



..... 8

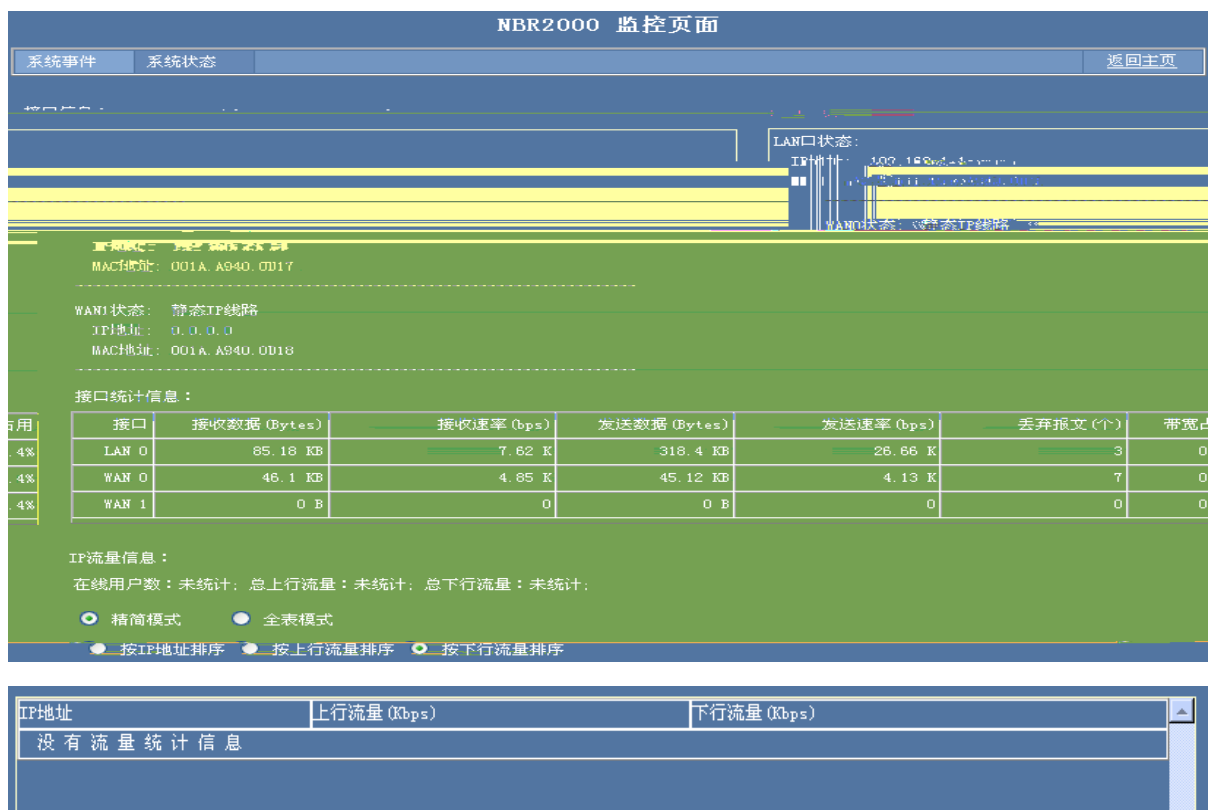
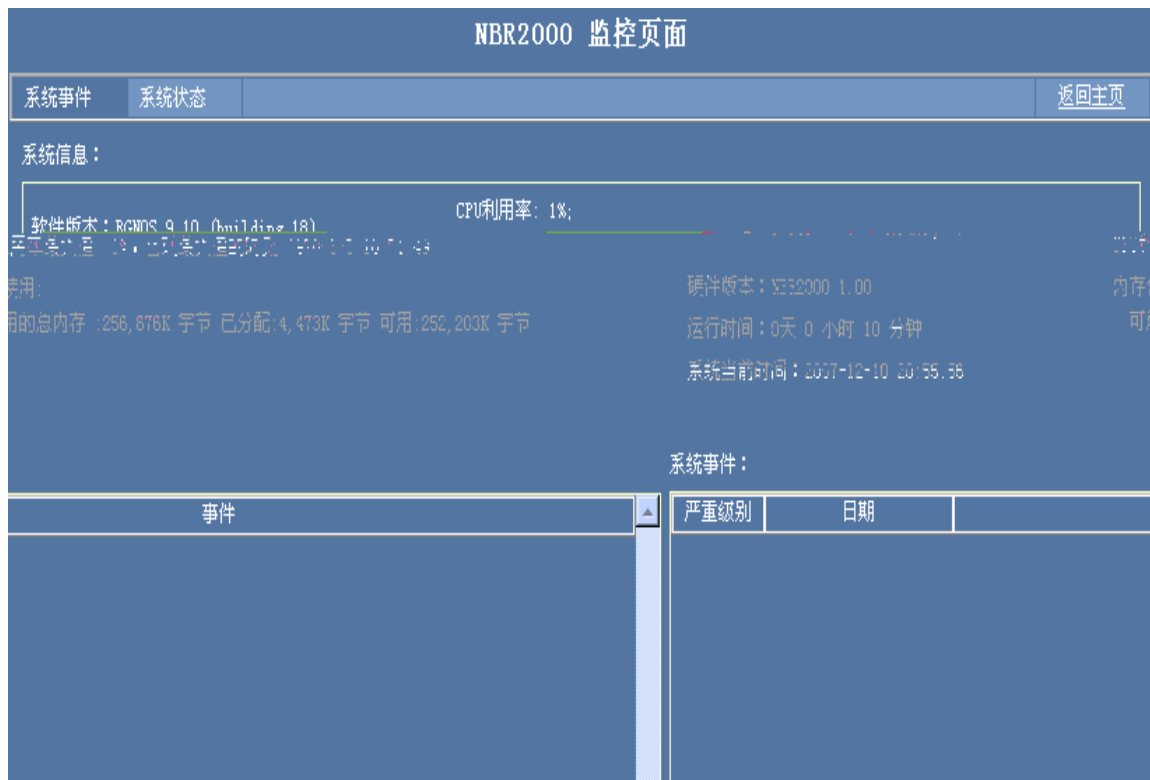


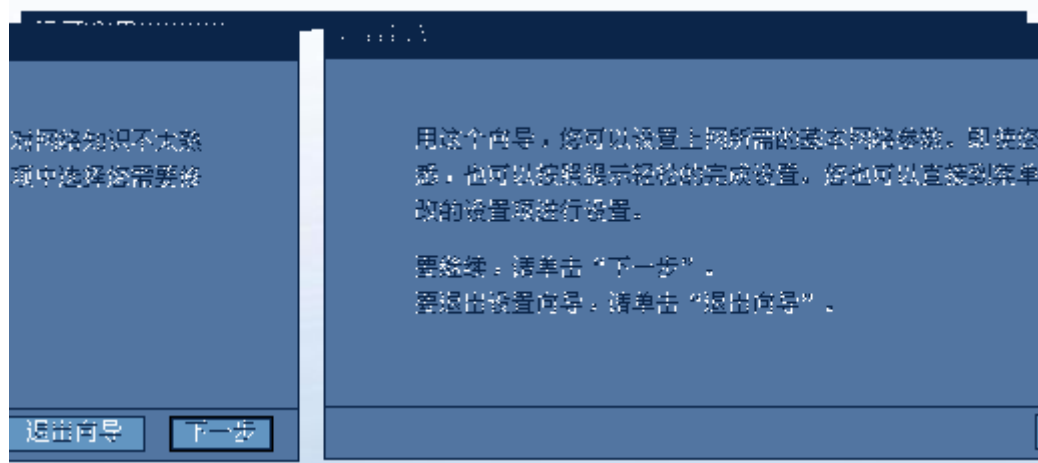
NBR9.10 部署：

1. NBR 部署在核心交换机上，通过配置 NBR 的 IP 地址，实现 NBR 与核心交换机的连接。
2. 在核心交换机上配置 NBR 的 IP 地址，并配置 NBR 的接口。
3. 在 NBR 上配置 IP 地址，并配置 NBR 的接口。
4. 在 NBR 上配置 NAT 规则，实现 NBR 与核心交换机的连接。
5. 在 NBR 上配置 NAT 规则，实现 NBR 与核心交换机的连接。
6. 在 NBR 上配置 NAT 规则，实现 NBR 与核心交换机的连接。
7. 在 NBR 上配置 NAT 规则，实现 NBR 与核心交换机的连接。
8. 在 NBR 上配置 NAT 规则，实现 NBR 与核心交换机的连接。

