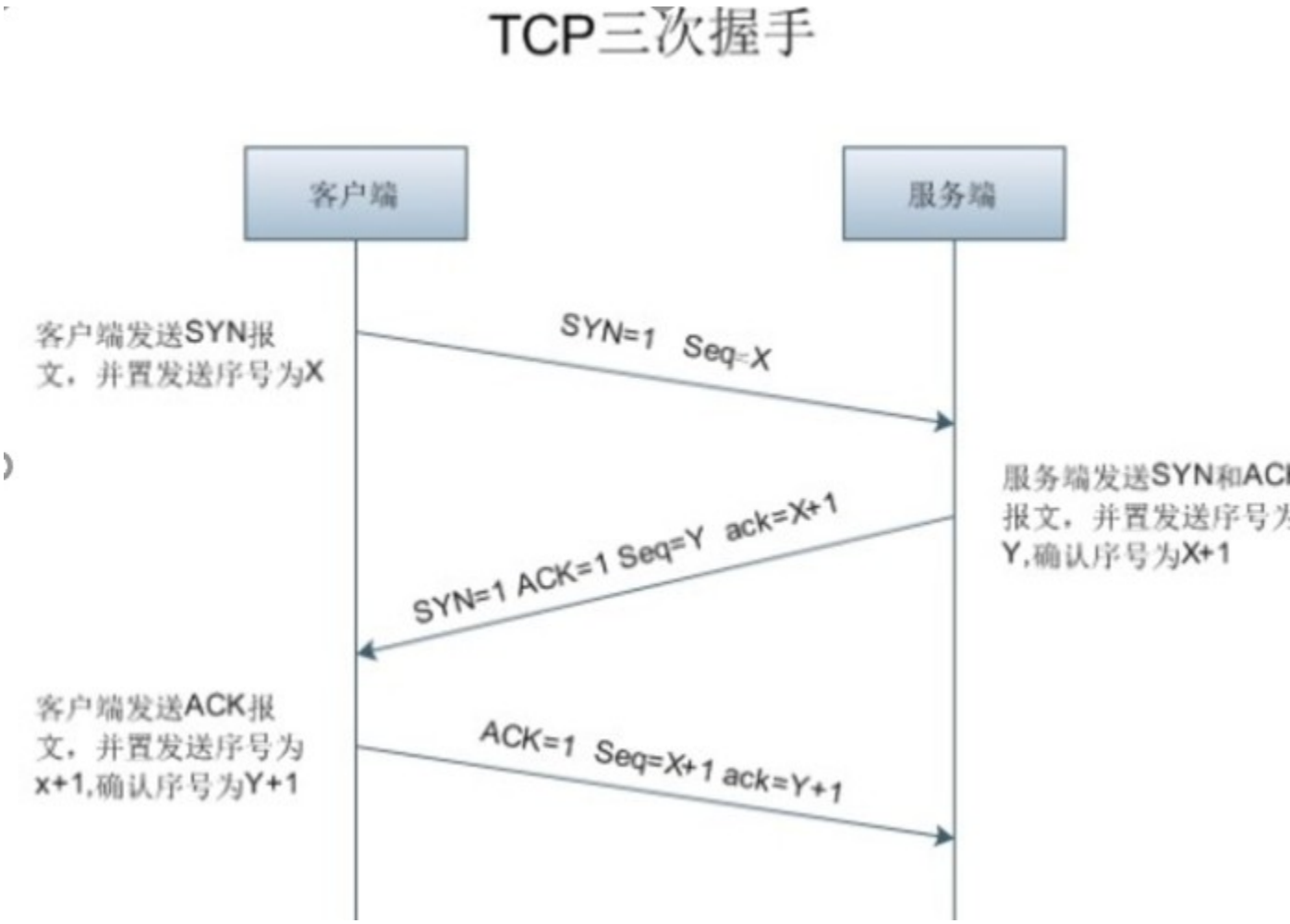
HCRSE112-Security 技术

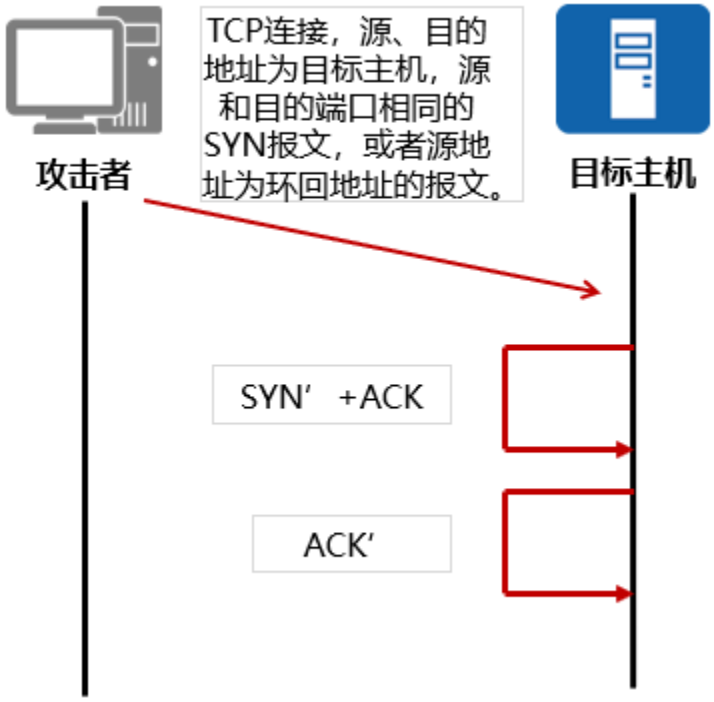


第一次握手
客户端主动发送 SYN=1，随机产生 seq number = x 的数据包到服务器

第二次握手
服务器收到请求后要确认联机信息，向客户端发送 SYN=1，ACK=1，随机产生 seq number= y ，
ack number = 客户端的 seq number +1 （ x+1 ）

