DHCP 协议原理与配置
Dynamic Host Configuration Protocol 动态主机配置协议

CHADDR：Client Hardware Address

前言

- 一个网络如果要正常地运行，则网络中的主机（Host）必需要知道某些重要的网络参数，如IP地址、网络掩码、网关地址、DNS服务器地址、网络打印机地址等等。显然，在每台主机上都采用手工方式来配置这些参数是非常困难的、或是根本不可能的。
- 为此，IETF于1993年发布了动态主机配置协议（DHCP：Dynamic Host Configuration Protocol）。DHCP的应用，实现了网络参数配置过程的自动化。那么DHCP技术具体是如何实现的呢？面对网络规模的扩大，DHCP又是如何应对的？面对网络中的攻击，DHCP又是如何防护的呢？

手工配置网络参数存在的问题

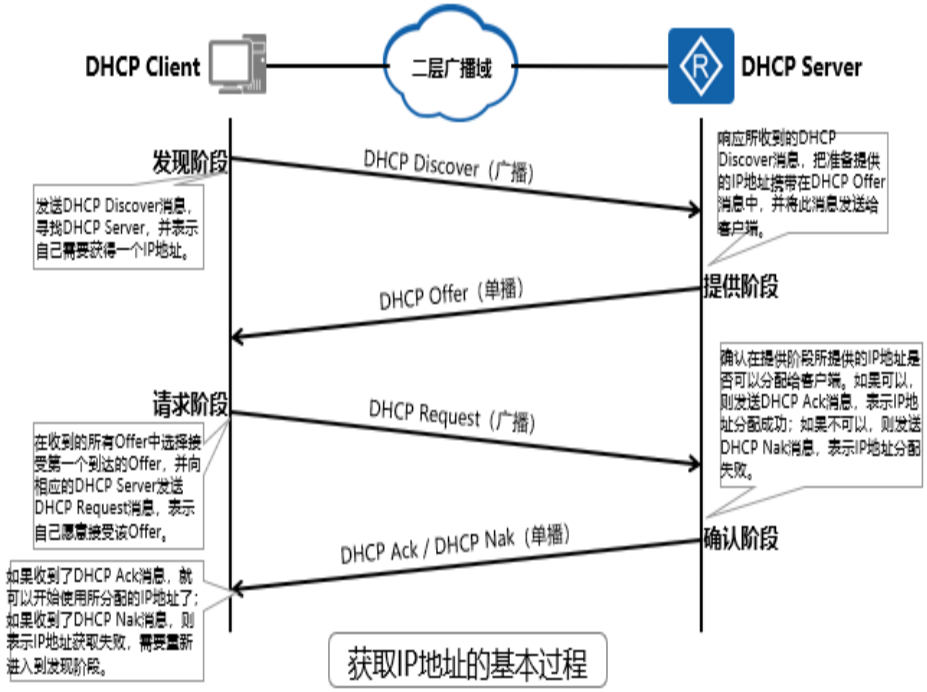
- 传统的手工配置网络参数需要每个用户都手动配置IP地址、掩码、网关、DNS等多个参数。
- 这样就会存在一些问题：
  - 人员素质要求高
  - 容易出错
  - 灵活性差
  - IP地址资源利用率低
  - 工作量大

- 人员素质要求高
- 主机的使用者需要懂得如何进行网络参数的配置操作方法，这在实际中是难以做到的。
- 容易出错
- 手工配置过程中非常容易出现人为的误操作情况。
- 灵活性差
- 网络参数发生改变时，需要重新进行配置操作。例如，如果某主机在网络中的位置发生了变化，则该主机的网关地址也可能会发生变化，这时就需要重新配置该主机的网关地址。
- IP 地址资源利用率低
- IP 地址无法得到重复利用。
- 工作量大
- 配置工作量会随着主机数量的增加而增大。

DHCP概念的提出

- 随着用户规模的扩大及用户位置的不固定性，传统的静态手工配置方式已经无法满足需求，为了实现网络可以动态合理地分配IP地址给主机使用，需要用到动态主机配置协议DHCP。
- DHCP相对于静态手工配置有如下优点：
  - 效率高
  - 灵活性强
  - 易于管理

DHCP基本工作过程 (1)

