

## (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局(43) 国际公布日  
2008 年 11 月 27 日 (27.11.2008)

PCT

(10) 国际公布号  
WO 2008/141584 A1

(51) 国际专利分类号:

*H04L 12/56* (2006.01)    *H04L 12/26* (2006.01)  
*H04L 29/06* (2006.01)    *H04L 12/66* (2006.01)[CN/CN]; 中国广东省深圳龙岗坂田华为基地行政  
总部办公楼, Guangdong 518129 (CN)。

(21) 国际申请号:

PCT/CN2008/071043

(72) 发明人; 及

(22) 国际申请日:

2008 年 5 月 22 日 (22.05.2008)

(75) 发明人/申请人 (仅对美国): 谭学飞(TAN, Xuefei)  
[CN/CN]; 中国广东省深圳龙岗坂田华为基地行政  
总部办公楼, Guangdong 518129 (CN)。

(25) 申请语言:

中文

(74) 代理人: 北京挺立专利事务所(BEIJING TINGLI  
PATENT AGENCY); 中国北京市西城宣武门西大  
街129号金隅大厦804-806室, Beijing 100031 (CN)。

(26) 公布语言:

中文

(81) 指定国 (除另有指明, 要求每一种可提供的国家  
保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB,  
BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU,  
CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,  
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP,  
KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS,

[见续页]

(71) 申请人 (对除美国外的所有指定国): 华为技术  
有限公司(HUAWEI TECHNOLOGIES CO., LTD.)

(54) Title: MESSAGE PROCESSING METHOD, SYSTEM, AND EQUIPMENT

(54) 发明名称: 报文处理方法、系统和设备

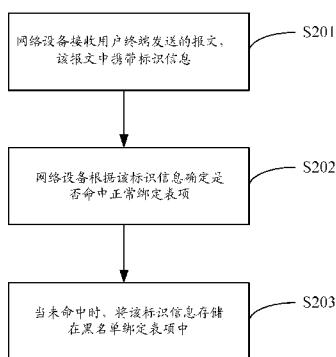


图 2 / Fig. 2

S201 NETWORK EQUIPMENT RECEIVES MESSAGE TRANSMITTED BY USER TERMINAL, THE MESSAGE CARRIES THE IDENTIFIER INFORMATION  
 S202 NETWORK EQUIPMENT DETERMINES WHETHER IT HITS THE NORMAL BINDING TABLE ITEMS OR NOT ACCORDING TO THE IDENTIFIER INFORMATION  
 S203 WHEN IT DOES NOT HIT THE NORMAL BINDING TABLE ITEMS, THE IDENTIFIER INFORMATION IS STORED IN BLACKLIST BINDING TABLE ITEMS

**(57) Abstract:** Method for message processing is disclosed, which includes: receiving message transmitted by user terminal, the message carries the identifier information; getting the identifier information, and looking the binding table with the identifier information in the key words; when it doesn't hit the normal binding table items, storing the identifier information in blacklist binding table items of the binding table. Message processing system and equipment are also provided. A blacklist binding table items is added, which could efficiently track attacker's detail action and information, and benefit to locate and remove fault.

[见续页]



LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,

SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国国际公布:  
— 包括国际检索报告。

---

(57) 摘要:

本发明实施例公开了一种报文处理方法,包括:接收用户终端发送的报文,所述报文携带标识信息;获取所述标识信息,以所述标识信息为关键字查找绑定表;当未命中所述绑定表中的正常绑定表项时,将所述标识信息存储在所述绑定表中的黑名单绑定表项中。本发明实施例还提供了一种报文处理系统和设备。本发明实施例增加了一种黑名单绑定表项,可以有效跟踪攻击者的具体行为和信息,便于故障的定位和排除。

## 报文处理方法、系统和设备

### 技术领域

本发明涉及网络通信技术领域，尤其涉及一种报文处理方法、系  
5 统和设备。

### 背景技术

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复  
杂，经常出现计算机位置变化和计算机数量超过可分配 IP ( Internet  
10 Protocol, 因特网协议 ) 地址的情况，现有技术通常采用 DHCP  
( Dynamic Host Configuration Protocol, 动态主机配置协议 )，来解决  
IP 地址动态分配的问题，DHCP 具有对重新使用的网络地址进行自动  
分配和附加配置选项的功能。

DHCP 在应用过程中遇到很多安全方面的问题，攻击者利用  
15 DHCP 进行攻击的主要手段包括：DoS ( Denial of Service, 拒绝服务 )  
攻击、DHCP Server 仿冒攻击以及中间人攻击和 IP/MAC ( Media  
Access Control, 媒体接入控制 ) 欺骗攻击等。其中，中间人攻击和  
IP/MAC 欺骗攻击主要是由攻击者向受害者发送带有欺骗信息的虚假  
20 报文，让受害者学习到该欺骗信息，并根据该欺骗信息进行报文的转  
发，从而使得受害者无法正常接收或发送报文。

现有技术通常采用在接入用户终端的网络设备处使能 DHCP  
Snooping ( Dynamic Host Configuration Protocol Snooping, 动态主机  
配置协议监听 ) 功能，DHCP Snooping 协议栈通过监听 DHCP 报文，  
建立 IP、MAC、端口和 VLAN ( Virtual Local Area Network, 虚拟局  
域网 ) 绑定表；在转发报文时，利用绑定表对 ARP( Address Resolution  
25 Protocol, 地址解析协议 ) 报文、IP 报文进行检查，解决上述的欺骗  
攻击安全问题。

图 1 是现有技术中采用 DHCP Snooping 解决欺骗攻击安全问题  
的示意图。如图 1 所示，在接入用户终端的网关交换机上，使能 DHCP

Snooping 功能，则无论是正常用户终端，如用户终端 B，还是其它可能有攻击行为的用户终端，如用户终端 C，首先必须通过 DHCP 进行首次 IP 地址申请。网关交换机监听申请过程中的所有 DHCP 报文，通过分析往来的 DHCP 报文，建立图 1 所示的 DHCP Snooping 绑定表。那么，当攻击者发起欺骗攻击时，如用户终端 C 发起一个免费 ARP 报文给 B 欺骗用户终端 B 说，IP 地址为 10.1.1.1 网关路由器的 MAC 为 C，那么在网关交换机处将对此 ARP 报文进行检测，该 ARP 报文携带的信息，包括其源 MAC 地址，源 IP 地址以及入接口信息，如图 1 所示，MAC 地址为 C、IP 地址为 10.1.1.1、PORT（端口）为 E2、VLAN（Virtual Local Area Network，虚拟局域网）为 3，去查找绑定表，由于没有对应的表项，因此网关交换机将该报文丢弃，则此欺骗 ARP 报文将无法到达其它任何用户终端，包括用户终端 B，从而制止了用户终端 C 的攻击行为。

