

H3C S3610_5510-CMW520-R5309P02 版本说明书

杭州华三通信技术有限公司



H3C S3610_5510-CMW520-R5309P02 版本说明书

关键词：版本信息 版本变更说明 版本存在问题和规避措施 解决问题列表

摘 要：对相应产品版本的各方面的事项进行了详细说明，包括版本信息、版本变更说明、版本存在问题和规避措施、解决问题列表、配套资料、版本升级操作指导。

缩略语：

缩略语	英文全名	中文解释
MIB	Management Information Base	管理信息库
ACL	Access Control List	访问控制列表
NMF	Network Management Framework	网络管理框架
NCC	Network Configuration Center	网络配置中心
GARP	General Attribute Registration Protocol	一般属性注册协议
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
RRPP	Rapid Ring Protection Protocol	快速环网保护协议
OAM	Operation, Administration and Maintenance	操作，管理和维护
DLDP	Device Link Detection Protocol	设备链路检测协议
MCE	Multi-Custom Edge	多用户网络边缘
EAD	Endpoint Admission Defense	端点准入防御

目 录

1 版本信息	5
1.1 版本号	5
1.2 历史版本信息	5
1.3 版本配套表	6
2 版本使用限制及注意事项	7
3 版本特性说明	7
3.1 版本硬件特性	7
3.2 版本软件特性	9
4 版本变更说明	14
4.1 特性变更说明	14
4.2 命令行变更说明	18
4.3 MIB变更说明	32
4.4 操作方式变更说明	32
4.4.1 CMW520-R5309P02 版本操作方式变更	32
4.4.2 CMW520-F5305P02 版本操作方式变更	32
4.4.3 CMW520-R0001P02 版本操作方式变更	32
4.4.4 CMW520-R0001 版本操作方式变更	32
5 存在问题与规避措施	32
6 解决问题列表	33
6.1 CMW520-R5309P02 版本解决问题列表	33
6.2 CMW520-R5309 版本解决问题列表	34
6.3 CMW520-R5308 版本解决问题列表	35
6.4 CMW520-R5306 版本解决问题列表	37
6.5 CMW520-F5305P06 版本解决问题列表	37
6.6 CMW520-F5305P02 版本解决问题列表	38
6.7 CMW520-R5303 版本解决问题列表	40
6.8 CMW520-F5302P01 版本解决问题列表	42
6.9 CMW520-F5302 版本解决问题列表	42
6.10 CMW520-R5301 版本解决问题列表	43
6.11 CMW520-R0001P02 版本解决问题列表	45
6.12 CMW520-R0001 版本解决问题列表	46

6.13 CMW520-E0001 版本解决问题列表	47
7 配套资料	47
7.1 配套资料清单	47
7.2 配套产品资料的获取方法	47
8 版本升级操作指导	47
8.1 通过命令行远程升级	48
8.2 BootRom菜单	49
8.3 利用串口（Xmodem协议）完成软件升级	51
8.4 利用以太网口（FTP/TFTP协议）完成软件升级	53
8.4.1 通过TFTP完成软件升级	53
8.4.2 通过FTP完成软件升级	54

表目录

表 1 历史版本信息表	5
表 2 版本配套表	6
表 3 产品硬件特性	7
表 4 产品软件特性	9
表 5 特性变更说明	14
表 6 命令行变更说明	18
表 7 MIB文件变更说明	32
表 8 配套手册清单	47
表 9 从网站查询和下载资料的说明	47

1 版本信息

1.1 版本号

版本号：Comware Software, Version 5.20, Release 5309P02

注：该版本号可在命令行任何视图下用 `display version` 命令查看，见注①

1.2 历史版本信息

表1 历史版本信息表

版本号	基础版本号	发布日期	备注
S3610_5510-CMW520-R5309P02	S3610_5510-CMW520-R5309	2009-06-17	修改问题
S3610_5510-CMW520-R5309	S3610_5510-CMW520-R5308	2009-04-03	修改问题
S3610_5510-CMW520-R5308	S3610_5510-CMW520-F5306	2009-03-26	修改问题
S3610_5510-CMW520-R5306	S3610_5510-CMW520-F5305P06	2009-01-12	增加新特性
S3610_5510-CMW520-F5305P06	S3610_5510-CMW520-F5305P02	2008-11-21	增加新特性
S3610_5510-CMW520-F5305P02	S3610_5510-CMW520-R5303	2008-07-02	增加新特性
S3610_5510-CMW520-R5303	S3610_5510-CMW520-F5302P01	2008-03-12	支持新的硬件
S3610_5510-CMW520-F5302P01	S3610_5510-CMW520-F5302	2007-12-18	修改缺陷
S3610_5510-CMW520-F5302	S3610_5510-CMW520-R5301	2007-10-30	增加新特性
S3610_5510-CMW520-R5301	S3610_5510-CMW520-R0001P02	2007-8-27	合入新特性
S3610_5510-CMW520-R0001P02	S3610_S5510-CMW520-R0001	2007-5-28	无
S3610_S5510-CMW520-R0001	S3610_S5510-CMW520-E0001	2006-12-4	无
S3610_S5510-CMW520-E0001	首次发布	2006-7-28	无

1.3 版本配套表

表2 版本配套表

产品系列	S3610&S5510 series
型号	S3610-52P/S3610-28TP/S3610-28F/S3610-28P/S5510-24F/S5510-24P/S3610-52M
内存需求	最小 128M
FLASH 需求	最小 32M/
BOOTROM 版本号	V206 及以上版本(该版本号可在命令行任何视图下用 display version 命令查看，见注②)
目标文件名称	S3610_5510-CMW520-R5309P02.bin
iMC 版本号	iMC EAD 3.60-E6102 iMC PLAT 3.20-R2602 + P06 iMC UAM 3.60-E6102 iMC QoSM 3.20-E0603 + P01
iNode	iNode PC 3.60-E6111

示例：查看 S3610&S5510 系列交换机的软件版本和 BootRom 版本号方式如下：

```
<H3C>display version
```

```
H3C Comware Platform Software
```

```
Comware Software, Version 5.20, Release 5309P02 ----- 注①
```

```
Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
```

```
H3C S3610-52P uptime is 0 week, 0 day, 0 hour, 2 minutes
```

```
H3C S3610-52P
```

```
128M      bytes DRAM
```

```
16M       bytes Flash Memory
```

```
Config Register points to FLASH
```

```
Hardware Version is REV.A
```

```
CPLD Version is CPLD 001
```

```
Bootrom Version is 206 ----- 注②
```

```
[SubSlot 0] 48FE Hardware Version is REV.A
```

2 版本使用限制及注意事项

- 百兆端口强制工作在不同速率模式互连，端口不停的 up/down;
- 报文被重定向到出端口后，总是 untag 的;
- ACL 无法匹配分片报文的最后一分片报文;
- 起 dot1x 的端口，只能实现端口的入方向单向受控。
- 由于硬件和软件配合的原因，对于出厂的软件版本号为 R5303 的设备，不可将版本降级到早于此版本的软件，否则会提示降级失败。
- 对于 S3610-52M 设备，不可对接口板进行热插拔，必须掉电更换，否则会导致主机损坏。
- F5305P02 及之后的版本与 bootrom 142 之前（不包含 142）的版本不匹配，因此升级 F5305P02 及之后的版本时，必须首先升级或者同时升级 Bootrom 到版本配套表指定的 Bootrom 版本。

3 版本特性说明

3.1 版本硬件特性

表3 产品硬件特性

项目	描述
外形尺寸（宽×高×深）	440×43.6×260 mm（S3610） 440×43.6×360 mm（S5510） 436×86×390mm（S3610-52M）
重量（满插板）	S3610-52P: 3.8KG S3610-28P: 3.6KG S3610-28TP: 3.7KG S3610-28F: 3.8KG S3610-52M: 8.5KG S5510-24F/S5510-24P(不含电源模块): 4.6KG S5510 电源模块: 0.8~1KG
管理端口	1个Console口
业务端口描述	S3610-28P: 24个10/100M电口和4个千兆SFP口