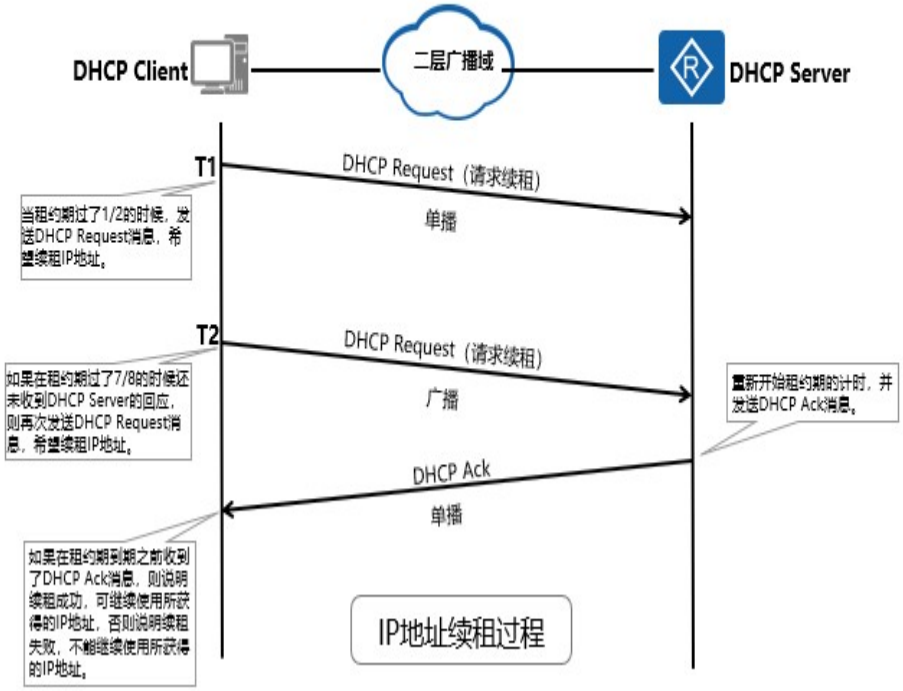


- DHCP 采用了 Client/Server 模型；DHCP Client 需要从

DHCP Server 那里获得各种网络配置参数，这个过程是通过 DHCP Client 与 DHCP Server 之间交互各种 DHCP 消息来实现的。DHCP 消息是封装在 UDP 报文中的，DHCP Server 使用端口号 67 来接收 DHCP 消息，DHCP Client 使用端口号 68 来接收 DHCP 消息。本课程中，我们主要关心 DHCP Client 是如何获得自己的 IP 地址的。

- 如图所展示的是 DHCP Client 通过 DHCP 来申请获取自己的 IP 地址的基本过程，这一过程包含了四个阶段：
- 发现阶段：
- 发现阶段也就是 PC 上的 DHCP Client 寻找 DHCP Server 的阶段。PC 上的 DHCP Client 开始运行后，会以广播的方式发送一个 DHCP Discover 消息。
- 需要说明的是，图中所示的二层广播域中除了路由器 R 上运行了 DHCP Server 外，可能还有其它设备也运行了 DHCP Server。如果是这样，那么所有这些 DHCP Server 都会接收到 PC 发送的 DHCP Discover 消息，也都会对所收到的 DHCP Discover 消息做出回应。
- 提供阶段
- 提供阶段也就是 DHCP Server 向 DHCP Client 提供 IP 地址的阶段，每一个接收到 DHCP Discover 消息的 DHCP Server（包括路由器 R 上运行的 DHCP Server）都会从自己维护的地址池中选择一个合适的 IP 地址，并通过 DHCP Offer 消息将这个 IP 地址发送给 DHCP Client。DHCP Server 是以单播的方式来发送 DHCP Offer 消息的。

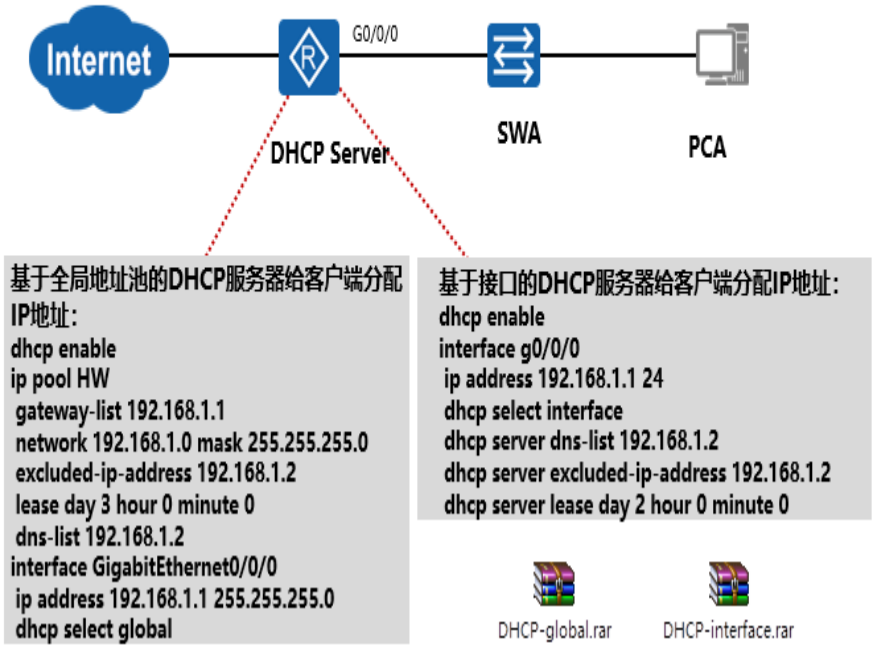
DHCP基本工作过程 (2)



- DHCP Server 每次给 DHCP Client 分配一个 IP 地址时，只是跟 DHCP Client 定立了一个关于这个 IP 地址的租约（Lease）。每个租约都有一个租约期（Duration of Lease），DHCP 协议规定租约期的缺省值不得小于 1 个小时，而实际部署 DHCP 时，租约期的缺省值通常都是 24 小时。在租约期内，DHCP Client 才能使用相应的 IP 地址。当租约期到期之后，DHCP Client 是不被允许继续使用这个 IP 地址的。在租约期还没有到期的时候，DHCP Client 可以申请续租这个 IP 地址，其过程如图所示。
- DHCP 协议规定，在缺省情况下，图中的 T1 时刻是租约期到了一半的时刻，而 T2 时刻则是租约期到了 87.5%的时刻。在 T1 时刻，PC 上的 DHCP Client 会以单播方式向 R 上的 DHCP Server 发送一个 DHCP Request 消息，请求续租 IP 地址（也就是请求重新开始租约期的计时）。如果在 T2 时刻之前，

PC 上的 DHCP Client 收到了回应的 DHCP Ack 消息，则说明续租已经成功。如果直到 T2 时刻，PC 上的 DHCP Client 都未收到回应的 DHCP Ack 消息，那么在 T2 时刻，PC 上的 DHCP Client 会以广播方式发送一个 DHCP Request 消息，继续请求续租 IP 地址。如果在租约期到期之前，PC 上的 DHCP Client 收到了回应的 DHCP Ack 消息，则说明续租成功。如果直到租约期到期时，PC 上的 DHCP Client 仍未收到回应的 DHCP Ack 消息，那么 PC 就必须停止使用原来的 IP 地址，也就是说，PC 只能重新从发现阶段开始来重新申请一个 IP 地址。