在实现本发明的过程中，发明人发现现有技术至少存在以下问题：现有技术中采用 DHCP Snooping 解决攻击者攻击的方法中，由于对攻击者的行为没有任何记录，因此，无法有效跟踪攻击者的具体行为和信息，从而导致故障的定位和排除非常困难。

## 发明内容

本发明实施例提供一种报文处理方法、系统和设备，以解决现有技术中采用 DHCP Snooping 解决报文攻击安全问题时，对攻击者的行为没有跟踪记录，故障定位排除困难的缺陷。

为达上述目的，本发明实施例提供了一种报文处理方法，包括：

接收用户终端发送的报文，所述报文携带标识信息；

根据所述标识信息确定是否命中正常绑定表项；

当未命中时，将所述标识信息存储在黑名单绑定表项中。

本发明实施例还提供了一种报文处理系统，包括：

用户终端，用于向网络设备发送报文，所述报文携带标识信息；

网络设备，用于判断所述报文是否命中正常绑定表项，当未命中时，将所述标识信息存储在黑名单绑定表项中。

本发明实施例还提供了一种网络设备，包括：

报文判断单元，用于判断所接收的报文是否命中正常绑定表项；

5 信息存储单元，用于当所述报文未命中所述正常绑定表项时，将所述报文的标识信息进行存储。

与现有技术相比，本发明实施例增加了黑名单绑定表项，可以有效跟踪攻击者的具体行为和信息，方便了故障的定位和排除。

## 10 附图说明

图 1 是现有技术中采用 DHCP Snooping 解决欺骗攻击安全问题的示意图；

图 2 是本发明实施例一的报文处理方法流程图；

图 3 是本发明实施例二的报文处理方法流程图；

15 图 4 是本发明实施例绑定表信息异常丢失的示意图；

图 5 是本发明实施例设置黑名单绑定表项的示意图；

图 6 是本发明实施例重新建立绑定表项的示意图；

图 7 是本发明实施例三的报文处理方法流程图；

图 8 是本发明实施例一种报文处理系统的示意图。

20

## 具体实施方式

本发明实施例提供了一种报文处理方法。现有技术中的绑定表只包括有KEY，如图1中所示的源MAC、源IP、PORT和VLAN，本发明的实施例在保持现有技术KEY不变的基础上，增加了两个字段，其中一个字段用来表示该绑定表项的类型，一类是正常DHCP Snooping绑定表项，另一类是非正常DHCP Snooping绑定表项，由于某报文没有命中正常绑定表项而从该报文中提取相关信息创建的绑定表项，也称为黑名单绑定表项；另一个字段用来表示该黑名单绑定表项被命中的

频率。通过对用户终端 100 的信息在黑名单绑定表项被命中频率的统计，从而有效监控攻击者的行为和信息。本发明实施例采用一个字段来标识同一绑定表中的正常绑定表项和黑名单绑定表项，当然，在实际应用中，也可采用单独的绑定表来分别存储正常绑定表项和黑名单绑定表项的信息。  
5

本发明实施例一的报文处理方法的流程图，如图 2 所示，包括以下步骤：

步骤 S201，网络设备 200 接收用户终端 100 发送的报文，该报文中携带标识信息。该报文包括用户终端 100 的正常上网报文，当然也可能存在攻击者发送的攻击报文。  
10

步骤 S202，网络设备 200 根据该标识信息确定是否命中正常绑定表项。

网络设备 200 所接收的报文中包括用户终端 100 的正常上网报文，但是也可能存在攻击者发送的攻击报文，网络设备 200 需要对所接收的报文进行辨别。  
15

由于在网络设备 200 的入端口使能了 DHCP Snooping 功能，因此，网络设备 200 需要对所有接收到的报文进行分析判断，解析所接收报文的标识信息，该标识信息包括报文的：源 MAC 地址、源 IP 地址、PORT 和 VLAN，然后将该源 MAC 地址、源 IP 地址、PORT 20 和 VLAN 与网络设备 200 正常绑定表项中对应的源 MAC 地址、源 IP 地址、PORT 和 VLAN 信息进行匹配。也就是说，网络设备 200 根据所接收报文的标识信息，查找正常绑定表项中有无对应的信息，若查找到对应信息，则信息匹配成功；若没有查找到对应信息，则信息匹配不成功。若信息匹配成功，则称命中正常绑定表项；若信息匹配不成功，则称没有命中正常绑定表项。本发明实施例中是将报文标识信息中的源 MAC 地址、源 IP 地址、PORT 和 VLAN 进行匹配，当然，在实际应用中，用来进行匹配的标识信息也可根据具体需要，在源 MAC 地址、源 IP 地址、PORT 和 VLAN 之间进行任意搭配。  
25

步骤 S203，当未命中时，网络设备 200 将该标识信息存储在黑

名单绑定表项中。

当网络设备 200 接收到的报文未命中正常绑定表项时，网络设备 200 从没命中正常绑定表项的报文中提取源 MAC 地址、源 IP 地址、PORT 和 VLAN 信息，并将该些源 MAC 地址、源 IP 地址、PORT 和 VLAN 信息存储在黑名单绑定表项的对应各表项中。并且网络设备 200 记录该没命中正常绑定表项报文的接收时间和命中次数，通过记录的接收时间和命中次数计算出该非正常报文的发送频率，并将计算出的发送频率存储在黑名单绑定表项中用来存储频率信息的字段中。  
5

上述本发明的实施例，在现有绑定表的基础上增加黑名单绑定表项类型，用来存储没命中正常绑定表项的报文的相关信息，并且通过对报文命中黑名单绑定表项的频率进行统计，从而可实现对攻击者的攻击行为和信息进行有效跟踪和监控。  
10

在实际应用中，也会出现用户终端 100 发送的正常报文无法命中网络设备 200 正常绑定表项的情况，例如：网络设备 200 中正常绑定表项信息的异常丢失。网络设备 200 正常绑定表项信息异常丢失的原因有很多种，包括：  
15

