

[2008-03-27]Quidway S3026EFGTC&E026_E026T系列交换机R0039L02版本发布

彭天付 2008-04-03 发表

Quidway S3026EFGTC&E026_E026T系列交换机R0039L02版本发布

一 使用范围及配套说明:

Quidway S3026EFGTC&E026_E026T系列交换机R0039L02版本正式发布, 发布范围为ARP攻击防御局点。版本配套关系请参考如下版本配套表:

产品系列	S3000-EI系列
型号	S3026C/S3026G/S3026T/S3026C-PWR S3026E/S3026E-FS/S3026E-FM
内存需求	64M
FLASH需求	8M
BOOTROM版本号	S3026E/S3026E-FS/S3026E-FM产品优先使用Bootrom130 其他S3000-EI产品如果需要支持百兆BIDI接口板和新的千兆光接口板优先使用Bootrom190, 如果不需要支持那么优先使用Bootrom160
目标文件名称	S3026EFGTC_PWR-VRP310-R0039L02.bin (3,773,336字节)
QUIDVIEW版本号	Quidview DM 3.10-R3118 (优先使用该版本) Quidview NMF 3.10-R3118 (优先使用该版本) Quidview NCC 3.10-R3118 (优先使用该版本)
CAMS版本号	CAMS 2.10-R0209 (优先使用该版本)
WEB版本号	推荐使用wnm2.2.2-R0008

产品系列	E系列
型号	E026/E026T
内存需求	64M
FLASH需求	8M
BOOTROM版本号	如果需要支持百兆BIDI接口板和新的千兆光接口板优先使用Bootrom190, 如果不需要支持那么优先使用Bootrom160
目标文件名称	E026_E026T-VRP310-R0039L02.bin (3,773,336字节)
QUIDVIEW版本号	Quidview DM 3.10-R3118 (优先使用该版本) Quidview NMF 3.10-R3118 (优先使用该版本) Quidview NCC 3.10-R3118 (优先使用该版本)
CAMS版本号	CAMS 2.10-R0209 (优先使用该版本)
WEB版本号	推荐使用wnm2.2.2-R0008

二 增减特性说明:

1 新增特性:

1、ARP攻击防御

2 删除特性:

无

3 修改特性:

无

三 相比前一版本解决的问题说明:

1. OPTED07258

首次发现版本: VRP310-R0039P01

问题产生的条件:

1. 建立集群, 在集群视图下设置SNMP读写团体名, 解散集群后再建立集群。
2. 建立集群后再建立堆叠, 在集群视图下设置SNMP读写团体名, 然后解散堆叠。

问题现象:

1. 条件1导致 SNMP 读写团体名没有被恢复为默认配置。
2. 条件2导致建立集群后自动配置的 SNMP 团体名被删除。

2. OPTED07539

首次发现版本: VRP310-R0039P01

问题产生的条件: 设备使能DHCP option82功能。

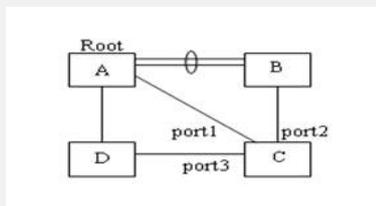
问题现象: DHCP CLIENT能够正确获取IP地址, 但是设备向DHCP CLIENT转发了多份ACK报文。

3. OPTED06910

首次发现版本: VRP310-R0039P01

问题产生的条件:

组网:



上图四台设备开启STP功能，反复修改设备C上端口port1的cost值，在端口port2上执行shutdown命令。

问题现象：设备C上端口port3的STP状态不能快速迁移。

4. OPTED07496

首次发现版本：VRP310-R0039P01

问题产生的条件：设备上没有配置文件时，交换机会默认创建VLAN interface 1并shutdown。

问题现象：设备连接到网络中时，如果这个网络的集群管理VLAN是VLAN 1，则集群不能即插即用。需要人为的到该设备上删除VLAN interface 1的配置才行。