DHCP配置实现



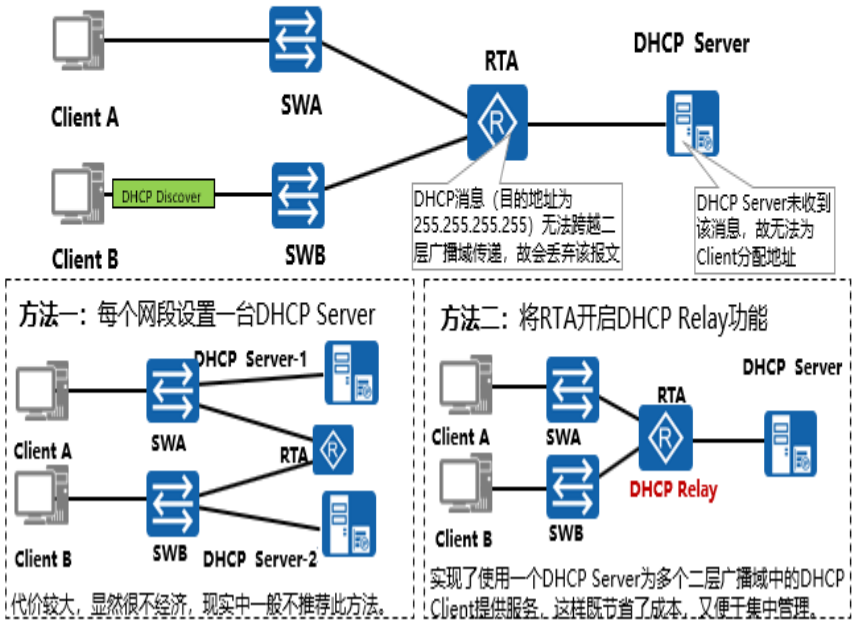
- DHCP Server 配置基于接口的地址分配方式，只会响应该接口接收的 DHCP 请求；配置基于全局地址池的地址分配方式，可以响应所有端口接收的 DHCP 请求。
- dhcp enable　　//使能 DHCP 功能，在配置 DHCP 服

务器时必须先执行该命令，才能配置 DHCP 的其他功能并生效

- ip pool HW　　//设置一个名为 HW 的全局地址池
- gateway-list 192.168.1.1　　//设置分配的网关 IP
- network 192.168.1.0 mask 255.255.255.0　　//设置分配的地址网段
- excluded-ip-address 192.168.1.2　　//设置不参与自动分配的 IP 地址范围
- lease day 3 hour 0 minute 0　　//设置地址池中 IP 地址的租用有效期限，默认 1 天
- dns-list 192.168.1.2　　//设置分配的 DNS 服务器地址
- interface GigabitEthernet0/0/0
- ip address 192.168.1.1 255.255.255.0
- dhcp select global　　//接口下使能全局方式分配地址

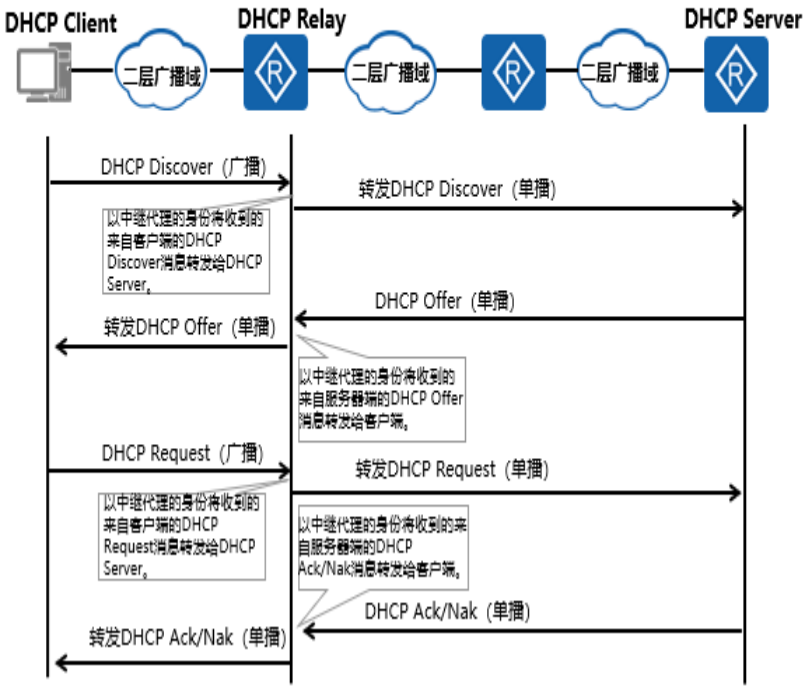
为什么需要DHCP Relay?

- 随着网络规模的扩大，网络中就会出现用户处于不同网段的情况：



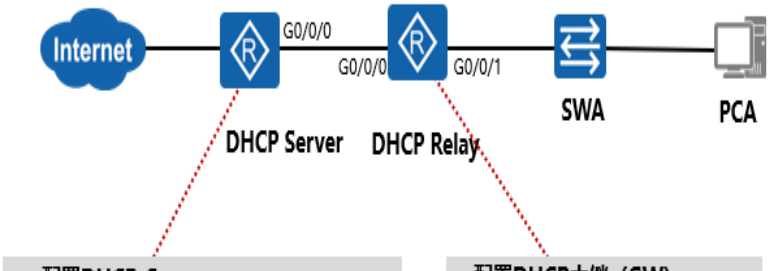
- 从前面的描述中可知，DHCP Client 和 DHCP Server 必须在同一个二层广播域中才能接收到彼此发送的 DHCP 消息。DHCP 消息无法跨越二层广播域传递。
- 一个实际的 IP 网络通常都包含了多个二层广播域，如果需要部署 DHCP，那么可以有两种方法：
- 方法一：在每一个二层广播域中都部署一个 DHCP Server（代价太大，现实中一般不推荐此方法）。
- 方法二：部署一个 DHCP Server 来同时为多个二层广播域中的 DHCP Client 服务，这就需要引入 DHCP Relay。

