MSR路由器 SSH登录 + RSA认证功能的配置 关键词: MSR;SSH;Stelnet;RSA 一、组网需求: MSR开通SSH服务, 主机通过RSA认证方式SSH登录到MSR 设备清单: MSR路由器1台 二、组网图: MSR E0/0 1.0.0.1/24 三 配置步骤: 设备和版本: MSR、Version 5.20, Beta 1105。 MSR配置命令1 //MSR生成1024位的rsa本地密钥对 [MSR]rsa local-key-pair create The range of public key size is (512 ~ 2048). NOTES: If the key modulus is greater than 512, It will take a few minutes. Input the bits in the modulus[default = 512]:1024 Generating keys... .....+++++++ .....+++++++ .....++++++++ .....++++++++ Done! [MSR] MSR配置命令2——粘贴客户端SSHKey.exe转换好的公钥 //粘贴主机生成rsakey格式的1024位公钥,命名为msr [MSR]rsa peer-public-key msr You already have RSA public key named msr. RSA public key view: return to System View with "peer-public-key end". //开始引入公钥 [MSR-rsa-public-key]public-key-code begin RSA key code view: return to last view with "public-key-code end". //将主机的公钥粘贴至命令行 [MSR-rsa-key-code]30818602 818062CF E079DC75 0296B626 17B90530 3470676C [MSR-rsa-key-code]1475FEB5 13DC9A54 07DA9A63 F5EE69B8 82CF15E3 1835FDF2 [MSR-rsa-key-code]C527F1B4 11278117 2F7B8BDE 65EFFF78 6C0A885D 10A93315 [MSR-rsa-key-code]204A2C12 81636A4C 5541941F 33813E77 08F11EDD D7B1336C [MSR-rsa-key-code]ABBD81C6 7A97C3FF 84A465F2 274D5F22 AEF1B0CD E46FC791 [MSR-rsa-key-code]17DC4A54 A3E0ACA9 2FC36652 9DBB0201 25 //完成公钥粘贴 [MSR-rsa-key-code]public-key-code end //完成公钥文件生成 [MSR-rsa-public-key]peer-public-key end MSR配置命令2——直接引入客户端KeyGen.exe生成的公钥 //通过文件引入方式引入公钥,要求主机的sshkey格式公钥文件下载到路由器 [msr]rsa peer-public-key msr import sshkey msr MSR关键配置脚本

# //并岩砂墨田白粉量为5	
configure-user count 5	
#	
rsa peer-public-key msr	
308186	
028180	
69B882CF 15E31835 FDF2C527 F1B41127 81172F7B 8BDE65EF FF786C0A 8	A63F5EE
3315204A 2C128163 6A4C5541 941F3381 3E7708F1 1EDDD7B1 336CABBD 8	31C67A97
C3FF84A4 65F2274D 5F22AEF1 B0CDE46F C79117DC 4A54A3E0 ACA92FC3	8 66529DBB
25	
public-key-code end	
#	
interface Ethernet0/0	
port link-mode route	
#	
//SSH服务器配置,	
ssh server enable	
ssh user client1 assign rsa-key msr	
//SSH登录用户client1及对应的认证类型为rsa	
ssn user client1 authentication-type rsa //SSH田户client1的服务类型为stelnet 即安全Telnet	
ssh user client1 service-type stelnet	
#	
//vtv登录用户需要进行aaa认证	
authentication-mode scheme	
//指定登录用尸的级别 user privilege level 3	
#	
Puttv制作公钥对并登录示意	
打开PuttyGen.exe,根据下图配置好参数,如选择生成SSH2 RSA密钥,密钥长度	
1024, 然后点击Generate	
PuTTY Key Generator	
Public and private key generation for PuTTY	
Ney No keu	
Actions	
Generate a public/private kev pair	
Load an evicting private key tile	
Load an existing private key hie Load	
Load an existing private key file Load   Save the generated key Save public key	
Load an existing private key file Load   Save the generated key Save public key   Parameters Save file	
Load an existing private key hile Load   Save the generated key Save public key   Parameters   Type of key to generate:   C SSH2 DSA	
Load an existing private key hile Load   Save the generated key Save public key   Parameters Save private key   Type of key to generate: SSH1 (RSA)   SSH1 (RSA) SSH2 RSA   Number of bits in a generated key: 1024	