由于一个网络设备 200 上要接入大量的用户终端 100，而用于存放正常绑定表项的空间有限，因此，需要对长期没有命中的正常绑定表项项进行删除；

20 或者，由于使能DHCP Snooping功能的网络设备 200 重新启动，而原正常绑定表项保存恢复过程中发生部分数据丢失；

或者，使能DHCP Snooping功能的网络设备 200 由于自身内部通信原因，而造成的正常绑定表项中的数据丢失；

再或者，网络设备 200 的一个端口上一旦使能DHCP Snooping 功能，那么在使能前已经通过DHCP获得IP地址的用户终端 100 将在网络设备 200 中没有DHCP绑定表项，此时也可以理解为该用户终端 100 的绑定表数据异常丢失。  
25

现有技术中采用 DHCP Snooping 对报文进行监听，一旦用户终端 100 通过 DHCP 动态申请 IP 地址成功以后，能否上网，完全取决

于用户终端 100 报文的相关信息能否与网络设备 200 正常绑定表项中某一项匹配，如果不匹配，用户终端 100 报文将被丢弃，用户终端 100 将无法上网。在由于上述正常绑定表项异常丢失，导致用户终端 100 无法正常上网的情况下，如果用户终端 100 需要继续上网，则只能通过手工触发用户终端 100 重新通过 DHCP 进行 IP 地址申请，或者等目前申请的 IP 地址过期后再上网。

所谓手工触发用户终端 100 重新通过 DHCP 进行 IP 地址申请，是指用户终端 100 释放现有的 IP 地址，然后向网络设备 200 重新发送 IP 地址申请请求；通过重新发送 IP 地址申请，用户终端 100 重新获得新的 IP 地址，同时在网络设备 200 上建立新的绑定表信息。手工触发用户终端 100 重新进行 IP 地址申请，需要用户终端 100 首先感知到已无法正常上网的情况，但是在实际应用中，从用户终端 100 无法正常上网到用户终端 100 感知到无法正常上网的时间会比较长，因此会导致较长时间的用户终端 100 上网中断。

所谓等目前申请的 IP 地址过期后再上网，是指等用户终端 100 目前申请的 IP 地址过期后，用户终端 100 会检测到 IP 地址过期，然后自动向网络设备 200 发送 IP 地址申请请求；通过重新发送 IP 地址申请，用户终端 100 重新获得新的 IP 地址，同时在网络设备 200 上建立新的绑定表信息。等目前申请的 IP 地址过期后再上网，显然更需要用户终端 100 等待较长的时间，从而会导致用户终端 100 长时间的上网中断。

针对上述的问题，本发明实施例二在网络设备 200 接收到用户终端 100 发送的报文无法命中正常绑定表项的情况下，主动向用户终端 100 发送 IP 地址不可用信息，触发用户终端 100 向网络设备 200 重新发送 IP 地址申请请求，立即申请新的 IP 地址，快速恢复上网。如图 3 所示，为本发明实施例二的报文处理方法流程图，包括以下步骤：

步骤 S301，网络设备 200 接收用户终端 100 发送的报文无法命中正常绑定表项。

在网络设备 200 上由于前述的某种原因，或者其它原因，导致网

络设备200的正常绑定表项信息丢失，则一般用户终端100无法感知此情况的发生，甚至很有可能都不知道在网络设备200上使能了DHCP Snooping功能。此时，用户终端100会继续正常上网，并向网络设备200发送报文，该发送的报文包括两种类型：一种是用户终端100正常上网的数据报文，如IP报文或ARP报文等；另一种是由于IP租约期将至，用户终端100发送的租期续约请求报文。

10 网络设备200从所接收的报文中提取源MAC地址、源IP地址、PORT和VLAN信息，然后将该源MAC地址、源IP地址、PORT和VLAN信息与网络设备200正常绑定表项中对应的源MAC地址、源IP地址、PORT和VLAN信息进行匹配，无法匹配成功，也即用户终端100发送的报文没有命中网络设备200的正常绑定表项。

15 例如，如图4所示的本发明实施例绑定表信息异常丢失示意图。用户终端100B向网关交换机发送报文，该报文中携带有用户终端100的源IP地址和源MAC地址信息，源IP地址信息为：10.1.1.2，源MAC地址信息为：B。网关交换机接收到该报文后，从中提取源MAC地址信息和源IP地址信息，再加上网关交换机的端口信息，也即网关交换机的端口号和VLAN信息，去查找绑定表中的对应信息。但是，由于网关交换机中对应用户终端100B的绑定表信息丢失，因此无法查找到绑定表中的对应信息，也就无法命中绑定表。

20 步骤S302，网络设备200将没命中正常绑定表项的报文标识信息存储在黑名单绑定表项中。

25 网络设备200从没命中正常绑定表项的报文中提取源MAC地址、源IP地址、PORT和VLAN信息，并将该些源MAC地址、源IP地址、PORT和VLAN信息存储在黑名单绑定表项中。并且网络设备200在黑名单绑定表项中，记录该没命中正常绑定表项报文的接收时间和命中次数，通过记录的接收时间和命中次数计算出该没命中正常绑定表项的报文发送频率，并将计算出的发送频率存储在黑名单绑定表项中用来存储频率信息的字段中。

仍以步骤S301中的举例为例，用户终端100B发送的报文没能命

中网关交换机的绑定表，因此该报文被网关交换机判定为非正常报文。网关交换机会对应绑定表中的存储表项，从该报文中提取源 IP 地址、源

MAC地址信息、端口号和VLAN等信息，将该些信息存入绑定表的对应表项中。网关交换机还会记录该报文的接收时间和当前命中次数，通过记录的接收时间和命中次数计算出该没命中正常绑定表项的报文发送频率，并将计算出的发送频率存储在黑名单绑定表项中用来存储频率信息的字段中。在黑名单绑定表项中建立一个字段来标识该段绑定表信息的类型，即非正常报文。举例来说，该黑名单绑定表项如图5中所示，在绑定表中建立BLK字段，在该BLK字段中设置不同的标识，代表该段绑定表的不同类型。Y代表该段绑定表为正常绑定表项，N代表该段绑定表为黑名单绑定表项；并在绑定表中建立一个 RATE（频率）字段，将计算出没命中正常绑定表项的报文发送频率存储在RATE字段中。

