网络地址转换协议 NAT 和动态主机配置协议 DHCP

(Network Address Translation & Dynamic Host Configuration Protocol)

生活中的问题

问题：学校里、家里使用专用地址的主机如何上网？

全球地址和专用地址

- 全球地址 —— 也称为公有地址，全球唯一的 IP 地址，必须向因特网管理机构申请。
- 专用地址 —— 也称为私有地址、内部地址，仅在机构内部使用的 IP 地址，可以由本机构自行分配，不需要向因特网的管理机构申请。

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

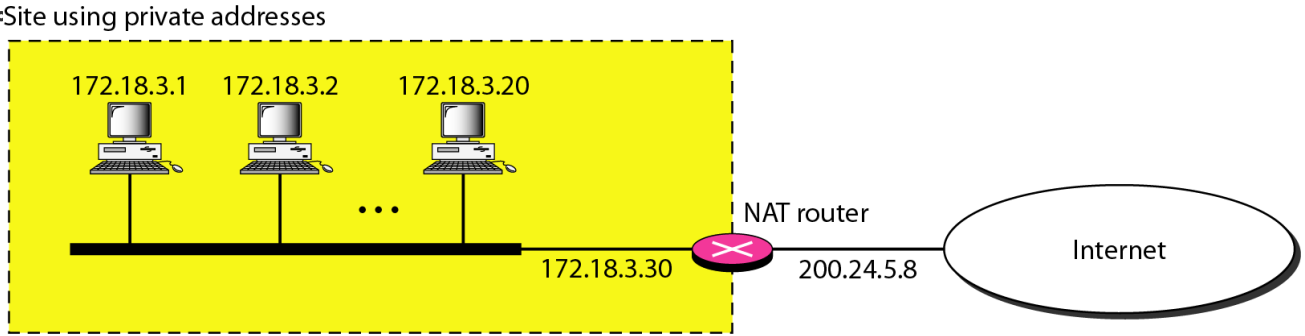
01

全球地址和专用地址

- 采用专用 IP 地址的网络称为专用互联网、本地互联网或专用网，专用 IP 地址也称为可重用地址。
- 专用地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信。
- 专用地址只能用作本地地址而不能用作全球地址。在因特网中的所有路由器，对目的地址是专用地址的数据报**一律不进行转发**。

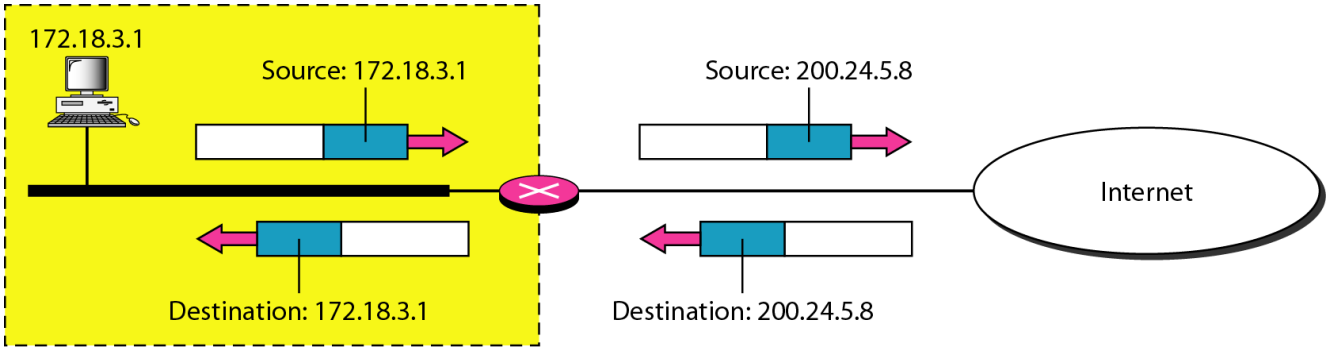
02 NAT 协议原理

- 1994 年提出的 NAT 用于在本地网络中使用私有地址、在连接互联网时转而使用全局 IP 地址的技术，是为解决 IPv4 地址短缺而开发的。
- NAT 通过将一个外部 IP 地址和端口映射到更大的内部 IP 地址集来转换 IP 地址。



