H3C SecPath ACG1000 系列应用控制网关

快速开局指导

目 录

1 导读

本手册可帮助您对 ACG1000 系列应用控制网关的使用过程有初步的认识，并完成 ACG 的基本配置，如 ACG 的常见组网方式，如何将 ACG 设备快速接入 Internet，如何快速实现企业网络的应用控制、行为审计和常用的设备运维操作等。如果您想深入了解和使用 ACG 其他更多、更丰富的应用控制功能，具体查阅对应产品的手册。

本手册使用 ACG1000 设备的 R6614 版本举例，不同的版本的设备界面可能存在差异，仅供参考具体配置请以实际情况为准。本手册所描述的内容适用于如下款型及版本：

表1-1 ACG1000 系列款型

ACG1000 系列	款型
ACG1000-AK系列	ACG1000-AK280、ACG1000-AK270、ACG1000-AK260、ACG1000-AK250、ACG1000-AK240、ACG1000-AK230、ACG1000-AK220、ACG1000-AK210、ACG1000-AK215、ACG1000-AK225、ACG1000-AK255、ACG1000-AK265、ACG1000-AK275、ACG1000-AK285
ACG1000系列	ACG1000-XE1、ACG1000-PE、ACG1000-EE、ACG1000-AE、ACG1000-ME、ACG1000-TE、ACG1060-X1、ACG1070-X1、ACG1010-X1、ACG1030-X1、ACG1050-X1、ACG1000-SE-PWR、ACG1000-BE-PWR、ACG1000-SE、ACG1000-BE、ACG1005-PWR
ACG1000-C9000系列	ACG1000-C9130、ACG1000-C9150、ACG1000-C9160、ACG1000-C9170

在不区分具体型号时，后续章节统称为 ACG1000 系列设备。

2 设备外观介绍

2.1.1 ACG1000 面板介绍

图2-1 ACG1000-B、ACG1005、ACG1000-C、ACG1010、ACG1020、ACG1000-AK110、ACG1000-AK120 设备前面板

表2-1 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 蓝色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，

说明区域	区域说明	详细说明
		绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持3G上网功能
③Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
④业务接口区	系统管理和业务网络接口	10/100/1000BASE-T自适应以太网接口，缺省情况下，ge0是管理接口

图2-2 ACG1000-S、ACG1030、ACG1040、ACG1050、ACG1000-AK140 设备前面板

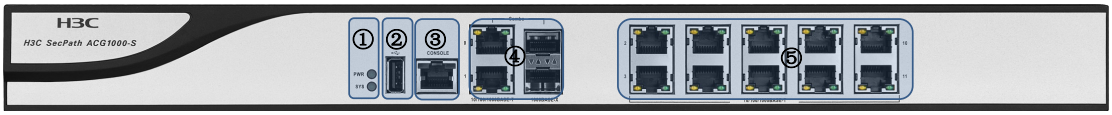


表2-2 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
③Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
④COMBO业务接口区	系统管理和业务网络接口	光电复用接口： 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用，缺省情况下，ge0是管理接口
⑤业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图2-3 ACG1000-M、ACG1000-T、ACG1060、ACG1000-A、ACG1070、ACG1000-AK160、ACG1000-AK170 设备前面板

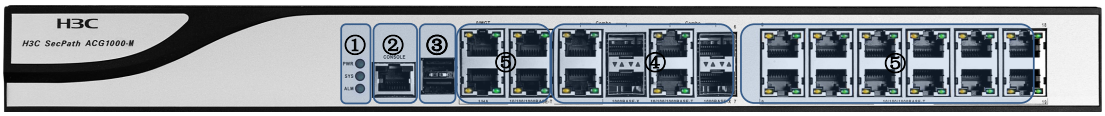


表2-3 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④COMBO业务接口区	系统管理和业务网络接口	光电复用接口： 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑤业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，缺省情况下，ge0是管理接口

图2-4 ACG1000-E、ACG1000-P、ACG1000-X、ACG1000-AK180 设备前面板

表2-4 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，

说明区域	区域说明	详细说明
		绿色闪烁表示系统正常运行
②Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④管理接口区	系统管理接口	10/100自适应以太网管理接口①
⑤板载接口区	板载业务网络接口，板载为光电复用接口	光电复用接口：缺省情况下，系统识别板载区为槽位1，接口形态为ge1-0~ge1-3 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑥、⑦、⑧扩展接口区	安装扩展接口子卡槽位	扩展插槽，各槽位对子卡的适配能力一致： 适配4COMBO子卡、1XG子卡、4XG子卡，可根据实际业务需求进行选择扩展

图2-5 ACG1000-AK130、ACG1000-BE-PWR、ACG1000-BE、ACG1005-PWR 设备前面板

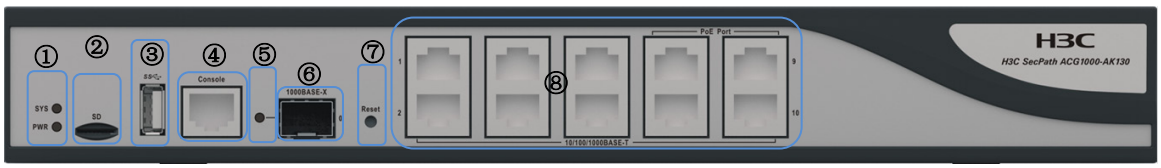


表2-5 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤SFP接口指示灯	光模块接口状态指示灯	指示光模块状态常亮表示光模块link，闪烁表示有数据收发，常灭表示未link
⑥ SFP接口	连接光模块的接口	1000BASE-X光模块接口,接口形态为ge0

说明区域	区域说明	详细说明
⑦ 按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑧业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图2-6 ACG1000-AK150、ACG1000-SE-PWR、ACG1000-SE 设备前面板

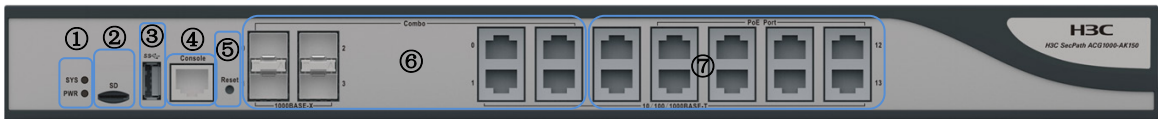


表2-6 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图2-7 ACG1000-XE1

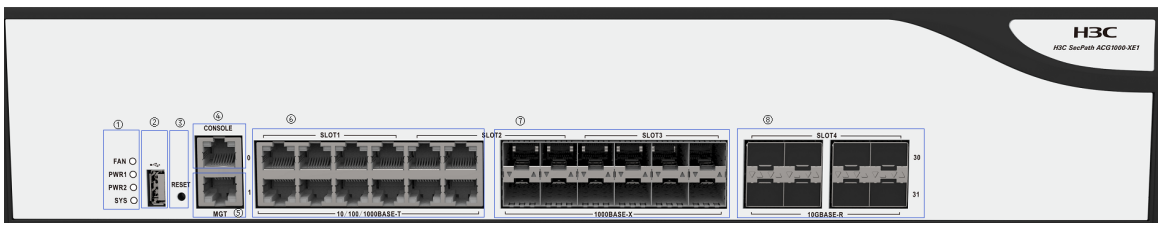


表2-7 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
③reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑥千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑦千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑧万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

