访问控制列表配置
实验指导手册

学生版

华为技术有限公司

版权所有 © 华为技术有限公司 2020。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://e.huawei.com

华为认证体系介绍

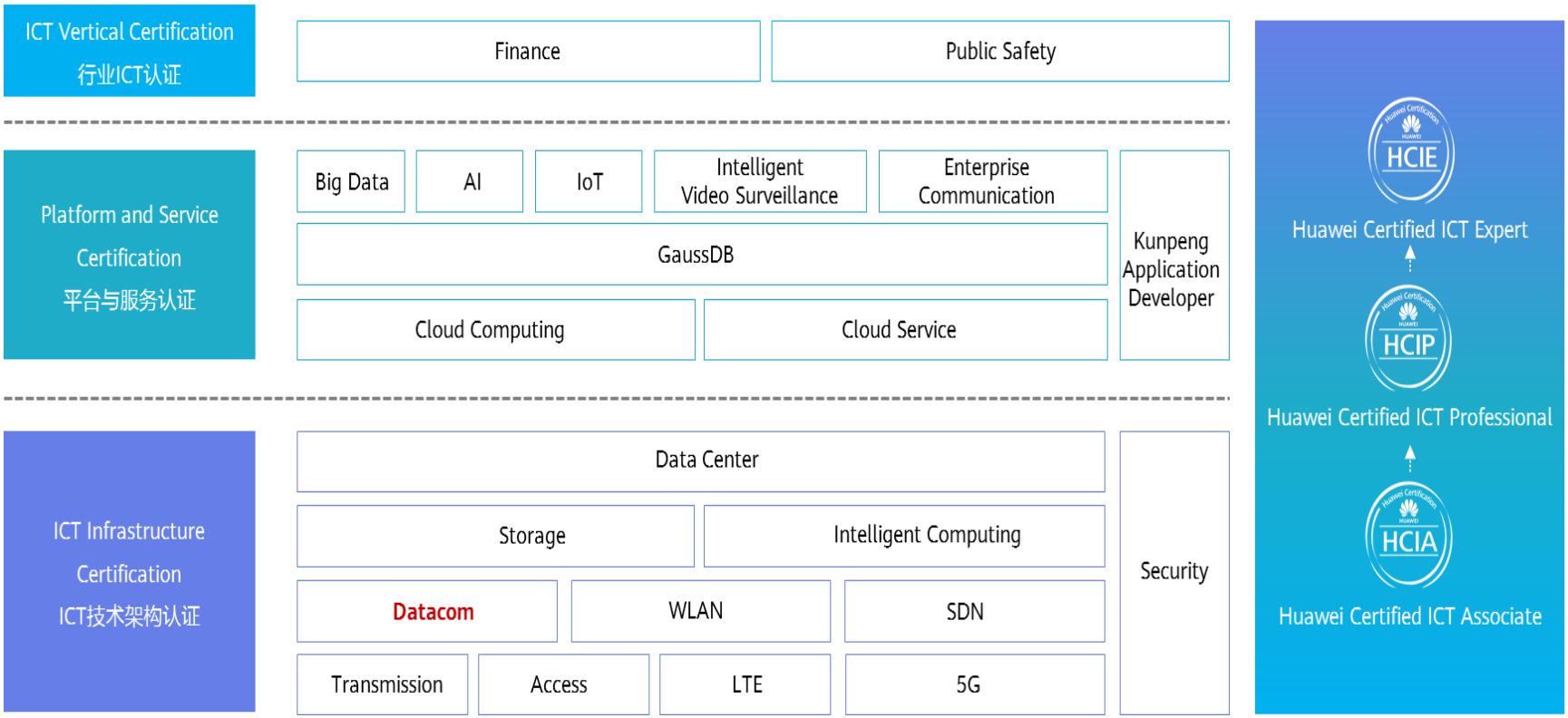
华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新ICT技术架构，打造的ICT技术架构认证、平台与服务认证、行业ICT认证三类认证，是业界唯一覆盖ICT（Information and Communications Technology 信息通信技术）全技术领域的认证体系。