DHCP Relay基本工作原理



- DHCP Relay 的基本作用就是专门在 DHCP Client 和 DHCP Server 之间进行 DHCP 消息的中转。
- 如图所示，DHCP Client 利用 DHCP Relay 来从 DHCP Server 那里获取 IP 地址等配置参数时，DHCP Relay 必须与 DHCP Client 位于同一个二层广播域，但 DHCP Server 可以与 DHCP Relay 位于同一个二层广播域，也可以与 DHCP Relay 位于不同的二层广播域。DHCP Client 与 DHCP Relay 之间是以广播方式交换 DHCP 消息的，但 DHCP Relay 与 DHCP Server 之间是以单播方式交换 DHCP 消息的（这就意味着，DHCP Relay 必须事先知道 DHCP Server 的 IP 地址）。

DHCP Relay配置实现



配置DHCP-Server:
(以基于全局地址池分配地址为例)

```
dhcp enable
ip pool DHCP-relay
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 24
 dns-list 10.1.1.1
interface g0/0/0
 ip address 10.1.1.1 24
 dhcp select global
ip route-static 192.168.1.0 24 10.1.1.2
```

配置DHCP中继（GW）：

```
dhcp server group DHCP
dhcp-server 10.1.1.1
dhcp enable
interface g0/0/1
 ip address 192.168.1.1 24
 dhcp select relay
 dhcp relay server-select DHCP
interface g0/0/0
 ip address 10.1.1.2 24
```

DHCP-Relay.rar

- 配置 DHCP-Server：

//DHCP 服务器可以采用全局地址分配或者接口地址分配，此处以全局地址池分配地址为例

- dhcp enable
- ip pool DHCP-relay /

/"DHCP-relay"仅为 DHCP 地址池名称

- ip route-static 192.168.1.0 24 10.1.1.2 //由于中继后的 DHCP 报文是一个源地址为 192.168.1.1 的单播报文，需要有回去的路由，当前为了简单，使用静态路由完成，正常网络内可以配置 IGP 使得地址能够通信
- 配置 DHCP 中继（GW）：
- dhcp server group DHCP //配置 DHCP 服务器组名
- dhcp-server 10.1.1.1 //设定

DHCP 服务器地址

- dhcp enable //

中继设备也需要开启 DHCP，否则后面接口下的命令不能使能

- interface g0/0/1 //进入

连接客户端的接口

- ip address 192.168.1.1 24
- dhcp select relay //启动

DHCP Relay 功能

- dhcp relay server-select DHCP //设定 DHCP

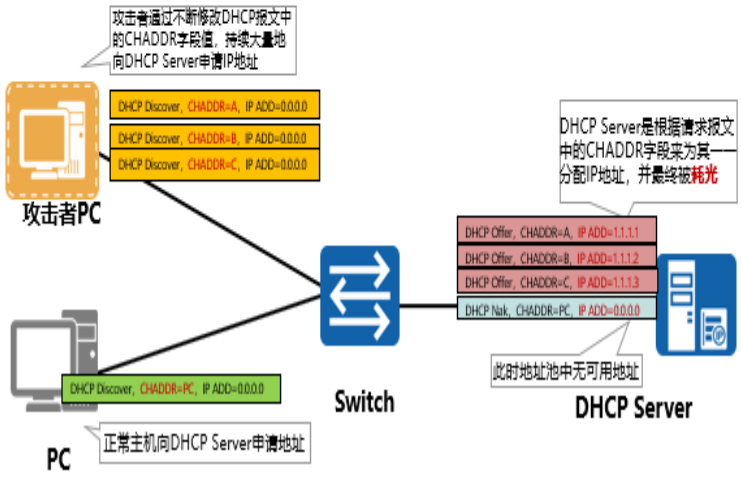
Relay 要使用的服务器组

DHCP面临的安全威胁

- 网络攻击行为无处不在，针对DHCP的攻击行为也不例外。例如，某公司突然出现了大面积用户无法上网的情况，经检查用户终端均未获取到IP地址，且DHCP Server地址池中的地址已经全部被分配出去了，这种情况很有可能就是DHCP受到了饿死攻击而导致的。
- DHCP在设计上未充分考虑到安全因素，从而留下了许多安全漏洞，使得DHCP很容易受到攻击。实际网络中，针对DHCP的攻击行为主要有以下三种：
  - DHCP饿死攻击
  - 仿冒DHCP Server攻击
  - DHCP中间人攻击

DHCP饿死攻击

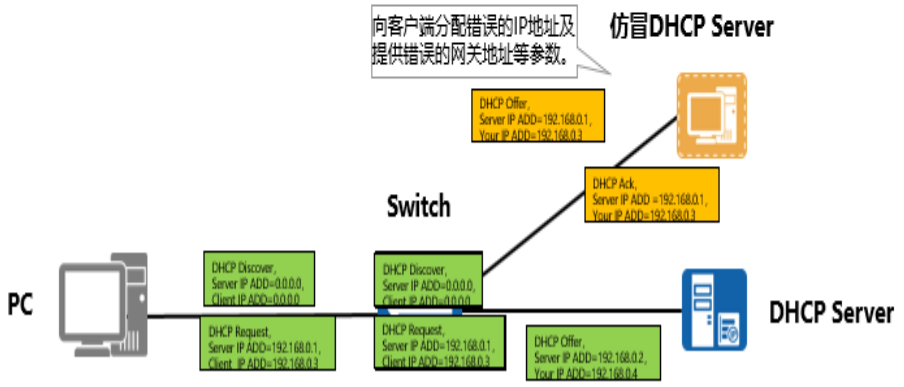
- 攻击原理：攻击者持续大量地向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。
- 漏洞分析：DHCP Server向申请者分配IP地址时，无法区分正常的申请者与恶意的申请者。



