**实验一 Paramiko实现SSH登录并配置设备实验**

**班级\_\_云计算2304\_\_\_\_\_\_\_ 学生姓名\_\_梁佳莉\_\_\_\_\_\_\_ 学号\_230502115\_\_\_\_\_\_\_**

**一、实验目的**

**1、掌握SSH服务配置原理**

熟悉华为交换机SSH服务配置流程，理解口令认证与密钥认证的区别及适用场景。

2、**理解网络设备远程安全管理机制**

通过SSH协议实现加密远程登录，分析其对明文传输（如Telnet）的安全改进。

3、**提升网络设备运维技能**

掌握交换机基础配置、用户管理、SSH服务调试及连通性测试方法。

4、**增强网络安全防护意识**

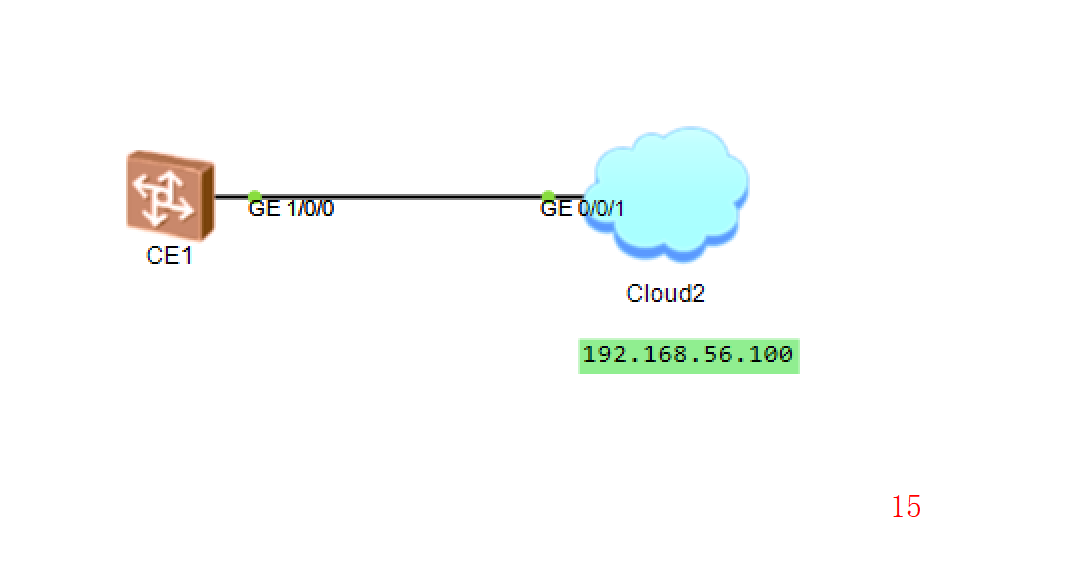
认识弱密码风险，学习密钥认证的高安全性实践，培养安全运维习惯。

**二、实验内容**

**1、实验环境准备**

* **设备**：
  + 交换机：华为CE12800（管理IP: 192.168.56.100/24）
  + 主机：Windows 10（虚拟网卡IP: 192.168.56.1）
* **工具**：
  + 华为eNSP模拟器（搭建拓扑）
  + OpenSSH（生成密钥对）
* **网络要求**：主机与交换机通过Cloud1虚拟网卡互联（拓扑参照实验手册），使用ping 192.168.56.100验证连通性。

**实验拓扑图截图**：（标注学号末两位）



**2、 交换机基础配置**

（1）配置管理IP与端口：

system-view

sysname CE1

interface vlanif 1

ip address 192.168.56.100 24

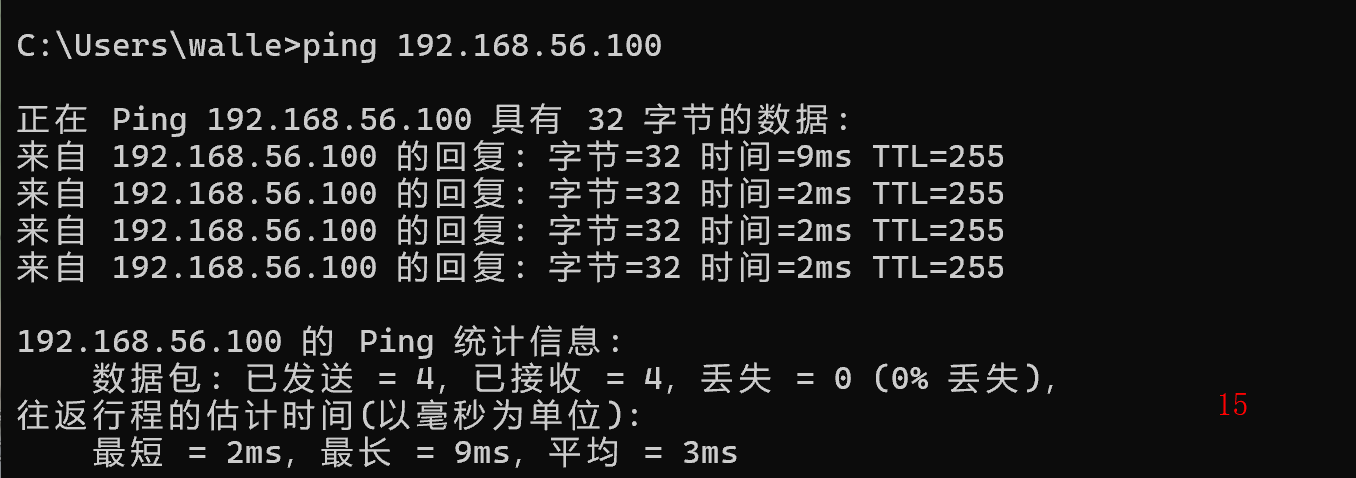
quit

interface GE1/0/0

undo shutdown

（2）结果验证：

主机执行 ping 192.168.56.100 测试连通性。  
**Ping测试截图**：（标注学号末两位）



**3、配置SSH服务与用户**

（1）启用SSH服务并创建用户：

stelnet server enable

user-interface vty 0 4

authentication-mode aaa

protocol inbound ssh

quit

aaa

local-user python password irreversible-cipher Huawei12*#$*

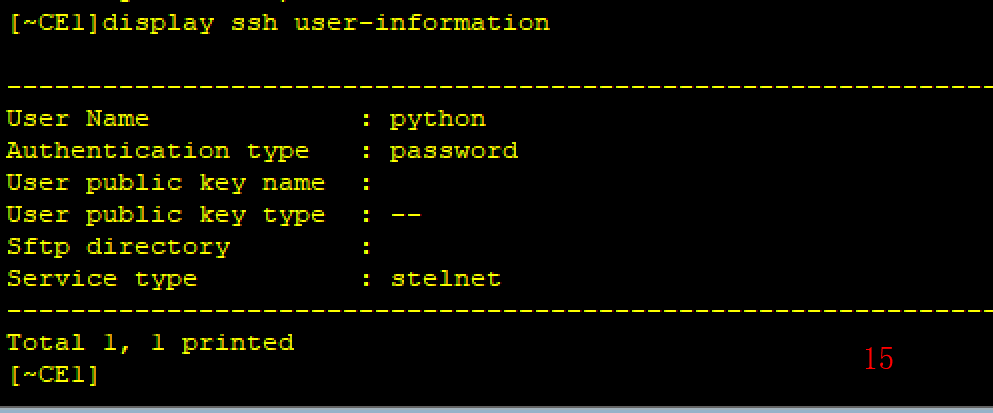
local-user python service-type ssh

local-user python user-group manage-ug

quit

（2）结果验证：执行 display ssh user-information 查看用户配置。

**用户配置截图**：（标注学号末两位）



**4. SSH口令认证测试**

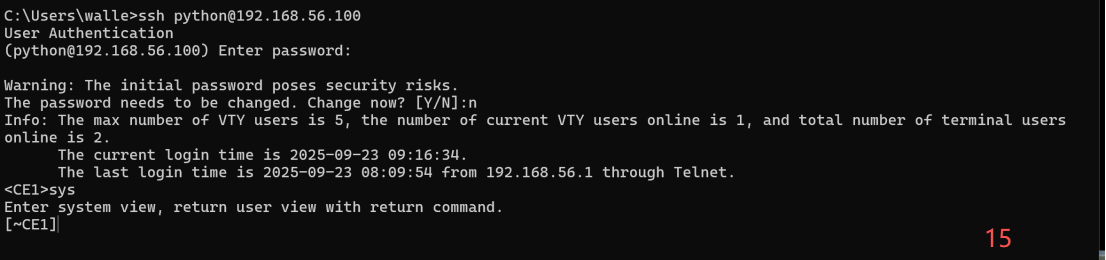
（1）设置认证类型为口令：

ssh user python authentication-type password

ssh user python service-type stelnet

（2）登录测试：主机cmd命令行执行 ssh python@192.168.56.100，输入密码 Huawei12#$

**登录成功界面截图**：（标注学号末两位）

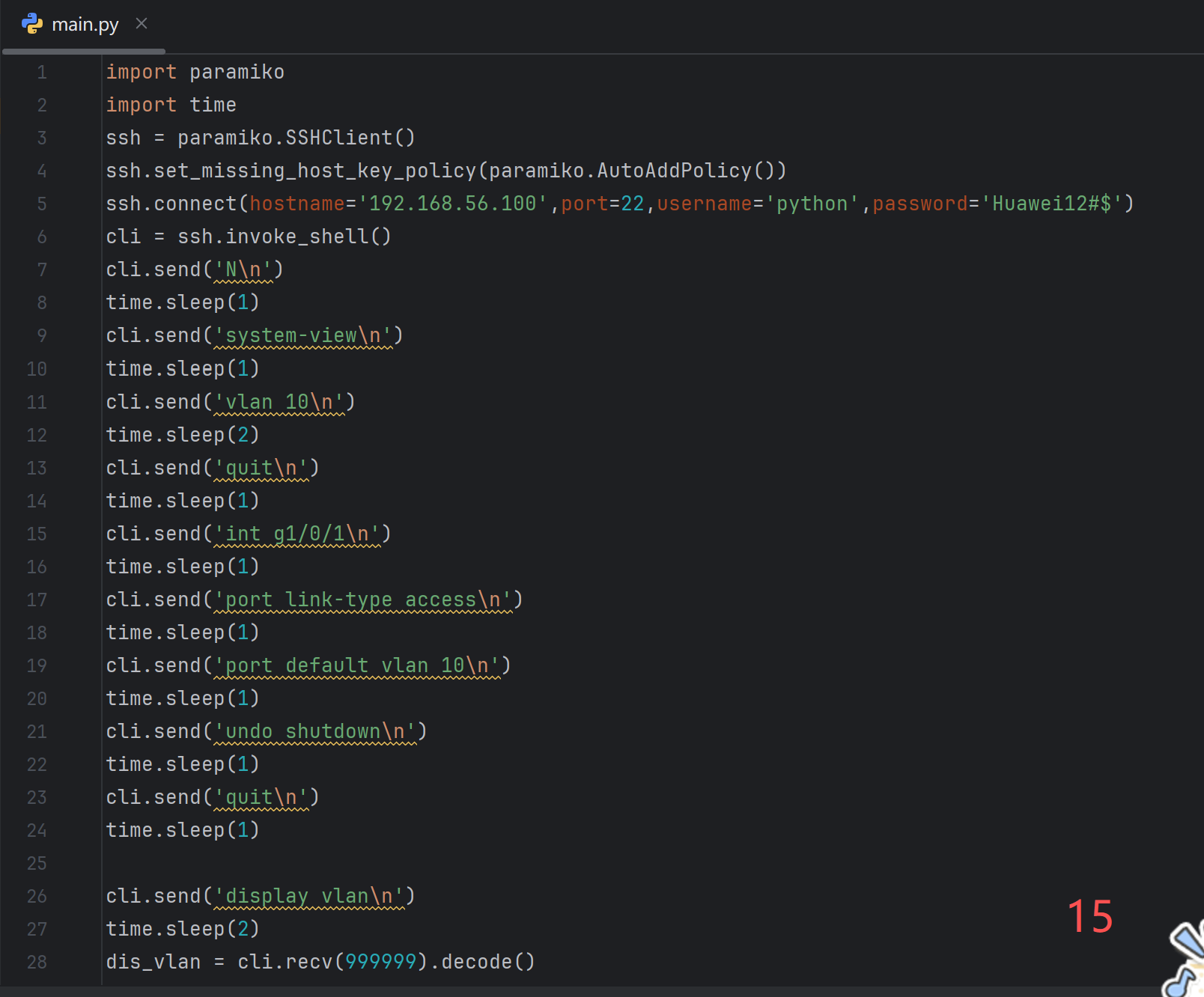


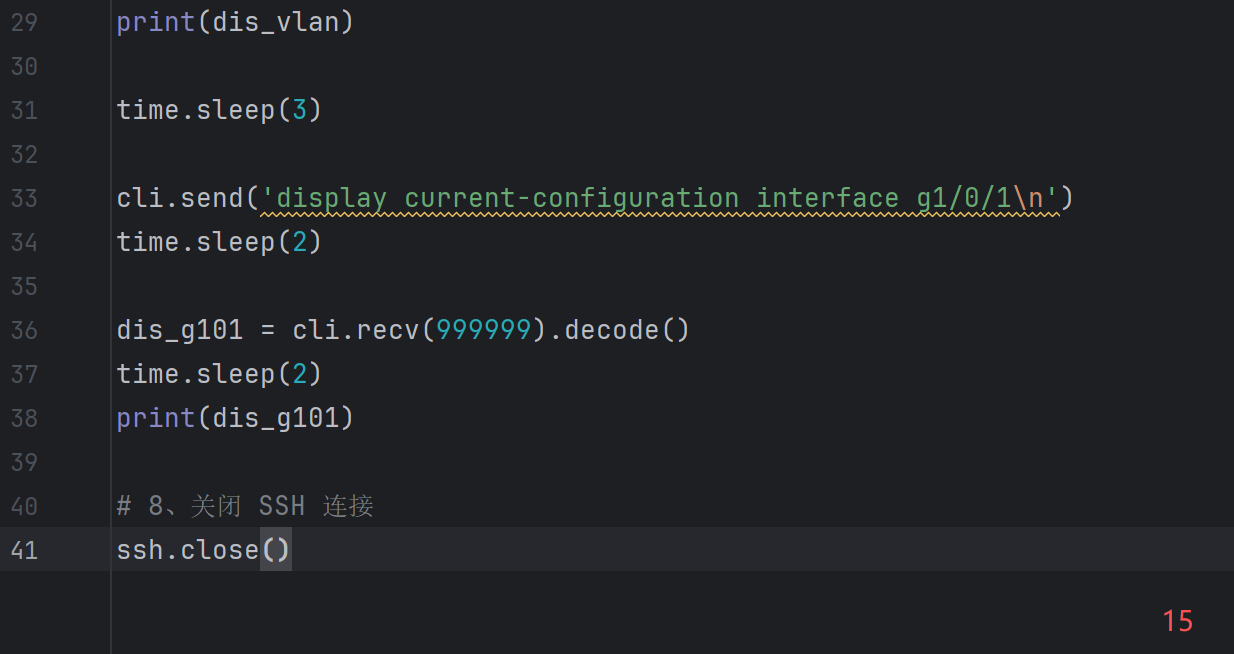
5、**编写SSH登录，并且对设备进行相关配置的python代码**

**（1）SSH登录**

**（2）创建VLAN10，并且将端口gi1/0/1划分到VLAN10**

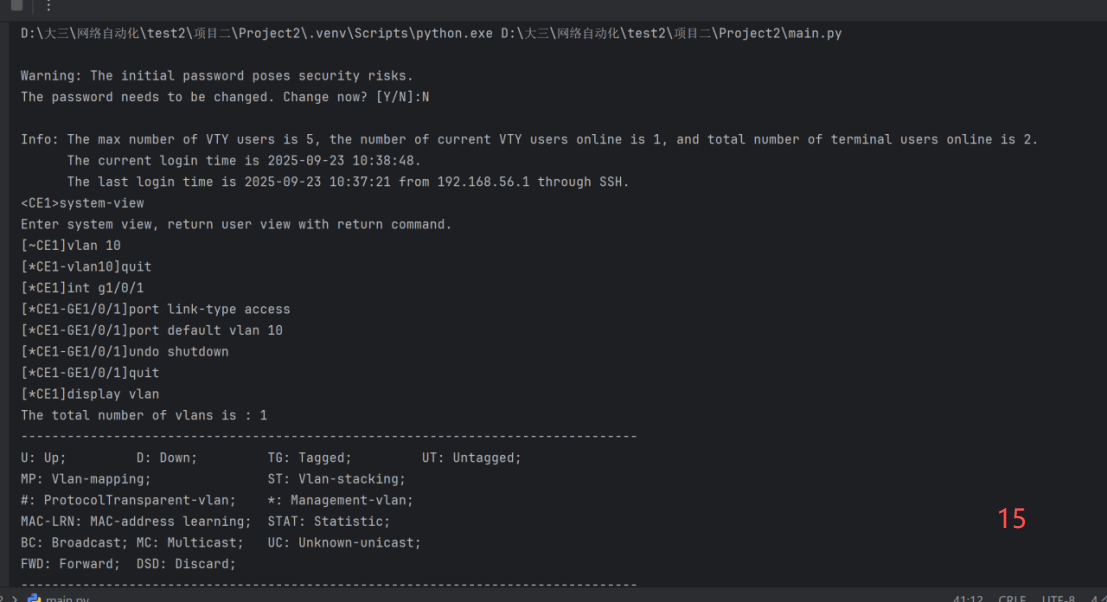
**代码截图**：（标注学号末两位）

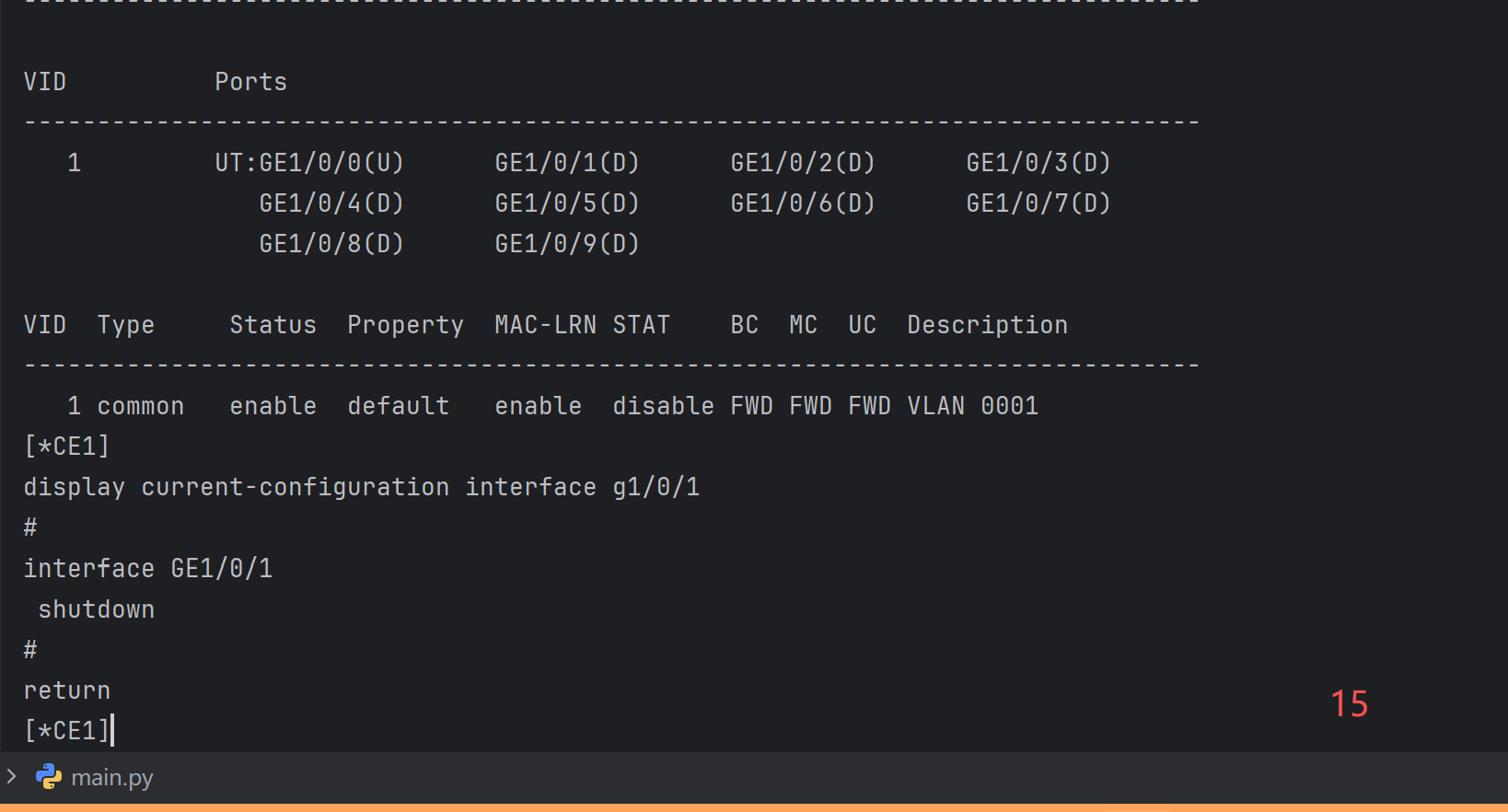




6、运行程序登录设备获取**显示VLAN，显示端口相关信息，并输出**display cu的结果

**运行结果截图**：（标注学号末两位）





1. **实验体会**

**通过本次实验，我掌握了华为交换机SSH服务的完整配置流程，包括管理IP设置、用户创建、服务启用及认证方式配置。使用Paramiko库成功实现了Python自动化登录设备并执行VLAN创建、端口划分等操作，验证了SSH远程管理的安全性与高效性。实验中进一步认识到加密通信对网络运维的重要性，为后续自动化运维实践奠定了基础。**