CEC 中国电子 | MAIPU 迈普

交换机安全技术

课程目标

■熟悉园区网的常见攻击及其带来的影响

■熟练掌握解决园区网攻击的防护方法及其配置应用

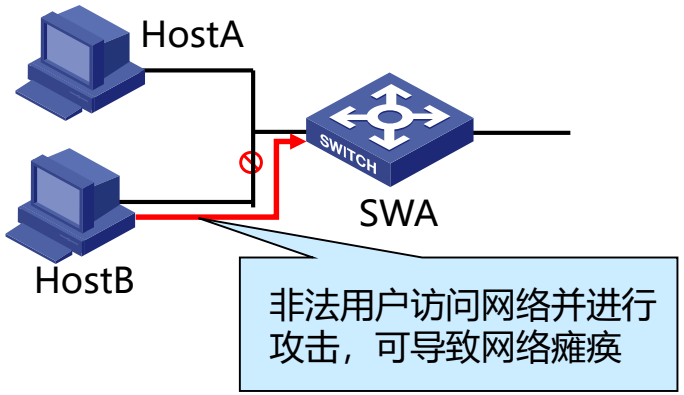
网络安全概念

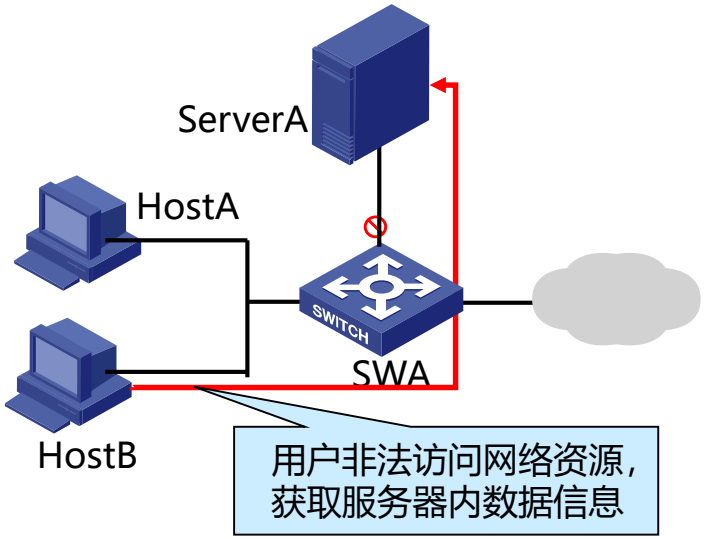
- 两层含义
  - 保证内部局域网的安全
  - 保证内网和外网数据交换的安全
- 关注的内容
  - 保护网络设备、物理线路不会轻易遭受攻击
  - 有效识别合法和非法用户
  - 访问控制、病毒防范等
- 目标
  - 明确要保护什么、明确可能的网络安全威胁、明确可采取的安全防护措施

