

安网智能

教你认识ARP防御的重要性

2003年，SARS的恐怖记忆仍历历在目.....



■2003年SARS半年时间波及33个国家和地区，8437人受到感染，共造成813人死亡，其中中国大陆死亡人数高达349人，其次为香港298人。

■2003年非典十大流行语：

1.非典(SARS) 2.疫情3.消毒4.隔离5.抗击非典6.疑似7.口罩8.体温9.防控10.世界卫生组织(WHO)

2007年网络江湖，“ARP病毒”令人闻之色变

病毒排名	英文名	中文名
1	Virus.Autorun.**	U盘寄生虫
2	无	ARP病毒
3	Trojan/PSW.GamePass.**	网游大盗
4	Worm/MSN.SendPhoto.*	MSN性感相册
5	Exploit.ANIfile	ANI病毒
6	Trojan/Agent.pgz	机器狗
7	Trojan/Agent	代理木马
8	Trojan/KillAV.ak	AV杀手
9	Exploit.JS.Real	Real脚本病毒
10	Worm.Viking.**	熊猫烧香



(2007年度江民科技十大病毒排行 数据来源：江民科技)

据瑞星统计：截止到2007年12月份，ARP病毒累计感染计算机34414793台

- 病毒名称：“ARP”类病毒
- 病毒中文名：“ARP”类病毒
- 病毒类型：木马
- 危险级别：★★★
- 影响平台：Win 9X/ME/NT/2000/XP/2003

过期的网页上，仍可体会到ARP病毒曾经的肆虐

The screenshot shows a Microsoft Internet Explorer browser window displaying the SYSU ITS Helpdesk website. The browser's address bar shows the URL: <https://helpdesk.sysu.edu.cn/content/view/22/1/>. The website header features the SYSU logo and the text "ITS HELPDESK 信息技术服务帮助台". A navigation menu includes links for "关于帮助台", "IT服务FAQ", "提交服务请求", "下载", "我的中大", "紧急响应组", and "防病毒支持". The main content area is dominated by a red alert titled "红色警告！校园ARP欺骗泛滥！" (Red Alert! Campus ARP Spoofing Epidemic!). The alert text describes the threat of ARP spoofing, its impact on network stability and security, and provides instructions for users to install antivirus software and update their systems. A sidebar on the left contains a "主菜单" (Main Menu) with links to "首页", "最新服务信息", "运维事件通告", "NetID及密码", "IT服务人员", and "内容管理人员". A sidebar on the right contains a "温馨提示" (Warm Reminder) and an "信息安全意识宣传" (Information Security Awareness Campaign) section with a graphic that reads "安全意识是信息安全的第二道防线" (Security awareness is the second line of defense for information security).

中山大学
ITS HELPDESK
信息技术服务帮助台
信息与网络中心

关于帮助台 IT服务FAQ 提交服务请求 下载 我的中大 紧急响应组 防病毒支持

帮助台是校园信息技术服务与支持的统一入口。您可以通过电子邮件、语音呼叫和FAQ知识库来获取我们的帮助。我们的技术团队将为您提供快速、专业和礼貌的服务支持。

南校区：020-84036866 北校区：020-87330831
珠海校区：0756-3568500 东校区：020-39332608
Email: helpdesk@mail.sysu.edu.cn

红色警告！校园ARP欺骗泛滥！
2007-12-08, 00:00
近期，校园ARP木马（病毒）在各大高校不断泛滥的现象，此类木马发送大量ARP欺骗的数据包，导致同一子网的计算机上网时频频断网或不稳定。该木马的真正意图是窃取网络上其他计算机中的游戏帐号及密码、QQ帐号及密码、银行帐号及密码等重要隐私信息，不法分子获得这些信息后，利用各种途径非法犯罪并从中获利。

目前，各校区的教学科研、行政办公、宿舍的网络每天都受到该木马（病毒）的困扰，甚至连学校极其重要工作场所的网络中，也曾有过该木马（病毒）的身影，该木马（病毒）不但影响工作和生活，而且存在信息泄密的危险。

为防止病毒攻击的进一步扩大，保障校园信息安全，保障信息服务的质量，大家应该一起行动起来，使用正确的方法予以防范。大家应在自己工作或家庭（宿舍）的计算机上及时进行安全改善工作，并养成良好的计算机使用习惯：

- 安装正规的防病毒软件，并将防病毒引擎和病毒库升级到最新，定期运行查

温馨提示
如果您在使用学校信息服务中遇到问题，可以点击左上方菜单的“提交服务请求”按钮，使用NetID登录后，将问题或服务请求发送给我们……

信息安全意识宣传
安全意识是信息安全的第二道防线

建立信息安全意识……

2008，我们仍然深受其害！

ARP欺骗肆虐 百余宿舍网络端口被封

清华大学李同学反映：我住在学校紫荆公寓5号楼，从4月份开始，宿舍网速就变得非常慢，而且电脑总出现死机现象。开始我以为是电脑出了问题，但后来发现舍友和其他宿舍同学的电脑都不同程度出现这种情况。因为网速慢，许多需要用邮件交作业的同学，都要跑到学校外面的网吧上网。我每次网上提交申请出国的手续都要反复许多次才能成功，耽误了不少时间。不知道学校校园网中的电脑病毒什么时候能够治愈？

清华大学的校园BBS上，有多名同学抱怨学校宿舍网速太慢，并频频出现掉线现象。引起这种现象的是一种名为“ARP欺骗”的电脑病毒。从4月10日起，已经陆续有100多个宿舍网络端口被封闭，给学生们的正常上网带来了影响。

清华大学网管会服务组工作人员回复：一个物理端口受到“ARP病毒”攻击，整个IP地址段内的电脑都会无法上网，一个IP地址段最多有200多个用户，从4月份开始，学校累计已经超过万台电脑受到了影响，给学生生活和学习，以及教师的办公都带来了很大影响。

清华大学网络中心工作人员回复：这种病毒2006年首次在清华大学出现。到2006年年底，病毒已经演变成了十几个变种，不仅造成局域网的通信故障，还会截取局域网内所有的通讯数据。为防止病毒肆虐，去年寒假期间，对学校44栋学生宿舍楼进行了大规模的联合查杀，查杀之后，病毒消失了一段时间，但今年4月份开始又卷土重来，只要有一台电脑受到病毒感染，病毒就会通过网络的物理端口，感染给局域网内的其他电脑。现在只能是发现中毒端口便立即封闭，但这种封闭都有一定的期限，是为了防止病毒的蔓延，封闭期间这些宿舍学生不能上网。

发表于：2008-06-06，修改于：2008-06-06 11:23，已浏览1921次，有评论4条 [推荐](#) [投诉](#)

中国的最高学府也不例外！

2008，我们仍然深受其害！

行政楼ARP病毒处理情况通报 - 武汉科技大学中南分校网络中心 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(Q) http://nc.znust.edu.cn/html/xinzigonggao/20080624/49.html

武汉科技大学中南分校网络中心
Network & Information Center Of ZNUST

首页 中心介绍 信息公告 网站建设 信息建设 业务受理 常见问题 规章制度 常用软件下载 留言板

Home >> 信息公告 >>

行政楼ARP病毒处理情况通报
日期：2008-06-24 阅读次数：24

行政楼ARP病毒处理情况通报

针对近期ARP病毒肆虐造成的行政楼1、5、6楼办公室电脑不能正常上网的情况，我中心技术人员快速的深入到行政楼各个科室，进行了的清查。在我们的努力下，47网段的ARP病毒已经被全部清除，网络也已恢复到正常状态。