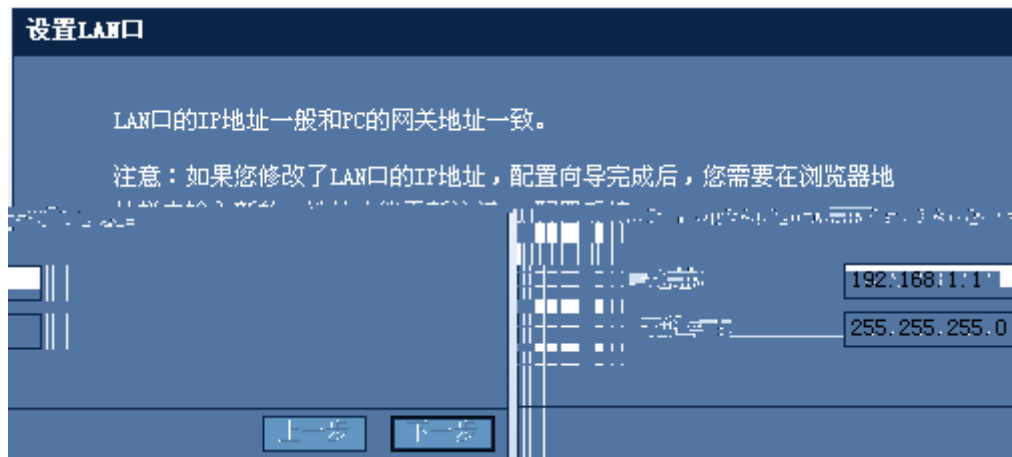
配置 web

IE 浏览器访问 NBR 的 IP 地址，配置 NBR 的 WEB 页面。

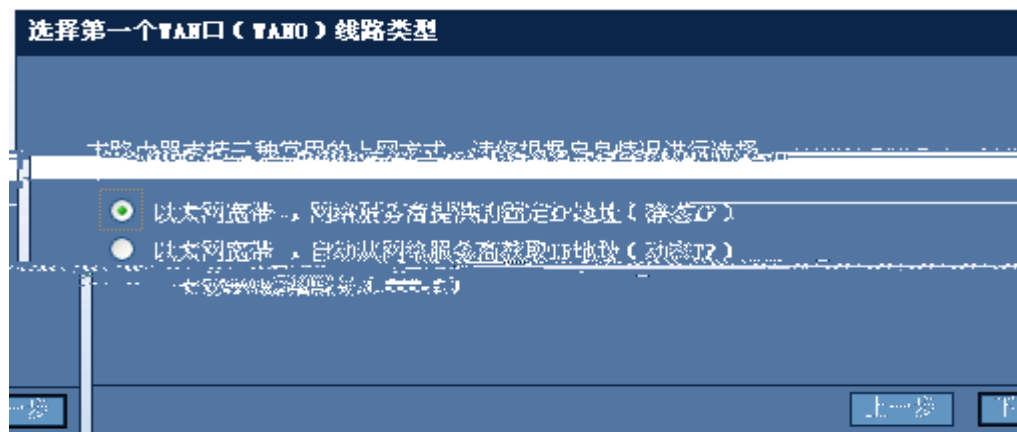




LAN IP 192.168.1.1 子网掩码 255.255.255.0



WAN IP 192.168.1.1 子网掩码 255.255.255.0



WAN IP 192.168.1.1 子网掩码 255.255.255.0



$\gamma \sim \tau$ LAN o WAN0 o
 $\sim \gamma \mathcal{D}_p$ “ ” $\sim \gamma \mathcal{D}_p$ “ ” k
 $\psi \sim \mathcal{D}_p$ “ ” i r WAN o $\mathcal{D}_p$ “
 ”

为第二线路（WAN1）设置动态获取IP（DHCP）

第二线路（WAN1）设置为动态获取IP（DHCP）。如果要继续，单击“下一步”，如果要修改设置，单击“上一步”。

上一步

下一步

↑ A ↓ D_p “ ” D_p “ ”

k

设置完成

配置向导已经完成配置，您的配置如下：

LAN口配置：

IP: 192.168.1.1

掩码: 255.255.255.0

WAN0配置：

IP: 222.103.128.100

掩码: 255.255.255.0

网关: 222.103.128.254

WAN1配置：

以太网宽带，自动从网络服务商获取IP地址（动态IP）

上一步

完成

4 PPPOE ~

“ADSL ~ PPPOE” D_p “ ”

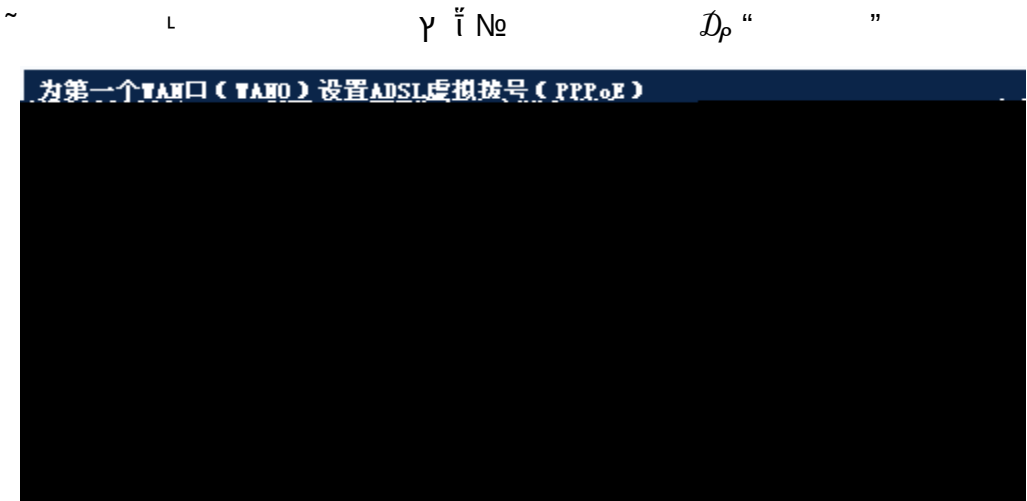
选择第一个WAN口（WAN0）线路类型

本路由器支持三种常用的上网方式，请您根据自身情况进行选择。

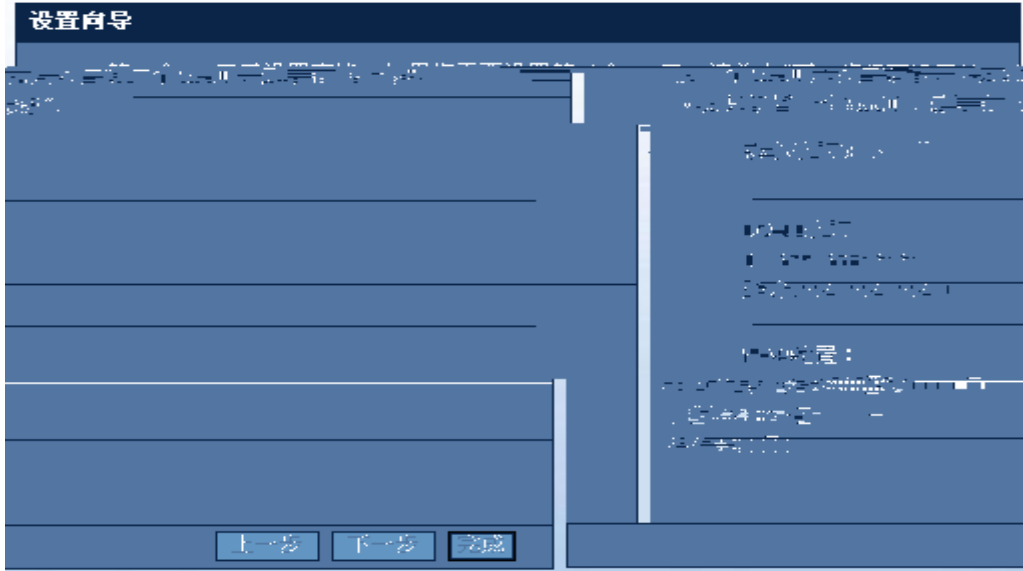
- ☐ 以太网宽带，网络服务商提供的固定IP地址（静态IP）
- ☐ 以太网宽带，自动从网络服务商获取IP地址（动态IP）
- ☒ ADSL虚拟拨号（PPPoE）

上一步

下一步



↓ A ↓ Dp “ ” Dp “ ” k



Dp “ ”