项目	描述
	S3610-28TP: 24 个 10/100M电口, 2 个千兆SFP口和 2 个 10/100/1000M电口 S3610-52P: 48 个 10/100M电口和 4 个千兆SFP口 S3610-28F: 24 个百兆SFP口, 2 个千兆SFP口和 2 个 10/100/1000M电口 S5510-24P-AC/ S5510-24P-DC: 24 个 10/100/1000M电口和 4 个千兆SFP口 (Combo) S5510-24F-AC/S5510-24F-DC: 24 个千兆SFP口和 4 个 10/100/1000M电口 (Combo) S3610-52M: 根据选插模块决定, 最多 48 个 10/100M 电口或 48 个 100M SFP 口, 后面板固定 4 个千兆 SFP 口和 4 个 10/100/1000M 电口
接口线缆介质类型及最大传输距离	100BASE-TX 2 对 5 类非屏蔽双绞线 (支持 100m) 或 2 对屏蔽双绞线 (支持 100m) 10/100/1000BASE-T 4 对 5 类非屏蔽双绞线 (支持 100m) 100BASE-FX-MM-SFP 62.5/125μm多模光纤 2km, (1310nm) 100BASE-FX-SM-SFP 9/125μm单模光纤 15km, (1310nm) 100BASE-FX-SM-LR-SFP 9/125μm单模光纤 40km, (1310nm) 100BASE-FX-SM-VR-SFP 9/125μm单模光纤 80km, (1550nm) 1000BASE-SX-SFP 50/125μm多模光纤 550m (850nm) 1000BASE-SX-SFP 62.5/125μm多模光纤 275m (850nm) 1000BASE-LX-SFP 单模光纤 10km (1310nm) 1000BASE-LH-SFP 单模光纤 30km (1310nm) 1000BASE-ZX-LR-SFP 单模光纤 40km (1550nm) 1000BASE-ZX-VR-SFP 单模光纤 40km (1550nm) 1000BASE-T-AN-SFP 五类双绞线 100m
输入电压	AC:

项目	描述
	额定电压范围：100-240V AC；50/60Hz 最大电压范围：90-264V AC；50/60Hz DC： 额定电压范围：-48 ~ -60V 最大电压范围：-36 ~ -72V
系统最大功耗（满负荷时）	S3610-52P：45W S3610-28P：35W S3610-28TP：40W S3610-28F：60W S5510-24P-AC/S5510-24P-DC：80W S5510-24F-AC/S5510-24F-DC：75W SS610-52M：110W
工作环境温度	0℃~45℃
工作环境相对湿度	10%~90%

3.2 版本软件特性

表4 产品软件特性

业务	特性及描述
二三层线速转发	S3610 端口交换容量为(28 端口/52 端口)：12.8Gbps/17.6Gbps S3610 包转发率(28 端口/52 端口)：9.53Mpps/13.1Mpps S5510 端口交换容量为：48Gbps S5510 包转发率：35.71Mpps
端口汇聚	支持FE（Fast Ethernet）端口聚合 支持GE（Gigabit Ethernet）端口聚合 支持静态聚合 支持手工聚合
MAC地址	支持 16K个MAC地址 支持黑洞MAC地址 支持设置端口MAC地址学习最大个数
端口	支持 IEEE 802.3x 流控（全双工） 支持 Back-pressure based flow control（背压式流控）（半双工）

业务	特性及描述
	支持基于端口速率百分比的风暴抑制 支持设置端口优先级 支持以太网端口流量阈值控制(Storm Constrain)
OAM	支持 OAM 802.3ah
VLAN	支持端口 VLAN(4094 个) 支持协议 VLAN 基于 IPv4 子网 VLAN 支持 Voice VLAN 支持 GARP/GVRP 支持 VLAN VPN (QinQ)，灵活 QinQ，BPDU tunnel 支持 VLAN Mapping
DHCP	支持 DHCP Server (支持 MCE) 支持 DHCP-Relay (支持 MCE) 支持 DHCP Client 支持 DHCP Snooping DHCP Snooping 支持 Option82
UDP Helper	支持 UDP Helper
DNS	支持静态域名解析 支持动态域名解析客户端
ARP	支持 ARP 支持免费 ARP 支持 ARP Proxy 支持 ARP Detection 支持 ARP Snooping 支持 MFF(MAC-Forced Forwarding)
IP 路由	支持静态路由和缺省路由 支持 RIP (Routing Information Protocol) v1/2 支持 RIPng 支持 OSPFv1/v2 (Open Shortest Path First) 支持 OSPFv3 支持 IS-IS 支持 IS-ISv6

业务	特性及描述	
	支持 BGP (Border Gateway Protocol) 支持 BGP4+ for IPV6 支持等价路由 支持路由策略	
MCE	支持 MCE 工作模式	
组播	支持 IGMP (Internet Group Management Protocol) Snooping 支持 IGMPv1/v2/v3 支持 PIM-DM (Protocol Independent Multicast-Dense Mode) 支持 PIM-SM (Protocol Independent Multicast-Sparse Mode) 支持 MSDP(Multicast Source Discovery Protocol) 支持 MLD Snooping 支持 MLDv2 Snooping 支持 未知组播丢弃	
二层环路保护协议	支持 STP/RSTP/MSTP 支持 RRPP 支持 Smart Link	
IPv6	支持 ND(Neighbor Discovery) 支持 PMTU 支持 IPv6 Ping, IPv6 Tracert 支持 IPv6 Telnet 支持 IPv6 TFTP	
IPv6 over IPv4 Tunnel	支持手动配置 Tunnel 支持 6to4 tunnel 支持 ISATAP(Intra-site Automatic Tunneling Protocol) tunnel 支持 Auto-tunnel (即 IPv4 compatible tunnel)	
QoS/ACL	支持 ACL	支持基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、四层端口、协议类型、

业务	特性及描述	
		VLAN 等信息的流分类 支持基本 ACL 支持高级 ACL 支持二层 ACL 支持用户自定义 ACL
	支持 ACL 流模板	支持用户自定义流模板 支持系统缺省流模板
	支持 QoS	支持基于流的流量限速 支持基于流的标记优先级、 支持基于流的修改报文 VLAN ID 支持基于流的报文重定向到端口或 IP 下一跳 支持基于流的流量统计 支持基于流的流镜像 支持端口队列调度 (SP/WRR/SP+WRR) 支持端口镜像和 RSPAN(远程端口镜像) 支持端口流量整形 支持端口拥塞丢弃
	支持 IPv6 ACL	支持基于源 IPv6 地址、目的 IPv6 地址、四层端口、协议类型等信息的流分类 支持基本 IPv6 ACL 支持高级 IPv6 ACL
	支持时间段 (Time Range)	
	支持策略路由	
	支持 IP Source guard	
安全特性	支持用户分级管理和口令保护 支持 IEEE 802.1X 认证 支持 AAA 支持 Radius 认证 支持 HWTacacs 支持集中式 MAC 地址认证	

业务	特性及描述
	支持端口隔离 支持 IP+MAC+端口绑定 支持 HTTPS 支持 EAD 支持端口安全 System-Guard 防攻击
可靠性	支持 VRRP (Virtual Redundancy Routing Protocol) 支持双向转发检测 (BFD) 支持连通错误检测 (CFD) 支持 Track 联动 支持平滑重启
加载与升级	支持 XModem 协议实现加载升级 支持 FTP (File Transfer Protocol) 加载升级 支持 TFTP (Trivial File Transfer Protocol) 加载升级
管理	支持命令行接口 (CLI) 配置 支持 Telnet 远程配置 支持通过 Console 口配置 支持 SNMP (Simple Network Management Protocol) v1/v2c/v3 支持 RMON (Remote Monitoring) 1, 2, 3, 9 组 MIB 支持华为 QuidView 网管系统 支持 WEB 网管 支持系统日志 支持分级告警 支持集群管理 HGMP (Huawei Group Management Protocol) v2 支持 Modem 远端拨号 支持 NTP 支持 SSH 支持 SSHv2.0 支持电源的状态检测和告警 支持堆叠管理 (IRF Lite) 支持 sFlow 支持 LLDP

业务	特性及描述
维护	支持调试信息输出 支持 Ping、Tracert 支持 NQA 支持 Telnet 远程维护 支持虚拟电缆检测(Virtual Cable Test)

4 版本变更说明

4.1 特性变更说明

表5 特性变更说明

版本号	项目	描述
S3610_5510- CMW520- R5309P02	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性：Super VLAN 删除特性：无
S3610_5510- CMW520-R5309	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性：无 删除特性：无
S3610_5510- CMW520-R5308	硬件特性更新	新增特性：无 删除特性：无

