

细说ARP安全

李洋

51CTO blog: patterson.blog.51cto.com

提纲

- ❖ ARP攻击类型
- ❖ 常用防范措施
- ❖ 主流产品简介

什么是ARP

❖ ARP（Address Resolution Protocol）

☞ 简单的说，ARP就是IP和MAC的对应关系

❖ ARP原理

☞ ARP请求

- ❖ 某机器A要向主机B发送报文，会查询本地的ARP缓存表，找到B的IP地址对应的MAC地址后，进行数据传输
- ❖ 如果未找到，则广播一个ARP请求报文

☞ ARP应答

- ❖ 网上所有主机包括B都收到ARP请求，理想情况是只有主机B向主机A发回一个ARP响应报文，其中包含有B的MAC地址

☞ 存在风险

- ❖ 不幸的是，网内所有的主机均可向A发回一个ARP响应报文，并且可以随意修改ARP响应报文中的IP和MAC

什么是ARP攻击

❖ ARP攻击

- ❧ 就是通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量使网络阻塞
- ❧ 攻击者只要持续不断的发出伪造的ARP响应报文就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击
- ❧ ARP攻击的危害主要存在于局域网网络中
- ❧ 如果局域网中有一个人感染ARP病毒，则感染该ARP病毒的系统将会试图通过“ARP欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障