7 0

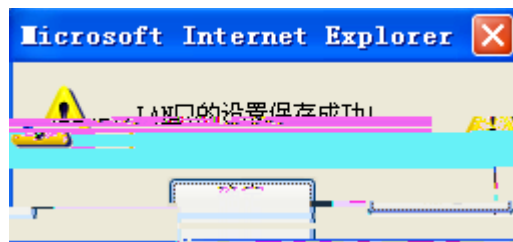
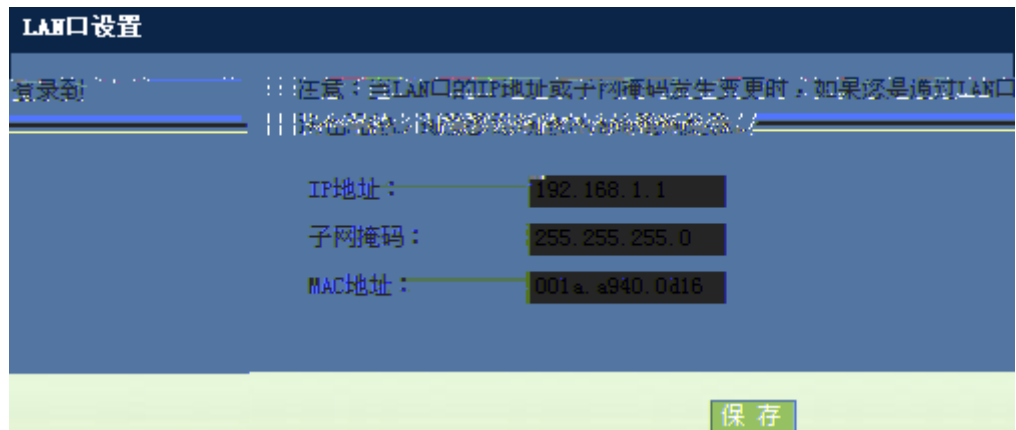
1. LAN

6 k LAN o IP

ĩ MAC

Đp “ Ġ ” ^

a k



2. WAN

“ WAN ”



~ D_p " $\bar{G}$ " Ψ $\bar{G}$ w D_p "

”



PPPoE ~ k " ~ " $\bar{i}$ " " $\bar{i}$ T " " G

$\downarrow$ a v



IP 地址 子网掩码 网关 动态 IP

WAN口设置

设置WAN口的基本网络参数。

请选择WAN口: WAN1

请选择WAN口线路类型: 动态IP

IP地址: 刷新

子网掩码:

网关:

DNS地址1:

DNS地址2:

保存

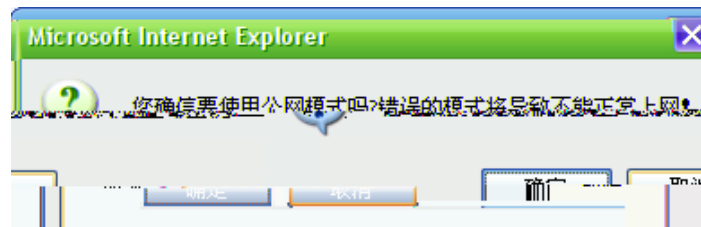
3.

公网模式

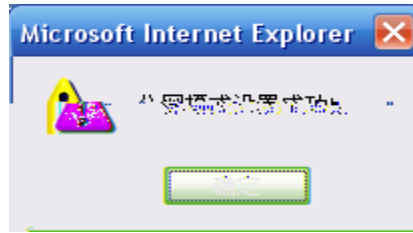
说明: 公网模式会删除WAN模式下的相关命令, 进入公网模式后, 若需更改WAN口配置, 需重新进入WAN模式下的配置页面进行配置。

公网模式 进入公网模式

公网模式 公网模式



公网模式 公网模式



4.

o 38 o "E G I No “



5. WAN

TAB口线路检测



注意：防火墙规则是有先后顺序的，排在前面的规则会优先匹配。如果策略条目很多，操作时间会相对变长。

设备	设备	设备	设备	设备	设备
设备	top	设备	设备	设备	1000
设备	top	设备	设备	设备	445
设备	ip	设备	设备	设备	设备

“ ψ ” G ψ $\uparrow$
 $\top$ $\downarrow$ $\top$ $\uparrow$ $\sim$ $\uparrow$ “ — ” “ ” “ ” $\mathbf{b}$
 ψ $\uparrow$ $\neg$ $\int$ β $\sim$ D_p “ $\neg$ ” a $\uparrow$
G **$\uparrow$** **γ** **$\models$** **$\neg$** **$\top$** **γ** **$\int$** **$\uparrow$**

[illegible]

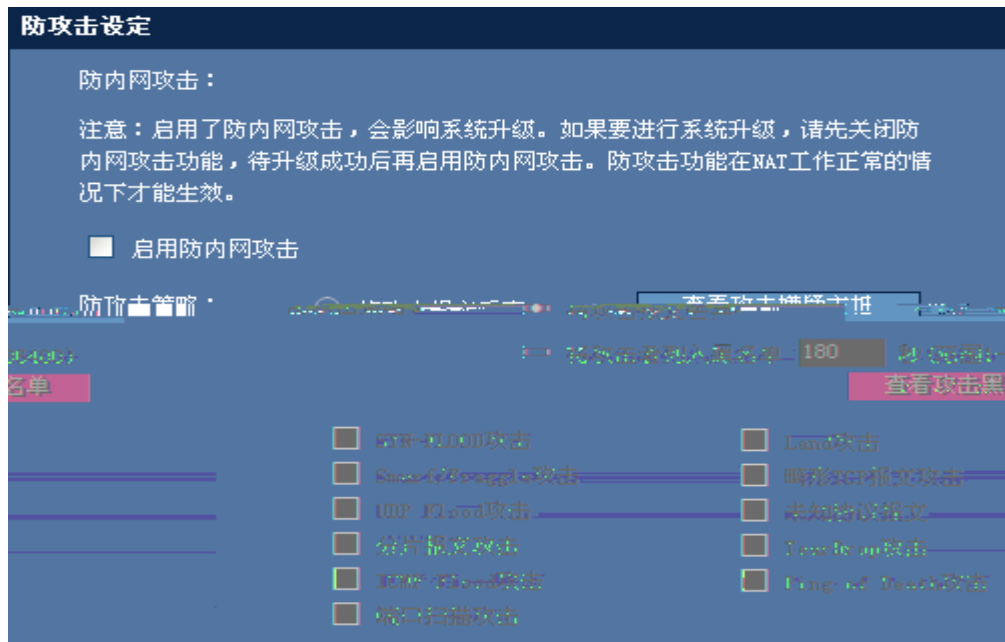


8.

D_p “ ” PC

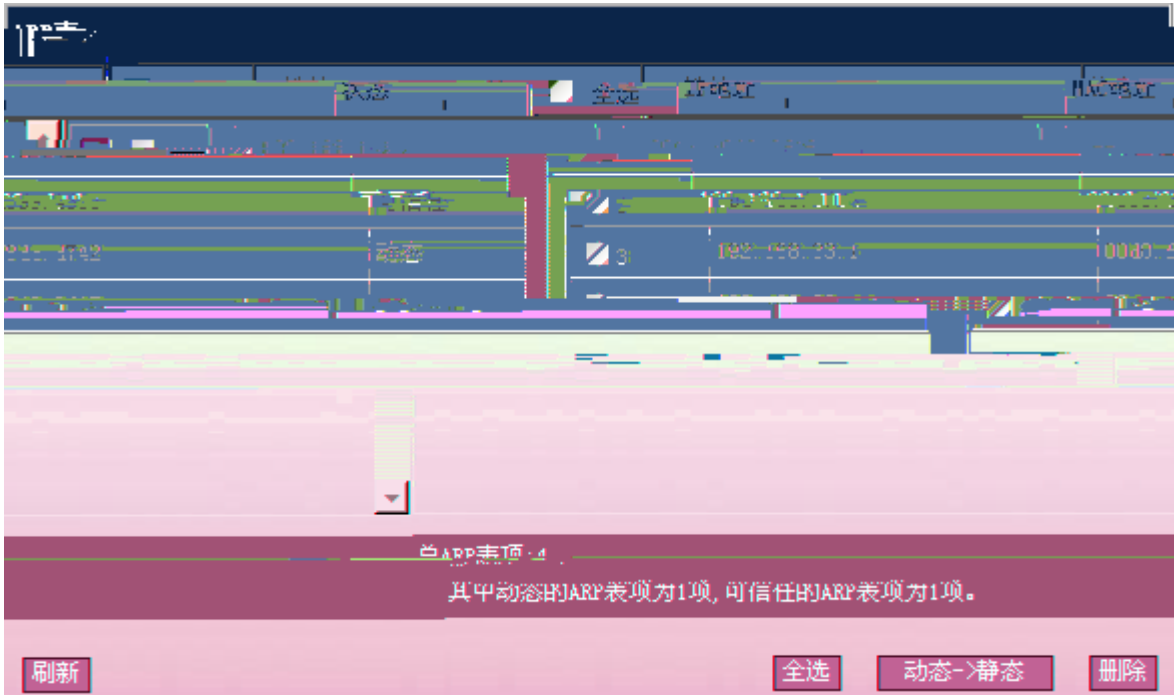
9.