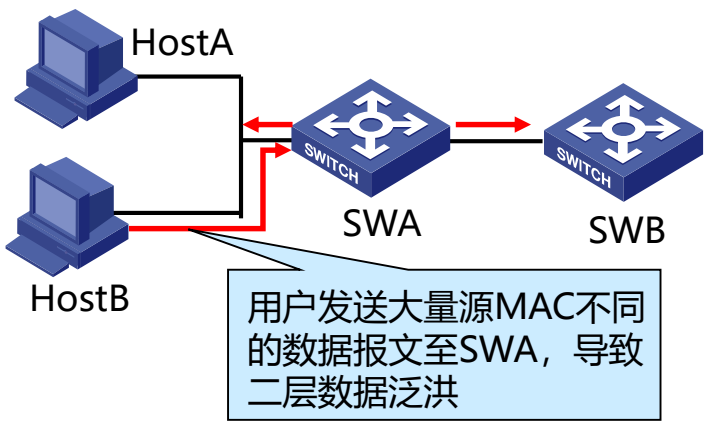
需要保护的资源

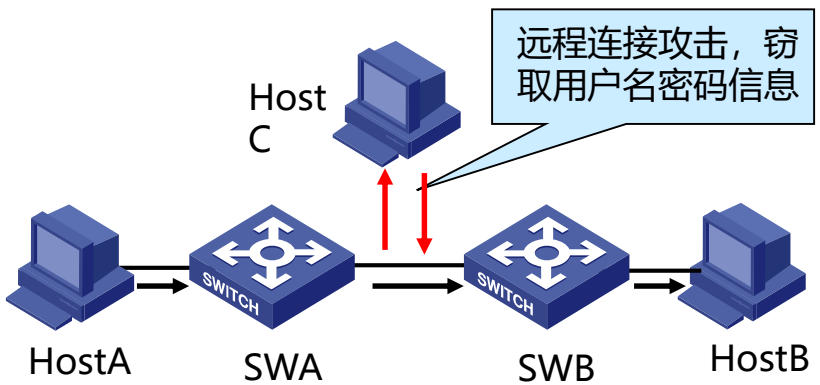
- 网络设备：路由器、交换机
- 运行信息：路由表、MAC地址表
- 带宽资源：带宽、速率
- 网络终端：服务器、用户主机
- 网络数据：IP包
- 用户信息：用户ID、密码等