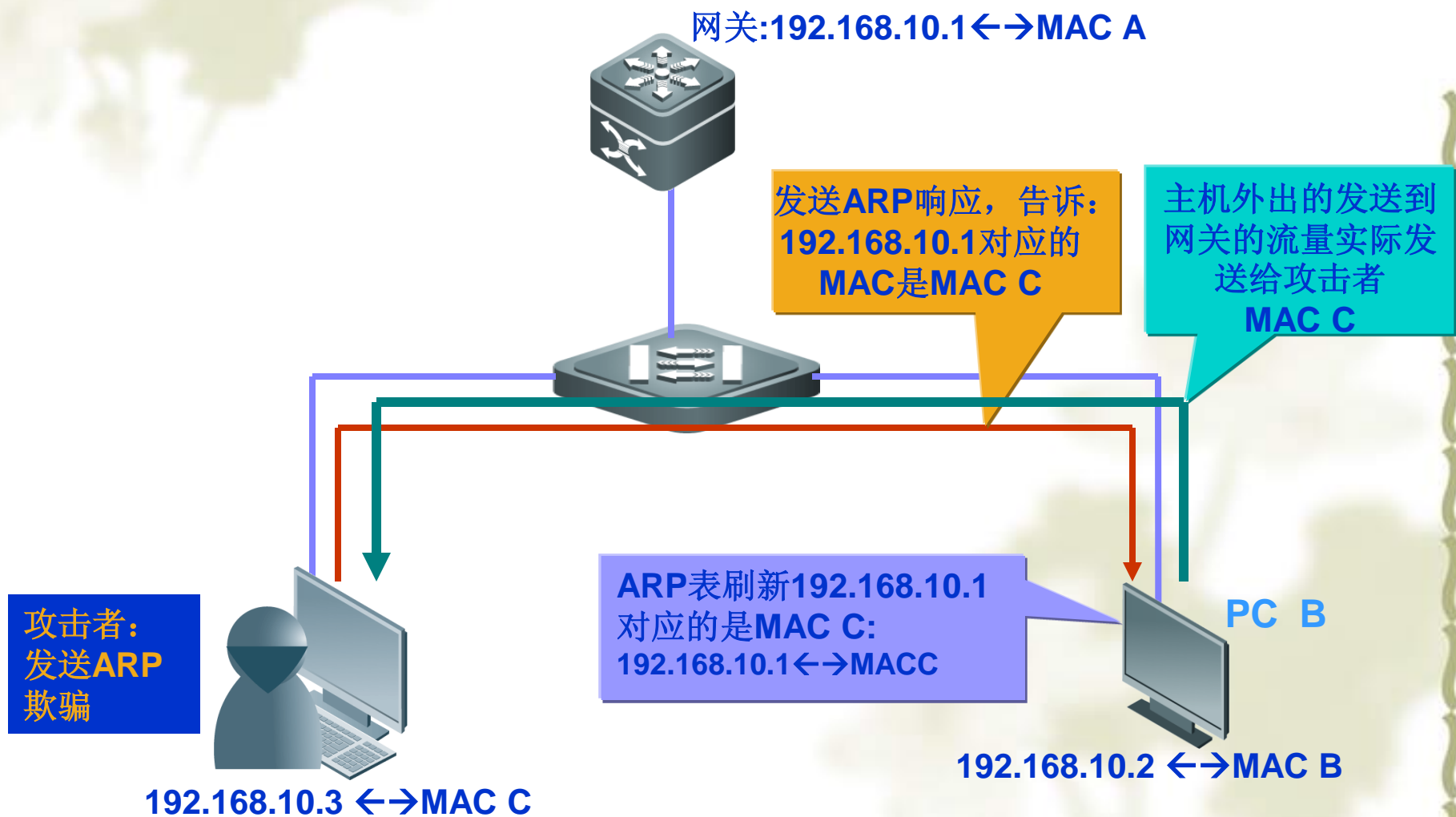
ARP攻击的主要现象

- ❖ 上网速度慢
 - 🌀 网络上有大量ARP报文
- ❖ 某一区域不能上网或时通时断
- ❖ 同样配置只有某一台机器不能上网
- ❖ 正在使用某一类应用的PC依次掉线或时通时断
- ❖ 不断弹出“本机的0-255段硬件地址与网络中的0-255段地址冲突”的对话框，等等

ARP攻击的主要形式

- ❖ **ARP欺骗攻击**
 - ☞ 欺骗主机攻击
 - ❖ 冒充网关攻击
 - ☞ 欺骗网关攻击
 - ☞ 中间人攻击
- ❖ **ARP泛洪攻击**
 - ☞ 消耗带宽攻击
 - ☞ 拒绝服务攻击
 - ☞ ARP溢出攻击
- ❖ **ARP扫描攻击**
- ❖ **IP地址冲突**
 - ☞ 单播型的IP地址冲突
 - ☞ 广播型的IP地址冲突
- ❖ **虚拟主机攻击**

