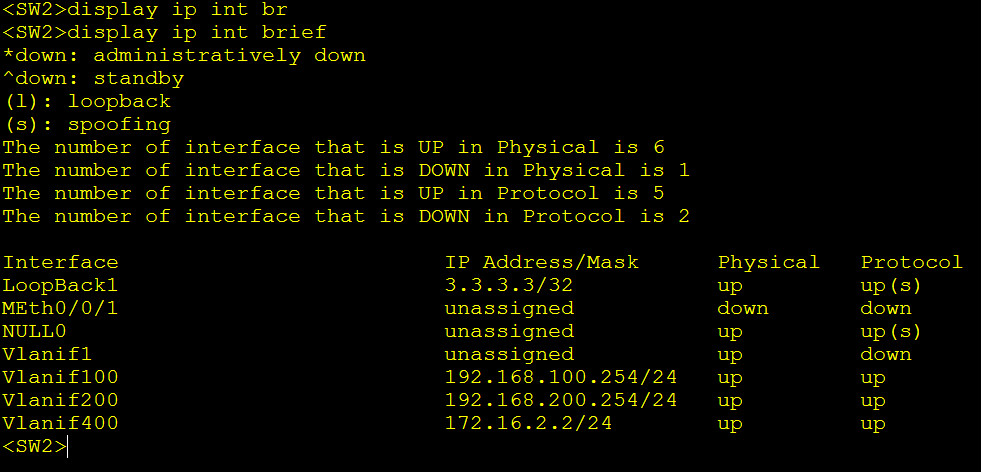
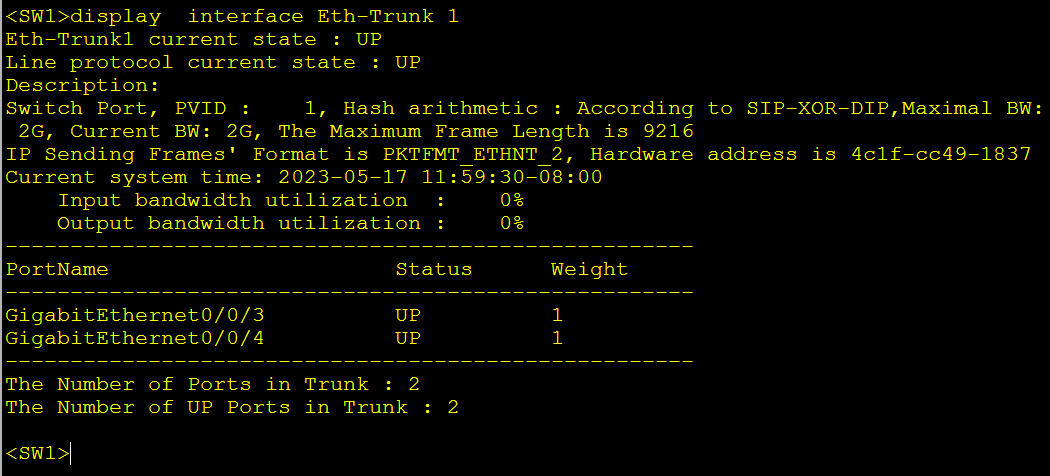
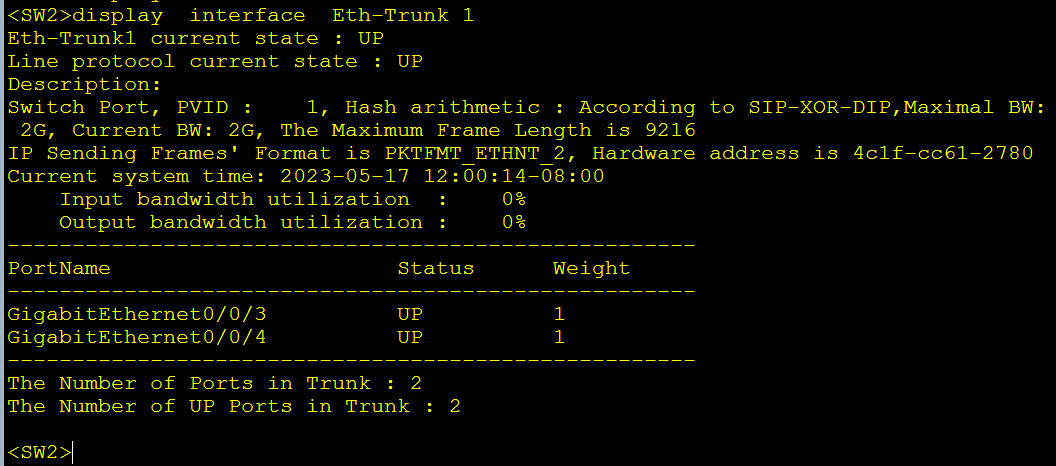
## 一、网络安全防护（28分）

