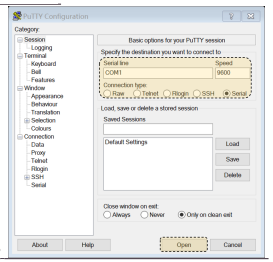
访问网络设备的命令行界面

使用CONSOLE线本地连接

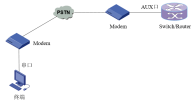
拓扑图



协议Serial，接口com口，波特率9600

适用于设备的初次调试

通过AUX口连接远程访问

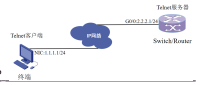


拓扑图

用户字符终端通过PSTN（公共交换电话网络）建立拨号连接，接入网络设备的AUX口

不常用

使用TELNET远程访问



自由主题

拓扑图

配置

1. 配置网络设备接口的IP地址，并保证该IP可达 [H3C-interfacX] ip address ip-address { mask | mask-length }
2. 启动Telnet服务器 [H3C] telnet server enable
3. 进入VTY用户线视图 [H3C] line vty first-num [last-num]
4. 配置VTY用户角色 [H3C-line-vtyX] user-role role-name
5. 为VTY用户配置验证方式 [H3C- line -vtyX] authentication-mode {none | password | scheme}
6. 为Telnet用户配置验证信息
   - none验证方式，此步可省略
   - password验证方式配置验证密码 [H3C-line-vtyX] set authentication password { hash | simple } password
   - scheme验证方法
     - 配置本地用户 [H3C] local-user username class manage
     - 配置用户密码 [H3C-luser-manage-username] password { hash | simple } password
     - 配置用户服务类型 [H3C-luser-manage- username] service-type telnet
     - 配置用户角色（权限） [H3C-luser-manage- username] authorization-attribute user-role role-name

适用于设备上架配置好后的维护管理，数据明文传输，安全性差

使用SSH远程访问

数据传输过程加密，安全的远程访问，比telnet安全

拓扑图

配置

Password验证方法配置

1. 配置网络设备接口的IP地址，并保证该IP可达 [H3C-interfacX] ip address ip-address { mask | mask-length }
2. 生成 RSA、DSA密钥对
   - [H3C] public-key local create rsa
   - [H3C] public-key local create dsa
3. 启动SSH服务器，设置用户认证超时时间和认证尝试次数
   - [H3C] ssh server enable
   - [H3C] ssh server authentication-timeout time-out-value（非必选）
   - [H3C] ssh server authentication-retries times（非必选）
4. 配置VTY使用scheme验证方法，支持SSH协议
   - [H3C] line vty first-num [last-num]
   - [H3C-line-vty0-63]authentication-mode scheme
   - [H3C-line-vty0-63]protocol inbound ssh
5. 为SSH服务器配置本地用户
   - 配置本地用户 [H3C] local-user username class manage
   - 配置用户密码 [H3C-luser-manage-username] password { hash | simple } password
   - 配置用户服务类型 [H3C-luser-manage- username] service-type ssh
   - 配置用户角色（权限） [H3C-luser-manage- username] authorization-attribute user-role role-name

Publickey验证方法配置

客户端生成密钥对操作

- Putty软件（免费）可以生生成密钥对
- 生成私钥、公钥文件名分别为private.key、public.key

服务器端操作与配置

1. 将客户端所保存的公钥文件上传到SSH服务器端（网络设备）
2. 配置网络设备接口的IP地址，并保证该IP可达 [H3C-interfacX] ip address ip-address { mask | mask-length }
3. 生成 RSA、DSA密钥对
   - [H3C] public-key local create rsa
   - [H3C] public-key local create dsa
4. 启动SSH服务器，设置用户认证超时时间和认证尝试次数
   - [H3C] ssh server enable
   - [H3C] ssh server authentication-timeout time-out-value（非必选）
   - [H3C] ssh server authentication-retries times（非必选）
5. 配置VTY使用scheme验证方法，支持SSH协议
   - [H3C] line vty first-num [last-num]
   - [H3C-line-vty0-63]authentication-mode scheme
   - [H3C-line-vty0-63]protocol inbound ssh
6. 为SSH服务器配置本地用户
   - 配置本地用户 [H3C] local-user username class manage
   - 配置用户服务类型 [H3C-luser-manage- username] service-type ssh
   - 配置用户角色（权限） [H3C-luser-manage- username] authorization-attribute user-role role-name
7. 从公钥文件public.key中导入客户端的公钥，并命名为devicekey [H3C] public-key peer devicekey import sshkey public.key
8. 设置本地SSH用户认证方式为publickey，并指定公钥为devicekey [H3C] ssh user username service-type stelnet authentication-type publickey assign publickey devicekey