版本号	项目	描述
	软件特性更新	新增特性：无 修改特性： 1. DHCP Server 支持 MCE。 2. DHCP Relay 与 DHCP Snooping 支持同时配置。 3. 路由端口接口支持 NDP。 4. MCE 模式下，OSPF 进程最大支持数量扩充到 16 个。 5. 全局支持端口的 Policy-mode 设定（ip-source-guard、mode voice-vlan），增加命令行 “policy mode multi-service-cooperation” 删除特性：无
S3610_5510-CMW520-R5306	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性： 1. 物理端口可配置 IP 地址，工作在路由模式。 2. 对单播、组播的流量抑制功能。 3. BFD 与 OSPF 联动功能。 删除特性：无
S3610_5510-CMW520-F5305P06	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性： 1. 支持基于TCP 标志位的ACL 2. super密码远程认证，及不可达转本地认证 3. GTS 支持 CBS 参数配置 4. Link-delay 5. IP check 与 Car 联动以及 Voice vlan 与 Car 联动 6. ARP-detection 静态绑定模式 7. 动态 vlan 按名字下发 删除特性：无
S3610_5510-CMW520-F5305P02	硬件特性更新	新增特性：无 删除特性：无

版本号	项目	描述
	软件特性更新	新增特性： 1. Storm constrain 2. RRPP 保护 VLAN 可配 3. Smart link 4. 端口安全 5. 连通错误检测 6. 基于 VRRP 的 BFD 7. 堆叠管理(IRF Lite) 8. Track 联动功能 9. sFlow 10. VLAN Mapping 11. ARP detection 12. ARP snooping 13. System-guard 14. LLDP 15. arp rate-limit 16. GR 平滑重启 17. MFF 18. IP Source Guard 相关 19. burst-mode 20. mld-snooping drop-unknown 删除特性： 1. stp bpdu-transparent-forwarding 2. stp bpdu-tagged 修改特性：无
S3610_5510- CMW520-R5303	硬件特性更新	新增特性：硬件更换新的包缓存芯片，软件做相应的支持。 删除特性：无
	软件特性更新	新增特性：无 删除特性：无 修改特性：二层协议报文发出时携带的源 MAC 信息由统一的 MAC 地址修改为每个端口独立的 MAC 地址方式。这些二层协议包括：Cluster、DLDP、HABP、LACP、LLDP、MSTP、NDP、NTDP、GVRP 等。

版本号	项目	描述
S3610_5510- CMW520- F5302P01	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性：无 删除特性：无
S3610_5510- CMW520-F5302	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性： 1. MCE 2. EAD 3. BFD for static route 4. Enable/disable vlan ingress filter 5. bpdu tunnel related features 6. MAC 地址同步 删除特性：无
S3610_5510- CMW520-R5301	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性： 1. 高端内存 2. ESFP 3. RRPP 4. OAM 5. DLDP 修改特性：无。
S3610_5510- CMW520- R0001P02	硬件特性更新	新增特性：无 删除特性：无
	软件特性更新	新增特性：无 修改特性：修改 802.3ad 实现，不支持纯动态 LACP 模式，支持 Manual 和 Static 模式
S3610_S5510- CMW520-R0001	硬件特性更新	新增特性：无 删除特性：无

版本号	项目	描述
	软件特性更新	新增特性： 1. IPV4/IPV6 模式切换， 2. IPV6 防攻击 删除特性：无
S3610_S5510- CMW520-E0001	硬件特性更新	首次发布。
	软件特性更新	首次发布。

4.2 命令行变更说明

表6 命令行变更说明

版本号	项目	描述
S3610_5510- CMW520- R5309P02	新增命令	Super Vlan相关命令，具体参见随版本提供的《Super VLAN配置》和《Super VLAN命令》手册： 1. supervlan 【命令】 supervlan undo supervlan 【视图】 VLAN视图 【参数】 无 【描述】 supervlan命令用来设置当前VLAN的类型为Super VLAN。undo supervlan命令用来取消一个VLAN的Super VLAN类型的设置。 【举例】 # 将VLAN2配置为Super VLAN。 <pre><Sysname> system-view [Sysname] vlan 2 [Sysname-vlan2] supervlan</pre> 2. subvlan 【命令】 subvlan vlan-list undo subvlan [vlan-list]

版本号	项目	描述
		【视图】 VLAN视图 【参数】 vlan-list: Sub VLAN列表 【描述】 subvlan命令用来建立Super VLAN和Sub VLAN间的映射关系。当前VLAN为Super VLAN，vlan-list参数里指定的VLAN为Sub VLAN。undo subvlan命令用来取消Sub VLAN和Super VLAN间的映射关系。 【举例】 # 将Super VLAN10和Sub VLAN3、4、5、9对应起来。 <pre><Sysname> system-view [Sysname] vlan 10 [Sysname-vlan10] subvlan 3 to 5 9</pre> 3. display supervlan 【命令】 display supervlan [supervlan-id] 【视图】 任意视图 【参数】 supervlan-id: Super VLAN的编号，取值范围为1~4094。 【描述】 display supervlan命令用来显示Super VLAN和Sub VLAN的映射关系，以及标识Super VLAN和Sub VLAN映射关系的端口。 相关配置可参考命令supervlan和subvlan。
	删除命令	无
	修改命令	无
S3610_5510-CMW520-R5309	新增命令	无
	删除命令	无
	修改命令	无
S3610_5510-CMW520-R5308	新增命令	1. 全局支持端口的 Policy-mode 设定（ip-source-guard、mode voice-vlan），增加

版本号	项目	描述
		命令行 “policy mode multi-service-cooperation”。 【命令】 policy mode multi-service-cooperation undo policy mode multi-service-cooperation 【视图】 系统视图 【缺省级别】 2: 系统级 【参数】 无 【描述】 policy mode multi-service-cooperation 命令用于全局使能对 IP Source Guard 表项的报文或被设备识别为语音数据的报文进行匹配分类和执行流行为的动作。设备配置此命令后，等同于 classifier behavior 命令中携带了 ip-source-guard 和 voice-vlan 参数。 参见：命令手册-QoS 分册-QoS 策略配置命令-classifier behavior。 【举例】 # 配置交换机使能 multi-service-cooperation。 <Sysname> system-view [Sysname] policy mode multi-service-cooperation 2. 三层以太网端口接口视图下，增加命令行 “ndp enable”
	删除命令	无
	修改命令	无
S3610_5510-CMW520-R5306	新增命令	下列特性相关的命令，详细参见随版本发布的各特性配置手册和命令手册。 3. 物理端口可配置 IP 地址，工作在路由模式。 4. 对单播、组播的流量抑制功能。 5. BFD 与 OSPF 联动功能。
	删除命令	无
	修改命令	无

版本号	项目	描述
S3610_5510- CMW520- F5305P06	新增命令	1. super密码远程认证 命令一： 【命令】 super authentication-mode scheme [local] undo super authentication-mode 【视图】 系统视图 【参数】 scheme：用户级别切换采用 HWTACAS 认证方式。 local：在远程认证认证不可用时转本地认证，直接使用用户输入密码与预设 super 密码进行比较进行认证 【描述】 super authentication-mode 命令用来设置切换低级别用户到高级别用户的认证方式。undo super authentication-mode 命令用来恢复缺省情况。 缺省情况下，切换低级别用户到高级别用户时采用 super 密码本地认证方式。 【举例】 # 配置 VTY 0 用户从当前级别向高级别切换时采用 HWTACAS 认证，若远程认证不可达，则自动转本地认证。 <H3C> system-view System View: return to User View with Ctrl+Z. [H3C] super authentication-mode scheme local 命令二： 【命令】 authentication super hwtacacs-scheme hwtacacs-scheme-name undo authentication super 【视图】 ISP 域视图

版本号	项目	描述
		【参数】 hwtaacs-scheme hwtaacs-scheme-name : HWTACACS 方案名，为不超过 32 个字符的字符串。 【描述】 authentication super 命令用来配置当前 ISP 域用户切换级别所使用的 HWTACACS 认证方案。 undo authentication super 命令用来取消当前 ISP 域用户切换级别所使用的 HWTACACS 认证方案。 缺省情况下，没有配置当前 ISP 域用户切换级别所使用的 HWTACACS 认证方案。 当使用 authentication super 命令为当前 ISP 域指定用户切换级别所使用的 HWTACACS 方案时，所使用的 HWTACACS 方案必须是已经设置好的。 【举例】 System View: return to User View with Ctrl+Z. # 指定当前 ISP 域 aabbcc.net 用户切换级别所使用的 HWTACACS 认证方案为 ht。 <H3C> system-view System View: return to User View with Ctrl+Z. [H3C] domain aabbcc.net New Domain added. [H3C-isp-aabbcc.net] authentication super hwtaacs-scheme ht 2. GTS支持CBS参数配置 【命令】： qos gts { any queue queue-number } cir committed-information-rate [cbs committed-burst-size] undo qos gts { any queue queue-number } 【视图】： 以太网端口视图/端口组视图 【参数】： any： 对所有的数据包进行流量整形。 queue queue-number： 对队列上的数据包进行流量整形，queue-number 为匹配的队列号，取值范围为 0~7。

