在一个企业园区网络中，来自企业外部的流量使用防伙墙设备进行防御，但是来自企业内部的攻击与安全隐患也是企业面临的挑战。根据上述网络设计于配置，不考虑来自企业外部的攻击，当前网络是否存在一些网络安全上的隐患?请列举可能存在的网络攻击场景并提供对应的解决方案

1.DHCP server仿冒攻击

在当前网络中存在仿冒的DHCP服务器，该DHCP服务器上存在一些无法正常供内部用户上网的地址段（网络信息），一旦给用户提供了错误的ip地址，会使得用户无法正常访问使用网络服务

解决方案：使用DHCP snooping信任端口技术，只将链接合法DHCP服务器的接口设置成trust端口，其余端口均保持为非信任的untrust端口

只会处理并接收信任端口发来的dhcp offer/ack报文，非信任端口发来的offer/ack丢弃

2.DHCP饿死攻击

因为默认情况下，DHCP服务器只要是收到了用户发来的DHCP discovery报文，就会主动回复offer报文。此时如果网络中存在攻击者，恶意去找网络中的DHCP服务器不断地申请IP地址做使用

场景1：不变更MAC地址，只变更discovery报文中的chaddr字段

因为DHCP服务器默认是根据chaddr字段的变化，从而感知到要为不同设备分配ip地址

如果现在有攻击者在不断的变化这个字段，则对服务器而言，他就会为这些设备不断地给该用户提供ip地址，直到自身地址池耗尽，从而无法对网络中其余的合法设备提供服务

解决方案：开启检查chaddr字段功能，使用DHCP检测chaddr字段和报文的MAC地址是否一致

开启之后，如果发现报文的chaddr字段和报文的MAC地址不一致，丢弃该DHCP报文

场景2：变更MAC地址，也变更discovery报文中的chaddr字段

攻击者不仅变更报文chaddr字段中的MAC地址，还变化报文头部的源MAC地址，这种情况，无法单纯的靠检测CHADDR字段来判断是否存在攻击

解决方案：不止开启检查chaddr字段功能，同时也要开启同一接口下最大学习MAC地址的数量（也可以使用更优一点的端口安全技术中的sticky mac）

3.ARP欺骗攻击（中间人攻击）

企业内网尝发生ARP欺骗攻击，攻击者主动向USER A发送伪造USER B的ARP报文，导致USER A的ARP表中记录了错误的USER B的地址映射关系，攻击者就可以获取到USER A原本要发往给USER B的数据，同样，攻击者也可以获取到USER B原本要发往给USER A的数据，形成中间人攻击

解决方案：动态ARP检测机制，动态ARP检测机制会用到两张表（静态绑定表/DHCP snooping绑定表）（ip-mac-vlan-端口）

4.源IP地址欺骗攻击，攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄密

解决办法：IPSG（IP源防护）针对IP地址欺骗攻击提供防护机制，IPSG利用绑定表（ip-mac-vlan-端口）

当设备试能了ipsg功能之后，在接收到数据包时，就会检查数据包的四要素，如果跟表里一直，认为是合法的报文，具备访问网络的权限，如果不一致，丢弃报文，不具备访问网络的权限。

5.MAC地址泛洪攻击

非法用户不断的变化自身设备的MAC地址，让交换机学习的MAC地址数量不断在增加，直到超出该设备可以容纳的最大MAC地址数量，合法设备的MAC地址无法正常学习到，导致合法设备不具备网络访问权限，其次后续的MAC地址都作为为止单播帧处理（泛洪的方式处理），让其他设备接收到不必要的报文

解决方案：使用端口安全技术，限制每个接口下最大学习MAC地址的数量，同时，可以将合法设备MAC地址通过静态安全MAC跟sticky MAC的方式记录到设备，这样可以保证合法设备正常接入网络又防止非法设备不断变化MAC侵占网络资源

6.WIFI密码暴力破解场景

因为园区内部的WIFI信号是对所有用户公布的，只要尝试测试WIFI密码次数够多，总会试出当前WIFI密码，从而进入到内部无线中，获取信息资源

解决方案：防暴力破解技术，延缓密码泄露的时间。使用了这个技术之后，会对某个wifi信号配置相关操作，比如当ssid在一定的时间内只能被用户试错几次（一分钟只能错误5次），若超出错误次数，则临时将该用户加入到动态黑名单内（最大拉黑时间3600s），在被拉黑的时间内，就算密码测试正确，也提示该用户被锁定，无法登录到网络中。

同时，给园区内密码设置强密码