南京大学 软件学院
NANJING UNIVERSITY · SOFTWARE INSTITUTE

DHCP

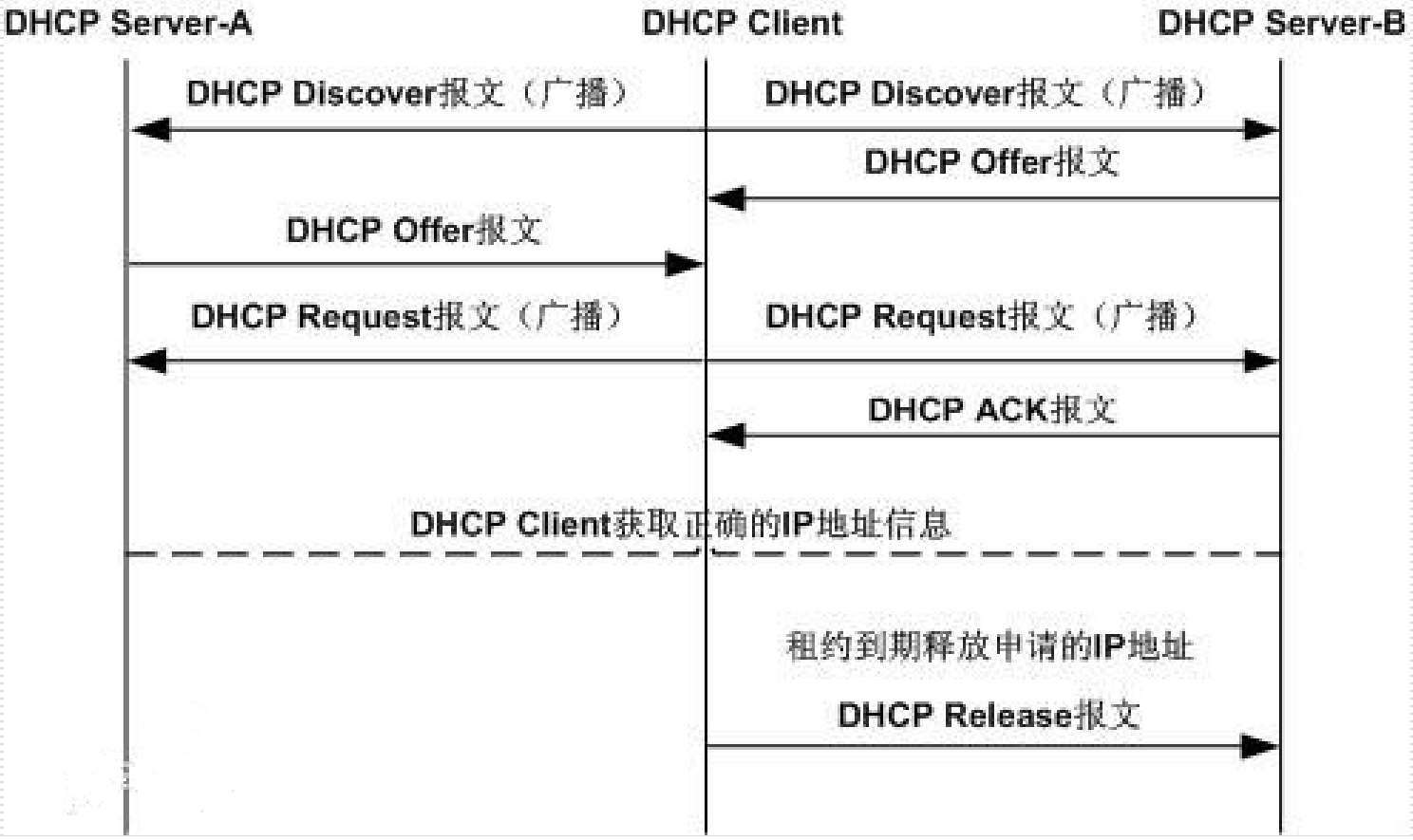
DHCP

- DHCP工作原理
- DHCP欺骗及防范

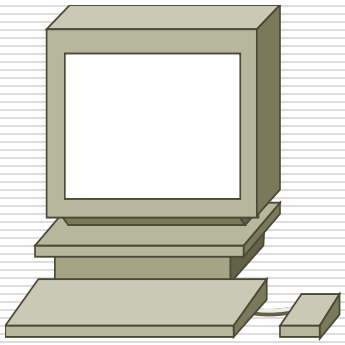
DHCP概述

- 一个协议软件在使用之前先作正确协议配置，具体配置内容取决于协议。
- 连接到因特网的计算机的协议软件需要配置的项目包括：
  - IP 地址
  - 于网掩码
  - 默认路由器的IP 地址
  - 域名服务器的IP 地址
- Dynamic Host Configuration Protocol可以高效地分配IP地址
  - 局域网的网络协议
  - 使用UDP来实现