此次查杀ARP病毒的过程中，我们为全楼160多台电脑安装了安全防护软件，进行了木马查杀和漏洞补全工作，最终将感染ARP病毒的毒找出并将其系统进行了重装。

现将病毒源主机的IP和网卡物理地址（MAC地址）公布如下：

所在楼层号	病毒源主机IP	病毒源主机MAC
1	172.16.47.144	00-11-5b-01-76-21
1	172.16.47.44	00-1e-8c-22-41-cf
1	172.16.47.41	00-19-e0-04-2f-d2
1	172.16.47.46	00-58-7a-12-1a-a2
1	172.16.47.47	00-1d-0f-0d-95-9e
1	172.16.47.222	50-78-4c-6f-07-38
1	172.16.47.133	00-10-21-54-05-40

Internet

2008，我们仍然深受其害！

The screenshot shows a Microsoft Internet Explorer browser window displaying the website <http://www.sxyqwater.gov.cn/ReadNews.asp?NewsID=980>. The page features a green header with the site's logo and name, "阳泉水利信息网" (Yangquan Water Information Network), which is highlighted with a red box. Below the header is a navigation bar with various menu items and a search box. A banner for the 2008 Beijing Olympics is visible, with the text "预祝北京奥运会圆满成功!" (Wishing the Beijing 2008 Olympics a successful conclusion!). The main content area displays a news article titled "关于防范ARP病毒的公告及防范办法" (Announcement and Prevention Measures for ARP Virus), also highlighted with a red box. The article's publication date is "2008年6月30日" (June 30, 2008), and the author is "水利人" (Water Person). The article text begins with "近期我局局域网爆发一种新的“ARP欺骗”木马病毒..." (Recently, a new "ARP spoofing" Trojan virus has broken out in our local area network...). The browser's address bar and menu bar are also visible at the top of the window.

关于防范ARP病毒的公告及防范办法

阳泉水利信息网

阳泉水利信息网 当前在线 1 人

全部内容 全部大类 全部小类 关键字 搜索

网站首页 | 本站专题 | 图片新闻 | 留言板 | 水利视频 | 网上办公 | 资料下载

预祝北京奥运会圆满成功!
让我们共同期待2008奥运会 2008.8.8-8.24

政府信息公开 | 水利新闻 | 水利工程 | 水土保持 | 水利水资源 | 防汛抗旱 | 农建园地 | 政策法规 | 水利党建 | 水利百科 | 水利信息化

栏目导航 网站首页 >> 水利信息化 >> 电脑课堂

共有 90 位读者读过此文 字体颜色: 选择颜色 【字体: 放大 正常 缩小】

【单击鼠标左键自动滚屏】 【图片上滚动鼠标滚轮变焦图片】

关于防范ARP病毒的公告及防范办法

发表日期: 2008年6月30日 【编辑录入: 水利人】

关于防范ARP病毒的公告及防范办法

近期我局局域网爆发一种新的“ARP欺骗”木马病毒, 病毒发作时其症状表现为计算机网络连接时断时通, 严重影响了局域网的正常使用, 为了保证网络的安全畅通, 现就有关事项公告如下:

一、故障现象及原因分析

下面向您介绍：

- ARP攻击引发的常见网络故障

- ARP攻击原理及防治难度

- ARP攻击防治思路

三个概念说明

大家可能发现经常出现下面三个不同的说法：

- ARP病毒
- ARP欺骗
- ARP攻击

“ARP病毒”：一般将导致ARP攻击的软件称为ARP病毒，例如一些游戏的盗号木马通过ARP攻击，将“终端—网关”数据传输路径改成“终端--中木马终端—网关”实现盗号目的。但也有一些ARP攻击是使用某些软件造成的，例如网络执法官、网络剪刀手、局域网终结者等，并不适合称为“ARP病毒”。但是习惯叫法之一。

“ARP欺骗”：由于ARP协议的缺陷，攻击者用虚假的网关ARP报文欺骗局域网内终端，用虚假的终端ARP报文欺骗网关，以及在终端之间进行欺骗。还有一种方式是发送大量ARP欺骗报文形成泛洪攻击。是习惯叫法之一。

“ARP攻击”：“ARP欺骗”和ARP泛洪攻击都是对局域网使用的破坏，都是利用ARP协议的缺陷对局域网的攻击破坏，因此都可以称为“ARP攻击”，等同于“ARP欺骗”概念。是习惯叫法之一。

ARP攻击引发的常见网络故障

- 上网速度慢，或者网络内共享文件很慢
——表现为利用网络抓包工具，抓到局域网中有大量ARP报文。
- 全网同样配置下，唯独某台电脑无法上网
——表现为掉线后，重启电脑或者禁用网卡再启用就恢复正常，但一会又掉线
- 大面积同时掉线，或时通时断（即通常说的“卡”）
——表现为某一片区域，某台网络设备下挂的所有PC出现上网不正常。
- 电脑挨个掉线，或时通时断（即通常说的“卡”）
——表现为正在使用某一类应用程序的PC依次掉线。
- 变种机器狗病毒、变种磁碟机病毒利用ARP攻击传播
——表现为某台电脑感染变种机器狗或变种磁碟机病毒后，局域网内其他电脑也会中毒

下面向您介绍：

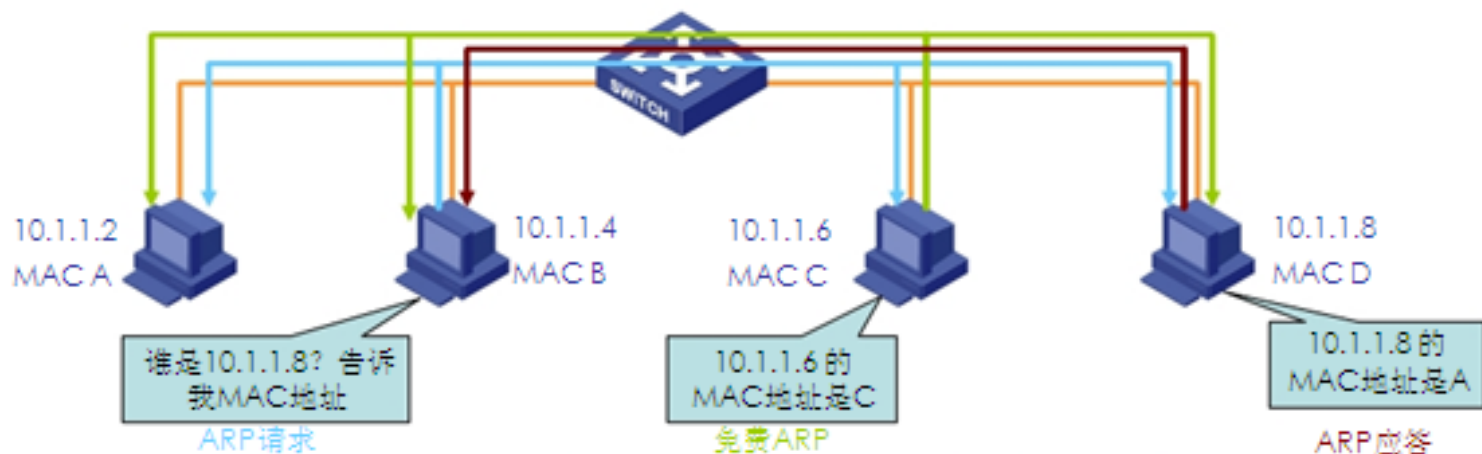
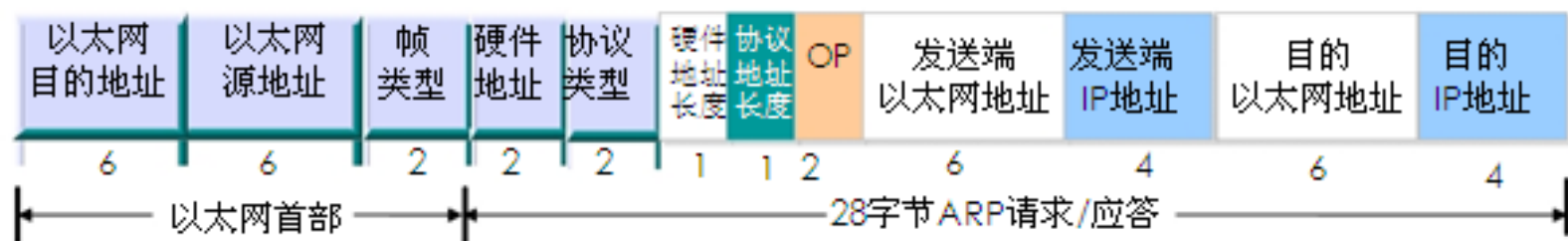
- ARP攻击引发的常见网络故障