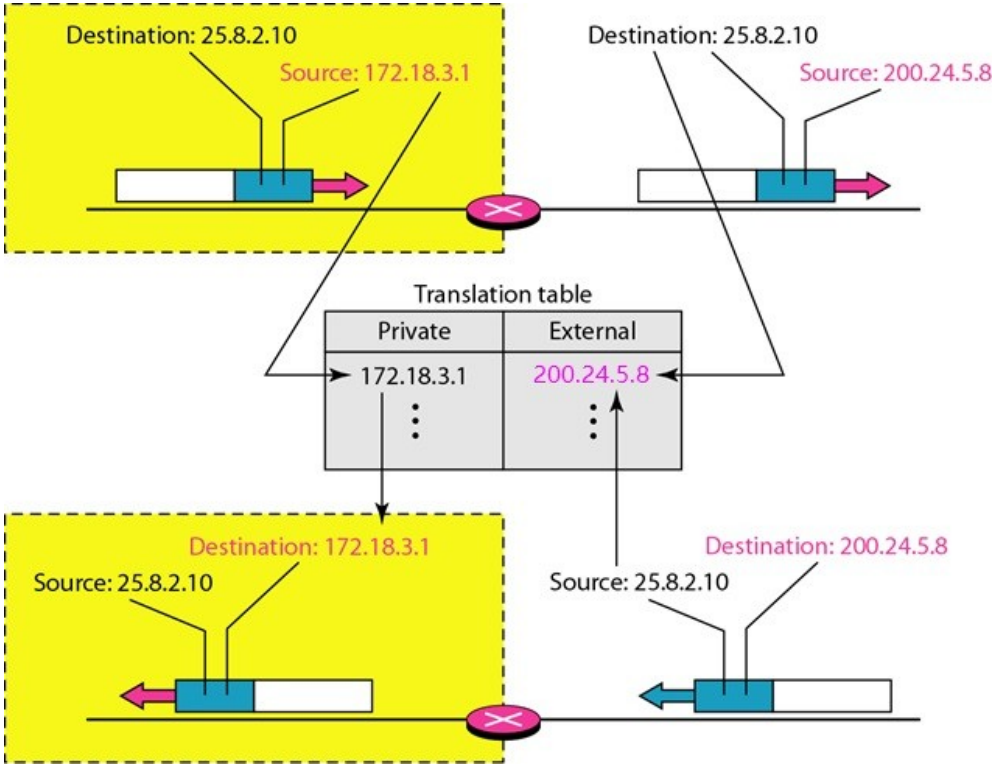
NAT 协议原理

- NAT 不仅能解决 IP 地址不足的问题，还能有效避免来自网络外部的攻击，隐藏并保护网络内部的计算机。 NAT 之内的 PC 联机到 Internet 上面时，其所显示的 IP 是 NAT 主机的公共 IP，外界在进行端口扫描时，侦测不到源端的 PC 。



02

NAT 转换表


Destination: 25.8.2.10
Source: 172.18.3.1
Destination: 25.8.2.10
Source: 200.24.5.8
Translation table
Private
External
172.18.3.1
200.24.5.8
Destination: 172.18.3.1
Source: 25.8.2.10
Source: 25.8.2.10
Destination: 200.24.5.8

NAT 的类型

- 静态 NAT （Static NAT) 实现了私有地址和全球公有地址的一对一映射，一个公有 IP 地址只会分配给唯一且固定的内网主机。
- 动态 NAT （Dynamic NAT）是指将内部网络的私有 IP 地址转换为公有 IP 地址时， IP 地址对是不确定的、随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的公有 IP 地址。当 ISP 提供的公有 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。
- 网络地址端口转换 PAT （Port Address Translation）是把内部地址映射到外部网络的一个 IP 地址的不同端口上。 PAT 与动态地址 NAT 不同，它将内部连接全部映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的端口号。