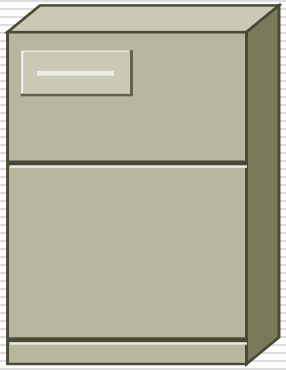
DHCP工作过程


DHCP Server-A
DHCP Client
DHCP Server-B
DHCP Discover报文（广播）
DHCP Discover报文（广播）
DHCP Offer报文
DHCP Offer报文
DHCP Request报文（广播）
DHCP Request报文（广播）
DHCP ACK报文
DHCP Client获取正确的IP地址信息
租约到期释放申请的IP地址
DHCP Release报文

发现阶段



DHCP Discover
UDP Broadcast



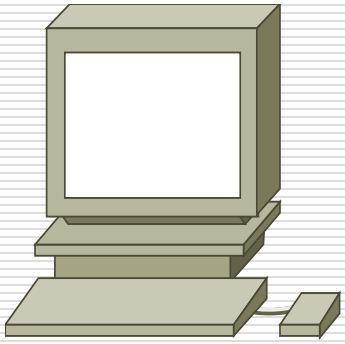
MAC: Known
IP: Unknown

DHCP server

IP1
IP2
IP3

- DHCP Client开始并不知道DHCP Server的ip地址,因此以广播的方式发出DHCP Discover报文

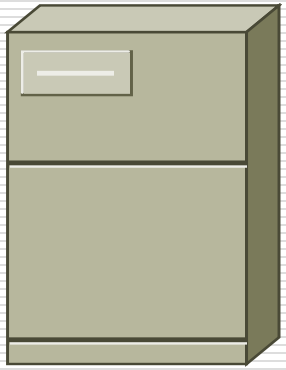
响应阶段



MAC: Known
IP: Unknown

DHCP Offer
UDP Unicast

IP Address
Gateway
IP of servers
And more …

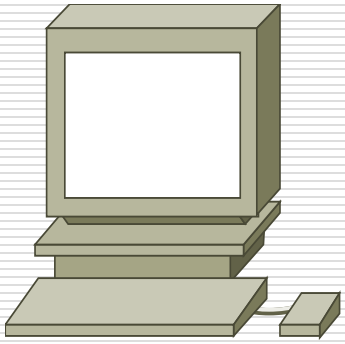


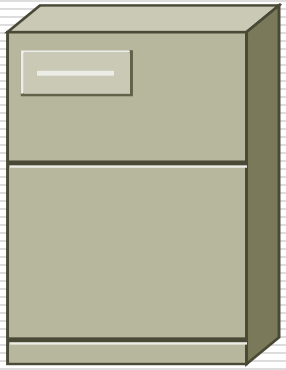
DHCP server

IP1
IP2
IP3

- DHCP Server在IP地址池中查找合法的IP地址通过DHCP Offer报文提供给DHCP Client

选择阶段





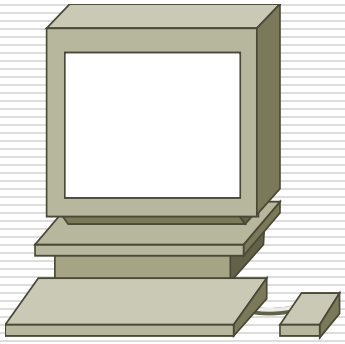
MAC: Known
IP: Unknown

DHCP server

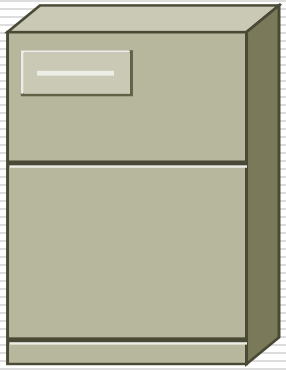