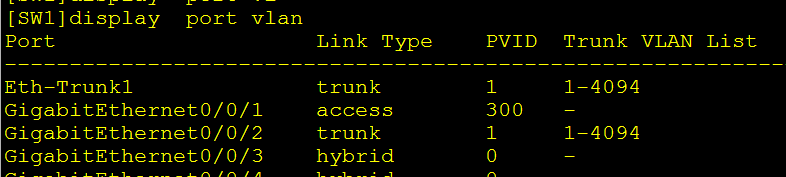
1、根据拓扑图以及预先配置的内容，在SW2上为研发部门配置网关。配置完毕后，对查看交换机SW2的接口IP的输出结果进行截图，将截图粘贴于答题卡的相应位置。（8分）

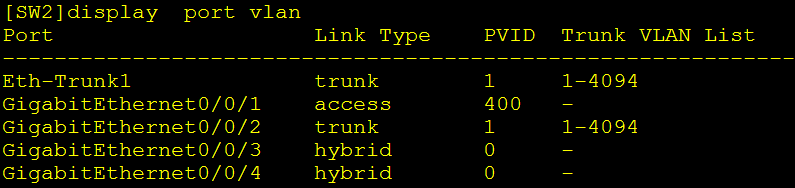


2、根据拓扑图以及预先配置的内容，在汇聚层交换机SW1、SW2上配置链路聚合，聚合组为1，提高链路的带宽，并放行所有的VLAN。配置完毕后，对查看链路聚合状态的输出结果进行截图，将截图粘贴于答题卡的相应位置。（8分）

