以SR6600为代表的路由器产品如何在本端查看公钥位数

证书 认证 **刘平泽** 2020-02-14 发表

问题描述

在本端display public-key peer 命令用来显示保存在本地的远端主机的公钥信息的时候，**但是本端看不到自己公钥相关的长度信息。**

解决方法

1， 我们的正式对外软件版本中，本地通过命令 disp public-key local rsa public **的确没有办法查看公钥位数。**，

2， 我们有其他的方法可以间接的在本地设备查看：如下

一：可以把显示的local public key配置成peer key，则可以直接看到（在本地创建一个peer key，然后复制local public key的秘钥，

后disp public-key peer即可，不需要传给对方，在对方侧查看）

二.公钥位数与行数有一定关系，如固定的 512 1024 2048 均对应固定的行数（可以自己在设备处创建并查看），但是遇到公钥并非这几个标准的位数的，就不能看了。

三： rsa公钥位数可以从如下的asn1编码准确看出（**但是过程比较繁琐，以下为举例**）：

```
=============================================
Key name: 5
Key type: RSA
Time when key pair created: 04:49:38 2011/01/01
Key code:
//30序列开始，81长度字段一字节，c9是序列长度;
//02整数开始，81整数长度1字节，c1(193字节)是整数长度，就是192*8=1536位，
//                    首字节00是asn1整数的编码规则要求的，正数首字节最高位如果是1前边加一字节00
//具体可以参考asn1编码规则。

3081DF300D06092A864886F70D01010105000381CD003081C90281C100CA76C13E6CE79B96


8EB52A345A46DED4DA14B38FBC0AFD94C399512BE68E10F3857BF9FA81399705F4267F0029
  2B9436FA59777C39EA61016DF507D05409C5488810645330E54D22313607CEAFAFF373CB5A

AC64B25CB48CEAE9E1A70BB43C531ABF39282D0B11B4CC016A31A1D040833EC1193BC2779C

98A285AEFBDAB00DA0C28D545D76455745BBC5F48F63B90840EB9829DA7B8360F3C03F76F5

1FAAE5FE66CD6DD24E056198BE663EDC03C93F2D22FCE4BF275323AE457E9C8E608CB5B902
  03010001

=============================================
Key name: 4
Key type: RSA
Time when key pair created: 04:49:25 2011/01/01
Key code:

  307C300D06092A864886F70D0101010500036B0030680261009DA10058E773E04E8A1E3D07  ---这个是0x60=96字节，就是768位的key

2FDD8B95DBE1A3D94138AE1EBBDBE68FFF7CF458EC22A39A22D4049E722E18319156EE4CD3

A7506232F0A2DD86C0DE11B10C671C38BF6DB312CAE5C46FAB2AC310CB484848255D14CB06
  139B3D551F3BA2A404BD0203010001

=============================================
```