版本号	项目	描述
		均速率在承诺速率以内时的突发流量，单位为byte，取值范围为4000～16000000，建议大于(100/16)*CIR 【描述】：qos gts命令用来配置流量整形。undo qos gts命令用来取消流量整形配置。 qos gts any用来为所有的流配置流量整形。qos gts queue用来为某一个队列的数据包配置流量整形。 【举例】： # 下面的命令将在端口Ethernet 1/0/1上对所有报文进行流量整形。速率小于等于650kbps时正常发送，速率大于650kbps时，进入缓存队列，承诺突发尺寸为1000,000bytes [Sysname-Ethernet1/0/1] qos gts any cir 650 cbs 1000000 3. Link-delay 【命令】：link-delay n 【视图】：以太网端口视图 【参数】：n <2-10>，延时秒数。 【描述】：对端口UP做延迟处理。 【举例】： [System -Ethernet1/0/1]link-delay 2 4. IP check与Car联动以及Voice vlan与Car联动 【命令】：classifier classifier-name behavior behavior-name [mode { do1q-tag-manipulation ip-source-guard voice-vlan }] undo classifier classifier-name 【视图】：策略视图 【参数】：classifier-name：类名。 behavior-name：流行为名。 mode dot1q-tag-manipulation：设置该类和流行为对应关系用于VLAN映射功能。

版本号	项目	描述
		mode ip-source-guard: 设置该类和流行为对应关系用于IP source guard功能，可与ip-source-guard特性中的user-bind或ip check source功能结合使用，从而将dhcp snooping动态绑定表项或user bind表项与CAR限速等策略结合，实现对合法用户的限速等功能。 mode voice-vlan: 设置该类和流行为对应关系用于voice vlan功能。可与voice vlan功能结合，对符合voice vlan OUI的语音流进行CAR限速等功能。 【描述】: 新增的mode扩展命令主要针对动态用户实现CAR限速等Qos策略。 新增的mode ip-source-guard命令，可将Qos策略与Ip check source或user bind功能结合使用，从而将dhcp snooping动态绑定表项或user bind表项与CAR限速等策略结合，实现对合法用户的限速等策略。如：开启dhcp-snooping及ip check source后，希望对动态申请到IP地址的合法用户进行流量限速，则可以在用户侧端口下发mode ip-source-guard的CAR策略，这样，申请到IP地址的用户会自动与CAR规则绑定，实现限速。参见举例部分。 新增的mode voice-vlan命令，可将Qos策略与voice vlan功能结合使用，与mode ip-source-guard类似，它对符合voice vlan OUI的动态加入的语音流进行CAR限速等功能。 注意: 1) classifier的定义必须为if-match any 2) mode dot1q-tag-manipulation 与 mode ip-source-guard不能同时在一个policy中定义 3) 必须先在端口下发policy策略，再使用ip-source-guard或voice vlan特性，才能使两者关联起来。 【举例】: 使用dhcp-snooping及ip check source端口过滤功能，当用户通过DHCP方式获取到IP地址后，自动将合法的用户与CAR限速策略绑定，限速带宽为10Mbps。同时，使用user-bind静态绑定功能，对IP为1.1.1.1，mac为0000-0000-0002的用户也与

版本号	项目	描述
		CAR限速绑定，限速10Mbps。 #创建car限速策略，对用户限速10Mbps(若用户共享带宽，可配置聚合CAR): <pre>[system]traffic classifier cl [system-classifier-car]if-match any [system]traffic behavior be [system-behavior-be]car cir 10000 [system]qos policy ipcheck [system-qospolicy-ipcheck]classifier cl behavior be mode ip-source-guard</pre> #在端口应用策略 <pre>[system]interface Ethernet 1/1/1 [system-Ethernet1/1/1]qos apply policy ipcheck inbound</pre> #使能ip check source: <pre><SwitchA> system-view [SwitchA] interface ethernet1/0/1 [SwitchA-Ethernet1/0/1] ip check source ip-address mac-address [SwitchA-Ethernet1/0/1]quit [SwitchA] dhcp-snooping</pre> #使能user-bind <pre>[SwitchA-Ethernet1/0/1]user-bind ip-address 1.1.1.1 mac-address 0-0-2</pre> 5. ARP-detection静态绑定模式 命令一: 【命令】: <pre>arp detection mode { dhcp-snooping dot1x static-bind } undo arp detection mode { dhcp-snooping dot1x static-bind }</pre> 【视图】: 系统视图

版本号	项目	描述
		【参数】： 关于dhcp-snooping和dot1x选项说明，请参考ARP操作手册。 新增static-bind：基于IP和MAC静态绑定表项的检查。主要针对仿冒网关的攻击。不论对于ARP非信任端口，还是信任端口，只要配置了基于IP和MAC静态绑定表项检查模式且所属VLAN使能了ARP Detection功能，则从该端口上送的ARP报文需进行基于IP和MAC静态绑定表项检查。对于源IP存在绑定关系但是MAC地址不符的ARP报文，设备认为是非法报文进行丢弃处理；对于源IP不存在绑定关系和源IP存在绑定关系且MAC地址相符的ARP报文，设备认为是合法报文，检查通过。 【描述】：arp detection mode命令用来配置ARP Detection检查模式。undo arp detection mode命令用来取消指定的ARP Detection检查模式。 用户合法性检查是根据ARP报文中源IP地址和源MAC地址检查用户是否是所属VLAN所在端口上的合法用户，包括基于DHCP Snooping安全表项的检查、基于802.1x安全表项的检查和基于IP和MAC静态绑定表项的检查。用户可以任意选择使能哪些功能，各功能可以共存。如果使能多种功能，则先进行DHCP Snooping安全表项检查，然后进行802.1x安全表项检查，最后进行IP和MAC静态绑定表项检查。 缺省情况下，没有配置ARP Detection检查模式，认为所有报文都是非法的。 【举例】： [Quidway]arp detection mode static-bind 命令二： 【命令】 arp detection static-bind ip-address mac-address undo arp detection static-bind [ip-address] 【视图】 系统视图 【参数】 ip-address：静态绑定表项的IP地址部分。mac-address：静态绑定表项的MAC地址部分，格式为H-H-H。

版本号	项目	描述
		【描述】 arp detection static-bind命令用来配置IP和MAC的静态绑定表项。undo arp detection static-bind命令用来删除已经配置的IP和MAC的静态绑定表项。 缺省情况下，没有静态绑定表项。 对于源IP存在绑定关系但是MAC地址不符的ARP报文，设备认为是非法报文进行丢弃处理；对于源IP不存在绑定关系和源IP存在绑定关系且MAC地址相符的ARP报文，设备认为是合法报文，通过检查。 需要注意的是，如果undo命令中没有指定IP地址，则删除已经配置的所有IP和MAC的静态绑定表项。 【举例】 # 配置IP和MAC的静态绑定表项。 <pre><Sysname> system-view [Sysname] arp detection static-bind 192.168.1.2 2-1-201</pre> 2. 动态vlan按名字下发 【视图】： VLAN视图 【命令】： name string 【参数】： string：表示当前VLAN名称的字符串，长度为1～32个字符。 【描述】： name命令用来为当前的VLAN命名；undo name命令用来恢复当前VLAN名称的缺省值。缺省情况下，当前VLAN的名称为该VLAN的VLAN ID，如"VLAN 0001"。 【举例】： <pre>[System-vlan2] name hello</pre>
	删除命令	无
	修改命令	支持基于TCP 标志位的ACL 3000～3999范围的规则TCP后面的关键字“established”修改为各个TCP flag: ack、fin、psh、rst、syn、urg。
S3610_5510-CMW520-F5305P02	新增命令	burst-mode: 系统视图下: burst-mode enable 说明：增大设备对网络突发流量的缓存能力。 下列特性相关的命令，详细参见随版本发布的各特

版本号	项目	描述
		性配置手册和命令手册。 1. Storm constrain 2. RRPP 保护 VLAN 可配 3. Smart link 4. 端口安全 5. 连通错误检测 6. 基于 VRRP 的 BFD 7. 堆叠管理(IRF Lite) 8. Track 联动功能 9. sFlow 10. VLAN Mapping 11. ARP detection 12. ARP snooping 13. System-guard 14. LLDP 15. arp rate-limit 16. GR 平滑重启 17. MFF 18. IP Source Guard 相关 19. mld-snooping drop-unknown
	删除命令	1. stp bpdu-transparent-forwarding 2. stp bpdu-tagged 3. bpdu-tunnel dot1q enable