步骤S303，网络设备200向用户终端100发送IP地址不可用信息。

网络设备200向用户终端100发送IP地址不可用信息，以告知该用户终端100当前的IP地址已经不可用。用户终端100接收到网络设备200发送的IP地址不可用信息后，得知当前的IP地址已经不能再使用，用户终端100若再使用当前的IP地址已不能再上网。若用户终端100需要继续上网，可以向网络设备200重新发送IP地址申请请求，重新申请新的IP地址。

接续步骤S302中的举例，网关交换机将该没命中正常绑定表项的报文重定向到DHCP Snooping功能模块，并由DHCP Snooping功能模块向用户终端100B发送一个DHCPNAK报文，仿冒DHCP服务器告知用户终端100B其IP地址不可用。DHCPNAK，是DHCP服务器用来告诉用户终端100其IP地址已经不正确，或租约期时间过期，而向用户终端100发送的报文。如果用户终端100B收到DHCPNAK消息后，它将不再使用原有的IP地址，而重新启动DHCP配置流程来重新申请新的IP地址。

步骤S304，用户终端100接收到IP地址不可用信息后，向网络设备200重新发送IP地址申请请求。

5 用户终端100接收到网络设备200发送的IP地址不可用信息后，得知当前的IP地址已经不能再使用，用户终端100若再使用当前的IP地址已不能再上网。若用户终端100需要继续上网，则可以向网络设备200重新发送IP地址申请请求，重新申请新的IP地址。网络设备200按照正常的DHCP Snooping流程，通过监听用户终端100发送的DHCP报文，重新建立针对该用户终端100的绑定表，则该用户终端100在申请IP地址成功之后可以照常上网了。

10 接续步骤S303中的举例，用户终端100B接收到网关交换机发送的DHCPNAK报文后，得知当前的IP地址已经不能再使用，于是按照DHCP流程，用户终端100B向网关交换机重新发起首次IP地址申请的请求。网关交换机按照正常的DHCP Snooping流程，通过监听用户终端100B发送的DHCP报文，重新建立针对用户终端100B的绑定表项，  
15 如图6所示，图6是本发明实施例重新建立绑定表项的示意图，该重新建立的绑定表项包括源IP地址、源MAC地址、端口号、VLAN和BLK等信息，由于用户终端100B在网关交换机上重新建立的绑定表项属于正常绑定表项，绑定表项中的BLK标识为Y，而RATE表项是用来记录没命中正常绑定表项的报文的频率信息，因此该重新建立的绑定表项中也就不存在RATE信息，也可认为RATE信息为空。用户终端100B  
20 在申请新的IP地址成功之后即可照常上网了。

上述本发明的实施例，在网络设备200接收到的报文无法命中正常绑定表项的情况下，主动向用户终端100发送IP地址不可用信息，从而能够触发因网络异常导致无法正常上网的用户终端100重新发起IP地址申请流程，即可快速恢复上网功能，大大提高了网络服务质量。  
25

但是，考虑到实际应用中，攻击者会向网络设备200频繁发送无法通过DHCP Snooping认证的报文，由于该报文无法命中正常绑定表项，按照本发明实施例二的流程，网络设备200则会频繁向用户终端100发送IP地址不可用信息，从而会增加网络设备200的处理工作量，

降低系统性能。

针对上述问题，本发明实施例三对前述的实施例进行改进，在网络设备200中设定一个阀值，将黑名单绑定表项中的报文发送频率和该阀值进行比较，当报文发送频率大于阀值的时候，网络设备200则  
5 停止向发送该报文的用户终端100发送IP地址不可用信息。当然，上述阀值可以预先在网络设备200上设定好，也可在实际应用中根据具体情况进修改，重新设定。

如图7所示，是本发明实施例三的报文处理方法流程图，具体包括以下步骤：

10 步骤S701，网络设备200接收用户终端100发送的报文无法命中正常绑定表项。该步骤的具体实施过程与前述相同，在此不再多述。

步骤S702，网络设备200将没命中正常绑定表项的报文标识信息存储在黑名单绑定表项中。该步骤的具体实施过程与前述相同，在此也不再多述。

15 步骤S703，网络设备200根据黑名单绑定表项中的频率信息判断是否向用户终端100发送IP地址不可用信息。

该频率信息是网络设备200根据记录报文的发送时间和命中次数计算出来的，网络设备200每收到一次该没命中正常绑定表项的报文，则记录该报文的发送时间和命中次数，然后根据记录的发送时间和命中次数计算出该报文的频率信息。网络设备200将该频率和设定的阀值进行比较，若该频率小于阀值，则网络设备200向用户终端100发送IP地址不可用信息；若该频率大于阀值，则网络设备200停止向用户终端100发送IP地址不可用信息。网络设备200将发送频率大于阀值的报文判定为攻击报文，网络设备200对该攻击报文直接丢弃，不做再  
20 任何处理。  
25

上述本发明的实施例，将发送频率大于设定的阀值的报文判定为攻击报文，并停止向发送攻击报文的用户终端100发送IP地址不可用信息，可有效避免攻击者的频繁攻击。

本发明的实施例还提供了一种报文处理系统，如图8所示，包括：

用户终端100和网络设备200。其中，用户终端100，用于向网络设备200发送报文。

网络设备200，用于将所接收报文中，没命中正常绑定表项的报文标识信息存储在黑名单绑定表项中。

5 其中，网络设备200包括：报文判断单元210和信息存储单元220。报文判断单元210，用于获取接收的报文携带的标识信息，以该标识信息为关键字查找绑定表，确定接收的报文是否命中正常绑定表项。报文判断单元210根据所接收报文的标识信息，查找正常绑定表项中有无对应的信息，若查找到对应信息，则信息匹配成功；若没有查找到对应信息，则信息匹配不成功。若信息匹配成功，则命中正常绑定表项；若信息匹配不成功，则没有命中正常绑定表项。信息存储单元220，用于在所述绑定表中的黑名单绑定表项中，存储没命中正常绑定表项的报文标识信息。网络设备200从没命中正常绑定表项的报文中提取相关信息，并将该些信息存入信息存储单元220的对应表项中。

15 信息存储单元220包括：标识信息存储子单元221、记录子单元222、频率计算子单元223和频率存储子单元224。标识信息存储子单元221，用于存储没命中绑定表报文的标识信息。记录子单元222，连接标识信息存储子单元221，用于记录没命中绑定表报文的接收时间和命中次数。频率计算子单元223，连接记录子单元222，用于根据记录子单元222中所记录报文的接收时间和命中次数计算没命中绑定表报文的发送频率。频率存储子单元224，连接频率计算子单元223，用于存储没命中绑定表报文的发送频率。