IP1
IP2
IP3

- DHCP Client选择一个DHCP Offer报文（一般选择最先收到的DHCP Offer报文），向网络发送一个DHCP Request广播数据包

租约确认阶段



Broadcast DHCP Ack



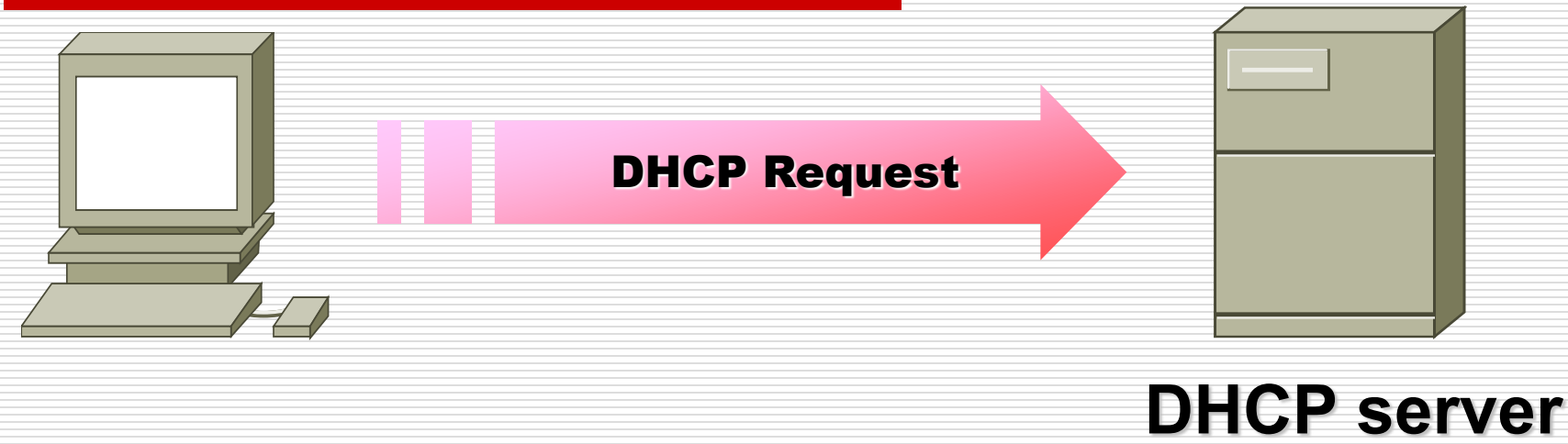
MAC: Known
IP: Unknown

DHCP server

IP1
IP2
IP3

- DHCP Server接收到DHCP Request消息后，以DHCP ACK消息向DHCP Client广播成功的确认；出错则广播否定确认消息DHCP NAK

租期续约



- 在租期中，DHCP Client直接向为其提供IP地址的DHCP Server发送DHCP Request消息，收到回应的DHCP ACK消息后， DHCP Client根据所提供的新的租期以及其它更新的TCP/IP参数更新自己的配置，IP租用更新完成

租期释放

- 当DHCP Client不再需要使用分配IP地址时，就会主动向DHCP Server发送Release报文，告知不再需要分配IP地址，DHCP Server会释放被绑定的租约

DHCP报文结构

OP	HTYPE	HLEN	跳数(Hops)
事务ID(XID)			
秒数(Seconds)		标志(flags)	
客户机IP地址(ciaddr)			
你的IP地址(yiaddr)			
服务器IP地址(siaddr)			
中继代理IP地址(giaddr)			
客户机硬件地址(chaddr)			
服务器的主机名(sname)			
启动文件名(file)			
选项(option)			

DHCP报文类型

- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP ACK
- DHCP NAK
- DHCP Release
- DHCP Decline
- DHCP Inform