版本号	项目	描述
	修改命令	1. 聚合配置命令： 全局下的 link-aggregation 命令 修改为 interface Bridge-Aggregation 2. Voice VLAN Voice VLAN id 的配置由全局视图改为端口视图可分别配置。 3. traffic classifier 命令 if-match dot1p 删除，修改为： if-match customer-dot1p 和 if-match service-dot1p 4. NQA 全局视图下删除 nqa STRING<1-32>， 修改为：nqa agent entry schedule server 5. level local-user 视图下，命令 level 删除，修改为 authorization-attribute level
S3610_5510-CMW520-R5303	新增命令	1. 端口下关闭VLAN入过滤检查命令： [undo] vlan-check disable 详细参见：命令手册-接入分册- QinQ 命令-1.1.6 vlan-check disable
	删除命令	无
	修改命令	无
S3610_5510-CMW520-F5302P01	新增命令	无
	删除命令	无
	修改命令	无

版本号	项目	描述
S3610_5510-CMW520-F5302	新增命令	1. 新增特性MCE 操作说明见《H3C S3610 系列以太网交换机命令手册》 2. 新增特性EAD快速部署 操作说明见《802.1X 命令手册》 3. 新增特性BFD for static route 操作说明见《H3C S3610 系列以太网交换机命令手册》 4. 新增特性Enable/disable vlan ingress filter 端口视图下： [undo] vlan-check ignored》 5. 新增bpdu tunnel相关特性 端口视图下： stp bpdu-transparent-forwarding 系统视图下： stp bpdu-transparent-forwarding vlan 端口视图下： stp bpdu-tagged 系统视图下： stp interface interface_list bpdu-tagged 6. 新增特性MAC地址同步 以太网接口视图 mac- mirroring < index > src-vlan < source_vlan_list > dest-vlan < destination_vlan_id > mac- mirroring < index > src-vlan < source_vlan_id > dest-vlan < destination_vlan_list > undo mac- mirroring { < index > }
	删除命令	无
	修改命令	无
S3610_5510-CMW520-R5301	新增命令	1. 增加高端内存操作命令 操作说明见《H3C S3610 系列以太网交换机命令手册》 2. 增加 ESFP 操作命令 display transceiver [manuinfo alarm] interface [STRING<1-256> STRING<1-256> STRING<1-256>]

版本号	项目	描述
		<code>display transceiver diagnosis interface [STRING<1-256> STRING<1-256> STRING<1-256>]</code> 操作说明见《H3C S3610 系列以太网交换机命令手册》 3. 增加特性 RRPP 操作说明见《H3C S3610 系列以太网交换机操作手册》 4. 增加特性 OAM 操作说明见《H3C S3610 系列以太网交换机操作手册》 5. 增加新特性 DLDP 操作说明见《H3C S3610 系列以太网交换机操作手册》
	删除命令	无
	修改命令	无
S3610_5510-CMW520-R0001P02	新增命令	无
	删除命令	1. 端口视图下删除如下命令： <code>[H3C-GigabitEthernet1/0/1]lacp enable</code> <code>[H3C-GigabitEthernet1/0/1]undo lacp enable</code> 命令所在模块：聚合模块 说明：由于静态聚合也支持 LACP 协议，不需要 <code>lacp enable</code> 命令，也完全可以代替纯动态 LACP 功能。
	修改命令	无
S3610_S5510-CMW520-R0001	新增命令	在系统视图下增加如下命令 <code>[H3C]switch-mode</code> 命令所在模块：系统管理 说明：设置设备工作的模块，是 IPV4 单栈模式，还是 IPV4,IPV6 双栈模式。在修改模式后，必须重启设备。
	删除命令	无。
	修改命令	无。
S3610_S5510-CMW520-E0001	新增命令	首次发布。
	删除命令	首次发布。
	修改命令	首次发布。

4.3 MIB 变更说明

表7 MIB 文件变更说明

版本号	项目	MIB 文件名 称	模块名	说明
S3610_5510- CMW520- R5309P02	新增	无		无
	修改	无		无

4.4 操作方式变更说明

4.4.1 CMW520-R5309P02 版本操作方式变更

无。

4.4.2 CMW520-F5305P02 版本操作方式变更

1. ip redirects enable 命令由默认开启变为默认关闭。
2. ip unreachable enable 命令由默认开启变为默认关闭。
3. NDP 协议使用的 MAC 地址默认变为 0180-C200-000A。

4.4.3 CMW520-R0001P02 版本操作方式变更

1. 删除动态聚合。

4.4.4 CMW520-R0001 版本操作方式变更

1. 添加了模式切换命令，模块切换后，需要重启设备。
2. qinq ethernet-type 命令移到端口模式下。

5 存在问题与规避措施

1. D08420

- 首次发现版本：CMW520-R0001
- 问题描述：对目的IP为E类地址范围的（240.0.0.0----255.255.255.255）PACKETS作了转发处理。

- 规避措施：配置ACL来实现过滤。

2. LSD05495

- 首次发现版本：CMW520-R0001
- 问题描述：普通终结手工隧道，link local 地址无法 ping 通 以及使用普通路由由终结时解封装后如果是组播报文，则该组播报文被丢弃。
- 规避措施：采用快速终结隧道方式。

6 解决问题列表

6.1 CMW520-R5309P02 版本解决问题列表

1. LSD36815

- 首次发现版本：CMW520- R5309
- 问题产生条件：

设备工作在 IPv6 模式，运行 OSPF v3 协议，并且与另一台设备建立 OSPF 邻居。然后，在本设备通过命令 qos vlan-policy 下发针对 VLAN 的 ACL。
- 问题现象：

两台设备的 OSPFV3 邻居关系变为 down。

2. LSD38325

- 首次发现版本：CMW520- R5309
- 问题产生条件：

S5510 设备上，在后 16 个端口中的一个或多个端口下发基于 time range 的 ACL。
- 问题现象：

有效时间段过后，ACL 不能删除。

3. ZDD02045

- 首次发现版本：CMW520- R5309
- 问题产生条件：

交换机开启 SNMP 功能。

- 问题现象：

某些交换机的 snmp local-engineid 相同，导致网管无法正常管理。

4. LSD38527

- 首次发现版本：CMW520- R5309

- 问题产生条件：

创建聚合组并包含成员端口，在 VLAN 视图下将聚合组划入该 VLAN 中。

- 问题现象：

聚合组中的成员端口并没有划入该 VLAN。

5. LSD38439

- 首次发现版本：CMW520- R5309

- 问题产生条件：

设备开启 LLDP 功能，与某些厂家的 VoIP Phone 连接。

- 问题现象：

无法建立 LLDP 邻居。

6. LSD40506

- 首次发现版本：CMW520- R5309

- 问题产生条件：

使用 ACL rule 规则定义 TCP flag 字段中的某个位如：ACK，其他位不关心。

- 问题现象：

若想被该 ACL 规则匹配，则实际报文中的 TCP flag 字段的未定义位必须为 0 才可以。

6.2 CMW520-R5309 版本解决问题列表

1. LSD37888

- 首次发现版本：CMW520- R5308

- 问题产生条件：

设备工作在低温环境中。

- 问题现象：

极少量设备转发出现少量 CRC 错包。

6.3 CMW520-R5308 版本解决问题列表

1. LSD32811

- 首次发现版本：CMW520- R5303

- 问题产生条件：

删除文件过程中，设备掉电。

- 问题现象：

FLASH 文件系统被破坏，启动文件损坏或丢失，导致设备不能启动。

2. LSD35029

- 首次发现版本：CMW520- R5306

- 问题产生条件：

端口切换到 Route 模式

- 问题现象：

该端口的接口视图下，不支持 NDP 配置。

3. LSD35505

- 首次发现版本：CMW520- R5306

- 问题产生条件：

VLAN 下发“允许 ICMP 报文及指定源 IP 地址和目的 IP 地址的 TCP 报文通过，其他 IP 报文禁止通过”的 ACL。

- 问题现象：

ICMP 报文可以通过，但 telnet 报文被丢弃。

4. LSD35657

- 首次发现版本：CMW520- R5306

- 问题产生条件：

设备同时使能 DHCP Snooping 和 VLAN Mapping。

- 问题现象：
VLAN Mapping 功能工作异常。

5. LSD36612

- 首次发现版本：CMW520- R5306
- 问题产生条件：
支持 802.3ad 协议 43.5 章节的 mark 协议的 PC 机使用网卡虚拟 LACP 聚合，ping 设备上的接口 IP 地址。
- 问题现象：
ping 结果统计，时延过大。