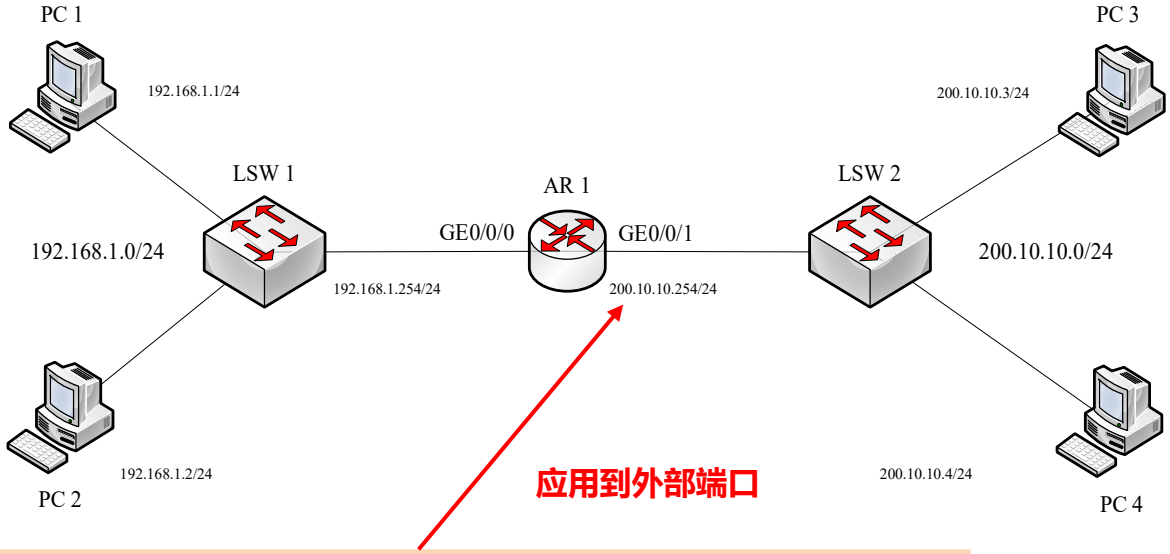
03 NAT 的类型

- PAT 把专用网内不同的源 IP 地址，都转换为同样的全球 IP 地址。
- 对源主机所采用的 TCP 或 UDP 端口号（无论是否相同），转换为不同的新的端口号。
- 从层次的角度看， PAT 的机制有些特殊：
  - 普通路由器在转发 IP 数据报时，源 IP 地址或目的 IP 地址都不改变，但 NAT 路由器在转发 IP 数据报时，一定要更换其 IP 地址（转换源地址或目的地址）。
  - 普通路由器在转发分组时工作在网络层，但 PAT 路由器要查看和转换传输层的端口号，属于传输层的范畴。

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	2400	TCP
172.18.3.2	1401	25.8.3.2	2401	TCP
. . .	. . .	. . .	. . .	. . .

03 静态 NAT

主机	私有 IP 地址	公有 IP 地址
PC1	192.168.1.1	200.10.10.1
PC2	192.168.1.2	200.10.10.2




```
[Huawei-GigabitEthernet0/0/1]nat static global 200.10.10.1 inside 192.168.1.1

[Huawei-GigabitEthernet0/0/1]nat static global 200.10.10.2 inside 192.168.1.2
```

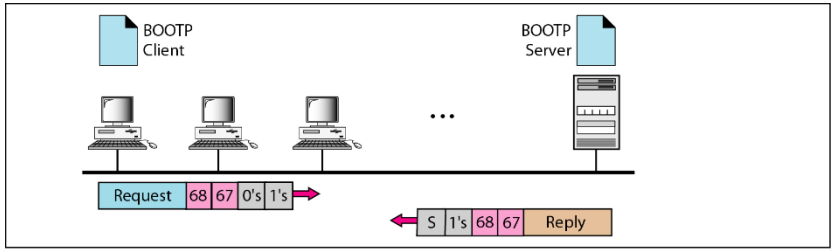
问题：如何检验 NAT 已配置成功?