本发明另一实施例在上述网络设备200的基础上，增设了信息发送单元230和频率比较单元240。信息发送单元230，连接信息存储单元220，用于向用户终端100发送IP地址不可用信息。频率比较单元240，连接信息存储单元220，用于将信息存储单元220中没命中绑定表报文的发送频率和设定的阀值进行比较，作为是否向用户终端100发送IP地址不可用信息的依据，当报文的发送频率小于设定的阀值时，通知信息发送单元230向用户终端100发送IP地址不可用信

息。

本发明的实施例增加了一种黑名单绑定表项类型，可以有效跟踪攻击者的具体行为和信息，了解攻击者的攻击频率，以及主要攻击对象。本发明的实施例中，在用户终端 100 的报文无法命中绑定表，从而导致用户终端 100 无法正常上网的情况下，可以主动触发用户终端 100 重新发起地址申请流程，即可快速恢复上网功能，大大提高了网络服务质量。本发明实施例中的网络设备 200 包括交换机、路由器等具有报文处理能力的网络设备 200。且本发明实施例中对应的软件可以存储在一个计算机可读取存储介质中。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

## 权利要求

1、一种报文处理方法，其特征在于，包括：

接收（201）用户终端发送的报文，所述报文携带标识信息；

5 获取（202）所述标识信息，以所述标识信息为关键字查找（202）  
绑定表；

当未命中所述绑定表中的正常绑定表项时，将所述标识信息存储  
(203, 302, 702) 在所述绑定表中的黑名单绑定表项中。

2、如权利要求 1 所述方法，其特征在于，所述将所述标识信息  
10 存储 (203, 302, 702) 在所述绑定表中的黑名单绑定表项之后，还  
包括：向用户终端发送 (303) IP 地址不可用信息。

3、如权利要求 1 所述方法，其特征在于，所述将所述标识信息  
信息存储 (203, 302, 702) 在所述绑定表中的黑名单绑定表项中之后，  
还包括：记录 (703) 所述报文的发送频率，将所述发送频率与阀值  
15 进行比较(703)，当所述发送频率小于阀值时，向用户终端发送 (703)  
IP 地址不可用信息。

4、如权利要求 3 所述方法，其特征在于，所述记录 (703) 所述  
报文的发送频率具体包括：

记录所述报文的接收时间和命中次数；

20 根据所述接收时间和命中次数计算所述报文的发送频率；

将所述发送频率存储在所述黑名单绑定表项中。

5、如权利要求 4 所述方法，其特征在于，将所述发送频率存储  
(702) 在所述黑名单绑定表项中具体为：将所述发送频率存储 (304)  
在黑名单绑定表项的频率字段中。

25 6、如权利要求 1 所述方法，其特征在于，所述绑定表包含绑定  
表项类型字段，标识正常绑定表项和黑名单绑定表项。

7、如权利要求 1 所述方法，其特征在于，所述标识信息包括：  
所述报文的源媒体接入控制 MAC 地址、源 IP 地址、端口 PORT 和  
虚拟局域网 VLAN。

8、一种报文处理系统，其特征在于，所述系统包括网络设备（200），用于与用户终端（100）通信，具体为：

接收用户终端（100）发送的报文，所述报文携带标识信息；

获取所述标识信息，以所述标识信息为关键字查找绑定表；

5 当未命中所述绑定表中的正常绑定表项时，将所述标识信息存储在所述绑定表中的黑名单绑定表项中。

9、如权利要求8所述报文处理系统，其特征在于，所述网络设备（200）还用于在将所述标识信息存储在所述绑定表中的黑名单绑定表项之后，向用户终端（100）发送IP地址不可用信息。

10、如权利要求8所述报文处理系统，其特征在于，所述网络设备（200）还用于在将所述将标识信息存储在所述绑定表中的黑名单绑定表项中之后，记录所述报文的发送频率，将所述发送频率与阀值进行比较，当所述发送频率小于阀值时，向用户终端（100）发送IP地址不可用信息。

15 11、一种网络设备（200），其特征在于，包括：

报文判断单元（210），用于获取接收的报文携带的标识信息，以所述标识信息为关键字查找绑定表，确定所述报文是否命中正常绑定表项；

20 信息存储单元（220），用于当所述报文未命中所述正常绑定表项时，将所述报文的标识信息存储在所述绑定表中的黑名单绑定表项中。

12、如权利要求11所述网络设备（200），其特征在于，所述信息存储单元（220）包括：

标识信息存储子单元（221），用于存储所述报文的标识信息；

25 记录子单元（222），用于记录所述报文的接收时间和命中次数；

频率计算子单元（223），与所述记录子单元（222）通信，用于根据所述接收时间和命中次数计算所述报文的发送频率；

频率存储子单元（224），与所述频率计算子单元（223）通信，用于将所述发送频率存储在所述黑名单绑定表项中。

13、如权利要求 11 所述网络设备（200），其特征在于，所述网络设备（200）还包括：信息发送单元（230），用于向用户终端（100）发送 IP 地址不可用信息。

14、如权利要求 13 所述网络设备（200），其特征在于，所述网络设备（200）还包括频率比较单元（240），与所述信息存储单元（220）通信，用于将所述报文的发送频率和设定的阀值进行比较，当所述报文的发送频率小于所述阀值时，通知所述信息发送单元（230）向用户终端（100）发送 IP 地址不可用信息。  
5

