصر" بلط ليغشت دنع
("نارتقالا ءاغلإ" تقوم تحت هنيوكت مت يذلا تقولا) ةنيعم ةرتف رطنتو ليمعلا ىلإ BSS
مث ،ةينمزالا ةرتفلا كلت لالخال امادزا لقا لوصول ةطقن ىلإ لواجتلاب ليمعلا مقوي مل اذا
لليمعلا نارتقا ءاغلإ لوصول ةطقن لمكت

كيشولا نارتقالا ءاغلإ نيكمت عم BSS لاقنتنا ةرادا راطلإ ىلع لاثم

```

+ 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...

```

BSS لاقتننا ةرادا ةباجتسا

ةرادا ةباجتسا لاسرا نكمي ال وا نكمي BSS لاقتننا ةرادا بلط Wireless Clean يقلت دعب ةلاجال زمر عم اهلسري هناف رخا لوصو ةطقن لى ل لاقتننا اب ليمع ال ما اق اذا BSS لاقتننا اهلسري هناف بابسا ةدعل اهسفن لوصولا ةطقن لى لع اءاق بلط ططخي ناك اذا نكلو، "لوبق" ضم فرلا ببس لى ل ةفاض ال اب "ةلاجال زمر ضم فر" عم

BSS لاقتننا ةرادا ةباجتسا راطا لى لع لاثم

```

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

```

ةطقن لى ل لوجت ي الو لوصولا ةطقن حشرم ةمئاق يكلسال ال ليمع ال ضم فر لاثم الا اذ ي ةلماك ةمئاق لى لع لوصول ل ESS ل ليمع ال كرت ببس 1 ةلاجال زمر حضوي. ةفلتخم لوصو IEEE 802.11-2012 نم 8-253 لودجال عجار ةلاجال زمر تافيرعتب

ةيساس ال اءابلطتم

ءابلطتم

ءالمع رفوت مزلي، 802.11v ةردق ب (WLAN) ةيكلسال ةيلحم ةكبش تانك م نم ةءافتسال ال 802.11v راي عم نوم عدي نيكلسال