第三次握手
客户端收到后检查 ack number 是否正确，即第一次发送的 seq number +1 ,以及位码 ACK 是否为 1，
若正确客户端会再次发送 ack number = y+1　,seq number = x+1，服务端收到后确认 seq number 值与 ACK=1，则连接建立成功。

单包攻击防范举例 - LAND 攻击



单包攻击属于拒绝服务攻击的一种，单包攻击分类：
扫描探测攻击：扫描型攻击是一种潜在的攻击行为，并不具备直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为。如 IP 地址扫描攻击、端口扫描攻击。
畸形报文攻击：畸形报文攻击通常指攻击者发送大量有缺陷的报文，从而造成主机或服务器在处理这类报文时系统崩溃。如 LAND 攻击，Smurf 攻击。
特殊控制报文攻击：特殊控制报文攻击通常使用正常的报文对系统或网络进行攻击，通常会导致系统崩溃、网络中断，或者

用于刺探网络结构。如超大 ICMP 报文攻击、ICMP 不可达报文攻击。

Smurf 攻击是一种病毒攻击，以最初发动这种攻击的程序“Smurf”来命名。这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。

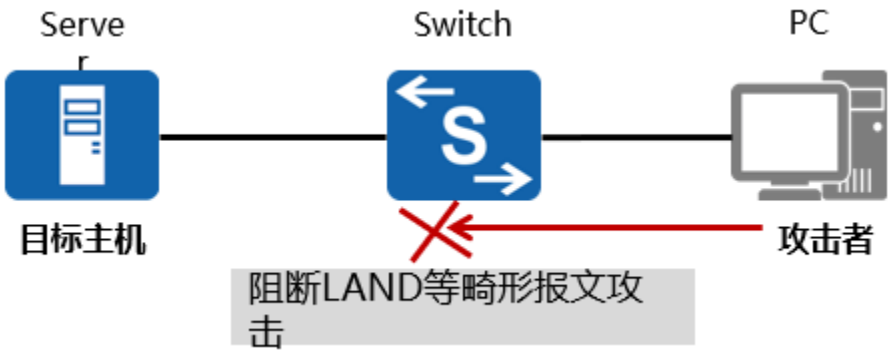
LAND 攻击原理

攻击者利用 TCP 连接三次握手机制中的缺陷，向目标主机发送一个源地址和目的地址均为目标主机、源端口和目的端口相同的 SYN 报文，目标主机接收到该报文后，将创建一个源地址和目的地址均为自己的 TCP 空连接，直至连接超时。在这种攻击方式下，目标主机将会创建大量无用的 TCP 空连接，耗费大量资源，直至设备瘫痪。

LAND 攻击防范原理

攻击者通过向目标设备发送畸形报文，使得目标设备在处理畸形报文时出错、崩溃，给目标设备带来损失。为了避免设备在畸形报文攻击的情况下瘫痪，保证正常的网络服务，需要配置畸形报文攻击防范功能。使能畸形报文攻击防范之后，设备就会对本机进行畸形报文防攻击检测。

启用畸形报文攻击防范后，设备采用检测 TCP SYN 报文的源地址和目的地址的方法来避免 LAND 攻击。如果 TCP SYN 报文中的源地址和目的地址一致，则认为是畸形报文攻击，丢弃该报文。



启用畸形报文攻击防范功能（系统视图）。默认开启
anti-attack abnormal enable

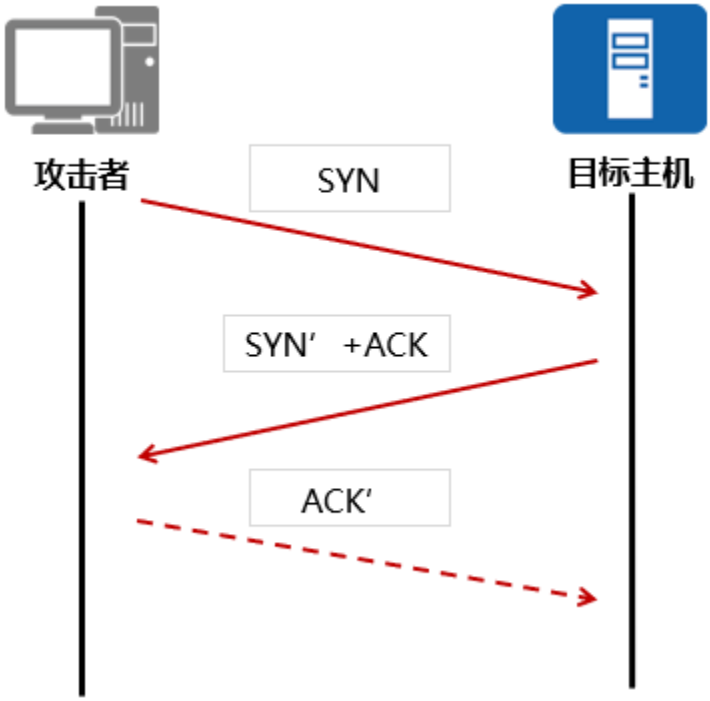
配置完成后，可以查看　dis anti-attack statistics

```
[SW1]dis anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------
AntiAtkType  TotalPacketNum         DropPacketNum
             (H)         (L)        (H)         (L)
-------------------------------------------------------
URPF          0           0          0           0
Abnormal      0           0          0           0
Fragment      0           0          0           0
Tcp-syn       0           0          0           0
Udp-flood     0           0          0           0
Icmp-flood    0           0          0           0
-------------------------------------------------------
```