- DHCP 饿死攻击是攻击者通过持续大量地向 DHCP Server 申请 IP 地址来实现的，其目的是耗尽 DHCP Server 地址池中的 IP 地址，导致 DHCP Server 没有 IP 地址分配给正常的用户。DHCP 消息中有一个名叫 CHADDR（Client Hardware Address）的字段，该字段是由 DHCP 客户端填写的，表示的是客户端的硬件地址（也就是客户端的 MAC 地址）。DHCP Server 是针对 CHADDR 来分配 IP 地址的，对于不同的 CHADDR，DHCP Server 会分配不同的 IP 地址；DHCP Server 无法区分什么样的 CHADDR 是合法的，什么样的 CHADDR 是非法的。利用这个漏洞，攻击者每申请一个 IP 地址时，就在 DHCP 消息的 CHADDR 字段中填写一个不同的值，以此来冒充是不同的用户在申请 IP 地址。

仿冒DHCP Server攻击

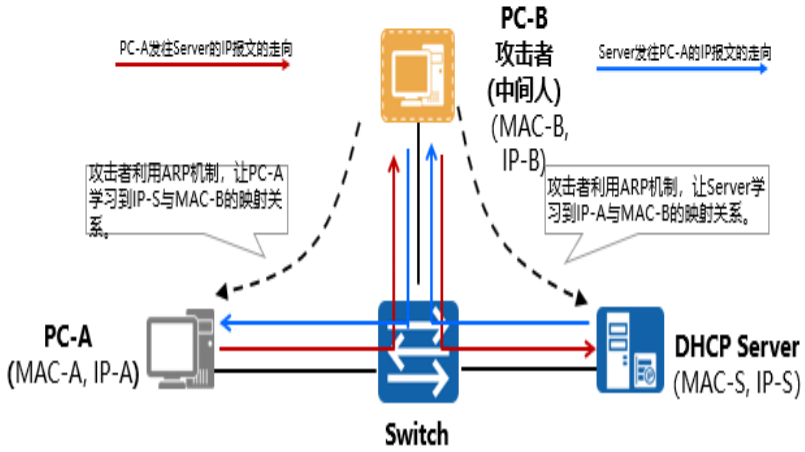
- 攻击原理：攻击者仿冒DHCP Server，向客户端分配错误的IP地址及提供错误的网关地址等参数，导致客户端无法正常访问网络。
- 漏洞分析：DHCP客户端接收到来自DHCP Server的DHCP消息后，无法区分这些DHCP消息是来自仿冒的DHCP Server，还是来自合法的DHCP Server。



- 攻击者私自安装并运行 DHCP Server 程序后，便可以把自己装扮成一个合法的 DHCP Server，这就是所谓的仿冒 DHCP Server。仿冒 DHCP Server 与合法的 DHCP Server 在工作原理上是完全一样的，所不同的是，仿冒 DHCP Server 会向客户端分配错误的 IP 地址及提供错误的网关地址等参数，导致客户端无法正常访问网络。
- 我们知道，客户端以广播方式发送 DHCP Discover 消息后，仿冒 DHCP Server 和合法的 DHCP Server 都能够收到该 DHCP Discover 消息，并且都会回应 DHCP Offer 消息。如果客户端最先收到的 DHCP Offer 消息是来自仿冒 DHCP Server，那么客户端就会继续向仿冒 DHCP Server（而不是合法的 DHCP Server）请求获得 IP 地址等参数，而仿冒 DHCP Server 就会乘机向客户端分配错误的 IP 地址及提供错误的网关地址等参数。

DHCP中间人攻击

- 攻击原理：攻击者利用ARP机制，让PC-A学习到IP-S与MAC-B的映射关系，又让Server学习到IP-A与MAC-B的映射关系。如此一来，PC-A与Server之间交互的IP报文都会经过攻击者中转。
- 漏洞分析：从本质上讲，中间人攻击是一种Spoofing IP/MAC攻击，中间人利用了虚假的IP地址与MAC地址之间的映射关系来同时欺骗DHCP的客户端和服务器。



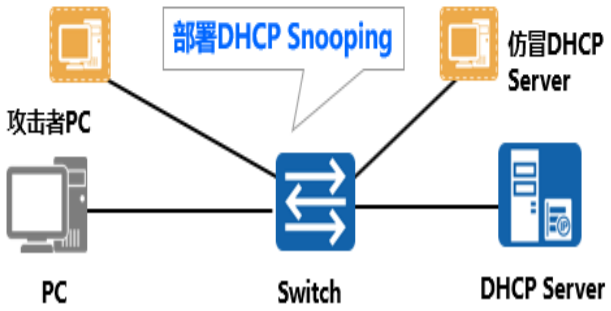
- 如图所示，攻击者利用 ARP 机制，让 PC-A 学习到 IP-S 与 MAC-B 的映射关系，又让 Server 学习到 IP-A 与 MAC-B 的映射关系。当 PC-A 向 DHCP Server 发送 IP 报文时，目的 IP 地址为 IP-S，源 IP 地址为 IP-A，而封装这个 IP 报文的帧的目的 MAC 地址为 MAC-B，源 MAC 地址为 MAC-A，所以这个帧会首先到达攻击者 PC-B。攻击者收到这个帧后，将这个帧的目的 MAC 地址更换为 MAC-S，源 MAC 地址更换为 MAC-B，然后将这个帧发往 Server。如此“偷梁换柱”，Server 是看不出任何破绽的。另一方面，当 DHCP Server 向 PC-A 发送 IP 报文时，目的 IP 地址为 IP-A，源 IP 地址为 IP-S，而封装这个 IP 报文的帧的目的 MAC 地址为 MAC-B，源 MAC 地址为 MAC-S，所以这个帧也会首先到达攻击者 PC-B。攻击者收到这个帧后，将这个帧的目的 MAC 地址更换为 MAC-A，源 MAC 地址更换为 MAC-B，然后将这个帧发往 PC-A。同样，PC-