- ARP攻击原理及防治难度

- ARP攻击防治思路

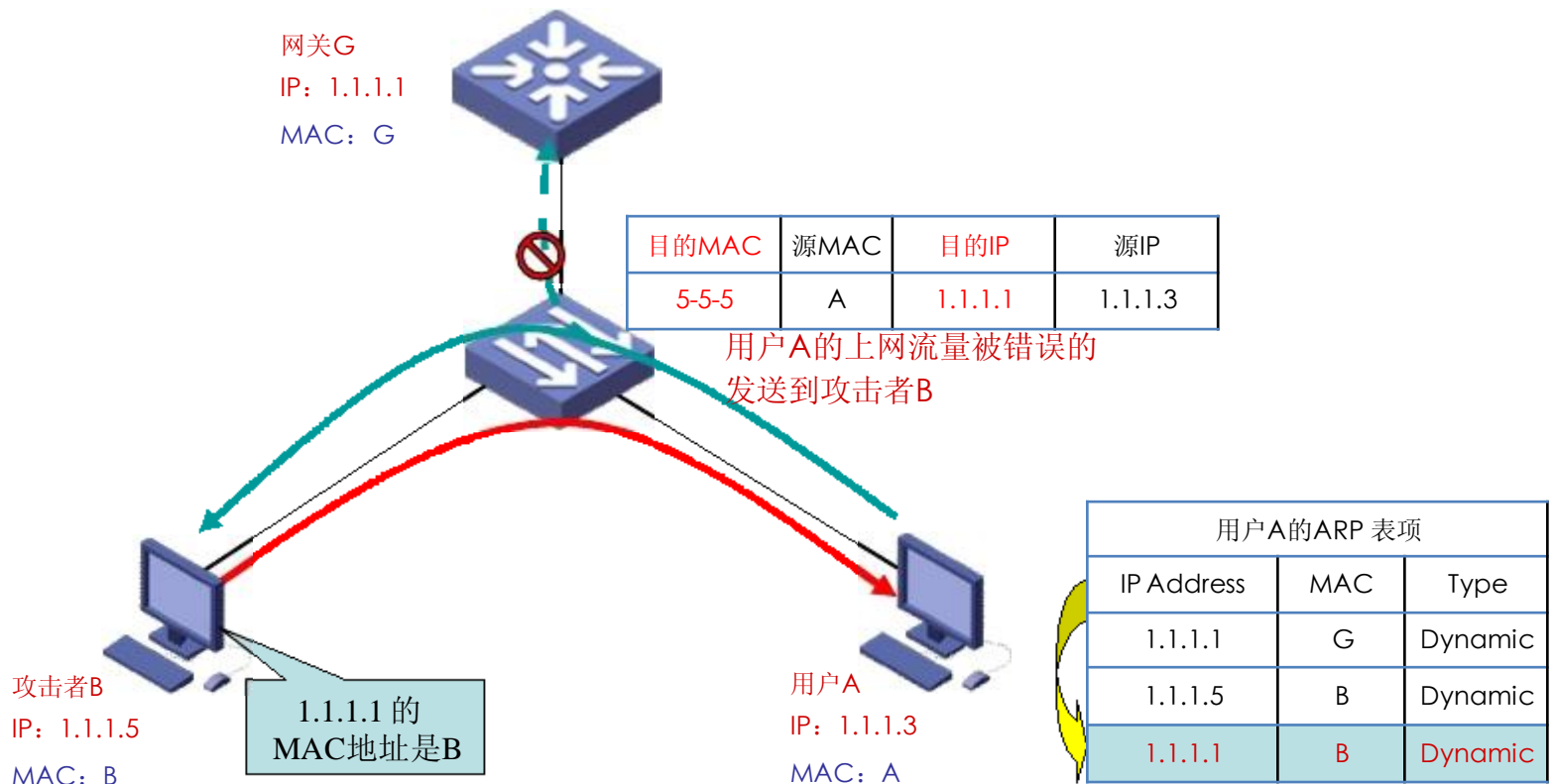
ARP协议介绍

- ARP——Address Resolution Protocol地址解释协议，RFC826
- 为IP地址到MAC地址提供动态映射，定位到目的IP的对应MAC才能实现数据交换



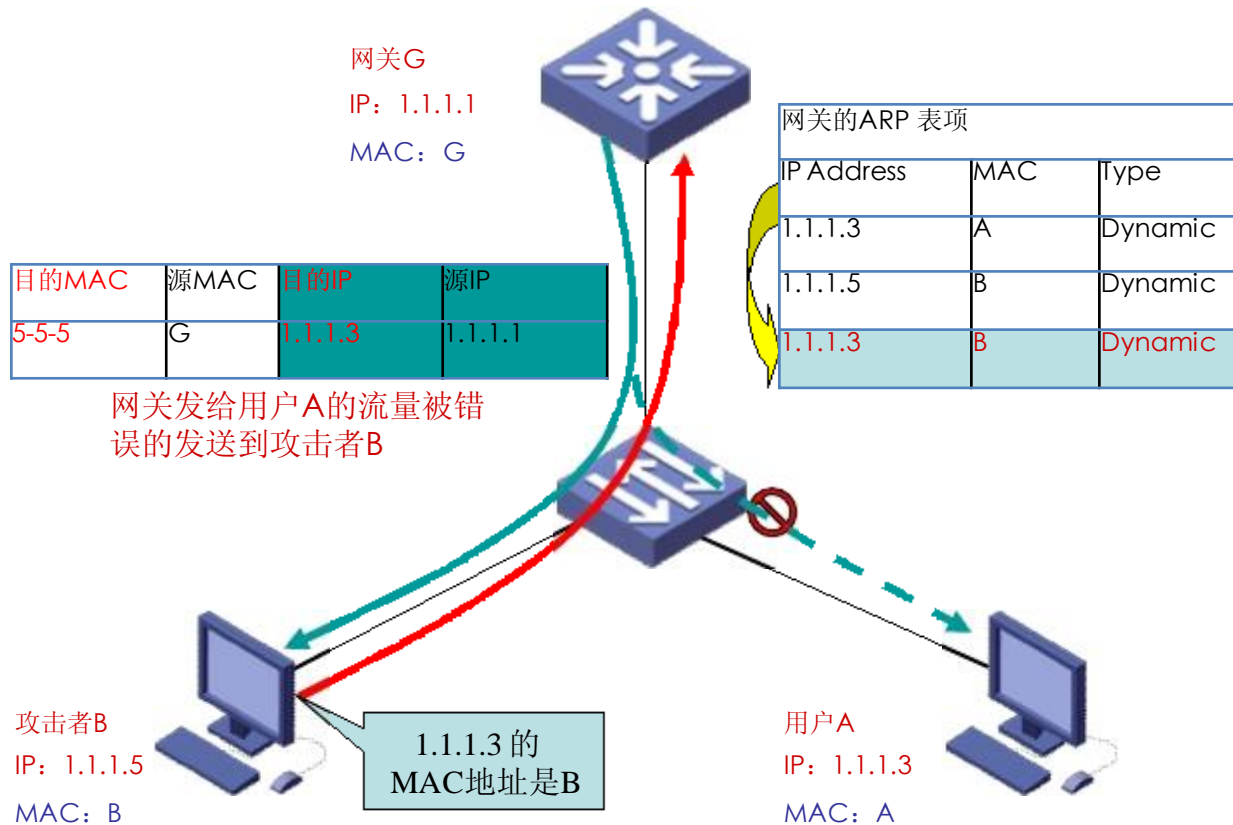
① ARP欺骗攻击—仿冒网关

- 攻击者发送伪造的网关ARP报文，可广播给同网段内的所有其他主机
- 主机访问网关的流量，被重定向到错误的MAC地址，无法正常访问外网
- 是最常见的ARP攻击方式，导致网络瘫痪，甚至数据被窃取