欺骗主机攻击



欺骗网关攻击

网关:192.168.10.1 ↔ MAC A

ARP表刷新, 192.168.10.2
对应的是MAC C:
192.168.10.2 ↔ MAC C

发送ARP响应, 告诉:
192.168.10.2对应的
MAC是MAC C

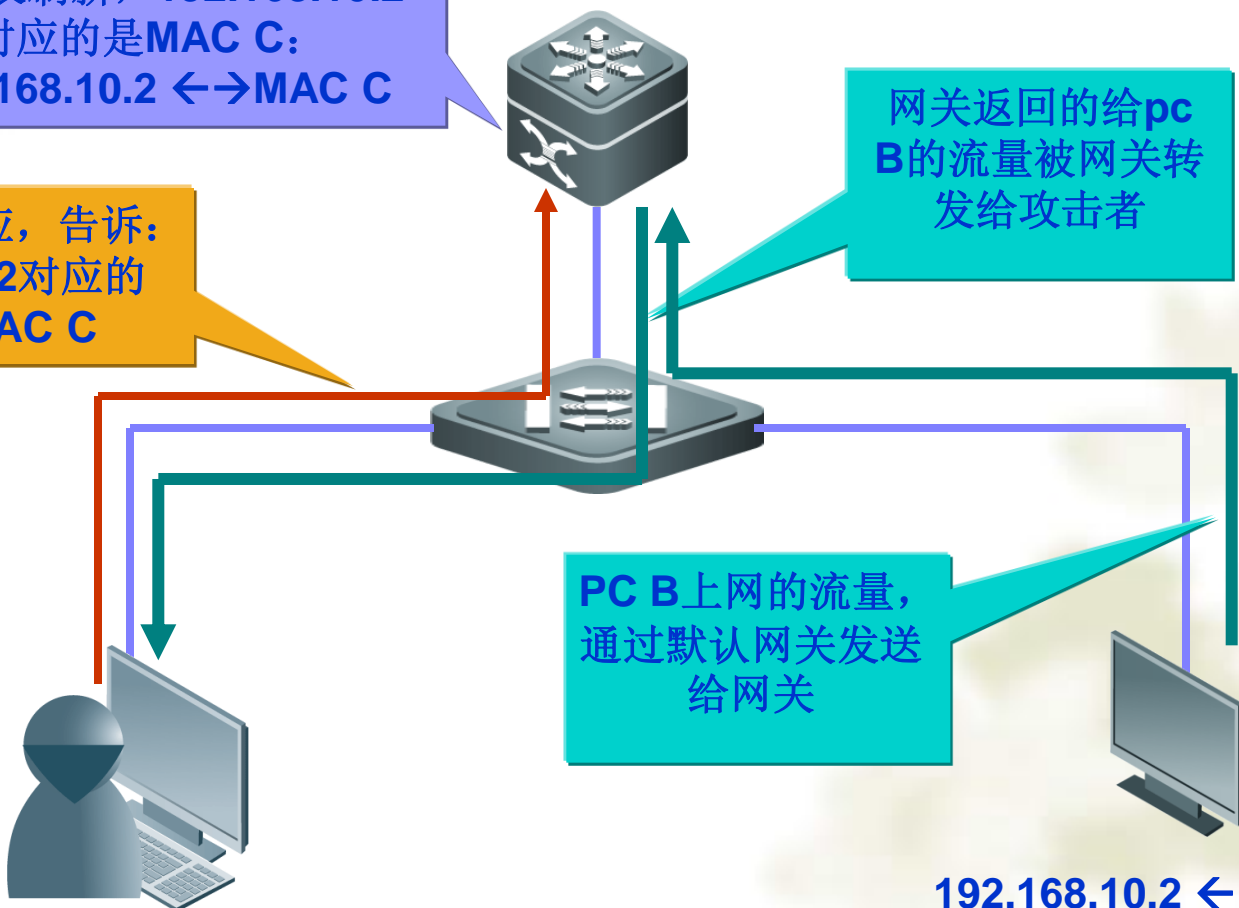
网关返回的给PC
B的流量被网关转
发给攻击者

PC B上网的流量,
通过默认网关发送
给网关

攻击者:
发送ARP
欺骗

192.168.10.3 ↔ MAC C

192.168.10.2 ↔ MAC B



中间人攻击

ARP表刷新，
192.168.10.2对应的
的是MAC C

发送ARP响应，告诉：
192.168.10.2对应的
MAC是MAC C

攻击者再把流量
转发给真正的
网关MAC A

攻击者：
发送ARP
欺骗

192.168.10.3
MAC C

ARP表刷新，
192.168.10.1对应
的是MAC C

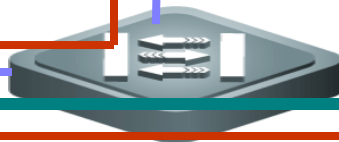
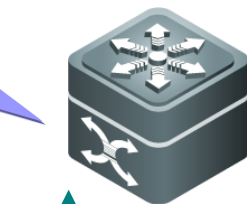
192.168.10.1
MAC A