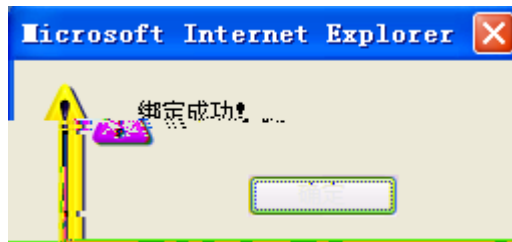
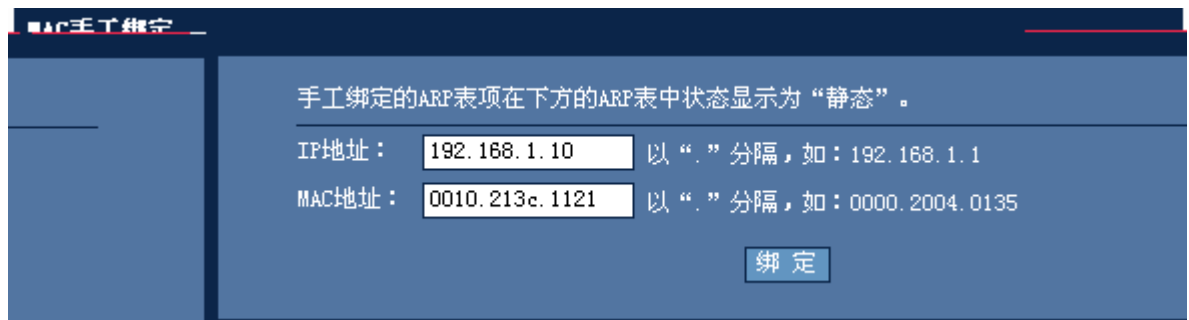
$D_p W$ “ D_p ” “ $\dot{p}$ D_p ” 7 “ $\sqrt{\sim}$
 w 9.10_b18 $H \parallel$ $\dot{p}$ D_p $v \sim H$ D_p
 D_p κ NBR $\psi h'$ $\dot{p}$ PC $\tilde{u}$ τ D_p η κ ψ
 $\sim$ PC $\sqrt{\sim}$ γ D_p “ D_p h ” $\tilde{i}$ β $\dot{p}$ D_p
 D_p $\downarrow \sim$ $\downarrow$ ψ 1-86400s ψ 180s NBR
 ψ $\dot{p}$ $\dot{p}$ D_p “ D_p ”
 $\sim$ “ τ γ ” ω ψ “ ” D_p
 $\downarrow e \sim$ $\parallel \sim$ γ D_p









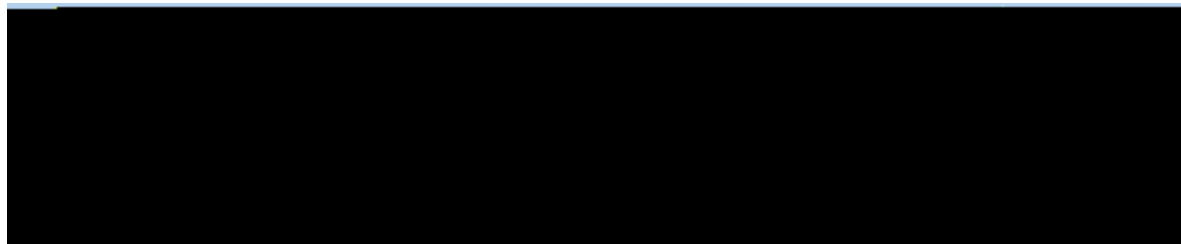


手工绑定的ARP表项在下方的ARP表中状态显示为“静态”。

IP地址： 192.168.1.10 以“.”分隔，如：192.168.1.1

MAC地址： 0010.213c.1121 以“.”分隔，如：0000.2004.0135

绑定



13. ARP

ARP欺骗定位功能，路由器可以对主机的报文进行分析，找出有ARP欺骗嫌疑的主机。

在配置页面上，可以设置路由器的ARP欺骗定位功能。路由器可以对主机的报文进行分析，找出有ARP欺骗嫌疑的主机。

保存





h $\hat{\gamma}$ $\mathcal{D}_\rho$ h "

$\mathcal{D}_\rho$ " h IP MAC γ i ψ τ γ

14. DNS

$$\begin{array}{ccccccc} & \vdash & & \vdash & \Psi & \text{DNS} & \text{DNS} \\ \sim & \Upsilon & D_\rho & \text{" " } & \chi^\sim & - & \text{DNS} \\ & D_\rho & - & \text{DNS} & \text{" " } & @ \text{ DNS} & \vdash \\ & D_\rho & \text{" " } & \dot{\imath} & \Upsilon & \text{DNS} & \Upsilon \\ & \Upsilon & \gamma & \text{PC} & \text{DNS}^\sim & \gamma & \Psi \end{array}$$



路由设置

源地址子网掩码：

0.0.0.0

目的地址子网掩码：

0.0.0.0

下一跳IP：

192.168.33.1

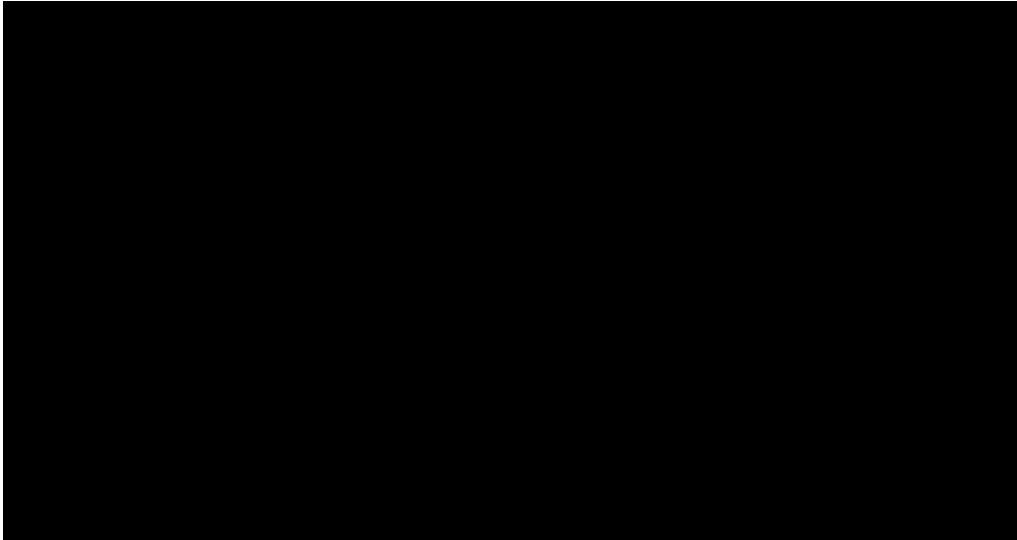
接口：

WANO

增加路由

16.