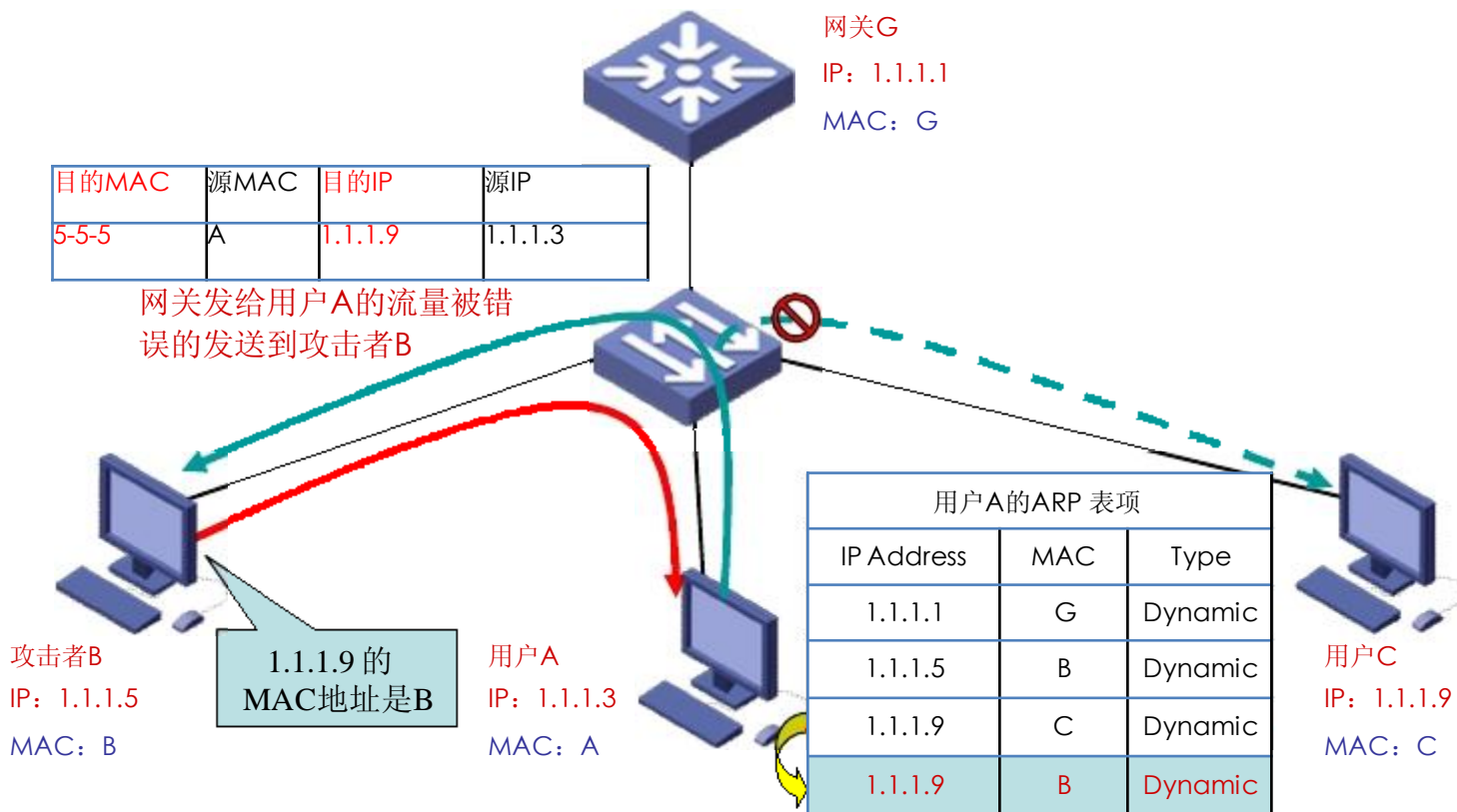
② ARP欺骗攻击—欺骗网关

- 攻击者伪造虚假的用户ARP报文，发给网关
- 网关发给该用户的数据重定向到错误的MAC地址，该用户收不到网关返回的数据而无法访问外网



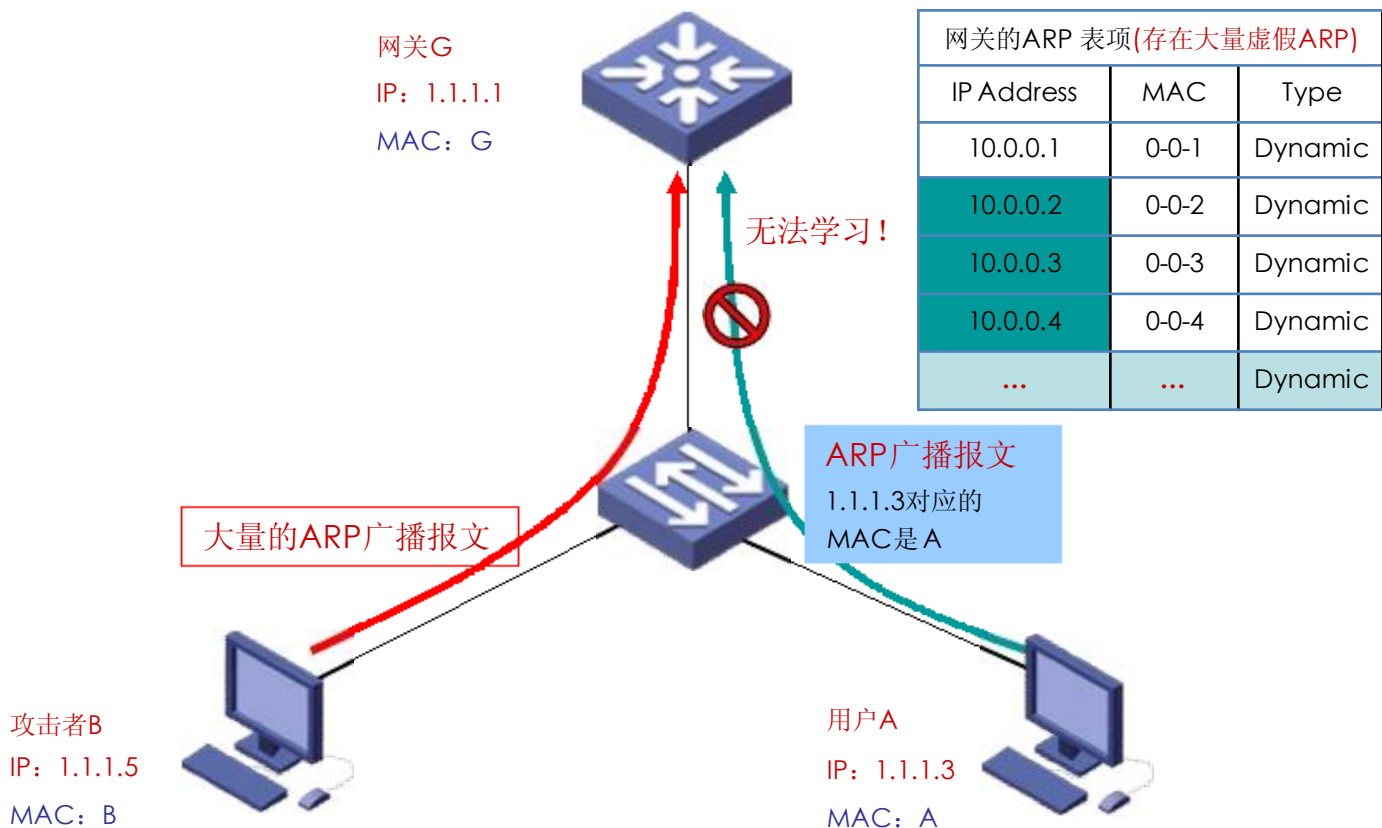
③ ARP欺骗攻击—欺骗终端用户

- 攻击者伪造虚假的用户ARP报文，发送给网段内的其他主机
- 网段内的其他主机发给该用户的数据被重定向到错误的MAC地址，该用户与其他主机无法互访



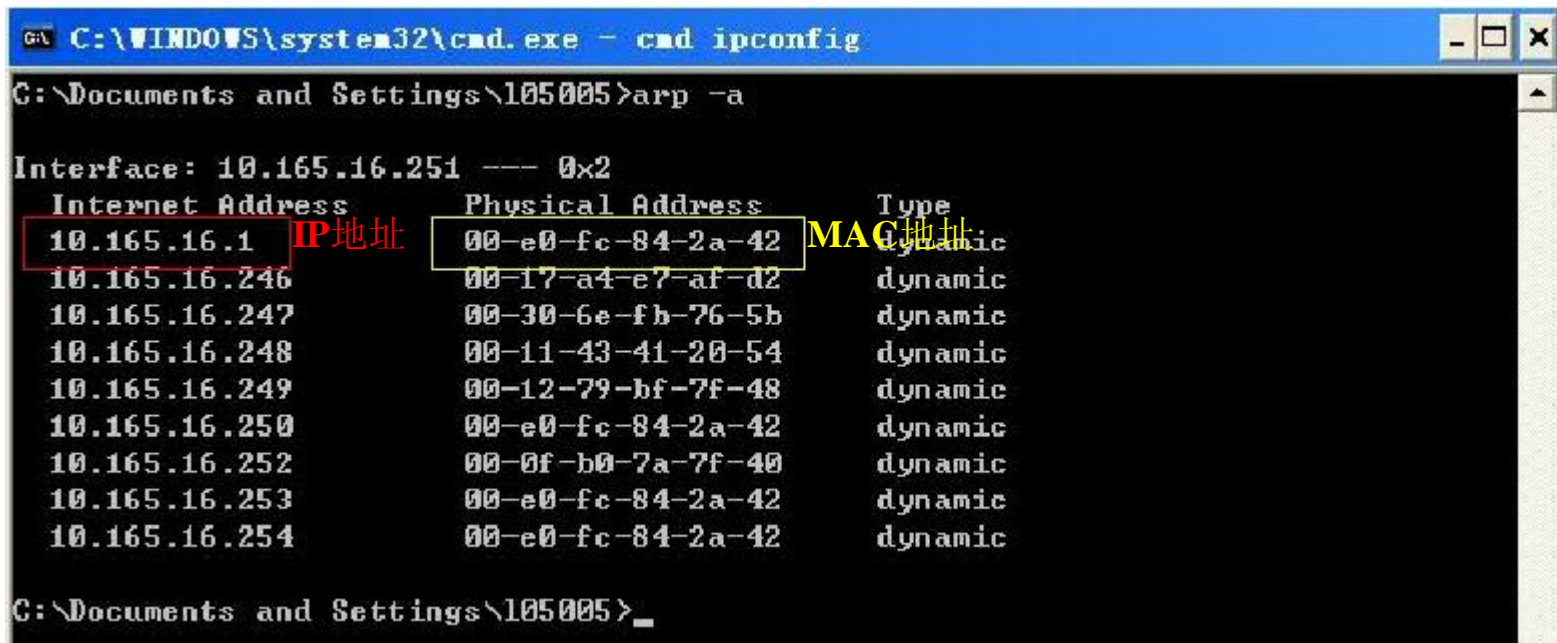
④ ARP泛洪攻击

- 攻击者伪造大量不同ARP报文在网段内进行广播
- 导致网关ARP表项被占满，无法正常学习合法用户的ARP，网络瘫痪
- 大量广播报文消耗交换机和网络资源，网络明显变慢



什么是ARP?

如果把“IP地址”看成“人名”，“MAC地址”看成“电话号码”，那么“ARP”就是“电话簿”！



```
C:\WINDOWS\system32\cmd.exe - cmd ipconfig
C:\Documents and Settings\105005>arp -a

Interface: 10.165.16.251 --- 0x2
  Internet Address      Physical Address      Type
  10.165.16.1          00-e0-fc-84-2a-42    dynamic
  10.165.16.246        00-17-a4-e7-af-d2    dynamic
  10.165.16.247        00-30-6e-fb-76-5b    dynamic
  10.165.16.248        00-11-43-41-20-54    dynamic
  10.165.16.249        00-12-79-bf-7f-48    dynamic
  10.165.16.250        00-e0-fc-84-2a-42    dynamic
  10.165.16.252        00-0f-b0-7a-7f-40    dynamic
  10.165.16.253        00-e0-fc-84-2a-42    dynamic
