

MSR系列路由器L2TP使用Shiva进行认证及地址分配功能的配置

丘子隽 2007-01-27 发表

MSR系列路由器

L2TP使用Shiva进行认证及地址分配功能的配置

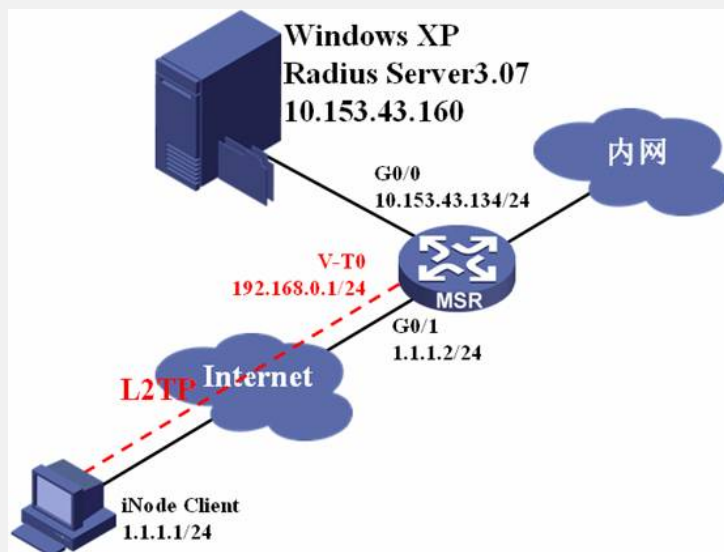
关键字: MSR;L2TP;Shiva;AAA;Radius;地址分配;iNode

一、组网需求:

MSR作为LNS服务器和NAS服务器, 对接入的iNode进行Radius认证, 并使用Radius服务器配置的地址分配给iNode, Radius服务器使用Shiva3.07

设备清单: MSR系列路由器1台

二、组网图:



三、配置步骤:

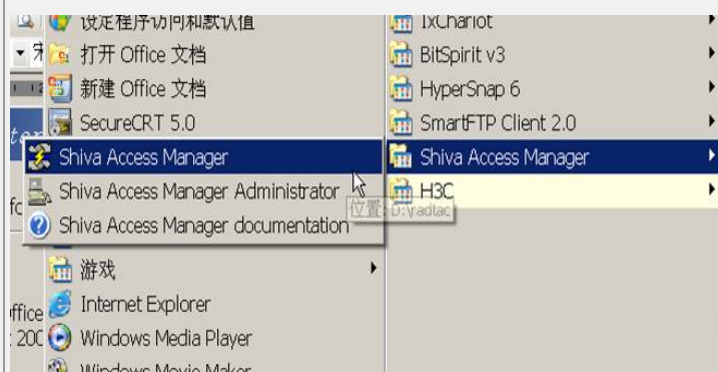
适用设备和版本: MSR系列、Version 5.20, Beta 1202后所有版本。

Center配置

```
#
//使能L2TP
l2tp enable
#
//配置Radius方案shiva
radius scheme shiva
server-type standard
//配置主认证服务器地址和端口1645
primary authentication 10.153.43.160 1645
//主计费服务器地址和端口
primary accounting 10.153.43.160 1646
//认证密码为h3c, 注意要与Shiva服务器配置一致
key authentication h3c
//计费密码为h3c, 注意要与Shiva服务器配置一致
key accounting h3c
//可以选择认证用户名不带域名, 此时Shiva服务器上配置用户不带用户名
user-name-format without-domain
#
//配置域h3c.com
domain h3c.com
//配置PPP认证方案shiva
authentication ppp radius-scheme shiva
//配置ppp授权方案shiva
authorization ppp radius-scheme shiva
//配置ppp计费方案shiva
accounting ppp radius-scheme shiva
access-limit disable
state active
idle-cut disable
self-service-url disable
#
//配置L2TP组1
l2tp-group 1
//取消隧道验证, 要与iNode配置一致
undo tunnel authentication
//配置LCP重协商, 可选配置
mandatory-lcp
//绑定的虚模板
allow l2tp virtual-template 0
#
//虚模板配置
interface Virtual-Template0
//配置ppp认证方式, 必须配置, 否则无法触发认证
ppp authentication-mode pap
//虚模板地址
ip address 192.168.0.1 255.255.255.0
#
//连接Shiva服务器的接口
interface GigabitEthernet0/0
port link-mode route
ip address 10.153.43.134 255.255.255.0
#
//连接iNode客户端的接口
interface GigabitEthernet0/1
port link-mode route
ip address 1.1.1.2 255.255.255.0
#
```