点击Generate后,开始生成密钥对,在这个过程中需要鼠标在红框内反复移动

Key Please generate some randomness by moving	the mouse over the bla	ink area.
Please generate some randomness by moving	the mouse over the bla	ink area.
		K
Actions		
Actions Generate a public/private kev pair		Generate
Actions Generate a public/private key pair		<u>G</u> enerate
Actions Generate a public/private key pair Load an existing private key file		<u>G</u> enerate Load
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Save p <u>u</u> blic key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Save <u>pu</u> blic key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:	Save pyblic key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate: SSH1 (RSA)	Save p <u>u</u> blic key	Generate Load Save private key H2 DSA

密钥对生成之后会有一些显示信息,我们需要保存公钥和私钥,分别有对应的按钮Sa ve public key和Save private key

ITTY Key (	Generator	×
ublic and private key	generation for PuTTY	
<ey< th=""><th></th><th></th></ey<>		
Public key for pasting	g into OpenSSH authorized_keys	2 file:
ssh-rsa AAAAB3NzaC1yc2E KpnQUxW6w3F3Dt wELUYWeC7SupKe YKc= rsa-key-20060	:AAAABJQAAAIEAIR20E9G8PR; Oodprh8sy3JVJjJ4VW2EtCuILW/ ir+pgws+zSka2/b0RpAJb+W/3zs J926	gsbzRU3lfxYB4GWbjDvuJM2vYa iG15zPsuVv+x+KINVP1Kmuaz0Yj yt0AT1mMzURsFejHMKR+CG16
Key fingerprint:	ssh-rsa 1024 7e:62:4d:d7:57:	4e:2a:8f:72:e6:d5:59:b0:b8:54:0d
Key <u>c</u> omment:	rsa-key-20060926	
Key p <u>a</u> ssphrase:		
C <u>o</u> nfirm passphrase:		
Actions		
Generate a public/pi	ivate key pair	<u>G</u> enerate
Load an existing priv	ate key file	Load
Save the generated	key Sav	e pyblic key
<u></u>		
'arameters		
Parameters Type of key to gener OSSH <u>1</u> (RSA)	ate:	C SSH2 <u>D</u> SA

保存公钥,注意公钥名称和保存目录,这个保存的公钥可以直接上传到路由器,路由器直接使用rsa peer-public-key进行引入即可,可以不用进行转换等工作

Save publ	ic key as:		?×
保存在 (I):	🗁 SSH-putty	💽 G 🔊 🛤 🗖	
表最近的文档 () 変面 表的文档 () 変更 () () () () () () () () () ()	Codekey.exe Modified.txt Original.txt Original_IPv6_FIB.txt pc Putty.exe puttygen.exe sshkey.exe		
我的电脑 () 网上邻居	文件名 @): msr 保存类型 []: All Files	× ×	保存(5) 取消

保存私钥时有警告,这是因为没有配置私钥的访问密码,这没有关系,选择"是"

PuTTYger	n Warning	×
Ar w	re you sure you want to save this ke ithout a passphrase to protect it?	y .
	是(Y) 否(N)	
注意私钥文件	名和保存目录	_
Save priva	ate key as:	<u>?</u> ×
保存在 (I):	SSH-putty	] G 🕫 🛤 🖬 🖛
表最近的文档	CodeKey.exe Modified.bt Original.bt Original_IPv6_FIB.bt Putty.exe Sputty.gen.exe sshkey.exe	
我的电脑 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	文件名 @): pc 保存类型 (I): All Files	▼ 保存 (S) ▼ 取消

通过PuttyGen生成的公钥是不能直接用来**粘贴**的,必须转换,使用工具SSHKey.exe ,点击浏览选择公钥文件,点击"转换"

ssn key convert		-
SSH公钥文件名:	浏览 (2)	结束②
转换后的RSA公钥		
	<u>_</u>	转换 (2)
		保存(2)
	<b>_</b>	
转换前SSH格式公钥		
		-

绿框内为转换前的公钥,上面为转换后的RSA公钥,点击保存将转换后的公钥保存



保存好转换后的公钥就可以让路由器进行**粘贴**工作了,在路由器成功**粘贴**公钥或**引入** 工作并配置好SSH User,PC就可以使用SSH进行登录了,此时需要打开Putty.exe, 如下图所示指定SSH服务器(MSR)的地址,端口,然后到左边目录树的SSH->Auth

