iMC与迈普交换机做802.1x EAD由于radius accounting-request中authenticarot全0导致认证过后EAD下线问题的解决方法

李瑞峰 2009-11-30 发表

iMC与迈普交换机做802.1x EAD由于radius accounting-request中authenticarot全0导致认证过后EAD下线问题的解决方法

一、 组网：

iNode与迈普交换机配合做802.1x EAD，radius server采用iMC UAM

二、 问题描述：

户端能正常通过身份认证，但几秒钟之后，客户端INODE提示“安全检查服务器同步用户失败，当前连接即将被强行中断”；具体的INODE客户端认证过程如下：

2009-11-26 09:54:24 连接网络...

2009-11-26 09:54:24 开始进行身份验证... [post123]

2009-11-26 09:54:24 正在验证用户密码...

2009-11-26 09:54:25 您的身份验证成功

2009-11-26 09:54:33 安全检查服务器同步用户失败，当前连接即将被强行中断

2009-11-26 09:54:36 连接已断开

三、 过程分析：

从故障现像来看很像是UAM没有在线表，查看UAM果然没有在线表。uam的调试级别日志如下：

% 2009-11-26 11:05:55 ; [WARNING (2)] ; EAP ; SYS ; (NULL) ; (NULL) ; (NULL) ; [commonEap::getAttrFromPacket] no attribute of Service-Type.

% 2009-11-26 11:05:55 ; [WARNING (2)] ; EAP ; SYS ; (NULL) ; (NULL) ; (NULL) ; [commonEap::getAttrFromPacket]no attribute of Framed-IP-Address.

% 2009-11-26 11:05:55 ; [WARNING (2)] ; EAP ; SYS ; (NULL) ; (NULL) ; (NULL) ; [commonEap::getAttrFromPacket] no attribute of Service-Type.

% 2009-11-26 11:05:55 ; [WARNING (2)] ; EAP ; SYS ; (NULL) ; (NULL) ; (NULL) ; [commonEap::getAttrFromPacket]no attribute of Framed-IP-Address.

% 2009-11-26 11:05:55 ; [L_DEBUG (4)] ; LAN ; post123 ; 2 ; 87f3fbd7d1b94ee4bb0e1fe87e5eee6e ; 5B87KIus ; Send message attribut list:

Code = 2

ID = 38

ATTRIBUTES:

Service_Type(6) = 0

State(24) = 5B87KIus

Termination-Action(29) = 1

Session-Timeout(27) = 86400

Acct-Interim-Interval(85) = 600

% 2009-11-26 11:05:55 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

% 2009-11-26 11:05:58 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

% 2009-11-26 11:06:01 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

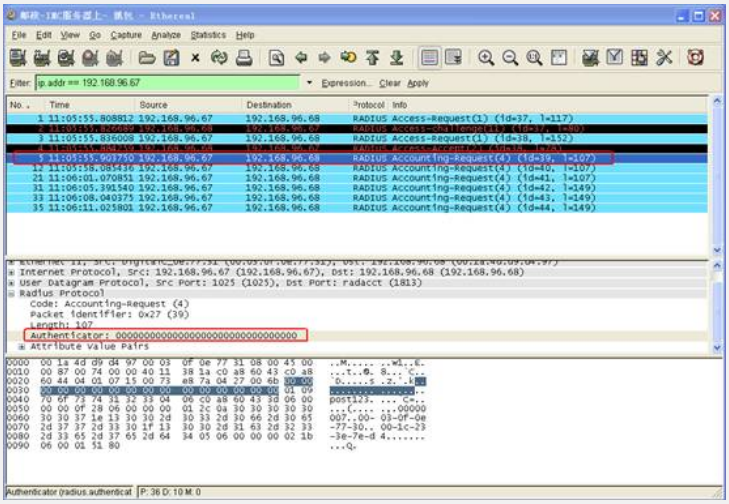
% 2009-11-26 11:06:05 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

% 2009-11-26 11:06:08 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

% 2009-11-26 11:06:11 ; [WARNING (2)] ; UAM ; SYS ; (NULL) ; (NULL) ; (NULL) ; Invalid Message Authenticator(from 192.168.96.67).

从UAM的调试级别日志中看到UAM回应了access-accept,这也是用户可以认证通过的原因，但在处理迈普设备(192.168.96.67)发过来的accounting-request时报错“invalid message authenticator”.

进一步在UAM上抓包，发现了原因，原来设备发送过来的交换机authenticator为全0.



问题至此定位：设备radius实现有问题，rfc 2866(radius accounting)对authenticator有明确的要求，如下。rfc2866中要求authenticator是一个MD5的值，这个值不可能是全0的。

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used to authenticate the messages between the client and RADIUS accounting server.In Accounting-Request Packets, the Authenticator value is a 16 octet MD5 [5] checksum, called the Request Authenticator.

The NAS and RADIUS accounting server share a secret. **The Request Authenticator field in Accounting-Request packets contains a one-way MD5 hash calculated over a stream of octets consisting of the Code + Identifier + Length + 16 zero octets + request attributes +shared secret (where + indicates concatenation).** The 16 octet MD5 hash value is stored in the Authenticator field of the Accounting-Request packet.

Note that the Request Authenticator of an Accounting-Request can not be done the same way as the Request Authenticator of a RADIUS Access-Request, because there is no User-Password attribute in an Accounting-Request.

四、 解决方法：

以下两种方案任选其一即可。

1. 迈普交换机按rfc标准实现
2. 使用iMC UAM的混合组网特性。