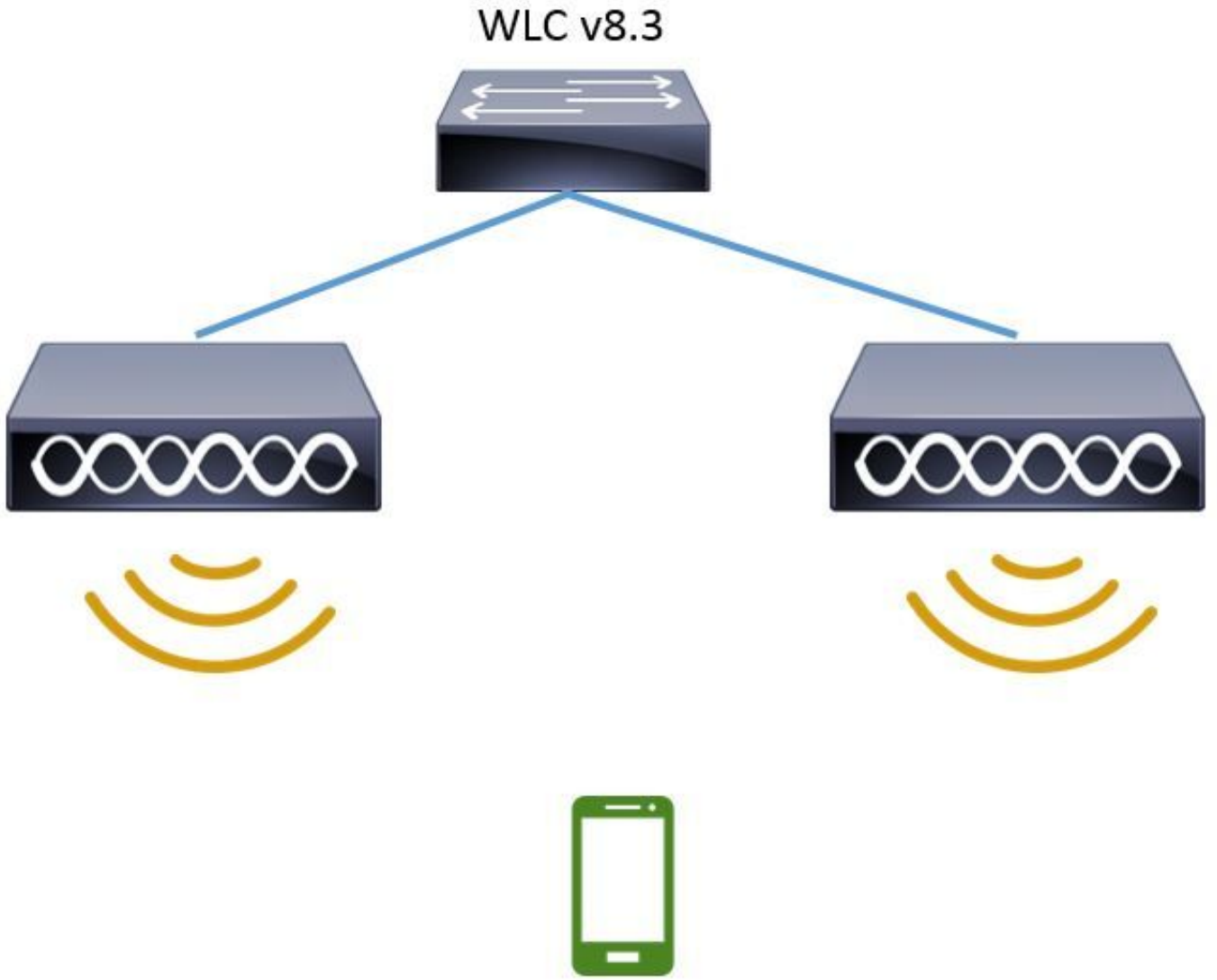
ةمدختسم ال تانوكم

WLC v8.3

10.1.1 رادص ال نم سءاسال ليجل ال Ipod Touch

نيوكتل

ةكبش ل ل يطي طخت ل ا مسر ل ا



ت ا ني و ك ت ل ا

ه ج و م ل ا د د ع ت م ل ا ث ب ل ا ة م د خ (DMS)

DMS ن ي ك م ت ل WLAN ة ك ب ش ر ب ع ن ي و ك ت ل ا

ر م ا و ا ل ا ر ط س ة ه ج ا و ن ي و ك ت

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

8.3 ر ا د ص ا ل ا ن م ر ف و ت م (GUI) ة ي م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ن ي و ك ت

DMS ن ي ك م ت ل WLAN ة ك ب ش ي ل ع ر ق ن ا و WLAN-ID > WLAN ت ا ك ب ش ي ل ا ل ق ت ن ا 1. ة و ط خ ل ا

هجوم ال ددتم ال ثب ال ةمدخ ني كم وتو BSS 11v ل اقاتنا معد > م دقتم ي ل ل قتنا 2. ةوطخل

WLANs > Edit '11v'

BSS ل لومخل ةرتفل ي صقألا دحل ةراد

ةرتفل ي صقألا دحل ةراد ل ني كم تل (WLAN) ةي كل ل س ال ال ةي ل حم ال ةكبش ال ربع ني وكت ال BSS لومخ:

رم أو ال رطس ةه جاو ني وكت:

```
> 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

ةيوسررلا مدختسمللا ةهجاو نيوك:

ةرتف نييعتل WLAN ةكبش ىلع رقناو WLAN-ID > WLAN تاكبش ىلإ لقتنا 1. ةوطخلا BSS Max لومخ

WLAN ID	Type	Profile Name
6	WLAN	phone-open
7	WLAN	11v

BSS ةمدخ نيكمتو تلوو 11 ةردقب BSS لاقنتنا معد > ةمدقتم تاراخي ىلإ لقتنا 2. ةوطخلا BSS Max Idle.

WLANs > Edit '11v'

General Security QoS Policy-Mapping Advanced

HexConnect Local Switching Enabled

FlexConnect Local Auth Enabled

Learn Client IP Address Enabled

Vlan 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

HTTP Profiling

Universal AP Admin Support

Universal AP Admin

11v BSS Transition Support

BSS Transition

Disassociation Imminent

Disassociation Timer(0 to 3000 TBTT) 200

Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40

BSS Max Idle Service

Directed Multicast Service

mDNS

mDNS Snooping Enabled

mDNS Profile default-mdns-profile

ةبسنلاب 8.3 رادصلإا يف هذه ةيوسررلا مدختسمللا ةهجاو تاراخي ميديقت متي: **ةظحالم**
`config wlan bssmaxidle enable <wlan-id>` رمال مدختسا، ةقباسللا تاراوصلإا

ةميقي نييعتب مقوليمعمال مدختسمللا ةلماخ ةلهم > ةمدقتم تاراخي ىلإ لقتنا 3. ةوطخلا ناوٲ يف ةلهملا


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

ةيوسررلا مدختسمللا ةهجاو نيوكت:

BSS. لاقتنا نكمي و مدقتم > WLAN ةكبش فرعم > WLAN تاكبش للاقنا 1. ةوطخل

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 5	<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"/>
				BSS Max Idle Service <input checked="" type="checkbox"/>
				Directed Multicast Service <input checked="" type="checkbox"/>
11k				mDNS
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		mDNS Snooping <input checked="" type="checkbox"/> Enabled
Neighbor List	<input checked="" type="checkbox"/>	Enabled		mDNS Profile <input type="text" value="default-mdns-profile"/>
Neighbor List Dual Band	<input type="checkbox"/>	Enabled		
Denial Maximum Count	<input type="text" value="2"/>			
Prediction Minimum Count	<input type="text" value="2"/>			

هيف بوغرمللا ريغ لمحللا ديصرر بلط

رم اوألا رطس ةهجاو نيوكت:

```
> 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>
```

ةيوسررلا مدختسمللا ةهجاو نيوكت:

لاقنا > (WLAN) ةيكلساللا ةيحلللا ةكبش فرعم > WLAN تاكبش للاقنا 1. ةوطخل
امهنم نكمي و مدقتم لمعمللا لمح ةنزاومو BSS.

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		None		Management Frame Protection (MFP)
URL ACL		None		MFP Client Protection 2 <input type="text" value="Optional"/>
P2P Blocking Action		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		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"/>

هفي بوفورملا ريغ نسحملا لاوجتلا بلط

رم اوألا رطس ةهجاو نيوكت

```
> 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
```

ةموسرلا مدختسملا ةهجاو نيوكت

لاقنا > (WLAN) ةيكللساللا ةيحلحملا ةكبشلا فرعم > WLAN تاكبش يلى لقتنا 1. ةوطخلا
هنكمتو مدقتملا ةيطغتلا ءحتف فاشتك او BSS

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"/>			

لاوجت الة عضو الة نكم و نسمح الة لاوجت الة > مدقتم > يكلس الة لاصت الة 2. ةوطخ الة دن تسمل الة اذ ة ءار ة نسمح الة لاوجت الة تام لعم لوح تام ولعمل الة نم ديزمل. قاطن لل نسمح الة 8.0 رادص الة، (HDX) ة لالاع الة ة فاثل الة ة برجت رشن ل ل ل د

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

كيش و ككفت

رم او ال رطس ةه جاو ني وكت