gory:				
Session 🖌	Basic o	ptions for your PuTTY	session	
Logging -	- C			
Terminal	Specily your con	nection by nost name t	I I D i	
- Keyboard	Host Name (or IF	<sup>2</sup> addressj	Port	- 10
Bell	1.0.0.1		22	
i Features	Protocol:		-	
Window	C Baw C	<u>T</u> elnet C Rlogin		
Appearance			_	
Behaviour	Load, save or de	elete a stored session		
- Translation	Saved Sessions		_	
Selection				
Colours	Default Settings		Load	
Connection	5452			-
- Data	5455		Sa <u>v</u> e	
Proxy	0406			-
Telnet			Delete	
Hlogin				
E SSH				
Kex	Close window or	n exit:		
Auth	C Always C	Never 📀 Only o	n clean exit	
Tunnola	-			
i di ineis	_			
About			Cancel	
 h页面中, 需要;	选择私钥,如下图	Upen 图所示,然后就可	」 可以点击Op	Den登
 uth页面中,需要: PuTTY Conf	选择私钥,如下图 figuration	 图所示,然后就可	可以点击Op	 pen登
 uth页面中,需要 PuTTY Conf	选择私钥,如下图 figuration	Upen 图所示,然后就可	可以点击Op	 )en登
uth页面中,需要 PuTTY Conf egory:	选择私钥,如下图 figuration	型pen 图所示,然后就可 controlling SSH authe	可以点击Op ntication	 pen登
uth页面中,需要: PuTTY Conf egory: Session Logging	选择私钥,如下图 f <b>iguration</b>	型pen 图所示,然后就可 controlling SSH authe ethods	可以点击Op ntication	」) Den登
uth页面中,需要: PuTTY Conf egory: 	选择私钥,如下图 figuration	型pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS	可以点击Op ntication H-1)	 Den登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Period	选择私钥,如下图 Figuration	型pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive'' auth	TUL点击Op 可以点击Op ntication H-1)	 pen登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features	选择私钥,如下图 figuration ①	型pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth	可以点击Op 可以点击Op ntication H-1) n (SSH-2)	Den登
uth页面中,需要: PuTTY Conf egory: - Session - Logging - Terminal - Keyboard - Bell - Features - Window	选择私钥,如下图 Figuration Options Authentication m Attempt TIS 不 Attempt "key Authentication pu	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters	可以点击Op ntication H-1) h(SSH-2)	Den登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Apprearance	选择私钥,如下留 figuration Options Authentication m Attempt TIS 又 Attempt "key Authentication pp Authentication pp	型pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive" auth arameters forwarding	TUL点击Op TUL点击Op ntication H-1) 1(SSH-2)	Den登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour	选择私钥,如下留 figuration ①ptions	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna	可以点击Op ntication H-1) h (SSH-2) me in SSH-2	Den登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation	选择私钥,如下的 figuration Options Authentication m Attempt TIS Attempt "key Authentication p Authentication p Authentication p Allow agtent Bivate key file fr	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS bioard-interactive" auth arameters forwarding ted changes of userna ar authentication;	可以点击Op 可以点击Op ntication H-1) n(SSH-2) me in SSH-2	 pen登
uth页面中,需要: PuTTY Conf agory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection	法择私钥,如下图 figuration Options Authentication m □ Attempt Tis ○ Attempt "key Authentication p. □ Allow agent [ □ Allow atemp Private key file fr [D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive'' auth arameters forwarding ted changes of userna re-authentication; H-putty/pc	ptication htication H-1) h(SSH-2) me in SSH-2	Den登
uth页面中,需要: PuTTY Conf agory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours	选择私钥,如下图 figuration Options Authentication m Authentication m Authentication pu Authentication pu Allow agent j Private key file for D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty/pc	TUL点击Op 可以点击Op ntication H-1) n(SSH-2) me in SSH-2	Den 登
uth页面中,需要: Putty Conf egory: Session - Logging Terminal - Keyboard - Bell - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection	选择私钥,如下图 figuration Options Authentication m Authentication pr Attempt TIS t 不 Attempt "key Authentication pr Allow agent t Allow attemp Prixate key file fr D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive" auth arameters forwarding ted changes of userna ar authentication; H-puty/pc	T以点击Op T以点击Op ntication H-1) n(SSH-2) me in SSH-2	Den 登
uth页面中,需要: PuTTY Conf agory: - Session - Logging - Terminal - Keyboard - Bell - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection - Data	选择私钥,如下留 figuration Options Authentication m Authempt Tiss Authentication pu Authentication pu Authentication pu Authentication pu Authentication pu Division agent f Division the second	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty\pc	T以点击Op 可以点击Op ntication H-1) h(SSH-2) me in SSH-2	Den登