[illegible]





η γ $\mathcal{D}_p$ “ ” $\gamma \eta$ a
 $\mathcal{D} \bar{G}$ a $\mathcal{D}$ Ψ 500Kbit $\mathcal{D}$ τ_H
 $\sim$ $\mathcal{D}$ Ψ 1000Kbit $\sim$ a Ψ 600 $\bar{G}$
 a Ψ 500Kbit τ_H $\sim$
 Ψ 1000Kbit $\sim$ a Ψ 600 $\Psi \mathcal{D}$



19.

o ~ `E IP ü ð a IP h 卜 WEB FTP
“ ð ” Ω ü 卜 ð h IP “ ” Ω `E IP
PPPoE ~ - ü o
“ ” 卜 √ TCP UDP Ω 卜
o DMZ h “ ” √ “ √ DMZ h ”
Dp “ √ ” o √ b
γ ð IP192.168.1.3 卜 WEB 卜 `E IP222.103.128.100 √ 卜 :

端口映射设置

说明：端口映射将广域网服务端口和局域网网络服务器对应起来，则所有对该广域网服务端口的访问将会被重定向到指定的局域网网络服务器。

内网： IP地址

外网： ☒ IP地址

WAN0

映射关系： ☒ 指定网络地址 TCP

内网端口

外网端口

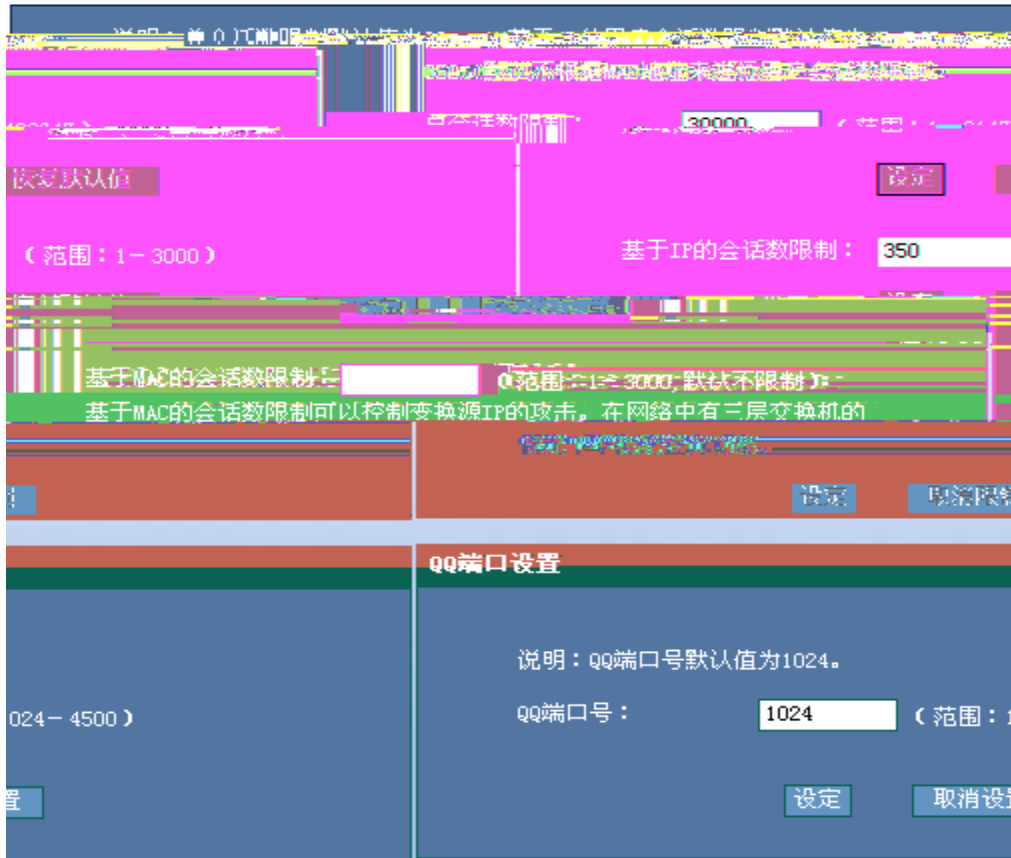
地址	外网端口	接口	☐	协议	内部IP地址	内网端口	外部IP地址
222.103.128.100	80		☐	TCP	192.168.1.3	80	222.103.128.100

0

上	0
FTP()	
FTP(L)	
TELNET	



QQ PC 1023 QQ



21.

“ ” ~ γ ρ h η ε η γ
www.baidu.com 4 0 || 0 T “ DNS ” ρ 3
DNS 1



Dp “

G ”

4~

※ DHCP 卜

23. DHCP

DHCP 卜 ^ γ 4 ρ h ˊ № IP
 D LAN o IP 4 192.168.1.1 4 255.255.255.0
 4 ρ h ˊ № IP
 ˊ “ DHCP 卜 ” Ω “ ” 4 “ 192.168.1.0 ” “
 ” 4 “ 255.255.255.0 ” γ || h IP 4 “ 192.168.1.1——
 192.168.1.254 ” G IP G DHCP № D ˊ №
 卜 Ω “ G IP ” “ ” IP №
 a 4 “ 5 ” , “ 7 ” Ω
 LAN o IP “ DNS 卜 ” Ω № DNS 卜



24. IP

IP 地址 通过 DHCP 服务器 IP 地址池 分配给客户端。如果客户端的 IP 地址与 DHCP 服务器 IP 地址池中的 IP 地址冲突，客户端将无法获取 IP 地址。此时，客户端的 IP 地址为 0.0.0.0，无法访问网络。此时，需要检查 DHCP 服务器的配置，确保 IP 地址池中的 IP 地址与客户端的 IP 地址不冲突。

MAC 地址 与 IP 地址绑定。MAC 地址是网络设备的唯一标识，IP 地址是网络设备的逻辑地址。通过 DHCP 服务器，可以将 IP 地址与 MAC 地址绑定，确保客户端获取的 IP 地址与 MAC 地址对应。

例如，MAC 地址为 00d0.f800.0001 的客户端，通过 DHCP 服务器获取 IP 地址 192.168.1.254。

DHCP静态IP绑定

本页配置DHCP静态IP分配。

如果在增加时发现客户名称出现重复，原有的那条静态IP绑定将会被新的静态IP绑定取代，不同的MAC地址不能同时绑定到同一个IP地址。

客户名称 (用来区分每一条IP/MAC绑定)

客户端IP：

客户MAC地址： (格式:00D0.F800.0021) 增加

	客户名称	客户端IP	客户端MAC
☐	PC1	192.168.1.254	00d0.f800.0001

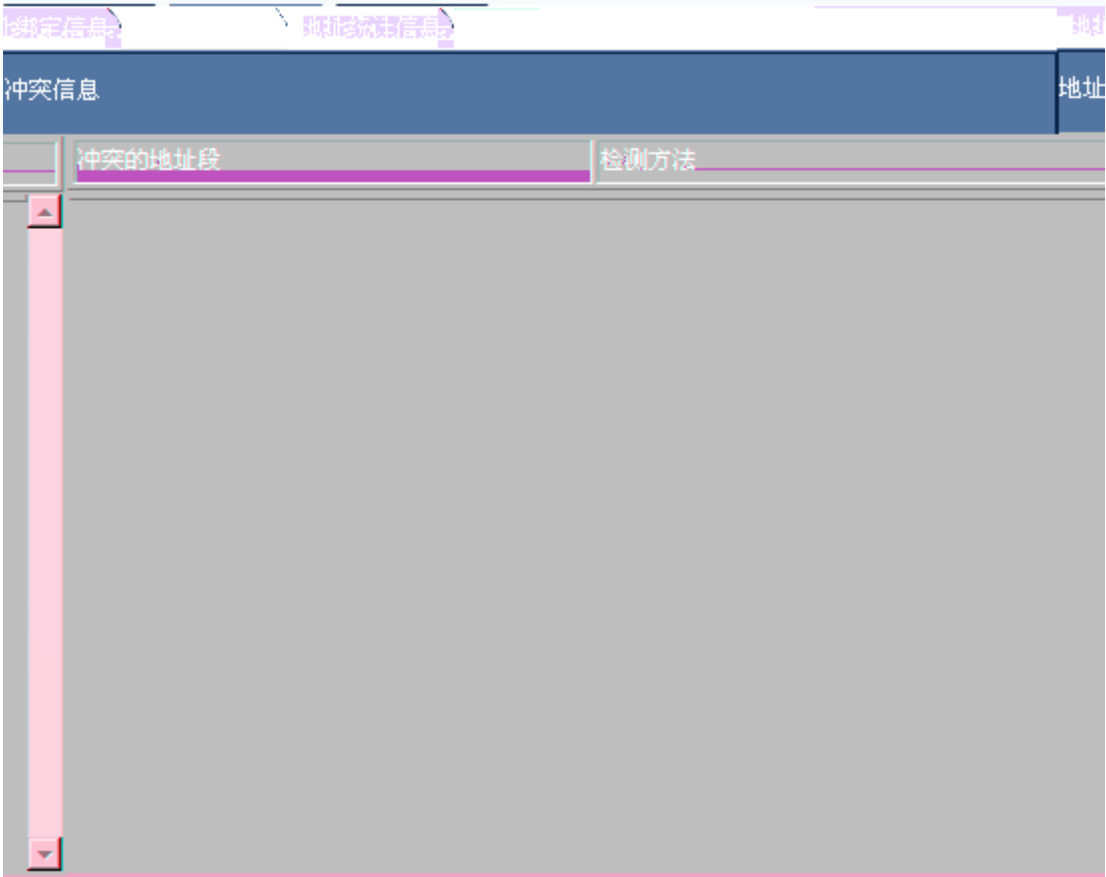
通过 DHCP 服务器 IP 地址池 分配给客户端。如果客户端的 IP 地址与 DHCP 服务器 IP 地址池中的 IP 地址冲突，客户端将无法获取 IP 地址。此时，客户端的 IP 地址为 0.0.0.0，无法访问网络。此时，需要检查 DHCP 服务器的配置，确保 IP 地址池中的 IP 地址与客户端的 IP 地址不冲突。

25.