A 也是看不出任何破绽的。

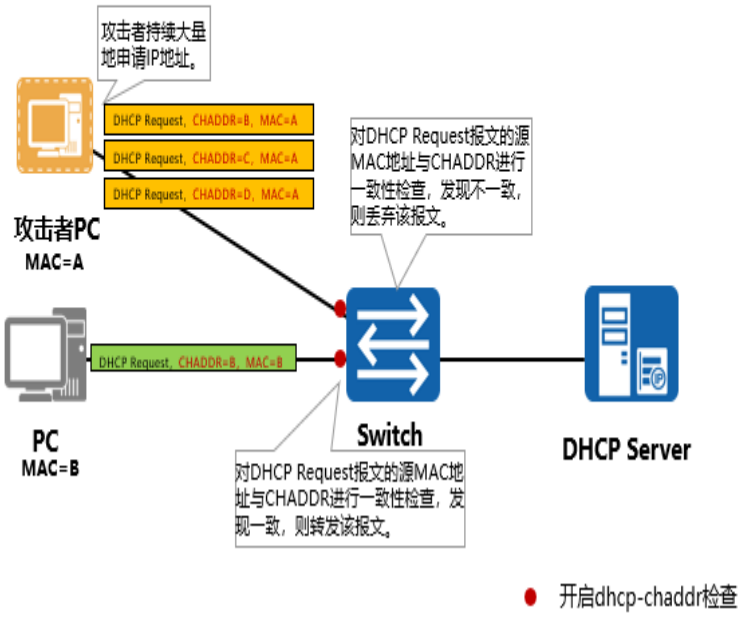
- 由于往来于 PC-A 与 DHCP Server 之间的 IP 报文都会经过攻击者（中间人）进行中转，攻击者便很容易窃取这些 IP 报文中的某些信息，并利用这些信息来进行其他的破坏行为。攻击者也可以很容易对往来于 PC-A 与 DHCP Server 之间的 DHCP 消息（这些消息是封装在 UDP 报文中的，而 UDP 报文又是封装在 IP 报文中的）进行篡改，达到直接攻击 DHCP 的目的。

DHCP Snooping技术的出现

- 为了增强网络安全，防止DHCP受到攻击，一种称为DHCP Snooping的技术应运而生。DHCP Snooping不是一种标准技术，尚未有统一的标准规范，不同的网络设备制造商在DHCP Snooping的实现上也不尽相同。
- DHCP Snooping部署在交换机上，其作用类似于在DHCP客户端与DHCP服务器端之间构筑了一道虚拟的防火墙。