根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。华为认证覆盖ICT全领域，符合ICT融合的技术趋势，致力于提供领先的人才培养体系和认证标准，培养数字化时代新型ICT人才，构建良性ICT人才生态。

HCIA-Datacom（Huawei Certified ICT Associate-Datacom ，华为认证网络通信工程师数据通信方向）主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为数通产品技术人士。HCIA-Datacom认证在内容上涵盖路由交换原理、WLAN基本原理、网络安全基础知识、网络管理与运维基础知识以及SDN与编程自动化基础知识等内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在数通领域的潮头浪尖！

Huawei Certification



目 录

1 前言

1.1 项目背景

访问控制列表 ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL 本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用 ACL 的业务模块的处理策略来允许或阻止该报文通过。

如组网图所示，R3 为服务器，R1 为客户端，客户端与服务器之间路由可达。其中 R1 和 R2 间互联物理接口地址分别为 10.1.2.1/24 和 10.1.2.2/24，R2 和 R3 间互联物理接口地址分别为 10.1.3.2/24 和 10.1.3.1/24。另外，R1 上创建两个逻辑接口 LoopBack 0 和 LoopBack 1 分别模拟两个客户端用户，地址分别为 10.1.1.1/24 和 10.1.4.1/24。

其中一个用户（R1 的 LoopBack 1 接口）需要远程管理设备 R3，可以在服务器端配置 Telnet，用户通过密码登录，并配置基于 ACL 的安全策略，保证只有符合安全策略的用户才能登录设备。

1.2 项目目的

- 掌握 ACL 的配置方法
- 掌握 ACL 在接口下的应用方法
- 掌握流量过滤的基本方式

1.3 项目拓扑

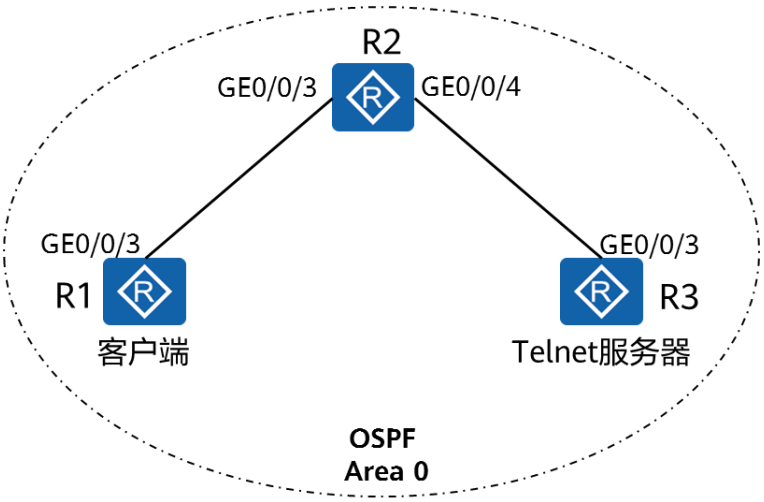


图1-1 ACL 配置实验拓扑

2 项目实施

2.1 项目思路

1.配置设备 IP 地址

2.配置 OSPF，使得网络路由可达

3.配置 ACL，匹配特定流量

4.配置流量过滤

2.2 项目任务

步骤 1　步骤 1 配置设备 IP 地址

配置 R1、R2 和 R3 的 IP 地址

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.1.1.1 24
[R1-LoopBack0]quit
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.1.4.1 24
[R1-LoopBack0]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.1.3.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.1.3.1 24
[R3-GigabitEthernet0/0/3]quit
```

步骤 2　步骤 2 配置 OSPF 使网络互通

在 R1、R2 和 R3 上配置 OSPF，三台设备均在区域 0 中，实现全网互联互通

在 R3 上执行 Ping 命令，检测网络的连通性

步骤 3　配置 R3 为 Telnet 服务器

在 R3 使能 Telnet 功能，配置用户权限等级为 3 级，登录密码为 Huawei@123