发送ARP响应，告诉：
192.168.10.1对应的
MAC是MAC C

发送到网关的流量
均发到攻击者
MAC C

PC B

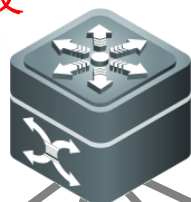
192.168.10.2
MAC B



ARP泛洪攻击

1、发送大量ARP请求报文

2、发送大量虚假的
ARP响应报文



网关E
IP:192.168.10.254
Mac: E

1、消耗网络带宽资源。ARP扫描往往是进一步攻击的前奏。

2、网关E的CPU利用率上升，难以响应正常服务请求。

3、网关E被错误ARP表充满，导致无法更新维护正常ARP表

IP	MAC
192.168.10.1	MAC A
192.168.10.2	MAC B
192.168.10.3	MAC C
192.168.10.4	MAC D
.....
192.168.10.N	MAC N

主机A
IP:192.168.10.1
Mac: MAC A

主机B
IP:192.168.10.2
Mac:MAC B

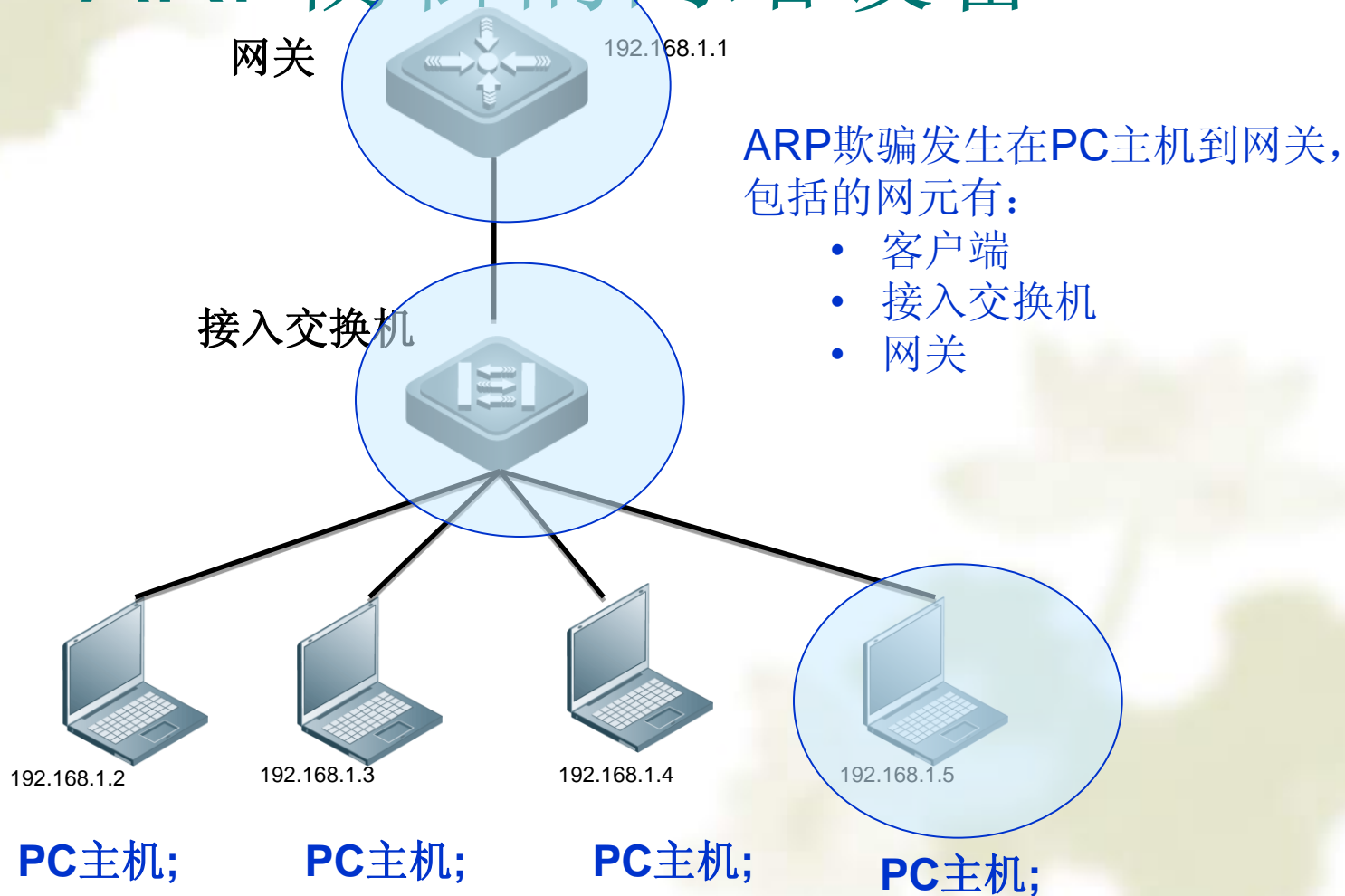
主机C
IP:192.168.10.3
Mac:MAC C

主机D
IP:192.169.10.4
Mac:MAC D

ARP泛洪攻击

- ❖ 攻击主机持续把伪造的**MAC-IP**映射对发给受攻击主机，对于局域网内的所有主机和网关进行广播，抢占网络带宽和干扰正常通信。这种攻击方式的主要攻击特征包含：
 - ⚡ 通过不断发送伪造的**ARP**广播数据包使得**交换机**忙于处理广播数据包而耗尽网络带宽
 - ⚡ 令局域网内部的主机或网关找不到正确的通信对象，使得正常通信被阻断
 - ⚡ 用虚假的地址信息占满主机的**ARP**高速缓存空间，造成主机无法创建缓存表项，无法正常通信，这种攻击特征作者将其命名为**ARP**溢出攻击
 - ❖ 主机**ARP**缓存溢出
 - ❖ 交换机**CAM**表溢出
- ❖ **ARP**泛洪攻击不是以盗取用户数据为目的，它是以破坏网络为目的，属于损人不利己的行为