6. LSD36654

- 首次发现版本：CMW520- R5303
- 问题产生条件：
出厂软件版本为 R5303 的设备进行软件降级，降到 R5303 以前的版本。
- 问题现象：
降级失败。

7. LSD36699

- 首次发现版本：CMW520- R5306
- 问题产生条件：
设备使能 DHCP Relay。
- 问题现象：
下挂的能发送 DHCP Inform Message (option 53) 的 DHCP 的客户端 (如 Window Vista)，DHCP IP 地址申请失败。

8. LSD36871

- 首次发现版本：CMW520- R5306
- 问题产生条件：
设备配置了聚合组，聚合组中的端口的链路状态为 UP，此端口的对端 shutdown 掉或拔下网线。
- 问题现象：
聚合组中的相应端口变为 INACTIVE，但链路状态保持 UP。

6.4 CMW520-R5306 版本解决问题列表

无

6.5 CMW520-F5305P06 版本解决问题列表

1. LSD29079

- 首次发现版本：VRP520- F5305P02
- 问题产生条件：
使用 Bootrom135 或 Bootrom137 与 F5305P02 版本配套使用。
- 问题现象：
交换机不断重启。

2. LSD31267

- 首次发现版本：VRP520- F5305P02
- 问题产生条件：
交换机存在大量等价路由，且三层路由转发的流量比较多。
- 问题现象：
CPU 占用率偏高。

3. LSD31725

- 首次发现版本：VRP520- F5305P02
- 问题产生条件：
在端口下发策略为空的 qos policy。
- 问题现象：
该配置无法取消。

4. LSD32146

- 首次发现版本：VRP520- F5305P02
- 问题产生条件：
在端口上配置一条灵活 QinQ 的映射，再通过命令“undo raw-vlan-id inbound”取消映射，再配置另一条不同的 QinQ 映射，然后重新配置第一条灵活 QinQ 的映射。

- 问题现象：

第二条 QinQ 映射不生效。

5. LSD32434

- 首次发现版本：VRP520- F5305P02

- 问题产生条件：

CAMS 与交换机配合，并通过认证。

- 问题现象：

计费网管软件读取不到用户的 IP 地址。

6. LSD32577

- 首次发现版本：VRP520- F5305P02

- 问题产生条件：

个别 100M SFP 模块插入 100M SFP 接口。

- 问题现象：

无法识别模块类型，display interface 显示为 UNKNOWN_SFP。

6.6 CMW520-F5305P02 版本解决问题列表

1. LSD27375

- 首次发现版本：CMW520-R5303
- 问题产生的条件：使用 SNMP 的 MIB 工具对 ospfExtLsdbAdvertisement 节点进行 walk 操作。
- 问题现象：操作出现 timeout，设备 cpu 升高且持续一段时间。

2. LSD26450

- 首次发现版本：CMW520-R5301
- 问题产生的条件：使用 “ip route-static” 命令配置静态路由，如果目的 IP 地址和掩码相与后为 0.0.0.0，但掩码不为全 0，如：
`ip route-static 120.1.1.2 1 10.1.1.2`
- 问题现象：符合该网段的路由会走软件三层转发。

3. LSD27579

- 首次发现版本: CMW520-R5303

问题产生的条件: 设备仅配置 “telnet server enable”，通过集群命令交换机管理该设备，并创建 VLAN，但在 VLAN 视图下不做任何操作；或仅配置 VLAN1 接口 IP，及 Telnet 相关，然后通过 Telnet 方式远程登录到这台交换机，创建 VLAN，但在 VLAN 视图下不做任何操作。

- 问题现象: 通过 display current-configuration 命令会发现并没有这些 VLAN 的信息，这时如果保存配置，重启交换机，那么除 VLAN 1 之外的其他 VLAN 的相关信息都会丢失。

4. LSD27860

- 首次发现版本: CMW520-R5301
- 问题产生的条件: 设备插入 ESFP 光模块。
- 问题现象: 可能引起 CPU 升高。

5. LSD27408

- 首次发现版本: CMW520- R5303
- 问题产生的条件: 配置为集群命令交换机，在 cluster 视图下，反复进行 “build”、“undo build” 操作。
- 问题现象: 内存缓慢泄漏。

6. LSD00015

- 首次发现版本: CMW520-R5303
- 问题产生的条件: 通过命令行 “snmp-agent target-host trap ”
- 问题现象: 无法配置 IPV6 类型的目标主机。

7. LSD26273

- 首次发现版本: CMW520-R5303
- 问题产生的条件: 对于 S3610-52M 设备，在 combo SFP 口插入千兆电口模块，并与另一台设备相连，将该端口关闭（shut down），然后重启 S3610-52M。
- 问题现象: 重启后，对端设备与该 combo 口相连的端口处于 UP 状态。

8. LSD21330

- 首次发现版本: CMW520-R5303

- 问题产生的条件: 打开环路检测功能, 在端口上启用 QinQ , 当该端口下连接的网络存在环路时。
- 问题现象: 该端口无法检测到所有 VLAN 的环路。

9. LSD26473

- 首次发现版本: CMW520-R5303
- 问题产生的条件: 在端口上同时启用基本 QinQ 和灵活 QinQ, 如:

```
#  
interface Ethernet1/0/1  
port access vlan 800  
qinq enable  
qinq vid 900  
raw-vlan-id inbound all  
#
```

向该端口发送 vlan tag 的优先级不为 0 的报文。

- 问题现象: 报文没有被添加 vlan900 的外层 tag, 而是 vlan 800 的 tag。

10. LSD25635

- 首次发现版本: CMW520-R5303
- 问题产生的条件: 使用 IPv6 协议, 组网如: SW2-----SW1-----PC , 其中 SW1 和 SW2 之间配置 IPV6 接口, PC 与 SW1 通过隧道方式连接, 当 SW1 设备没有 SW2 接口 IP 的 ND 表项时。
- 问题现象: 从 PC 无法 ping 通 SW2 的接口 IP。

6.7 CMW520-R5303 版本解决问题列表

1. LSD23047

- 首次发现版本: CMW520-F5302P01
- 问题产生的条件: 两台 3500EA设备运行VRRP协议, 组成VRRP组, 同时打开debug tcp调试开关, 并且进行NQA测试。
- 问题现象: 可能导致VRRP状态切换。

2. HSD28837

- 首次发现版本: CMW520-F5302P01

- 问题产生的条件:两台IPv6 主机与本交换机相连，通过三层互通，其中一台主机与交换机建立ISATAP隧道，从该主机向对端主机PING大于 1432 字节的包。
- 问题现象: 无法PING通。

3. LSD24388

- 首次发现版本: CMW520-F5302P01
- 问题产生的条件:在交换机上启用EAD快速部署，在某端口启用DOT1X，并且通过添加静态MAC表允许该端口下的一台PC访问网络。
- 问题现象: 当从该PC上通过WEB页访问交换机的接口IP登录时，网页被重定向到指定的CAMS服务器上。

4. ZDD01560

- 首次发现版本: CMW520-F5302P01
- 问题产生的条件:在交换机上启用DHCP snooping，下挂的一台DHCP客户端通过交换机从DHCP server获取IP地址。
- 问题现象: 从DHCP客户端无法使用“slpinfo /d”命令获取Service Location信息。

5. ZDD01566

- 首次发现版本: CMW520-F5302P01
- 问题产生的条件:在交换机上启用OSPF，配置一条静态路由，且该路由的下一跳落在OSPF network指定的网段范围内，将静态路由引入OSPF，反复shut/undo shut相应的VLAN接口。
- 问题现象: 可能导致任务异常。

6. LSD24384

- 首次发现版本: CMW520-F5302P01
- 问题产生的条件: 在交换机上启用EAD快速部署，当进行了Free-ip等相关参数的配置后。
- 问题现象: 通过WEB页显示的“EAD quick deploy configuration”的相关信息不完整。

6.8 CMW520-F5302P01 版本解决问题列表

1. LSD20766

- 首次发现版本: CMW520-F5302
- 问题产生的条件: 在一个端口下配置多个IP子网VLAN。并配置IP地址。
- 问题现象: ping 不通IP子网VLAN的虚接口IP地址。

2. LSD21908

- 首次发现版本: CMW520-F5302
- 问题产生的条件: 交换机上同时存在AREA0 和NSSA区域，并且AREA0 中没有network网段。
- 问题现象: 交换机本身不应该是ABR路由器，但在NSSA区的其他路由器上错误的产生了到交换机的ABR路由。