15、一种网关交换机，其特征在于，包括：

10 报文判断单元（210），用于获取接收的报文携带的标识信息，以所述标识信息为关键字查找绑定表，确定所述报文是否命中正常绑定表项；

15 信息存储单元（220），用于当所述报文未命中所述正常绑定表项时，将所述报文的标识信息存储在所述绑定表中的黑名单绑定表项中。

16、一种计算机程序，其特征在于，包括若干指令用以执行前述权利要求 1-7 任意一项所述的报文处理方法。

17、一种存储介质，其特征在于，存储权利要求 16 所述的计算机程序。

20 18、一种计算机设备，其特征在于，包括用以执行权利要求 16 所述的计算机程序的软件及与软件配合的硬件。

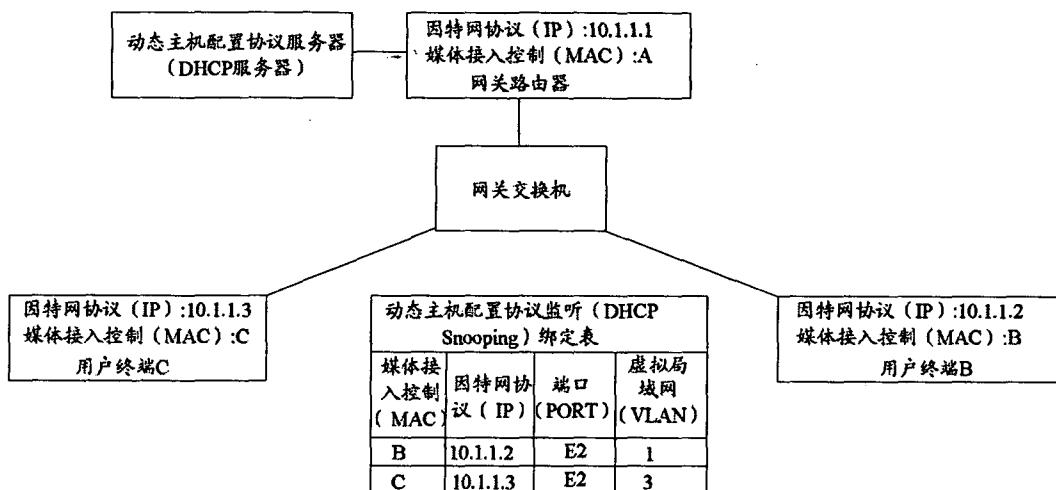


图 1

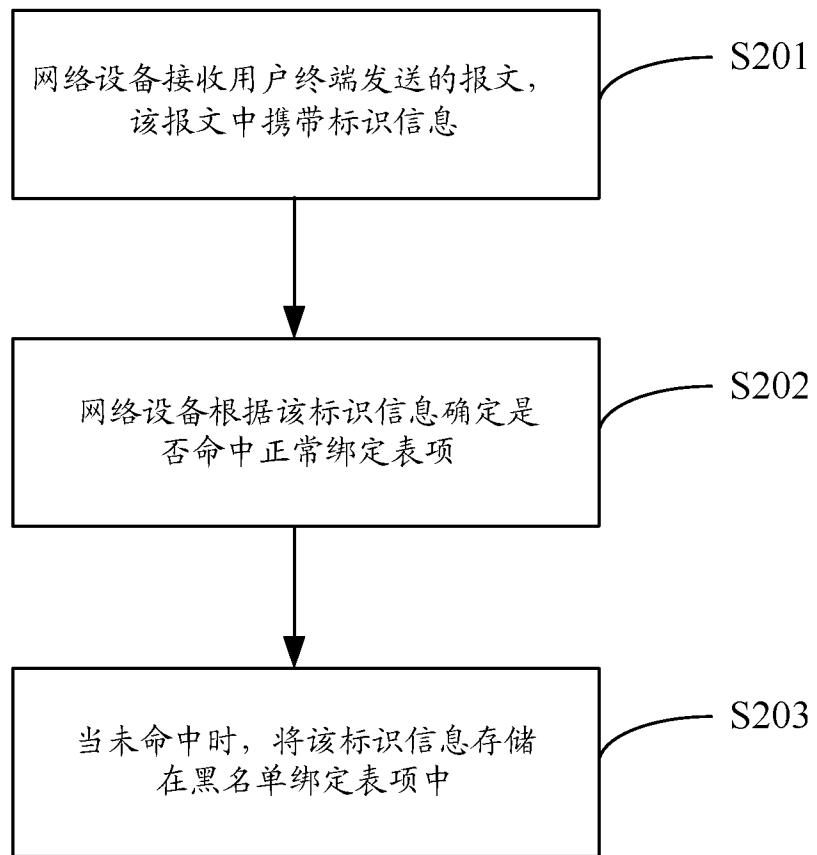


图 2

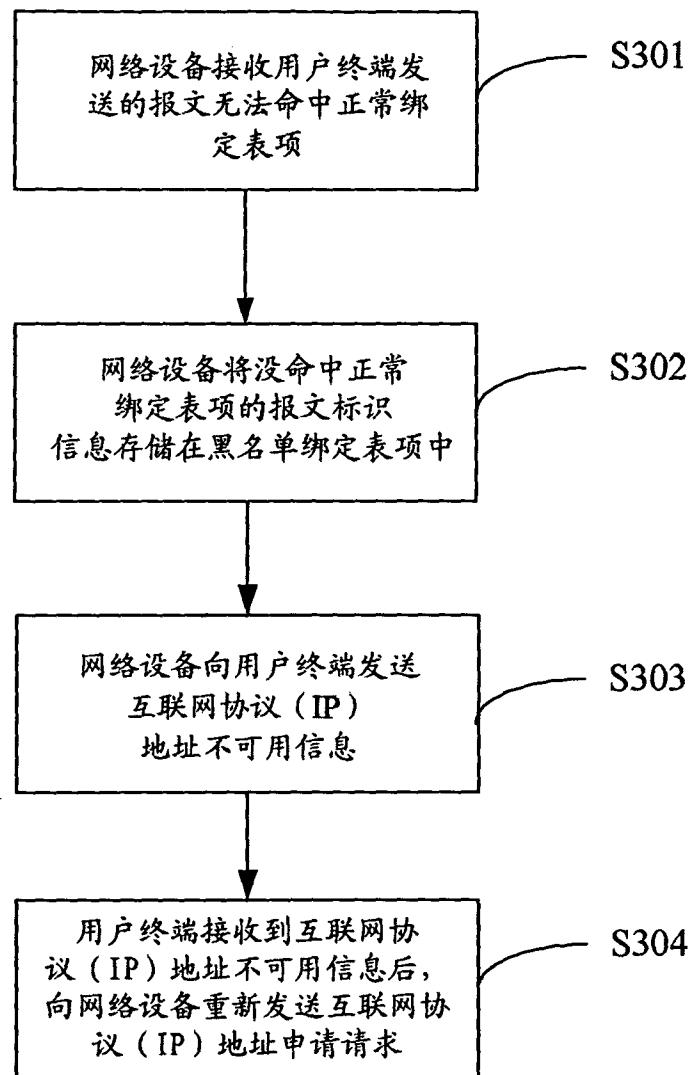


图 3

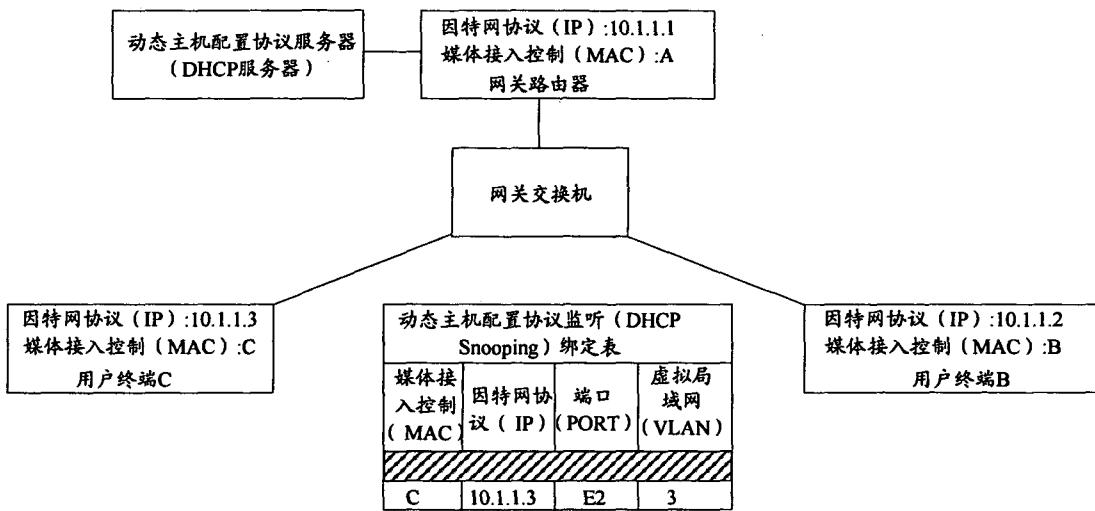


图 4

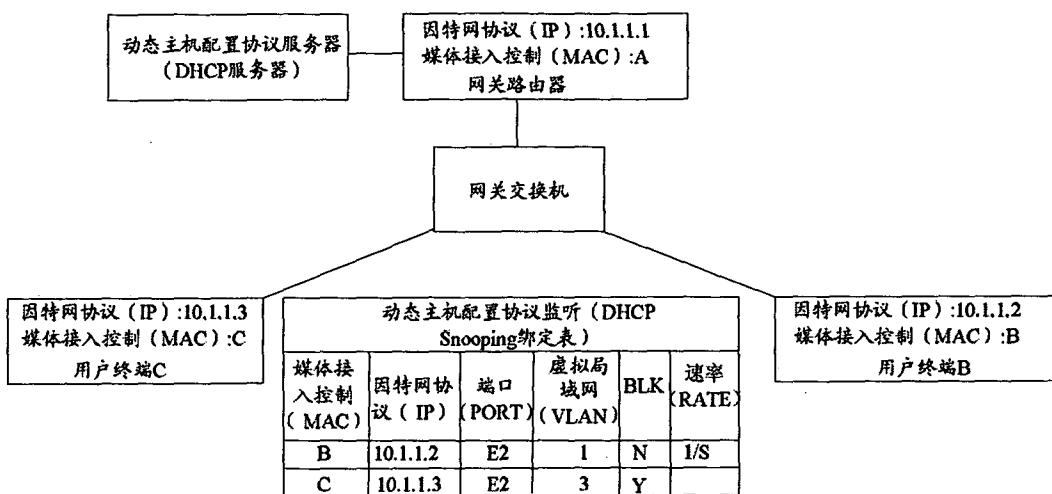


图 5

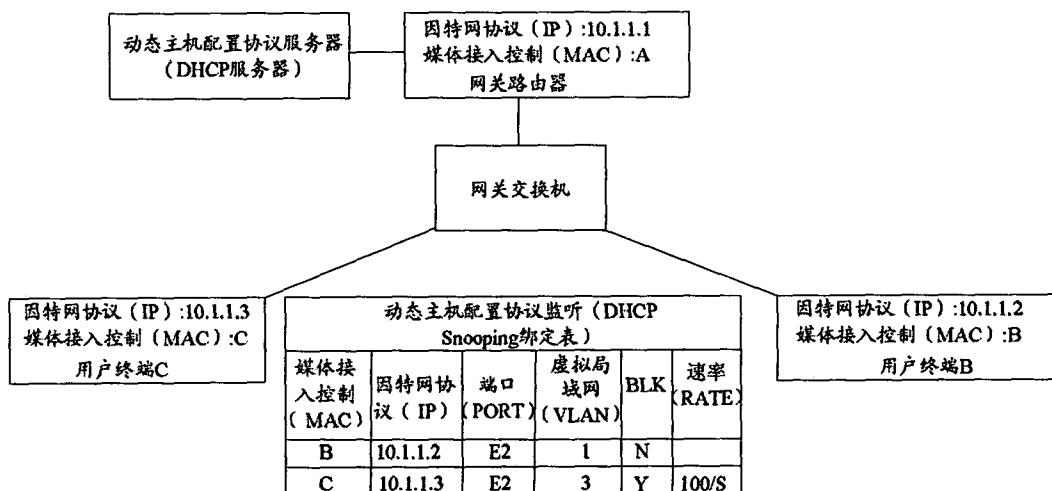


图 6

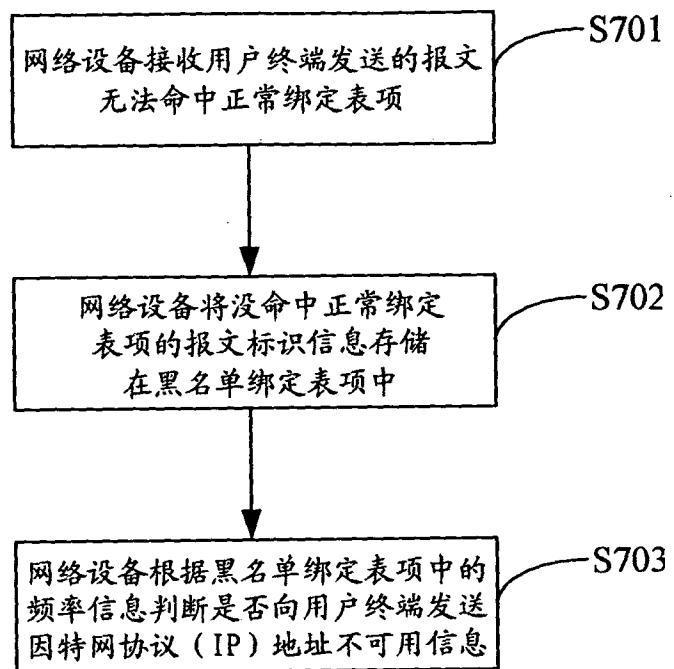


图 7

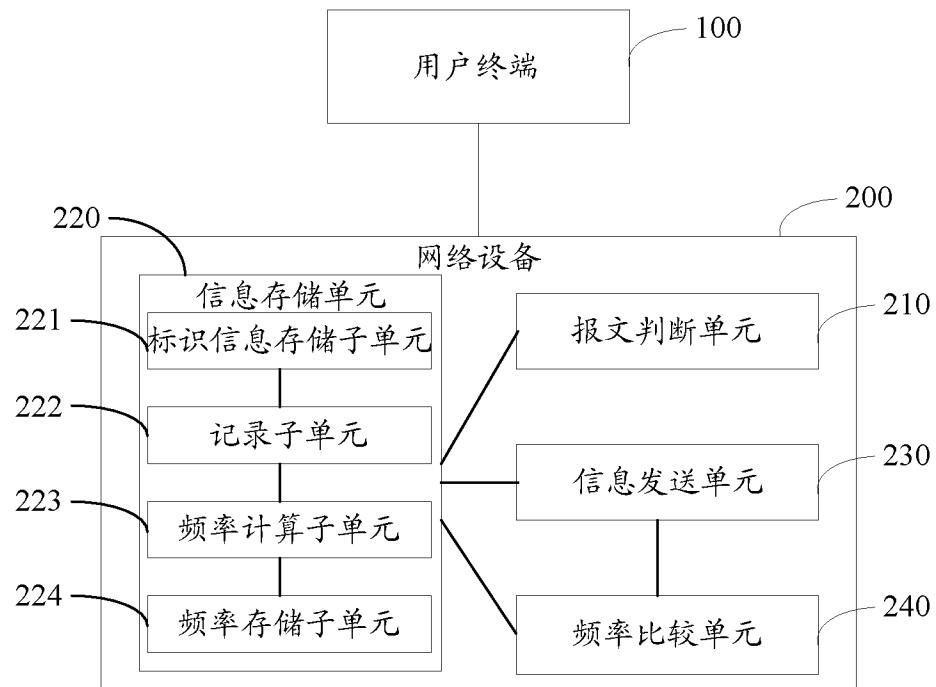


图 8

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2008/071043

## A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

message+ DHCP information? +normal hit+ blacklist? binding match+ mismatch+ attack+ whitelist?

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN1416239A(HUAWEI TECHNOLOGIES CO.,LTD.) 07 May 2003 (07.05.2003) Description page 8 line 3 to page 11 line 11, fig 1-3	1-2,6-9,11,13,15-18
Y	CN1874303A (HUAWEI TECHNOLOGIES CO.,LTD.) 06 Dec.2006 (06.12.2006) Description page 5 line 2 to line 17	1-2,6-9,11,13,15-18
A	WO2006/047927A1 (MAIL PROVE LIMITED) 11 May 2006 (11.05.2006) the whole document	1-18