图2-8 ACG1000-PE、ACG1000-EE

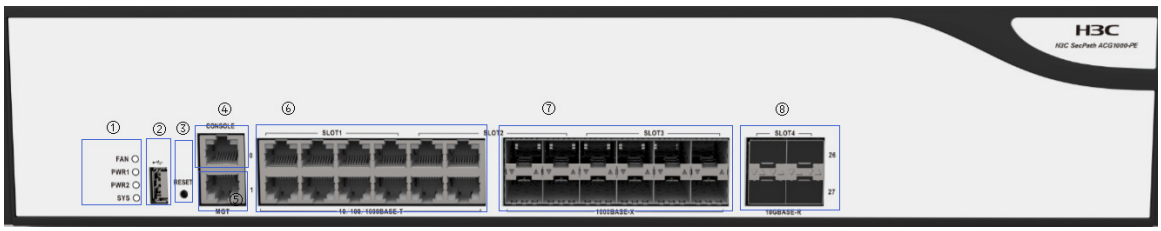


表2-8 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，

说明区域	区域说明	详细说明
		绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
③reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑥千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑦千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑧万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

图2-9 ACG1000-AE

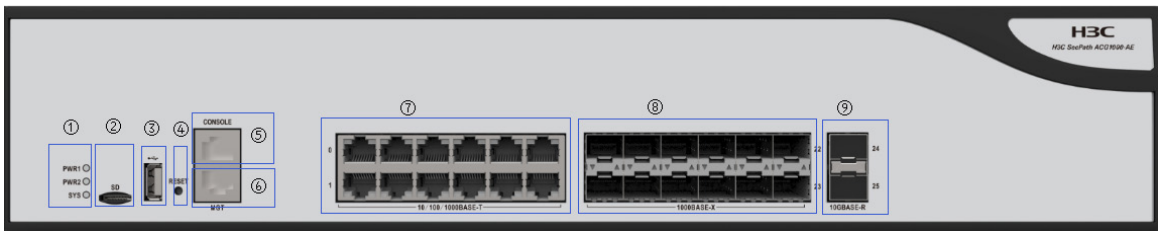


表2-9 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键：

说明区域	区域说明	详细说明
		支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑨万兆光口业务接口区	业务网络接口	10GEX以太网接口

图2-10 ACG1000-XE1、ACG1000-ME、ACG1000-TE、ACG1060-X1、ACG1070-X1

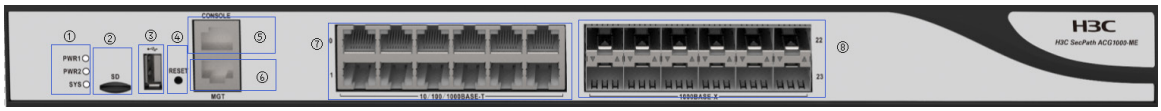


表2-10 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接	业务网络接口	10/100/1000BASE-T自适应以太网接口

说明区域	区域说明	详细说明
口区		
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口

图2-11 ACG1000-AK210

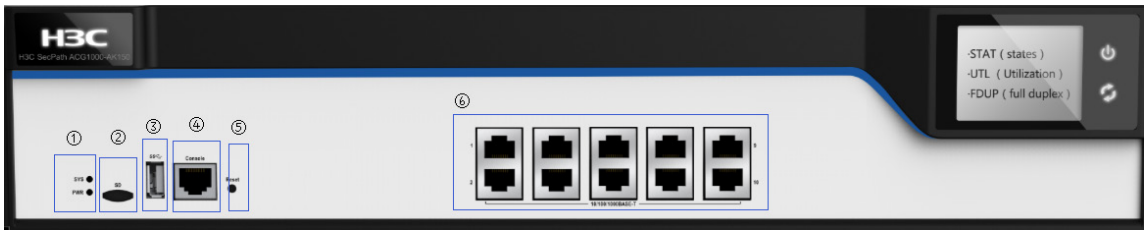


表2-11 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤reset按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑥业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图2-12 ACG1000-AK220

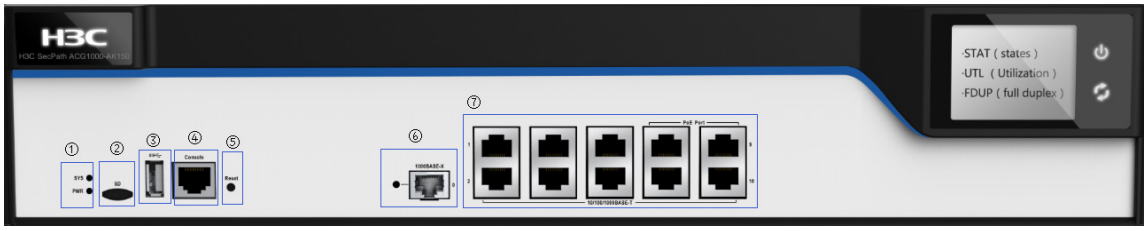


表2-12 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤reset按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑥ SFP接口	连接光模块的接口	1000BASE-X光模块接口,接口形态为ge0 指示灯指示光模块状态常亮表示光模块link，闪烁表示有数据收发，常灭表示未link
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图2-13 ACG1000-AK230

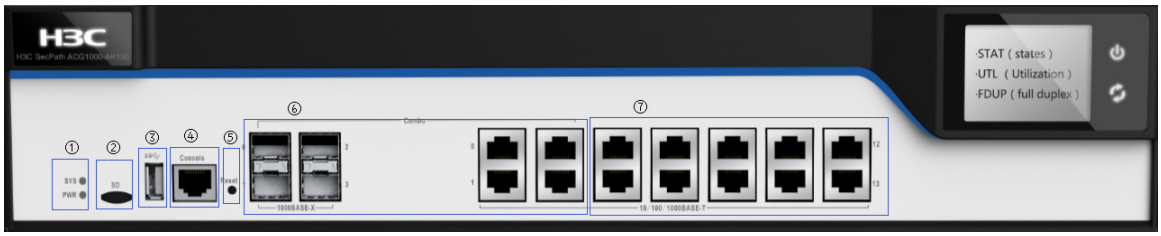


表2-13 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本

说明区域	区域说明	详细说明
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图2-14 ACG1000-AK240

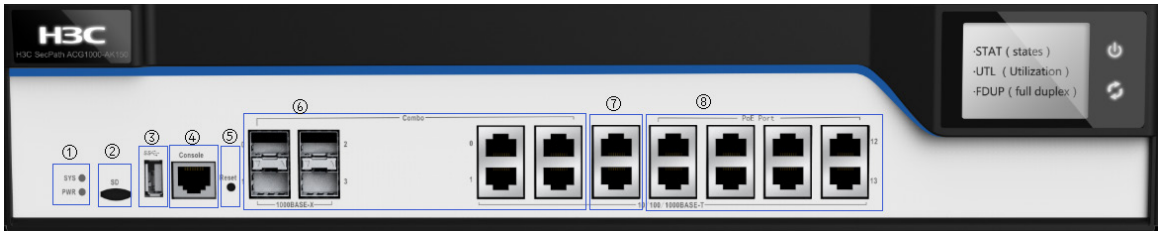


表2-14 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

说明区域	区域说明	详细说明
⑧POE业务接口区	POE业务接口	10/100/1000BASE-T自适应以太网接口，支持POE供电

图2-15 ACG1000-AK250、ACG1000-AK260、ACG1000-AK270

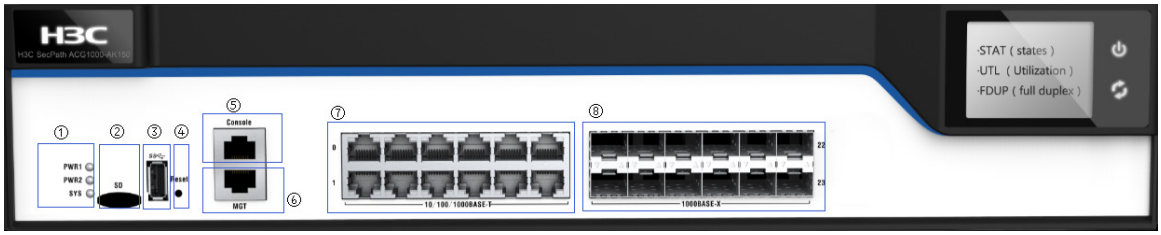


表2-15 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口

图2-16 ACG1000-AK280

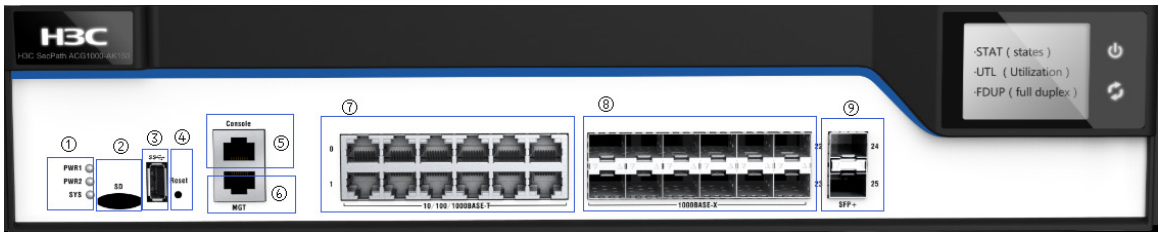


表2-16 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑨万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

这里，支持的扩展接口单板如下：

表2-17 支持的扩展接口卡

单板名称	单板类型	单板俗称	单板印丝名称	备注
4 Combo接口卡	业务卡	4COMBO子卡	NSQM1GC4	4个COMBO口，其中后一对电口支持断电和启动过程硬件bypass，不支持热插拔

单板名称	单板类型	单板俗称	单板印丝名称	备注
1 SFP+接口卡	业务卡	1万兆	NSQM1TGS1	1个万兆SFP+，不支持热插拔
4 SFP+接口卡	业务卡	4万兆	NSQM1TGS4	4个万兆SFP+，不支持热插拔

2.1.2 Bypass接口介绍

Bypass 功能是指通过特定的触发状态（断电或死机）让通过 Bypass 接口互联的两个网络直接物理导通，不再经过网络设备。这样可以有效避免因设备失效而导致的网络单点故障。

当需要使用接口的 Bypass 功能时，接口只能工作在二层模式。如果接口工作在三层模式，则 Bypass 功能不生效。

ACG1000 系列应用控制网关支持 Bypass 功能的款型及其 Bypass 接口如下表所示。

表2-18 支持 Bypass 接口的款型表

Bypass 接口	设备型号
GE0和GE1	• ACG1000-SE-PWR、ACG1000-SE、ACG1000-TE、ACG1000-ME、ACG1000-AE、ACG1000-C9170 • ACG1000-AK150、ACG1000-AK230、ACG1000-AK240、ACG1000-AK250、ACG1000-AK260、ACG1000-AK270、ACG1000-AK280、ACG1000-AK255、ACG1000-AK265、ACG1000-AK275 • ACG1030-X1、ACG1050-X1、ACG1060-X1、ACG1070-X1、ACG1000-C9130、ACG1000-C9150、ACG1000-C9160
GE0和GE1、GE2和GE3	ACG1000-PE、ACG1000-EE、ACG1000-XE1、ACG1000-AK285

3 ACG的工作原理

3.1 基本概念

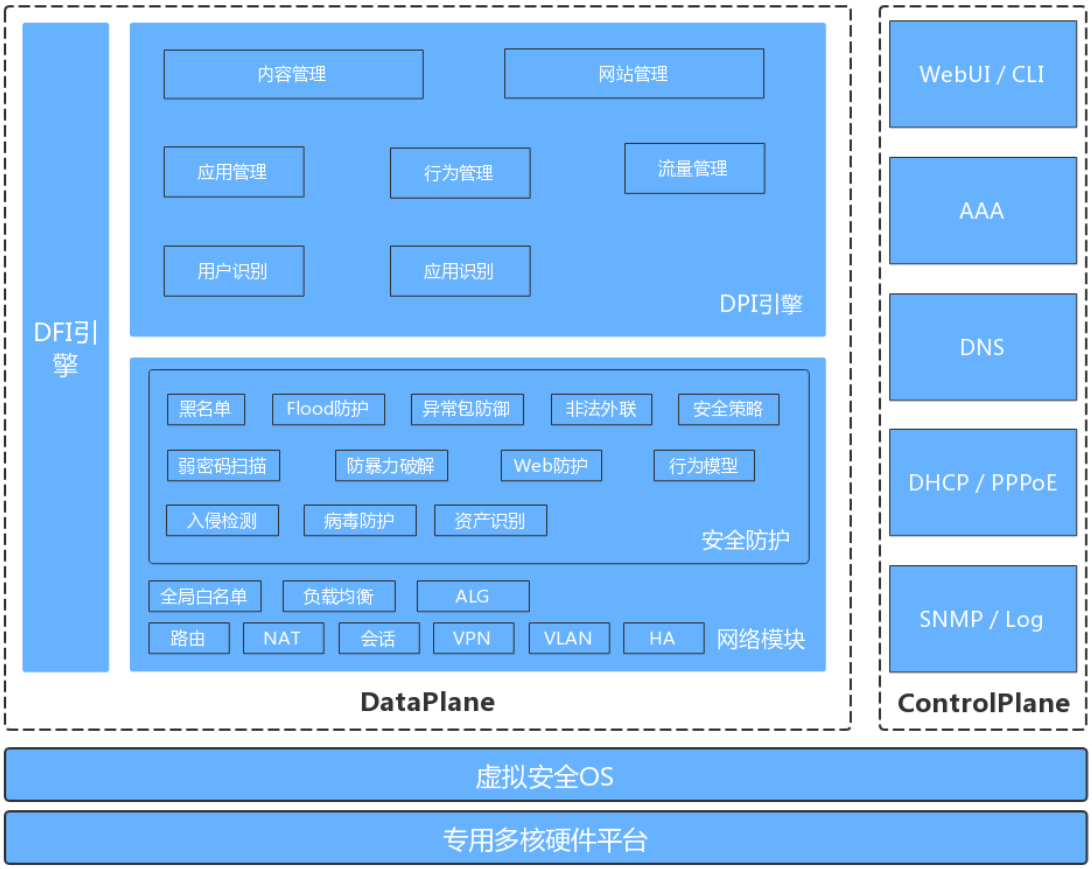
SecPath ACG1000 是 H3C 推出的最新一代应用控制网关。该产品融合了应用控制、行为审计、网络优化等全面功能，为用户提供一个综合、完整的全业务应用场景解决方案。

ACG1000 系列应用控制网关可通过路由模式、透明桥接模式或混合模式部署在网络的关键节点上，对数据进行 2~7 层的全面检查和分析。深度识别、管控和审计近千种 IM 聊天软件、P2P 下载软件、炒股软件、网络游戏应用、流媒体在线视频应用等常见应用，并利用智能流控、智能阻断、智能路由等技术提供强大的带宽管理特性。配合创新的网络应用行为精细化管理功能、清晰易管理日志等功能，提供全面、完善的网络行为管理解决方案。

通过用户管理和应用识别能力，ACG 可以基于七元组（源/目的 IP、源/的端口、服务、应用、用户）来部署安全策略，针对特定用户的特定流量进行包过滤以及内容安全监控，以应对灵活多变的现代网络环境，满足移动办公等 IP 地址不固定的网络场景。

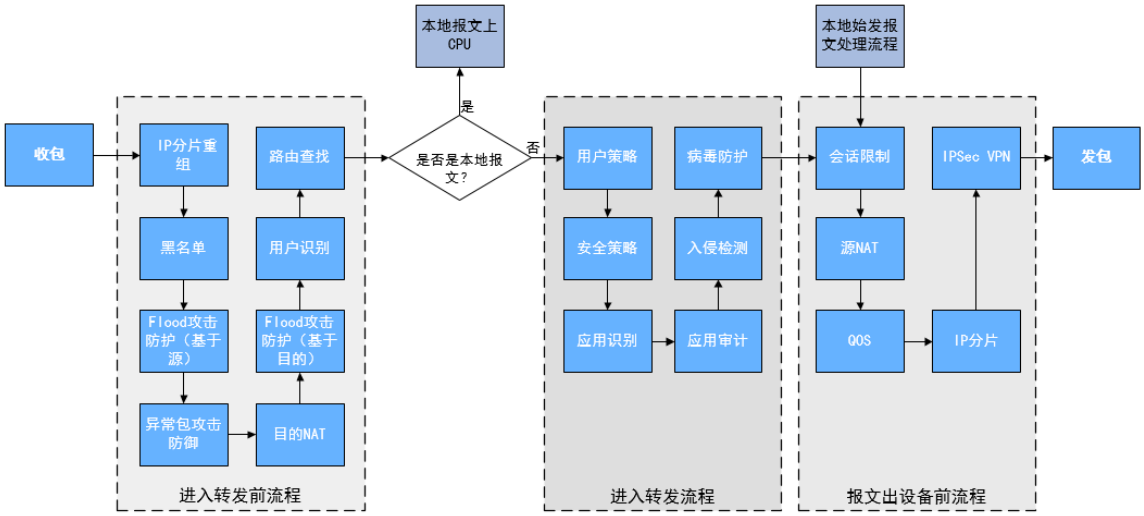
3.2 软件架构

ACG1000 系列应用控制网关采用最新最先进的多核硬件架构，在硬件架构上运行自主知识产权的安全 OS，高效的并行调度算法和内存管理机制提高了流量转发报文的性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统一部分 CPU 专职 CP 工作，大部分 CPU 专职 DP 工作。这样就避免了因系统调度，导致设备转发性能降级或者无法响应管理操作等现象。具体 DP 和 CP 的 CPU 分布根据用户场景定义。



3.3 转发流程

ACG 的转发原理和流程如下图所示：



4 完成ACG的初始配置

4.1 设备出厂配置

ACG 设备出厂配置如下表：

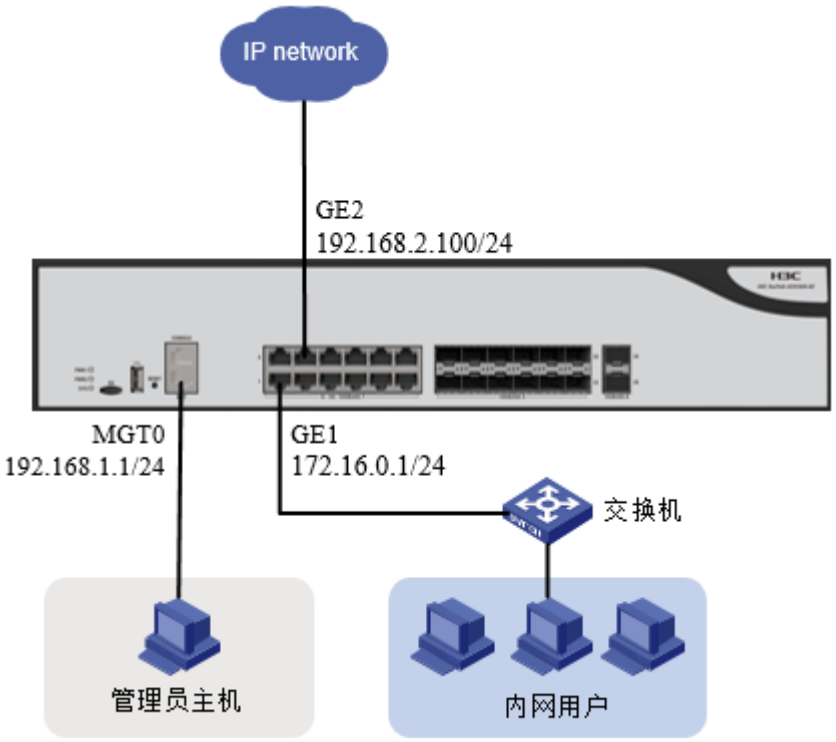
表4-1 ACG 出厂配置

登录信息项	默认配置	备注
用户名	admin	-
密码	admin	使用默认密码登录后，系统会强制要求修改密码，按照提示进行修改。
登录类型	• 通过 Web 界面登录设备 • 通过 Console 口登录设备	ACG支持通过CLI和Web方式进行配置，CLI支持Telnet、SSH等主流通信管理协议。
设备管理口的IP地址	• 接口号：GE0/MGT 接口 • IP 地址：192.168.1.1/24	MGT接口为设备的默认管理口（无MGT接口的设备默认GE0口为管理口） 默认允许对该接口进行PING，HTTPS操作。

4.2 应用场景组网

设备典型组网及连线如图 4-1所示，请根据实际组网需求连接设备。下图以ACG1000-XE1、ACG1000-ME、ACG1000-TE、ACG1060-X1、ACG1070-X1 型号为例：

图4-1 连接线缆图



按照图中的拓扑连接设备的管理网口 MGT0、业务网口 GE1 和 GE2。用网线连接管理员主机的网口与设备的管理网口，用于登录 Web 界面；通过网线将设备的 GE2 接口连接到运营商网络与外部进行通信，将设备的 GE1 口连接到公司内网（此处以 GE1 和 GE2 为例说明，您也可以根据需要使用其他接口）。

如果使用命令行配置设备，在首次登录设备，请使用 Console 配置线连接管理 PC 的串口和设备的 Console 口。

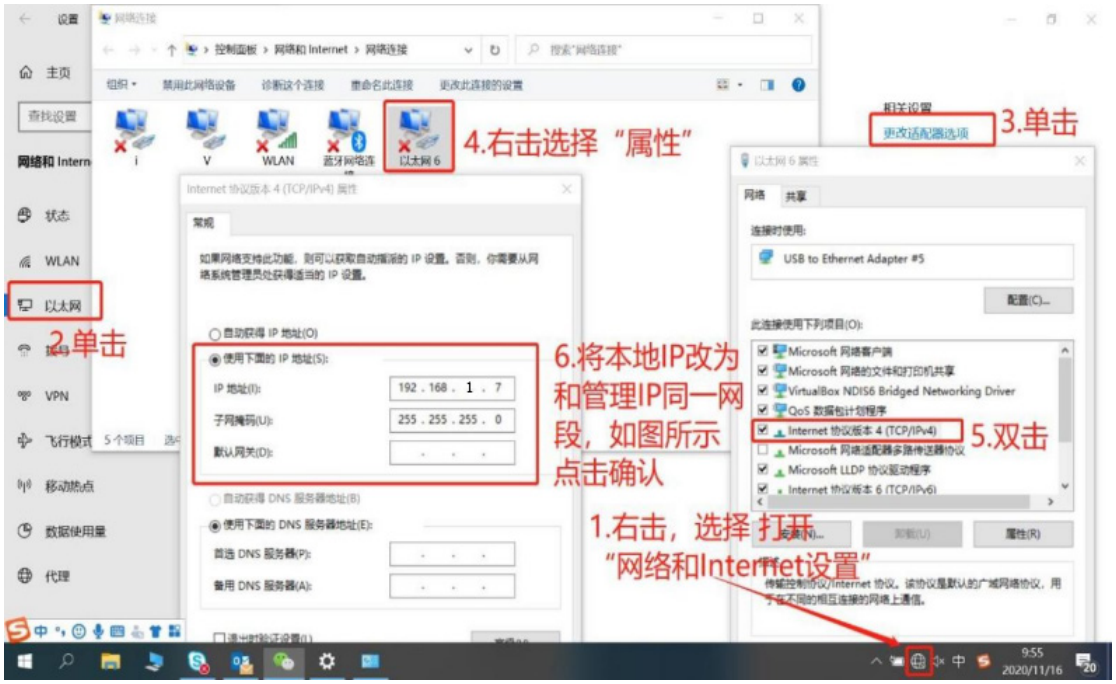
4.3 通过Web方式登录设备

说明

- 推荐使用 IE11.0 及以上版本的浏览器，或者 Google Chrome 69 及以上版本浏览器对设备进行 WEB 管理，。最佳显示分辨率为 1366 × 768，如使用其他版本浏览器可能出现显示上兼容性不佳的情况。

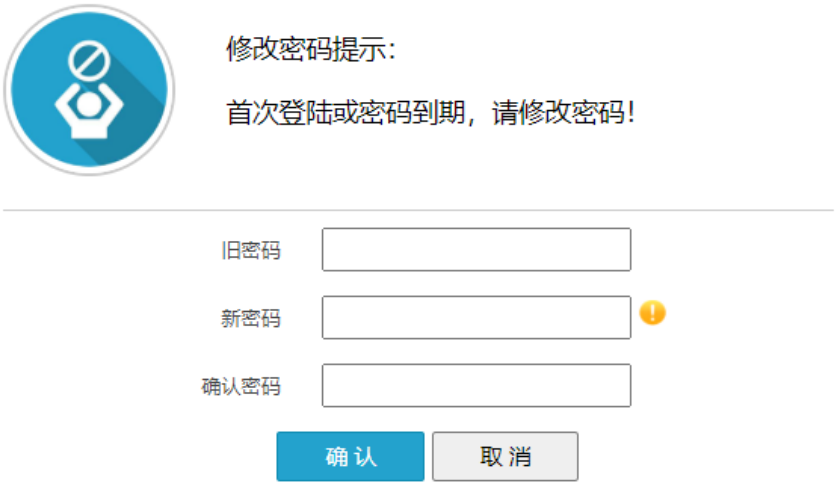
采用 Web 方式登录设备的步骤如下：

(1) 设置管理员 PC 的 IP 地址为 192.168.1.2/24～192.168.1.254/24 中的一个 IP（必须与设备管理接口 IP 地址在同一个网段）。



(2) 在 PC 的 Web 浏览器（推荐使用 Chrome 浏览器）地址栏中输入“https://192.168.1.1”并回车，即可进入设备的 Web 登录界面。

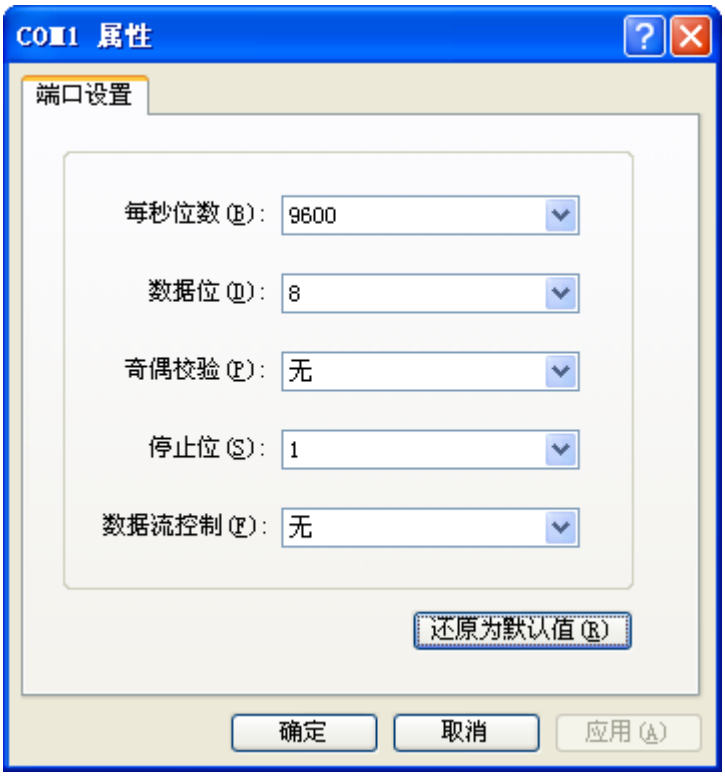
(3) 输入用户名、密码（缺省均为 admin）和验证码，选择系统语言，单击<登录>。首次登录后会提示修改密码，修改密码成功后，重新输入用户名和新密码，单击<登录>即可登录到设备 Web 管理界面主页。



4.4 通过命令行方式登录设备

(1) 连接配置线缆。将配置线缆的 RJ45 连接器端与设备的 CONSOLE 口连接，配置线缆的 DB9 连接器端与 PC 的串口连接。

(2) 在 PC 上使用串口工具登录设备，参照下图设置串口参数。



(3) 打开电源开关，设备会进行自检并且自动进行初始化配置。如果系统启动成功，会显示登录提示。

(4) 在登录提示后输入默认用户名和密码并按回车键，会提示修改密码，修改密码成功后即可进入命令行配置界面。

4.5 部署方式

4.5.1 部属方式简介

ACG 路由部署模式：在不同的网络需求环境下对网络设备部署方式也有严格的要求，ACG 能够工作在三种模式下：路由模式、透明模式、旁路模式。如果 ACG 以三层对外连接（接口具有 IP 地址），则认为 ACG 工作在路由模式下；若 ACG 通过第二层对外连接（接口无 IP 地址），则 ACG 工作在透明模式下；若在不影响网络拓扑的前提下增加网络安全性，则使用旁路模式 ACG。ACG ISP 路由部署模式：一般企业通常会申请多条线进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果联通的服务器通过电信访问，网速就会很慢。安全网关针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由通道，从而提高网络访问速度。

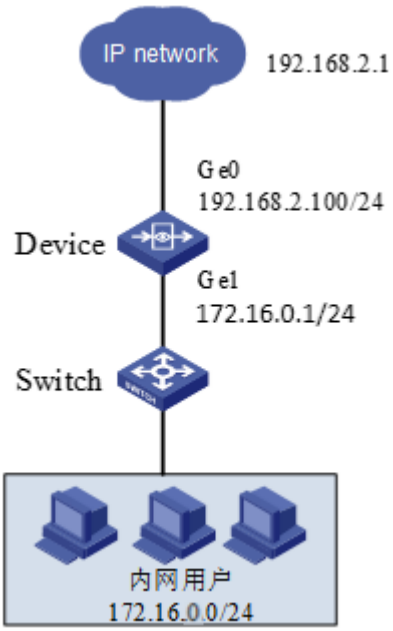
4.5.2 路由模式

1. 组网需求

网络管理人员决定启用路由模式 ACG 实现直接与外网相连，现在需要在 ACG 上做适当配置。

2. 组网图

图4-2 路由模式组网图



3. 配置思路

(1) 配置接口地址

(2) 配置路由

(3) 配置源 NAT

(4) 保存配置

(5) 配置客户端 IP 等信息

4. 配置步骤

(1) 登录 web 界面，进入“网络配置>接口配置>物理接口”，编辑各接口地址。

图4-3 配置接口地址

(2) 配置外网接口ge0，填写接口主地址，管理方式根据访问需要进行选择，接口属性选择“外网口”，如图 4-4所示。

图4-4 配置接口 ge0

若用户购买的上网方式是 ADSL 之类拨号，可在接口处选择“PPPOE”，用户名密码填写运营商提供的上网账号密码，PPPOE 属性中勾选“更新网关”、“更新 DNS”，这样拨号成功后设备会自动生成默认路由，无需手动配置默认路由，管理方式根据访问需要进行选择。

图4-5 ge0 接口配置

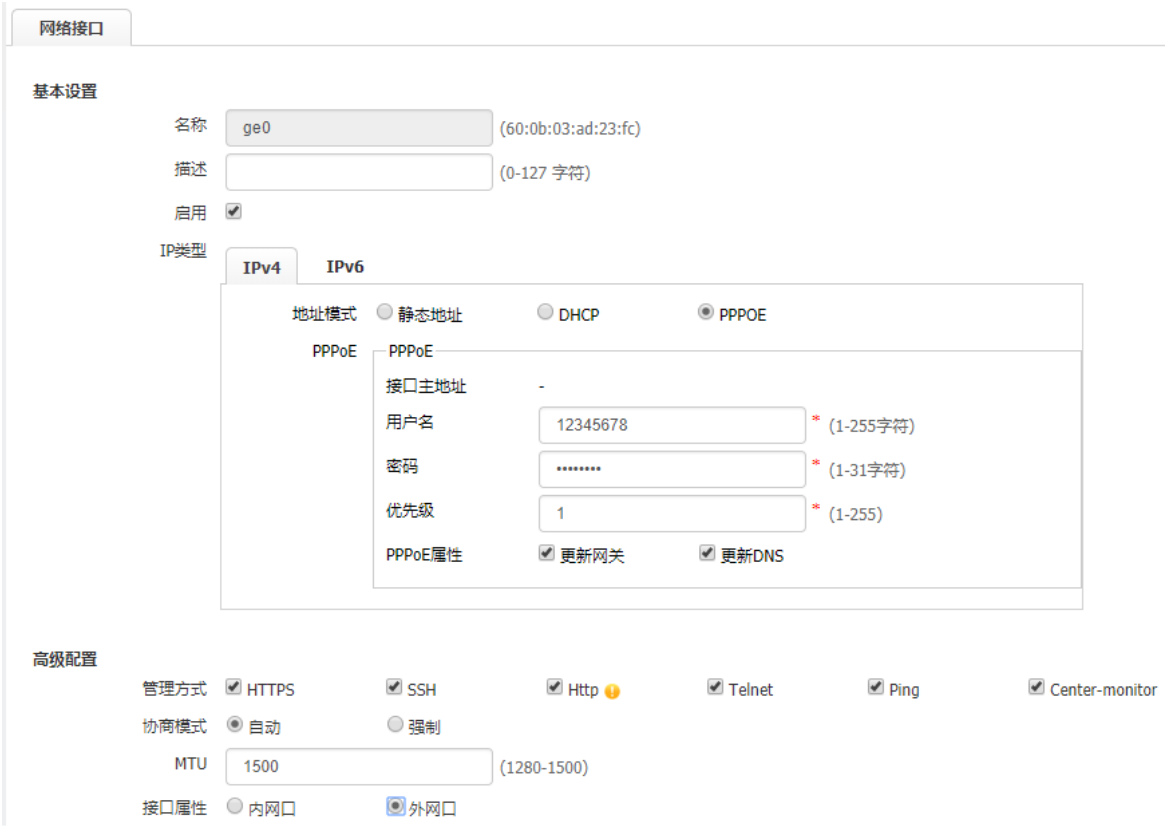

网络接口
基本设置
名称
ge0
(60:0b:03:ad:23:fc)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
PPPoE
PPPoE
接口主地址
-
用户名
12345678
(1-255字符)
密码
(1-31字符)
优先级
1
(1-255)
PPPoE属性
更新网关
更新DNS
高级配置
管理方式
HTTPS
SSH
Http
Telnet
Ping
Center-monitor
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口

图4-6 ge1 接口配置

(3) 配置路由

进入网络配置 > 路由管理 > 静态路由，单击<新建>进入静态路由配置页面，如图 4-7所示。

图4-7 静态路由配置

若公网接口地址模式配置为 PPPOE，拨号成功后，进入“网络配置 > 路由信息 > IPv4 路由表”，可以看到系统自动生成的默认路由，协议为 PPPOE。

(4) 配置源 NAT。进入“策略配置>NAT 转换策略>源 NAT”，点击页面左上角的<新建>按钮：将安全策略中匹配的上网地址（如：any）调用在 NAT 中，转换类型为出接口，接口选择连接外网的接口，配置完成后点击提交。

图4-8 配置源 NAT 规则

(5) 保存配置。

(6) 配置客户端 IP、网关以及 DNS，PC 即可通过 ACG1000 连接到网络中，可以通过 ping 命令检查 PC 的网络连通性。

图4-9 客户端

5. 注意事项

- 使用 PPPOE 拨号时需要更新网关；

- 在配置控制策略时添加上网地址后要点击添加到列表，如未点击添加到列表，则代表此策略不生效；
- NAT 转换时选择正确的出接口。

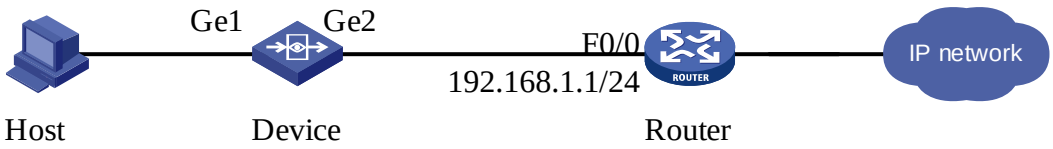
4.5.3 透明模式

1. 组网需求

当固定网络环境中需要添加 ACG 1000，考虑到以路由模式添加对原网络改动幅度较大。选择以透明模式 ACG 加入网络。只需要更改 ACG 两端的接口在同一桥接口内即可。

2. 组网图

图4-10 透明模式 ACG 组网图



3. 配置思路

(1) 配置桥接口

(2) 保存配置

(3) 配置客户端 IP 等信息

4. 配置步骤

(1) 登录 Web 界面，进入“网络配置>接口配置>网桥接口”，新建接口。

图4-11 新建桥接口

(2) 在新建接口内将 ge1、ge2 加入 bvi1 中，可以根据需要对桥接口进行 IP 地址配置。配置桥接口 IP 地址后，可以对 ACG 进行管理，管理方式根据访问需要进行选择。