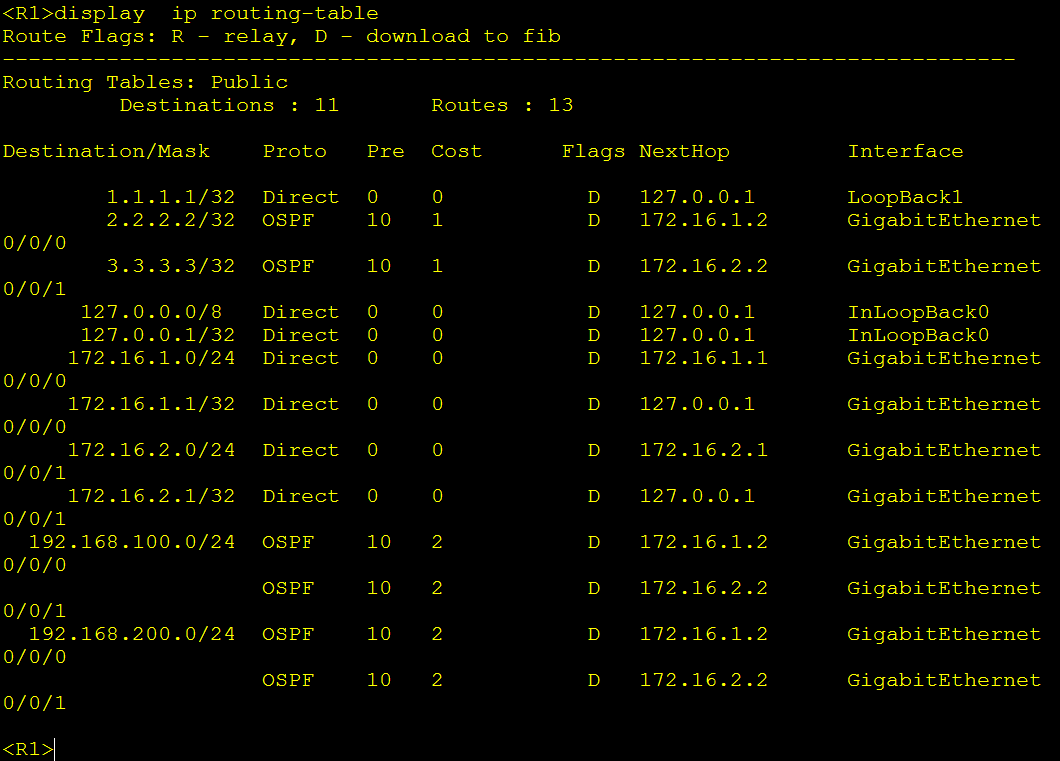




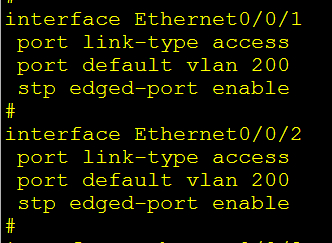




3、根据拓扑图以及预先配置的内容，配置OSPF动态路由协议（OSPF的进程号、接口或链路、区域规划如OSPF规划表所示），实现研发部门区域和服务器区域的互通。配置完毕后，对查看R1的路由表的输出结果进行截图，将截图粘贴于答题卡的相应位置。（10分）



4、考虑到网络的优化，需在SW3、SW4与终端或服务器相连接的接口上，配置STP边缘接口。配置完成后，在交换机SW4上对查看STP 边缘接口的完整命令进行截图，将截图粘贴于答题卡的相应位置。（2分）

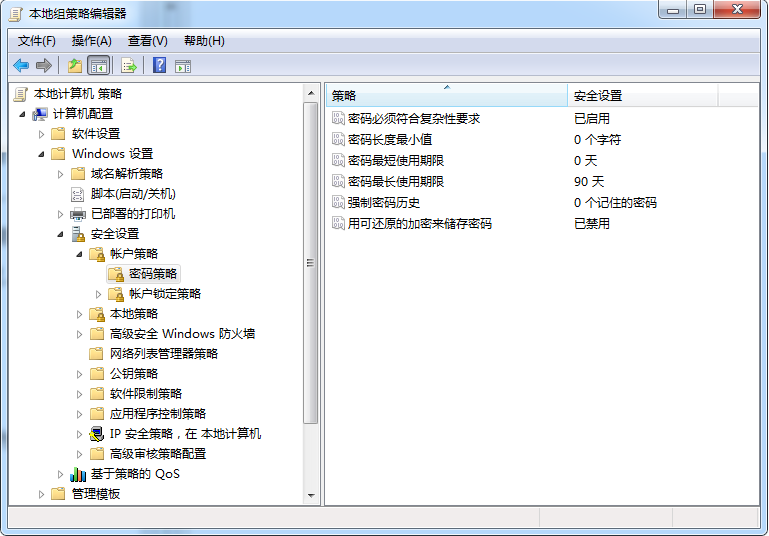


## 二、系统终端防护（16分）

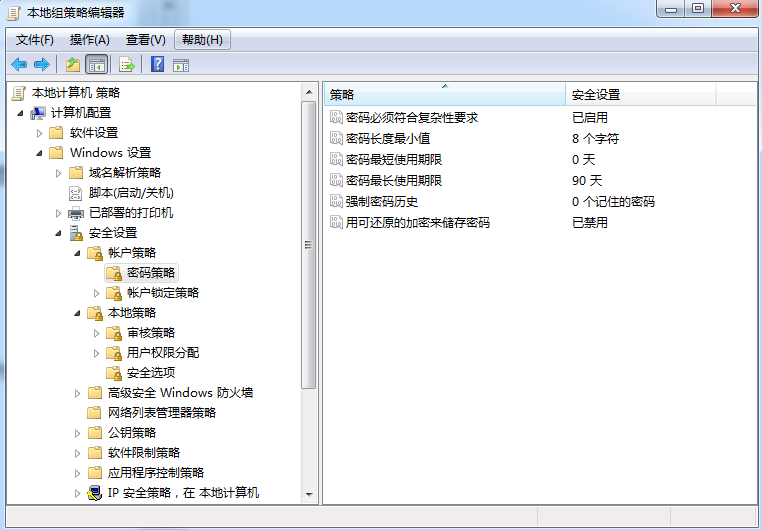
公司网络中的服务器系统存在安全性的问题，您作为网络的安全管理人员需合理配置操作系统安全策略，按照要求完成对操作系统的安全加固。