04 反向地址转换协议 RARP

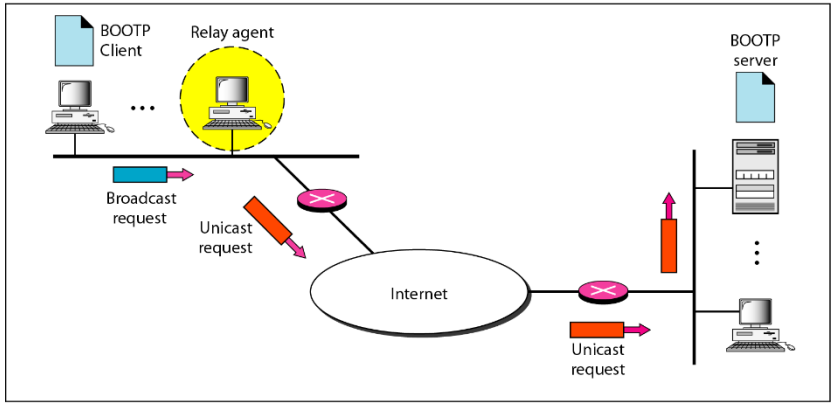
- RARP 允许局域网的机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。
- PC 从网卡上读取 MAC 地址，然后在网络上发送一个 RARP 请求的广播数据包，请求 RARP 服务器回复该 PC 的 IP 地址。RARP 服务器收到了 RARP 请求数据包，为其分配 IP 地址，并将 RARP 回应发送给 PC 。PC 收到 RARP 回应后，就使用得到的 IP 地址进行通信。
- 虽然 RARP 在概念上很简单，但是一个 RARP 服务器的设计与系统相关而且比较复杂。相反，提供一个 ARP 服务器很简单，通常是 TCP/IP 在内核中实现的一部分。由于内核知道 IP 地址和硬件地址，因此当它收到一个询问 IP 地址的 ARP 请求时，只需用相应的硬件地址来提供应答就可以了。
- 由于 RARP 的请求是在硬件层上的广播，不能通过路由转发，因此在每个网络都要设置一个 RARP 服务器。另外在同一网络中不同主机可能会同时进行 RARP 请求，增大了冲突的概率。

04 引导程序协议 BOOTP

- BOOTP （Bootstrap Protocol）是一种引导协议，基于 IP/UDP 协议，也称自举协议，是 DHCP 协议的前身。
- BOOTP 用于无盘工作站的局域网中，可以让无盘工作站从中心服务器获得 IP 地址。通过 BOOTP 协议可以为局域网中的无盘工作站分配动态 IP 地址，这样就不需要管理员去为每个用户去设置静态 IP 地址。
- DHCP 协议从 BOOTP 的基础上发展而来，它们都是主机配置协议，都可以大大减少管理员的工作量。BOOTP 可看成是简单版的 DHCP，是对主机的静态配置，而 DHCP 可以依据一些策略对主机进行动态配置。BOOTP 用于无盘工作站的启动和配置，而 DHCP 更适用于客户端接入变化的网络，即客户端接入时间、接入地点不固定。



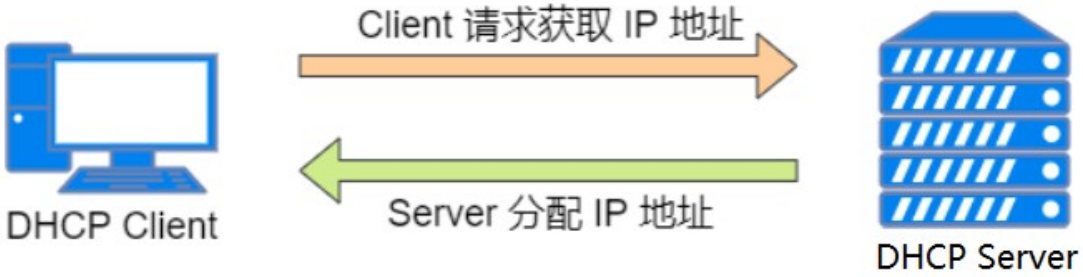
a. Client and server on the same network