ARP防御的网络设备



提纲

- ❖ ARP攻击类型
- ❖ 常用防范措施
- ❖ 主流产品简介

客户端ARP防御手段1—主机手动绑定ARP 表

❖ 优点

- ☞ 最节省成本的方式

❖ 缺点

- ☞ 配置麻烦，主机需要通信的目标很多，不可能一个一个都绑定

- ☞ 容易失效，这种方法进行的绑定，一拔掉网线或者关机、注销就全部失效了，如果想继续使用，就需要重新绑定

- ☞ 只能进行主机端的防御，如果网关遭欺骗则无能为力

- ☞ 主机端手动绑定也是只能实现部分防御，需要与其他方法结合来完善

客户端ARP防御手段2—主机安装 ARP防御软件

❖ 原理

☞ 每个主机都不停地发送免费ARP Response广播，来告诉别人自己的IP和MAC的绑定关系

❖ 优点

☞ 硬件无关性

❖ 缺点

☞ 如果攻击广播报文频率提升，ARP问题重现

☞ 主机ARP表更新频繁，容易掉线

交换机ARP防御手段—ARP欺骗

ARP报文

.....

Sender IP

Send MAC

.....

.....

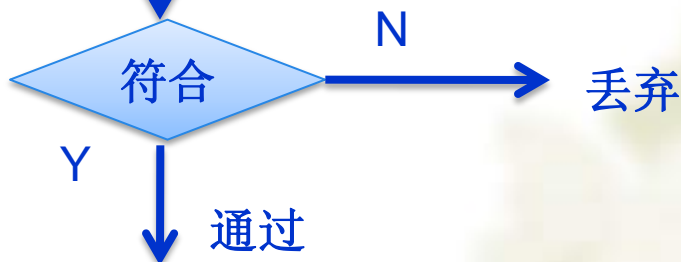
IP 和 MAC

第一步:

绑定用户正确的IP和MAC地址

第二步:

检查ARP报文中的IP和MAC



关键是如何建立真实的IP-MAC表

交换机防御ARP 欺骗1—接入交换机 手动绑定IP/MAC

❖ 交换机功能

- ☞ 支持在端口设置安全地址
- ☞ 支持在端口做ARP CHECK

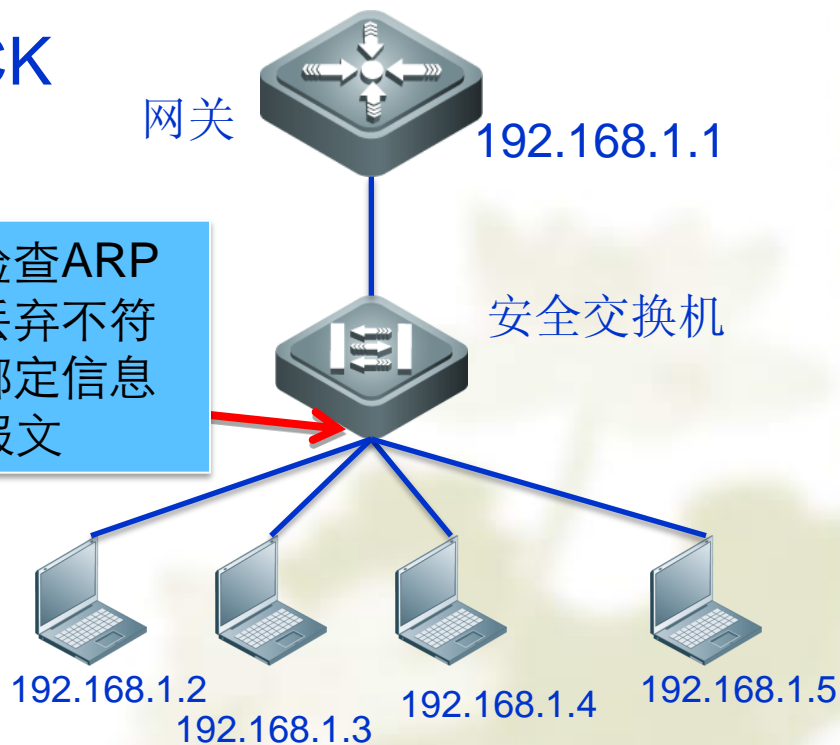
❖ 优点

- ☞ 成本低

❖ 缺点

- ☞ 工作量大，维护不方便
- ☞ 防范范围有限（到端口）
- ☞ 无法适应DHCP环境

在端口检查ARP
报文，丢弃不符
合端口绑定信息
的ARP报文



交换机防御ARP 欺骗2—动态

ARP检查DAI

❖ 交换机支持功能

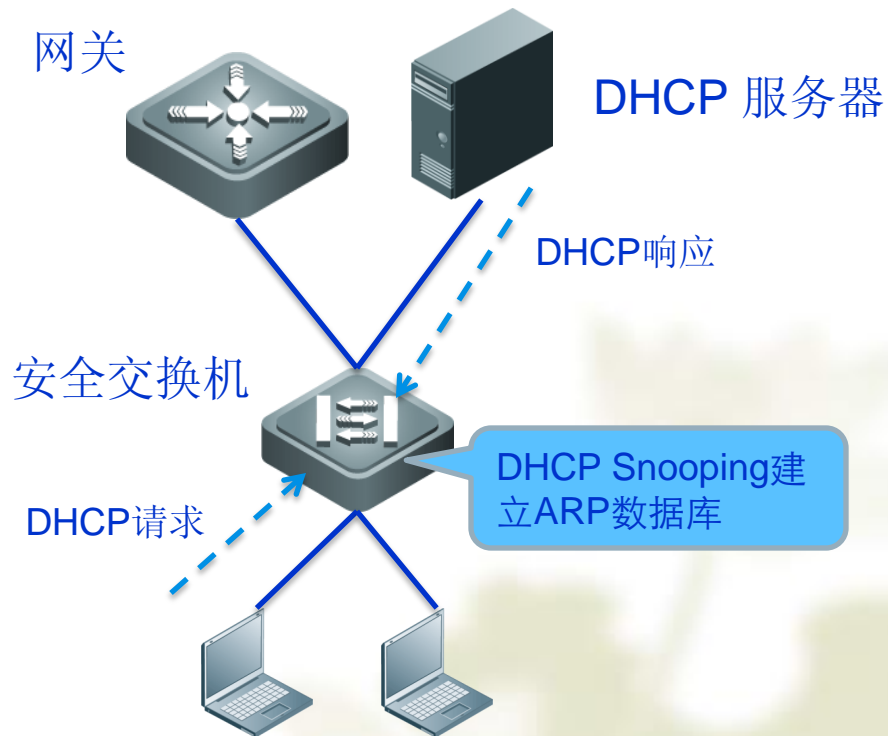
- ☞ 支持DHCP SNOOPING 功能
- ☞ 支持动态ARP检查 (DAI) 功能

❖ 优点

- ☞ 自动化实现ARP绑定
- ☞ 部署简单

❖ 缺点

- ☞ 适合于动态IP环境，如在静态IP环境则回归手动绑定的原始状态



交换机防御ARP欺骗3—接入交换机手动绑定网关

❖ 交换机功能

☞ 支持防网关欺骗功能

❖ 作用

☞ 防冒充网关攻击

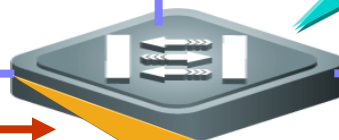
发送ARP响应，告诉：
192.168.10.1对应的
MAC是MAC C

攻击者：
发送ARP
欺骗

192.168.10.3 ↔ MAC C



网关:192.168.10.1↔MAC A



交换机非上联接口打开防网关ARP欺骗功能，过滤用户对网关ip的非法arp响应

下联口有对指定网关的arp响应，deny!