如果被检测报文是下列 5 种畸形报文之一，报文将会被直接丢弃：
没有 IP 载荷的泛洪
IGMP 空报文
LAND 攻击

Smurf 攻击
TCP 标志位非法攻击

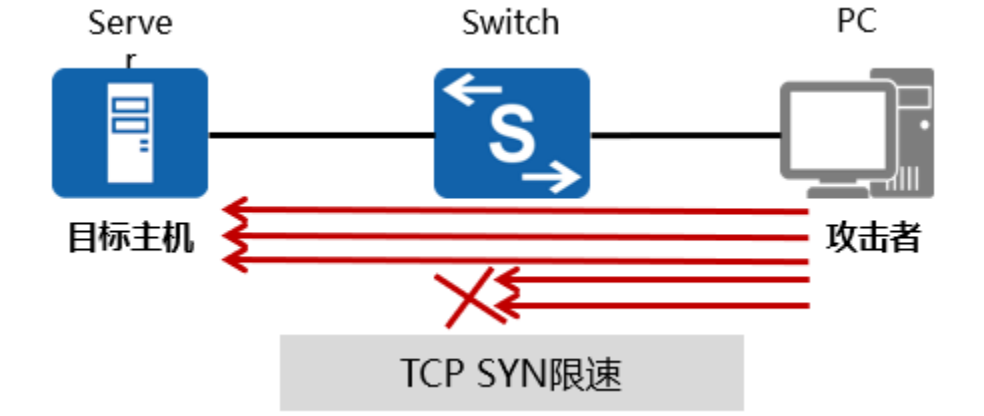
TCP SYN 泛洪攻击



泛洪攻击也是拒绝服务攻击的一种。
TCP SYN 攻击利用了 TCP 三次握手的漏洞。在 TCP 的 3 次握手期间，当接收端收到来自发送端的初始 SYN 报文时，向发送端返回一个 SYN+ACK 报文。接收端在等待发送端的最终 ACK 报文时，该连接一直处于半连接状态。如果接收端最终没有收到 ACK 报文包，则重新发送一个 SYN+ACK 到发送端。如果经过多次重试，发送端始终没有返回 ACK 报文，则接收端关闭会话并从内存中刷新会话。在这段时间内，攻击者可能将数十万个 SYN 报文发送到开放的端口，并且不回应接收端的 SYN+ACK 报文。接收端内存很快就会超过负荷，且无法再接受任何新的连接，并将现有的连接断开。

TCP SYN 泛洪攻击防范原理

启用 TCP SYN 泛洪攻击防范后，设备对 TCP SYN 报文进行速率限制，保证受到攻击时目标主机资源不被耗尽。



启用 TCP SYN 泛洪攻击防范功能（系统视图）。

anti-attack tcp-syn enable

anti-attack tcp-syn car cir 8000

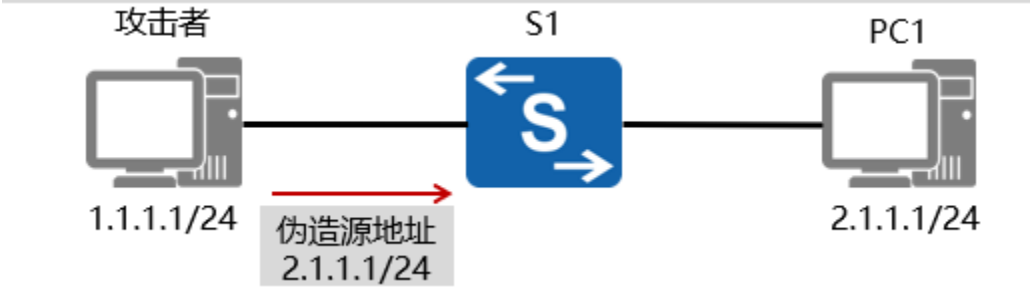
命令用来配置 TCP SYN 泛洪攻击报文的限制速率，缺省情况下，TCP SYN 泛洪攻击报文的限制速率为 155000000bit/s。

URPF 技术

URPF（Unicast Reverse Path Forwarding，单播反向路径转发技术）

源 IP 地址欺骗：网络中经常基于 IP 地址信任主机，而源 IP 地址欺骗就通过伪造源地址获得信任，从而窃取网络信息或破坏系统通信。

防止基于源 IP 地址欺骗的网络攻击行为，主要针对伪造 IP 源地址的 DoS 攻击。



URPF 的两种工作模式：
不但要求在转发表中存在相应表项，还要求接口一定匹配才能通过 URPF 检查时，配置为 strict 模式。
只要在转发表中存在表项就通过 URPF 检查，不要求接口一定匹配时，配置为 loose 模式；
anti-attack urpf strict
anti-attack urpf loose
anti-attack urpf loose allow-default-route acl 2000

使能严格 URPF 检查，同时允许对缺省路由进行特殊处理，并配置 ACL 编号为 2000

严格模式

严格模式下，设备不仅要求报文源地址在 FIB 表中存在相应表项，还要求接口匹配才能通过 URPF 检查。如图所示，在攻击者上伪造源地址为 2.1.1.1 的报文向 S1 发起请求，S1 响应请求时将向真正的“2.1.1.1”即 PC1 发送报文。这种非法报文对 S1 和 PC1 都造成了攻击。如果在 S1 上启用 URPF，则 S1 在收到源地址为 2.1.1.1 的报文时，URPF 检查到以此报文源地址对应的接口与收到该报文的接口不匹配，报文会被丢弃。建议在路由对称的环境下使用 URPF 严格模式，例如两个网络边界设备之间只有一条路径的话，这时，使用严格模式能够最大限度的保证网络的安全性。