DHCP 服务器 通过 DHCP 服务器 IP 地址池 分配给客户端。如果客户端的 IP 地址与 DHCP 服务器 IP 地址池中的 IP 地址冲突，客户端将无法获取 IP 地址。此时，客户端的 IP 地址为 0.0.0.0，无法访问网络。此时，需要检查 DHCP 服务器的配置，确保 IP 地址池中的 IP 地址与客户端的 IP 地址不冲突。



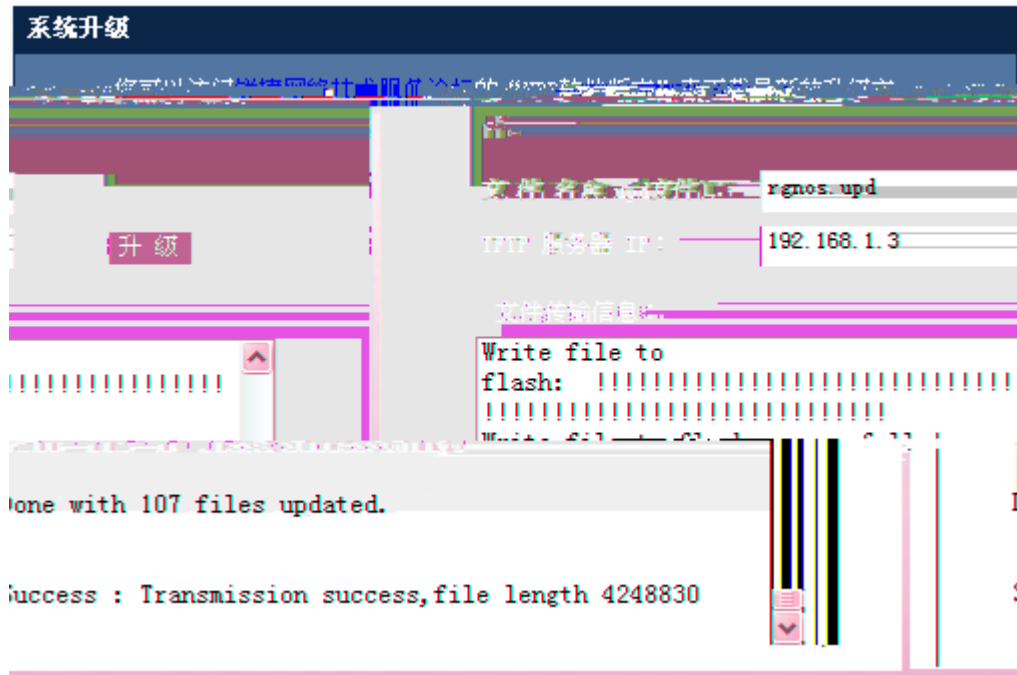
|| H || No IP



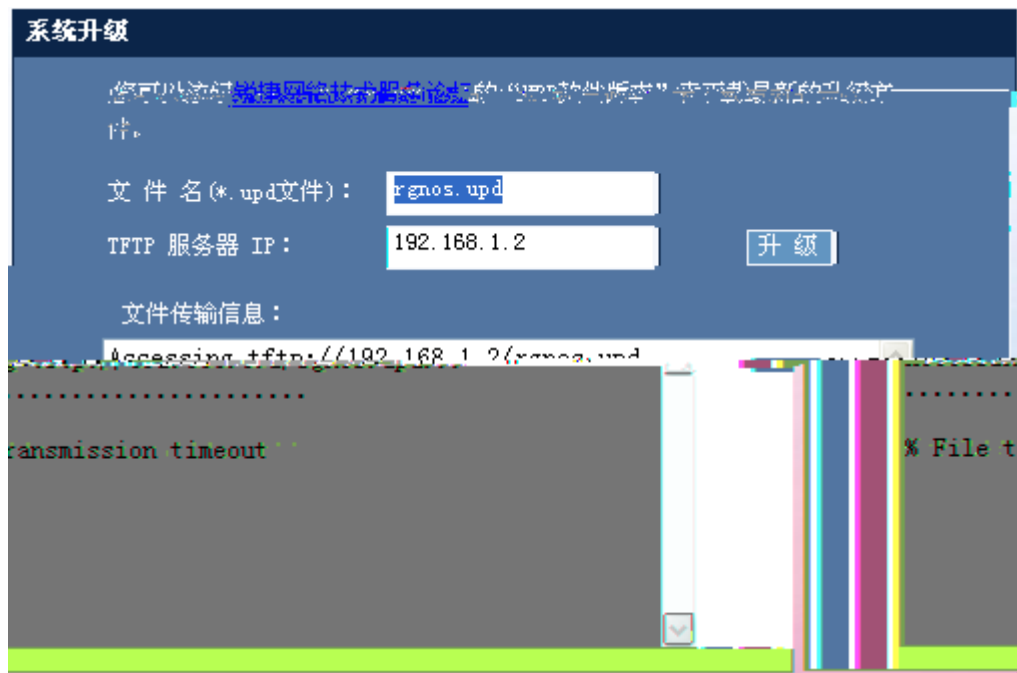
DHCP



$$\begin{aligned} & \text{G} \quad \text{Internet} \quad \vdash \quad \text{NTP/SNTP} \\ & \text{NTP/SNTP} \quad \vdash \quad \text{P} \\ & \text{IP} \quad \text{IP} \\ & \text{IP} \quad 1800 \\ & \text{IP} \quad \text{IP} \quad +8 \end{aligned}$$



~ TFTP 卜 TFTP 卜 ψ “ 1 ”

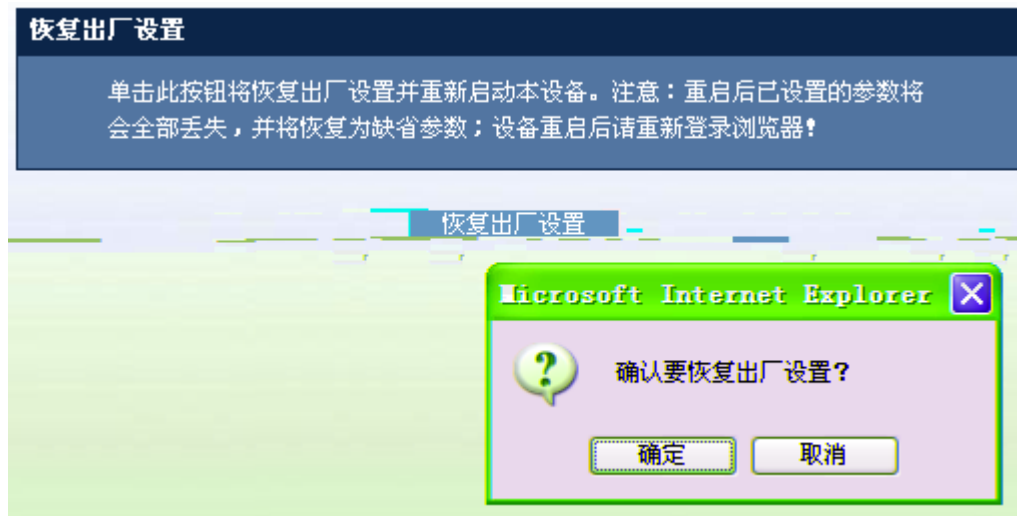




G π ~ ϑ γ 9.01_b5 ϑ γ ƒ “ γ ”
ψ 7 γ b T γ
√~

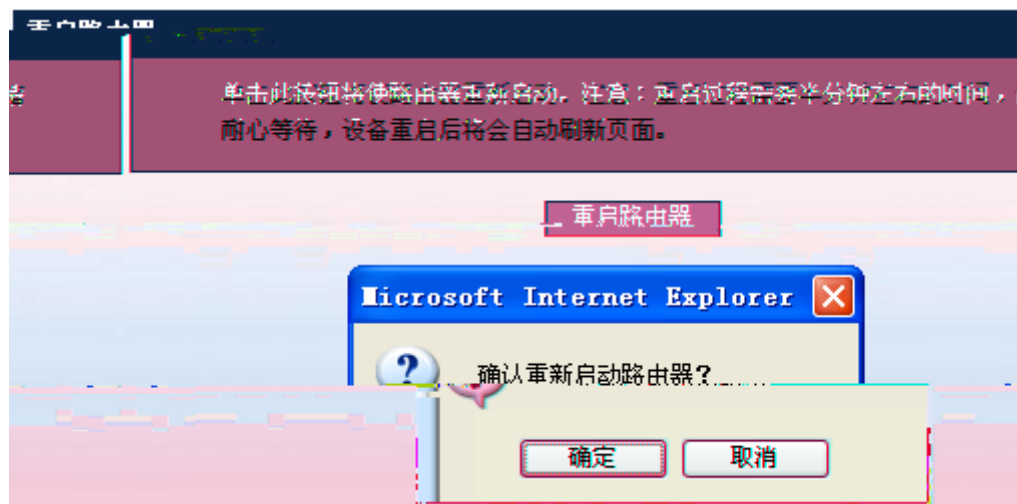
28.