A	US2005/0015626A1 (Chasin) 20 Jan. 2005 (20.01.2005) the whole document	1-18
PX	CN101060495 (HUAWEI TECHNOLOGIES CO.,LTD.) 24 Oct.2007 (24.10.2007) Description page 3 line 11 to page 10 line 25, fig 1-8	1-18

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 12 Aug. 2008 (12.08.2008)	Date of mailing of the international search report <b>11 Sep. 2008 (11.09.2008)</b>
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer <b>LI, YANJUN</b> Telephone No. (86-10)62413398

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2008/071043

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1416239A	07.05.2003	CN1167227C	15.09.2004
CN1874303A	06.12.2006	None	
WO2006/047927A1	11.05.2006	HK1068206A2 US2006095955A1 CN1770195A	22.04.2005 04.05.2006 10.05.2006
US2005/0015626A1	20.01.2005	WO2005010692A2	03.02.2005
CN101060495A	24.10.2007	None	

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/CN2008/071043

**CLASSIFICATION OF SUBJECT MATTER:**

H04L 12/56 (2006.01) i

H04L 29/06 (2006.01) i

H04L 12/26 (2006.01) i

H04L 12/66 (2006.01) i

**A. 主题的分类**

参见附加页

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

**B. 检索领域**

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI; EPODOC; PAJ; CNPAT; CNKI: 报文 信息 消息 正常 命中 黑名单 未命中 不正常 绑定 匹配 不匹配  
