

H3C MSR20_30_50路由器CMW520-R1719-SI版本发布

一、使用范围及配套说明:

H3C MSR20_30_50路由器CMW520-R1719-SI版本是对外正式发布的版本, 主要解决CMW520-R1718-SI的各种网上问题, 发布范围不受限。

表1 MSR20_MSR30_MSR50-CMW520-R1719-SI版本配套表

产品	MSR20_30_50路由器	
型号	MSR20-1X MSR 20-20_MSR 20-21_MSR 20-40 MSR30-11 MSR 30-16 MSR30-20_MSR 30-40_MSR 30-60 MSR 50-40_MSR 50-60_MSR 50-40 MPU-G2_MSR 50-60 MPU-G2	
BOOTROM版本号	MSR20-1X: 209及以上版本 MSR 20-20_MSR 20-21_MSR 20-40: 308及以上版本 MSR30-11: 211及以上版本 MSR30-16: 207及以上版本 MSR 30-20_MSR 30-40_MSR 30-60: 307及以上版本 MSR 50-40_MSR 50-60: 306及以上版本 MSR 50-40 MPU-G2_MSR 50-60 MPU-G2: 115及以上版本	
目标文件名称	MSR20-1X: MSR201X-CMW520-R1719.BIN	MD5校验和: e4a0374309b8d2d3ef76ecd5eddc66a1
	MSR 20-20_MSR 20-21_MSR 20-40: MSR20-CMW520-R1719-SI.BIN	MD5校验和: e4a0374309b8d2d3ef76ecd5eddc66a1
	MSR 30-20_MSR 30-40_MSR 30-60: MSR30-CMW520-R1719-SI.BIN	MD5校验和: 9309708ab5354408efbe4e8ca99cc2d1
	MSR 50-40_MSR 50-60: MSR50-CMW520-R1719-SI.BIN	MD5校验和: 87d17ab963482f31e01b33f514c2fe23
	MSR 3011: MSR3011-CMW520-R1719-SI.BIN	MD5校验和: 59a985d99e69c8e68370f60affa22c3
	MSR 3016: MSR3016-CMW520-R1719-SI.BIN	MD5校验和: c843b0ecb943411b8bedf2d88f71b4aa
	MSR 50-40 MPU-G2_MSR 50-60 MPU-G2: MSR50-CMW520-R1719-EP USI.BIN	MD5校验和: cd044165cfd4e0fcb5ea83b392ad8989
DM版本号	H3C DM 3.10-R3125 + P04	
iMC版本号	iMC ACLM 3.20-R2602 iMC EAD 3.60-E6102 iMC ICC 3.20-R2602 iMC MVM 3.50-E5201 iMC PLAT 3.20-R2602 iMC UAM 3.60-E6102	
iNode版本号	iNode PC 3.60-E6104	
TTYD版本	TTYD配套版本4.27	

二、增减特性说明:

表2 特性变更说明

版本号	项目	描述
	硬件特性更新	无
		新增特性: 1. OSPFv3支持配置网络类型和参考带宽特性 目前OSPFv3接口的网络类型是根据物理接口类型而定的, 但是在一些实际组网应用中用户希望接口的网络类型能够根据实际需要进行调整。本特性实现手工配置OSPFv3的接口网络类型。 另外, 目前接口根据公式参考带宽 (bit/s) /实际带宽 (bit/s) 自动计算接口运行OSPFv3协议所需的cost, 得到的cost值小于1时取整为1, 其中参考带宽值固定为10000000 (bit/s) 不可修改。但是在各个接口的实际带宽都