Ɖρ “ ƒ N ” ƒ ƒ N
NBR web admin



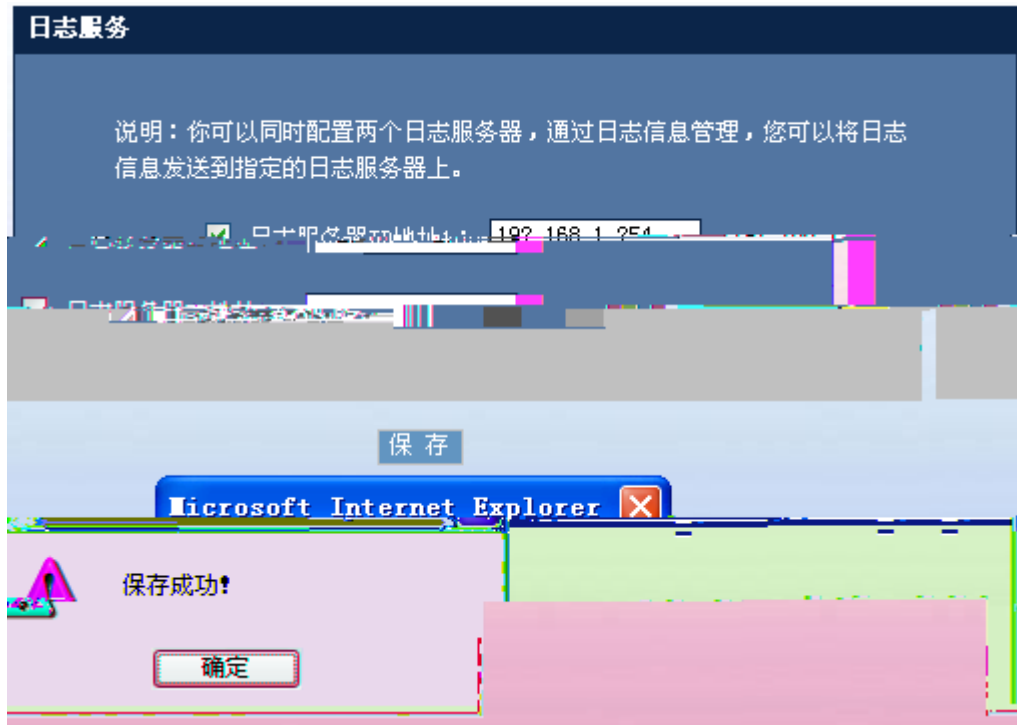
29.

Ɖρ “ ” ƒ



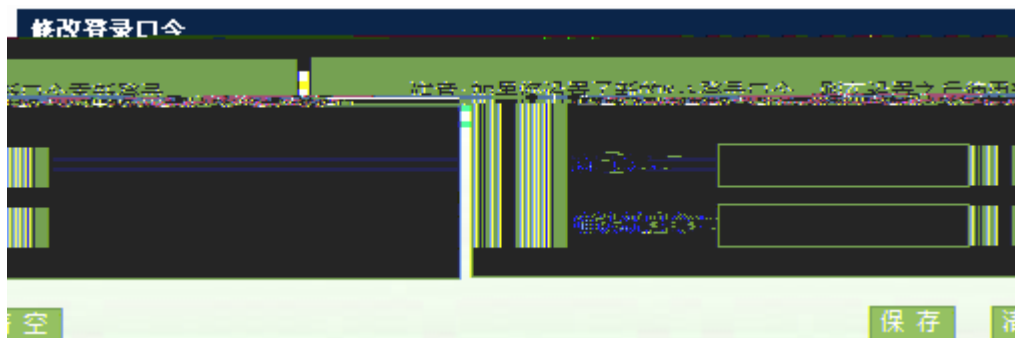
30.

“ 卜 ”~ Ü 卜 H ↑
 G № 卜 ĩ “ 1 ” ~ 卜 Dp “ Ĝ ” ¼~



31.

o 9 T~ №≠ 4 WEB ~ Telnet ĩ
 WEB ~ o 9 ~ o 9 Dp “ Ĝ ” ¼~ WEB
 ~ o 9 ~ o 9 ~ Dp “ ” ~





32.

流量统计信息

rrr.ruijie.com.cn



33. NAT

NAT 是网络地址转换，它可以将私网 IP 地址转换为公网 IP 地址，从而实现私网主机访问公网资源。H



34.

“H”是CPU的缩写，表示中央处理器。CPU是计算机的核心部件，负责执行指令和处理数据。

系统信息

CPU利用率: 1%

系统CPU利用率最大值: 1%, 出现最大值的时刻: 1970-3-5 10:51:49

内存使用:

可用的总内存: 256,676K 字节; 已分配: 4,741K 字节; 可用: 251,935K 字节

35.

“ 〇 H ” | LAN 〇 IP MAC WAN 〇 ~

IP MAC γ ī ④ 〇 , Dρ “ γ ”

↳ 〇 Dρ “ J ” ,

接口信息

LAN口状态:

IP地址: 0.0.0.0

MAC地址: 00D0.F86B.DC91

WAN0口状态 静态IP线路

MAC地址: 00D0.F86B.DC92

WAN1口状态 静态IP线路

IP地址: 0.0.0.0

MAC地址: 00D0.F86B.DC93

送速率(报文/秒)	丢弃报文(个)	带宽占用	接口	接收报文(个)	接收速率(报文/秒)	发送报文(个)	发
	172	0.4%	LAN 0	19,352	17	20,830	25
	3	0.4%	WAN 0	11,327	5	9,897	4
	3	0.4%	WAN 1	0	0	477	0

新

统计值清零

刷



“ H ” 3 H No $\Psi \Upsilon \Upsilon$

“ $\frac{L}{F}$ ” $\mathcal{T}^{\sim}$ $\int$ $\mathfrak{D}$ $\mathfrak{D}$



```
arp attacker-detect enable
security anti-war-attack level high
security anti-lan-attack drop
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 192.168.33.1
!
line con 0
line vty 0
    login
    password 7 093d061134111358
line vty 1
    login
    password 7 11003406015e0c33
line vty 2
    login
```

end

M H

[illegible]

$$D_p \ll \frac{1}{\lambda} \ll \frac{1}{\lambda_0}$$

The screenshot displays the 'Hosts' (主机) management interface. At the top, there's a navigation bar with 'Host Management' (主机管理) and 'Hosts' (主机). Below this is a table with the following headers: '主机名' (Host Name), '交换机IP' (Switch IP), '交换机型号' (Switch Model), '交换机端口' (Switch Port), and '活动状态' (Activity Status). The table body is empty. At the bottom of the page, there are five buttons: '全选' (Select All), '删除' (Delete), '刷新' (Refresh), '配置交换机' (Configure Switch), and '帮助' (Help).