松散模式

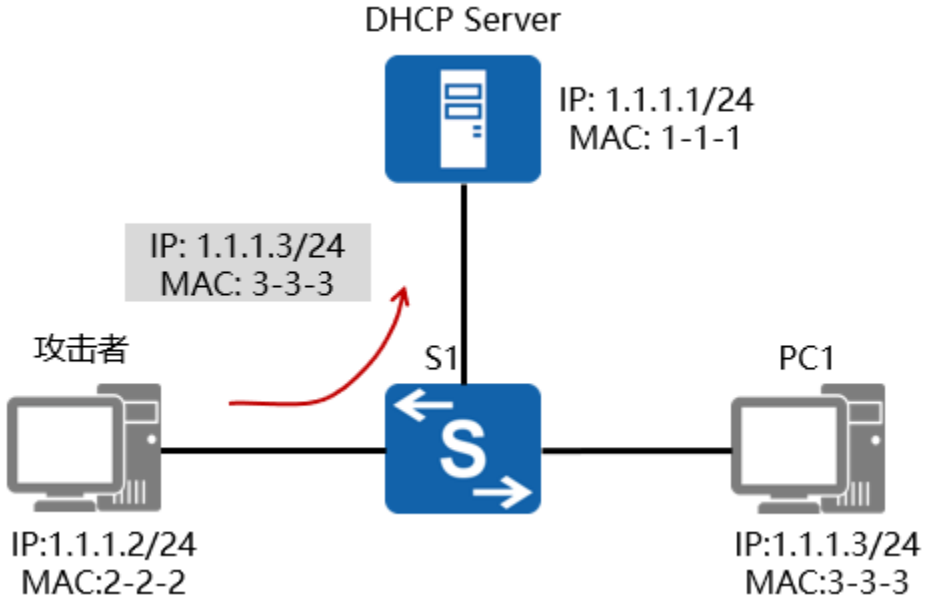
松散模式下，设备不检查接口是否匹配，只要 FIB 表中存在该报文源地址的路由，报文就可以通过。

建议在不能保证路由对称的环境下使用 URPF 的松散模式，例如两个网络边界设备之间如果有多条路径连接的话，路由的对称性就不能保证，在这种情况下，URPF 的松散模式也可以保证较强的安全性。

IPSG（IP Source Guard，IP 源防攻击）

是一种基于二层接口的源 IP 地址过滤技术，它能够防止恶意主机伪造合法主机的 IP 地址来仿冒合法主机，还能确保非授权主机不能通过自己指定 IP 地址的方式来访问网络或攻击网络。

基于绑定表（DHCP 动态和静态绑定表）对 IP 报文进行匹配检查防止源 IP 地址欺骗。



IPSG 基本原理

IPSG 功能是基于绑定表（DHCP 动态和静态绑定表）对 IP 报文进行匹配检查。当设备在转发 IP 报文时，将此 IP 报文中的

源 IP、源 MAC、端口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，表明是合法用户，则允许此报文正常转发，否则认为是攻击报文，并丢弃该 IP 报文。如图所示，在 S1 上配置 IPSG 功能，对进入接口的 IP 报文进行绑定表匹配检查，合法用户发送报文的信息和绑定表一致，允许其通过；攻击者伪造的报文信息和绑定表不一致，S1 将报文丢弃。

绑定表可以通过 DHCP 动态绑定，静态 IP 需要手工进行绑定（user-bind static 命令用来配置静态绑定表）。
交换机操作

```
user-bind static ip-address 192.168.1.1 int g0/0/1
user-bind static   ip-address 192.168.1.2 mac-address aaaa-bbbb-cccc
```

使能 IP 报文检查功能。
配置基于 VLAN 或接口的 IP 报文检查项，该命令只对动态绑定表生效。

```
vlan 1
ip source check user-bind enable
ip source check user-bind check-item mac-address
```

中间人攻击防范 - DAI

动态 ARP 检测 DAI（Dynamic ARP Inspection）
中间人攻击：顾名思义，攻击者位于客户端和服务器中间，对客户端，攻击者假冒为服务器，对服务器，攻击者假冒为客户端。
利用 DHCP Snooping 绑定表来防御中间人攻击的。当设备收到 ARP 报文时，将此 ARP 报文对应的源 IP、源 MAC、VLAN 以及接口信息和 DHCP Snooping 绑定表的信息进行比较，如果信息匹配，说明发送该 ARP 报文的用户是合法用户，允许此用户的 ARP 报文通过，否则就认为是攻击，丢弃该 ARP

报文。

PC1的ARP表项

IP地址	MAC地址	Type
10.1.1.3	3-3-3	Dynamic

ARP表项更新为

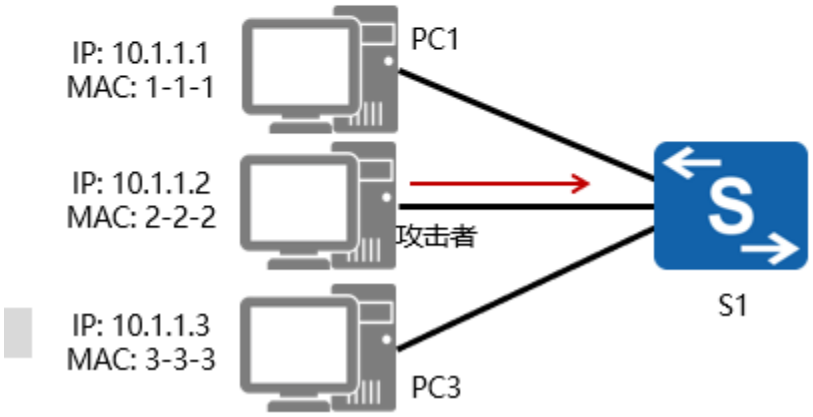
IP地址	MAC地址	Type
10.1.1.3	2-2-2	Dynamic

PC3的ARP表项

IP地址	MAC地址	Type
10.1.1.1	1-1-1	Dynamic

ARP表项更新为

IP地址	MAC地址	Type
10.1.1.1	2-2-2	Dynamic



攻击者主动向 PC1 发送伪造 PC3 的 ARP 报文，导致 PC1 的 ARP 表中记录了错误的 PC3 地址映射关系，攻击者可以轻易获取到 PC1 原本要发往 PC3 的数据；同样，攻击者也可以轻易获取到 PC3 原本要发往 PC1 的数据。这样，PC1 与 PC3 间的信息安全无法得到保障。

为了防御中间人攻击，可以在 S1 上部署动态 ARP 检测功能。当 S1 上部署动态 ARP 检测功能后，如果攻击者连接到 S1 并试图发送伪造的 ARP 报文，S1 会根据 DHCP Snooping 绑定表检测到这种攻击行为，对该 ARP 报文进行丢弃处理。如果 S1 上同时使能了动态 ARP 检测丢弃报文告警功能，则当 ARP 报文因不匹配 DHCP Snooping 绑定表而被丢弃的数量超过了告警阈值时，S1 会发出告警通知管理员。

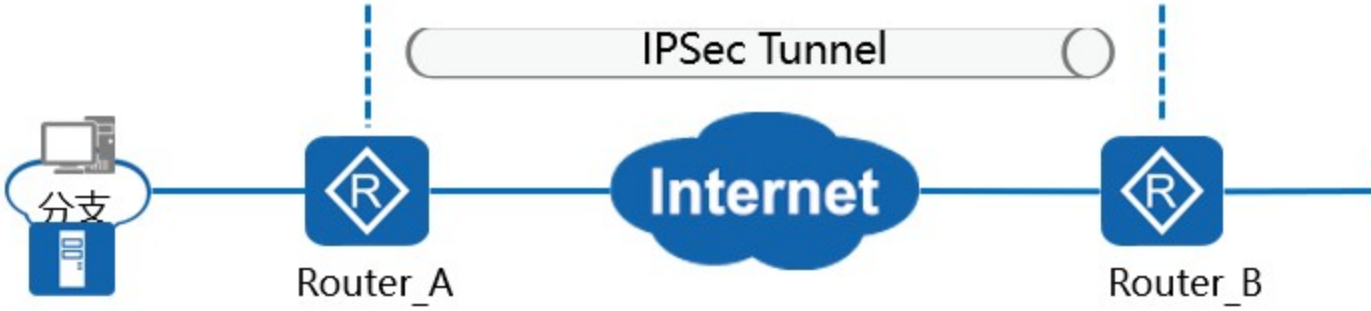
使能接口或 VLAN 下动态 ARP 检测功能，即对 ARP 报文进行

绑定表匹配检查功能。
dhcp enable
dhcp snooping enable
int g0/0/2
dhcp snooping trusted

vlan 1
arp anti-attack check user-bind enable

IPSec VPN

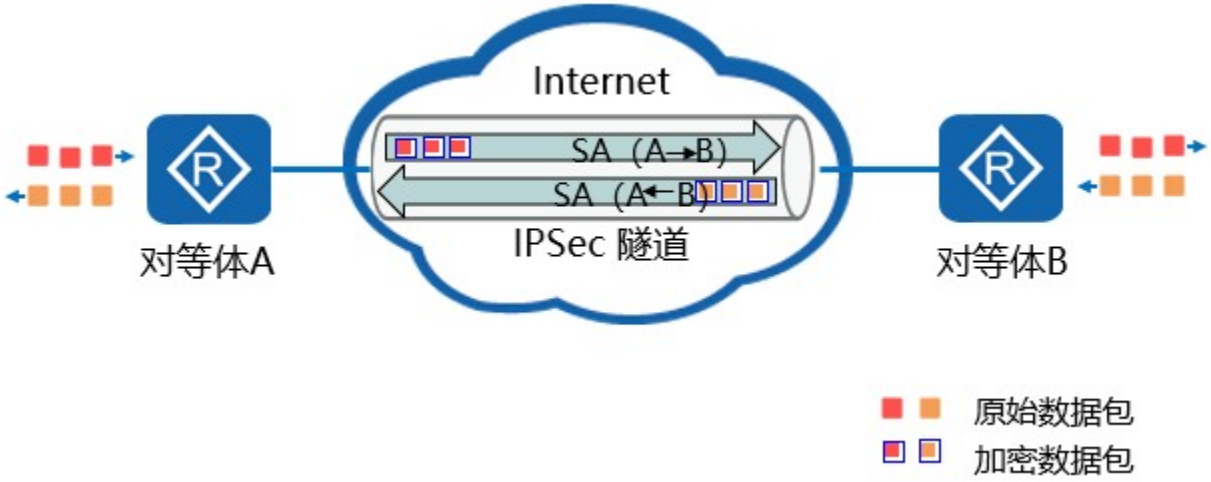
IPSec（Internet 协议安全）是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec 通过在 IPSec 对等体间建立双向安全联盟，形成一个安全互通的 IPSec 隧道，来实现 Internet 上数据的安全传输。
若在网络中部署 IPSec，便可对传输的数据进行加密、完整性校验及源认证等处理，降低信息泄漏的风险。



IPSec 安全传输数据的前提是在 IPSec 对等体（即运行 IPSec 协议的两个端点）之间成功建立安全联盟 SA（Security Association）。SA 是通信的 IPSec 对等体间对某些要素的约定。

SA 是通信的 IPSec 对等体间对某些要素的约定，例如：对等体间使用何种安全协议、需要保护的数据流特征、对等体间传输的数据的封装模式、协议采用的加密算法、验证算法，对等

体间使用何种密钥交换和 IKE 协议，以及 SA 的生存周期等。SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（Security Parameter Index）、目的 IP 地址和使用的安全协议号（AH 或 ESP）。

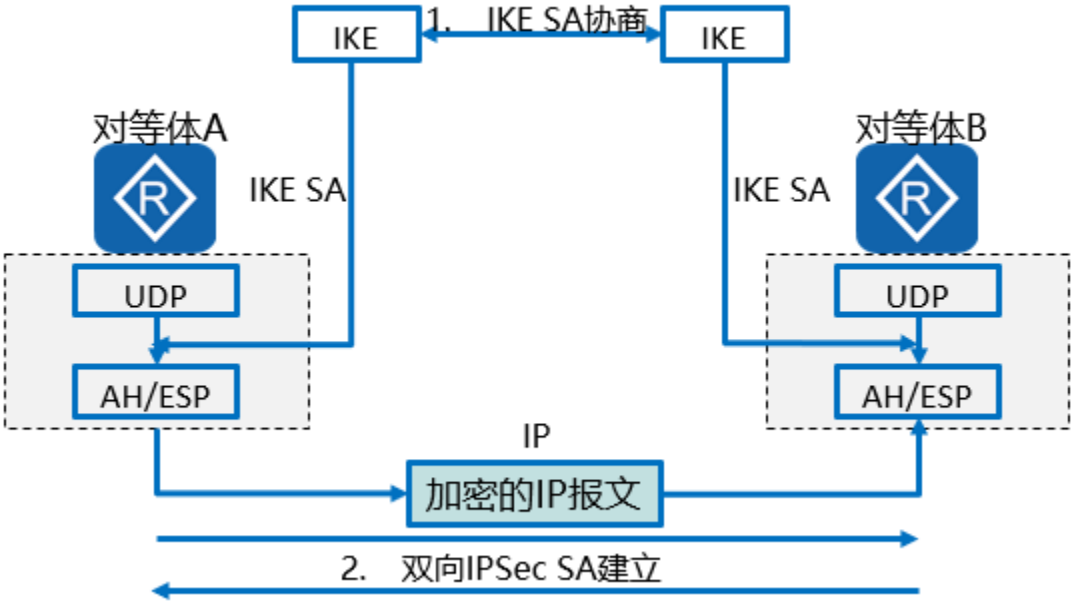


IKE （Internet Key Exchange）因特网密钥交换

IKE SA 是为 IPSec SA 服务的，为 IPSec 提供了自动协商密钥、建立 IPSec 安全联盟的服务。

因特网密钥交换 IKE（Internet Key Exchange）协议建立在 Internet 安全联盟和密钥管理协议 ISAKMP 定义的框架上，是基于 UDP 的应用层协议，可为数据加密提供所需的密钥，能够简化 IPSec 的使用和管理，大大简化了 IPSec 的配置和维护工作。

对等体之间建立一个 IKE SA 完成身份验证和密钥信息交换后，在 IKE SA 的保护下，根据配置的 AH/ESP 安全协议等参数协商出一对 IPSec SA。此后，对等体间的数据将在 IPSec 隧道中加密传输。



IPSec 安全协议

IPSec 通过验证头 AH（Authentication Header）和封装安全载荷 ESP（Encapsulating Security Payload）两个安全协议实现 IP 报文的安全保护。

安全协议	ESP				AH			
加密	DES	3DES	AES	SM1/SM4				
验证	MD5	SHA1	SHA2	SM3	MD5	SHA1	SHA2	SM3
密钥交换	IKE(ISAKMP,DH)							

AH 是报文头验证协议，主要提供数据源验证、数据完整性验证和防报文重放功能，不提供加密功能。

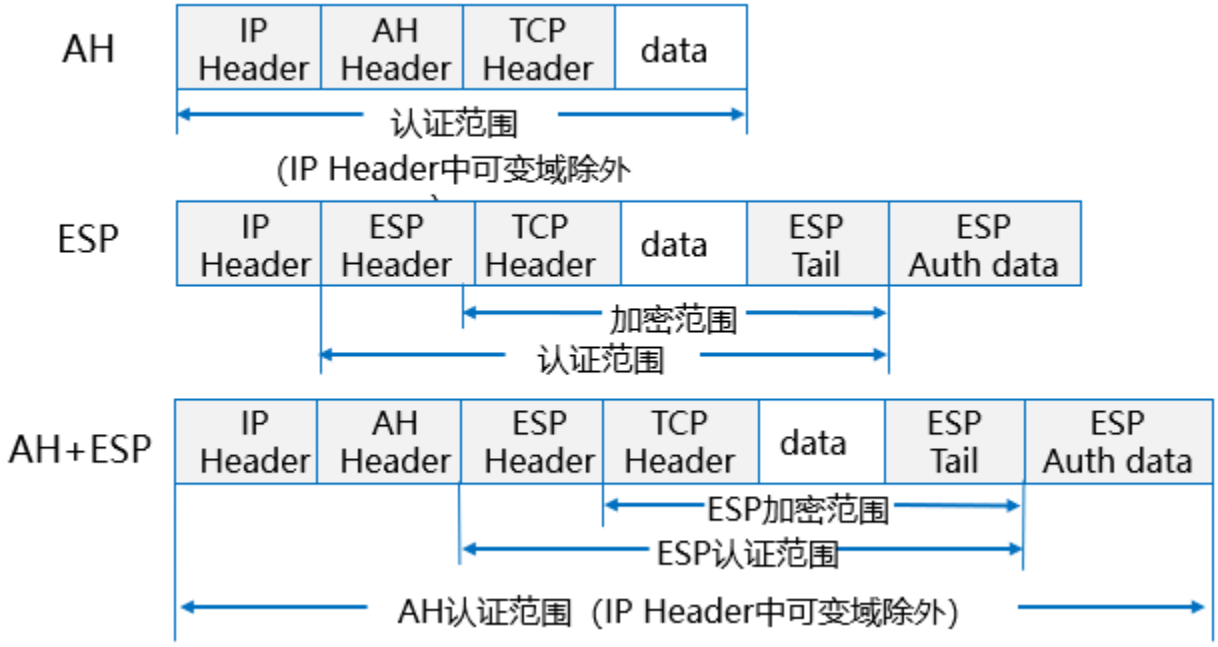
ESP 是封装安全载荷协议，主要提供加密、数据源验证、数据完整性验证和防报文重放功能。

AH 和 ESP 协议提供的安全功能依赖于协议采用的验证、加密算法。

IPSec 加密和验证算法所使用的密钥可以手工配置，也可以通过因特网密钥交换 IKE（Internet Key Exchange）协议动态协商。主要讲解手工方式的 IPSec 隧道建立。

封装模式 - 传输模式

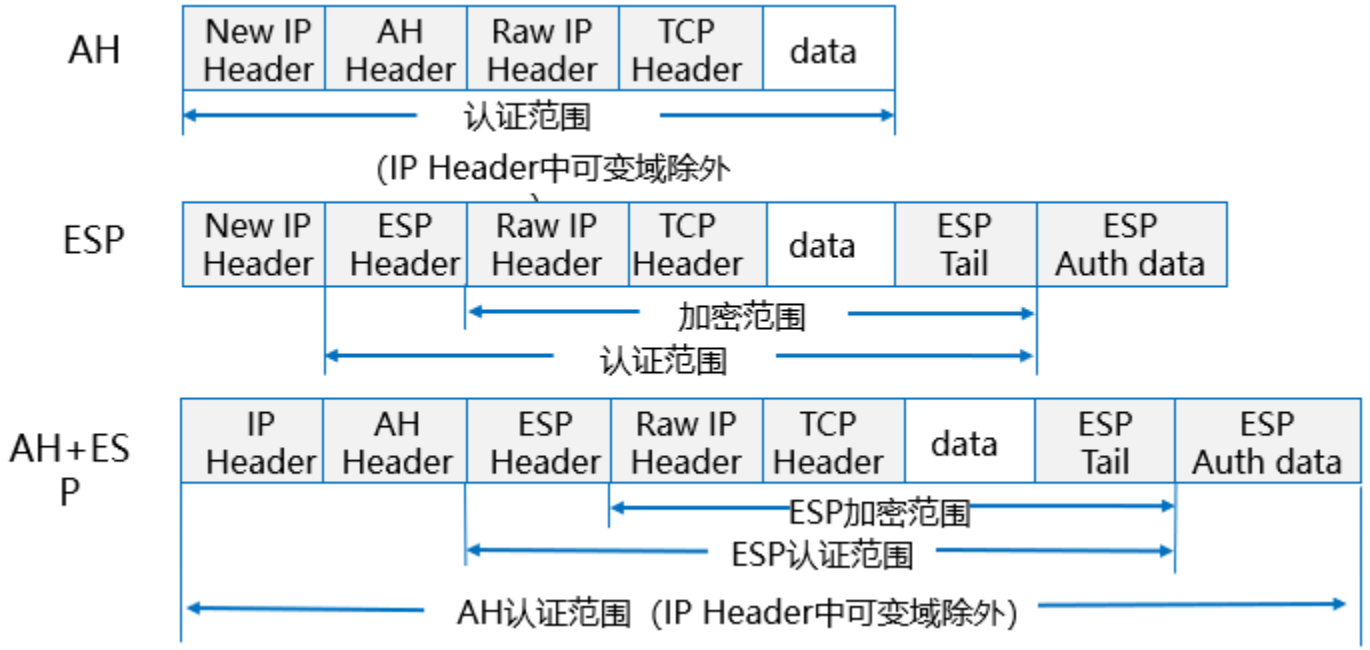
在传输模式中，AH 头或 ESP 头被插入到 IP 头与传输层协议头之间，保护 TCP/UDP/ICMP 负载。



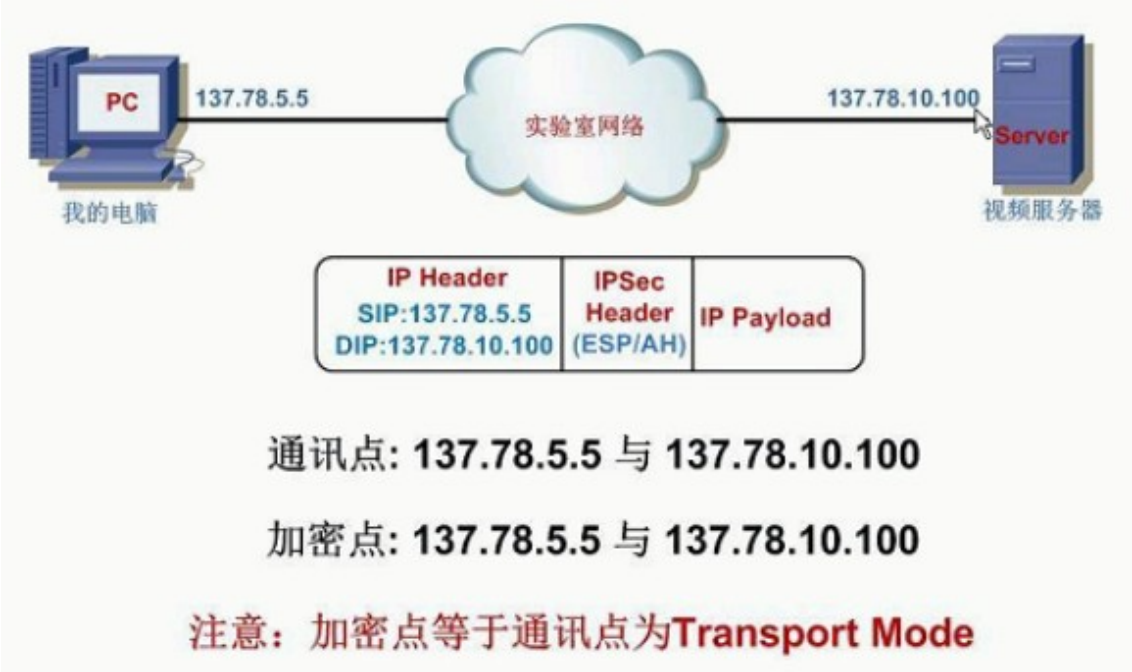
传输模式不改变报文头，故隧道的源和目的地址必须与 IP 报文头中的源和目的地址一致，所以只适合两台主机或一台主机和一台 VPN 网关之间通信。

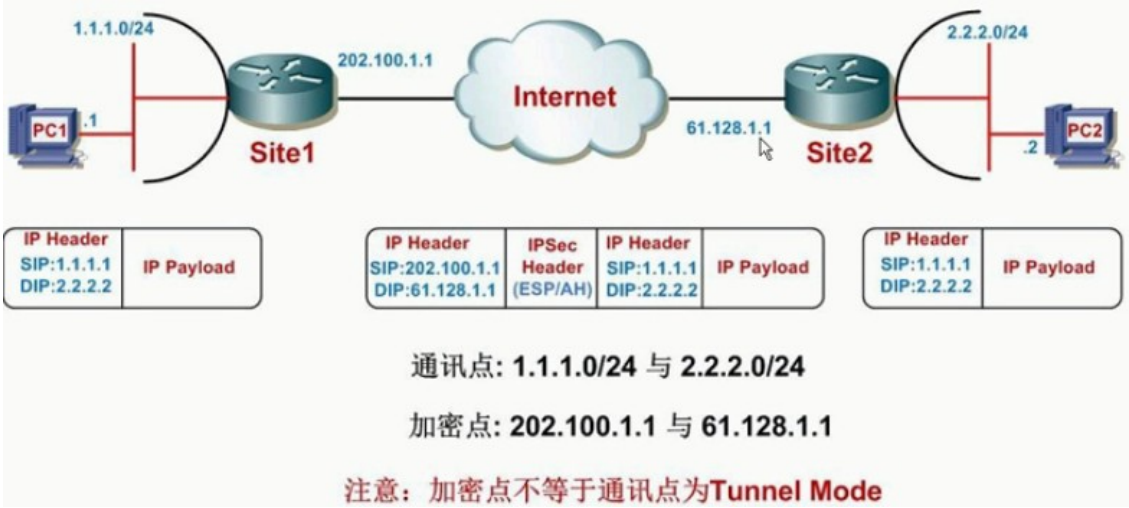
封装模式 - 隧道模式

在隧道模式下，AH 头或 ESP 头被插到原始 IP 头之前，另外生成一个新的报文头放到 AH 头或 ESP 头之前，保护 IP 头和负载。隧道模式主要应用于两台 VPN 网关之间或一台主机与一台 VPN 网关之间的通信。



传输模式和隧道模式的区别在于：





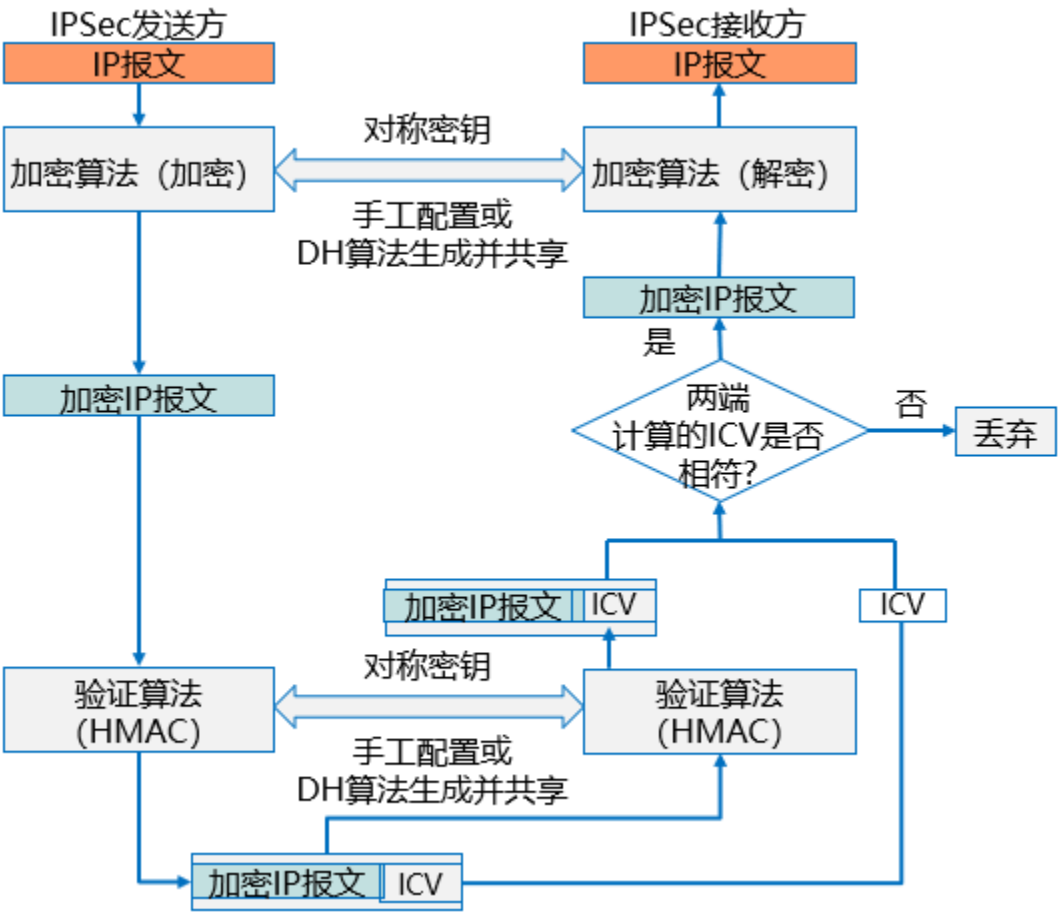
从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密。隧道模式下可以隐藏内部 IP 地址，协议类型和端口。从性能来讲，隧道模式因为有一个额外的 IP 头，所以它将比传输模式占用更多带宽。默认为 tunnel 模式

```
IPSec proposal name: tu
 Encapsulation mode: Tunnel
 Transform                    : esp-new
 ESP protocol               : Authentication
MD5-HMAC-96

Encryption          DES
```

IPSec 加解密及验证过程

IPSec 采用对称加密算法对数据进行加密和解密。



验证指 IP 通信的接收方确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。IPSec 采用 HMAC（Keyed-Hash Message Authentication Code）功能进行验证。HMAC 功能通过比较数字签名进行数据包完整性和真实性验证。

IPSec 使用 AH 协议对数据进行封装时，不具备对数据完整性校验的功能。（　　）

A.T

B.F

以下哪些攻击属于 DoS 攻击？（　　）。

A.畸形报文攻击

B.源 IP 地址欺骗

C.中间人攻击

D.泛洪攻击

- 参考答案：
- B。
- AD。