3. ZDD01488

- 首次发现版本: CMW520-F5302
- 问题产生的条件: 接收到length字段为 0 的igmp报文。
- 问题现象: 对于length字段为 0 的igmp报文处理不当，导致死循环，设备重启。

4. ZDD01486

- 首次发现版本: CMW520-F5302
- 问题产生的条件: 当系统在线Telnet用户达到最大值后,新建telnet不成功。
- 问题现象: 将原telnet关闭后，新建telnet仍不可用。

6.9 CMW520-F5302 版本解决问题列表

1. LSD20368

- 首次发现版本: CMW520-R5301
- 问题产生的条件: 配置burst traffic 命令不能使用端口组模式
- 问题现象: 配置burst traffic 命令不能使用端口组模式

6.10 CMW520-R5301 版本解决问题列表

1. LSD11730

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：使能或者不使能二层组播。
- 问题现象：未知组播数据报文都在 **vlan** 内广播。

2. LSD15695

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：**tftp server** 与 **auto-config** 设备不在同一个网段的情况下。
- 问题现象：**auto-config** 功能不能实现。

3. LSD15851

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：端口起了 **voice vlan** 和 **security** 功能后。打入带 **voice** 所在 **vlan** 的 **tag** 标签的二层流，源 **mac** 不断变化，反复学习 **mac** 地址，然后 **down** 掉端口。
- 问题现象：出现软件和硬件的 **MAC** 表不一致。

4. LSD15852

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：两台设备直联，当端口 **pvid** 所属 **vlan** 不存在时。
- 问题现象：端口收不到 **mstp** 协议报文，造成根桥选举错误。

5. LSD15883

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：有较多 **mac** 地址时，显示 **mac** 地址。
- 问题现象：显示较多 **MAC** 时，显示完第一屏，按 **ctrl+c**，没有中断显示，而是又显示一屏。

6. LSD15888

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：在端口上配置流镜像，再配置端口镜像，然后删除端口镜像，再重新配置端口镜像。
- 问题现象：重新配置端口镜像失败。

7. LSD15927

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：GE 光口插入 100M 光模块。
- 问题现象：打印信息存在错误。

8. LSD16134

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：在设备上使能 DHCP-Snooping，全局和端口上使能 dot1x。
- 问题现象：pc 没有通过 dot1x 认证也获取到地址。

9. LSD18121

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：在需要插 SFP 的 combo 口上配置类型为 Tunnel 的聚合组，设备重启后。
- 问题现象：该配置无法下发成功。

10. LSD18489

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：100M 端口 link up 时，进行内部环回测试。
- 问题现象：内部环回测试不成功。

11. LSD19076

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：后面 4 个 Combo 口配置成 tunnel 口后，去掉 tunnel 配置。
- 问题现象：端口状态不能恢复为 up。

12. LSD19593

- 首次发现版本：CMW520-R0001P02
- 问题产生的条件：端口检测到环路。
- 问题现象：端口上配置的静态 mac 地址被删除。

6.11 CMW520-R0001P02 版本解决问题列表

1. LSD10803

- 首次发现版本：CMW520-R0001
- 问题产生的条件：MAC 地址存在，同时指定 VLAN 和 MAC 查看 MAC 地址。
- 问题现象：查找该 MAC 失败。

2. LSD12067

- 首次发现版本：CMW520-R0001
- 问题产生的条件：将一个千兆光口加入环回组后，在该光口插入一个光模块或电模块。
- 问题现象：导致环回组的环回被清掉，不能再正确实现环回

3. LSD14473

- 首次发现版本：CMW520-R0001
- 问题产生的条件：配置聚合 CAR 的 CBS 值。
- 问题现象：第一次配置不生效，再次配置才可生效。

4. LSD14489

- 首次发现版本：CMW520-R0001
- 问题产生条件：端口配置上 mac 地址学习最大数量为 1 时，对端口进行 shut 操作后，然后进行 undo shut。
- 问题现象：端口将不再学习 mac。

5. LSD14759

- 首次发现版本：CMW520-R0001
- 问题产生条件：端口配置的PVID在交换机上不存在时。
- 问题现象：环回检测状态错误。

6. LSD14877

- 首次发现版本：CMW520-R0001
- 问题产生条件：设备空配置启动后，un shut combo口（26 口，光口，有连线）。
- 问题现象：设备重复上报几次up/down。

6.12 CMW520-R0001 版本解决问题列表

1. LSD08297

- 首次发现版本：CMW520-E0001
- 问题产生条件：S3610 百兆光口插入千兆SFP模块。
- 问题现象：自环后会LINK UP。

2. LSD08697

- 首次发现版本：CMW520-E0001
- 问题产生条件：在设备间建立手工隧道，通过隧道ping 超过 1500 的大包。
- 问题现象：不能ping通。

3. LSD08877

- 首次发现版本：CMW520-E0001
- 问题产生条件：设备上创建web用户名为 80 个字符。
- 问题现象：使用web登录时最长只能输入 79 个字符。

4. LSD08949

- 首次发现版本：CMW520-E0001
- 问题产生条件：同时配置基本QINQ和灵活QINQ后。
- 问题现象：只有基本QINQ在起作用，灵活QINQ不起作用。

5. LSD09713

- 首次发现版本：CMW520-E0001
- 问题产生的条件：设备做ftp server，在client成功登陆后。
- 问题描述：dir/lis目录回显信息只有目录信息。

6. LSD10356

- 首次发现版本：CMW520-E0001
- 问题产生的条件：端口下配置qinq ethernet-type。
- 问题描述：更改ethernet-type超过两次后更改失败。

7. LSD11079

- 首次发现版本：CMW520-E0001
- 问题产生条件：使用web 登陆到我们的设备查看设备信息，

- 问题现象：web显示了内部版本号。

6.13 CMW520-E0001 版本解决问题列表

首次发布。

7 配套资料

7.1 配套资料清单

表8 配套手册清单

手册名称	资料版本
《H3C S3610 系列以太网交换机 快速入门》	(V1.06)
《H3C S3610 系列以太网交换机 安装手册》	(V1.06)
《H3C S3610[S5510]系列以太网交换机 操作手册-Release 5309》	6W100
《H3C S3610[S5510]系列以太网交换机 命令手册-Release 5309》	6W100
《H3C S5510 系列以太网交换机 快速入门》	(V1.04)
《H3C S5510 系列以太网交换机 安装手册》	(V1.04)

7.2 配套产品资料的获取方法

通过 H3C 网站查询和下载与该版本配套的产品资料，方法如下。

表9 从网站查询和下载资料的说明

如何申请帐号	首先，登录到 http:// www.h3c.com.cn 网站的主页；单击 [注册/登录]，然后输入用户名、密码，并单击<注册>即可。
如何获取产品资料	单击主页的 [文档中心]，然后即可按产品类别来查询资料； 选择产品后即可弹出相应的产品明细列表； 指定了设备类型后，即可选择与该产品相关的手册。

8 版本升级操作指导



注意：

请勿轻易进行交换机软件升级，如有必要最好在技术支持人员的指导下进行。

因为某些原因，在交换机使用过程中，需要对交换机的软件进行升级。

一般的，S3610&S5510 交换机软件升级采用串口升级方式，但该方式升级缓慢，很耗时间，而且升级时要么跑到交换机的工作位置去升级，要么将交换机集中收回，一台一台的升级，很耗人力，为解决这一问题，S3610&S5510 交换机引入 TFTP 及 FTP 模块，实现了软件升级与文件下载的快捷与灵活。该版本的 S3610&S5510 提供了更简便的升级方式，可通过命令行升级版本，重新启动交换机即可。

8.1 通过命令行远程升级

网络管理人员在本地计算机上运行 FTP Server，注意配置文件所在目录正确（假设 IP 地址为 10.10.110.1），Telnet 远程登录到交换机上，利用 FTP 将主机程序传送到交换机上，假设主机程序为 appfile.bin，BOOTROM 程序为 bootfile.btm，在用户视图下执行：

```
<H3C> ftp 10.10.110.1
```

```
Trying ...
```

```
Press CTRL+K to abort
```

```
Connected.
```

```
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(none):lyt
```

```
331 Give me your password, please
```

```
Password:
```

```
230 Logged in successfully
```

```
[ftp] get appfile.app appfile.app
```

```
[ftp] get bootfile.btm bootfile.btm
```

```
[ftp] bye
```

```
<H3C> boot bootrom appfile.btm
```

```
please wait ...
```

```
Bootrom is updated!
```

```
<H3C> boot boot-loader appfile.app
```

```
<H3C> display boot-loader
```