1、Windows服务器上配置“本地组策略”，要求密码的最长使用期限配置为90天，对关键的配置步骤进行截图，将截图粘贴于答题卡的相应位置。（4分）

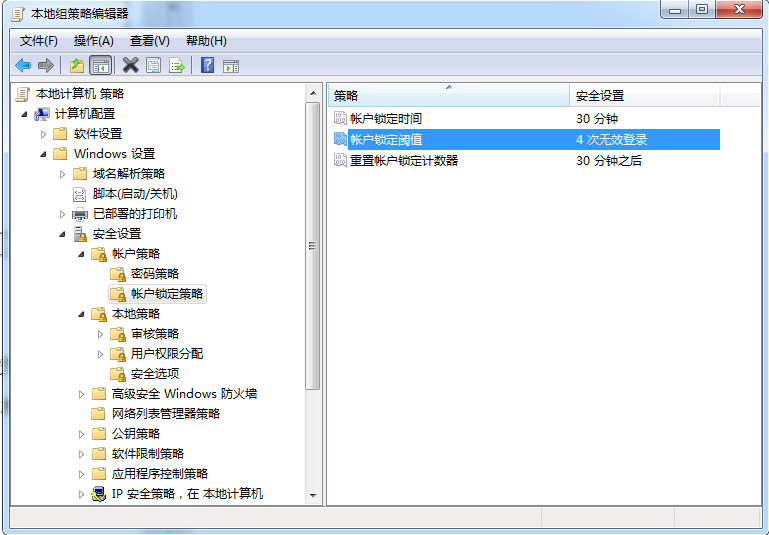
**Gpedit.exe**



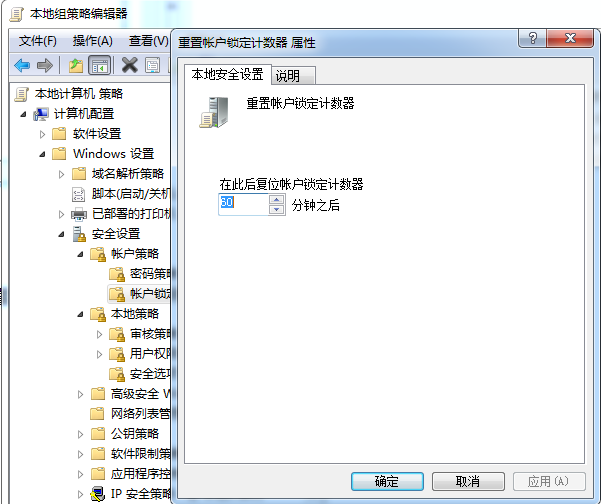
2、Windows服务器上配置“本地组策略”，的长度为8。对关键的配置步骤进行截图，将截图粘贴于答题卡的相应位置。（4分）



3、Windows服务器上配置“本地组策略”，要求用户若尝试登陆次数超过4次则锁定账户。对关键的配置步骤进行截图，将截图粘贴于答题卡的相应位置。（4分）



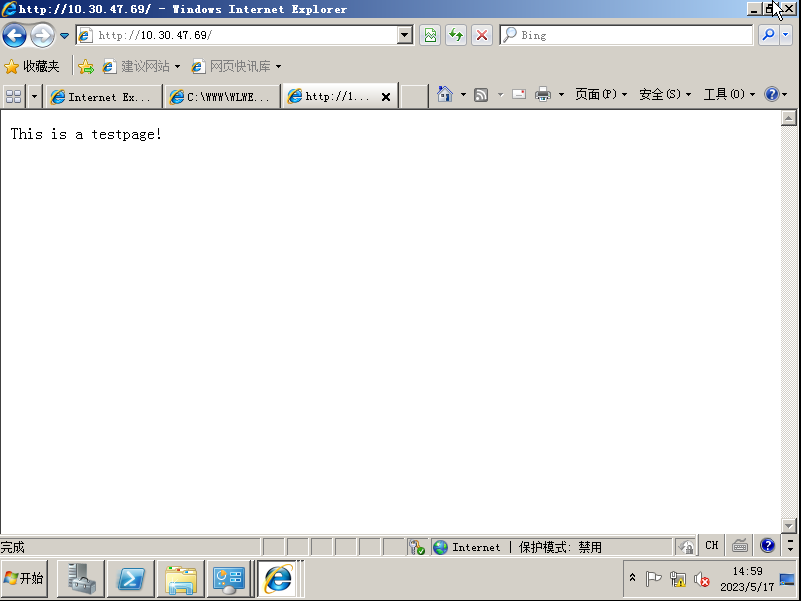
4、Windows服务器上配置“本地组策略”，要求如果账户被锁定，则锁定时间为60分钟。对关键的配置步骤进行，将截图粘贴于答题卡的相应位置。（4分）