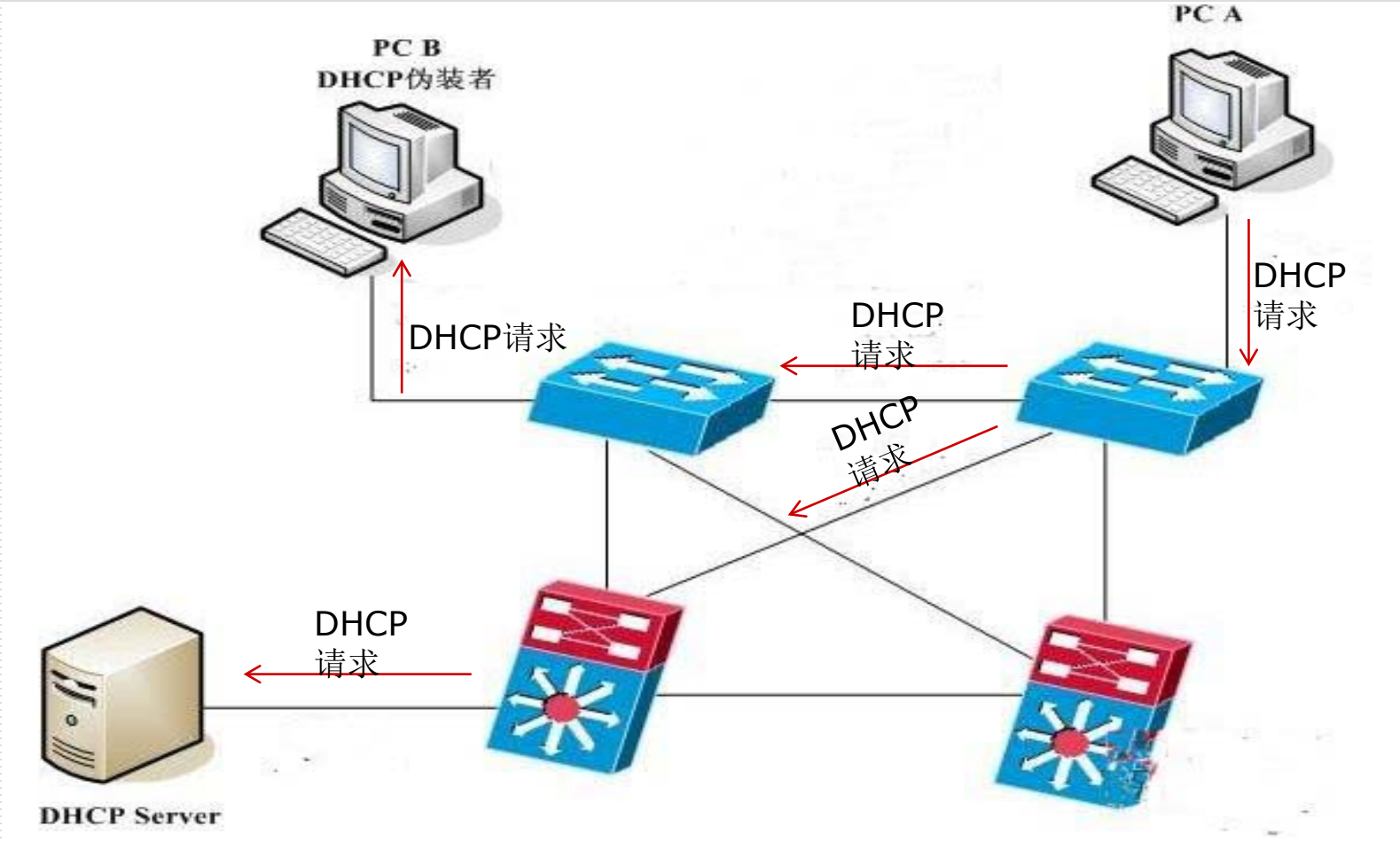
DHCP

- DHCP工作原理
- DHCP欺骗及防范

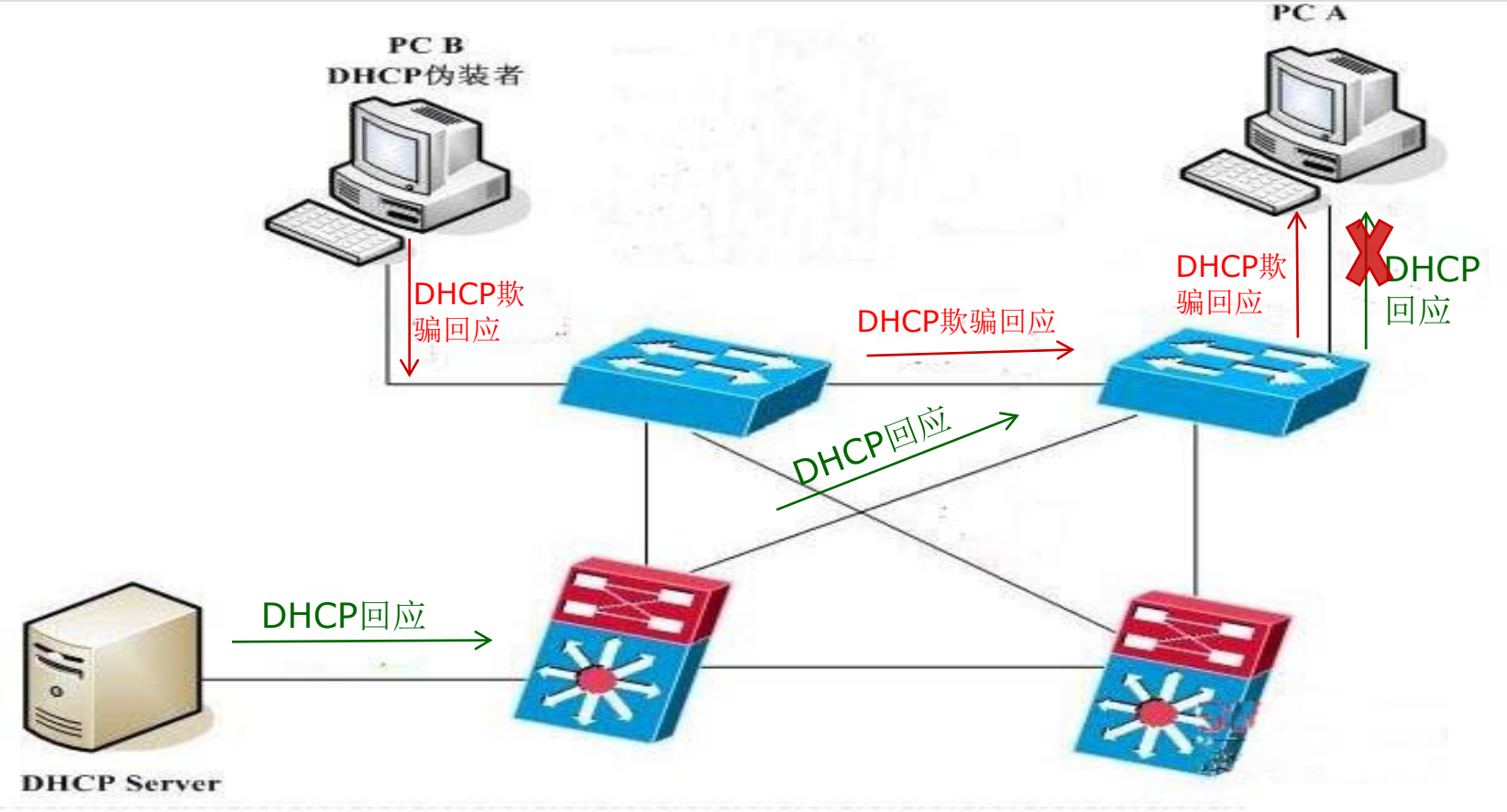
DHCP欺骗原理

- 客户端以广播的方式来寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数。
- 非授权的DHCP服务器先应答，客户端最后获得的网络参数即是非授权的，客户端即被欺骗。
- 在实际应用DHCP的网络中，基本上都会采用DHCP中继，因此本网络的非授权DHCP服务器一般都会先于其余网络的授权DHCP服务器的应答（由于网络传输的延迟），在这样的应用中，DHCP欺骗更容易完成。

