Return-Path: <tom.siep@ieee.org>
Received: from sj-iport-2.cisco.com (sj-iport-2-in.cisco.com [171.71.176.71])
by fruitpie.cisco.com (Mirapoint Messaging Server MOS 3.3.6-GR)
with ESMTP id AYL12109;
Wed, 14 Apr 2004 13:32:37 -0700 (PDT)
Received: from sj-core-5.cisco.com (171.71.177.238)
by sj-iport-2.cisco.com with ESMTP; 14 Apr 2004 12:41:49 +0000
Received: from sj-inbound-3.cisco.com (sj-inbound-3.cisco.com [128.107.250.144])
by sj-core-5.cisco.com (8.12.10/8.12.6) with ESMTP id i3EKWY2O005198
for <dhala@sj-core.cisco.com>; Wed, 14 Apr 2004 13:32:34 -0700 (PDT)
Received: from sccrmhc13.comcast.net (sccrmhc13.comcast.net [204.127.202.64])
by sj-inbound-3.cisco.com (8.12.10/8.11.2) with ESMTP id i3EKWpHB020160
for <dhala@cisco.com>; Wed, 14 Apr 2004 13:32:53 -0700 (PDT)
Received: from tms001 (c-24-1-206-221.client.comcast.net[24.1.206.221])
by comcast.net (sccrmhc13) with SMTP
id <20040414203217016003okkbe>; Wed, 14 Apr 2004 20:32:17 +0000
Reply-To: <tom.siep@ieee.org>
From: "Tom Siep" <tom.siep@ieee.org>
To: "'David Halasz'" <dhala@cisco.com>
Cc: <a.ickowicz@ieee.org>, "'stuart Kerry'" <stuart.kerry@philips.com>
Subject: RE: TGi comments
Date: Wed, 14 Apr 2004 15:32:12 -0500
Organization: TMS Consulting
Message-ID: <006601c4225f$91d3c970$6c00a8c0@TMS001>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0067_01C42235.A8FDC170"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.4510
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Importance: Normal
In-Reply-To: <4.3.2.7.2.20040414105239.026728c8@unitas.cisco.com>
X-from-outside-Cisco-experimental-header: 128.107.250.144
X-PMX-Version: 4.5.0.92886

Dave,

Based on our conversations and the email thread below, I hereby change my vote from no to yes, with

comments .

My first two technical comments are withdrawn, and the other comments should be considered editorial.

- Tom

-----Original Message-----
From: David Halasz [mailto:dhala@cisco.com]
Sent: Wednesday, April 14, 2004 9:58 AM
To: tom.siep@ieee.org
Subject: RE: TGi comments

What is the mechanism for the constraint on the MLME-SCAN.request ?
Clause 6 is an abstract interface. It is not normative and does not affect interoperability of implementations. The parameter is available and is used to fill a particular field in a transmitted frame, whose format is described in clause 7. Because the text is not normative, the value of the BSSID when sending a Probe Request to a single STA in an IBSS can contain a universally administered MAC address. It may be unconventional. But it is not prevented by the standard. Based on this, the comment is out of scope.
Stated another way, put the destination MAC address in the BSSID parameter.

What is the effect of potentially having identical BSSIDs on security?
The usage of a probe request/response remains the same as the base standard (802.11-1999). The probe request/response is used for discovery. Authentication of identity is done via 802.1X or pre-shared key. This is validated by the 4 way handshake.

Dave H.

At 09:48 AM 4/14/2004, Tom Siep wrote:

Hi David,

Your administrative points are well taken.

Did you have an answer to my technical question?

What is the mechanism for the constraint on the MLME-SCAN.request and what is the effect of potentially having identical BSSIDs on security?

- Tom

-----Original Message-----
From: David Halasz [mailto:dhala@cisco.com]
Sent: Wednesday, April 14, 2004 12:01 AM
To: tom.siep@ieee.org
Subject: RE: TGi comments

Hi Tom,

The second comment was discussed in TGi to a large extent. But with your first comment, I asked some people in TGi before responding. TGi meets on April 20 and 21. I would like to discuss your comment during April 20 and 21. Also, would you have a chance to discuss your comment this week? My cell # is 330-283-2715.