$\gamma \rightarrow \pi^+ \pi^-$ h IP $\gamma \rightarrow e^+ e^-$ β

$\downarrow$ $\downarrow$ S57 S29 S27 $\downarrow$ D $\downarrow$

10.1(4) γ

38.

$$\mathcal{D}_p \text{ " " } \gamma \text{ " " } \mathbb{F}$$



敏锐把握应用趋势 快捷满足客户需求

VLAN设置

说明：当接口模式为“trunk”时，如果不指定VLAN ID，接口将许可所有VLAN访问；

如果指定VLAN ID，则指定该接口为指定VLAN的端口，该接口只能配置为指定VLAN的端口，不能配置为其他VLAN的端口。

接口	接口模式	VLAN ID
GigabitEthernet 0/1	access	1
GigabitEthernet 0/2	access	1
GigabitEthernet 0/3	access	1
GigabitEthernet 0/4	access	1
GigabitEthernet 0/5	access	1
GigabitEthernet 0/6	access	1
GigabitEthernet 0/7	access	1
GigabitEthernet 0/8	access	1
GigabitEthernet 0/9	access	1

GigabitEthernet 0/15

access

1

IP

配置 S57 配置 IP 配置 SVI IP

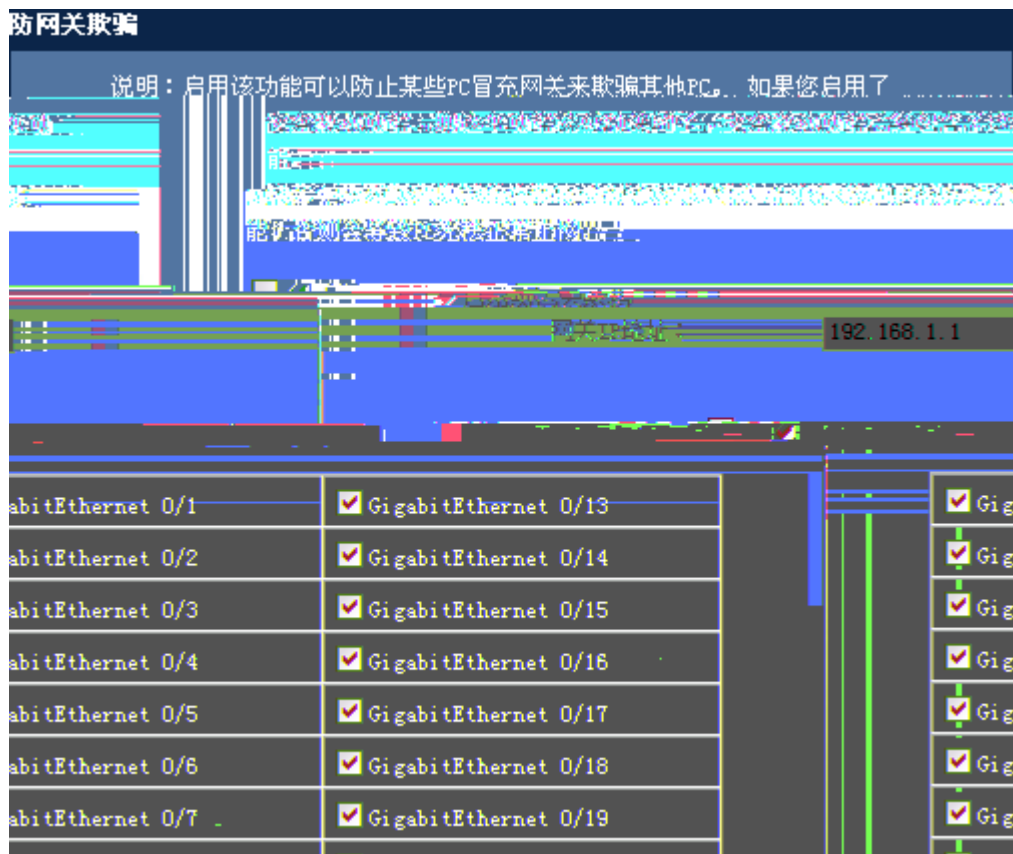
配置“ ”

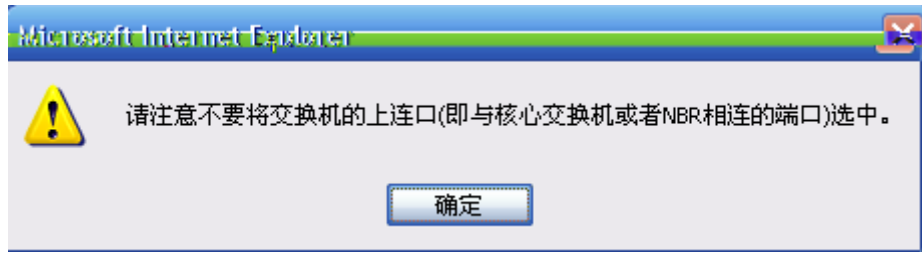
0040. f800. 0001	192. 168. 1. 100	静态	GigabitEthernet 0/1	1	1
------------------	------------------	----	---------------------	---	---

7

配置 PC 的 IP 地址，并配置 PC 的网关为 192.168.1.1，配置 PC 的 DNS 服务器为 192.168.1.1。

0





“ ” D o l G n



L

o L L PC D p

γ L G0/2 o "H Ũ 4000Kbit/s 2000Kbit/s 4 D

接口限速设置

说明：不限速的接口，保持对应文本框为空。限速值范围为312-1000000KBit/s。

接口	发送流量限制 (KBit/s)	接收流量限制 (KBit/s)
GigabitEthernet 0/1		
GigabitEthernet 0/2	4000	2000

Dp " G "

o

o 4 7 4 4 γ

GigabitEthernet 0/2 4 D

web登录口令设置

注意:如果你设置了新的web登录口令,则在设置之后请使用新的口令重新登录。

新口令:

确认新口令:

保存

清空

Telnet登录口令设置

新口令:

确认新口令:

保存

清空

H

~ γ ~ Đ ° ↓ ~

系统信息

交换机系统信息:

主机名: S2924G

设备型号: S2924G

设备序列号: 00000000000000000000000000000000

0

o ~ γ ∫ ' @ o Ì Û γ ĭ Û '

接口	接收速率 (bit/s)	发送速率 (bit/s)	接收报文	发送报文	错误报文
GigabitEthernet 0/0	0	0	0	0	0
GigabitEthernet 0/1	0	0	0	0	0
GigabitEthernet 0/2	0	0	0	0	0
GigabitEthernet 0/3	0	0	0	0	0
GigabitEthernet 0/4	0	0	0	0	0
GigabitEthernet 0/5	0	0	0	0	0
GigabitEthernet 0/6	0	0	0	0	0
GigabitEthernet 0/7	0	0	0	0	0
GigabitEthernet 0/8	0	0	0	0	0
GigabitEthernet 0/9	0	0	0	0	0
GigabitEthernet 0/10	0	0	0	0	0
GigabitEthernet 0/11	0	0	0	0	0
GigabitEthernet 0/12	0	0	0	0	0
GigabitEthernet 0/13	0	0	0	0	0
GigabitEthernet 0/14	0	0	0	0	0

o H

o o vlan 1

接口	状态	VLAN ID	模式	速率
GigabitEthernet 0/1	up	1	全双工	1000M
GigabitEthernet 0/2	down	1	--	--
GigabitEthernet 0/3	down	1	--	--
GigabitEthernet 0/4	down	1	--	--
GigabitEthernet 0/5	down	1	--	--
GigabitEthernet 0/6	down	1	--	--
GigabitEthernet 0/7	down	1	--	--
GigabitEthernet 0/8	down	1	--	--
GigabitEthernet 0/9	down	1	--	--
GigabitEthernet 0/10	down	1	--	--
GigabitEthernet 0/11	down	1	--	--
GigabitEthernet 0/12	down	1	--	--
GigabitEthernet 0/13	down	1	--	--
GigabitEthernet 0/14	down	1	--	--

39.

通过安全地址表，可以查出某IP的主机所接的交换机的IP、端口以及在交换机上的绑定状态。建议在看到有动态绑定的表项时，对该表项进行人工的合法性判断，然后通过点击“全网静态安全地址绑定”按钮将全部

安全地址

通过安全地址表，可以查出某IP的主机所接的交换机的IP、端口以及在交换机上的绑定状态。建议在看到有动态绑定的表项时，对该表项进行人工的合法性判断，然后通过点击“全网静态安全地址绑定”按钮将全部的动态表项绑定成静态表项。

IP地址被绑定为101.x.x.x的主机与其它主机存在IP地址冲突；

IP地址被绑定为100.132.x.x的主机存在 ARP攻击嫌疑；

如果以上条目出现在列表中，请对该主机进行合法性判断。

安全地址表

IP地址	交换机IP	交换机端口	绑定状态	绑定时间
192.168.1.2	Gi 0/23	1	192.168.1.14	0016.d399.eb16 动态绑定

总表项: 1项

其中动态绑定的表项为1项，静态绑定的表项为0项。

删除指定静态绑定

全网静态安全地址绑定

刷新

40.

“ ” ↓ e z “ b T H a
ρ