b. Client and server on different networks

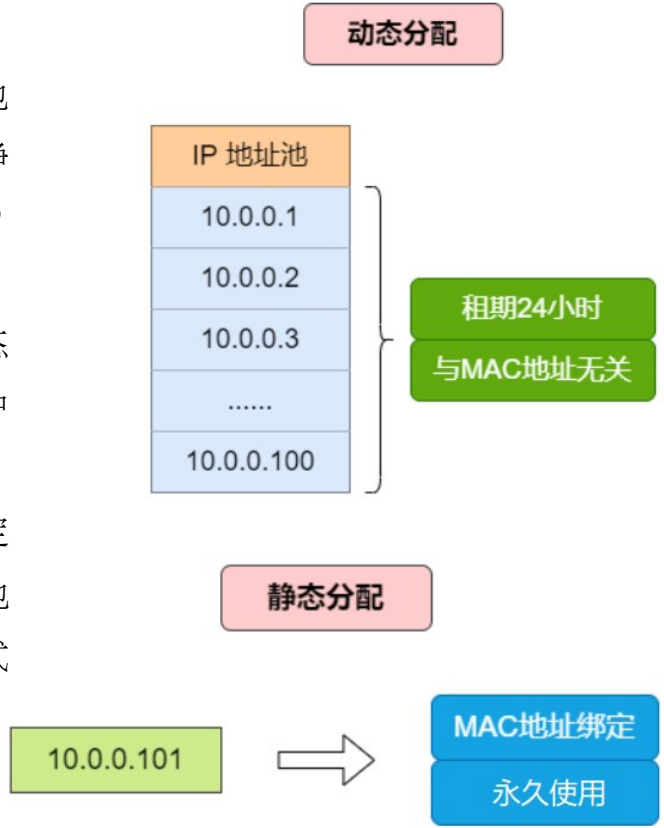
05 动态主机配置协议 DHCP

- DHCP （Dynamic Host Configuration Protocol）协议支持 C/S （客户端 / 服务器）结构，主要分为两部分： DHCP 客户端使用从 DHCP 服务器分配下来的 IP 信息，通常是主机或电脑、手机等网络设备； DHCP 服务器集中管理所有的 IP 网络设定信息，并处理客户端的 DHCP 请求，通常是提供 DHCP 服务功能的服务器或网络设备（路由器或三层交换机），如家用的无线路由器。
- 通常 DHCP 服务器至少向客户端提供 IP 地址、子网掩码、默认网关，还可以提供其他信息，如域名服务 (DNS) 服务器的地址和 Windows Internet 名称服务 (WINS) 服务器的地址。