```
> 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>
```

> (WLAN) ةي كل لس ال ال ةي ل حمل ال ةك ب ش ال فرعم > WLAN تاك ب ش ال ل لقتنا 1. ةوطخ ال
 اغل ل تقوم و نارتيق ال اغل ل تقوم ني عو كيش و ال نارتيق ال اغل ل BSS ل اقتنا نك م، مدقت م
 ن س حمل ل وحت م ال نارتيق ال

ةي م و س ر ل م دخت س م ال ةه جاو ني وكت

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"/>
				BSS Max Idle Service <input checked="" type="checkbox"/>
				Directed Multicast Service <input checked="" type="checkbox"/>
11k				mDNS
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		mDNS Snooping <input checked="" type="checkbox"/> Enabled
Neighbor List	<input checked="" type="checkbox"/>	Enabled		mDNS Profile <input type="text" value="default-mdns-profile"/>
Neighbor List Dual Band	<input type="checkbox"/>	Enabled		
Denial Maximum Count	<input type="text" value="2"/>			
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"/>
				BSS Max Idle Service <input checked="" type="checkbox"/>
				Directed Multicast Service <input checked="" type="checkbox"/>
11k				mDNS
Assisted Roaming Prediction Optimization	<input type="checkbox"/>	Enabled		

وهو، (فدهال هبنتلا لاسرا تقو) TBTT تادحو يف تي قوتلا تادحو ديدحت متي: **ةظحال** 100 لك ةرانم لك لاسرا متي يضارتفا لكشب. ةرانم لك نيبي نيمزلا لصال تقو = X تي قوتلا تادحو. ةي ناث يللم 1 tbtt = 100 يضارتفا لكشب كلذل، ةي ناث يللم $TBTT/10 = x$ ةي ناث.

ةحصلال نم ققحتلا

(ةي كل لصال ةي لصل ةكبشلا) ةي كل لصال ةي لصل ةكبشلا معد روصلا هذه رهظت. ةفل تخلم 802.11v تامدخل نيي كل لصال ةالمعلاو.

معد 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)

```

• BSS لاقتنا قراد


```
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)
```

عالم عمل معد

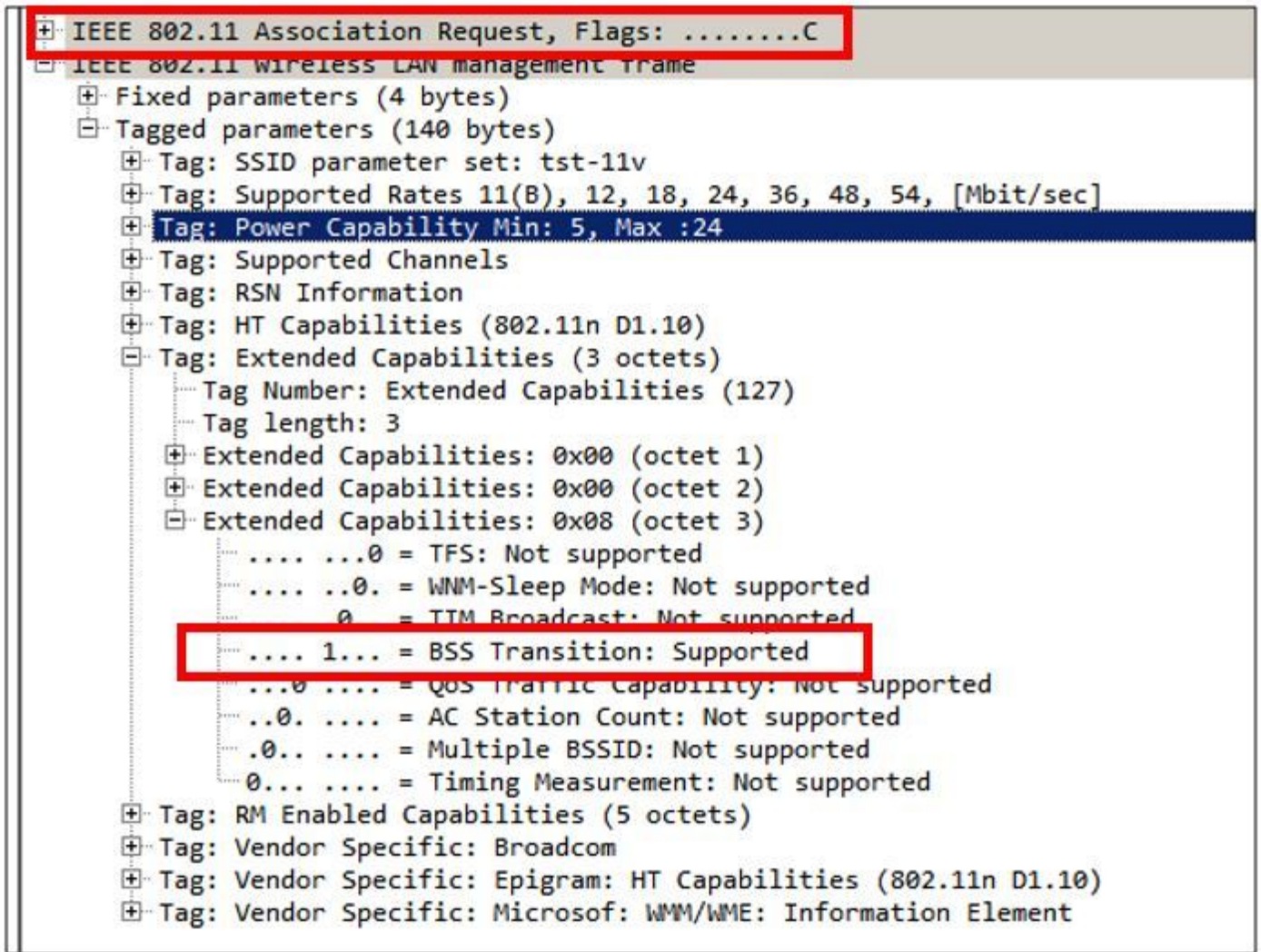
- DMS

```

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