版本号	项目	描述
CMW5 20-R1 719	软件特 性更新	<p>播流或者很小时，以目前固定的参考带宽值计算出来的cost值已经反映出接口间带宽的差异。本特性实现手工配置OSPFv3的接口参考带宽。</p> <p>2. EAD支持基于用户的QoS策略下发 EAD用户访问设备时，先进行身份认证。当认证通过时，认证服务器会将包含QoS策略的User Profile（需要事先在认证服务器上配置以及在设备上创建）下发给用户。当用户下线时，系统会自动取消通过User Profile下发的QoS策略。该特性能实现针对不同用户灵活下发QoS策略。</p> <p>3. 建行终端接入加密特性 该特性（Etelnet）实现连接串口终端的路由器与建行ccb telnet程序之间采用Telnet协议进行通信，同时支持AES和RC4两种加密算法。数据加密的密钥获取及保证密钥的安全等遵从建行终端安全传输项目规定的技术规范和要求的。</p> <p>4. RIP支持BFD RIP协议依赖周期性发送路由作为检测机制，当在指定时间内没有收到路由更新时，认为此条路由不再生效。这种方式不能快速响应链路故障。BFD的出现给RIP解决这一缺陷的方法：BFD检测链路是否正常，当链路出现故障时通知RIP协议，RIP协议让从此链路发送过来的路由不再生效，从而快速切换到备份路由。 RIP支持BFD实现了两种检测方式：控制报文方式和echo报文方式。直连邻居采用echo报文方式，非直连邻居采用control报文方式。</p> <p>5. QoS支持流速统计 本特性对经过QoS分类的报文流的发送和丢弃报文个数和速率进行统计，统计时间间隔可以通过命令进行设置，统计结果可以通过display qos policy interface命令或MIB显示。</p> <p>6. SIP消息等待指示业务</p> <div data-bbox="470 840 949 929" data-label="Diagram"> </div> <p>本特性遵循RFC3842，实现了具有主动通知功能的消息等待指示业务，能与符合标准的MWI业务服务器互通。当有目的方为用户A的呼叫转至语音邮箱后，如果语音邮箱的状态发生改变，服务器会通知路由器上的用户A；如果有用户A的新留言或者语音邮件等新消息，那么当用户A摘机时，就会听到消息等待指示音。</p> <p>7. 交换卡VLAN口支持网桥 该特性实现将VLAN接口加入到指定的网桥中。加入网桥后的VLAN接口，收到VLAN报文后，会根据网桥表中的对应关系，将报文转发到网桥中其他的接口上。</p> <p>8. EtoPPP和EtoFR特性 EtoPPP&EtoFR特性可以实现不同链路层协议二层转换功能，支持从以太网到PPP协议的二层转换以及从以太网到FR协议的二层转换，实现了高性能的不同类型链路间的报文的二层交换。</p> <p>9. NAT DNS-map特性 在路由器的公网接口上，通过nat server命令配置内部服务器，可将公网地址、端口等映射到私网内的服务器上，公网用户可通过域名或公网地址，访问内部服务器。在私网没有DNS服务器的条件下（DNS服务器在公网），通过配置DNS map可实现私网用户直接通过域名访问内部服务器的功能需求。</p> <p>10. SIP支持三方会议 本特性支持组织召开三方参与的会议功能，只支持FXS语音用户线下的设置，使能三方会议业务。只有主板上带VPM插槽的款型支持该特性。</p> <p>11. 语音Busyout特性 本特性通过“监控本地WAN接口网络层状态或远端IP地址是否可达”来判断语音设备是否可以和对端建立连接。如果发现不可以建立连接，则将相应的VE1/VT1接口置为Watch-Out状态。接口处于该状态时，PBX设备无法向该接口进行呼叫，可选择其它的备份链路进行拨号。</p> <p>12. NQA增强 本特性新增了语音测试类型、扩大UDP-Jitter测试规格、Server回应支持TOS选项、单向延迟和乱序统计等功能。</p> <p>13. USB 3G Modem特性 路由器能通过USB接口外接3G Modem，接入3G移动网络，支持数据业务传输，作为主链路的备份链路。</p> <p>14. BGP支持4字节AS号特性 该特性符合RFC4893，BGP协议的AS号支持4个字节。</p> <p>15. ARP防攻击特性 本特性主要由如下ARP防攻击子特性组成： ARP用户的合法性检查（基于DHCP Snooping的安全表项）； ARP报文限速； ARP报文有效性检查； 源MAC地址固定的ARP攻击检测； ARP源MAC一致性检查功能； ARP主动确认机制。</p> <p>16. FXO接口CID检测增强</p>

版本号	项目	兼容性可以兼容多种标准的CID，增强了实际组网能力；支持带极性反转的第一声振铃前的CID检测，第一声振铃和第二声振铃间的CID检测以及第二声振铃和第三声振铃间的CID检测。
		删除特性：无。