Some comments I have received so far are,
1) Text concerning comment 1, did not change in draft 9.
2) Clause 6 is an abstract interface. It is not normative and does not affect interoperability of implementations. The parameter is available and is used to fill a particular field in a transmitted frame, whose format is described in clause 7. Because the text is not normative, the value of the BSSID when sending a Probe Request to a single STA in an IBSS can contain a universally administered MAC address. It may be unconventional. But it is not prevented by the standard. Based on this, the comment is out of scope.

Dave H.

At 10:58 PM 4/10/2004, Tom Siep wrote:

Hi Dave,

We agree on the second comment: I accept that there is a placeholder for TGe and it befalls to that draft to afford compatibility with what is by then already in place. Consider that comment satisfied.

I am not sure you understand the point of the first comment. Yes it is permissible to have a specific MAC address in the BSSID, but as I read the security requirements there must be a constraint to do so to make this work. What is the mechanism for the constraint on the MLME-SCAN.request and what is the effect of potentially having identical BSSIDs on security?

- Tom

-----Original Message-----
From: David Halasz [mailto:dhala@cisco.com]
Sent: Saturday, April 10, 2004 5:38 PM
To: tomsiep@hotmail.com; tom.siep@ieee.org
Subject: TGi comments

Hi Tom,

The following is in regards to your first couple SB comment on TGi. I copied the first below. I copied sections from the base standard in Clause 10.3.2.1.2 of the MLME-SCAN.request. As you can see, the scan request already does allow for specifying an individual MAC address.

In regards to the second comment, TGi did discuss the interdependency with TGe. On earlier drafts, there was text for TGe. As we discussed, TGi is looking to go to REVCOM in June. So, we removed the text and made a placeholder for text needed. Hence you see a reserved field. The earliest that TGe can go to REVCOM is September. So, there is no reason that TGe cannot take the text removed from TGi and place it into 802.11e. This is the expected and desired events. While we don't want to let things fall

through the cracks, we also don't want to prevent progress from moving forward.

Dave H.

******** Fronm 802.11-1999 base standard **********
Clause 10.3.2.1.2
10.3.2.1.2 Semantics of the service primitive
The primitive parameters are as follows:
MLME-SCAN.request(
BSSType,
BSSID,
SSID,
ScanType,
ProbeDelay,
ChannelList,
MinChannelTime,
MaxChannelTime
)

BSSID MACAddress Any valid individual or broadcast MAC address Identifies a specific or broadcast BSSID.

********** Comment **********
Comment
Last paragraph in clause 11.3.2 states that a unicast probe request may be sent using an MLME-SCAN. request primitive: that is not possible. There is no mechanism in any of the SAPs for the SME to request a Unicast Probe Request.

This is because 802.11-1999 (R2003) clause 10.3.2.1 does not specify any parameters that would allow the MLME-SCAN.request to be constrained to a single DA. The BSSID parameter's valid range is "Any valid individual or broadcast MAC address", and the description of this is "Identifies a specific or broadcast BSSID"

In the IBSS BSSID 46 bits are random with the other bits set to indicate an individual locally administered IEEE MAC address. (802.11-1999 Clause 7.1.3.3.3) However, that doesn't guarantee that the IBSS BSSID is unique and different from the address of any STA in the BSS; as other STAs may also be using locally administered addresses.

Proposed Change

Extend the MLME-SCAN.request to add a DA field that would normally be set to the broadcast MAC address, but may be set to a specific MAC address to request a unicast Probe Request to be transmitted. This field cannot be used to identify a BSSID, so this would remove ambiguity even if a STA chose a locally administered address which matched the IBSS BSSID.

Add to section 10.3.2.1.2 in the list of primitive parameters an extra parameter "DestinationAddress".

Add to the table in section 10.3.2.1.2 the following line: DestinationAddress | MACAddress | A valid individual MAC Address or the broadcast MAC address | Identifies a specific STA or broadcast

Dave Halasz

Cisco Systems, Inc.

4125 Highlander Parkway

Richfield, OH 44286

Dave Halasz

Cisco Systems, Inc.

4125 Highlander Parkway

Richfield, OH 44286

Dave Halasz

Cisco Systems, Inc.

4125 Highlander Parkway

Richfield, OH 44286