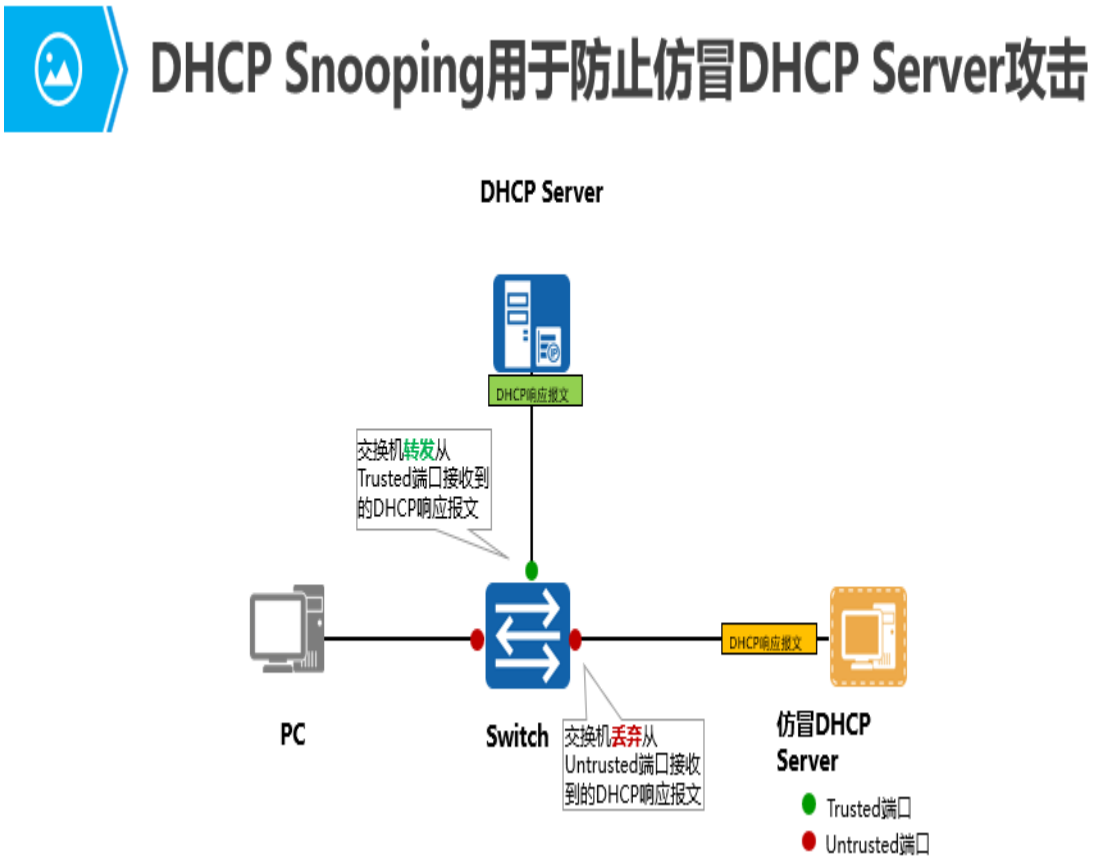
DHCP Snooping用于防止DHCP饿死攻击



- DHCP 饿死攻击是攻击者通过持续大量地向 DHCP Server 申请 IP 地址来实现的，其目的是耗尽 DHCP Server 地址池中的 IP 地址，导致 DHCP Server 没有 IP 地址分配给正常的用户。DHCP 消息中有一个名叫 CHADDR（Client Hardware Address）的字段，该字段是由 DHCP 客户端填写的，表示的是客户端的硬件地址（也就是客户端的 MAC 地址）。DHCP Server 是针对 CHADDR 来分配 IP 地址的，对于不同的 CHADDR，DHCP Server 会分配不同的 IP 地址；DHCP Server 无法区分什么样的 CHADDR 是合法的，什么样的 CHADDR 是非法的。利用这个漏洞，攻击者每申请一个 IP 地址时，就在 DHCP 消息的 CHADDR 字段中填写一个不同的值，以此来冒充是不同的用户在申请 IP 地址。
- 为了弥补上述漏洞，从而阻止饿死攻击，DHCP Snooping 技术支持在端口下对 DHCP Request 报文的源 MAC 地址

与 CHADDR 进行一致性检查：如果二者相同，则转发报文；如果二者不相同，则丢弃。如果要在某端口下实施源 MAC 地址与 CHADDR 的一致性检查，可以在该端口下使用命令 dhcp snooping check dhcp-chaddr enable。

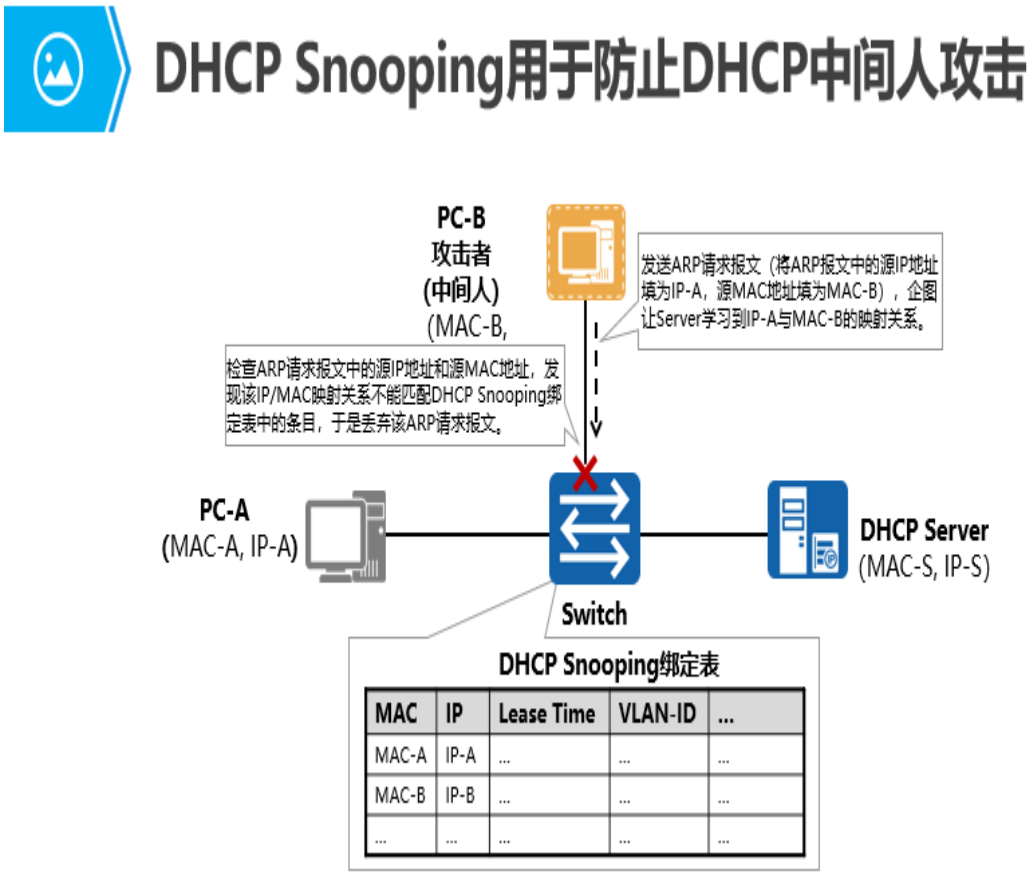
- 还可能存在这样一种饿死攻击，就是攻击者不断同时变换 MAC 地址和 CHADDR，并且每一次变换时，都让 CHADDR 与 MAC 地址相同，如此一来，便可以躲过上述源 MAC 地址与 CHADDR 的一致性检查！



- DHCP Snooping 将交换机上的端口分为两种类型，即信任端口（Trusted 端口）和非信任端口（Untrusted 端口）；与合法的 DHCP Server 相连接的端口应配置为 Trusted 端口，其他端口应配置为 Untrusted 端口。
- 交换机从 Trusted 端口接收到 DHCP 响应报文（例如 DHCP Offer 报文、DHCP Ack 报文等等）后，会转发这些报文，

从而保证合法的 DHCP Server 可以正常地分配 IP 地址及提供其他网络参数；交换机从 Untrusted 端口接收到 DHCP 响应报文（例如 DHCP Offer 报文、DHCP Ack 报文等等）后，会丢弃这些报文，从而阻止仿冒的 DHCP Server 分配 IP 地址及提供其他网络参数。