表3 命令行变更说明

版本号	项目	描述
		<p>1. 命令： rip bfd enable undo rip bfd enable 视图：接口视图 参数： 无 描述： rip bfd enable命令用来使能BFD提供的链路检测功能。undo rip bfd enable命令用来恢复缺省情况。RIP去使能接口的BFD功能会通知BFD删除相应的会话。缺省情况下，RIP下的接口不使用BFD提供的链路检测功能。 RIP的邻居是单跳的概念，适合采用BFD的echo单向检测方式，但是，经过多跳到达邻居时echo方式则会失效。 由于peer命令与邻居之间没有对应关系，undo peer操作并不能立刻删除邻居，因此不能立刻删除BFD会话。 举例 # 在接口Ethernet1/1使能RIP的BFD功能。 <Sysname> system-view [Sysname] interface ethernet 1/1 [Sysname-Ethernet1/1] rip bfd enable</p>
		<p>2. 命令： mwi enable undo mwi enable 视图：语音用户线视图 参数： 无 描述： mwi enable命令用来使能消息等待指示功能。undo mwi enable命令用来关闭消息等待指示功能。缺省情况下，消息等待指示功能处于关闭状态。该命令只适用于FXS语音用户线。 举例： # 在语音用户线3/0下使能消息等待指示功能。 <Sysname> system-view [Sysname] voice-setup [Sysname-voice] subscriber-line 3/0 [Sysname-voice-line3/0] mwi enable</p>
		<p>3. 命令： configuration encrypt { private-key public-key } undo configuration encrypt 视图：系统视图 参数： private-key：使用私有密钥进行加密。加密后的配置文件只有本设备能够解密和识别。 public-key：使用公有密钥进行加密。加密后的配置文件可以被所有支持配置文件加密功能的设备解密和识别。 描述： configuration encrypt命令用来使能配置文件加密功能。undo configuration encrypt命令用来恢复缺省情况。 缺省情况下，配置文件加密功能处于禁用状态，即直接将当前生效的配置保存到配置文件中。 使能该功能后，每次执行save操作，都会先将当前的生效的配置进行加密，再保存到配置文件中。 当使用private-key参数时，保存在主主控板上的配置文件使用主主控板的私钥加密，只有该主主控板可以解密；保存在备用主控板上的配置文件使用备用主控板的私钥加密，只有该备用主控板可以解密。（分布式设备） 当使用private-key参数时，保存在成员设备上的配置文件使用各成员设备自己的私钥加密，只有该成员设备可以解密。（集中式堆叠设备） 当使用private-key参数时，保存在主控板上的配置文件使用各主控板自己的私钥加密，只有该主控板可以解密。（分布式堆叠设备） 本命令的支持情况与设备的型号有关，请以设备的实际情况为准。 举例： # 设置保存配置文件时使用公有密钥进行加密。 <Sysname> system-view [Sysname] configuration encrypt public-key</p>