攻击 白名单 DHCP message? information? +normal hit+ blacklist? binding match+ mismatch+ attack+**C. 相关文件**

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN1416239A (华为技术有限公司) 07.5 月 2003 (07.05.2003) 说明书第 8 页第 3 行至第 11 页第 11 行、图 1-3	1-2,6-9,11,13,15-18
Y	CN1874303A (华为技术有限公司) 06.12 月 2006 (06.12.2006) 说明书第 5 页第 2 行至第 17 行	1-2,6-9,11,13,15-18
A	WO2006/047927A1 (MAIL PROVE LIMITED) 11.5 月 2006 (11.05.2006) 全文	1-18
A	US2005/0015626A1 (Chasin) 20.1 月 2005 (20.01.2005) 全文	1-18
PX	CN101060495A (华为技术有限公司) 24.10 月 2007 (24.10.2007) 说明书第 3 页第 11 行至第 10 页第 25 行、图 1-8	1-18

 其余文件在 C 栏的续页中列出。 见同族专利附件。

\* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&amp;” 同族专利的文件

国际检索实际完成的日期 12.8 月 2008 (12.08.2008)	国际检索报告邮寄日期 11.9 月 2008 (11.09.2008)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451	受权官员 李艳君 电话号码: (86-10) 62413398

国际检索报告  
关于同族专利的信息

国际申请号  
PCT/CN2008/071043

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1416239A	07.05.2003	CN1167227C	15.09.2004
CN1874303A	06.12.2006	无	
WO2006/047927A1	11.05.2006	HK1068206A2	22.04.2005
		US2006095955A1	04.05.2006
		CN1770195A	10.05.2006
US2005/0015626A1	20.01.2005	WO2005010692A2	03.02.2005
CN101060495A	24.10.2007	无	

续主题的分类:

H04L 12/56 (2006.01) i

H04L 29/06 (2006.01) i

H04L 12/26 (2006.01) i

H04L 12/66 (2006.01) i