- 关键配置命令：交换机的端口默认是 Untrusted 端口。如果需要将交换机的某个端口配置为 Trusted 端口，可以在该端口视图下使用命令 dhcp snooping trusted。如果需要将某个 Trusted 端口恢复为 Untrusted 端口，可以在该端口视图下使用命令 undo dhcp snooping trusted。

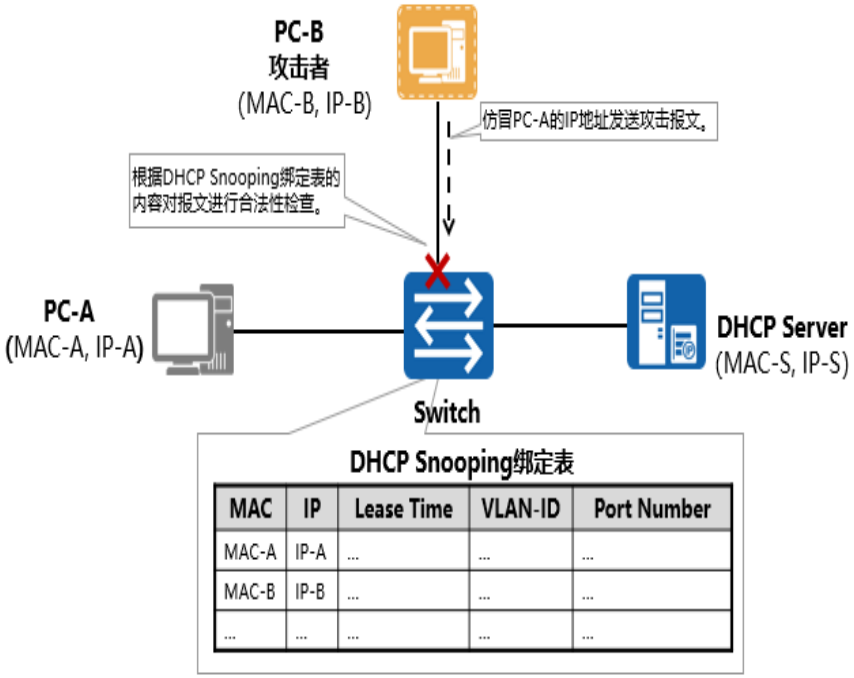


- 我们已经知道，DHCP 中间人攻击本质上是一种 Spoofing IP/MAC 攻击。要想防止 DHCP 中间人攻击，其实就是要防止 Spoofing IP/MAC 攻击。
- 运行了 DHCP Snooping 的交换机会“侦听（Snooping）”

往来于用户与 DHCP Server 之间的 DHCP 消息，并从中收集用户的 MAC 地址（这里的 MAC 地址是指 DHCP 消息中 CHADDR 字段的值）、用户的 IP 地址（这里的 IP 地址是指 DHCP Server 分配给相应 CHADDR 的 IP 地址）等信息，这些信息会集中存放在一个数据库中，该数据库也被称为 DHCP Snooping 绑定表。运行了 DHCP Snooping 的交换机会建立并动态维护 DHCP Snooping 绑定表，绑定表中除了包含了用户的 MAC 地址、用户的 IP 地址外，还包括 IP 地址租用期、VLAN-ID 等等信息。

- 如图所示，假设 DHCP Server 给 PC-A 分配了 IP 地址 IP-A，给 PC-B 分配了 IP 地址 IP-B，那么 IP-A 与 MAC-A 就形成了绑定关系，IP-B 与 MAC-B 也形成了绑定关系，这种绑定关系都存放于 DHCP Snooping 绑定表中。攻击者为了让 Server 学习到 IP-A 与 MAC-B 的映射关系，会发送 ARP 请求报文（将 ARP 报文中的源 IP 地址填为 IP-A，源 MAC 地址填为 MAC-B）。交换机接收到 ARP 请求报文后，会检查该 ARP 请求报文中的源 IP 地址和源 MAC 地址，发现该 IP/MAC（IP-A/MAC-B）映射关系不能匹配 DHCP Snooping 绑定表中的条目，于是会丢弃该 ARP 请求报文，这样就有效地防止了 Spoofing IP/MAC 攻击。
- 如果需要使用上面所描述的防止 Spoofing IP/MAC 攻击（进而防止中间人）的方法，就必须在交换机的系统视图下执行配置命令 arp dhcp-snooping-detect enable。

DHCP Snooping与IPSG技术的联动



- 网络中经常会存在针对源 IP 地址进行欺骗的攻击行为，例如，攻击者仿冒合法用户的 IP 地址来向服务器发送 IP 报文。针对这类攻击，相应的防范技术称为 IPSG（IP Source Guard）技术。
- 交换机使能 IPSG 功能后，会对进入交换机端口的报文进行合法性检查，并对报文进行过滤（如果合法，则转发；如果非法，则丢弃）。
- DHCP Snooping 技术可与 IPSG 技术进行联动，即：对于进入交换机端口的报文进行 DHCP Snooping 绑定表匹配检查，如果报文的信息和与绑定表一致，则允许其通过，否则丢弃报文。
- 报文的检查项可以是源 IP 地址、源 MAC 地址、VLAN 和物理端口号的若干种组合。例如，在交换机的端口视图下可支持 IP+MAC、IP+VLAN、IP+MAC+VLAN 等组合检查，在

交换机的 VLAN 视图下可支持：IP+MAC、IP+物理端口号、IP+MAC+物理端口号等组合检查。

- 关键配置命令：在交换机的端口视图下或 VLAN 视图下执行配置命令 ip source check user-bind enable。

思考题

1. DHCP客户端向DHCP Server进行续租时会发送哪种报文？（ ）

   A. DHCP Discover

   B. DHCP Offer

   C. DHCP Request

   D. DHCP Ack

2. DHCP常见攻击分为哪几种？（ ）

- 答案：C。
- 答案：DHCP 饿死攻击、仿冒 DHCP Server 攻击、DHCP 中间人攻击。