```
[R3]telnet server enable
```

telnet server enable 命令用来使能 Telnet 服务器。

```
[R3]user-interface vty 0 4
```

user-interface 命令用来进入一个用户界面视图或多个用户界面视图。

VTY（Virtual Type Terminal）用户界面，用来管理和监控通过 Telnet 或 SSH 方式登录的用户。

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.
Enter Password(<8-128>):Huawei@123
Confirm password:Huawei@123
[R3-ui-vty0-4] quit
```

步骤 4　配置 ACL 进行流量过滤

方式一：在 R3 的 VTY 接口匹配 ACL

在 R3 上配置 ACL，允许 R1 通过 LoopBack 1 口地址 Telnet 到 R3。

acl [number]

创建高级 ACL，使用编号（3000～3999）创建一个数字型的高级 ACL，并进入高级 ACL 视图。

当参数 protocol 为 TCP 时：

rule [rule-id] { deny | permit } { protocol-number | tcp } [destination { destination-address destination-wildcard | any } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { source-address source-wildcard | any } | source-port { eq port | gt port | lt port | range port-start port-end } | tcp-flag { ack | fin | syn } * | time-range time-name] *

protocol-number | tcp：指定 ACL 规则匹配报文的协议类型为 TCP。可以采用数值 6 表示指定 TCP 协议。

destination-port { eq port | gt port | lt port | range port-start port-end}：指定 ACL 规则匹配报文的 UDP 或者 TCP 报文的目的端口，仅在报文协议是 TCP 或者 UDP 时有效。如果不指定，表示 TCP/UDP 报文的任何目的端口都匹配。其中：

eq port：指定等于目的端口；

gt port：指定大于目的端口；

lt port：指定小于目的端口；

range port-start port-end：指定源端口的范围。

在 R3 的 VTY 接口上进行流量过滤

[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound

在 R3 上查看 ACL 配置信息
[R3]display acl 3000
display acl 命令用来查看 ACL 的配置信息。
高级访问控制列表，序号为 3000，共 2 条规则。
ACL 的步长为 5。
规则 5，允许特定的流量通过，当没有匹配的报文时，不显示 matches 字段。

方式二：在 R2 的物理接口匹配 ACL
在 R2 上配置 ACL，只允许 R1 通过物理接口地址 Telnet 到 R3。

在 R2 的 GE0/0/3 接口上进行流量过滤
traffic-filter 命令，用来在接口上配置基于 ACL 对报文进行过滤。
命令格式：traffic-filter { inbound | outbound } acl { acl-number | name acl-name }
inbound：指定在接口入方向上配置报文过滤。
outbound：指定在接口出方向上配置报文过滤。
acl：指定基于 IPv4 ACL 对报文进行过滤。
在 R2 上查看 ACL 配置信息
规则5，允许特定的流量通过，匹配的报文数目为21。

3 结果验证

检测 Telnet 访问，验证 ACL 配置结果

1）在 R1 上带源地址 10.1.1.1 telnet 到服务器。

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

telnet 命令用来从当前设备使用 Telnet 协议登录到其它设备。

-a s*ource-ip-address* ： 通过指定源地址，用户可以用指定的 IP 地址与服务端通信。

```
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Error: Can't connect to the remote host
```

2）在 R1 上带源地址 10.1.4.1 telnet 到服务器。

```
<R1>telnet -a 10.1.4.1 10.1.3.1
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Connected to 10.1.3.1 ...

Login authentication

Password:
<R3>quit
```

4 思考题与附加内容

仍使用实验组网图，若 R3 同时为 Telnet 服务器和 FTP 服务器，现要求客户端 R1 的 LoopBack 0 接口地址只能够访问 FTP 服务，R1 的 LoopBack 1 接口地址只能够进行 Telnet 对 R3 进行远程管理。

请通过配置 ACL，完成上述要求。