ARP表项重网关192.168.10.1
对应的依旧是MAC A:
192.168.10.1↔MAC A

PC B

192.168.10.2 ↔ MAC B

❖ 优点：操作简单

❖ 缺点：只能防冒充网关攻击，防范范围有限（到端口）

交换机防御ARP 欺骗4—结合802.1x技术

❖ 交换机支持功能

支持802.1x

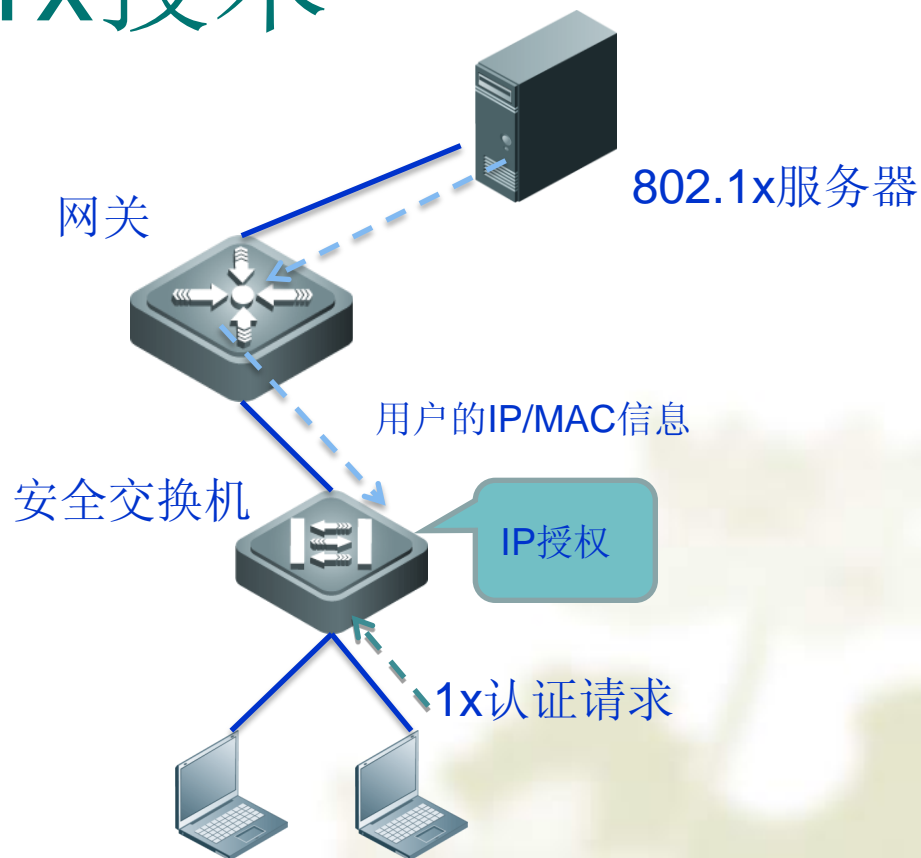
◆ 优点

认证过程中自动绑定IP-MAC

动/静态IP环境皆可

❖ 缺点

防范范围受限 (到端口)