版本号	项目	描述
CMW520-R1719	新增命令	<p>4. 命令: nat dns-map domain <i>domain-name</i> protocol <i>pro-type</i> undo nat dns-map domain <i>domain-name</i> 视图: 系统视图 参数: domain <i>domain-name</i>: 指定内部服务器的合法域名。其中, <i>domain-name</i>表示内部服务器的域名, 为不超过255个字符的字符串, 不区分大小写, 由一个或者多个label组成, 两个label间由"."分隔, 每个label最长为63个字符, 必须由字母或数字开头, 由字母或数字结尾, 中间字符可以是字母、数字或连字符"-"。 protocol <i>pro-type</i>: 指定内部服务器支持的协议类型。其中, <i>pro-type</i>表示具体的协议类型, 取值为tcp或udp。 ip <i>global-ip</i>: 指定内部服务器提供给外部网络访问的IP地址。其中, <i>global-ip</i>表示公网IP地址。 port <i>global-port</i>: 指定内部服务器提供给外部网络访问的服务端口号。其中, <i>global-port</i>表示服务端口号, 取值范围为1~65535。 描述: nat dns-map命令用来配置一条域名到内部服务器的映射。undo nat dns-map命令用来删除一条域名到内部服务器的映射。 需要注意的是, 目前设备最多可支持16条域名到内部服务器的映射。 相关配置可参考命令display nat dns-map。 本命令的支持情况与设备的型号有关, 请以设备的实际情况为准。 举例: # 某公司内部对外提供Web服务, 内部服务器的域名为www.server.com, 对外的IP地址为202.112.0.1。配置一条域名到内部服务器的映射, 使得公司内部用户可以通过域名访问内部Web服务器。 <Sysname> system-view [Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port www</p> <p>5. 命令: call-watch group <i>watch-number</i> { hard / soft } undo call-watch group <i>watch-number</i> [hard / soft] 视图: E1/T1接口视图 参数: <i>watch-number</i>: 所属监控组序号, 取值范围为1~255。 hard: 关联的方式为hard, 监控到本地链路网络层down后, 不管对应的E1/T1接口下是否存在呼叫, 均将E1/T1接口置为Watch-Out状态。 soft: 关联的方式为soft, 监控到本地链路网络层down后, 如果对应的E1/T1接口存在呼叫, 则不将E1/T1接口置为Watch-Out状态, 否则将接口置为Watch-Out状态。 描述: call-watch group命令用来指定接口与监控组关联, 并可以选择关联的方式。undo call-watch group命令用来取消接口与监控组关联。 缺省情况下, 没有接口与监控组关联。 需要注意的是: 一个接口只能与一个监控组关联; 如果监控组不存在, 命令行也可以进行配置, 只是不会生效。 举例: # 指定接口E1 1/0与监控组1关联, 关联的方式为soft方式。 <Sysname> system-view [Sysname] controller e1 1/0 [Sysname-e1 1/0] call-watch group 1 soft</p>

版本号	项目	描述
		<p>6. 命令： etopp translate interface <i>interface-type1 interface-number1 interface-type2 interface-number2</i> ip-address <i>ip-address1 ip-address2</i> undo etopp translate interface <i>interface-type1 interface-number1</i> 视图：系统视图 参数： <i>interface-type1 interface-number1</i>：接口类型和接口编号。 <i>interface-type2 interface-number2</i>：接口类型和接口编号。 <i>ip-address1</i>：与设备的接口<i>interface-type1 interface-number1</i>相连的对端的IP地址。 <i>ip-address2</i>：与设备的接口<i>interface-type2 interface-number2</i>相连的对端的IP地址，和<i>ip-address1</i>应该在同一网段。 描述： etopp translate命令用来在指定的两个接口间建立一条报文转换的通道。undo etopp translate命令用来取消两个接口间建立的报文转换的通道。 缺省情况下，没有建立报文转换的通道。 相关配置可参考命令display etopp translate。 举例： # 创建从Ethernet1/1到Serial2/0的EtoPPP映射。 <Sysname> system-view [Sysname] etopp translate interface ethernet 1/1 serial 2/0 ip-address 1.1.1.1 1.1.1.2</p>
		<p>7. 命令： conference enable undo conference enable 视图：语音用户线视图 参数： 无 描述： conference enable命令用来配置三方会议功能。undo conference enable命令用来恢复缺省情况。 缺省情况下，三方会议功能处于关闭状态。 ! 三方会议功能依赖于呼叫保持功能，所以只有使能呼叫保持后才能成功配置三方会议。 ! 在语音用户线下启用三方会议业务命令将使已经配置的智能识别本地呼叫功能失效。相关配置可参考命令distinguish-localtalk。 举例： # 在语音用户线1/0下配置三方会议功能。 <Sysname> system-view [Sysname] voice-setup [Sysname-voice] subscriber-line 1/0 [Sysname-voice-line1/0] conference enable</p>
		<p>8. 命令： codec-type { g711a g711u g729a } undo codec-type 视图：Voice测试类型视图 参数： g711a：G.711 A律语音编码格式。 g711u：G.711 μ律语音编码格式。 g729a：G.729 A律语音编码格式。 描述： codec-type命令用来配置语音测试的编码格式。undo codec-type命令用来恢复缺省情况。 缺省情况下，语音编码格式为G.711 A律。 举例： # 配置Voice测试的语音编码格式为G.729 A律。 <Sysname> system-view [Sysname] nqa entry admin test [Sysname-nqa-admin-test] type voice [Sysname-nqa-admin-test-voice] codec-type g729a</p>
		<p>9. 命令： ddns policy <i>policy-name</i> undo ddns policy <i>policy-name</i> 视图：系统视图 参数： <i>policy-name</i>：DDNS策略名称，为1~32个字符的字符串，不区分大小写。 描述： ddns policy命令用来创建DDNS策略，并进入DDNS策略视图。undo ddns policy命令用来删除DDNS策略。 缺省情况下，未创建任何DDNS策略。 相关配置可参考命令display ddns policy。 举例： # 创建名称为steven_policy的DDNS策略，并进入DDNS策略视图。 <Sysname> system-view [Sysname] ddns policy steven_policy [Sysname-ddns-policy-steven_policy]</p>