## 三、应用服务防护（14分）

公司网络需要架设一台IIS服务器，用于发布WEB服务和FTP服务，您作为网络的安全管理人员需要一同建设公司的服务网络。

1、Windows服务器上发布C:\WWW\WLWEB 目录下的站点，要求通过本地IP地址即可访问到。将访问成功及URL的内容进行截，将截图粘贴于答题卡的相应位置。（4分）

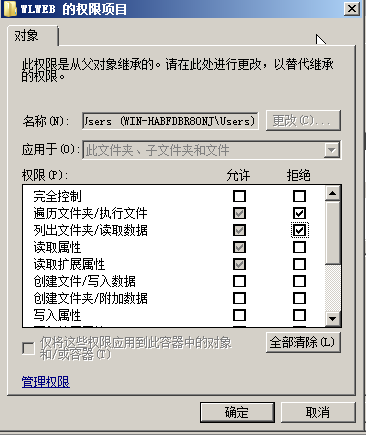


2、Windows服务器上发布FTP功能，目录位置为C:\WWW\WLFTP，要求通过本地IP地址输入账号密码即可登陆，账号密码不做要求。将访问成功的内容进行截图，将截图粘贴于答题卡的相应位置。（4分）

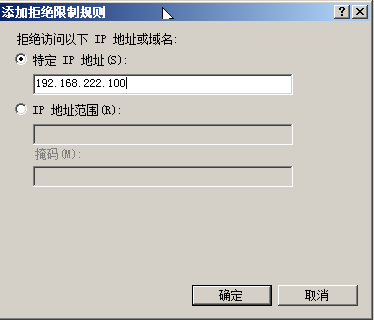
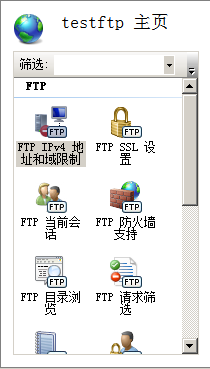


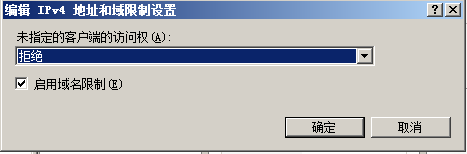
3、Windows服务器上关闭WEB服务的目录浏览功能。将目录浏览功能界面进行截图，将截图粘贴于答题卡的相应位置。（3分）





4、Windows服务器上配置FTP IP地址限制功能，不允许192.168.222.100这个主机地址访问FTP服务。将FTP IP地址和域限制界面进行截图，将截图粘贴于答题卡的相应位置。（3分）