网关防御ARP 欺骗手段—网关绑定

主机IP/MAC

❖ 作用

🔒 防欺骗网关攻击

用户的arp信息已经在网关的arp表项中，网关不再学习已存在表项的信息

网关:192.168.10.1 ↔ MAC A

网关绑定主机正确的ip ↔ mac关系:
Ip B ↔ mac B
Ip C ↔ mac C
.....
Ip N ↔ mac N

发送ARP响应，告诉：
192.168.10.2
对应的MAC是
MAC C

攻击者：
发送ARP
欺骗



192.168.10.3 ↔ MAC C

网关返回给PC B
的流量被网关正确
地发送给PC B

192.168.10.2 ↔ MAC B

PC B上网
的流量，通过默认网关
发送给网关



PC B

❖ 优点：成本低

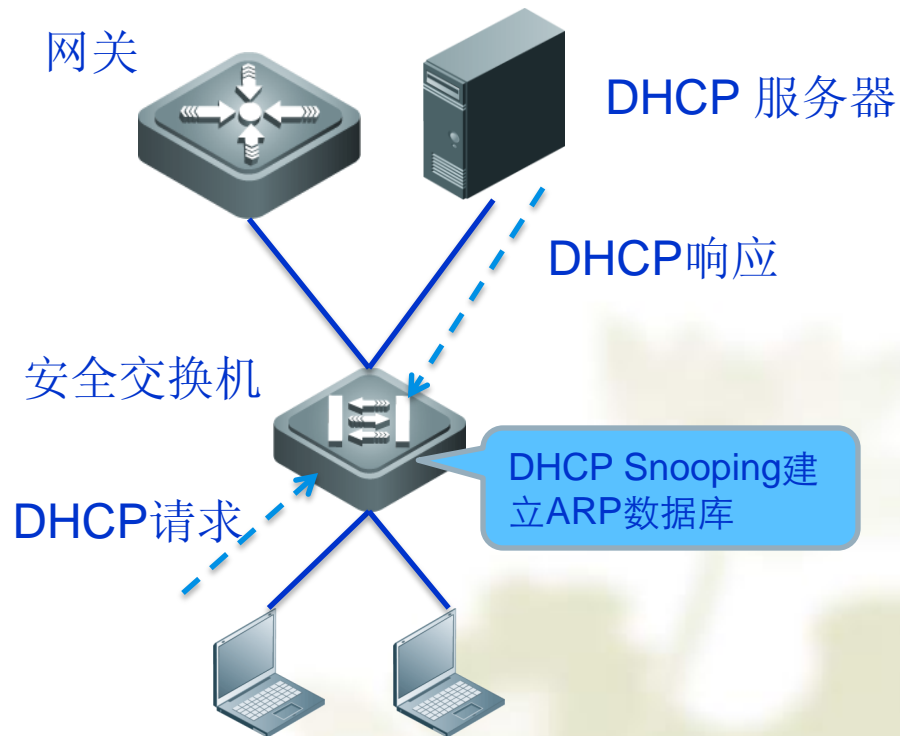
❖ 缺点：工作量大维护不方便；只能防欺骗网关攻击，不适应DHCP环境

交换机ARP防御手段—ARP泛洪攻击防御

❖ 交换机支持功能

❧ 支持ARP流限速

❧ 支持在端口下限速
或者在全局下限速



提纲

- ❖ ARP攻击类型
- ❖ 常用防范措施
- ❖ 主流产品简介

Cisco防ARP方法

❖ 交换机防ARP

- ❧ 安全端口

- ❧ DAI，配合DHCP SNOOPING

 - ❖ 利用DHCP SNOOPING建立的ARP数据库，过滤ARP包

 - ❖ 防主机欺骗攻击和网关欺骗攻击

 - ❖ 限制端口ARP报文数量，防ARP泛洪攻击

- ❧ IP Source Guard，配合DHCP SNOOPING，基于端口

 - ❖ 识别ARP报文是否是ARP欺骗

H3C防ARP方法

❖ 交换机防ARP

🔗 ARP CHECK

- ❖ 允许合法ARP报文通过
- ❖ 防主机欺骗和网关欺骗攻击

🔗 ARP DETECTION

- ❖ 利用DHCP SNOOPING建立的ARP数据库，过滤ARP报文
- ❖ 防主机欺骗攻击和网关欺骗攻击
- ❖ 限制端口ARP报文数量，防ARP泛洪攻击

🔗 核心交换机支持“授权ARP”

- ❖ 建立不被攻击者改动的ARP表
- ❖ 9055/7500/5600/5500/5510/5000/3600

🔗 ARP源抑制

- ❖ 限制ARP攻击流，防泛洪攻击

🔗 ARP源地址检查

- ❖ 识别ARP报文是否是ARP欺骗

🔗 支持“一键绑定”

- ❖ E126A/S3100/S3600/S5000/S5100，快速配置静态ARP

❖ CAMS

🔗 下传网关IP+MAC绑定到客户端

🔗 在网关建立用户IP+MAC的授权ARP表

神码防ARP方法

❖ 交换机

☞ 访问管理AM

- ❖ 类似安全地址+arp check, 防欺骗主机和欺骗网关攻击

☞ ARP Guard功能

- ❖ 类似anti-arp-spoofing, 防冒充网关攻击

☞ DHCP SNOOPING

- ❖ 建立ARP数据库, 实现端口地址动态绑定

☞ Anti-arpscan

- ❖ ARP限速, 防ARP泛洪攻击、防ARP扫描攻击


❖ DCBI

☞ 静态地址环境, DCBI下发用户IP+MAC到客户端

☞ 动态地址环境, 接入交换机上传用户IP+MAC到DCBI

防ARP方案厂商对比表

防ARP功能	锐捷	H3C	神码	Cisco	作用
端口安全地址	安全地址	端口绑定	AM功能	安全端口	防欺骗主机和欺骗网关攻击
端口ARP包检查	ARP-CHECK	ARP CHECK		无	
建立ARP数据库	DHCP SNOOPING	DHCP SNOOPING	DHCP SNOOPING	DHCP SNOOPING	防欺骗主机和欺骗网关攻击，防泛洪攻击
动态ARP包检查	DAI	ARP Detection	无	DAI	
防网关ARP欺骗	Anti-arp-spoofing	无	ARP Guard	无	防冒充网关攻击
ARP防攻击	ARP-Guard	无	无	无	识别、隔离和清除ARP攻击源，防泛洪攻击，防扫描攻击
ARP流限速	NFPP, DAI	ARP源抑制, ARP Detection	Anti-arpscan	无	防泛洪攻击
ARP源地址检查	无	ARP源地址检查	无	ARP源地址检查	判断ARP源地址的真实性，防ARP欺骗
特色ARP表	可信ARP表	授权ARP	无	无	建立不被攻击者更改的ARP表，防ARP欺骗
全局安全系统	GSN实现三重立体防ARP	CAMS实现网关和客户端两层，交换机通过ARP SNOOPING学习用户IP+MAC	静态地址，DCBI把用户IP+MAC下发交换机；动态地址，交换机把用户IP+MAC发给DCBI	无	通过网关、接入交换机、用户端三层实现全局自动防ARP
其它		交换机支持“一键绑定”			实现快速静态ARP绑定



谢 谢！