uth页面中,需要: PutTTY Conf egory: - Session - Logging - Terminal - Keyboard - Bell - Features - Window - Appearence - Behaviour - Translation - Selection - Colours - Colours - Connection - Data - Proxy	选择私钥,如下的 figuration Options Authentication m Authentication pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Authentication pr Authentication pr Authentication pr Authentication pr Construction pr Authentication pr Construction pr Authentication pr Construction	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna ar <u>authentication</u> H-putty\pc	TU以点击Op 可以点击Op ntication H-1) n (SSH-2) me in SSH-2	
Uth页面中,需要: PutTTY Conf agory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet	选择私钥,如下图 figuration Options Authentication m Authentication p 不 Attempt "key Authentication p Authentication p Authentication p Authentication p Private key file fr D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive'' auth arameters forwarding ted changes of userna in authentication; H-putty/pc	TU以点击Op 可以点击Op ntication H-1) n(SSH-2) me in SSH-2	
uth页面中,需要: PuTTY Conf egory: - Session - Logging - Terminal - Keyboard - Bell - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection - Data - Proxy - Teihet - Riogin	选择私钥,如下图 figuration Options Authentication m Authentication pr Attempt TIS V Attempt "key Authentication pr Allow agent J Allow attemp Private key file for D:\software\SS	Upen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive'' auth arameters forwarding ted changes of userna an authentication; H-putty/pc	TUL点击Op TUL点击Op ntication H-1) n(SSH-2) me in SSH-2	jeen ∰
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Appearance Bell Features Window Colours Colours Constain Proxy Tennet Blogin Bell Selection Colours Colours Constain Proxy Tennet Blogin Bell Colours	选择私钥,如下图 figuration Options Authentication m Authentication pr Attempt TIS t 不 Attempt "key Authentication pr Allow agent f Private key file fr D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty\pc	可以点击Op 可以点击Op ntication H-1) h(SSH-2) me in SSH-2	jeen ∰
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin E SSH	选择私钥,如下图 figuration Options Authentication m Authentication p Authentication p	Upen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty\pc	TU以点击Op 可以点击Op ntication H-1) n(SSH-2) me in SSH-2	Deen 登
uth页面中,需要: PutTY Conf egory: - Session - Logging - Terminal - Keyboard - Bell - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Colours - Connection - Data - Proxy - Telnet - Riogin - SSH - Kex - Auth	选择私钥,如下图 figuration Options Authentication m Authentication p 不 Attempt "key Authentication p Authentication p Authentication p Authentication p Construct the set of	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive'' auth arameters forwarding ted changes of userna ar authentication; H-putty/pc	ntication H-1) n(SSH-2) me in SSH-2	Deen 登
uth页面中,需要: PuTTY Conf egory: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telett Rlogin BSH Kex	选择私钥,如下图 figuration Options Authentication m Authentication pu 不 Attempt Tis 不 Attempt Tis Authentication pu Allow agent j Allow agent j D:\software\SS	Upen 图所示, 然后就可 controlling SSH authe ethods or CryptoCard auth (SS iboard-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty/pc	ntication H-1) h(SSH-2) me in SSH-2	
th页面中,需要: PuTTY Conf pory: Session Logging Terminal Keyboard Peatures Window Appearance Behaviour Translation Selection Connection Data Proxy Telnet Rogin SH Kex Auth Tunnels	选择私钥,如下图 figuration Options Authentication m Authentication m Attempt TIS V Attempt "key Authentication pu Allow agent ] Private key file for D:\software\SS	型Pen 图所示,然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive" auth arameters forwarding ted changes of userna ar authentication H-putty/pc	TUL点击Op 可以点击Op ntication H-1) n(SSH-2) me in SSH-2	
	选择私钥,如下图 figuration Options Authentication m Authentication pu Authentication pu Authentication pu Authentication pu Authentication pu Authentication pu Authentication pu Authentication pu Software VSS	Upen 图所示, 然后就可 controlling SSH authe ethods or CryptoCard auth (SS board-interactive" auth arameters forwarding ted changes of userna ar authentication; H-putty\pc	TUL点击Op 可以点击Op ntication H-1) h(SSH-2) me in SSH-2 【Erowse.	→ pen ⅔

四、**配置关键点**:

1) MSR上需要生成本地密钥对;

2) PC上也需要生成RSA密钥对,如使用Putty自带的PuttyGen + SSHKey;

3) MSR上可以通过文件引入SSH格式的公钥,也可以通过文字粘贴RSA格式的公钥,

即MSR配置命令2可以各选其一;

4) SSH为特定用户指定其公钥;

5) 将登录用户认证类型改为rsa。