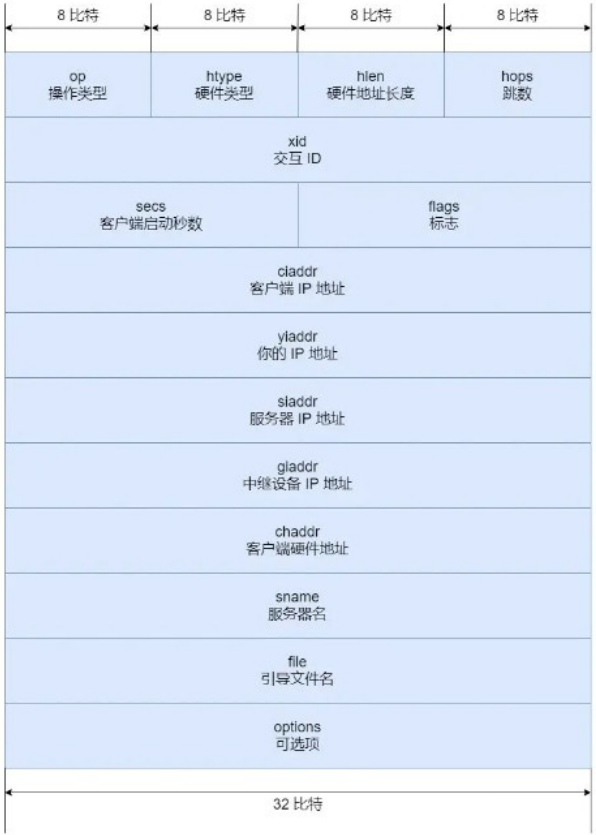
05 动态主机配置协议 DHCP

- DHCP 提供人工的或自动的 、静态或动态的地址配置。静态地址配置与 BOOTP 相同，与 BOOTP 后向兼容，客户机可请求静态地址， DHCP 服务器有一个数据库静态地绑定物理地址和 IP 地址。 DHCP 还有一个动态数据库，即一个可用的 IP 地址池。DHCP 客户机向 DHCP 服务器发送请求时，服务器先查询静态数据库，如有则返回永久 IP 地址；如没有则从可用 IP 地址池中选择一个 IP 地址，指定给该用户并添加到动态数据库。
- DHCP 服务器为客户端分配 IP 地址有三种形式：将 IP 地址固定分配给一个客户端、随机地将地址永久性分配给客户端、随机地将地址分配给客户端使用一段时间。第三种是最常见的使用形式，地址的有效使用时间段称为租用期。



05 DHCP 报文

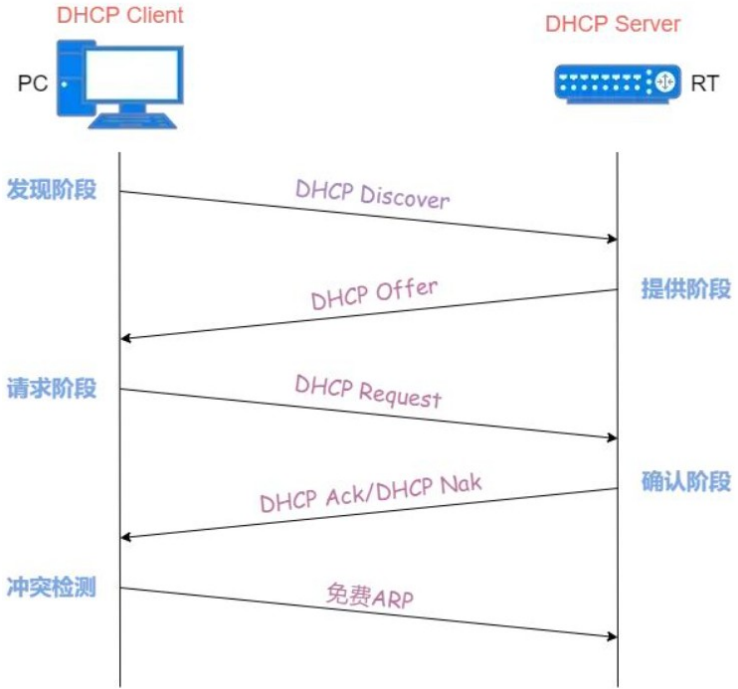
- op （操作类型）：表示报文的格式。当值为 1 时，表示客户端的请求报文；当值为 2 时，表示服务器的响应报文。
- htype （硬件类型）：不同的硬件类型取不同的值，最常见的以太网，值是 1 。
- hlen （硬件地址长度）：表示硬件地址长度，以太网的值是 6 ，也就是 MAC 地址的长度。
- hops （跳数）： DHCP 报文经过的 DHCP 中继的数量。
- xid （交互 ID ）： DHCP 客户端取的随机值，收到 DHCP 服务器的响应报文时，查看 xid 值是否相同，来判断报文是否是发送给自己的。
- secs （客户端启动秒数）：记录 IP 地址的使用时间。
- flags （标志）：广播响应标志位，当值为 0 时，表示服务器以单播形式发送响应报文；当值为 1 时，服务器以广播形式发送响应报文。
- ciaddr （客户端 IP 地址）：客户端的 IP 地址，可以是分配的地址，也可以是正在使用的地址，还可以是的 0.0.0.0 。 0.0.0.0 是客户端初始状态没有地址的时候，仅用于临时通信，不是有效的地址。
- yiaddr （分配的 IP 地址）：当服务器发送响应报文时，将分配给客户端的 IP 地址填入这个字段。
- siaddr （服务器 IP 地址）：用来标识服务器的 IP 地址。
- giaddr （中继设备 IP 地址）：表示 DHCP 中继的 IP 地址，服务器通过识别这个字段来判断出客户端的网段地址，从而选择合适的地址池，为客户端分配该网段的 IP 地址。
- chaddr （客户端硬件地址）：用来标识客户端的硬件地址，当客户端发送广播发现报文时，这个字段就是自己的硬件地址。
- sname （服务器名）：可选项， DHCP 服务器填写这个字段。
- file （引导文件名）：可选项， DHCP 服务器填写这个字段。
- options （可选项）：可选项， DHCP 客户端获取网络参数， DHCP 服务器提供网络参数，都使用这个字段。内容包括租期、子网掩码、默认网关地址、 DNS 服务器地址等。



