华为交换机防止同网段ARP欺骗攻击配置案例Linux认证考试
 阻止仿冒网关IP的arp攻击 1.1 二层交换机实现防攻击 1.1.1 配置组网图1二层交换机防ARP攻击组网 S3552P是三层设备，其中IP：100.1.1.1是所有PC的网关，S3552P上的网关MAC地址为000f-e200-3999。PC-B上装有ARP攻击软件。现在需要对S3026_A进行一些特殊配置，目的是过滤掉仿冒网关IP的ARP报文。 1.1.2配置步骤 对于二层交换机如S3026C等支持用户自定义ACL(number为5000到5999)的交换机，可以配置ACL来进行ARP报文过滤。 全局配置ACL禁止所有源IP是网关的ARP报文 aclnum5000 rule0deny0806ffff2464010101ffffffff40 rule1permit0806ffff24000fe2003999ffffffffffff34 其中rule0把整个S3026C_A的端口冒充网关的ARP报文禁掉，其中斜体部分64010101是网关IP地址100.1.1.1的16进制表示形式。Rule1允许通过网关发送的ARP报文，斜体部分为网关的mac地址000f-e200-3999。 注意：配置Rule时的配置顺序，上述配置为先下发后生效的情况。 在S3026C-A系呈油枷路cl规则：[S3026C-A]packet-filteruser-group5000 这样只有S3026C_A上连网关设备才能够发送网关的ARP报文，其它主机都不能发送假冒网关的arp响应报文。 