  10.165.16.254        00-e0-fc-84-2a-42    dynamic

C:\Documents and Settings\105005>_
```

假设: 电话簿上张三的电话号码被人改了, 你还能联系到他吗?

ARP攻击的类型

ARP攻击的本质就是修改网络中的“电话簿”，轻则造成网络故障，重则引起网络瘫痪。

虽然ARP病毒的种类很多，但基本攻击手段只有以下四种：

1. 仿冒网关攻击
2. 欺骗网关攻击
3. 欺骗终端用户攻击
4. Flood泛洪攻击

电话簿的故事……



老总和三个员工，每个人的电话簿都记录了其他人的号码。

王五这次没升经理，心里不平衡，准备搞点事，他有以下几个损招：

① 仿冒网关攻击——网络首害

修改所有人电话簿中老总的电话号码，大家都无法向老总汇报工作。老总很生气，后果很严重。

现象：瞬间全网瘫痪。查看每台PC机的ARP表，发现网关的MAC地址错误

```
C:\Documents and Settings\hbc>arp -a  
  
Interface: 10.165.16.138 --- 0x2 MAC地址错误  
Internet Address      Physical Address      Type  
10.165.16.1           00-e0-fc-84-2a-42   dynamic
```

重启网卡后恢复正常，但过一段时间网络又瞬间瘫痪。

防御思路：

- 1.接入交换机防御攻击报文(ARP入侵检测)
- 2.电脑上手工配置静态网关地址，防止网关“电话号码”被修改

② 欺骗网关攻击——暗箭伤人

修改老总电话簿中员工的号码。老总本来想通知张三国外考察，我看这小子不顺眼，小样的整不死你。

现象：

网络中PC逐台掉线，查看路由器ARP表项，发现很多错误地址。重启路由器后恢复正常，但过一段时间PC又开始掉线，导致很多用户怀疑是路由器故障。

序号	IP地址	MAC地址
1	10.165.16.224	0011-117d-fb92
2	10.165.16.138	0012-3f1c-cc7f
3	10.165.16.20	000f-e258-7e89
4	10.165.16.50	000f-e22c-b107
5	10.165.16.16	000f-e237-40bd
6	10.165.16.17	000f-e237-3fd6
7	10.165.16.15	000f-e237-409c