园区网常见安全威胁


HostA
SWITCH
SWA
HostB
非法用户访问网络并进行攻击，可导致网络瘫痪


ServerA
HostA
SWITCH
SWA
HostB
用户非法访问网络资源，获取服务器内数据信息


HostA
SWITCH
SWITCH
SWA
SWB
HostB
用户发送大量源MAC不同的数据报文至SWA，导致二层数据泛洪

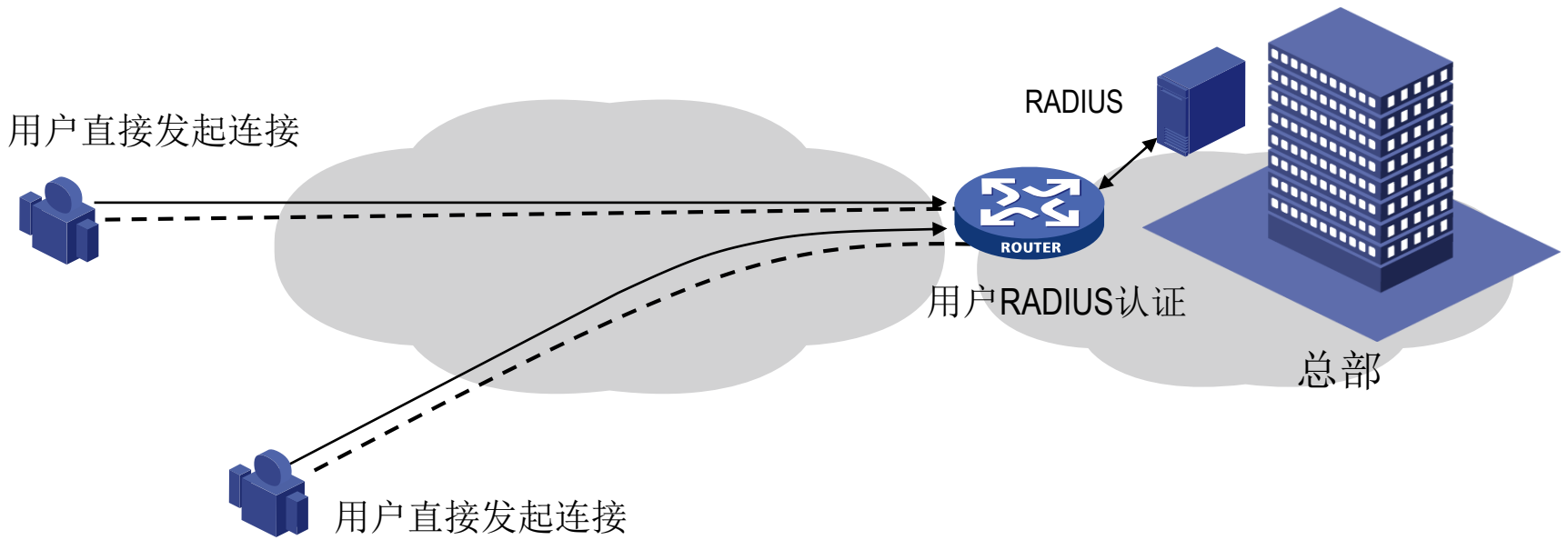

远程连接攻击，窃取用户名密码信息
Host C
SWITCH
SWITCH
HostA
SWA
SWB
HostB

AAA技术概念

- AAA是认证、授权和统计（Authentication, Authorization and Accounting）的简称。
- 它提供了一个用来对这三种安全功能进行配置的一致性框架。AAA的配置实际上是对网络安全的一种管理。
- 这里的网络安全主要指访问控制。包括：
  - ✓哪些用户可以访问网络服务器?
  - ✓具有访问权的用户可以得到哪些服务?
  - ✓如何对正在使用网络资源的用户进行记账?

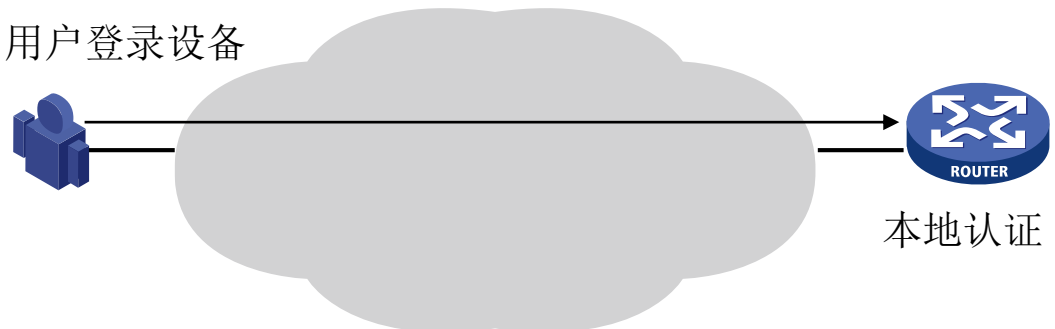
用户接入认证授权

- 用户有着多种接入认证授权方式
  - 本地认证授权
  - RADIUS认证授权
  - CA认证授权

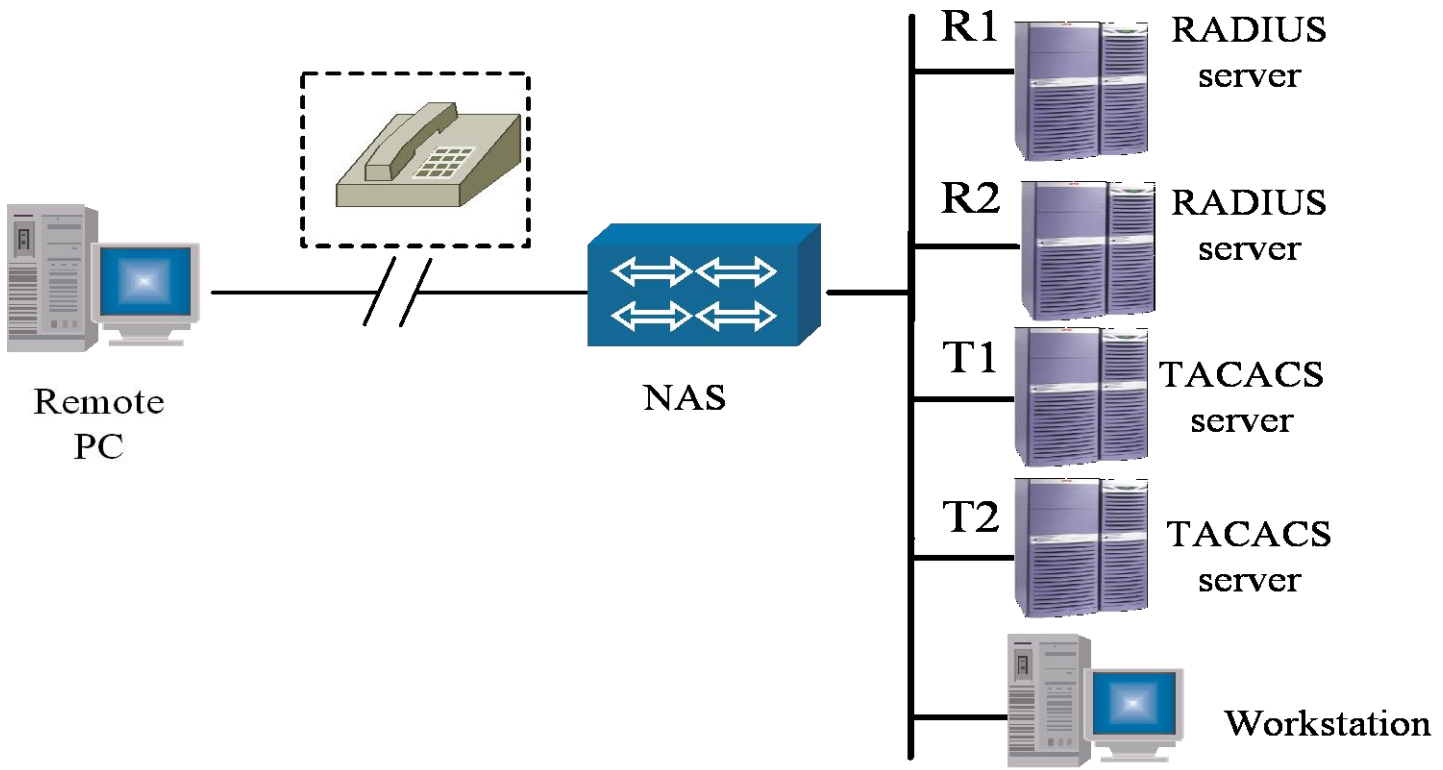


登录设备认证授权

- 登录设备有着多种接入认证授权方式
  - 本地认证授权
  - RADIUS认证授权



AAA基本原理



NAS：网络接入服务器（Network Access Server）。在路由器上启动AAA安全服务作为NAS。当用户想要登录NAS或与 NAS建立连接（比如拨号连接）从而获得访问其他网络的权限时，NAS起到了验证用户的作用

RADIUS：远程身份认证拨入用户服务（Remote Authentication Dial In User Service）

Tacacs：Tacacs是终端访问控制系统（Terminal Access Controller Access Control System）的简称

AAA认证简单设置命令

命令	描述	配置模式
aaa new-model	*启动AAA	config
aaa authentication login	*配置AAA登陆认证	config
aaa authentication enable	*配置进入特权模式认证	config

配置范例

router(config-if)# **aaa new-model**

启动AAA功能

router(config-if)# **aaa authentication login default local**

对登陆用户根据本地用户数据库进行身份认证

default只是一个名字

端口安全介绍

- 端口安全一般应用在接入层。它能够对通过设备访问网络的主机进行限制，允许某些特定的主机访问网络。
- 端口安全功能将用户的MAC地址、IP地址、VLAN ID以及PORT号四个元素灵活绑定，杜绝非法用户接入网络。
- 通过三种规则来限制可以访问网络的主机：
  - ✓ **MAC规则**： MAC绑定，MAC+IP绑定，MAC+VID绑定
  - ✓ **IP规则**：针对某一IP也可以针对一系列IP
  - ✓ **MAX规则**：用以限定端口可以学习到的（按顺序）最多MAC地址数目，这个地址数目不包括MAC规则和IP规则产生的合法MAC地址

端口安全匹配顺序

MAC端口安全的规则依靠终端设备的ARP报文进行触发，当设备接收到ARP报文时，端口安全从中提取各种报文信息，根据匹配结果控制端口的二层转发表，以控制端口对报文的转发行为。并与配置的三种规则进行匹配，依次往下顺序为：

- **匹配MAC规则**
- **匹配IP规则**
- **匹配MAX规则**

端口安全应用实例

实例描述：交换机interface gigabitethernet 0/1接用户网络，要求MAC地址为0005.5de4.0e25的主机任意时刻都允许接入，MAC地址为001f.c627.3823的主机任意时刻不允许被接入，除此之外，该端口最多允许接入100台主机。交换机配置如下：

命令	描述
switch(config)#interface gigabitethernet 0/1	进入端口
switch (config-if-gigabitethernet0/1)#port-security enable	启用端口安全
switch (config-if-gigabitethernet0/1)#port-security permit mac-address 0005.5de4.0e25	允许主机0005.5de4.0e25通信
switch (config-if-gigabitethernet0/1)#port-security deny mac-address 001f.c627.3823	拒绝主机001f.c627.3823通信
switch (config-if-gigabitethernet0/1)#port-security maximum 100	允许100台主机接入
switch (config-if-gigabitethernet0/1)#exit	退出端口

端口安全监控命令

命令	描述
show port-security mac-address [portId]	显示指定端口MAC规则对应登陆的主机信息
show port-security ip-address [portId]	显示指定端口IP规则对应登陆的主机信息。
show port-security active-address [configured |learned|port|link-aggregation]	显示当前所有登陆的主机的信息。

监控命令

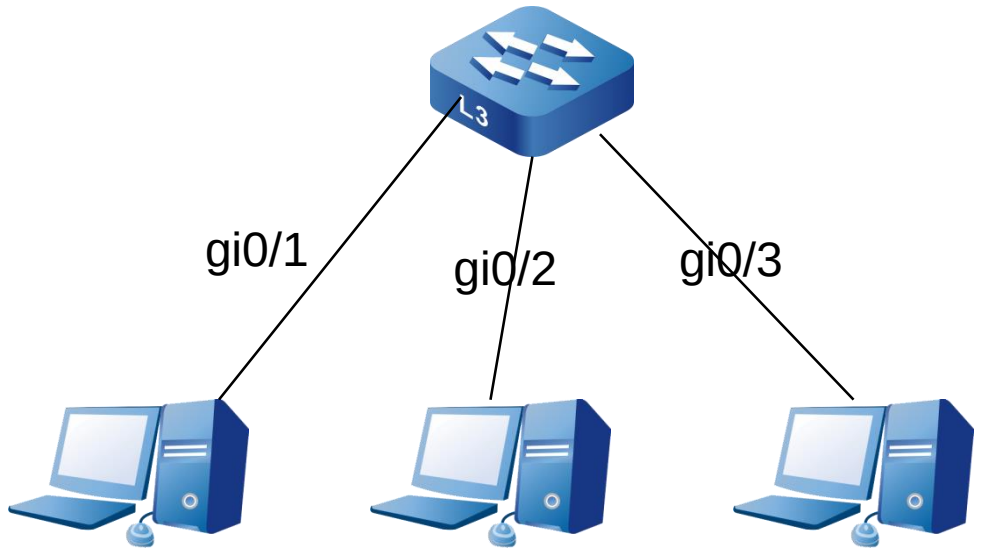
```
switch#show port-security mac-address
-------------------------------------------------------------------------------------
Entry Interface          Action MAC address      VID  IP Addr       ConfigType     description
-------------------------------------------------------------------------------------
1     gi0/1              permit 00:01:7A:00:00:01 ---  ---           MAC            ---
2     gi0/1              permit 00:01:7A:00:00:02 2    ---           MAC+VID        ---
3     gi0/1              permit 00:01:7A:00:00:03 ---  192.168.1.1   MAC+IP         ---
```

端口隔离介绍

- 端口隔离是基于端口的安全特性。用户可以根据需要指定端口的被隔离端口，实现端口和被隔离端口之间二层、三层数据的隔离
- 为了实现同一VLAN中的任意指定端口不能通信，可以在指定端口模式下，配置端口需要被隔离的端口，从而使配置了端口隔离的端口不能与指定的被隔离的端口进行通信。
- 端口隔离特性与端口所属VLAN无关。

端口隔离应用实例

实例描述： switch设备的三个端口分别连接三个终端设备， interface gigabitethernet 0/1 、interface gigabitethernet 0/2和interface gigabitethernet 0/3分别连接终端1，终端2和终端3。并且interface gigabitethernet 0/1 、interface gigabitethernet 0/2和interface gigabitethernet 0/3同属于一个VLAN。现在需要实现终端1不能与终端2和终端3进行通信。可以使用上述命令完成该功能的配置。



端口隔离应用实例

switch配置:

命令	描述
switch(config)#interface gigabitethernet 0/1	进入端口配置模式
switch (config-if-gigabitethernet0/1)#isolate-port interface gigabitethernet 0/2-0/3	配置gi 0/1隔离gi 0/2和gi 0/3
switch (config-if-gigabitethernet0/1)#exit	退出端口配置模式

监控命令

router#show isolate-port

Interface :gigabitethernet0/1

Isolated Interface:gi0/2 gi0/3

描述与分析

Interface：端口名称

Isolate-Interface：被隔离端口的信息

该显示结果表明gi0/1端口隔离了端口gi 0/2和gi 0/3。也就是，经过gi 0/1要到达gi 0/2和gi 0/3的报文将会被丢弃。

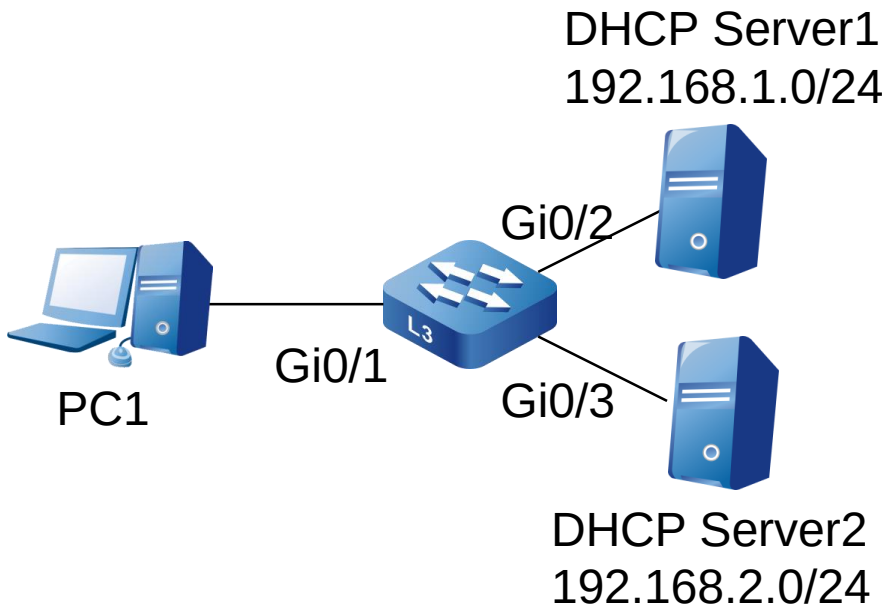
DHCP Snooping

DHCP snooping是DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）的一种安全特性，主要具有如下两种功能：

- 记录DHCP客户端MAC地址与IP地址的对应关系；
- 保证客户端从合法的服务器获取IP地址，实现防私设DHCP服务器功能；

DHCP Snooping应用实例

实例描述： DHCP Server1为合法的DHCP服务器，DHCP Server2为非法的DHCP服务器。现配置DHCP snooping功能，使得PC1只能从DHCP Server1获取地址。



DHCP Snooping应用实例

switch配置:

命令	描述
switch(config)#interface gigabitethernet 0/2	进入端口配置模式
switch (config-if-gigabitethernet0/2)#dhcp-snooping trust	配置gi 0/2口为信任端口
switch (config-if-gigabitethernet0/2)#exit	退出端口配置模式

监控命令

```
switch#show dhcp-snooping database
        dhcp-snooping database:
        database entries count:1
        database entries delete time :300
        --------------------------------
        macAddr          ipAddr          transtion-id     vlan   interface          leaseTime(s)     status
        0013.0100.0002   192.168.1.101    1                2      gi0/1              107990           active
        ------
Total valid DHCP Client binding table for this criterion: 2
```

PC1只能从DHCP Server1获取地址。

CEC中国电子 | MAIPU 迈普

迈普，让网络服务更智能

迈普信息科技集团 迈普通信技术股份有限公司 | 客服电话/400-886-8669 | 网址/www.maipu.com.cn | 微博/weibo.com/maipu

运营中心：北京市北四环西路58号理想国际大厦8层 电话：010-82607185 | 总部基地：成都市高新区九兴大道16号迈普大厦 电话：028-65544888