```

• BSS لاقتنا قراداً



ءاطخألا حيصت ليمع طاشن

رمأوالا هذه رفوت 11v ليمع طاشن ةبقارمل

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

DMS تانالكما ب دوزم ليمع

تلوف 11 دهج لمعلال لىل رداق ليمعلال

```
*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
لوبق لوصولا ةطقن لسريو 9 ءانيم 224.0.0.251 udp ةومجملل DMS بلط ليمعلال لسري
DMS
```

```
*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 lrادمac7c: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 lrادمac 7c:0e:ce:7d:d9:10

```

الصتم ليمعال نوكي ثيح لوصول اطقن نم

```
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

```

ةيكلسلاللة لىلحمال ةكبشلال لىل ع DMS تانايب ةدعاق لىل لىمعال ةفاضا متت ،كلذ دعب ةلسلس سفنل DMS ةفاضا-بلط لاسراب نوموقى نىذلء المعال عىمى درس متى (WLAN). هسفن DMS فرعم نمض ددعتمللا ثبلا

```
> 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

```

الصتم ليمعال اذه نوكي ثيح لوصول اطقن فى DMS تانايب ةدعاق نىزخت متى

```
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},

DMS ةلازا بلط لسري هنإف ، DMS قفدت قالغاب يكلساللا ليمعلا موقى نأ درجم

```
*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
```

سرب دتيشوسأل نم

```
*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
```

ليمعلا BSS لاقتنا ةينكام

تلوف 11 دهج لمعلا لىل رداق ليمعلا

```
*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
```

BSS لاقتنا ةرادا لمعلا لسري

```
*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
```

عطق متي، الكيشو "طاب ترالال ك ف" تنك دق (WLAN) ةي كلسال ال ةي لحلم ال ةكبش لل نأل ارظن
"طاب ترالال ك ف" تقؤم ءاهتنا دعب لي عم لل لاصتا

```
*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
```

لامحال ةنزاوم ببسب BSS لاقتنا ةراد راطل AP لسري

```
*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
```


ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا