

eNSP Pro
V100R001C00

产品文档

文档版本	01
发布日期	2023-06-30



版权所有 © 华为技术有限公司 2023。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



HUAWEI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：<https://www.huawei.com>

客户服务邮箱：support@huawei.com

客户服务电话：4008302118

目 录

1 文档指南	1
1.1 文档约定	1
1.2 获取技术支持	4
1.3 变更记录	4
2 规划与设计	5
2.1 产品描述	5
2.1.1 产品定位和特点	5
2.1.2 应用场景	5
2.1.3 产品架构	5
2.2 功能描述	6
2.3 模拟器特性列表	6
2.3.1 NE 路由器模拟器	6
2.3.2 CE 交换机模拟器	25
2.3.3 S 交换机模拟器	31
2.3.4 AR 路由器模拟器	37
2.3.5 USG 防火墙模拟器	44
2.3.6 客户端模拟器（PC-Client）	50
2.3.7 服务端模拟器（PC-Server）	50
3 软件安装	51
3.1 软件获取	51
3.2 硬件要求	51
3.3 设备规格要求	52
3.4 数通模拟器部署	52
3.4.1 部署数通模拟器（Windows 系统）	52
3.4.1.1 软件要求	52
3.4.1.2 部署虚拟机	52
3.4.1.3 删除虚拟机	57
3.4.2 部署数通模拟器（Linux 系统）	59
3.4.2.1 软件要求	59
3.4.2.2 部署虚拟机	59
3.4.2.3 删除虚拟机	60
4 操作与维护	62

4.1 帐号注册.....	62
4.2 数通模拟器登录.....	65
4.3 沙箱操作.....	67
4.3.1 创建沙箱.....	67
4.3.2 修改沙箱.....	68
4.3.3 导出沙箱.....	68
4.3.4 导入沙箱.....	69
4.4 设备操作.....	70
4.4.1 添加设备.....	70
4.4.2 导入配置.....	73
4.4.3 启动设备.....	74
4.4.4 导出配置.....	75
4.4.5 配置命令行.....	77
4.4.6 修改设备名称.....	78
4.4.7 获取报文.....	79
4.4.8 停止设备.....	81
4.4.9 对齐设备.....	82
4.4.10 删除设备.....	84
4.4.11 配置 PC Client 终端.....	84
4.4.12 配置 PC Server 终端.....	87
4.5 连线操作.....	92
4.5.1 添加连线.....	92
4.5.2 删除连线.....	93
4.6 其他操作.....	94
4.6.1 添加文本.....	94
4.6.2 绘制图形.....	95
5 FAQ.....	97
5.1 网络环境切换导致登录失败.....	97
5.2 登录数通模拟器网页时报无法访问此页面.....	97
6 参考.....	99
6.1 GUI 参考.....	99
6.2 命令参考.....	101
7 缩略语.....	103

1 文档指南

1.1 文档约定

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗字体 表示。

格式	意义
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从两个或多个选项选取一个。
[x y ...]	表示从两个或多个选项选取一个或者不选。
{ x y ... } *	表示从两个或多个选项选取多个，最少选取一个，最多选取所有选项。
[x y ...] *	表示从两个或多个选项选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

图形界面元素引用约定

在本文中可能出现下列图形界面元素，它们所代表的含义如下。

格式	意义
“ ”	带双引号“ ”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

安全声明

- 密码配置声明
 - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
 - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@"或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。
 - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法声明

目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。

- 个人数据声明

您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

- 公网IP地址使用声明

出于特性介绍及配置示例的需要，产品资料中会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

因开源及第三方软件中自带公网地址（包括公网IP地址、公网URL、邮箱地址），本产品没有使用这些公网地址，这遵循业界实践，也符合开源软件使用规范。

- 数通模拟器仅用于培训学习场景，不具备完备的DDOS攻击防护能力，建议用户在使用模拟器过程中，将模拟器部署于安全网络环境中；模拟器使用过程中，用户创建的设备实例会消耗一定的CPU和内存资源，过度使用可能会导致模拟器资源耗尽而失去响应，建议您根据实际资源配置情况酌情使用。
- 数通模拟器登录时需要认证跳转服务，用于完成用户认证，实现数通模拟器的用户登录功能，域名为tc.stm.huawei.com。“Cookies 使用确认”中可以开启“功能性Cookies”，其有效期为1年。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于描述该产品检测通信传输中的故障和错误的目的使用，不涉及采集、处理任何个人数据或用户通信内容。
- 为获取设备之间的通信报文，数通模拟器引入了tcpdump功能。该报文获取功能仅限于数通模拟器内部使用，不涉及用户其他网络平面和网络设备上的报文获取，由于获取报文时获取的cap文件可能存在安全风险，请您注意妥善保管该cap文件。

特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 您购买的产品、服务或特性等应受华为技术有限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，华为技术有限公司对本文档内容不做任何明示或默示的声明或保证。
- 本文档中提供的最大值是设备在实验室特定场景（例如被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 本手册中出现的接口编号仅作参考，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

缺省帐号和密码清单

您可以在《eNSP Pro缺省帐号和密码》文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

通信矩阵

您可以在《eNSP Pro V100R001C00 安全手册》中获取。

1.2 获取技术支持

用户请通过如下方式获取技术支持：

- 客户服务邮箱：servicetool@huawei.com

1.3 变更记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

- **文档版本 01（2023-06-30）**
第一次正式发布。本资料版本对应软件版本为V100R001C00。

2 规划与设计

2.1 产品描述

2.1.1 产品定位和特点

数通模拟器是华为公司数据通信产品线推出的设备模拟器，主要应用在数据通信技能培训，为使用者提供华为数据通信产品设备命令行学习环境，具备以下特点：

1. 多产品模拟能力：支持数据通信产品线NE路由器、CE交换机、S交换机、AR路由器、USG防火墙等，并持续更新支持网元类型。
2. 配置模拟能力：具备设备命令行配置模拟能力，支持HCIA-Datacom认证和HCIA-Security认证特性配置，并持续丰富HCIE认证高级特性。
3. 部署能力：以虚拟机镜像发布，支持个人PC、物理服务器等环境的灵活部署。

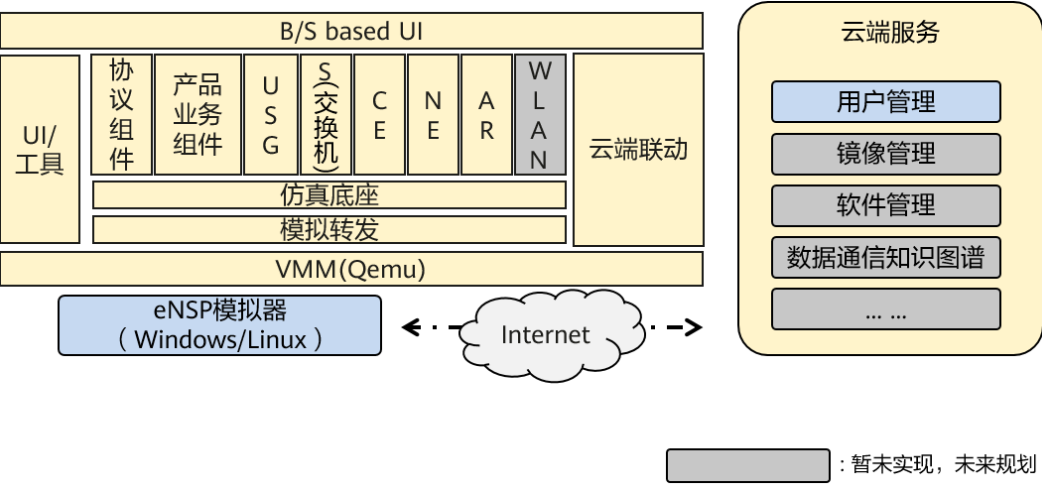
2.1.2 应用场景

数通模拟器在华为数据通信产品线培训、认证、学习解决方案中，向用户提供一站式的数据通信产品模拟环境。

2.1.3 产品架构

数通模拟器提供低耦合、支持灵活扩展的软件总体架构，如图2-1所示。

图 2-1 软件总体架构



2.2 功能描述

数通模拟器工具支持的特性如表2-1所示。

表 2-1 数通模拟器的功能 1

功能	描述信息
Uniportal登录	基于华为Uniportal认证系统，实现用户登录认证功能。
拓扑功能	支持拓扑编辑，连线，调色板，文本框，获取报文等能力。
终端模拟	支持终端模拟，终端支持DHCP、SSH、Ping等能力。
设备模拟	支持对多种类型的华为设备进行模拟，当前已经支持的款型包括NE路由器、CE交换机、S交换机、AR路由器、USG防火墙。不对标实体设备系列和规格。

2.3 模拟器特性列表

须知

特性约束：当前版本数通模拟器特性并非对标华为真实设备，而是基于培训认证需求对标HCIA-Datacom认证和HCIA-Security认证所涉及的特性。特性清单中细化到二级特性的支持，如果您在使用过程中发现存在设备特性无法满足HCIA认证场景需求的问题，请寻求技术支持，获取方式参见1.2获取技术支持。

2.3.1 NE 路由器模拟器

NE路由器模拟器支持的特性如表2-2所示。

表 2-2 NE 路由器模拟器支持的特性

一级特性	二级特性	描述信息
基础配置	TTY	终端类型TTY（Terminal Type）也叫做终端服务，为用户配置设备时提供接入接口和人机交互机制。
	Telnet	Telnet（Telecommunication Network Protocol）起源于1969年的ARPANET，是一种最早的Internet应用。Telnet连接是一种TCP（Transmission Control Protocol）连接，用来传输数据和少量的Telnet控制信息。Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端。Telnet采用客户端/服务器模式。
	SSH	Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet和FTP通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH（Secure Shell）是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。
	CLI	命令行接口CLI（Command Line Interface）是用户与路由器进行交互的常用工具。用户登录到路由器出现命令行提示符后，即进入命令行接口。系统向用户提供一系列命令，用户可以通过命令行接口输入命令，由命令行接口对命令进行解析，实现用户对路由器的配置和管理。

一级特性	二级特性	描述信息
	FS: FTP TFTP	FTP协议是一种基于TCP/IP协议族的Internet标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP采用两条TCP连接将一个文件从一个系统复制到另一个系统，连接通常是以客户-服务器的方式建立，这两条TCP连接分别是控制连接（服务器端为21号端口）和数据连接（服务器端为20号端口）。 TFTP（Trivial File Transfer Protocol）即简单文件传送协议，属于UDP（User Datagram Protocol）协议，使用69号端口。TFTP客户端通过发送请求给TFTP服务器来读、写文件和建立连接。文件以固定的长度传输，长度为512字节。小于512字节的数据包表示至此传输结束。每个数据包包含一个数据块，在传输过程中出现数据丢失时该数据块可以控制是否重新传输。
	CFG	为满足业务需求用户对系统进行的一系列命令行操作，将这些操作进行保存然后重启系统依然能够继续生效。
系统管理	VS	虚拟设备（Virtual System）：网络管理员将物理设备PS（Physical System）通过硬件和软件级别的仿真，分割成多个执行单独路由任务的虚拟设备。不同的虚拟设备共享相同的软件和所有的公共资源，即不同的VS可以共享相同的主控板和接口板，每个接口只能归属于一个VS。
	FM	故障管理功能是电信管理网的五大功能（性能管理、配置管理、安全管理、故障管理和计费管理）之一，主要对设备和网络的异常运行情况进行实时监视，完成对故障信息和设备运行情况的监视、报告和存储。而且通过告警的显示可以使用户能尽快采取相应措施，对故障进行隔离和校正，恢复受影响的业务。
	PM	PM是Performance Management的简称，又被称为性能管理，是一种用于监控和采集系统中的各项性能指标（如CPU利用率、接口收发报文数据）的技术。PM对各项性能数据进行周期性的统计，提供当前性能数据的统计信息、历史性能数据的统计信息供用户查询。
	LAD	链路自动发现协议LAD（Link Automatic Discovery）是定义在链路层的私有邻居发现协议。LAD协议规定设备可以通过命令行或者网管下发链路搜索请求，并根据收到的链路搜索应答，在本端设备生成邻居信息。

一级特性	二级特性	描述信息
	LLDP	LLDP（Link Layer Discovery Protocol，链路层发现协议）是IEEE 802.1ab中定义的第二层发现协议。通过在网络中部署LLDP协议，NMS的能力迅速提升，既能掌握更详细的网络拓扑信息以及网络拓扑变化信息，还能及时发现网络中实际存在的不合理的配置，这些信息有助于网络管理员实时监控网络状态，有效提升了网络的安全性和稳定性。
	OPS	开放可编程系统OPS（Open Programmability System）是指设备通过提供统一的应用程序接口OPS API（OPS Application Programming Interface）来开放系统，使得系统具备可编程能力，可以运行第三方应用程序。
	KPI	KPI是Key Performance Indicator的简称，表示某一时刻设备运行状态的性能值，KPI可能由多级KPI汇聚而来。通过主控板和接口板调度采集KPI数据（格式为：xxx.dat）并存储在CF卡中，工具根据约定好的文件解析格式进行解析后转换成Excel文件，用户可根据此Excel文件快速定位故障及了解业务受损情况。
	PADS	支持基于PADS（Protocol-Aided Diagnosis System）的智能诊断。使用该系统可以完成业务故障的自动预防、自动发现、自动诊断，并支持联动自愈系统完成故障的自动恢复。
网络可靠性	BFD： BFD for IP BFD for PST BFD for Link-bundle BFD for Per-Link BFD Dampening SBFD for SR-MPLS SBFD for SR-MPLS支持配置回程路径 BFD for BGP支持TTL有效性检查	双向转发检测BFD（Bidirectional Forwarding Detection）用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。为了减小设备故障对业务的影响，提高网络的可靠性，网络设备需要能够尽快检测到与相邻设备间的通信故障，以便及时采取措施，保证业务继续进行。
	MPLS OAM	MPLS作为可扩展的下一代网络的关键承载技术，提供具有QoS保障的多业务能力，并且MPLS引入了一个独特网络层次，新的网络层会引起的相应的故障。因此，MPLS网络需要具备OAM（Operations, Administration, and Maintenance）能力。

一级特性	二级特性	描述信息
	MPLS-TP OAM	MPLS-TP (Multiprotocol Label Switching Transport Profile) 是一种融合了MPLS包交换和传统传送网特性的传输技术, 可以替代原有传送网作为未来的承载网。MPLS-TP OAM可以有效检测、识别和定位MPLS-TP用户层面故障, 在链路或节点出现故障时迅速进行保护倒换。运维管理OAM是降低网络维护成本的有效手段, MPLS-TP OAM机制用于MPLS-TP用户层的运维管理。
	VRRP	虚拟路由冗余协议VRRP (Virtual Router Redundancy Protocol) 通过把几台路由设备联合组成一台虚拟的路由设备, 使用一定的机制保证当主机的下一跳路由设备出现故障时, 及时将业务切换到备份路由设备, 从而保持通讯的连续性和可靠性。VRRP是相关标准定义的一种冗余容错协议, 通过物理设备和逻辑设备的分离, 实现在多个出口网关之间选路。
	ETH-OAM: EFM CFM Y.1731	支持基于EFM (Ethernet in the First Mile) 协议检测以太网链路的连通性及链路质量。 支持基于CFM (Connectivity Fault Management) 的连通性检测、环回功能和链路跟踪功能, 用于以太网络的质量监测和故障定位。 EFM和CFM的组合应用, 基本上能够解决运营商对于链路故障的问题定位需求, 但是更深层次的需求例如业务性能的检测, 则需要部署Y.1731。Y.1731实际上是在CFM的基础上增加了性能检测的部分功能。
	ETH-LPT	LPT (Link-state Pass Through) 即链路状态穿透, 就是把网络本端的链路状态透传到网络对端, 使得对端可根据本端状态进行联动。
	RBS	双机备份是指在部署了主备协议 (比如VRRP、E-Trunk) 的场景下, 将主用设备上的用户业务控制数据实时备份到备用设备, 当主用设备或者链路出现故障时, 能够快速将用户业务切换至备用设备; 当主用设备或者链路的故障恢复时, 用户业务能够顺利由备用设备回切至主用设备, 保证了用户业务的不中断。
接口与链路	IFM	接口管理。接口是该设备与网络中的其它设备交换数据并相互作用的部件, 分为物理接口和逻辑接口两类: 物理接口是真实存在、有器件支持的接口; 逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。

一级特性	二级特性	描述信息
局域网与城域网接入	Eth	以太网技术起源于一个实验网络，该实验网络的目的是把几台个人计算机以3M的速率连接起来。“以太网”一般是指由DEC（Digital Equipment Corporation）、Intel和Xerox组成的DIX（DEC-Intel-Xerox）联盟开发并于1982年发布的10 Mbit/s的以太网标准。而IEEE 802.3规范则是基于以太网的标准制定的，并与以太网标准相互兼容。在TCP/IP中，RFC标准分别定义了以太网的IP数据报文封装格式和IEEE802.3网络的IP数据报文封装格式。当今最常使用的封装格式是Ethernet II，又称为Ethernet DIX。
	Trunk： Eth-Trunk E-Trunk	Eth-trunk通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。捆绑在一起的链路通过相互间的动态备份，可以有效地提高链路的可靠性。 Trunk是一种捆绑技术。将多个物理接口捆绑成一个逻辑接口，这个逻辑接口称为Trunk接口，捆绑在一起的每个物理接口称为成员接口。Trunk技术可以实现增加带宽、提高可靠性和负载分担的功能。
	GVRP	GARP（Generic Attribute Registration Protocol）协议主要用于建立一种属性传递扩散的机制，以保证协议实体能够注册和注销该属性。GARP作为一个属性注册协议的载体，可以用来传播属性。将GARP协议报文的内容映射成不同的属性即可支持不同上层协议应用。GVRP（Generic VLAN Registration Protocol）是GARP的一种应用，用于注册和注销VLAN属性。GARP协议通过目的MAC地址区分不同的应用。在IEEE Std 802.1Q中将01-80-C2-00-00-21分配给VLAN应用，即GVRP。
	VLAN	VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的LAN在逻辑上划分成多个广播域（多个VLAN）的通信技术。每一个VLAN都包含一组拥有相同需求的计算机，与物理上形成的LAN具有相同的属性。但是由于VLAN是在逻辑划分而不是在物理上划分，所有同一个VLAN内的各个工作站无需放置在同一个物理空间。VLAN内的主机间可以直接通信，而VLAN间不能直接互通，即使两台计算机有着同样的网段，但是它们不属于同一个VLAN，它们各自的广播流不会互相转发，从而将广播报文限制在一个VLAN内。由于VLAN间不能直接互访，因此提高了网络安全性。

一级特性	二级特性	描述信息
	EVC	以太虚连接EVC（Ethernet Virtual Connection）由城域以太网论坛MEF（Metro Ethernet Forum）提出，定义了统一的二层承载业务模型和配置模型。MEF（Metro-Ethernet Forum）定义了EVC可关联ISP（Internet service provider）网络中两个或以上用户网络接口。在EVC模型中，使用广播桥域BD（Bridge Domain）隔离用户网络。
	STP/RSTP	以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，并导致广播风暴以及MAC地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议STP（Spanning Tree Protocol）。RSTP在STP基础上进行了改进，实现了网络拓扑快速收敛。
	MSTP	IEEE于2002年发布的802.1S标准定义了MSTP。MSTP通过设置VLAN映射表（即VLAN和生成树实例的对应关系表），把VLAN和生成树实例联系起来。同时它把一个交换网络划分成多个域，每个域内形成多棵生成树实例，生成树实例之间彼此独立。MSTP将环路网络修剪成为一个无环的树形网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现VLAN数据的负载均衡。MSTP兼容STP和RSTP。
	RRPP	快速环网保护协议（Rapid Ring Protection Protocol，以下简称RRPP）是一个专门用于破除以太网数据环路的链路层（二层）协议。运行该协议的设备通过RRPP报文检测网络中是否存在环路，并适时对某些接口进行阻塞以消除环路。RRPP Snooping是将RRPP环路变化通知到VPLS（Virtual Private LAN Service）网络的技术。
	ERPS	ERPS（Ethernet Ring Protection Switching）是ITU-T定义的一种二层破环协议标准，标准号为ITU-T G.8032/Y1344，因此又称为G.8032。它定义了R-APS（Ring Auto Protection Switching）协议报文和保护倒换机制。如果环网内厂商的设备都支持该协议，则可以实现互通。
	BPDU Tunnel	BPDU（Bridge Protocol Data Unit）Tunnel是BPDU报文在运营商网络透明传输的路径。不同用户网络的分支通过运营商网络的BPDU Tunnel可以实现透明传输各自的BPDU报文。

一级特性	二级特性	描述信息
	VXLAN: Underlay Overlay EVPN VXLAN 集中式网关 分布式网关 三段式VXLAN	VXLAN是NVO3中的一种网络虚拟化技术，通过将虚拟机发出的数据包封装在UDP中，并使用物理网络的IP、MAC作为outer-header进行封装，然后在IP网络上传输，到达目的地后由隧道终结点解封装并将数据发送给目标虚拟机。
	VXLANv6	相对于VXLAN，VXLANv6使用的是IPv6 UDP封装。
IP业务	ARP: ARP代理 ARP双活	地址解析协议ARP（Address Resolution Protocol）是用来将IP地址解析为MAC地址的协议。
	ND: ND代理 ND双活	邻居发现协议ND（Neighbor Discovery Protocol）是IPv6协议体系中一个重要的基础协议。邻居发现协议替代了IPv4的ARP协议（Address Resolution Protocol）和ICMP路由器发现（Router Discovery），它定义了使用ICMPv6报文实现路由器发现、重复地址检测、地址解析，邻居不可达检测，以及重定向等功能。
	DHCP: DHCP DHCP Relay DHCP Snooping	动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议分为DHCP和DHCPv6，分别应用于IPv4网络和IPv6网络的地址申请和动态配置。DHCP和DHCPv6都采用客户端/服务器模式，但是操作模式和实现原理完全不同，支持DHCP Client通过DHCP 获得ip地址，但不支持通过DHCP获得server端ip pool 中的DNS server信息。

一级特性	二级特性	描述信息
	DHCPv6: DHCPv6 DHCPv6 Relay DHCPv6 Snooping	动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议分为DHCP和DHCPv6，分别应用于IPv4网络和IPv6网络的地址申请和动态配置。DHCP和DHCPv6都采用客户端/服务器模式，但是操作模式和实现原理完全不同。不支持DHCPv6 Client 相关配置。
	DNS	域名系统（DNS，Domain Name System）是一种用于TCP/IP应用程序的分布式数据库，提供域名与IP地址之间的转换。
	MTU（只支持IP的MTU）	最大传输单元（Maximum Transmission Unit）定义了一个接口在无需分片的情况下能够发送的最大长度的IP报文。如果IP报文的长度大于MTU的值，那么它会在发送出接口前被分片。
	IPv4: ICMP TCP UDP RawIP Socket	IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议。它工作在TCP/IP协议栈的互联网络层。该层与OSI参考模型的网络层相对应。IP层将信息分割成数据单元，并添加地址信息和控制信息，使得数据包能够按照路由转发。IP层提供的是不可靠、无连接数据传输服务。不可靠的意思是它不能保证IP数据报能成功地到达目的地。IP仅提供最好的传输服务。如果发生某种错误时，如某个路由器暂时用完了缓冲区，IP会丢弃该数据报，然后发送ICMP消息报给信源端。任何要求的可靠性必须由上层来提供（如TCP）。无连接的意思是IP并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP数据报可以不按发送顺序接收。如果一信源向相同的信宿发送两个连续的数据报（先是A，然后是B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此B可能在A到达之前先到达。
	IPv6: IPv6 ICMPv6 Path MTU TCP6 UDP6 RawIP6	IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。它是IETF（Internet工程任务组）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版本。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制在未来的市场竞争中充满了活力。

一级特性	二级特性	描述信息
IP路由	IP路由	路由是数据通信网络中最基本的要素。路由信息就是指导报文发送的路径信息，路由的过程就是报文中继转发的过程。
	静态路由： 静态路由 BFD for 静态路由 NQA for 静态路由	静态路由是一种需要管理员手工配置的特殊路由。
	RIP： RTP-1 RTP-2 BFD for RIP	RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议IGP（Interior Gateway Protocol），主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP是一种基于距离矢量（Distance-Vector）算法的协议，它通过UDP报文进行路由信息的交换，使用的端口号为520。RIP使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在RIP中，缺省情况下，路由器到与它直接相连网络的跳数为0，通过一个路由器可达的网络的跳数为1，其余依此类推。也就是说，度量值等于从本网络到达目的的网络间的路由器数量。为限制收敛时间，RIP规定度量值取0~15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。
	RIPng： 水平分割 毒性逆转	RIPng（RIP next generation，下一代RIP协议）是对原来的IPv4网络中RIP version 2协议在IPv6网络上的扩展，大多数RIP的概念都可以应用于RIPng。RIPng协议是基于D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在RIPng协议中，从一个设备到其直连网络的跳数为0，到通过另一台设备可达的网络的跳数为1，如此类推，当跳数大于或等于16时，目的网络或主机就被定义为不可达。
	OSPF： OSPF OSPF TE OSPF VPN OSPF NSSA BFD for OSPF OSPF GTSM OSPF Smart-discover	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。

一级特性	二级特性	描述信息
	OSPFv3: OSPFv3 BFD for OSPFv3 OSPFv3 GR OSPFv3 VPN	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。OSPFv3在OSPFv2基础上进行了增强，是一个独立的路由协议。
	IS-IS: IS-IS IS-IS for IPv6 IS-IS TE IS-IS Wide Metric BFD for IS-IS IS-IS MT IS-IS Local MT IS-IS GR	IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）最初是国际标准化组织ISO（the International Organization for Standardization）为它的无连接网络协议CLNP（ConnectionLess Network Protocol）设计的一种动态路由协议。随着TCP/IP协议的流行，为了提供对IP路由的支持，IETF在相关标准中对IS-IS进行了扩充和修改，使它能够在同时应用在TCP/IP和OSI环境中，称为集成IS-IS（Integrated IS-IS或Dual IS-IS）。
	BGP: BGP AIGP BGP联盟 RR 路由交叉 MP-BGP BFD for BGP BGP Peer Tracking BGP 6PE BGP ORF VPN ORF BMP BGP Best External BGP Add-Path BGP下一跳迭代震荡抑制 BGP-LS RPD 熵标签	BGP（Border Gateway Protocol）是一种用于自治系统AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，主要用于交换AS之间的可达路由信息，构建AS域间的传播路径，防止路由环路产生，并在AS级别应用一些路由策略。当前使用的版本是BGP-4。BGP作为事实上的Internet外部路由协议标准，被广泛应用于ISP（Internet Service Provider）之间。

一级特性	二级特性	描述信息
IP组播	IP组播基础	IP组播是单一的信息流被同时发送给一组用户，相同的组播数据流在每一条链路上最多仅有一份，从而降低了带宽的消耗。随着Internet网络的不断发展，网络中交互的各种数据、语音和视频信息越来越多，同时新兴的电子商务、网上会议、网上拍卖、视频点播、远程教学等服务也在逐渐兴起。这些服务大多符合点对多点的模式，对信息安全性、有偿性、网络带宽提出了较高的要求。
	IGMP: IGMP IGMP SSM Mapping IGMP on-demand	随着组播应用的发展，加入组播组接收组播数据的主机越来越多，如何在组播路由器上管理组播组和相应的成员成为一个重要问题。IGMP（Internet Group Management Protocol）因特网组管理协议，是TCP/IP协议族中负责IPv4组播成员管理的协议，用来在IP主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。通过在接收者主机和与其直连的组播路由器上配置IGMP，可以实现主机动态加入组播组和组播路由器对本地网络组成员信息的管理。
	PIM: PIM-DM PIM-SM PIM-SSM 组播 over P2MP TE 隧道	PIM表示组播路由协议与网络中的单播路由协议类型无关，即：只要网络中各设备间存在可达的单播路由，PIM协议就可以借助单播路由表为IP组播数据提供路由。目前在实际网络中，PIM的实现方式主要有PIM-DM、PIM-SM和PIM-SSM，PIM-SM和PIM-SSM可应用于IPv4和IPv6网络，而PIM-DM仅应用于IPv4网络。
	MSDP	组播源发现协议MSDP（Multicast Source Discovery Protocol）是基于多个PIM-SM（Protocol Independent Multicast-Sparse Mode）域互连而开发的一种域间组播解决方案，目前只支持IPv4。
	组播路由管理： RPF单播逆向路由检查 组播负载分担	组播转发表由一组(S,G)表项组成。(S,G)表示由源S向组播组G发送的组播数据的路由信息。组播路由管理支持多种组播路由协议，组播转发表中汇集了由多种协议生成的组播路由表项。组播路由管理（Multicast Route Management）用于管理组播转发表，能够控制组播路由创建或改变组播路由。
	Rosen MVPN: Rosen MVPN 组播VPN Extranet BGP A-D方式的组播VPN	Rosen方式的MVPN（Multicast VPN，组播VPN）解决方案基于相关标准制定的MD（Multicast Domains）方案，是为了在现有MPLS/BGP VPN上开通组播业务。

一级特性	二级特性	描述信息
	NG MVPN: NG MVPN私网组播路由原理 NG MVPN公网隧道原理 NG MVPN Extranet UMH选路规则 NG MVPN应用	NG MVPN是IP组播数据流量穿越BGP/MPLS VPN网络的新一代框架，提供基于BGP的信令传递模式和PIM SM、PIM SSM、P2MP TE、mLDP等多种数据承载模式，使组播和单播业务统一在同一个VPN架构中。
	BIER: IS-IS for BIER NG MVPN over BIER	基于比特索引的显式复制BIER是一种新的组播技术。和传统组播技术相比，这种组播技术通过将组播报文目的节点的集合以比特串的方式封装在报文头部进行发送，从而使网络中间节点无需为每一个组播流(Per-flow)建立组播树及保存组播流状态，仅需根据报文头部的目的节点的集合进行复制转发。
	BIERv6	IPv6封装的比特索引显式复制BIERv6（Bit Index Explicit Replication IPv6 Encapsulation）是一种在IPv6网络中，通过将组播报文目的节点的集合以比特串（称为BitString）的方式封装在报文头部发送，从而使网络中间节点无需为每一条组播流建立组播分发树和保存流状态，仅需根据报文头部的比特串完成复制转发的组播方案。
	MLD	MLD（Multicast Listener Discovery）组播侦听者发现协议，是负责IPv6组播成员管理的协议，用来在IPv6主机和与其直连的组播设备之间建立、维护组播组成员关系。到目前为止，MLD有两个版本：MLDv1版本、MLDv2版本。所有MLD版本都支持ASM（Any-Source Multicast）模型。MLDv2版本可以直接应用于SSM（Source-Specific Multicast）模型，而MLDv1则需要通过使用SSM Mapping机制来支持SSM模型。
	二层组播: IGMP Snooping SSM Mapping IGMP Snooping Proxy MLD Snooping	二层组播是指组播数据在数据链路层上的传输。在二层设备上部署二层组播后，通过对上游三层设备和主机之间交互的IGMP/MLD协议报文进行侦听，建立数据链路层组播转发表，实现组播数据报文在数据链路层的按需分发，保障数据链路层组播业务的有效开展。

一级特性	二级特性	描述信息
MPLS	MPLS	MPLS位于TCP/IP协议栈中的链路层和网络层之间，用于向IP层提供连接服务，同时又从链路层得到服务。MPLS以标签交换替代IP转发。标签是一个短而定长的、只具有本地意义的连接标识符，与ATM的VPI/VCI以及Frame Relay的DLCI类似。标签封装在链路层和网络层之间。
	MPLS LDP: LDP 熵标签 LDP LSP BFD for LDP LDP CRC LDP MTU LDP over TE LDP GTSM mLdp mLDP P2MP BFD for P2MP Tunnel LDP 跨域扩展	LDP（Label Distribution Protocol，标签分发协议）是MPLS（Multi-Protocol Label Switching，多协议标签交换）的一种控制协议，相当于传统网络中的信令协议，负责FEC（Forwarding Equivalence Class，转发等价类）的分类、标签的分配以及LSP（Label Switched Path，标签交换路径）的建立和维护等操作。LDP规定了标签分发过程中的各种消息以及相关处理过程。
	MPLS TE: MPLS-TE RSVP-TE CR-LSP SRLG MPLS-TE 隧道保护组 BFD for TE CR-LSP BFD for TE Tunnel BFD for P2MP TE BFD for RSVP Self-Ping DS-TE 熵标签 CBTS P2MP TE	MPLS TE（MPLS Traffic Engineering），即MPLS流量工程。MPLS流量工程可以在不进行硬件升级的情况下对现有网络资源进行合理调配和利用，并对网络流量提供带宽和QoS保证，最大限度的节省运营商成本。由于其基于MPLS技术实现，因此易于在现有网络部署和维护。同时，MPLS流量工程具有丰富的可靠性技术，能够给运营商的骨干网络提供电信级和设备级的可靠性。

一级特性	二级特性	描述信息
Segment Routing	Segment Routing MPLS: Segment Routing MPLS SR-MPLS BE IS-IS for SR-MPLS OSPF for SR-MPLS SR-MPLS TE BGP for SR-MPLS 跨域E2E SR-MPLS TE IP over SR L3VPN over SR L2VPN over SR EVPN over SR SBFD for SR-MPLS SR-MPLS OAM SR-MPLS TE Policy MPLS in UDP SR-MPLS TTL	段路由SR（Segment Routing）是基于源路由理念而设计的在网络上转发数据包的一种协议。Segment Routing MPLS是指基于MPLS转发平面的Segment Routing，下文简称为Segment Routing。Segment Routing将网络路径分成一个个段，并且为这些段和网络中的转发节点分配段标识ID。通过对段和网络节点进行有序排列（Segment List），就可以得到一条转发路径。
	Segment Routing IPv6: 支持SRv6 Policy Over GRE隧道 SRv6 Policy 封装模式 ShortCut方式迭代SRv6 Policy SRv6 Policy Flow-Group引流 SRv6 Policy支持网络切片 SRv6 BE支持网络切片 SRv6 Policy支持头压缩 支持Ping/Tracert SRV6隧道不指定OP	SRv6（Segment Routing IPv6，基于IPv6转发平面的段路由）是基于源路由理念而设计的在网络上转发IPv6数据包的一种协议。SRv6通过在IPv6报文中插入一个路由扩展头SRH（Segment Routing Header），在SRH中压入一个显式的IPv6地址栈，并由中间节点不断的进行更新目的地址和偏移地址栈的操作来完成逐跳转发。

一级特性	二级特性	描述信息
VPN	VPN	虚拟专用网VPN（Virtual Private Network）是依靠Internet服务提供商ISP（Internet Service Provider）和网络服务提供商NSP（Network Service Provider）在公共网络中建立的虚拟专用通信网络。
	GRE： GRE mGRE	通用路由封装（GRE: Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在异构栈网络中进行传输，当前支持IPv4/IPv6 over GRE。
	L2TPv3	L2TP（Layer 2 Tunneling Protocol）协议结合了L2F（Layer 2 Forwarding）协议和PPTP（Point-to-Point Tunneling protocol）协议的优点，成为IETF有关二层隧道协议的工业标准。L2TP功能可以简单描述为在非点对点的网络上建立点对点的PPP会话连接。L2TPv3（Layer 2 Tunneling Protocol Version 3）是一种二层隧道技术，运用于CE（Customer Edge）端的二层接入链路在PSN网络中透明传递。
	TNLM： TNLM	隧道管理TNLM（Tunnel Management）是为管理隧道而设立的一个模块，是将隧道的状态通报给使用隧道的应用程序，并根据相关的配置为应用程序选择隧道。
	BGP/MPLS IP VPN： BGP/MPLS IP VPN Hub&Spoke Multi-VPN-Instance CE 跨域VPN 运营商的运营商 HVPN BGP SoO 公私网路由相互引入 BGP/MPLS IPv6 VPN 扩展 VPN双栈接入	BGP/MPLS IP VPN是一种L3VPN（Layer 3 Virtual Private Network）。它使用BGP（Border Gateway Protocol）在服务提供商骨干网上发布VPN路由，使用MPLS（Multiprotocol Label Switch）在服务提供商SP（Service Provider）骨干网上转发VPN报文。这里的IP是指服务提供商骨干网络是IP网络。

一级特性	二级特性	描述信息
	VPWS: VPWS CCC方式VPWS Martini方式VPWS SVC方式VPWS BGP方式VPWS L2VPN异种介质互通 VCCV VPWS跨域技术 VLL over SRV6	VPWS (Virtual Private Wire Service)：是指在分组交换网络PSN (Packet Switched Network) 中尽可能真实地模仿ATM、帧中继、以太网、低速TDM (Time Division Multiplexing) 电路和SONET (Synchronous Optical Network) /SDH (Synchronous Digital Hierarchy) 等业务的基本行为和特征的一种二层业务承载技术。VPWS是对传统租用线业务的仿真，使用IP网络模拟租用线，提供非对称、低成本的DDN (Digital Data Network) 业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于传统的租用线。VPWS技术是一种点到点的虚拟专线技术，能够支持几乎所有的链路层协议。
	VPLS: VPLS VPLS二层功能 LDP方式的VPLS BGP方式的VPLS HVPLS BGP AD VPLS VPLS跨域方式 组播VPLS VPLS Multi-homing VPLS业务隔离	VPLS称为虚拟专用局域网业务 (Virtual Private LAN Service)，是公用网络中提供的一种点到多点的L2VPN (Layer 2 Virtual Private Network) 业务，使地域上隔离的用户站点能通过MAN/WAN (Metropolitan Area Network/ Wide Area Network) 相连，并且使各个站点间的连接效果像在一个LAN (Local Area Network) 中一样。它是一种基于MPLS (MultiProtocol Label Switching) 和以太网的二层VPN技术，也被称为透明局域网业务TLS (Transparent LAN Service)。
	L2VPN接入L3VPN: VPWS接入L3VPN VPLS接入L3VPN	MPLS以其可靠性高、安全性好、基于IP层面具有好的运行维护能力和支持QoS (Quality of Service) 等优点，在城域网中得到了大量的应用。L2VPN (Layer 2 Virtual Private Network) 提供基于MPLS网络的二层VPN (Virtual Private Network) 服务，在MPLS网络上透明传输用户二层数据，能够为用户提供隧道化的路径，同时减少了中间设备需要维护的LSP (Label Switched Path) 链路。

一级特性	二级特性	描述信息
	EVPN: EVPN EVPN-MPLS EVPN多归技术 EVPN Seamless MPLS的基本原理 EVPN的服务模式 EVPN-VXLAN EVPN-VPWS PBB-EVPN EVPN E-Tree EVPN MAC迁移抑制 EVPN 6VPE EVPN拼接场景 跨域EVPN-Option C方式 BGP EVPN over E2E SR EVPN支持接入侧环网接入 EVPN支持MAC quality学习 支持基于EVPN VPLS模式下UMR (unknown-MAC-Route) 接入	EVPN (Ethernet Virtual Private Network) 是下一代全业务承载的VPN解决方案。EVPN统一了各种VPN业务的控制面，利用BGP扩展协议来传递二层或三层的可达性信息，实现了转发面和控制面的分离。
	PBB VPLS	PBB (Provider Backbone Bridges) 技术由IEEE 802.1ah规定，通过在用户MAC之前封装公网MAC，实现了用户网络与运营商网络的完全隔离。与传统的以太网局域网相比较，公网MAC与用户MAC分离，既保证了网络的稳定，也降低了对公网设备的MAC转发表项数量的需求；另外，PBB对业务实例 (帧格式的I-SID: 24bit) 的支持突破了4K VLAN ID的限制，能够满足以太网传送网对转发隧道数量的需求。
安全	AAA	AAA是Authentication (认证)、Authorization (授权) 和Accounting (计费) 的简称，提供了在网络接入服务器NAS (Network Access Server) 设备上配置访问控制的管理框架。

一级特性	二级特性	描述信息
	HWTACACS（仅支持配置，无法验证功能）	HWTACACS（Hua Wei Terminal Access Controller Access-Control System，华为终端访问控制器访问控制系统）基于TACACS+协议的标准开发，并加入了一些华为的私有属性，例如：用户组名、FTP目录、用户权限、用户接入类型。HWTACACS协议是为控制平面服务的华为终端访问控制器访问控制系统协议，为AAA提供了访问控制服务。（仅支持配置，无法验证功能）
	RADIUS（仅支持配置，无法验证功能）	RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证）协议是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未经授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。（仅支持配置，无法验证功能）
	NQA： NQA for IP(Ping/Trace/Jitter) NQA for MPLS(Ping/Trace/Jitter) NQA for VPN(Ping/Trace/Jitter) NQA MAC Ping	NQA（Network Quality Analysis），即网络质量分析，位于链路层之上，覆盖网络层、传输层和应用层，独立于底层硬件。NQA可以监测网络上运行的多种协议的性能，使运营商能够实时采集到各种网络运行指标，例如：TCP连接时延、报文丢包率、路径MTU等。通过对这些指标进行控制，运营商可以为用户提供不同等级的网络服务，收取不同的费用。同时，NQA也是网络故障诊断和定位的有效工具。
	Ping和Tracert： Ping/Tracert MPLS Ping/Tracert PW Ping/Tracert CE Ping EVPN MAC Ping GMAC Ping/Trace 802.1ag MAC Ping/Trace EVPN VPWS Ping/Tracert SRv6 SID Ping/Tracert SRv6 Policy Ping/Tracert	ping命令是最常见的用于检测网络设备可访问性的调试工具，它使用ICMP（Internet Control Message Protocol）的echo信息来决定远程设备是否可用或延迟情况或包丢失情况。tracert命令用于测试数据包从发送主机到目的地所经过的路径。当设备出现故障时，可以首先使用ping与tracert测试网络连接是否正常工作。

一级特性	二级特性	描述信息
	TWAMP: TWAMP for IP TWAMP for L3VPN TWAMP for L3VXLAN	TWAMP（Two-Way Active Measurement Protocol，双向主动测量协议）是一种用于IP链路性能测量技术，可以在正反两个方向进行双向的性能统计。TWAMP使用UDP数据包作为测量探针，统计网络双向延迟、抖动和丢包率。同时，该协议具有安全性，能够保证控制和测量功能的分离。通过已经部署TWAMP协议的网络设备之间的合作，有效地获取设备间IP性能统计数据。
IPv6过渡技术	IPv4 over IPv6隧道技术	IPv4 over IPv6隧道指在IPv6网络上用于连接IPv4局部网络的隧道。
	IPv6 over IPv4隧道技术	IPv6 over IPv4隧道指在IPv4网络上用于连接IPv6局部网络的隧道。

2.3.2 CE 交换机模拟器

CE交换机模拟器支持的特性如表2-3所示。

表 2-3 CE 交换机模拟器支持的特性

一级特性	二级特性	描述信息
基础与维护	TTY	终端类型TTY（Terminal Type）也叫做终端服务，为用户配置设备时提供接入接口和人机交互机制。
	Telnet	Telnet（Telecommunication Network Protocol）起源于1969年的ARPANET，是一种最早的Internet应用。Telnet连接是一种TCP（Transmission Control Protocol）连接，用来传输数据和少量的Telnet控制信息。Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端。Telnet采用客户端/服务器模式。

一级特性	二级特性	描述信息
	SSH	Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet和FTP通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH（Secure Shell）是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。
	CLI	命令行接口CLI（Command Line Interface）是用户与设备进行交互的常用工具。用户登录到设备出现命令行提示符后，即进入命令行接口。系统向用户提供一系列命令，用户可以通过命令行接口输入命令，由命令行接口对命令进行解析，实现用户对设备的配置和管理。
	FS： FTP TFTP	FTP协议是一种基于TCP/IP协议族的Internet标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP采用两条TCP连接将一个文件从一个系统复制到另一个系统，连接通常是以客户-服务器的方式建立，这两条TCP连接分别是控制连接（服务器端为21号端口）和数据连接（服务器端为20号端口）。 TFTP（Trivial File Transfer Protocol）即简单文件传送协议，属于UDP（User Datagram Protocol）协议，使用69号端口。TFTP客户端通过发送请求给TFTP服务器来读、写文件和建立连接。文件以固定的长度传输，长度为512字节。小于512字节的数据包表示至此传输结束。每个数据包包含一个数据块，在传输过程中出现数据丢失时该数据块可以控制是否重新传输。
	CFG	为满足业务需求用户对系统进行的一系列命令行操作，将这些操作进行保存然后重启系统依然能够继续生效。

一级特性	二级特性	描述信息
	AAA用户管理	AAA（Authentication Authorization Accounting）是一种提供认证、授权和计费的技术。认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。授权（Authorization）：授权用户可以使用哪些服务。计费（Accounting）：记录用户使用网络资源的情况。
网络可靠性	VRRP	虚拟路由冗余协议VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由设备出现故障时，及时将业务切换到备份路由设备，从而保持通讯的连续性和可靠性。VRRP是相关标准定义的一种冗余容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。
接口管理	接口管理配置： 二层以太网接口 三层以太网接口 TRUNK接口 Hybrid接口 三层以太子接口 VLANIF接口 BDIF接口	接口管理。接口是该设备与网络中的其它设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类：物理接口是真实存在、有器件支持的接口；逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。
以太网交换	STP/MSTP	以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，并导致广播风暴以及MAC地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议STP（Spanning Tree Protocol）。RSTP在STP基础上进行了改进，实现了网络拓扑快速收敛。
	Bridge Domain	Bridge Domain用来创建用来创建广播域桥域BD桥域BD,在VXLAN网络中,广播域统一表现为BD，将二层子接口关联BD后，可实现数据报文通过BD转发。
	MAC转发	支持基本的MAC学习与老化，基于MAC做的基础的二层转发。
	VLAN转发	支持基础VLAN功能，支持基于接口/基于MAC划分VLAN，实现基于VLAN+MAC的二层转发。

一级特性	二级特性	描述信息
	Eth-Trunk	Eth-trunk通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。捆绑在一起的链路通过相互间的动态备份，可以有效地提高链路的可靠性。
	LACP	LACP（Link Aggregation Control Protocol，链路聚合控制协议），ETH-TRUNK的管理控制协议，实现动态的链路捆绑及负载分担功能。
VXLAN	VXLAN	VXLAN是NVO3中的一种网络虚拟化技术，通过将虚拟机发出的数据包封装在UDP中，并使用物理网络的IP、MAC作为outer-header进行封装，然后在IP网络上传输，到达目的地后由隧道终结点解封装并将数据发送给目标虚拟机。 • VXLAN L2转发。 • VXLAN L3网关。 • VXLAN 三层转发（动态VXLAN隧道）。 • IPv6 VXLAN 三层转发（动态VXLAN隧道）。
IP业务	IPv4基础	IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议。它工作在TCP/IP协议栈的互联网络层。该层与OSI参考模型的网络层相对应。IP层将信息分割成数据单元，并添加地址信息和控制信息，使得数据包能够按照路由转发。IP层提供的是不可靠、无连接数据传输服务。不可靠的意思是它不能保证IP数据报能成功地到达目的地。IP仅提供最好的传输服务。如果发生某种错误时，如某个设备暂时用完了缓冲区，IP会丢弃该数据报，然后发送ICMP消息报给信源端。任何要求的可靠性必须由上层来提供（如TCP）。无连接的意思是IP并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP数据报可以不按发送顺序接收。如果一信源向相同的信宿发送两个连续的数据报（先是A，然后是B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此B可能在A到达之前先到达。

一级特性	二级特性	描述信息
	IPv6基础	IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。它是IETF（Internet工程任务组）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制在未来的市场竞争中充满了活力。
	负载分担	当存在多条不同链路到达同一目的地址的网络环境中，通过负载分担(ECMP)可以有效地增加传输带宽，提升链接可靠性。
	MTU	最大传输单元（Maximum Transmission Unit，MTU），用于控制链路上可承载的报文的最大有效载荷，设备会根据MTU对报文进行分片，以保障报文可以在链路上正常传输。
	DHCP	动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议应用于IPv4网络的地址申请和动态配置。支持DHCP Client通过DHCP获得ip地址，但不支持通过DHCP获得server端ip pool 中的DNS server信息。
IP路由	OSPF	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。
	OSPFv3	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。OSPFv3在OSPFv2基础上进行了增强，是一个独立的路由协议。

一级特性	二级特性	描述信息
	BGP	BGP（Border Gateway Protocol）是一种用于自治系统AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，主要用于交换AS之间的可达路由信息，构建AS域间的传播路径，防止路由环路产生，并在AS级别应用一些路由策略。当前使用的版本是BGP-4。BGP作为事实上的Internet外部路由协议标准，被广泛应用于ISP（Internet Service Provider）之间。
	IS-IS	IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）最初是国际标准化组织ISO（the International Organization for Standardization）为它的无连接网络协议CLNP（ConnectionLess Network Protocol）设计的一种动态路由协议。随着TCP/IP协议的流行，为了提供对IP路由的支持，IETF在相关标准中对IS-IS进行了扩充和修改，使它能够在同时应用在TCP/IP和OSI环境中，称为集成IS-IS（Integrated IS-IS或Dual IS-IS）。
	RIP	RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议IGP（Interior Gateway Protocol），主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP是一种基于距离矢量（Distance-Vector）算法的协议，它通过UDP报文进行路由信息的交换，使用的端口号为520。RIP使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在RIP中，缺省情况下，设备到与它直接相连网络的跳数为0，通过一个设备可达的网络的跳数为1，其余依此类推。也就是说，度量值等于从本网络到达目的网络间的设备数量。为限制收敛时间，RIP规定度量值取0～15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。

一级特性	二级特性	描述信息
	RIPng	RIPng（RIP next generation，下一代RIP协议）是对原来的IPv4网络中RIP version 2协议在IPv6网络上的扩展，大多数RIP的概念都可以应用于RIPng。RIPng协议是基于D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在RIPng协议中，从一个设备到其直连网络的跳数为0，到通过另一台设备可达的网络的跳数为1，如此类推，当跳数大于或等于16时，目的网络或主机就被定义为不可达。
VPN	GRE	通用路由封装（GRE: Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在异构栈网络中进行传输，当前支持IPv4/IPv6 over GRE。
IPv6过渡技术	IPv6 over IPv4隧道	IPv6 over IPv4隧道指在IPv4网络上用于连接IPv6局部网络的隧道。
	IPv4 & IPv6双栈协议	IPv4 & IPv6双栈协议。

2.3.3 S 交换机模拟器

S交换机模拟器支持的特性如表2-4所示。

表 2-4 S 交换机模拟器支持的特性

一级特性	二级特性	描述信息
基础与维护	TTY	终端类型TTY（Terminal Type）也叫做终端服务，为用户配置设备时提供接入接口和人机交互机制。
	Telnet	Telnet（Telecommunication Network Protocol）起源于1969年的ARPANET，是一种最早的Internet应用。Telnet连接是一种TCP（Transmission Control Protocol）连接，用来传输数据和少量的Telnet控制信息。Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端。Telnet采用客户端/服务器模式。

一级特性	二级特性	描述信息
	SSH	Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet和FTP通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH（Secure Shell）是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。
	CLI	命令行接口CLI（Command Line Interface）是用户与设备进行交互的常用工具。用户登录到设备出现命令行提示符后，即进入命令行接口。系统向用户提供一系列命令，用户可以通过命令行接口输入命令，由命令行接口对命令进行解析，实现用户对设备的配置和管理。
	FS： FTP TFTP	FTP协议是一种基于TCP/IP协议族的Internet标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP采用两条TCP连接将一个文件从一个系统复制到另一个系统，连接通常是以客户-服务器的方式建立，这两条TCP连接分别是控制连接（服务器端为21号端口）和数据连接（服务器端为20号端口）。 TFTP（Trivial File Transfer Protocol）即简单文件传送协议，属于UDP（User Datagram Protocol）协议，使用69号端口。TFTP客户端通过发送请求给TFTP服务器来读、写文件和建立连接。文件以固定的长度传输，长度为512字节。小于512字节的数据包表示至此传输结束。每个数据包包含一个数据块，在传输过程中出现数据丢失时该数据块可以控制是否重新传输。
	CFG	为满足业务需求用户对系统进行的一系列命令行操作，将这些操作进行保存然后重启系统依然能够继续生效。

一级特性	二级特性	描述信息
	AAA用户管理	AAA（Authentication Authorization Accounting）是一种提供认证、授权和计费的技术。认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。授权（Authorization）：授权用户可以使用哪些服务。计费（Accounting）：记录用户使用网络资源的情况。
网络可靠性	VRRP	虚拟路由冗余协议VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由设备出现故障时，及时将业务切换到备份路由设备，从而保持通讯的连续性和可靠性。VRRP是相关标准定义的一种冗余容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。
接口管理	接口管理配置	接口管理。接口是该设备与网络中的其它设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类：物理接口是真实存在、有器件支持的接口；逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。
以太网交换	STP/MSTP	以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，并导致广播风暴以及MAC地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议STP（Spanning Tree Protocol）。RSTP在STP基础上进行了改进，实现了网络拓扑快速收敛。
	Bridge Domain	Bridge Domain用来创建用来创建广播域桥域BD桥域BD,在VXLAN网络中,广播域统一表现为BD，将二层子接口关联BD后，可实现数据报文通过BD转发。
	MAC转发	支持基本的MAC学习与老化，基于MAC做的基础的二层转发。
	VLAN转发	支持基础VLAN功能，支持基于接口/基于MAC划分VLAN，实现基于VLAN+MAC的二层转发。

一级特性	二级特性	描述信息
IP业务	Eth-Trunk	Eth-trunk通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。捆绑在一起的链路通过相互间的动态备份，可以有效地提高链路的可靠性。
	LACP	LACP（Link Aggregation Control Protocol，链路聚合控制协议），ETH-TRUNK的管理控制协议，实现动态的链路捆绑及负载分担功能。
	IPv4基础	IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议。它工作在TCP/IP协议栈的互联网络层。该层与OSI参考模型的网络层相对应。IP层将信息分割成数据单元，并添加地址信息和控制信息，使得数据包能够按照路由转发。IP层提供的是不可靠、无连接数据传输服务。不可靠的意思是它不能保证IP数据报能成功地到达目的地。IP仅提供最好的传输服务。如果发生某种错误时，如某个设备暂时用完了缓冲区，IP会丢弃该数据报，然后发送ICMP消息报给信源端。任何要求的可靠性必须由上层来提供（如TCP）。无连接的意思是IP并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP数据报可以不按发送顺序接收。如果一信源向相同的信宿发送两个连续的数据报（先是A，然后是B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此B可能在A到达之前先到达。
	IPv6基础	IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。它是IETF（Internet工程任务组）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版本。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制在未来的市场竞争中充满了活力。
	负载分担	当存在多条不同链路到达同一目的地址的网络环境中，通过负载分担（ECMP）可以有效地增加传输带宽，提升链接可靠性。

一级特性	二级特性	描述信息
	MTU	最大传输单元（Maximum Transmission Unit，MTU），用于控制链路上可承载的报文的最大有效载荷，设备会根据MTU对报文进行分片，以保障报文可以在链路上正常传输。
	DHCP	动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议应用于IPv4网络的地址申请和动态配置。 支持DHCP Client通过DHCP 获得ip地址，但不支持通过DHCP获得server端ip pool 中的DNS server信息。
IP路由	OSPF	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。
	OSPFv3	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。OSPFv3在OSPFv2基础上进行了增强，是一个独立的路由协议。
	BGP	BGP（Border Gateway Protocol）是一种用于自治系统AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，主要用于交换AS之间的可达路由信息，构建AS域间的传播路径，防止路由环路产生，并在AS级别应用一些路由策略。当前使用的版本是BGP-4。BGP作为事实上的Internet外部路由协议标准，被广泛应用于ISP（Internet Service Provider）之间。

一级特性	二级特性	描述信息
	IS-IS	IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）最初是国际标准化组织ISO（the International Organization for Standardization）为它的无连接网络协议CLNP（ConnectionLess Network Protocol）设计的一种动态路由协议。随着TCP/IP协议的流行，为了提供对IP路由的支持，IETF在相关标准中对IS-IS进行了扩充和修改，使它能够同时应用在TCP/IP和OSI环境中，称为集成IS-IS（Integrated IS-IS或Dual IS-IS）。
	RIP	RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议IGP（Interior Gateway Protocol），主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP是一种基于距离矢量（Distance-Vector）算法的协议，它通过UDP报文进行路由信息的交换，使用的端口号为520。RIP使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在RIP中，缺省情况下，设备到与它直接相连网络的跳数为0，通过一个设备可达的网络的跳数为1，其余依此类推。也就是说，度量值等于从本网络到达目的网络间的设备数量。为限制收敛时间，RIP规定度量值取0～15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。
	RIPng	RIPng（RIP next generation，下一代RIP协议）是对原来的IPv4网络中RIP version 2协议在IPv6网络上的扩展，大多数RIP的概念都可以应用于RIPng。RIPng协议是基于D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在RIPng协议中，从一个设备到其直连网络的跳数为0，到通过另一台设备可达的网络的跳数为1，如此类推，当跳数大于或等于16时，目的网络或主机就被定义为不可达。

一级特性	二级特性	描述信息
VPN	GRE	通用路由封装（GRE: Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在异构栈网络中进行传输, 当前 支持IPv4/IPv6 over GRE。
IPv6过渡技术	IPv6 over IPv4隧道	IPv6 over IPv4隧道指在IPv4网络上用于连接IPv6局部网络的隧道。
	IPv4 & IPv6双栈协议	IPv4 & IPv6双栈协议。

2.3.4 AR 路由器模拟器

AR路由器模拟器支持的特性如[表2-5](#)所示。

表 2-5 AR 路由器模拟器支持的特性

一级特性	二级特性	描述信息
基础与维护	TTY	终端类型TTY（Terminal Type）也叫做终端服务，为用户配置设备时提供接入接口和人机交互机制。
	Telnet	Telnet（Telecommunication Network Protocol）起源于1969年的ARPANET，是一种最早的Internet应用。Telnet连接是一种TCP（Transmission Control Protocol）连接，用来传输数据和少量的Telnet控制信息。Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端。Telnet采用客户端/服务器模式。

一级特性	二级特性	描述信息
	SSH	Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet和FTP通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH（Secure Shell）是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。
	CLI	命令行接口CLI（Command Line Interface）是用户与路由器进行交互的常用工具。用户登录到路由器出现命令行提示符后，即进入命令行接口。系统向用户提供一系列命令，用户可以通过命令行接口输入命令，由命令行接口对命令进行解析，实现用户对路由器的配置和管理。
	FS： FTP TFTP	FTP协议是一种基于TCP/IP协议族的Internet标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP采用两条TCP连接将一个文件从一个系统复制到另一个系统，连接通常是以客户-服务器的方式建立，这两条TCP连接分别是控制连接（服务器端为21号端口）和数据连接（服务器端为20号端口）。 TFTP（Trivial File Transfer Protocol）即简单文件传送协议，属于UDP（User Datagram Protocol）协议，使用69号端口。TFTP客户端通过发送请求给TFTP服务器来读、写文件和建立连接。文件以固定的长度传输，长度为512字节。小于512字节的数据包表示至此传输结束。每个数据包包含一个数据块，在传输过程中出现数据丢失时该数据块可以控制是否重新传输。
	CFG	为满足业务需求用户对系统进行的一系列命令行操作，将这些操作进行保存然后重启系统依然能够继续生效。

一级特性	二级特性	描述信息
	AAA用户管理	AAA（Authentication Authorization Accounting）是一种提供认证、授权和计费的技术。认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。授权（Authorization）：授权用户可以使用哪些服务。计费（Accounting）：记录用户使用网络资源的情况。
网络可靠性	VRRP	虚拟路由冗余协议VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由设备出现故障时，及时将业务切换到备份路由设备，从而保持通讯的连续性和可靠性。VRRP是相关标准定义的一种冗余容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。
接口管理	接口管理配置	接口管理。接口是该设备与网络中的其它设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类：物理接口是真实存在、有器件支持的接口；逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。
IP业务	IPv4基础	IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议。它工作在TCP/IP协议栈的互联网络层。该层与OSI参考模型的网络层相对应。IP层将信息分割成数据单元，并添加地址信息和控制信息，使得数据包能够按照路由转发。IP层提供的是不可靠、无连接数据传输服务。不可靠的意思是它不能保证IP数据报能成功地到达目的地。IP仅提供最好的传输服务。如果发生某种错误时，如某个路由器暂时用完了缓冲区，IP会丢弃该数据报，然后发送ICMP消息报给信源端。任何要求的可靠性必须由上层来提供（如TCP）。无连接的意思是IP并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP数据报可以不按发送顺序接收。如果一信源向相同的信宿发送两个连续的数据报（先是A，然后是B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此B可能在A到达之前先到达。

一级特性	二级特性	描述信息
	IPv6基础	IPv6（ Internet Protocol Version 6 ）是网络层协议的第二代标准协议，也被称为IPng（ IP Next Generation ）。它是IETF（ Internet工程任务组 ）设计的一套规范，是IPv4（ Internet Protocol Version 4 ）的升级版。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制在未来的市场竞争中充满了活力。
	负载分担	当存在多条不同链路到达同一目的地址的网络环境中，通过负载分担(ECMP)可以有效地增加传输带宽，提升链接可靠性。
	MTU	最大传输单元（ Maximum Transmission Unit， MTU ）,用于控制链路上可承载的报文的最大有效载荷，设备会根据MTU对报文进行分片，以保障报文可以在链路上正常传输。
	DHCP	动态主机配置协议DHCP（ Dynamic Host Configuration Protocol ）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议应用于IPv4网络的地址申请和动态配置。 支持DHCP Client通过DHCP 获得ip地址，但不支持通过DHCP获得server端ip pool 中的DNS server信息。

一级特性	二级特性	描述信息
	NAT	IPv4地址空间接近枯竭，公网地址短缺情况日益严重，网络中存在大量的服务和应用还是使用IPv4，切换到IPv6需要较长的周期，通过NAT技术可以通过私网地址到公网地址的映射，达到公网地址的统计复用，从而在相当长的时间内解决IPv4地址短缺问题。 • NAT: 适合大量的私网用户访问Internet场景。大量私网地址转换为少量公网地址，在转换过程中同时转换报文的地址和端口。 • Easy IP: 适合公网接口通过拨号方式动态获取公网地址，转换后IP地址不固定，无法在NAT地址池中配置固定的地址场景。或申请到的静态公网地址仅可用于配置公网接口，无法在NAT地址池中配置固定地址段的场景。 • NAT Server: 适用于私网地址与公网地址、私网地址与公网端口、私网端口与公网地址、私网端口与公网端口存在固定映射关系场景。通过配置nat server命令实现。 • 双向NAT: 适合源和目的地址同时需要转换，且目的地址转换前后存在固定映射关系的场景。需要分别配置源NAT策略和nat server命令实现。
IP路由	OSPF	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。
	OSPFv3	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。 OSPFv3在OSPFv2基础上进行了增强，是一个独立的路由协议。

一级特性	二级特性	描述信息
	BGP	BGP（Border Gateway Protocol）是一种用于自治系统AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，主要用于交换AS之间的可达路由信息，构建AS域间的传播路径，防止路由环路产生，并在AS级别应用一些路由策略。当前使用的版本是BGP-4。BGP作为事实上的Internet外部路由协议标准，被广泛应用于ISP（Internet Service Provider）之间。
	RIP	RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议IGP（Interior Gateway Protocol），主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP是一种基于距离矢量（Distance-Vector）算法的协议，它通过UDP报文进行路由信息的交换，使用的端口号为520。RIP使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在RIP中，缺省情况下，路由器到与它直接相连网络的跳数为0，通过一个路由器可达的网络的跳数为1，其余依此类推。也就是说，度量值等于从本网络到达目的网络间的路由器数量。为限制收敛时间，RIP规定度量值取0~15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。
	RIPng	RIPng（RIP next generation，下一代RIP协议）是对原来的IPv4网络中RIP version 2协议在IPv6网络上的扩展，大多数RIP的概念都可以应用于RIPng。RIPng协议是基于D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在RIPng协议中，从一个设备到其直连网络的跳数为0，到通过另一台设备可达的网络的跳数为1，如此类推，当跳数大于或等于16时，目的网络或主机就被定义为不可达。
VPN	GRE	通用路由封装（GRE: Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在异构栈网络中进行传输，当前支持IPv4/IPv6 over GRE。

一级特性	二级特性	描述信息
IPv6过渡技术	IPv6 over IPv4隧道	IPv6 over IPv4隧道指在IPv4网络上用于连接IPv6局部网络的隧道。
	IPv4 & IPv6双栈协议	IPv4 & IPv6双栈协议。
QoS	MQC	MQC(Modular QoS)，华为提供的模块化QoS命令行接口，可以简化用户QoS功能配置的配置工作量。
	流量监管	流量监管TP（Traffic Policing）是监督不同流量进入网络的速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。
	流量整形	流量整形TS（Traffic Shaping）是一种主动调整流量输出速率的措施，将上游不规整的流量进行削峰填谷，使流量输出比较平稳，从而解决下游设备的拥塞问题。
	拥塞管理	拥塞管理就是在网络间歇性出现拥塞，时延敏感业务要求得到比其他业务更高质量的QoS服务时，通过调整报文的调度次序来满足时延敏感业务高QoS服务的一种拥塞控制机制。通常使用队列技术来解决拥塞，主要的队列技术包含： • FIFO（First In First Out，先进先出）队列。 • PQ（Priority Queuing，优先队列）。 • CQ（Custom Queuing，定制队列）。 • WFQ（Weighted Fair Queuing，加权公平队列）。 • CBWFQ（Class Based Weighted Fair Queuing，基于类的加权公平队列）。
	拥塞避免	拥塞避免是指通过监控网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种拥塞控制机制。常用的两种丢弃报文方式为尾丢弃（Tail Drop）和WRED（Weighted Random Early Detection）。

一级特性	二级特性	描述信息
系统监控	NQA	NQA（ Network Quality Analysis ），即网络质量分析，位于链路层之上，覆盖网络层、传输层和应用层，独立于底层硬件。NQA可以监测网络上运行的多种协议的性能，使运营商能够实时采集到各种网络运行指标，例如：TCP连接时延、报文丢包率、路径MTU等。通过对这些指标进行控制，运营商可以为用户提供不同等级的网络服务，收取不同的费用。同时，NQA也是网络故障诊断和定位的有效工具。

2.3.5 USG 防火墙模拟器

USG防火墙模拟器支持的特性如表2-6所示。

表 2-6 USG 防火墙模拟器支持的特性

一级特性	二级特性	描述信息
基础与维护	TTY	终端类型TTY（ Terminal Type ）也叫做终端服务，为用户配置设备时提供接入接口和人机交互机制。
	Telnet	Telnet（ Telecommunication Network Protocol ）起源于1969年的ARPANET，是一种最早的Internet应用。Telnet连接是一种TCP（ Transmission Control Protocol ）连接，用来传输数据和少量的Telnet控制信息。Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端。Telnet采用客户端/服务器模式。

一级特性	二级特性	描述信息
	SSH	Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet和FTP通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH（Secure Shell）是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。
	CLI	命令行接口CLI（Command Line Interface）是用户与设备进行交互的常用工具。用户登录到设备出现命令行提示符后，即进入命令行接口。系统向用户提供一系列命令，用户可以通过命令行接口输入命令，由命令行接口对命令进行解析，实现用户对设备的配置和管理。
	FS： FTP TFTP	FTP协议是一种基于TCP/IP协议族的Internet标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP采用两条TCP连接将一个文件从一个系统复制到另一个系统，连接通常是以客户-服务器的方式建立，这两条TCP连接分别是控制连接（服务器端为21号端口）和数据连接（服务器端为20号端口）。 TFTP（Trivial File Transfer Protocol）即简单文件传送协议，属于UDP（User Datagram Protocol）协议，使用69号端口。TFTP客户端通过发送请求给TFTP服务器来读、写文件和建立连接。文件以固定的长度传输，长度为512字节。小于512字节的数据包表示至此传输结束。每个数据包包含一个数据块，在传输过程中出现数据丢失时该数据块可以控制是否重新传输。
	CFG	为满足业务需求用户对系统进行的一系列命令行操作，将这些操作进行保存然后重启系统依然能够继续生效。

一级特性	二级特性	描述信息
	AAA用户管理	AAA（Authentication Authorization Accounting）是一种提供认证、授权和计费的技术。认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。授权（Authorization）：授权用户可以使用哪些服务。计费（Accounting）：记录用户使用网络资源的情况。
网络可靠性	VRRP	虚拟路由冗余协议VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由设备出现故障时，及时将业务切换到备份路由设备，从而保持通讯的连续性和可靠性。VRRP是相关标准定义的一种冗余容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。
接口管理	接口管理配置	接口管理。接口是该设备与网络中的其它设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类：物理接口是真实存在、有器件支持的接口；逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。
IP业务	IPv4基础	IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议。它工作在TCP/IP协议栈的互联网络层。该层与OSI参考模型的网络层相对应。IP层将信息分割成数据单元，并添加地址信息和控制信息，使得数据包能够按照路由转发。IP层提供的是不可靠、无连接数据传输服务。不可靠的意思是它不能保证IP数据报能成功地到达目的地。IP仅提供最好的传输服务。如果发生某种错误时，如某个设备暂时用完了缓冲区，IP会丢弃该数据报，然后发送ICMP消息报给信源端。任何要求的可靠性必须由上层来提供（如TCP）。无连接的意思是IP并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP数据报可以不按发送顺序接收。如果一信源向相同的信宿发送两个连续的数据报（先是A，然后是B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此B可能在A到达之前先到达。

一级特性	二级特性	描述信息
	IPv6基础	IPv6（ Internet Protocol Version 6 ）是网络层协议的第二代标准协议，也被称为IPng（ IP Next Generation ）。它是IETF（ Internet工程任务组 ）设计的一套规范，是IPv4（ Internet Protocol Version 4 ）的升级版。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制在未来的市场竞争中充满了活力。
	负载分担	当存在多条不同链路到达同一目的地址的网络环境中，通过负载分担(ECMP)可以有效地增加传输带宽，提升链接可靠性。
	MTU	最大传输单元（ Maximum Transmission Unit， MTU ），用于控制链路上可承载的报文的最大有效载荷，设备会根据MTU对报文进行分片，以保障报文可以在链路上正常传输。
	DHCP	动态主机配置协议DHCP（ Dynamic Host Configuration Protocol ）是一种用于集中对用户IP地址进行动态管理和配置的协议。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等相应的配置信息，以实现IP地址等信息的动态配置。DHCP协议应用于IPv4网络的地址申请和动态配置。 支持DHCP Client通过DHCP 获得ip地址，但不支持通过DHCP获得server端ip pool 中的DNS server信息。

一级特性	二级特性	描述信息
	NAT	IPv4地址空间接近枯竭，公网地址短缺情况日益严重，网络中存在大量的服务和应用还是使用IPv4，切换到IPv6需要较长的周期，通过NAT技术可以通过私网地址到公网地址的映射，达到公网地址的统计复用，从而在相当长的时间内解决IPv4地址短缺问题。 • NAPT: 适合大量的私网用户访问Internet场景。大量私网地址转换为少量公网地址，在转换过程中同时转换报文的地址和端口。 • Easy IP: 适合公网接口通过拨号方式动态获取公网地址，转换后IP地址不固定，无法在NAT地址池中配置固定的地址场景。或申请到的静态公网地址仅可用于配置公网接口，无法在NAT地址池中配置固定地址段的场景。 • NAT Server: 适用于私网地址与公网地址、私网地址与公网端口、私网端口与公网地址、私网端口与公网端口存在固定映射关系场景。通过配置nat server命令实现。 • 双向NAT: 适合源和目的地址同时需要转换，且目的地址转换前后存在固定映射关系的场景。需要分别配置源NAT策略和nat server命令实现。
IP路由	OSPF	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。
	OSPFv3	OSPF（Open Shortest Path First）是IETF（Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议IGP（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2，针对IPv6协议使用OSPF Version 3。 OSPFv3在OSPFv2基础上进行了增强，是一个独立的路由协议。

一级特性	二级特性	描述信息
	BGP	BGP（Border Gateway Protocol）是一种用于自治系统AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，主要用于交换AS之间的可达路由信息，构建AS域间的传播路径，防止路由环路产生，并在AS级别应用一些路由策略。当前使用的版本是BGP-4。BGP作为事实上的Internet外部路由协议标准，被广泛应用于ISP（Internet Service Provider）之间。
	RIP	RIP是Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议IGP（Interior Gateway Protocol），主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP是一种基于距离矢量（Distance-Vector）算法的协议，它通过UDP报文进行路由信息的交换，使用的端口号为520。RIP使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在RIP中，缺省情况下，设备到与它直接相连网络的跳数为0，通过一个设备可达的网络的跳数为1，其余依此类推。也就是说，度量值等于从本网络到达目的网络间的设备数量。为限制收敛时间，RIP规定度量值取0~15之间的整数，大于或等于16的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。
	RIPng	RIPng（RIP next generation，下一代RIP协议）是对原来的IPv4网络中RIP version 2协议在IPv6网络上的扩展，大多数RIP的概念都可以应用于RIPng。RIPng协议是基于D-V（Distance Vector，距离矢量）算法的路由协议，用跳数来衡量到达目的主机的距离（也称为度量值或开销）。在RIPng协议中，从一个设备到其直连网络的跳数为0，到通过另一台设备可达的网络的跳数为1，如此类推，当跳数大于或等于16时，目的网络或主机就被定义为不可达。
VPN	GRE	通用路由封装（GRE: Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在异构栈网络中进行传输，当前支持IPv4/IPv6 over GRE。

一级特性	二级特性	描述信息
IPv6过渡技术	IPv6 over IPv4隧道	IPv6 over IPv4隧道指在IPv4网络上用于连接IPv6局部网络的隧道。
	IPv4 & IPv6双栈协议	IPv4 & IPv6双栈协议。

2.3.6 客户端模拟器（PC-Client）

客户端模拟器支持的特性如表2-7所示。

表 2-7 客户端模拟器支持的特性

设备特性	描述信息
基础IP特性	支持配置IP属性，包括地址、掩码等
DHCP	支持动态主机配置协议
命令行	支持Linux命令行

2.3.7 服务端模拟器（PC-Server）

服务端模拟器支持的特性如表2-8所示。

表 2-8 服务端模拟器支持的特性

设备特性	描述信息
基础IP特性	支持配置IP属性，包括地址、掩码等
HTTP	支持超文本传输协议
DHCP	支持动态主机配置协议
DNS	支持DNS服务
FTP	支持文件传输协议

3 软件安装

3.1 软件获取

- 华为技术支持网站：
- 运营商用户请登录[运营业务网站](#)，搜索并选择“eNSP Pro”。
 - 企业用户请登录[企业业务网站](#)，搜索并选择“eNSP Pro”。

须知

软件完整性验证指南：

华为为软件提供PGP和CMS格式的数字签名，分别用于人工和系统自动验证软件包的完整性。请您下载软件时同步下载数字签名，在软件使用前进行数字签名验证。

人工签名验证：使用PGPVerify或开源软件进行验证（[OpenPGP验证指南与工具](#)）。

自动签名验证：与软件同步上传网管/部署工具，由网管/部署工具进行验证。

3.2 硬件要求

数通模拟器支持在个人PC和物理服务器上部署安装，硬件要求如[表3-1](#)所示。

表 3-1 硬件配置要求

硬件	推荐配置
CPU	X86_64架构CPU，支持VT-x/AMD-V 8核或以上
内存	16G或以上
磁盘	40G

 说明

常见8核16G内存电脑支持模拟3台~6台设备，如需大规模组网，建议使用高规格服务器部署。

3.3 设备规格要求

设备内存和CPU规格要求如表3-2所示。

表 3-2 设备规格

设备	内存占用/台	使用CPU个数/台
NE路由器	2G	2
CE交换机	2G	2
S交换机	2G	2
AR路由器	2.5G	2
USG防火墙	2.5G	2.5
PC终端	250MB	0.2

3.4 数通模拟器部署

3.4.1 部署数通模拟器（Windows 系统）

3.4.1.1 软件要求

数通模拟器支持在虚拟机上安装，软件要求如表3-3所示。

表 3-3 软件配置要求

软件	推荐配置
浏览器	Chrome浏览器97或以上版本

3.4.1.2 部署虚拟机

前提条件

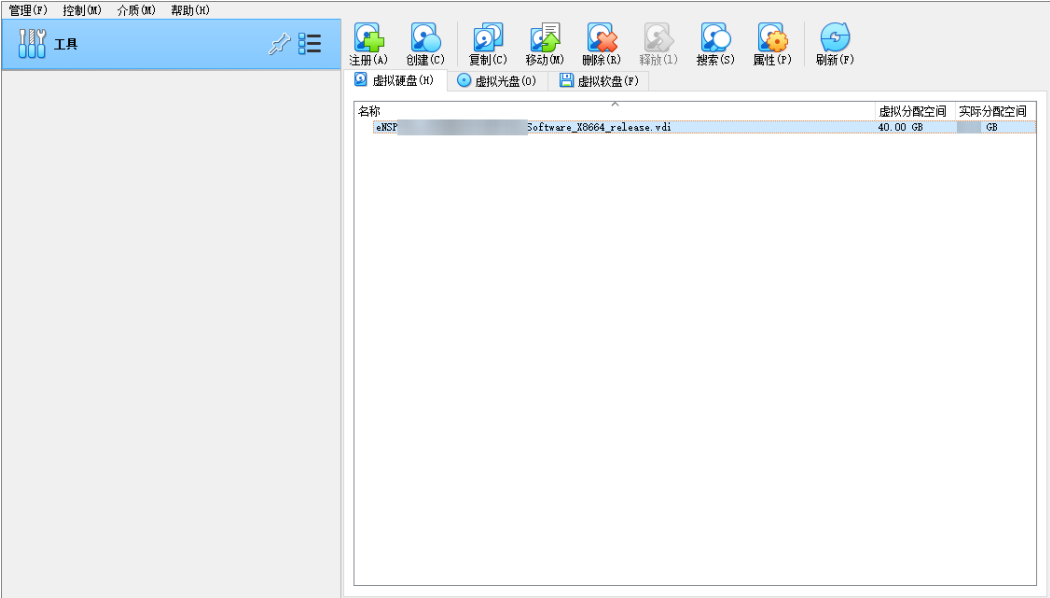
个人PC已经安装虚拟机和Chrome浏览器。

操作步骤

步骤1 解压下载的eNSP**_Software_X8664_release.tar.gz得到eNSP**_Software_X8664_release.vdi。

步骤2 注册虚拟硬盘。启动虚拟机，选择“管理 > 工具 > 虚拟介质管理”，单击注册(A)，选择解压后的eNSP*_Software_X8664_release.vdi，如图3-1所示。

图 3-1 注册



步骤3 新建虚拟机。

1. 选择“控制 > 新建”，填写界面参数，参数说明见表3-4所示，单击“Next”，如图3-2所示。

图 3-2 虚拟机名称和操作系统

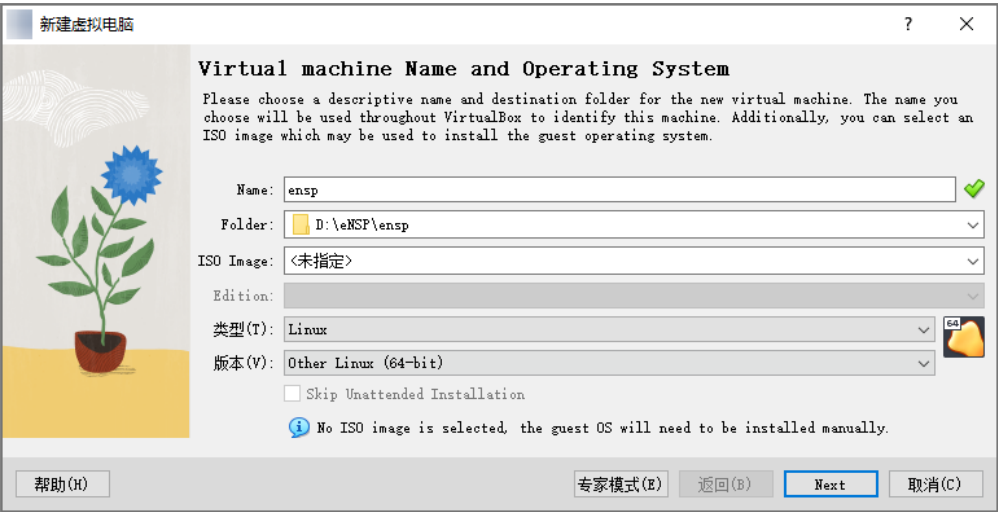


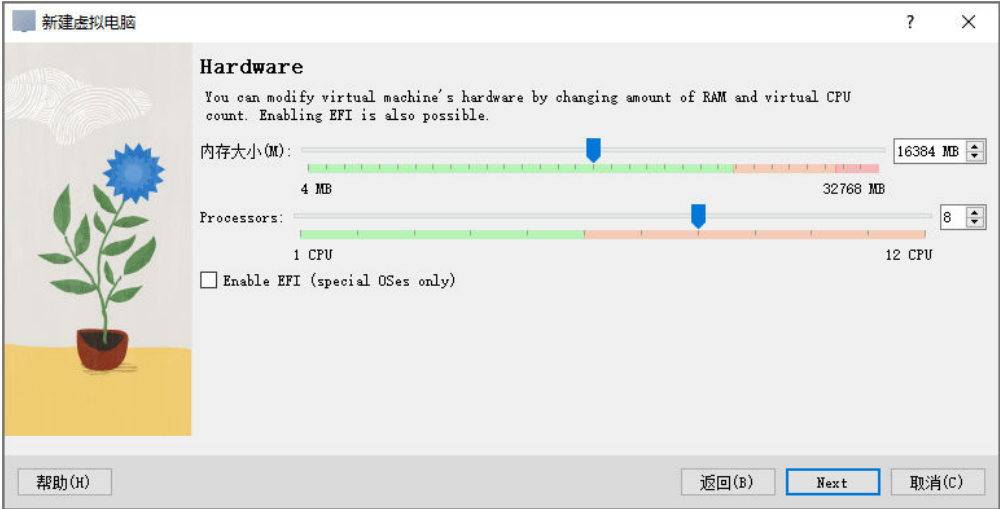
表 3-4 参数说明

参数	说明
Name	虚拟机的名称

参数	说明
Folder	虚拟机部署的路径
ISO Image	ISO镜像，选择“<未指定>”
类型	操作系统类型，选择“Linux”，
版本	发行版本，选择“Other Linux（64-bit）”

2. 请根据个人PC实际情况修改虚拟机内存和CPU个数（**建议不超过本机能力的70%**）。下图以“内存大小”为16384MB，“Processors”为8举例，单击“Next”，如**图3-3**所示。

图 3-3 硬件



说明

例如，模拟一台NE设备约消耗2G内存，使用2个CPU，请根据需要模拟组网的设备数量，合理分配内存和CPU资源。

3. 选中“Use an Existing Virtual Hard Disk File”，选择**步骤2**中注册的虚拟硬盘文件，单击“Next”，如**图3-4**所示。

图 3-4 虚拟硬盘

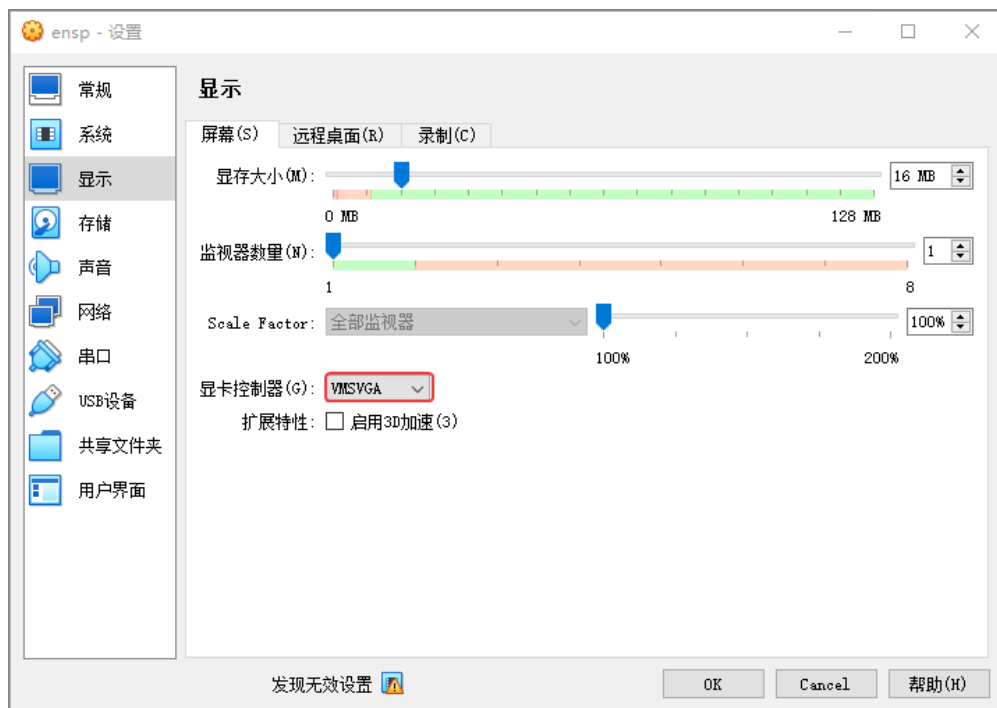


4. 单击“Finish”完成虚拟机创建。

步骤4 设置虚拟机。

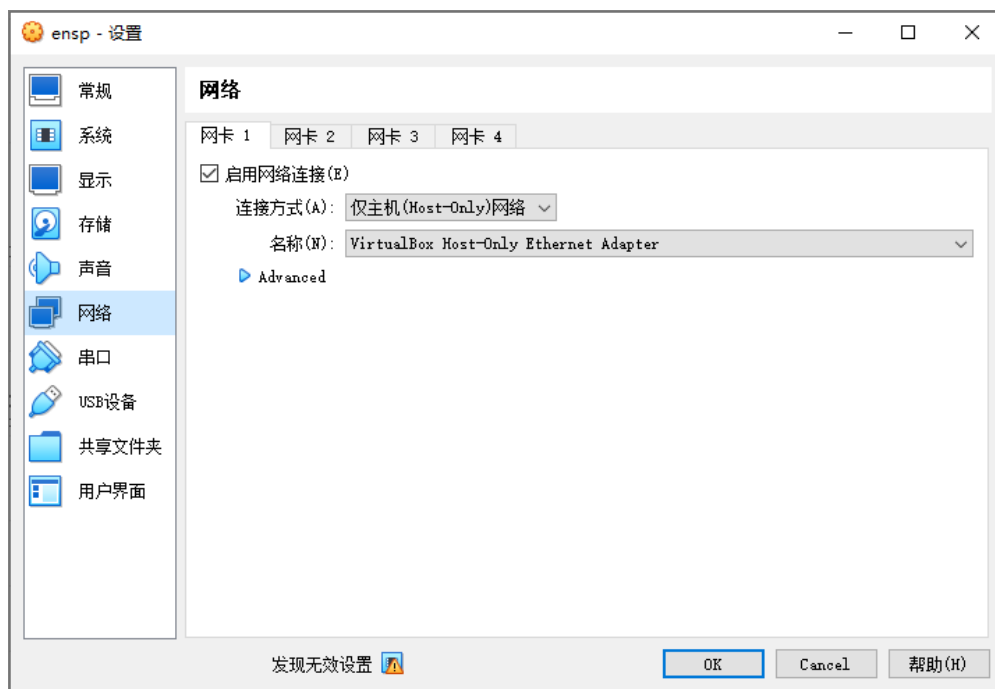
1. 右击创建好的虚拟机，单击“设置”。选择“显示 > 屏幕（S）”，“显卡控制器（G）”选择“VMSVGA”，如图3-5所示。

图 3-5 显示设置



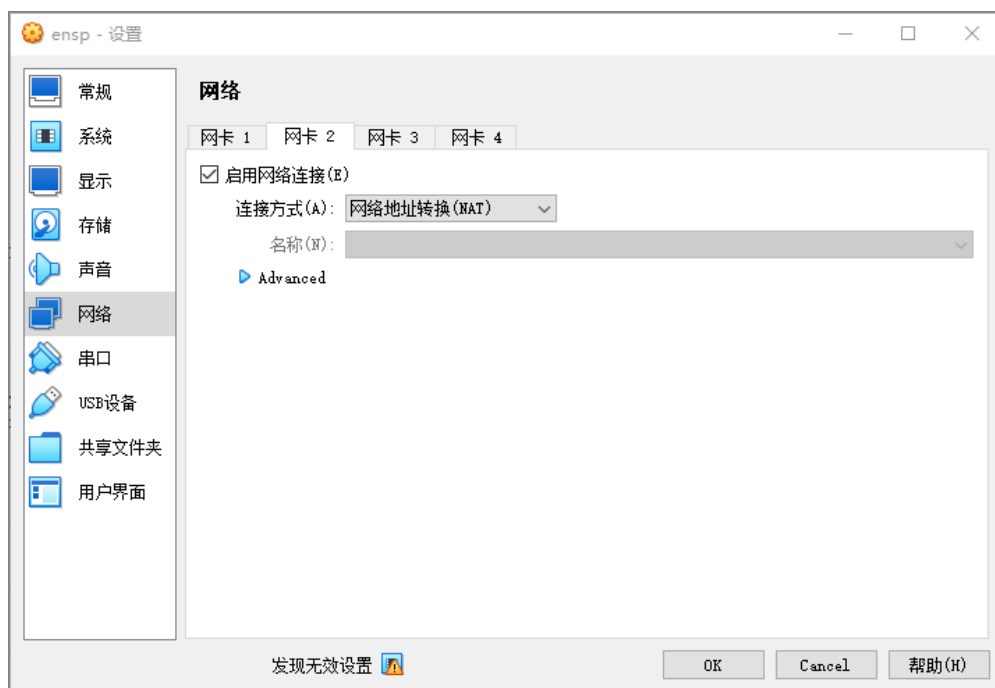
2. 选择“网络 > 网卡1 > 启用网络连接（E）”，“连接方式（A）”选择“仅主机（Host-Only）网络”如图3-6所示。

图 3-6 网卡 1 设置



3. 选择“网络 > 网卡2 > 启用网络连接（E）”，“连接方式（A）”选择“网络地址转换（NAT）”，如图3-7所示。

图 3-7 网卡 2 设置



4. 单击“OK”，完成虚拟机设置。

步骤5 启动虚拟机。双击已创建好的虚拟机或者单击  启动虚拟机。

步骤6 等待20s虚拟机启动完成，如图3-8所示。打开浏览器（推荐使用Chrome浏览器），在地址栏输入欢迎页屏幕上的网址访问数通模拟器。

图 3-8 欢迎页



----结束

3.4.1.3 删除虚拟机

操作步骤

步骤1 右击已经创建完成的虚拟机，单击“删除”如图3-9所示。

图 3-9 删除

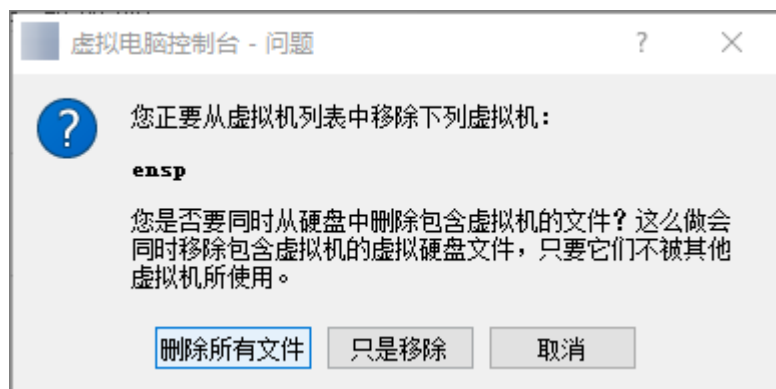


说明

1. 若已经部署了旧版本的虚拟机，部署新版本虚拟机前请删除已经部署的旧版本虚拟机。
2. 若虚拟机正在运行，请先停止运行虚拟机，然后才能删除虚拟机。

步骤2 单击“删除所有文件”，完成老版本虚拟机的删除，如图3-10所示。

图 3-10 删除所有文件



⚠ 注意

“删除所有文件”操作会删除虚拟机所有配置，执行删除操作前请提前备份关键数据。

----结束

3.4.2 部署数通模拟器（Linux 系统）

3.4.2.1 软件要求

数通模拟器支持在物理服务器上安装，软件要求如表3-5所示。

表 3-5 软件配置要求

软件	推荐配置
操作系统	Ubuntu 22.04 LTS或以上版本
模拟器	Qemu-system-x86-64 6.2或以上版本
浏览器	Chrome浏览器97或以上版本

3.4.2.2 部署虚拟机

前提条件

- 物理服务器已经安装Ubuntu 22.04 LTS和Chrome浏览器，如需远程访问，个人PC需安装Chrome浏览器。

操作步骤

步骤1 登录物理服务器并安装配套软件Qemu。

```
root@ensp06:~# apt-get install qemu-system-x86
Reading package lists... Done
Building dependency tree... Done
.....
```

步骤2 新建目录上传3.1 软件获取章节下载的eNSP*_Software_X8664_release.qcow2软件包。

```
root@ensp06:/disk1/ensp# ls
eNSP-Pro_V100R001C00_Software_X8664_release.qcow2
```

步骤3 （可选）使用命令ifconfig查询网卡的IP地址。

```
root@ensp06:/disk1/ensp# ifconfig
enp2s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::c6ff:1fff:fe9:c057 prefixlen 64 scopeid 0x20<link>
    ether c4:ff:1f:f9:c0:57 txqueuelen 1000 (Ethernet)
    RX packets 4129517 bytes 3635333146 (3.6 GB)
    RX errors 0 dropped 257235 overruns 0 frame 0
    TX packets 1922329 bytes 628804851 (628.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 26
```

步骤4 使用命令行`qemu-system-x86_64 -smp <n> -m <size> -cpu host -accel kvm -hda /disk1/ensp/eNSP**_Software_X8664_release.qcow2 -device e1000,netdev=net0 -netdev user,id=net0,hostfwd=tcp:<ip-address>:<physical-port>:-8443`运行虚拟机，关键参数如表3-6所示。

```
root@ensp06:/disk1/ensp# qemu-system-x86_64 -smp 8 -m 16384 -cpu host -accel kvm -hda /disk1/
ensp/eNSP-Pro_V100R001C00_Software_X8664_release.qcow2 -device e1000,netdev=net0 -netdev
user,id=net0,hostfwd=tcp:127.0.0.1:8443:-8443
```

表 3-6 Qemu 参数说明

参数	含义
-smp <n>	设置CPU的核数
-m <size>	设置虚拟机内存，默认单位为MB
-cpu <cpu model>	设置CPU型号
-accel kvm	指定硬件虚拟化使用kvm
-hda <disk path>	设置IDE磁盘路径
<ip-address>	IP地址。若物理服务器本地可以访问，推荐配置IP地址为127.0.0.1；若物理服务器本地不可以访问，需要远程访问，推荐配置IP地址为步骤3查询的IP地址192.168.1.1
<physical-port>	物理机端口
8443	虚拟机端口

📖 说明

更多参数信息请参见：<https://www.qemu.org/docs/master/>。

步骤5 等待90s虚拟机启动完成，打开浏览器（推荐使用Chrome浏览器），在地址栏输入<https://<ip-address>:<physical-port>>访问数通模拟器。

📖 说明

- <ip-address>步骤4中配置的IP地址。
- <physical-port>步骤4中映射的物理机端口。

步骤6 （可选）删除配套软件Qemu。

```
root@ensp06:~# apt remove qemu-system-x86
```

----结束

3.4.2.3 删除虚拟机

方法一

通过快捷键Ctrl + C停止Qemu进程删除虚拟机。

方法二

步骤1 通过命令`ps aux | grep qemu`查找Qemu进程PID。

```
root@ensp06:~# ps aux | grep qemu
root      17523  245  1.8 19773092 4910208 ?        Sl   Mar09 46506:43 qemu-system-x86_64 -smp 8 -m
16384 -cpu host -accel kvm -hda b007/eNSP_V100R001C00_Software_X8664_release.qcow2 -device
e1000,netdev=net0 -netdev user,id=net0,hostfwd=tcp:127.0.0.1:8443-:8443
root      155261  0.0  0.0  6608  2240 pts/0    S+   20:15   0:00 grep --color=auto qemu
```

步骤2 执行`kill -9 <pid>`杀死进程，删除虚拟机。

```
root@ensp06:~# kill -9 17523
```

----结束

4 操作与维护

4.1 帐号注册

数通模拟器中涉及帐号注册的操作，根据下面步骤操作。

操作步骤

步骤1 登录网址<https://uniportal.huawei.com>，进入“Uniportal帐号登录”界面，如**图 4-1**所示，单击“立即注册”。

图 4-1 Uniportal 帐号登录



Uniportal帐号登录

用户名输入框

密码输入框 (带“密码”提示和眼睛图标)

☐ 记住用户名

[短信验证码登录](#)

[登录](#)

[立即注册](#) | [忘记密码](#) | [修改密码](#)

[? 点击获取更多帮助?](#)

步骤2 Unipotal帐号使用“手机号码”或者“邮箱”注册，如[图4-2](#)所示，单击“注册”。

图 4-2 帐号注册

✉ 邮箱注册

手机注册

点击 [登录](#)

国家/地区

中国大陆 ▾

王

—

+86 中国大陆 ▾

19

.....

👁

密码应至少为8个字符,并包含字母、数字和特殊字符

123456

获取验证码

☒ * 提交此表格表明你同意接受 [隐私声明](#) 和 [用户注册协议](#)

注册

📖 说明

- 为了您的帐号安全，请定期修改密码，并且不要将密码泄露给他人。
- 请勿使用简单密码登录账户，建议增加密码长度、复杂度，提高密码安全性。系统默认检测密码复杂度，密码至少满足如下要求：
 - 密码长度至少8个字符；
 - 密码必须包含如下至少三种字符的组合：
 - 至少一个小写字母；
 - 至少一个大写字母；
 - 至少一个数字；
 - 至少一个特殊字符：`~!@#\$%^&*()-_+=~\|[]{};:'",<.>/?;
 - 密码不能包含帐号。

步骤3 完成帐号注册，Uniportal帐号是随机生成ID，如图4-3所示。

图 4-3 帐号信息

The screenshot displays the 'My Account' (我的帐号) interface. At the top right, there are links for 'My Account' (我的帐号), 'Change Password' (修改密码), 'Account Deletion' (帐号销户), and 'Logout' (退出). The main content area is titled '我的帐号' and lists the following account details:

Icon	Field Name	Value	Action Button
Person icon	帐号名	[Redacted]	历史记录
Person icon	姓名	王一	修改姓名
Person icon	昵称	未设置昵称	设置昵称
Phone icon	电话号码	+8 [Redacted]	修改手机
Envelope icon	E-mail	未绑定邮箱	绑定邮箱

说明

- 这里的“帐号名”即登录数通模拟器的Uniportal帐号。
- 更多帐号相关帮助信息请参考：<https://uniportal.huawei.com/uniportal1/help.html>。

----结束

4.2 数通模拟器登录

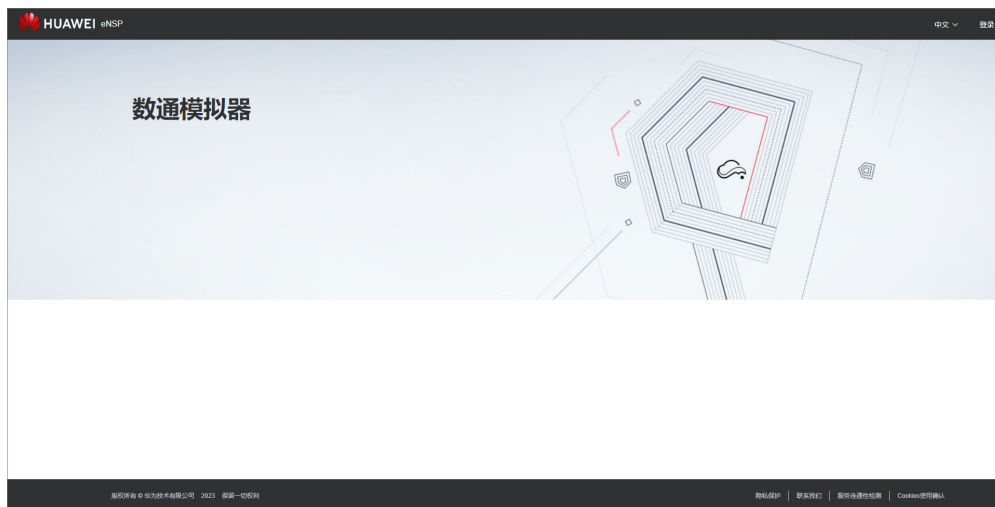
前提条件

1. 用户已获取到Uniportal帐号，获取方法请参见[4.1 帐号注册](#)。
2. Uniportal帐号有登录数通模拟器的权限。

操作步骤

步骤1 访问数通模拟器，如[图4-4](#)所示，单击右上角“登录”。单击“Cookies 使用确认”

图 4-4 数通模拟器



步骤2 如图4-5所示，使用注册的Uniportal帐号登录数通模拟器。

图 4-5 Uniportal 帐号登录

Uniportal帐号登录

☐ 记住用户名 [短信验证码登录](#)

登录

[立即注册](#) | [忘记密码](#) | [修改密码](#)

[? 点击获取更多帮助?](#)

说明

1. 当前版本数通模拟器仅支持单用户独占模式。数通模拟器环境部署后，被首个完成登录的用户占有，其他用户的登录请求将被拒绝。
2. 数通模拟器运行过程中产生的运行数据（包括用户的Uniportal帐号和模拟器运行数据）只存在于模拟器本地，您可以通过卸载数通模拟器的方式来清理数据。
3. 数通模拟器完成用户登录后，生成离线登录凭证，并将该登录凭证保存在浏览器的Cookie中，15天内无需在线登录。手动退出帐号后离线登录失效，需重新在线登录，直接关闭浏览器离线登陆不会失效。
4. 用户10分钟不进行交互性操作会导致会话超时，需要重新登录账户。

----结束

4.3 沙箱操作

须知

沙箱中显示的时间，如沙箱列表中“创建时间”，模拟网元中的时钟时间等均为eNSP VM的时间，而非物理服务器时间。

4.3.1 创建沙箱

操作步骤

步骤1 选择“仿真环境 > 沙箱”，单击“创建沙箱”，如图4-6所示，填写沙箱名称。

图 4-6 创建沙箱

说明

- “沙箱名称”长度在2个~20个字符，不支持部分特殊字符(例如:“\^/<>=&%#?+!空格等);
- 创建沙箱的数量不超过100个。
- 一个沙箱内创建或启动设备的数量不超过50个。

步骤2 单击“确定”沙箱创建成功，选择“仿真环境 > 沙箱”可以查看创建的沙箱，如图4-7所示。

图 4-7 沙箱列表



----结束

4.3.2 修改沙箱

操作步骤

步骤1 选择“仿真环境 > 沙箱”，如图4-8所示，单击沙箱列表操作列中的  按钮。

图 4-8 沙箱列表



步骤2 进入修改沙箱界面，如图4-9所示，修改沙箱名称。

图 4-9 修改沙箱



步骤3 单击“确定”，完成沙箱修改。

----结束

4.3.3 导出沙箱

选择“仿真环境 > 沙箱”，在沙箱列表中选择要导出的沙箱，如图4-10所示，单击“导出沙箱”，沙箱导出成功。

图 4-10 导出沙箱



说明

- 1. 导出的沙箱包括设备、图形、文字、连线等以及他们的配置，但不包括设备获取的报文。
- 2. 若沙箱中没有设备，导出沙箱时会提示沙箱导出失败，并显示没有设备沙箱的名称。

4.3.4 导入沙箱

操作步骤

步骤1 选择“仿真环境 > 沙箱”，单击“导入沙箱”，如图4-11所示，选择要导入的文件，填写沙箱名称，导入沙箱的参数见表4-1所示。

图 4-11 导入沙箱

仿真环境 > 导入沙箱

* 导入方式

使用本地文件

使用云端模板

* 模板文件

导入文件

请导入zip压缩格式(至少包含一份enx文件)的文件，大小不超过1MB

* 沙箱名称

请输入沙箱名称（长度限制为2~20）

返回

创建

表 4-1 参数说明

参数	说明
导入方式	只支持“使用本地文件”导入，暂不支持“使用云端模板”导入
模板文件	导入的沙箱模板。
沙箱名称	长度在2个~20个字符，不支持部分特殊字符(例如:,"^\/<>=&%#?+!空格等)

步骤2 单击“创建”，沙箱创建成功，可以在沙箱列表中查看新建的沙箱，如图4-12所示。

图 4-12 沙箱列表

仿真环境 - 沙箱				
+ 新建沙箱 ↓ 导入沙箱 ↑ 导出沙箱 🔍 搜索				
☐	沙箱名称	创建时间	状态	操作
☐	沙箱	© 2023-03-06 16:14:11	正常	🔗 🗑️
共 1 条 10 条/页 1 / 1 页 前往 1 页				

----结束

4.4 设备操作

前提条件

- 1. 用户已经登录数通模拟器，详细步骤请参见[4.2 数通模拟器登录](#)；
- 2. 沙箱已经创建完成并且已经进入拓扑界面。

4.4.1 添加设备

设备添加的方法有两种，方法一单次只能添加一个设备，方法二单次可以批量添加1个~20个同型号设备。

方法一

单击，选择“货架”中需要的设备，鼠标左键拖动到画布合适的位置，如[图4-13](#)所示，设备添加成功。

图 4-13 添加设备



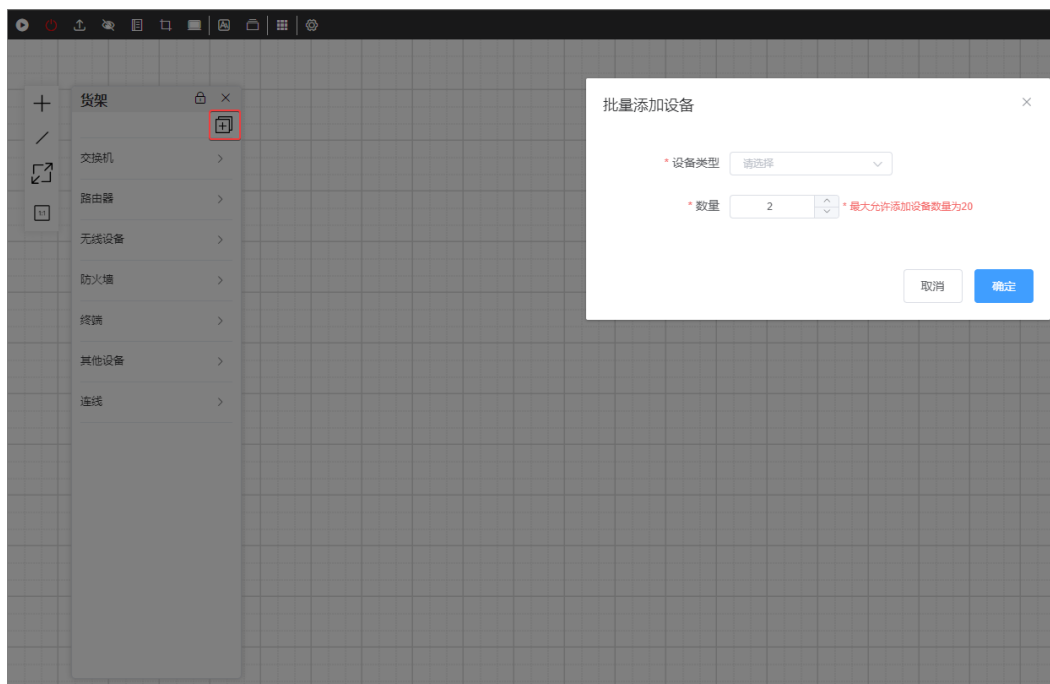
说明

货架中，设备图标是深蓝色，代表设备可用；设备图标是灰色，代表设备不可用。

方法二

步骤1 单击 ，选择“货架”右上方  按钮，弹出批量添加设备窗口，如图4-14所示。

图 4-14 批量添加



步骤2 选择“设备类型”，修改设备“数量”，单击“确定”，设备添加成功。

图 4-15 批量添加设备



说明

添加设备的数量与可启动设备数量无关。可以启动使用的设备数量受实际数通模拟器运行环境限制，无法保证沙箱内添加的所有设备均能成功启动。

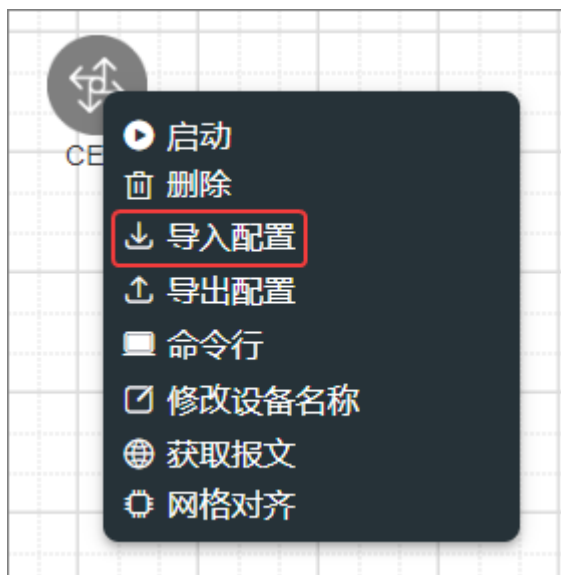
----结束

4.4.2 导入配置

操作步骤

步骤1 右击需要导入配置的设备，弹出如图4-16所示右键菜单，单击“导入配置”。

图 4-16 设备导入配置



说明

导入配置的功能需要设备未启动，启动中和启动完成的设备不能执行导入配置操作。

步骤2 如图4-17所示，单击“上传”，选择需要导入的配置文件。

图 4-17 导入配置



步骤3 提示“导入成功”以后单击“关闭”，如图4-18所示，导入配置完成。

图 4-18 导入成功



步骤4 登录设备，查看配置是否导入正确。

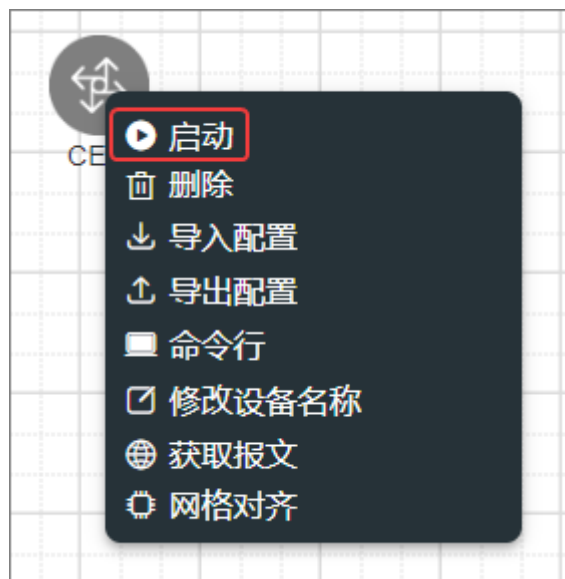
----结束

4.4.3 启动设备

操作步骤

步骤1 右击需要启动的设备，弹出如图4-19所示右键菜单，单击“启动”，设备开始启动。

图 4-19 启动设备



说明

1. 单击拓扑界面上方工具栏的图标，可以启动拓扑图中的所有设备。
2. 可以启动使用的设备数量受实际数通模拟器运行环境限制，无法保证沙箱内添加的所有设备均能成功启动。

步骤2 （可选）鼠标悬停在设备上可以查看当前设备的启动进度，如图4-20所示，设备状态说明参见表4-2所示。

图 4-20 启动进度

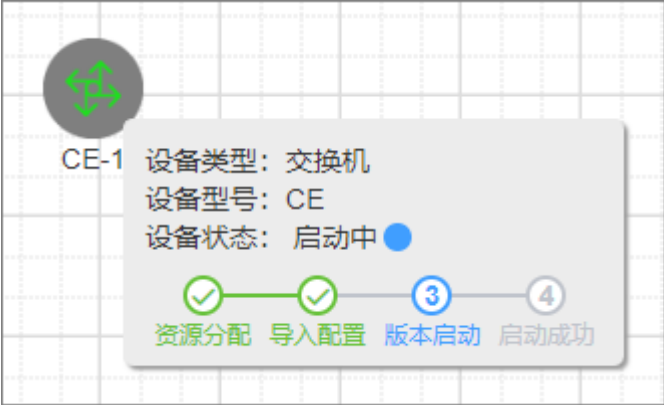


表 4-2 设备状态说明

图标	设备状态	说明
	灰色	设备未启动。
	半绿	设备启动中。
	全绿	设备启动成功。
	全红	设备启动失败。

----结束

4.4.4 导出配置

步骤1 保存配置。

- NE设备保存配置。

```
<HUAWEI> save ne.cfg
Warning: Are you sure to save the configuration to cfcad:/ne.cfg? [Y/N]:y
Now saving the current configuration to the slot 17
Info: Save the configuration successfully.
<HUAWEI> startup saved-configuration ne.cfg
Info: Succeeded in setting the configuration for booting system.
<HUAWEI>dir
Directory of cfcad:/  Idx  Attr   Size(Byte)  Date      Time      FileName
```

```
0 dr-x      - Mar 21 2023 06:17:08  $_checkpoint
1 dr-x      - Mar 11 2023 04:57:57  $_install_hpg      dir
2 dr-x      - Mar 11 2023 04:57:57  $_install_mod
3 dr-x      - Mar 21 2023 06:17:40  $_license
4 dr-x      - Mar 21 2023 06:17:46  $_security_info
5 dr-x      - Mar 21 2023 06:16:47  $_startup
6 dr-x      - Mar 21 2023 06:17:43  $_system
7 dr-x      - Mar 21 2023 06:17:43  $_user
8 -rw-      5 Mar 21 2023 06:16:32  VRPV800R022C10SPC100B315D0311_ne40e_x8664.cc
9 -rw-      2,934 Mar 21 2023 09:21:51  device.sys
10 -rw-      3,295 Mar 21 2023 09:21:32  ne.cfg
11 drwx      - Mar 21 2023 06:17:48  ztp                37,235,712 KB total (30,117,348 KB free)
```

- 其他设备导出配置。

```
<HUAWEI>save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Now saving the current configuration to the slot 1
Info: Save the configuration successfully.
<HUAWEI>dir
Directory of flash:/

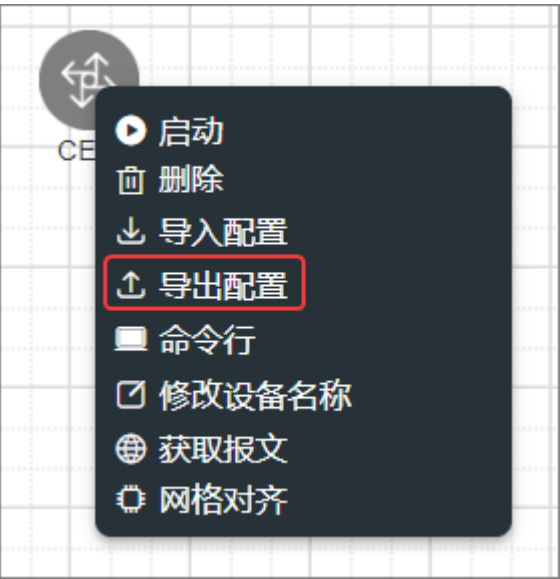
Idx Attr   Size(Byte) Date      Time      FileName
0  dr-x      - Mar 09 2023 08:48:35  $_checkpoint
1  dr-x      - Jun 24 2021 01:00:00  $_install_mod
2  dr-x      - Mar 09 2023 02:50:43  $_license
3  dr-x      - Mar 09 2023 02:49:32  $_startup
4  dr-x      - Mar 09 2023 02:51:08  $_system
5  dr-x      - Mar 09 2023 02:51:08  $_user
6  -rw-      3,229 Mar 09 2023 08:48:41  1.cfg
```

 说明

- 使用save [<configuration-file>]可以不指定参数configuration-file，系统默认保存配置名称为 1.cfg；若指定参数configuration-file，只能设置为1.cfg，否则无法导出配置。
- save保存配置后，需要等待一定时间（约20秒）再进行配置导出，否则可能导出配置失败。

步骤2 右击需要导出配置的设备，弹出如图4-21所示右键菜单，单击“导出配置”，配置导出成功。

图 4-21 设备导出配置



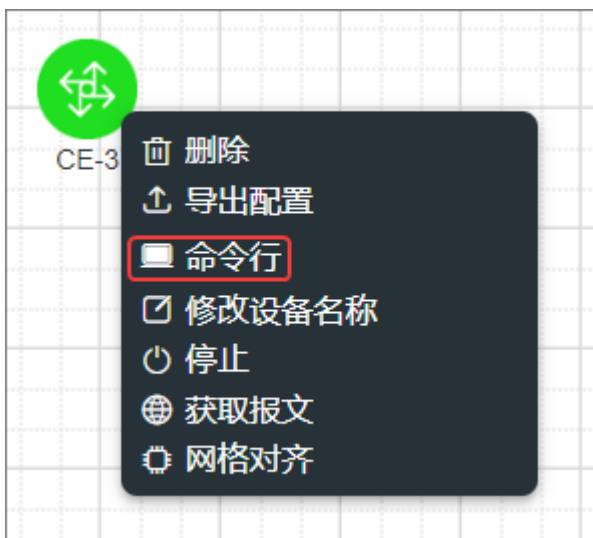
----结束

4.4.5 配置命令行

操作步骤

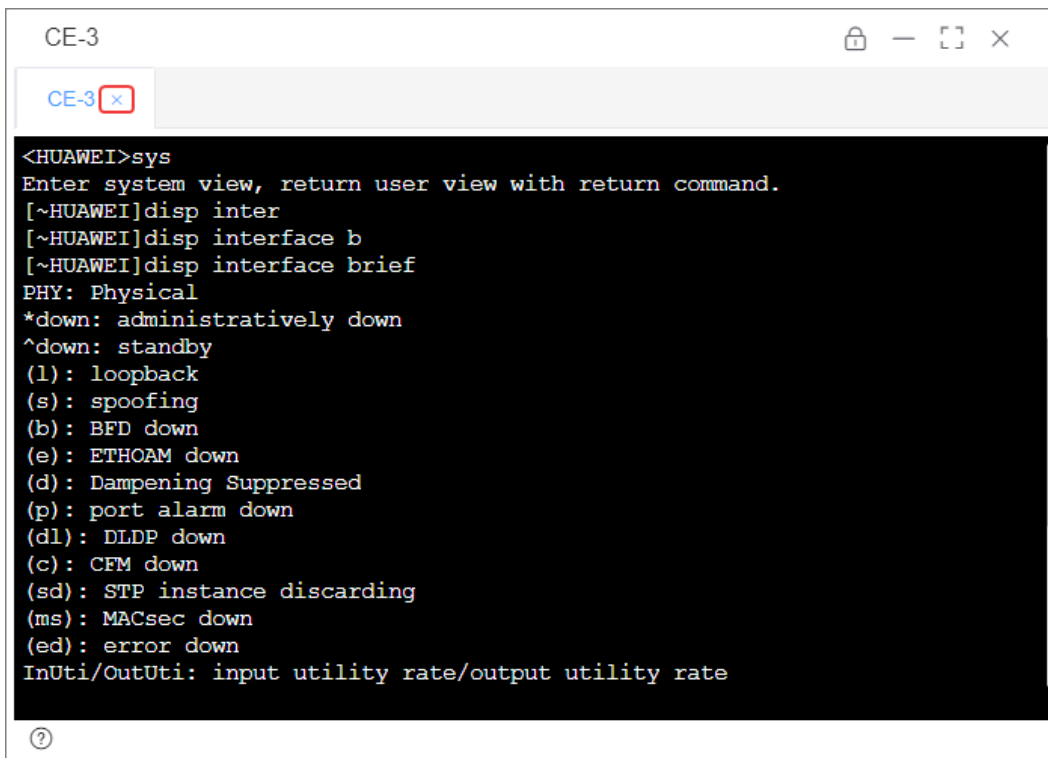
步骤1 右击已经启动成功的设备，弹出如图4-22所示右键菜单，单击“命令行”或者双击已经启动成功的设备。

图 4-22 命令行



步骤2 弹出的会话框可以输入命令行，如需关闭会话框，单击 ，如图4-23所示。

图 4-23 关闭单个设备会话框

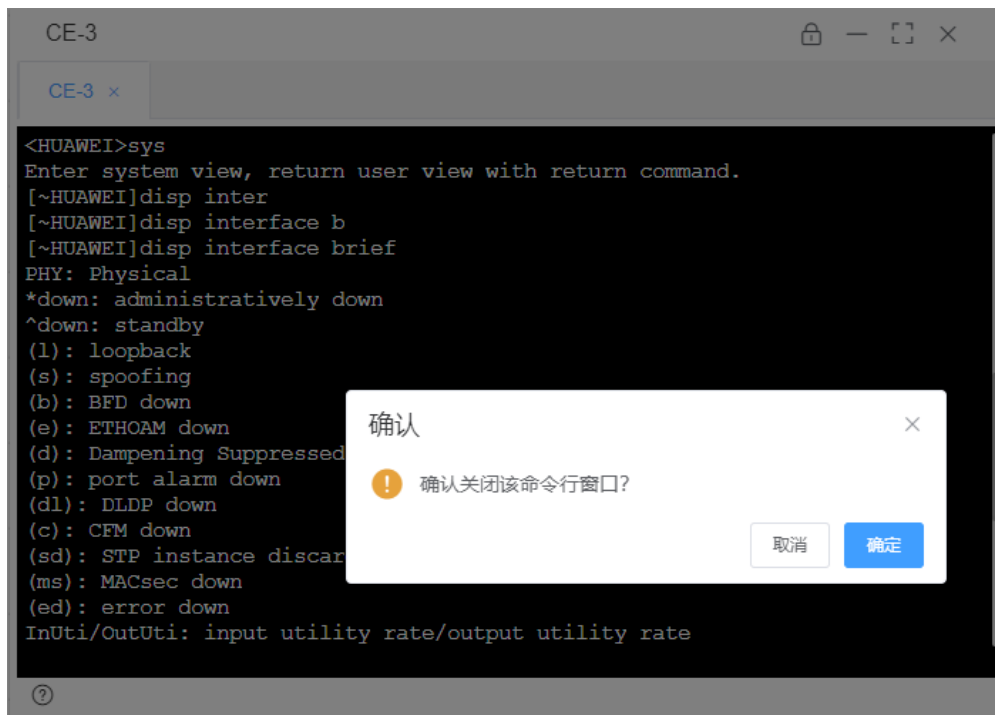


说明

1. 未启动成功的设备，单击“命令行”弹出的会话框会提示设备不可用。
2. 会话框输入的命令行支持复制粘贴，单次输入命令行不能超过8KB。
3. 命令行打开的多个设备的会话框可以通过按住鼠标左键拖动切换顺序。
4. 使用快捷键Alt+Q切换会话框窗口。

步骤3 单击“确定”，如图4-24所示，关闭会话框。

图 4-24 确认是否关闭会话框



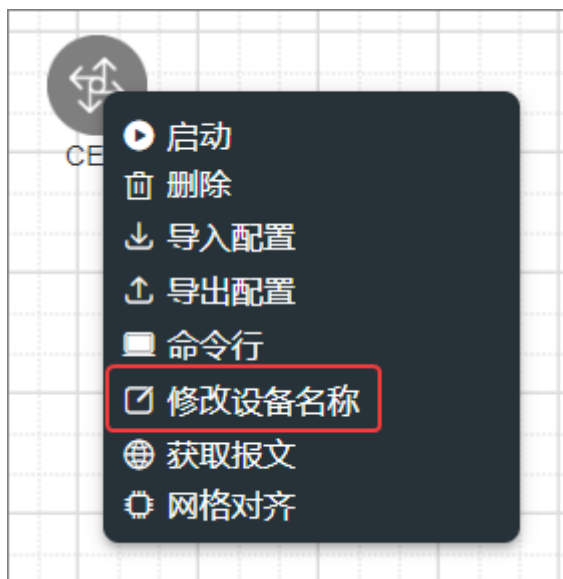
----结束

4.4.6 修改设备名称

操作步骤

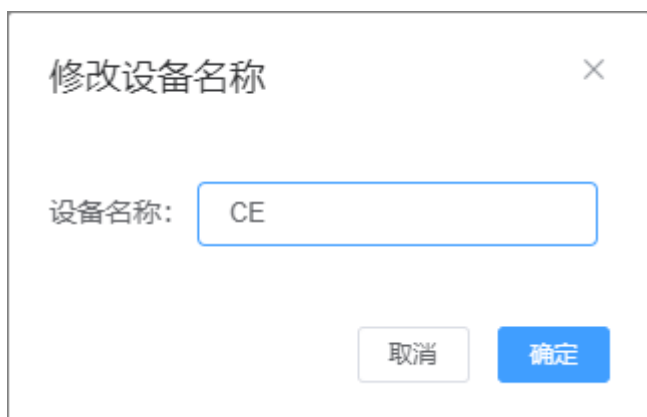
步骤1 右击需要修改名称的设备，弹出如图4-25所示的右键菜单，单击“修改设备名称”。

图 4-25 修改设备名称



步骤2 填写设备名称，如图4-26所示，单击“确定”，设备名称修改完成。

图 4-26 设备名称



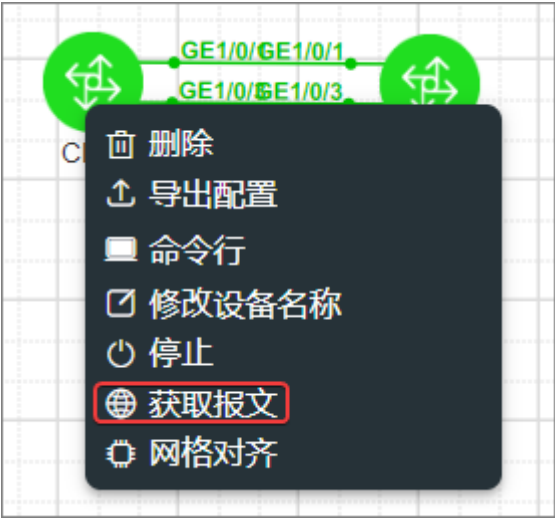
----结束

4.4.7 获取报文

操作步骤

步骤1 右击已经启动成功并且有接口连线的设备，弹出如图4-27所示右键菜单，单击“获取报文”。

图 4-27 获取报文



须知

为获取设备之间的通信报文，数通模拟器引入了tcpdump功能。该报文获取功能仅限于数通模拟器内部使用，不涉及用户其他网络平面和网络设备上的报文获取，由于获取报文时获取的cap文件可能存在安全风险，请您注意妥善保管该cap文件。

步骤2 选择接口和获取计时，填写获取计数和过滤器，单击“获取报文”，选择的设备接口开始获取数据报文，如[图4-28](#)所示。

图 4-28 获取数据报文



说明

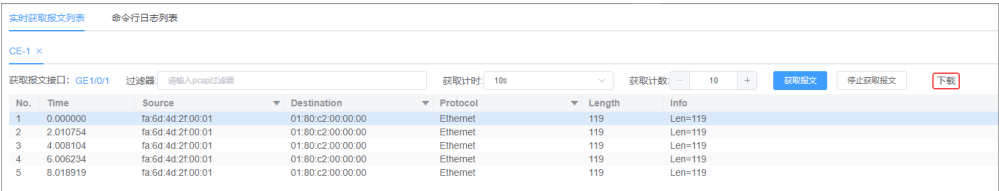
- 1. 设备启动成功、设备之间有连线并且接口前的图标为绿色时，是可采集数据报文状态。
- 2. 采集数据报文的接口可以选择1个或多个。
- 3. 采集数据报文的时长最小为10s，最大为30min。
- 4. 在“获取数据报文”或者“实时获取报文列表”中可配置pcap过滤器，过滤语句举例参见表4-3所示，更多过滤语句请参见<https://gitlab.com/wireshark/wireshark/-/wikis/CaptureFilters#useful-filters>。

表 4-3 过滤语句举例

过滤语句	语句举例
过滤出8888 TCP端口的封包	<code>tcp dst port 8888</code>
过滤出IP地址192.168.1.1的封包	<code>ip src host 192.168.1.1</code>
过滤出来源为UDP或TCP，且端口号在100到300之间的封包	<code>src portrange 100-300</code>

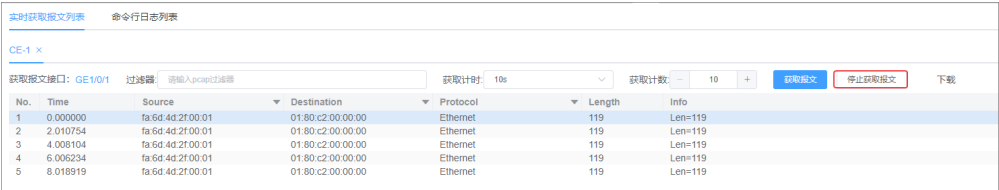
步骤3 （可选）单击“下载”，如图4-29所示，可以将获取的报文保存到指定的文件夹。

图 4-29 下载数据报文



步骤4 （可选）单击“停止获取报文”，获取报文停止，如图4-30所示。

图 4-30 停止获取报文

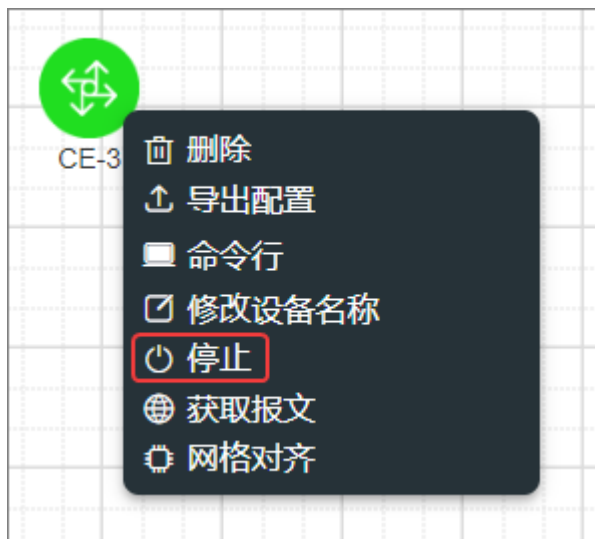


----结束

4.4.8 停止设备

右击需要停止的设备，弹出如图4-31所示的右键菜单，单击“停止”，设备停止。

图 4-31 停止设备



说明

单击拓扑界面上方工具栏的  图标，可以停止拓扑图中的所有设备。

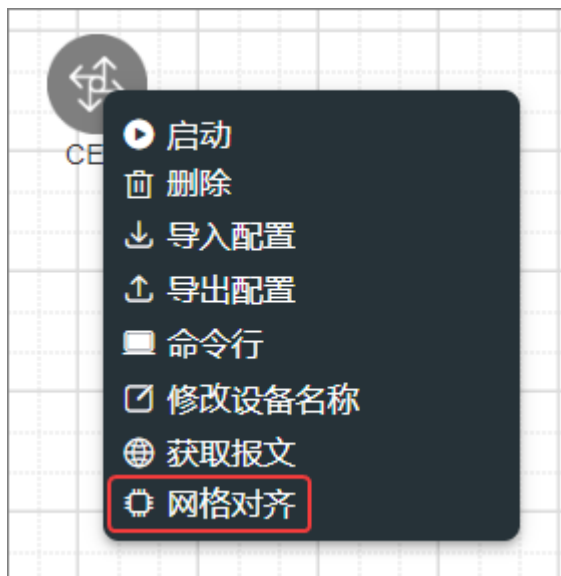
4.4.9 对齐设备

设备对齐的方法有两种。方法一只能网格对齐单个设备，方法二可以对齐多个设备。

方法一

右击需要对齐的设备，弹出如图4-32所示右键菜单，单击“网格对齐”，设备会自动布局在网格的交叉点。

图 4-32 网格对齐



方法二

1. 单击画布拖动框选多个设备，在选中的任意一个设备上右击，在弹出的菜单中单击“垂直对齐”，如图4-33所示，选中的多个设备垂直对齐，如图4-34所示。
“水平对齐”和“网格对齐”操作类似，此处不再赘述。

图 4-33 垂直对齐

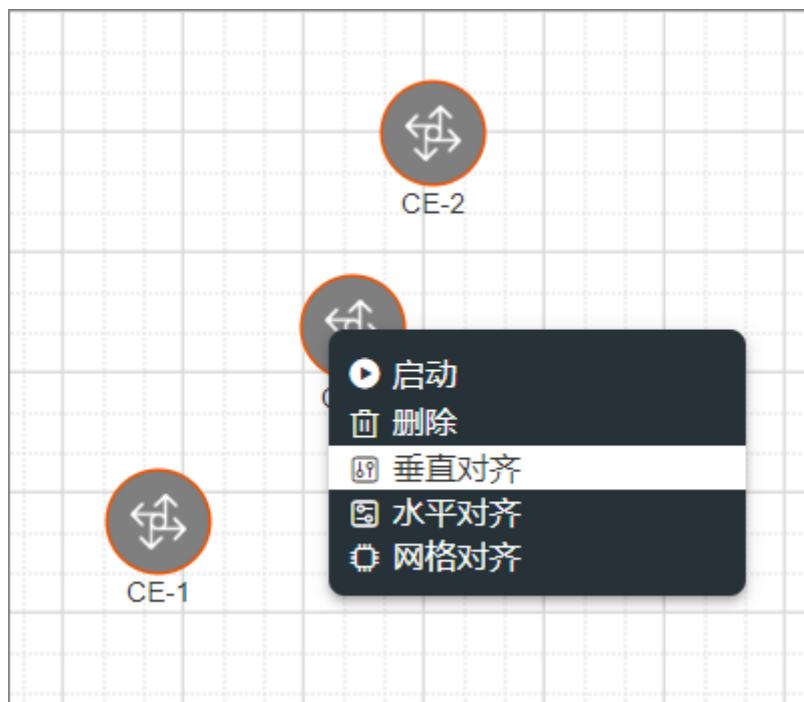
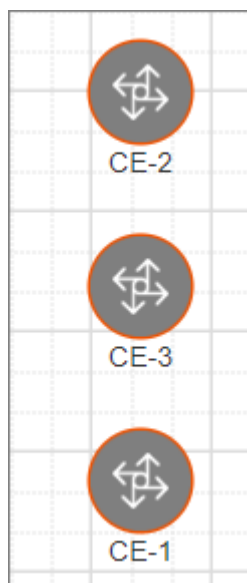


图 4-34 设备垂直对齐



4.4.10 删除设备

操作步骤

步骤1 右击需要删除的设备，弹出如图4-35所示右键菜单，单击“删除”。

图 4-35 删除设备



步骤2 单击“确定”，如图4-36所示，设备删除成功。

图 4-36 提示



----结束

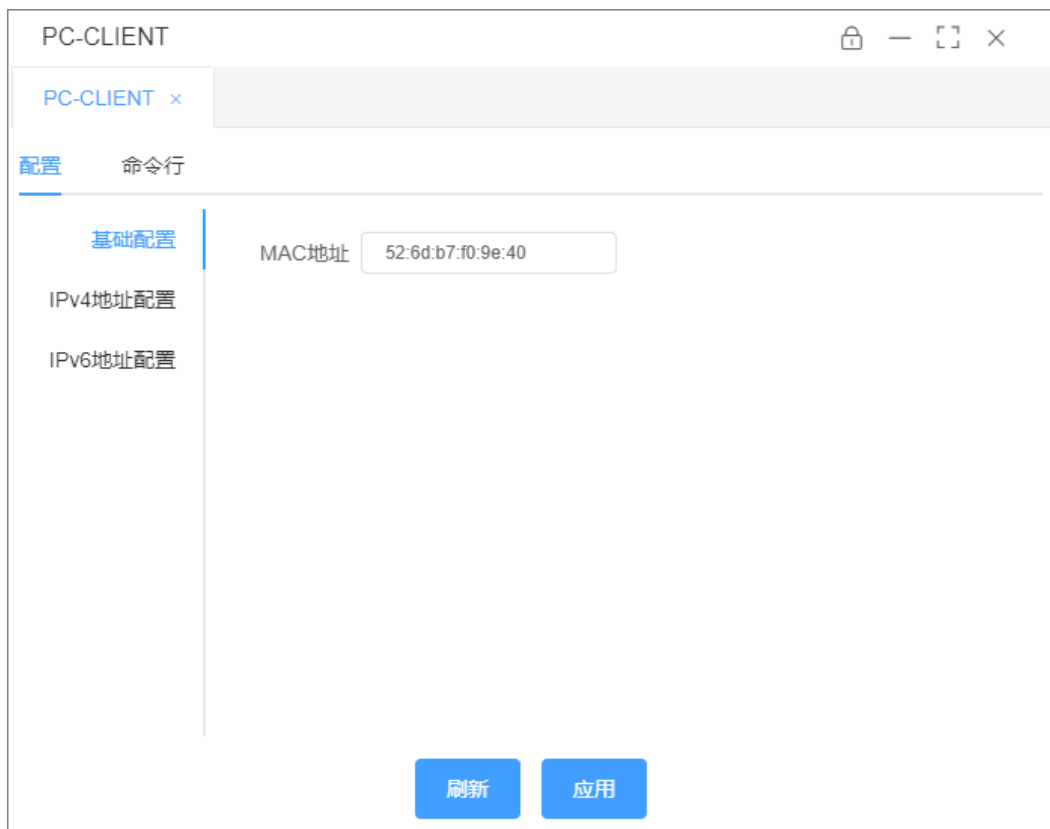
4.4.11 配置 PC Client 终端

PC Client终端需要使用界面配置。

操作步骤

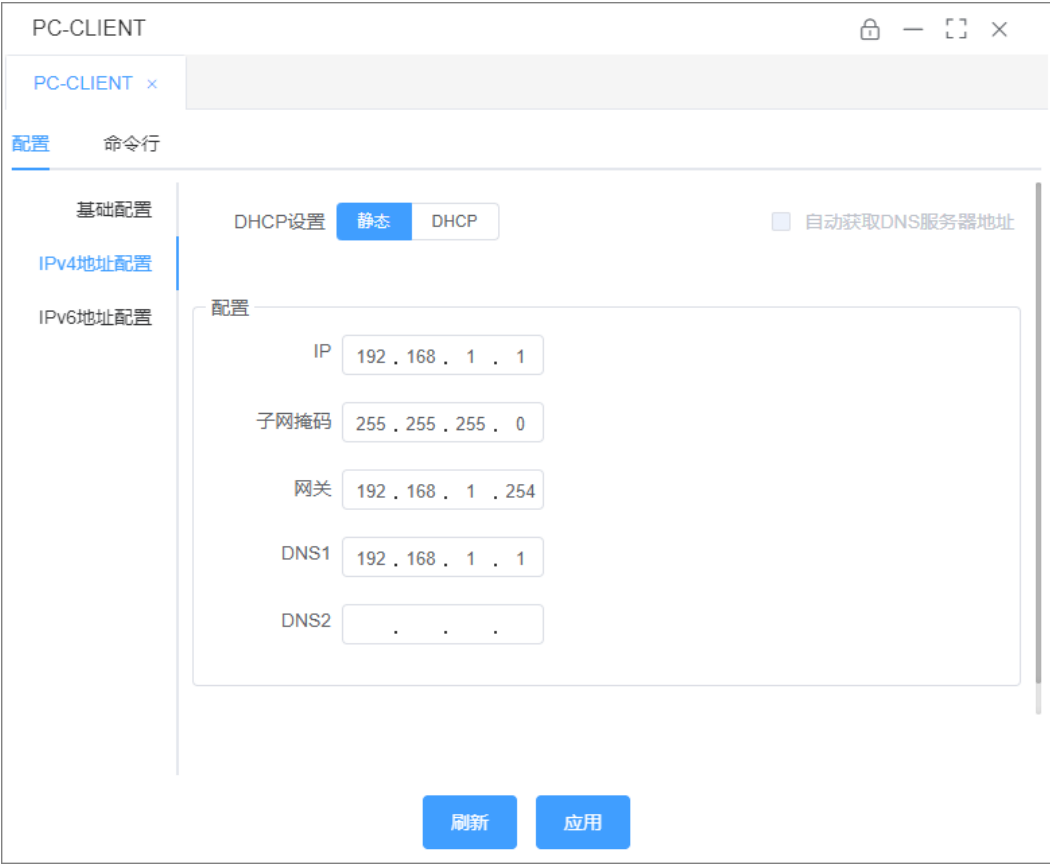
步骤1 双击已经启动成功的PC Client终端，在弹出窗口可以配置MAC地址，如图4-37所示，MAC地址有缺省值。

图 4-37 配置 MAC 地址



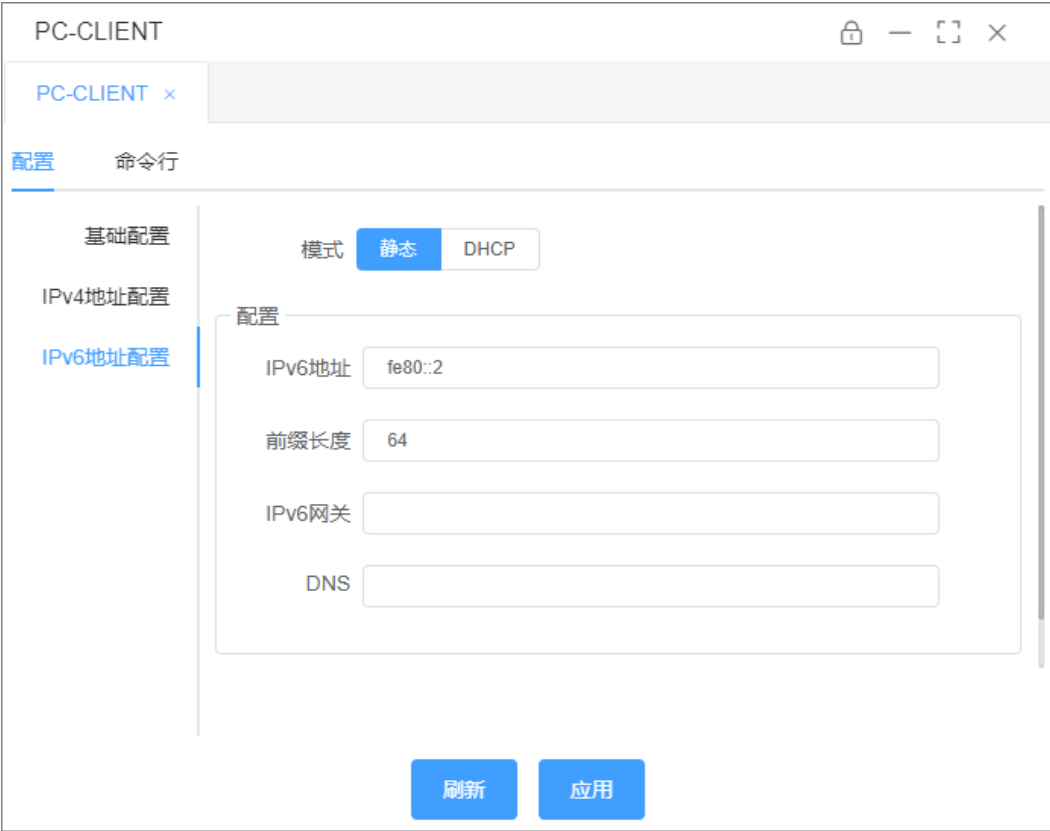
步骤2 单击“IPv4地址配置”，配置IPv4地址参数如图4-38所示。

图 4-38 配置 IPv4 地址



步骤3 单击“IPv6地址配置”，配置IPv6地址参数如图4-39所示。

图 4-39 配置 IPv6 地址



- 步骤4** 参数配置完成后单击“应用”，PC Client配置完成。
- 步骤5** 在“配置”界面单击“刷新”或者“命令行”界面使用ifconfig命令查看配置结果。

```
PC> ifconfig
Local IPv6 address.....: fe80::506d:b7ff:fef0:9e40
IPv6 address.....: fe80::2/64
IPv6 gateway.....: ::
IPv4 address.....: 192.168.1.1
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.1.254
Physical address.....: 52:6d:b7:f0:9e:40
DNS server.....: 192.168.1.1
```

----结束

4.4.12 配置 PC Server 终端

PC Server终端需要使用界面配置。配置PC Server的MAC地址、IPv4地址、IPv6地址与配置PC Client类似，此处不再赘述。

操作步骤

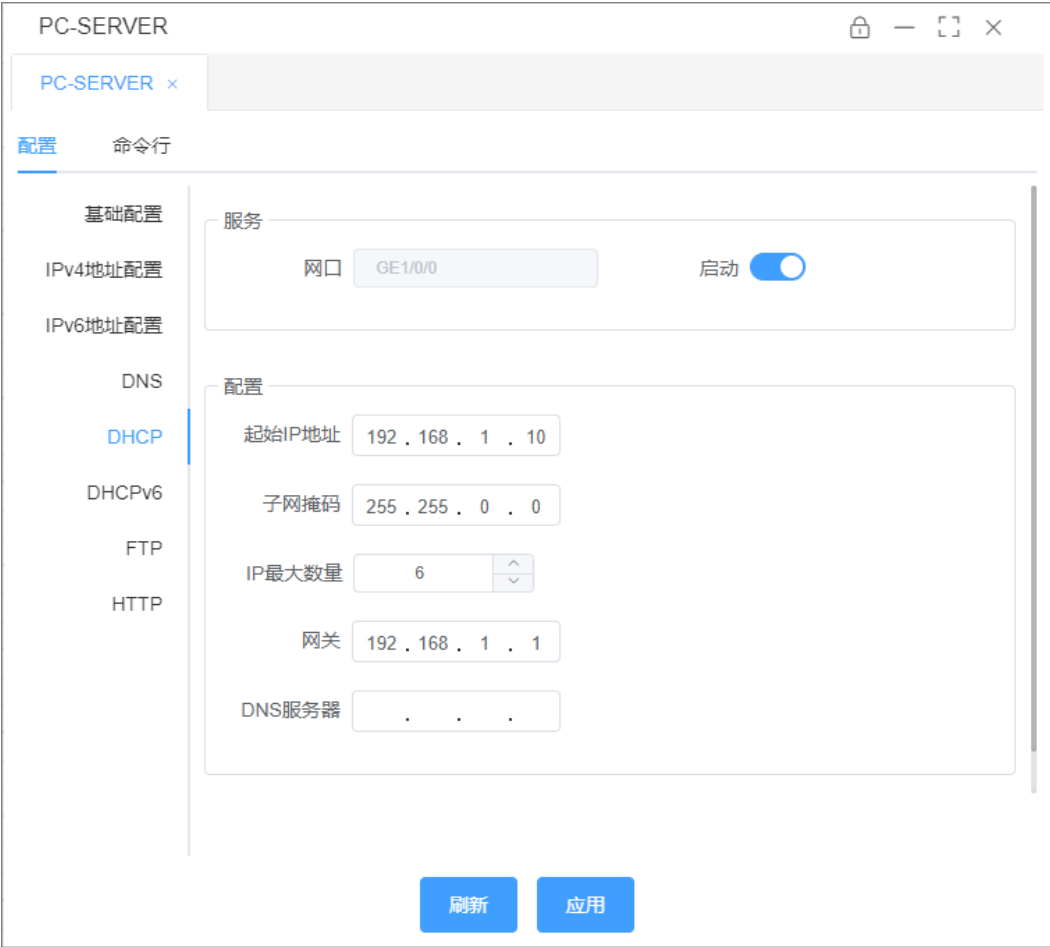
- 步骤1** 双击已经启动成功的PC Server终端，在弹出窗口单击“DNS”，配置DNS参数，如图4-40所示，DNS服务端口缺省值为53，启动状态默认为关闭。

图 4-40 配置 DNS



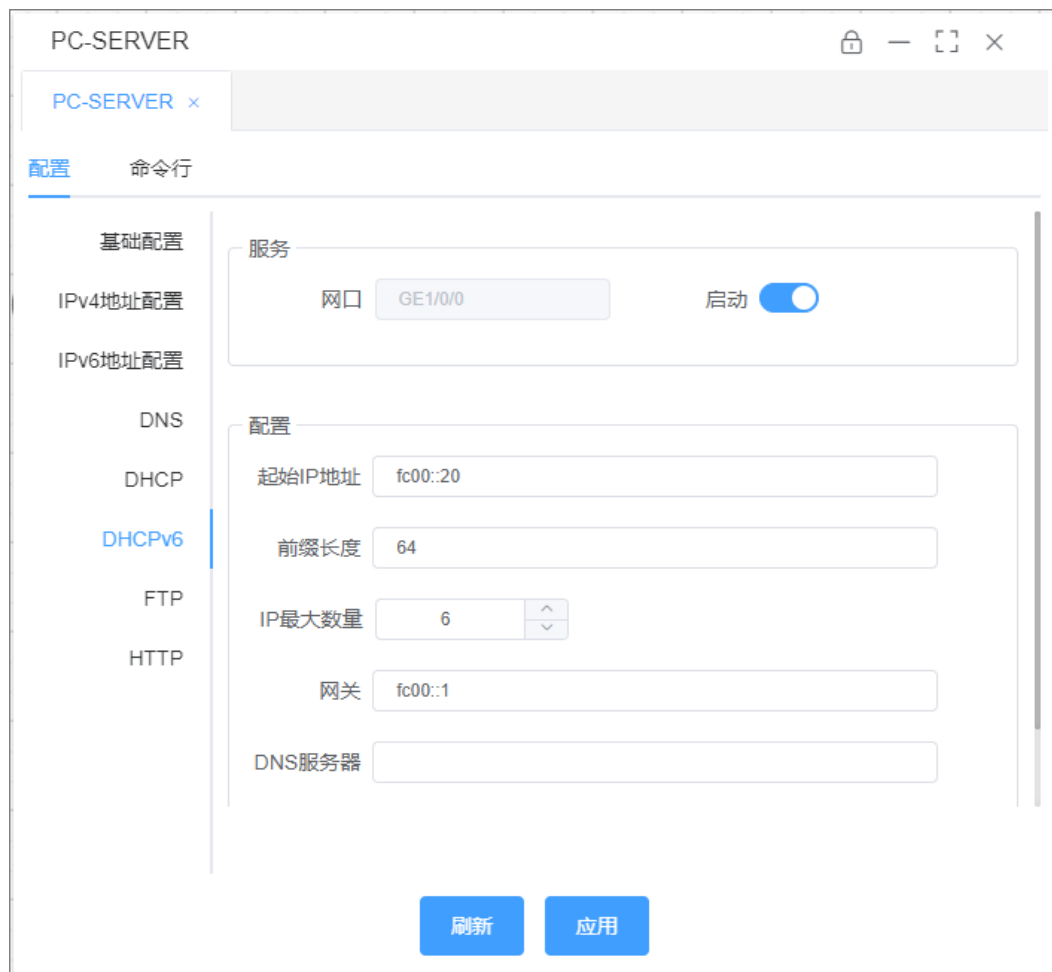
步骤2 单击“DHCP”，配置DHCP参数，如图4-41所示，DHCP服务启动状态默认为关闭。

图 4-41 配置 DHCP



步骤3 单击“DHCPv6”，配置DHCPv6参数，如图4-42所示，DHCPv6服务启动状态默认为关闭。

图 4-42 配置 DHCPv6



步骤4 单击“FTP”，配置FTP参数，如图4-43所示，FTP服务端口缺省值为21，启动状态默认为关闭。

图 4-43 配置 FTP



说明

PC Server设备中的FTP服务使用匿名帐号登录，登录帐号为ftp或者anonymous，无需密码；登录过程中提示输入邮箱信息可以无需理会，输入任何字符或者回车可以继续登录。

步骤5 单击“HTTP”，配置HTTP参数，如图4-44所示,HTTP服务端口缺省值为80，启动状态默认为关闭。

图 4-44 配置 HTTP



步骤6 参数配置完成后单击“应用”，PC Server配置完成。

步骤7 在“配置”界面单击“刷新”查看配置结果。

----结束

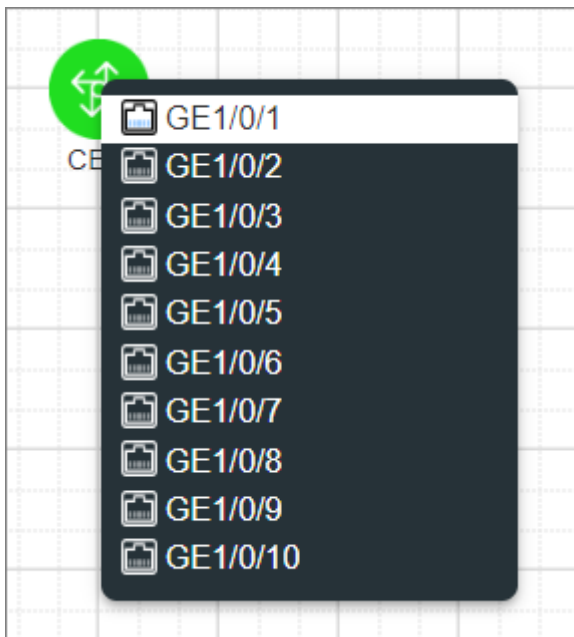
4.5 连线操作

4.5.1 添加连线

操作步骤

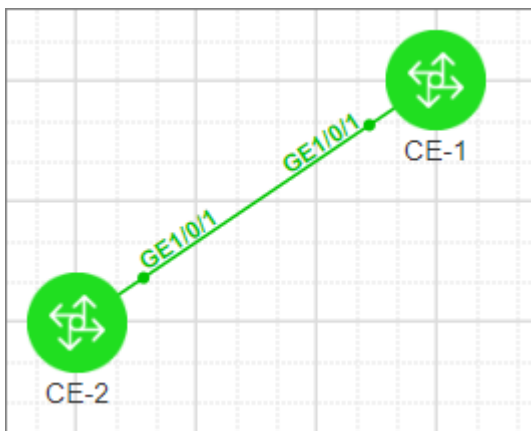
步骤1 单击 ，鼠标移动到画布，此时鼠标变成 ，单击第一个设备，在弹出选择接口的提示框选择接口，如图4-45所示。

图 4-45 设备接口



步骤2 选择第二个网元单击，在弹出选择接口的提示框选择接口，完成设备连线，如图4-46所示。

图 4-46 设备连线



----结束

4.5.2 删除连线

操作步骤

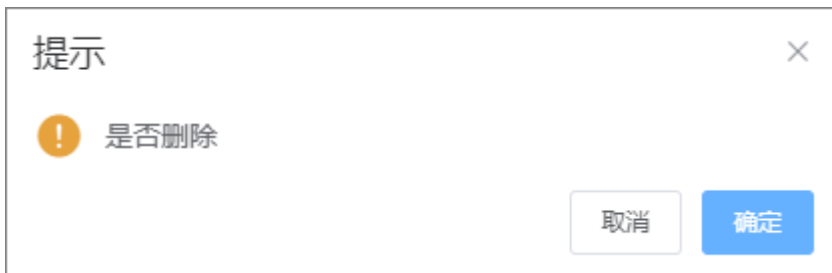
步骤1 鼠标右击需要删除的连线，单击“删除”，如图4-47所示。

图 4-47 删除连线



步骤2 单击“确定”，如图4-48所示，删除连线。

图 4-48 提示



----结束

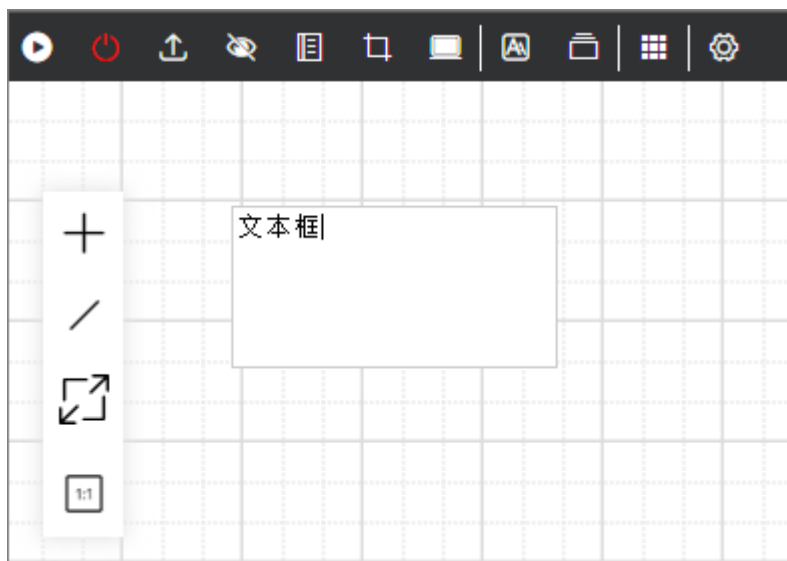
4.6 其他操作

4.6.1 添加文本

操作步骤

步骤1 单击 ，然后单击画布，画布上会出现一个文本框，即可在此位置添加文本，如图4-49所示。一个沙箱内创建文本框数量不超过100个。

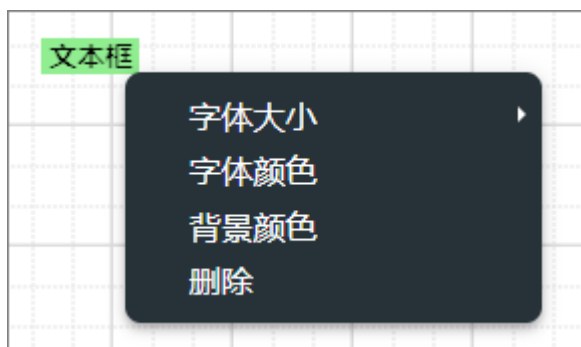
图 4-49 文本框



步骤2 在画布任意位置右击取消文本框，文本添加结束。

步骤3 （可选）右击文本区域，弹出如图4-50所示右键菜单，可以选择“字体大小”、“字体颜色”、“背景颜色”以及“删除”操作。

图 4-50 文本修改



----结束

4.6.2 绘制图形

操作步骤

步骤1 单击 ，选择形状、是否填充、边框类型、边框粗细，如图4-51所示，鼠标移至画布可以绘制所选图形。一个沙箱内创建调色板数量不超过100个。

图 4-51 调色板



步骤2 单击调色板右上角  绘制图形结束。

步骤3 （可选）右击图形区域，弹出如图4-52所示右键菜单，可以选择“置顶”、“置底”、修改“背景颜色”、“删除”、“编辑”操作。

图 4-52 调色板修改



----结束

5 FAQ

5.1 网络环境切换导致登录失败

若网络环境发生变更，则可能因为DNS未同步导致登录失败，如下图所示。



解决方案

重启虚拟机。

5.2 登录数通模拟器网页时报无法访问此页面

查看代理服务器开关是否开启，若代理服务器开关开启，需屏蔽代理服务器。

解决方案

步骤1 搜索框输入“代理”，单击“打开”，如图5-1所示。

图 5-1 打开代理服务器设置



步骤2 查看代理服务器开关开启，需要在屏蔽代理服务器栏中填写“192.*”，如图5-2所示，单击“保存”，屏蔽代理服务。

图 5-2 代理屏蔽



----结束

6参考

6.1 GUI 参考

前提条件

用户已经登录数通模拟器，并创建沙箱。

单击沙箱列表中的沙箱名称，进入沙箱拓扑界面，如图6-1所示，图标说明参见表6-1所示。

图 6-1 沙箱拓扑

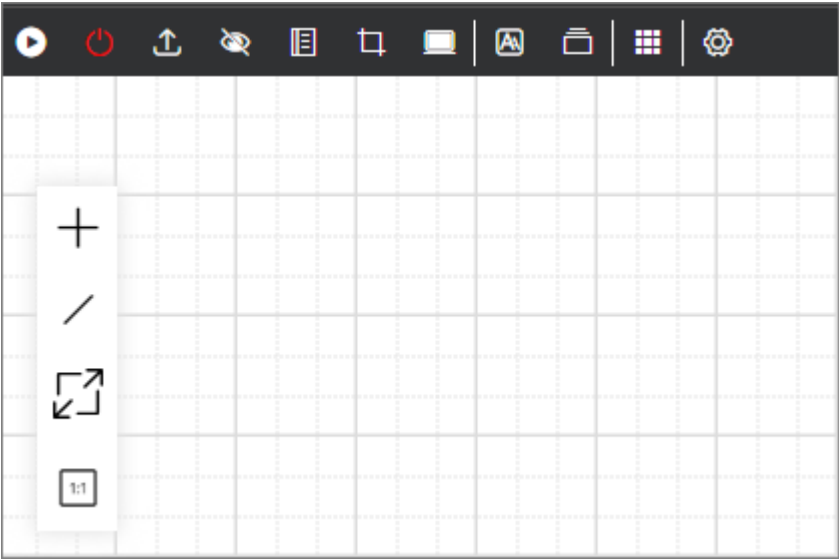


表 6-1 图标说明

图标	说明
	一键启动，可以一键启动拓扑图中所有设备。

图标	说明
	一键停止，可以一键停止拓扑图中所有设备。
	导出沙箱。
	隐藏接口。
	显示接口。
	查看接口列表。
	隐藏接口列表。
	网格，可以切换是否显示拓扑图中的网格线。
	打开所有命令行，可以打开所有设备的会话框。
	文本。
	调色板。
	下载列表。
	设置，可以设置命令行显示的字体、字形、字体大小、字体颜色、字体透明度和会话框的背景颜色。
	添加设备。
	添加连线。
	返回，连线完成后可以单击此图标返回。
	开启缩放，单击图标，缩放功能开启。
	关闭缩放，单击图标，缩放功能关闭。
	重设，恢复拓扑图中所有设备原大小。

6.2 命令参考

交换机，路由器，防火墙命令参考

您可以在[华为企业业务网站](#)上浏览和获取相关的文档，也可登录[info-Finder命令行查询界面](#)查询。

须知

文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。

表 6-2 模拟器对应的参考文档

模拟器名称	参考文档名称
NE路由器模拟器	《 NE40E V800R022C10SPC500 产品文档 》
CE交换机模拟器	《 CloudEngine 8800, 6800系列交换机 V300R022C00 产品文档 》
S交换机模拟器	《 CloudEngine S5700, S6700 V600R022C00 产品文档 》
AR路由器模拟器	《 NetEngine AR V600R022C00 产品文档 》
USG防火墙模拟器	《 HiSecEngine USG6000F V600R022C00 产品文档 》

PC 终端模拟器命令参考

目前PC终端模拟器支持四个命令ifconfig、ssh、ping、curl。

表 6-3 命令说明

命令	说明
ifconfig	查询网络设备状态命令
ssh	连接客户端命令
ping	报文发送命令
curl	数据传输命令

说明

更多参数信息可在设备“命令行”界面中输入{ **ssh** | **ping** | **curl** } **--help**命令获取。

7 缩略语

缩略语

缩略语	英文全名	中文解释
6VPE	IPv6 VPN Provider Edge	IPv6 VPN提供商边缘
AAA	Authentication, Authorization, and Accounting	认证、授权和计费
ARP	Address Resolution Protocol	地址解析协议
ATM	Asynchronous Transfer Mode	异步传输模式
BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议
BIER	Bit Index Explicit Replication	比特索引显式复制
BIERv6	Bit Index Explicit Replication IPv6 Encapsulation	IPv6封装的比特索引显式复制
BPDU	Bridge Protocol Data Unit	桥协议数据单元
CLI	Command Line Interface	命令行接口

缩略语	英文全名	中文解释
CRC	Cyclic Redundancy Check	循环冗余校验
DCN	Data Communication Network	数据通信网
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCPv6	Dynamic Host Configuration Protocol version 6 (DHCPv6)	IPv6动态主机配置协议
DNS	Domain Name System	域名系统
ERPS	Ethernet Ring Protection Switching	以太环网保护倒换
EVC	Ethernet Virtual Connection	以太虚连接
EVPN	Ethernet Virtual Private Network	以太网虚拟私有网络
FR	Frame Relay	帧中继
FS	File Service	文件服务
FRR	Fast Reroute	快速重路由
GRE	Generic Routing Encapsulation	通用路由封装协议
GVRP	Generic VLAN Registration Protocol	通用VLAN注册协议
HWTACACS	Huawei Terminal Access Controller Access Control System	华为终端访问控制器控制系统协议
ICMP	Internet Control Message Protocol	因特网控制报文协议
IGMP	Internet Group Management Protocol	因特网组管理协议

缩略语	英文全名	中文解释
IPv4	Internet Protocol version 4	第四版互联网协议
IPv6	Internet Protocol version 6	第六版互联网协议
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统
KPI	Key Performance Indicator	关键性能指标
L2TPv3	Layer 2 Tunneling Protocol Version 3	第二层隧道协议
L2VPN	Layer 2 Virtual Private Network	二层虚拟专用网
L3VPN	Layer 3 Virtual Private Network	三层虚拟专用网
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LAD	Link Automatic Discovery	链路自动发现
LDP	Label Distribution Protocol	标签分发协议
LLDP	Link Layer Discovery Protocol	链路层发现协议
MAC	Media Access Control	媒体接入控制
MLD	Multicast Listener Discovery	组播侦听者发现协议
MQC	Modular QoS Command Line Interface	模块化QoS命令行
MPLS	Multiprotocol Label Switching	多协议标签交换

缩略语	英文全名	中文解释
MPLS-TP	Multiprotocol Label Switching Transport Profile	多协议标签交换-传送子集
MSDP	Multicast Source Discovery Protocol	组播源发现协议
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTU	Maximum Transmission Unit	最大传输单元
MVPN	Multicast VPN	组播VPN
NAT	Network Address Translation	网络地址转换
ND	Neighbor Discovery	邻居发现
NETCONF	Network Configuration Protocol	网络配置协议
NG MVPN	Next-Generation Multicast VPN	下一代组播VPN
NQA	Network Quality Analysis	网络质量分析
NSF	Non-Stop Forwarding	不间断转发
OAM	Operations, Administration, and Maintenance	操作、管理和维护
OPS	Open Programmability System	开放可编程系统
OSPF	Open Shortest Path First	开放式最短路径优先
P2MP	Point-to-Multipoint	点到多点
PADS	Protocol-Aided Diagnosis System	协议辅助诊断系统

缩略语	英文全名	中文解释
PBB	Provider Backbone Bridge	运营商骨干网桥
PIM	Protocol Independent Multicast	协议无关组播
PPP	Point-to-Point Protocol	点对点协议
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号用户服务协议
RIP	Routing Information Protocol	路由信息协议
RIPng	RIP next generation	下一代RIP协议
RMON	Remote Network Monitoring	远程网络监控
RRPP	Rapid Ring Protection Protocol	快速环网保护协议
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	安全套接层
STP	Spanning Tree Protocol	生成树协议
TDM	Time Division Multiplexing	时分复用
TE	Traffic Engineering	流量工程
Telnet	Telecommunication Network Protocol	电信网络协议
TNLM	Tunnel Management	隧道管理
TTY	Terminal Type	终端类型

缩略语	英文全名	中文解释
TWAMP	Two-Way Active Measurement Protocol	双向主动测量协议
VLAN	Virtual Local Area Network	虚拟局域网
VPLS	Virtual Private LAN Service	虚拟专用局域网业务
VPN	Virtual Private Network	虚拟专用网
VPWS	Virtual Private Wire Service	虚拟专用线路业务
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议
VS	Virtual System	虚拟系统
VXLAN	Virtual Extensible LAN	虚拟扩展局域网
ZTP	Zero Touch Provisioning	零配置自动部署