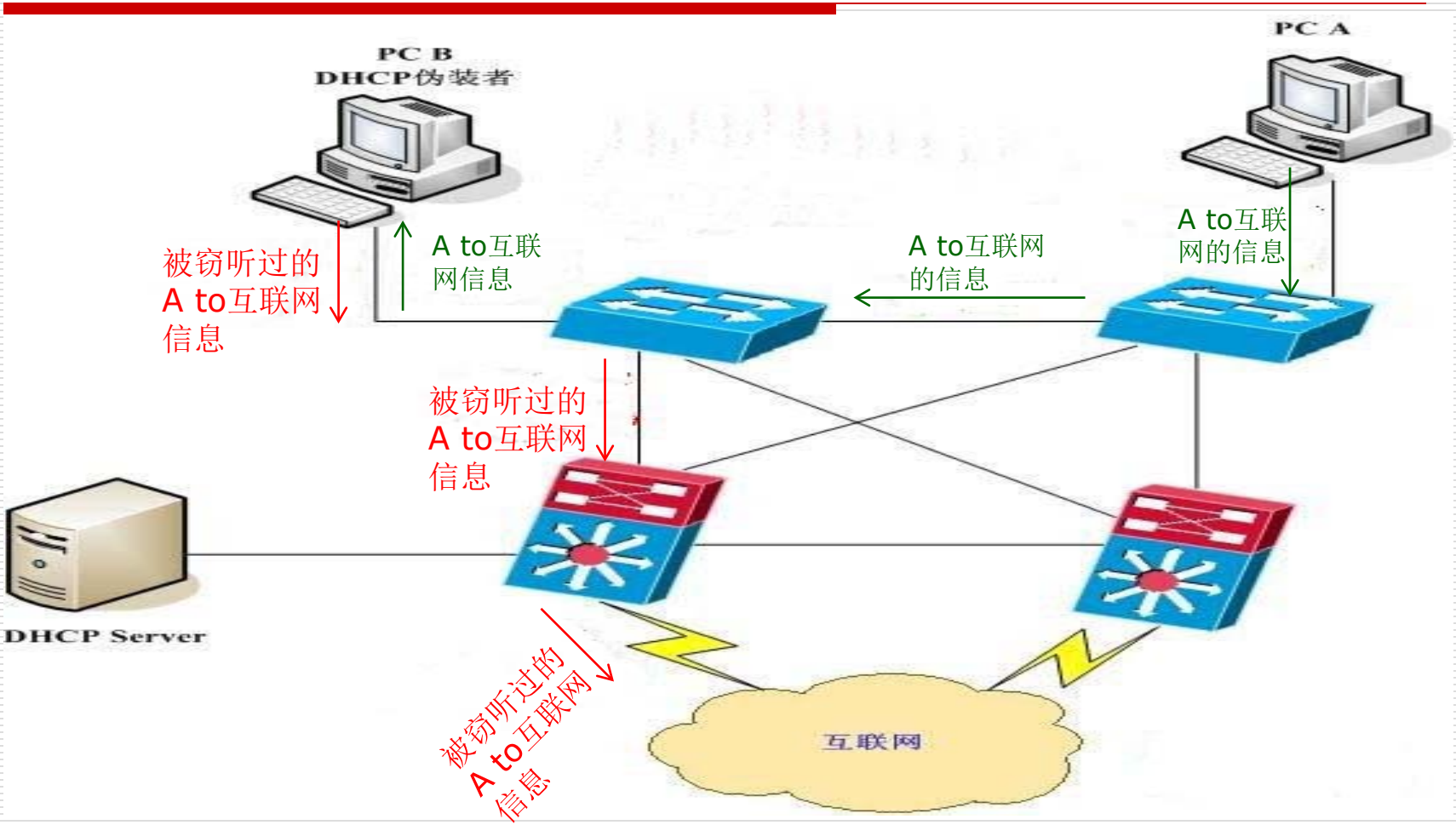
DHCP欺骗攻击


PC B
DHCP伪装者
PC A
DHCP请求
DHCP
请求
DHCP
请求
DHCP
请求
DHCP
请求
DHCP Server

DHCP欺骗攻击


PC B
DHCP伪装者
PC A
DHCP欺骗回应
DHCP欺骗回应
DHCP欺骗回应
DHCP回应
DHCP回应
DHCP回应
DHCP Server

DHCP欺骗攻击


PC B
DHCP伪装者
PC A
被窃听过的
A to互联网
信息
A to互联
网信息
A to互联网
的信息
A to互联
网的信息
被窃听过的
A to互联网
信息
DHCP Server
被窃听过的
A to互联网
信息
互联网

DHCP欺骗防范

- 在交换机上启用DHCP Snooping功能

  DHCP Snooping技术通过建立和维护DHCP Snooping绑定表过滤不可信任的DHCP信息

  - 在交换机的全局配置模式中启用DHCP Snooping

    switch (config)# ip dncp snooping

  - 在交换机的全局配置模式中开启需要启用DHCP Snooping的VLAN

    switch (config)# ip dhcp snooping vlan vlan号

  - 在端口配置子模式中将授权DHCP服务器所连的端口设为信任端口（缺省都是非信任的端口）

    switch (config-if)# ip dhcp snooping trust

谢 谢！