路由器中存的PC机
ARP信息不正确



防御思路：

这类攻击目标是网关设备，可以在任意一层网络设备上对攻击报文进行防御。

或者在路由器上面做IP与MAC的静态绑定

③ 欺骗终端用户攻击——移花接木

修改员工电话簿中其他员工的号码，妨碍员工间的交流。将张三的电话号码修改成自己的，听听别人跟张三说点什么。

现象：

局域网内电脑间无法相互通信。ARP - a发现其他电脑的ARP信息不正确

```
C:\Documents and Settings\hbc>arp -a

Interface: 10.165.16.138 --- 0x2
 Internet Address      Physical Address      Type
 10.165.16.1          00-e0-fc-84-2a-42    dynamic
 10.165.16.15         00-0f-e2-37-40-9c    dynamic
 10.165.16.16         00-0f-e2-37-40-bd    dynamic
 10.165.16.17         00-0f-e2-37-3f-d6    dynamic
 10.165.16.101        00-50-ba-19-3b-fb    dynamic
```

本地存的其他电脑的ARP信息不正确

防御思路：

通过接入交换机防御此类攻击报文。

④ 泛洪攻击——最没技术含量的

王五每天和老总通话24小时，另外两个人……

现象：

局域网一切正常，但无法访问外网。



防御思路：

这类攻击的目标是网关设备，可以在任意一层进行防御。

由于存在极多攻击报文，建议在接入交换机层进行防御，可以降低路由器和核心交换机的负担，更好的保证网络服务质量。

⑤ 其他攻击类型

基于四种基本攻击类型，ARP病毒可以略加改进，形成更多的攻击方式：

■有的ARP病毒专门在网吧中盗窃别人的QQ、网络游戏账号，使用的就是改进的仿冒网关攻击；还有用于监听内网通信的中间人攻击，就是由欺骗终端用户攻击演变来的。

■某些病毒和ARP攻击相结合，例如变种机器狗病毒、变种磁碟机病毒就借助ARP攻击在局域网内进行传播

万变不离其宗，只要能够防御四种基本攻击方式，ARP病毒就无计可施了。

ARP攻击防治难度

1. 千里之堤，溃于蚁穴

ARP病毒可以针对网络中的任意一层进行攻击，部分防御仍然存在风险

2. 组网差异，众口难调

企业、学校、酒店、网吧等组网都不同，不能靠一种方法解决所有问题

3. 类型多样，如何兼顾

ARP病毒种类众多，治标不治本只能是杯水车薪

下面向您介绍：

- ARP攻击引发的常见网络故障

- ARP攻击原理及防治难度

- ARP攻击防治思路

SARS病毒、ARP病毒相似之处

	SARS病毒	ARP病毒
传染源	非典患者及隐形感染者、动物（果子狸）不确定	感染ARP病毒的计算机
传播途径	直接接触、空气中飞沫传播	局域网
易感对象	所以不分年龄、性别，人群对该病毒普遍易感。	局域网、及局域网内所有设备
类型	传染病	网络传染病
危害	人类失去生命	局域网失效

SARS病毒防治方法

典型传染病防治措施 案例：**SARS**病毒防范

早发现、早诊断、早报告、早隔离、早治疗是预防传染病传播的主要措施

管理传染源

对呼吸道传染病，着重保持室内空气流通，必要时进行空气消毒、出门佩戴口罩等，必要时进行隔离

切断传播途径

非特异性措施：提高人群的一般抵抗力；
特异性措施：接种相应的疫苗

保护易感人群

ARP病毒防治方法

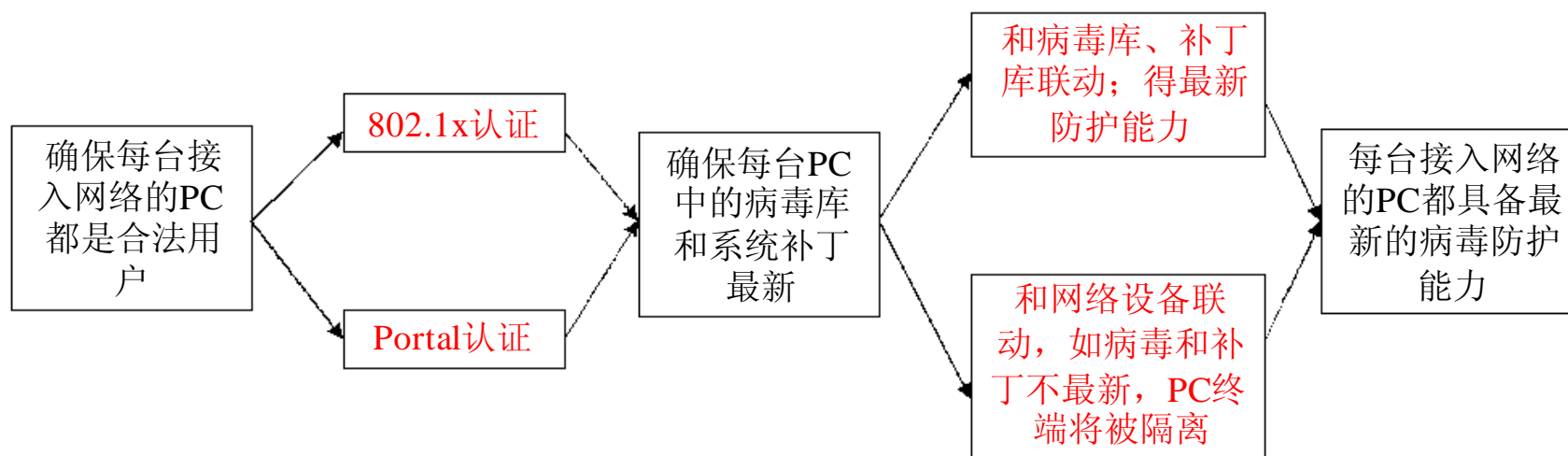
典型网络传染病防治措施 案例： ARP 病毒防范	
管理传染源	快速确定 ARP 病毒攻击源，定点清除
切断传播途径	切断 ARP 病毒攻击的传播途径
保护易感人群	保护PC机和网络设备不感染 ARP 病毒和未知病毒

通过和**SARS**病毒防治的类比，可以很容易举一反三！

保护PC机和网络设备不感染ARP病毒和未知病毒

保护易感人群

保护PC机和网络设备不感染ARP病毒和未知病毒



安网智能路由器如何防御ARP?