5. LSOD00356

首次发现版本：VRP310-R0039P01

问题产生的条件：交换机全局使能STP，某端口上去使能STP。

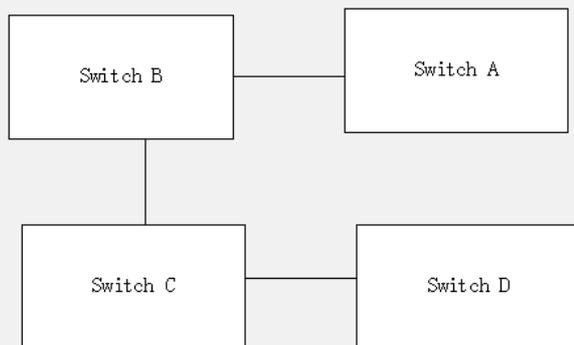
问题现象：在去使能STP的端口上进行“shutdown/undo shutdown”操作，仍然有端口discarding或者forwarding的日志信息。

6. LSOD00089

首次发现版本：VRP310-R0039P01

问题产生的条件：

组网：



如上图，Switch B和Switch C同时建立完全相同的集群。

问题现象：Switch B和Switch C两台交换机同时报集群私有IP冲突。

7. LSOD00620

首次发现版本：VRP310-R0039P01

问题产生的条件：在交换机上配置802.1X认证，用户通过认证会被下发到新的VLAN。

问题现象：某个用户认证失败，后面其他用户也会认证失败。

8. LSOD00928

首次发现版本：VRP310-R0039P01

问题产生的条件：在交换机上建立堆叠，更改设备的超级密码，执行“undo stacking enable”命令解散堆叠。

问题现象：串口无响应。

9. LSOD00933

首次发现版本：VRP310-R0039P01

问题产生的条件：堆叠组成员设备掉电重启。

问题现象：成员设备不能重新加入堆叠。

10. LSOD01349

首次发现版本：VRP310-R0039P01

问题产生的条件：设备开启DHCP-Snooping功能，某端口下的DHCP Client申请到IP地址。此后，启用802.1X认证，但端口没有通过802.1X认证。

问题现象：DHCP Client仍然可以收到DHCP续约报文，动态IP地址没有老化删除。

11. LSOD04977

首次发现版本：VRP310-R0039P01

问题产生条件：有radius攻击报文进入交换机进行处理，报文的code字段不是（2、3、5、11）。

问题现象：设备受到攻击后无法正常处理正确的radius报文，设备运行异常。

12. LSOD06368

首次发现版本: VRP310-R0039P01

问题产生条件: 在交换机上配置802.1X, 用户输入错误的用户名或密码, 使其认证不成功。

问题现象: 交换机发送的“failure”报文中EAP协议中的长度字段不正确。

13. LSOD06333

首次发现版本: VRP310-R0039P01

问题产生条件: 交换机运行时候CPU瞬高。

问题现象: 交换机无法进行telnet、802.1X等认证处理, 串口会输出“[RD_DEBUG] Error:Can not Send Message to Myself”告警信息。

14. LSOD06184

首次发现版本: VRP310-R0039P01

问题产生条件: 在线Local-user数不为0。

问题现象: 无法进入在线用户对应的local-user视图修改相关属性, 如密码等。

15. LSOD01726

首次发现版本: VRP310-R0039P01

问题产生的条件:

1. 进行802.1x认证, 认证方式设置为EAP;
2. 认证方法为PEAP+智能卡或其他证书;
3. 使用2003 IAS作radius server, 在线升级了SP2及其他补丁后, 导致认证的radius challenge报文交互次数超过16次。

问题现象: 认证由于radius challenge报文交互次数超过交换机的16次限制而失败。

16. LSOD03497

首次发现版本: VRP310-R0039P01

问题产生的条件: 交换机上使能802.1X认证, 用户上线后立即下线。

问题现象: 会出现用户上网费用被大量扣除的情况。

17. LSOD01241

首次发现版本: VRP310-R0039P01

问题产生的条件: 交换机上配置dhcp-snooping option82特性, 用户接在Ethernet 0/1外的其他端口。

问题现象: dhcp-snooping option82特性不能生效。

如要完整的了解该版本累计解决的软件BUG, 请参看配套发布的《Quidway S3026EF GTC_PWR-VRP310-R0039L02 版本说明书》和《Quidway E026_E026T-VRP310-R0039L02 版本说明书》。