06

DHCP 工作过程

DHCP 协议报文采用 UDP 方式封装， DHCP Server 侦听的端口号是 67 ， DHCP Client 的端口号是 68 。 DHCP 的基本工作流程分为 4 个阶段，即发现阶段、提供阶段、请求阶段、确认阶段。



06

DHCP 工作过程

- **DHCP DISCOVER 寻找服务器**

  当 DHCP 客户端首次登录网络的时候，如果发现本机上没有任何 IP 配置，则会向网络发出一个 DHCP Discover 广播，源地址为 0.0.0.0 ，目的地址则为 255.255.255.255 。

- **DHCP OFFER 分配 IP 地址**

  当 DHCP 服务器监听到客户端发出的 DHCP Discover 广播后，它会从那些还没有租出的地址范围内，按一定规律选择空置 IP ，连同其它 TCP/IP 设定，发给客户端一个 DHCP Offer ，DHCP Offer 会包含一个租约期限的信息。

DHCP 工作过程

- **DHCP REQUEST 请求使用**

  如果客户端收到网络上多台 DHCP 协议服务器的响应，只会挑选其中一个 DHCP Offer ，并向网络发送一个 DHCP Request 广播，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。同时，客户端还会向网络发送一个 ARP，查询网络上面有没有其它机器使用该 IP 地址；如果发现该 IP 已经被占用，客户端则会送出一个 DHCP Decline 给 DHCP 服务器，拒绝接受其 DHCP Offer ，并重新发送 DHCP Discover 信息。