方法一：启用PPPoE服务器，内网用户采用PPPoE拨号方式接入网络。

PPPOE能真正防止ARP的原因不在于PPPOE接口IP和以太网接口IP不同,也不是通讯建立后不再用MAC等原因.而是因为PPPOE根本就没用的ARP协议,尽管它是用以太帧封装的,但它获得服务器MAC的方法不是用ARP协议,而是通过PADI包,所以它可以防止ARP攻击。

基本设置

PPPoE Server状态： 启用 PPPoE Server

只允许使用PPPoE接入： 设置后，只有PPPoE拨号后才能访问路由器，用于防止攻击，真正交换层过滤！

PPPoE 服务器名字： (英文字符) 允许任意服务器名接入

PPPoE 服务器的地址：

PPPoE 服务器的子网掩码：

首选 DNS 服务器： (如果未设置，将是默认的服务器的地址)

备份 DNS 服务器： (如果未设置，将是默认的服务器的地址)

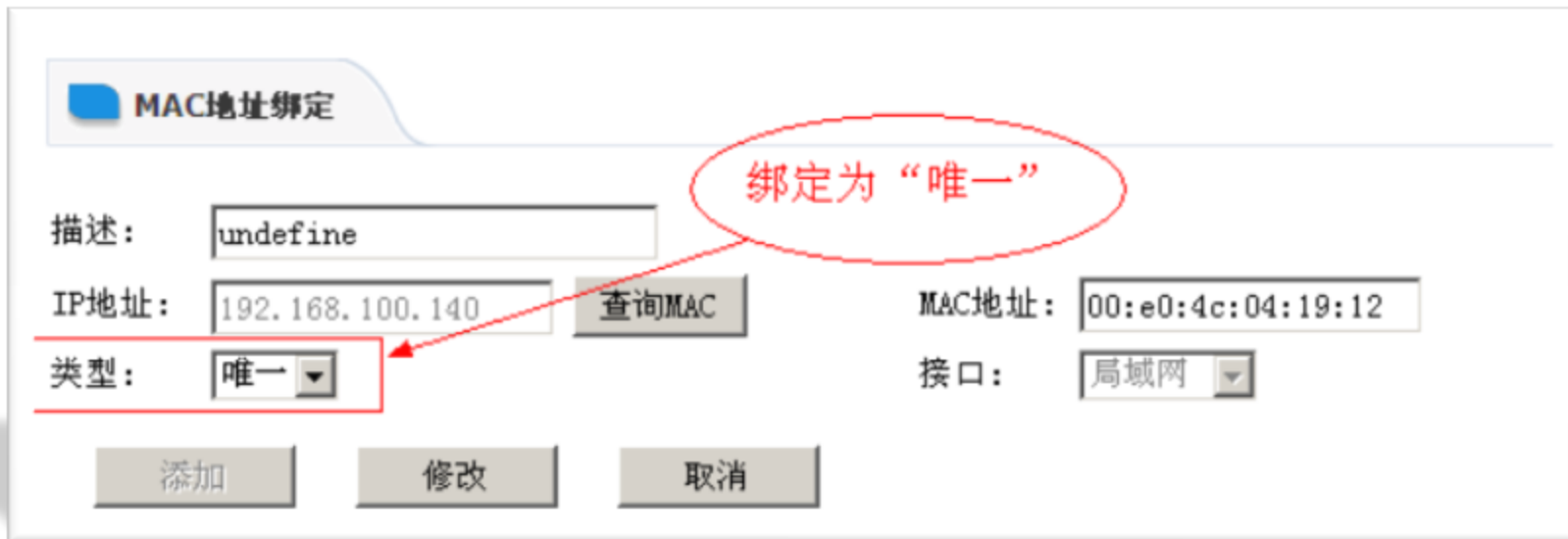
空闲检测时间： 秒(默认为6, 范围是 3-180)

多少个检测请求未应答则断开连接： 个(默认为10, 范围是 3-100)

认证方式： 不用加密的密码(PAP) 质询握手身份验证协议(CHAP) MS-CHAP MS-CHAP v2

方法二：启用IP/MAC绑定

为了防止用户随意更改IP地址或MAC地址，我们需要对IP地址和MAC地址进行绑定，但是这样并不能完全禁止用户自己修改IP或者MAC地址，更多的是防御ARP病的感染破坏。



The screenshot shows a configuration window titled "MAC地址绑定" (MAC Address Binding). The fields are as follows:

- 描述: undefine
- IP地址: 192.168.100.140 (with a "查询MAC" button next to it)
- MAC地址: 00:e0:4c:04:19:12
- 接口: 局域网
- 类型: 唯一 (highlighted with a red box and a red callout bubble containing the text "绑定为“唯一”")

At the bottom, there are three buttons: "添加" (Add), "修改" (Modify), and "取消" (Cancel).

方法三：启用ARP 防御



The image shows a configuration window titled "ARP安全防御" (ARP Security Defense). It contains three main sections:

- 防御“LAN口伪网关ARP攻击”** (Defense against LAN port fake gateway ARP attacks):
 - 启用: 启用 (Enabled)
 - 误差时间: ms (毫秒)
- 探测“LAN口非法网关”** (Detect illegal gateways on LAN port):
 - 启用: 启用 (Enabled)
 - 误差时间: s (秒)
- 智能分析处理** (Intelligent analysis and processing):
 - 处理级别: (Level: 中)