The app to boot at the next time is: flash:/ appfile.app

```
<H3C> reboot
```

通过以上命令即可完成主机软件升级。需要注意的是，升级主机软件必须通过 **reboot** 命令重起交换机才能使升级成功。

注意：如果 **Flash memory** 空间不够，可以首先完成 **BOOTROM** 的升级，然后再将主机程序通过 **FTP** 上载到交换机上完成主机程序的升级。

以下以 **S3610-52P** 为例介绍维护人员对交换机进行本地升级的常用方法。

8.2 BootRom 菜单

交换机上电后，将首先运行 **BOOTROM** 程序，终端屏幕上显示如下信息：

Starting.....

```
*****
*
*          H3C S3610-52P BOOTROM, Version 135          *
*
*****

Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd.
Creation date: Nov  9 2006, 16:46:58
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size      : 128MB

Initialize LSA1LTSG.....OK!
SDRAM fast selftest.....OK!
Flash fast selftest.....OK!
CPLD selftest.....OK!
Switch chip selftest.....OK!
Slot 1/1/1 has no module or get slot type error
Slot 1/1/2 has no module or get slot type error
Slot 1/1/3 has no module or get slot type error
Slot 1/1/4 has no module or get slot type error
PHY selftest.....OK!
```

Please check port leds.....finished!

The switch Mac is: 000F-E200-3900

Press Ctrl-B to enter Boot Menu... 5

此时，键入<Ctrl+B>，系统将进入 BOOT 菜单。

 说明：

必须在出现“Press Ctrl-B to enter Boot Menu...”的 5 秒钟之内，键入<Ctrl+B>，系统方能进入 BOOT 菜单，否则系统将进入程序解压过程；若程序进入解压过程后再希望进入 BOOT 菜单，则需要重新启动交换机。

系统提示：

Password :

要求输入 BOOTROM 密码，输入正确的密码后（交换机缺省设置为没有密码），系统进入 BOOT 菜单：

 注意：

交换机使用过程中，请牢记修改过的 BOOTROM 密码。

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9):

8.3 利用串口（Xmodem 协议）完成软件升级

第一步：在 BOOT 菜单中，键入<1>，回车后，系统进入下载程序菜单：

```
1. Set TFTP protocol parameter /设置 TFTP 协议参数/
2. Set FTP protocol parameter /设置 FTP 协议参数/
3. Set XMODEM protocol parameter /设置 XMODEM 协议参数/
0. Return to boot menu /返回 BOOT 菜单/
Enter your choice(0-3):3
```

第二步：在下载程序菜单中，键入<3>，选择采用 Xmodem 协议完成软件升级，回车后，系统界面如下：

Please select your download baudrate:

```
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return /返回下载程序菜单/
Enter your choice (0-5):
```

第三步：根据实际情况，选择合适的下载速率。若如上所示键入<5>，即选择 115200bps 的下载速率，回车后终端显示如下信息：

Download baudrate is 115200 bps. Please change the terminal's baudrate to 115200 bps, and select XMODEM protocol.

Press enter key when ready. /波特率更改完成后，请键入回车/

第四步：根据上面提示，改变配置终端设置的波特率，使其与所选的软件下载波特率一致，配置终端的波特率设置完成后，做一次终端的断开和连接操作，然后键入回车即可开始程序的下载，终端显示如下信息：

Now please start transfer file with XMODEM protocol.

If you want to exit, Press <Ctrl+X>. /若想退出程序下载/，请键入<Ctrl+X>
Loading ... CCCCC

 说明：

终端的波特率更改后，要进行一次终端仿真程序的断开和连接操作，新的设置才能起作用。

第五步：此时，从终端窗口选择[传送\发送文件]，在弹出对话框（如下图）中点击[浏览]按钮，选择需要下载的软件，并将下载使用的协议改为 Xmodem。



图1 [发送文件]对话框

第六步：点击[发送]按钮，系统弹出如下图所示界面。



图2 正在发送文件界面

第七步：程序下载完成后，系统界面如下：

Download completed.!

8.4 利用以太网口（FTP/TFTP 协议）完成软件升级

8.4.1 通过 TFTP 完成软件升级

本系列路由器提供的 TFTP 服务为 TFTP Client，即路由器作为 TFTP Client，文件服务器作为 TFTP Server，用户通过在终端输入相应命令，可将本路由器的配置文件或应用程序上传到文件服务器上，或从文件服务器下载配置文件或应用程序到路由器中。

1. TFTP 介绍

TFTP（Trivial File Transfer Protocol，简单文件传输协议）是 TCP/IP 协议族中一个用来在客户机与服务器之间进行简单文件传输的协议。

2. TFTP 应用

第一步：S3610 交换机选择一个用于下载的以太网口，交换机通过该接口与下载文件所在微机相连（需要知道该微机的 IP 地址），同时交换机通过配置口外接一台微机（此微机与下载文件所在微机可以是同一台）。

第二步：在与以太网口相连的微机上运行 TFTP Server 程序，并指定升级程序的文件路径。

注意：

H3C 系列交换机不随机提供 TFTP Server 程序。

第三步：在与配置口相连的微机上运行终端仿真程序，启动交换机，进入 BOOT 菜单。

第四步：在 BOOT 菜单中，键入<1>，回车后，系统进入下载程序菜单：

1. Set TFTP protocol parameter /设置 TFTP 协议参数/
2. Set FTP protocol parameter /设置 FTP 协议参数/
3. Set XMODEM protocol parameter /设置 XMODEM 协议参数/
0. Return to boot menu /返回 BOOT 菜单/

Enter your choice(0-3):1

第五步：在下载程序菜单中，键入<1>，选择采用 TFTP 协议完成软件升级，回车后，系统界面如下：

Please modify your TFTP protocol parameter:

Load File name /交换机要下载的文件名/

Switch IP address /本地 PC（或交换机等）的 IP 地址/

Server IP address /下载文件所在 PC（或交换机等）的 IP 地址/

第六步：根据实际情况，完成相关信息输入后回车，系统界面如下：

Are you sure to download file to flash? Yes or No(Y/N)

第七步：键入<Y>，系统开始文件下载；键入<N>，系统将返回 BOOT 菜单。以键入<Y>为例，回车后，开始程序加载，下载完成后，系统开始写 Flash（闪速存储器）的操作，当这一操作完成后，终端界面出现如下信息，表明下载完成：

Loadingdone

Writing to flash.....done

8.4.2 通过 FTP 完成软件升级

1. FTP 介绍

通过以太网口，S3610 交换机也可以通过 FTP 协议为用户提供另一种系统程序软件和配置文件的途径，下面举例进行说明。

2. FTP 应用

第一步：S3610 交换机选择一个用于下载的以太网口，交换机通过该接口与下载文件所在微机相连（需要知道该微机的 IP 地址），同时交换机通过配置口外接一台微机（此微机与下载文件所在微机可以是同一台）。

第二步：在与以太网口相连的微机上运行 FTP Server 程序，并指定升级程序的文件路径。

第三步：在与配置口相连的微机上运行终端仿真程序，启动交换机，进入 BOOT 菜单。

第四步：在 BOOT 菜单中，键入<1>，回车后，系统进入下载程序菜单：

1. Set TFTP protocol parameter /设置 TFTP 协议参数/

2. Set FTP protocol parameter /设置 FTP 协议参数/

3. Set XMODEM protocol parameter /设置 XMODEM 协议参数/

0. Return to boot menu /返回 BOOT 菜单/

Enter your choice(0-3):2

第五步：在下载程序菜单中，键入<2>，选择采用 FTP 协议完成软件升级，回车后，系统界面如下：

Please modify your FTP protocol parameter:

Load File name /交换机要下载的文件名/

Switch IP address /本地 PC（或交换机等）的 IP 地址/

Server IP address /下载文件所在 PC（或交换机等）的 IP 地址/

FTP User Name /登陆 FTP server 的用户名/

FTP User Password /登陆 FTP server 的用户口令/

第六步：根据实际情况，完成相关信息输入后回车，系统界面如下：

Are you sure to download file to flash? Yes or No(Y/N)

第七步：键入<Y>，系统开始文件下载；键入<N>，系统将返回 BOOT 菜单。以键入<Y>为例，回车后，开始程序加载，下载完成后，系统开始写 Flash（闪速存储器）的操作，当这一操作完成后，终端界面出现如下信息，表明下载完成：

Loadingdone

Writing to flash.....done