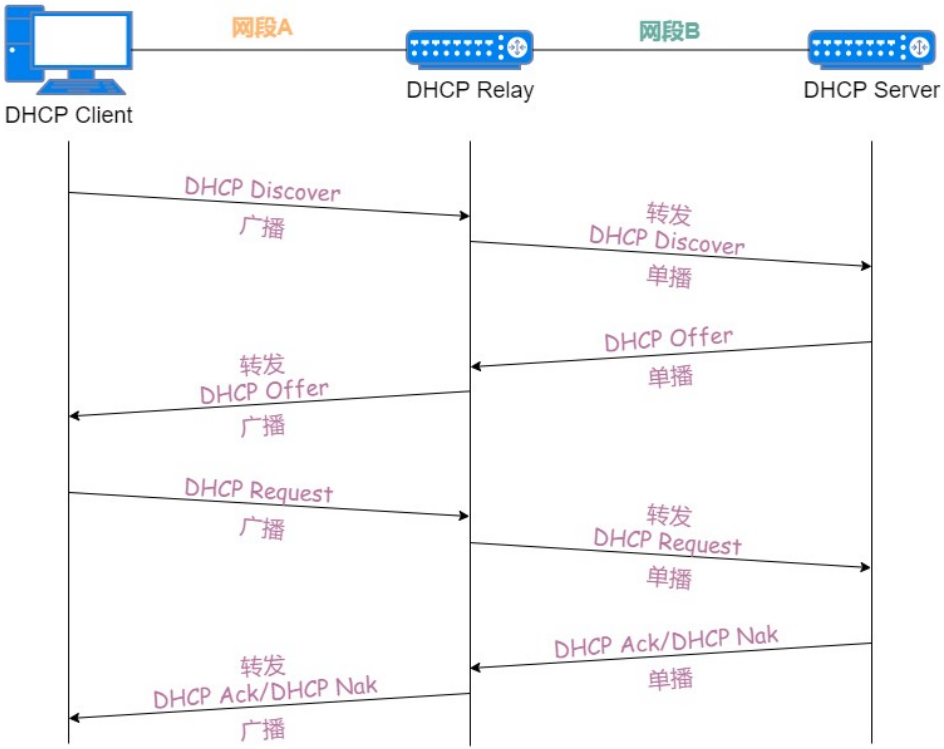
- **DHCP ACK IP 地址分配确认**

  当 DHCP 服务器收到 DHCP 客户机回答的 DHCP Request 请求信息之后， 它便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置的 DHCP ACK 确认信息，确认 IP 地址的正式生效。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定。除 DHCP 客户机选中的服务器外，其它的 DHCP 服务器都将收回曾提供的 IP 地址。

07

DHCP 中继

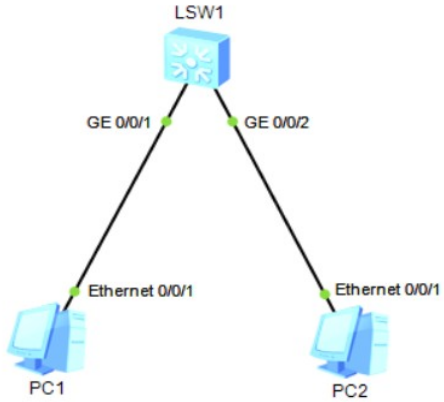
- 动态获取 IP 地址的过程中，使用广播方式发送报文，因此 DHCP 只适用于客户端和服务器在同一个子网内的情况。
- 如果为每个网段配置一个 DHCP 服务器，显然太浪费了。 DHCP Relay 可实现跨网段通信获取 IP 地址。这样，多个子网的客户端可以使用同一个 DHCP 服务器，既节省成本，又方便集中管理。
- 客户端发送 DHCP Discover 或 DHCP Request 广播报文，具有 DHCP Relay 功能的网络设备收到后，根据配置将报文单播给指定的 DHCP 服务器；
- DHCP 服务器进行 IP 地址的分配，单播发送给 DHCP Relay ， DHCP Relay 再将配置信息广播给客户端，完成对客户端的动态配置。



08 交换机配置 DHCP

1. 启用 DHCP 功能，为地址池命名；
2. 设置网段的地址和子网掩码、网关、租期等；
3. 创建 VLAN 10 ，将交换机的两个端口划分到 VLAN 10；
4. 为 VLAN 10 配置虚拟端口地址作为网关；
5. 开启虚拟端口采用全局地址池的 DHCP Server 功能。

```
[Huawei]dhcp enable
[Huawei]ip pool pool10
[Huawei-ip-pool-pool10]network 192.168.1.0 mask 24
[Huawei-ip-pool-pool10]gateway-list 192.168.1.1
[Huawei-ip-pool-pool10]lease day 5 hour 5
[Huawei-ip-pool-pool10]quit
[Huawei]int vlanif 10
[Huawei-Vlanif10]ip add 192.168.1.1 24
[Huawei-Vlanif10]dhcp select global
```



要求：

- 使用 display ip pool 查看交换机的地址池；
- 抓包查看 DHCP 的工作过程。