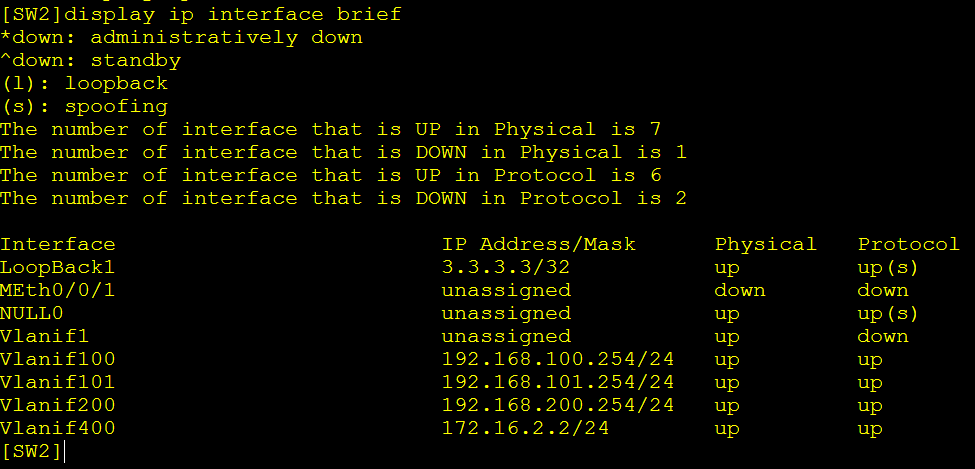




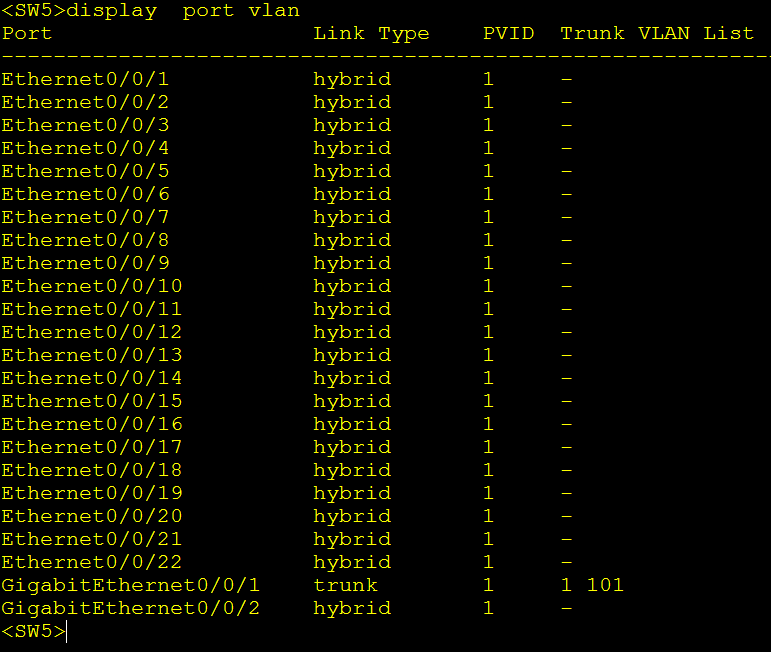
## 四、网络安全管理（12分）

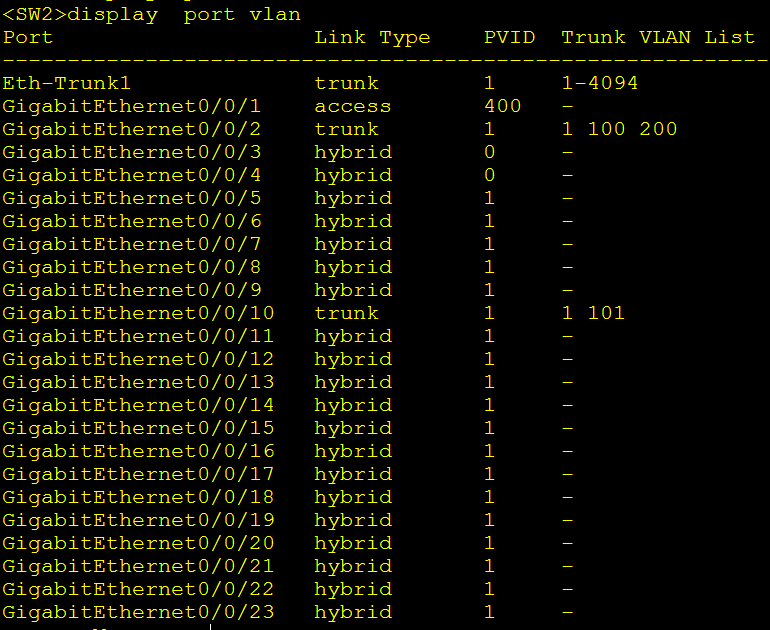
公司重新构造了新的网络结构，现在由于部门扩展的原因需要拓展网络拓扑，具体要求如下。

1、SW2的G0/O/10与一台新的二层交换机（SW5）G0/0/1接口相连，并在二层交换机（SW5）上创建VLAN101用于对研发部门进行拓展，并在SW2上配置VLAN101的管理IP：192.168.101.254。配置完毕后，对查看SW2的接口信息的输出结果进行截图，将截图粘贴于答题卡的相应位置。（2分）

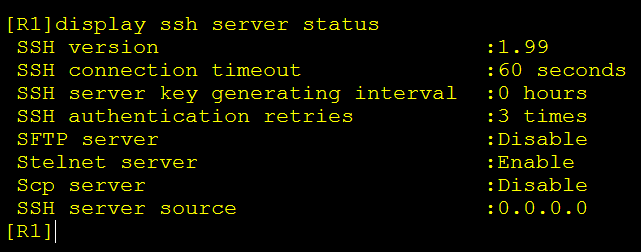


2、给新的二层交换机命名为SW5，并将SW5和SW2相连接的接口配置成中继类型（trunk），仅允许VLAN101通过。配置完毕后，对查看SW5的G0/0/1接口信息的输出结果进行截图，将截图粘贴于答题卡的相应位置。（4分）