版本号	项目	描述
		<p>10. 命令:</p> <pre>address sip { dns domain-name [port port-number] ip ip-address [port port-number] proxy } undo address sip { dns ip proxy }</pre> <p>视图: VoIP语音实体视图</p> <p>参数:</p> <p>dns domain-name: 被叫实体的域名, 为1~20个字符的字符串, 不区分大小写, 字符串中可以包含字母、数字、“-”、“_”或“.”。</p> <p>port port-number: DNS服务器的端口号, 取值范围为1~65535, 缺省值为5060。</p> <p>ip ip-address: 被叫的IP地址, 即VoIP语音实体的呼叫目的地址。</p> <p>port port-number: 端口号, 取值范围为1~65535, 缺省值为5060。</p> <p>proxy: 采用SIP代理服务器完成SIP消息交互过程。</p> <p>描述:</p> <p>address sip用来配置语音实体采用SIP选路方式。undo address sip用来取消已有配置。</p> <p>缺省情况下, 没有配置选路方式。</p> <p>举例:</p> <pre># 为VoIP语音实体10配置静态IP地址3.3.3.3。 <Sysname> system-view [Sysname] voice-setup [Sysname-voice-dial] entity 10 voip [Sysname-voice-dial-entity10] address sip ip 3.3.3.3 # 为VoIP语音实体10配置域名为cc.news.com。 <Sysname> system-view [Sysname] voice-setup [Sysname-voice-dial] entity 10 voip [Sysname-voice-dial-entity10] address sip dns cc.news.com</pre> <p>相关命令行变更详细信息请参见: 《H3C MSR 20/30/50系列路由器 用户手册》</p>
	删除命令	无
	修改命令	无

三、相比前一版本解决的问题说明:

1. RTD32154

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 带无线模块的MSR20-1X, 把设备的ETH0/0和VLAN-interface接口加入同一个桥组。

I 问题现象: 报文经过ETH0/0和VLAN-interface接口转发的时候会丢包。

2. RTD32324

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 路由器上启动portal认证, portal server发送portal request_info报文给路由器。

I 问题现象: 如果request_info报文中userIP在路由器上的状态为在线用户, 路由器不处理request_info报文。

3. RTD31926

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 启用路由器的日志功能, 并且在路由器上配置SNMP community参数。

I 问题现象: 查看日志信息会显示SNMP community的明文。

4. HSD44946

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 对路由器的ISDN接口进行TBR3测试。

I 问题现象: TBR3 Layer 3 test case TC12501 测试项目无法通过。

5. HSD44947

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 对路由器的ISDN接口进行TBR4测试。

I 问题现象: 路由器收到STATUS ENQUIRY消息, 回复STATUS应答, 导致TBR4某些测试项目无法通过。

6. RTD32392

I 首次发现版本: CMW520-R1718

I 问题产生的条件: 路由器的VLAN接口加入桥组, 并使能DLSw功能。

I 问题现象: DLSw电路无法通过VLAN接口正常建立。

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《H3C MSR20_MSR30_MSR50-CMW520-R1719-SI 版本说明书》

该公告已归档到知识案例库，归档ID号为16580

如有问题，请联系华三通信技术有限公司服务热线：4008100504/8008100504。