可有效防止内网非法网关对内网用户上网的影响，主动探测非法网关，保护正确的网关信息。

安网智能路由器产品介绍

产品介绍-NE系列

小型企业
理想解决方案

中小型企业
多WAN上网行为管理路由器

3WAN+1LAN
带机量60台



NE-1030W

4WAN+1LAN
带机量100台



NE-1040W

4WAN+1LAN
带机量150台



NE-2040

4WAN+1LAN
带机量250台

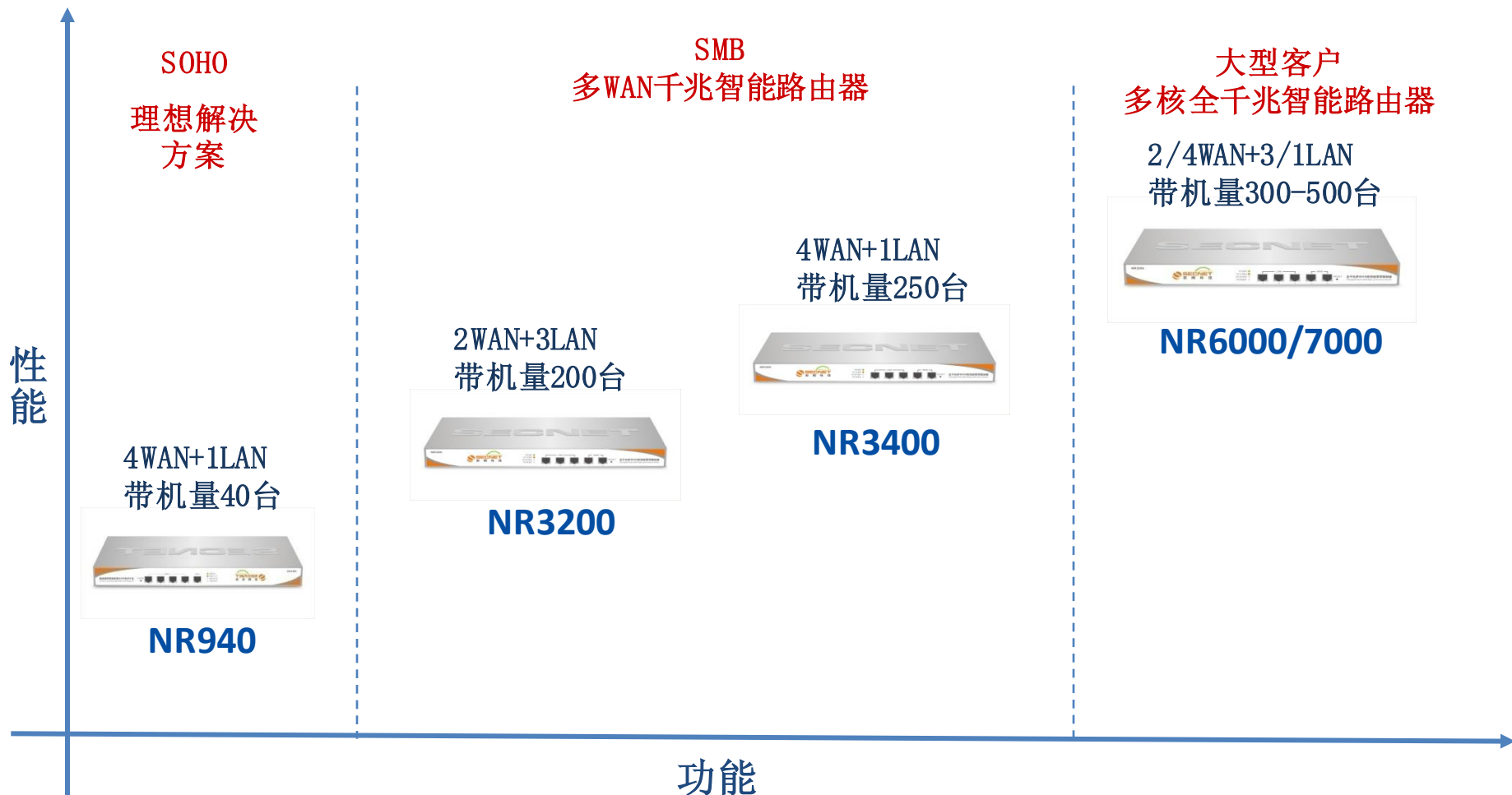


NE-3040

性能

功能

产品介绍-NR系列



安网智能路由器产品描述

一、多线负载均衡—多条宽带接入，提高网速又省钱

1、支持多线接入：具备4个WAN口，支持负载均衡、带宽汇聚、线路备份功能。可以使用多条ADSL取代光纤，或增加ADSL提升带宽，节省费用并且降低“单线故障”的风险，支持多种线路混合接入，采用多线程工具，可以达到叠加后的网络速度。

2、多线路分流策略：可依据来源IP、目的IP、来源端口、目的端口、域名进行线路分配或依据上网用户数量自动分配走向。同时根据线路带宽调节流量分配比例，使线路利用达到最佳，实现最佳的线路负载均衡。

3、安网智能均衡模式：在实现“电信流量走电信线路、联通流量走联通线路”的基础上，还可以同时接入长宽、教育网等不同运营商。自动优化业务数据，彻底解决不同运营商网络的互联互通问题；

4、线路通断检测与备份：线路自动检测备份，支持多种检测方式，确保企业网络永远在线。

二、智能化流量管理—智能分配带宽，网络不卡不掉线

1、 智能流控：只需要选择好广域网带宽，设备依据网络使用状况，时时优化带宽资源，保证游戏不卡，网页流畅。

2、 合理分配带宽：可以针对上下行选择不同的控制策略，可抢占或者固定带宽。可以指定时间段，从而可以根据需要自动加载预设的流控规则。可以针对不同接口的数据进行不同的流控，对于多线带宽相差较大的情况，可以更加合理的利用带宽，避免整体带宽资源的浪费。

3、 关键应用优先：用户可以自行指定需要保障优先的重要应用数据，从而对该部分数据在任何情况下优先保障传输，从而保证企业关键业务应用的通畅。

4、 支持带宽保证功能。

三、网络安全应用—防病毒抗攻击，网管省心又省力

- 1、ARP安全机制：领先的ARP信任机制与内网ARP防御功能结合，杜绝ARP病毒，防止内网掉线。
- 2、探测“LAN口非法网关”：领先的防御内网网关伪造功能。
- 3、内网防攻击功能：可以有效抵御内网的DDoS/SYN攻击，并防止常见的“land、spoofing等攻击。
- 4、连接限制功能：可以针对指定IP限制其网络连接数，从而可以有效的防止用户使用P2P软件滥用带宽。

四、上网行为管理--规范上网行为，员工工作效率高

- 1、URL网站分类，对各种类型网址进行分类管理，指定用户在指定时间内访问指定网站
- 2、URL黑白名单，让员工在上班时间只能访问工作相关网站，提高工作效率的同时避免中毒概率。
- 3、QQ黑白名单，让企业上班指定的客服QQ才能登陆。
- 4、P2P程序管理，多大21种P2P程序、在线视频、聊天工具管理。
- 5、访问控制权限，让指定部门只能访问内部网络和收发邮件，禁止访问INTELNET。
- 6、多子网隔离，让不同部门之间互相隔离，避免病毒传播和机密数据泄露。

五、内网PPPoE/WEB认证服务器/即插即用

支持PPPoE/Web认证功能，内网用户通过操作系统的PPPoE拨号功能或WEB认证后连接到路由器上网。

PPPoE Server优势：

- 1、网络管理：通过给每个用户指定账号，来有效管理用户对网络访问。
- 2、宽带计费：针对每个账号进行计费管理，支持到期提醒功能，用户在线查询以及修改密码等功能，让小区运营更加智能化。
- 3、防ARP欺骗：只允许PPPoE拨号上网，彻底杜绝内网用户修改IP地址、MAC地址等信息,有效的摆脱ARP数据包的困扰，彻底解决了网络中IP欺骗等绝大部分网络问题。
- 4、Web认证：用户通过指定账号访问网络，适合咖啡屋、酒店等公共场合，作为网络计费的同时可以达到宣传效果。在企业可作为员工上网权限管理。

5、即插即用：在设备上启用即插即用后，内网用户无需更改任何设置，即无论内网用户的IP地址、子网掩码、网关和DNS服务器如何变化，都可以通过本设备上网。极大地方便了酒店用户、出差办公用户随时随地地接入互联网，提高了网络管理的便捷性和效率

六、强劲无线性能，无线办公首选(大功率)

(安网NE1030W / NE1040W)支持IEEE 802.11b/g/n协议，提供300M无线速率；2x2MIMO架构，镀金SMA接口，配置2支5db可拆卸高增益全向天线，轻松应对小型企业、家庭、出租屋等无线网络环境。

相对传统54M和150M产品，能满足更多无线客户端接入；在无线客户端数量相同时，能够为每个客户端提供更高的无线带宽，避免数据拥塞，减小网络延时，为移动办公提供稳定的网络基础。

- 1、 支持64/128位WEP数据加密， WPA、 WPA2、 WPA/WPA2混合等多种加密与安全机制。
- 2、 支持IEEE 802.11n、 IEEE 802.11g、 IEEE 802.11b、 IEEE 802.3以及 IEEE 802.3u标准。
- 3、 支持多达5组无线SSID和隐藏无线SSID功能。
- 4、 基于不同SSID的MAC地址的访问控制(多达50组)。

七、虚拟VPN功能

支持PPTP/L2TP服务器与客户端功能，让企业的不同区域的部门随时访问公司局域网的ERP、CRM、企业邮局等系统，提高工作效率。外出差的员工也可以通过操作系统自带的拨号功能，随时随地通过私有的通道安全的访问到公司内部网络，获取相应资源。

八、网络通告功能

通告功能是一个特别人性化的网络管理功能，它可以发挥一种快速传达信息的工具和强大的广告宣传功效，尤其可以针对企业管理部门向员工传达的重大信息公告（即时信息的通告、问题决策的传达或临时会议通知等）、酒店提醒入住客人的注意事项（如用餐时间和种类、即时交通信息等）、小区即时公共信息的通告（如公共活动信息和台风、低温等即时天气信息等）、网吧的合法化经营（禁止未成年人上网、禁止访问非法网站的警示信息等）。

九、好使用易管理

1、内网管理轻松直观：通过直观的数据流量图和网络状态报告，每条线路的数据流量都一目了然。您可以实时统计每个IP的累计流量、实时流量、网络连接数等关键指标，全面分析每个IP的网络连接详情，网络问题的定位也易如反掌

2、配置备份与导入：可将每种配置文件保存到电脑，需要重新配置路由器时，可导入相应配置文件，缩短配置时间。

3、使用方便：全中文WEB配置及管理页面，配置简单，不需专业网管。支持免费软件升级功能，全面满足中小型企业、网吧用户对多WAN口接入的需求。

SECNET

安网智能流控方案解决专家

<http://www.secnet.cn>