Shiva配置

1、安装好Shiva3.07后打开Shiva Access Manager



2、输入用户名supermanager, 密码空后Login



3、选择Start Console Now, 打开控制台



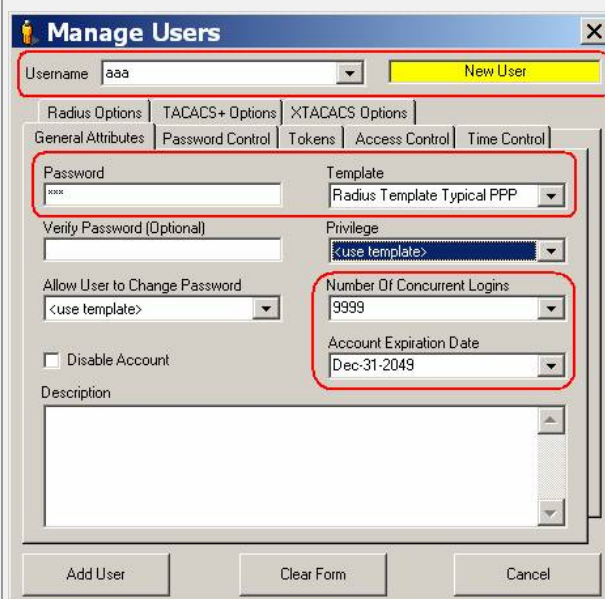
4、继续输入用户名supermanager，密码空后Login



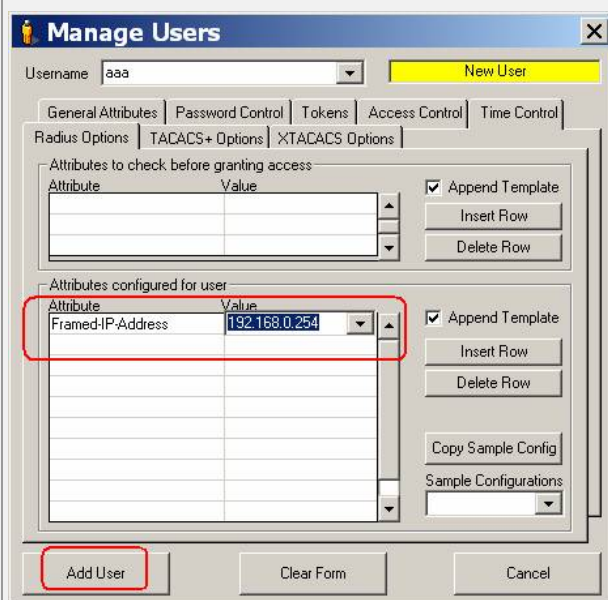
5、然后就可以对Shiva服务器进行配置了



6、菜单UseràManage Users进行添加用户aaa，注意下图中红框配置



7、上图中提示aaa是一个New User，密码也设置为aaa，Number Of Concurrent Logins设置为9999以便反复测试，Account Expiration Date设置为Dec-31-2049否则会失败，估计是Shiva的千年虫问题，之后打开Radius Options属性页



Manage Users

Username: New User

General Attributes | Password Control | Tokens | Access Control | Time Control

Radius Options | TACACS+ Options | XTACACS Options

Attributes to check before granting access

Attribute	Value

☒ Append Template

Insert Row Delete Row

Attributes configured for user

Attribute	Value
Framed-IP-Address	192.168.0.254

☒ Append Template

Insert Row Delete Row

Copy Sample Config

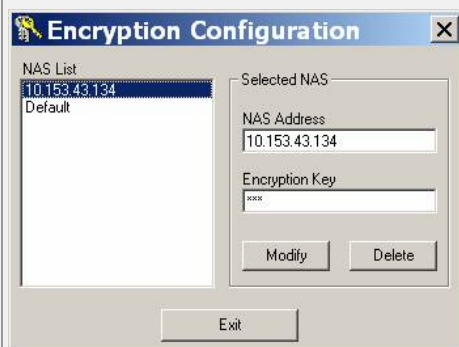
Sample Configurations:

Add User Clear Form Cancel

8、在填好IP地址后就可以Add User了，这时用户就已经添加完毕，此时打开如下菜单进行NAS的配置



9、配置NAS地址10.153.43.134及MSR路由器的地址，将Encryption Key设置为h3c，和MSR上配置保持一致



Encryption Configuration

NAS List

10.153.43.134
Default

Selected NAS

NAS Address:

Encryption Key:

Modify Delete

Exit

10、可以通过如下方法检查Shiva的端口信息，可以看到认证端口1645、计费端口1646



General Options

Misc Configuration

☐ Disable Start Up Login

Temp User Lifetime (days) 90

Change Password Prefix ##

RADIUS Protocol Configuration

Authentication UDP Port 1645

Accounting UDP Port 1646

TACACS+ Protocol Configuration

Username:

iNode配置
1. 创建了一个连接名叫h3c.com的L2TP Over IPsec连接

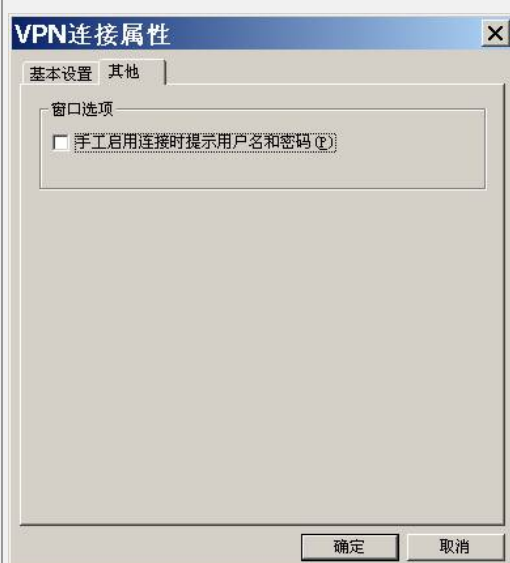


2、查看属性页配置，密码是aaa和Shiva服务器上配置保持一致，高级配置中添加隧道名称，由于没有隧道验证，所以可以任意

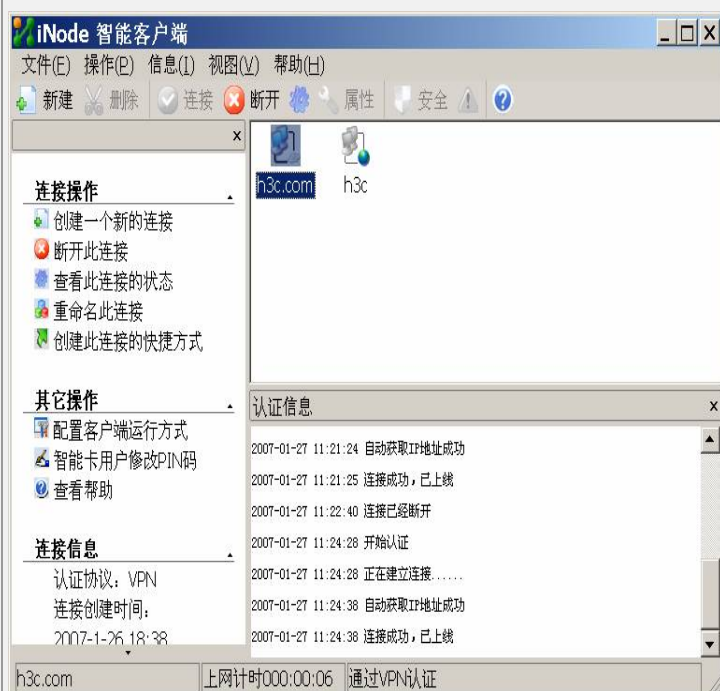




3、查看VPN连接属性的其他页中把勾去掉，测试更省事



4、点击连接，之后可以发现连接成功，上线了



四、配置关键点：

1) iNode与Shiva在用户名、密码配置上保持一致，MSR和Shiva在NAS配置验证字、端口等保持一致。