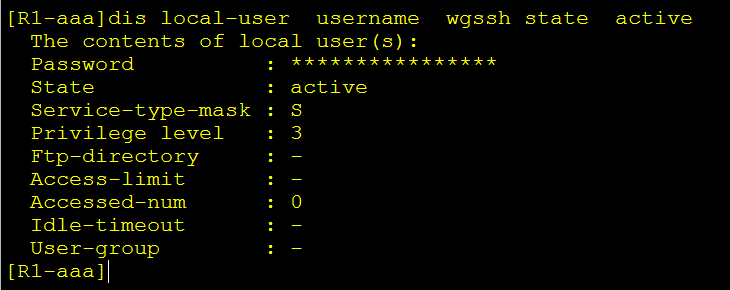


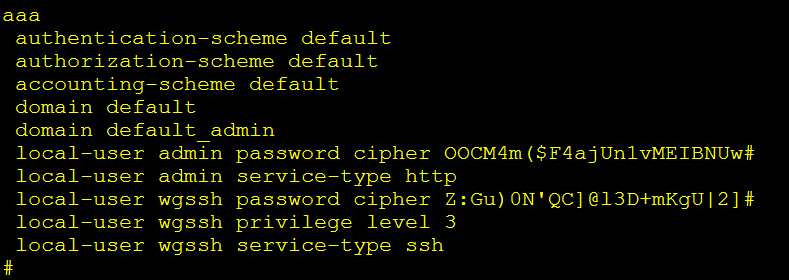
3、为了方便安全管理路由器R1，需要为R1配置SSH协议。配置完毕后，对查看R1的SSH 服务状态的输出结果进行截图，将截图粘贴于答题卡的相应位置。（3分）





4、考虑到设备的安全性，需要为路由器R1创建一个为SSH协议专用的用户，账号为wgssh，密码为wg@2023，权限等级为3。配置完毕后，对查看用户wgssh 的输出结果进行截图，将截图粘贴于答题卡的相应位置。（3分）

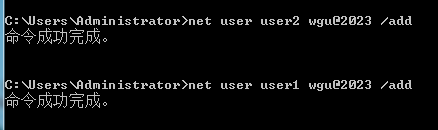




## 五、系统安全管理（18分）

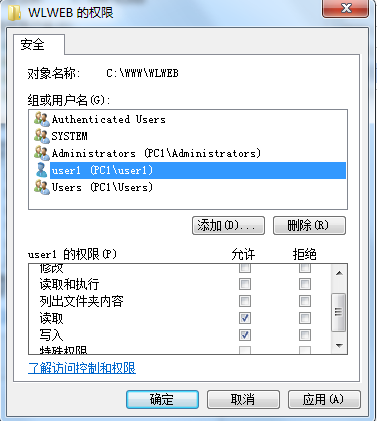
公司网络架设的IIS服务器，现在有不同需求的用户想要访问到该服务器，您作为网络安全的管理人员，需要创建这些用户并且根据用户的需求对目录文件提供访问控制，具体的要求如下。

1、Windows 服务器上通过CMD命令行的方式创建用户user1和user2，密码为wgu@2023。配置完毕后，对CMD执行命令界面截图，将截图粘贴于答题卡的相应位置。（4分）

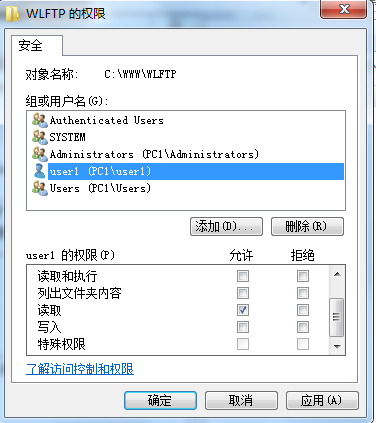




2、Windows服务器上要求user1 对C:\WWW\WLWEB文件夹有读取和写入的权限。配置完毕后，对该文件夹的权限属性进行截图，将截图粘贴于答题卡的相应位置。（4分）

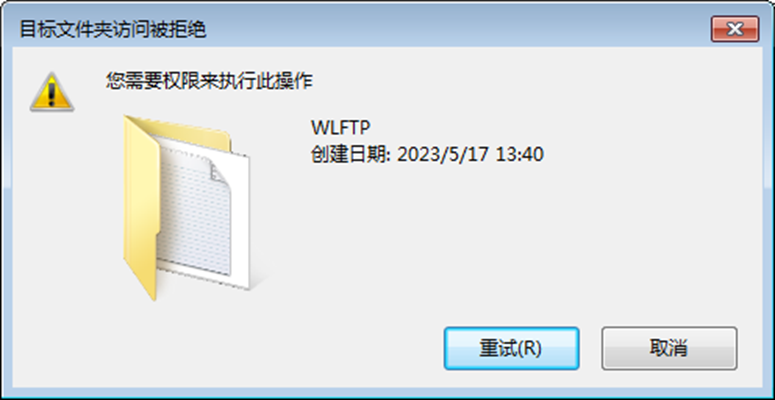


3、Windows服务器上要求user1 对C:\WWW\WLFTP文件夹只有读取权限。配置完毕后，对该文件夹的权限属性进行截图，将截图粘贴于答题卡的相应位置。（4分）



4、Windows服务器上要求user2 对C:\WWW\WLFTP 文件夹只能列出文件夹中的文件，其它所有的权限的类型都为拒绝。配置完毕后，使用user2 账号访问该文件夹目录下的“wlftp test”文件，对访问的结果进行截图，将截图粘贴于答题卡的相应位置。（6分）。

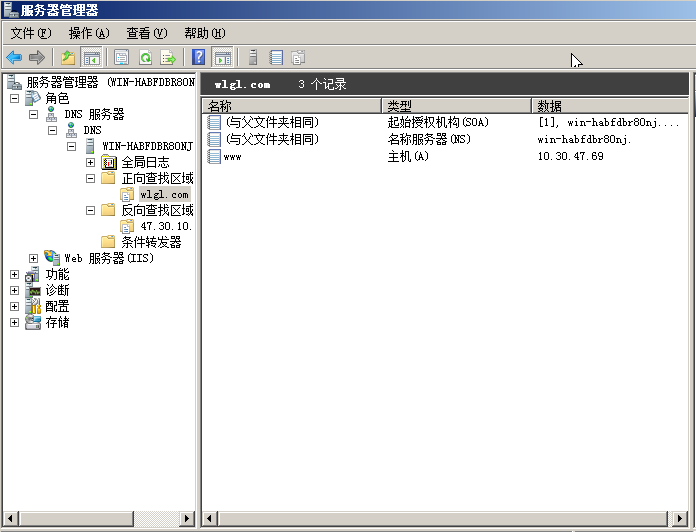




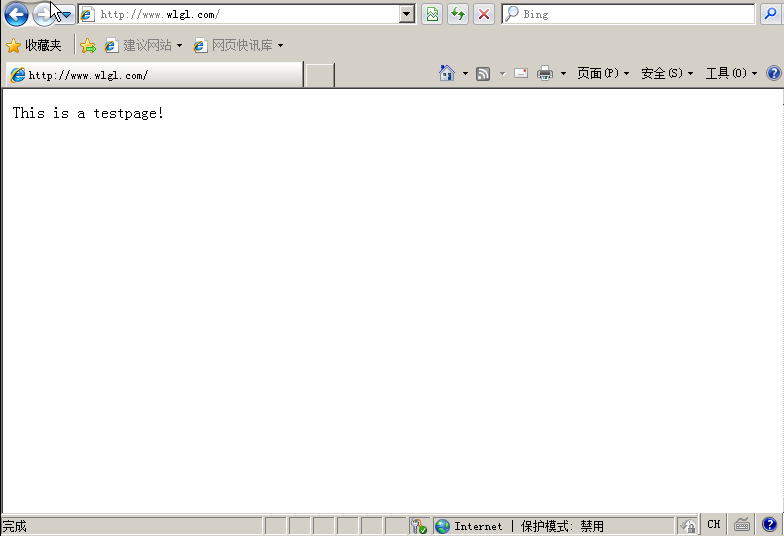
## 六、应用安全管理（12分）

公司期望使用域名的方式来访问到WEB应用服务器，您作为网络的安全管理人员需要一同参与DNS服务器的搭建工作，正确的配置和管理DNS域名，具体的需求如下。

1、Windows 服务器通过“服务器管理器”安装DNS服务，要求能通过www.wlgl.com 地址访问到应用防护模块中搭建的WEB应用服务器。配置完毕后，对DNS服务的正向区域的内容进行截图，将截图粘贴于答题卡的相应位置。（6分）



2、Windows服务器上使用浏览器访问http:\\www.wlgl.com，将浏览器访问结果整屏截图，将截图粘贴于答题卡的相应位置。（6分）



注意事项：

1、本机的DNS填写：本DNS服务器的IP；

2、