图4-12 配置桥接口

(3) 保存配置。

(4) 配置客户端 IP、网关以及 DNS。

5. 注意事项

- 透明模式需要配置桥接口，并把内外网接口加入到同一个桥接口下，数据便能通过二层转发。
- 控制策略按从上向下匹配的原则。状态为“ ”的上网策略才会生效。

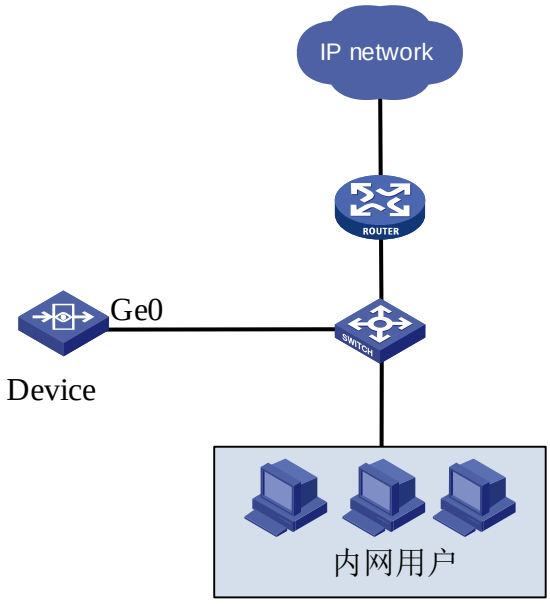
4.5.4 旁路模式

1. 组网需求

公司新增一台 ACG 用于监控用户流量，为了不影响现网拓扑，使用旁路模式部署。

2. 组网图

图4-13 旁路模式 ACG 组网图



3. 配置思路

(1) 配置旁路模式

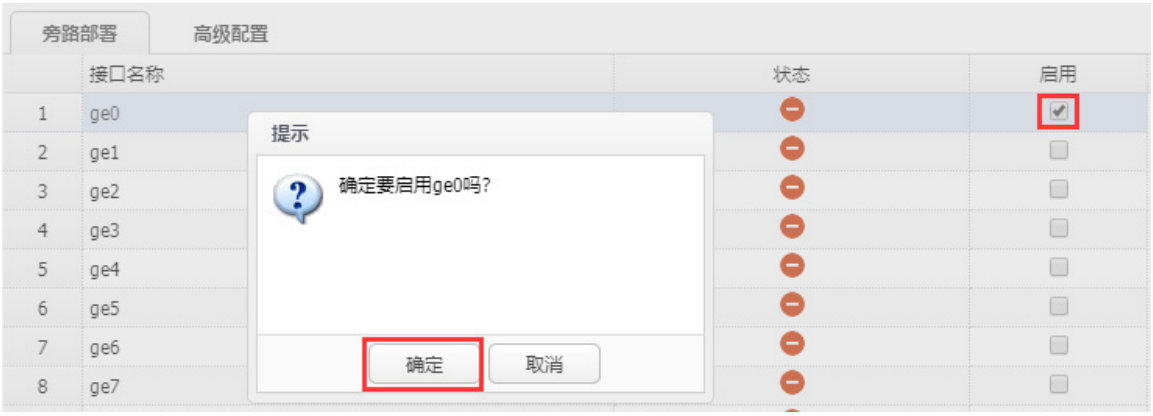
(2) 保存配置

(3) 在交换机上配置端口镜像

4. 配置步骤

(1) 进入“网络管理>基础网络>部署方式>旁路部署”，勾选 ge0 接口，在弹出的对话框中点击“确认”。

图4-14 配置旁路模式



(2) 保存配置。

(3) 在交换机上配置端口镜像，将网络中的双向流量镜像到设备中。

5. 注意事项

- ACG 默认行为为允许所有流量。
- 要将网络双向流量镜像到 ACG 中。

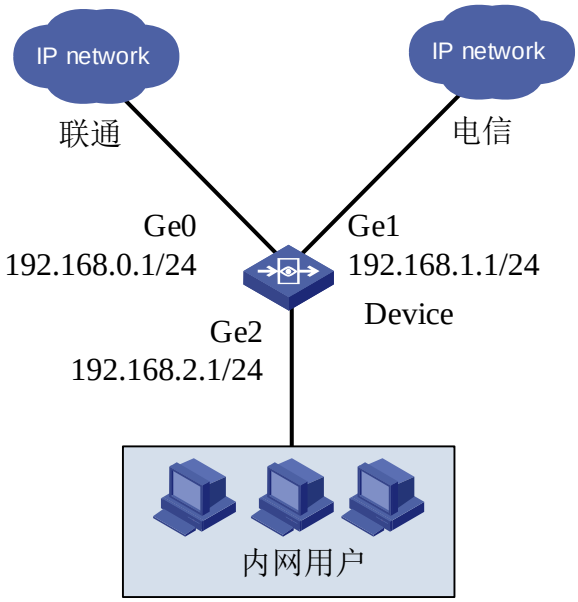
4.5.5 ISP 路由部署

1. 组网需求

公司出口设备，出口使用不同运营商两条线路，正常情况下访问电信网络使用电信线路，访问联通网络使用联通线路。当一条线路出现故障时，所有用户使用另外一条线路访问外网。

2. 组网图

图4-15 ISP 路由组网图



3. 配置思路

(1) 配置接口地址

(2) 配置地址对象

(3) 配置 ISP 路由

(4) 配置源 NAT

(5) 保存配置

(6) 配置客户端 IP 等信息

4. 配置步骤

(1) 配置接口地址

进入“网络配置>接口配置>物理接口”，编辑 ge0、ge1、ge2 接口。

图4-16 ge0

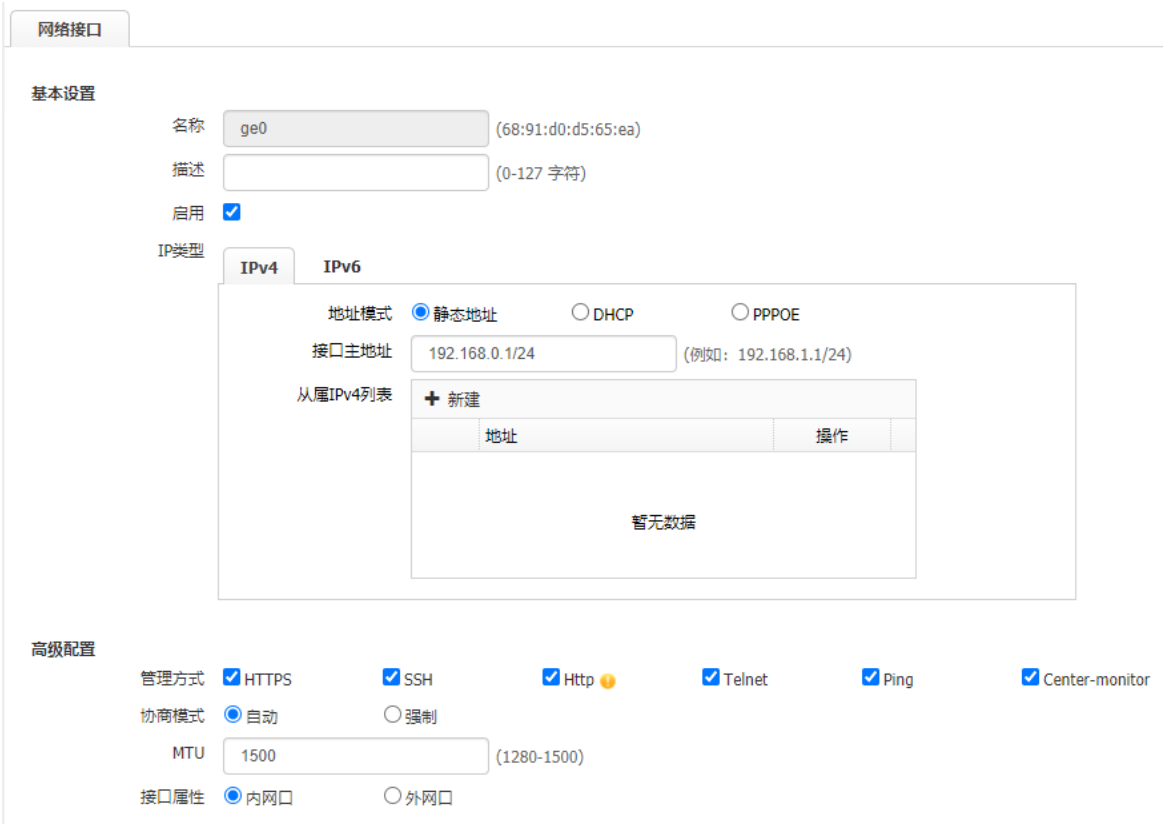

网络接口
基本设置
名称
ge0
(68:91:d0:d5:65:ea)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
接口主地址
192.168.0.1/24
(例如：192.168.1.1/24)
从属IPv4列表
新建
地址
操作
暂无数据
高级配置
管理方式
HTTPS
SSH
Http
Telnet
Ping
Center-monitor
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口

图4-17 ge1

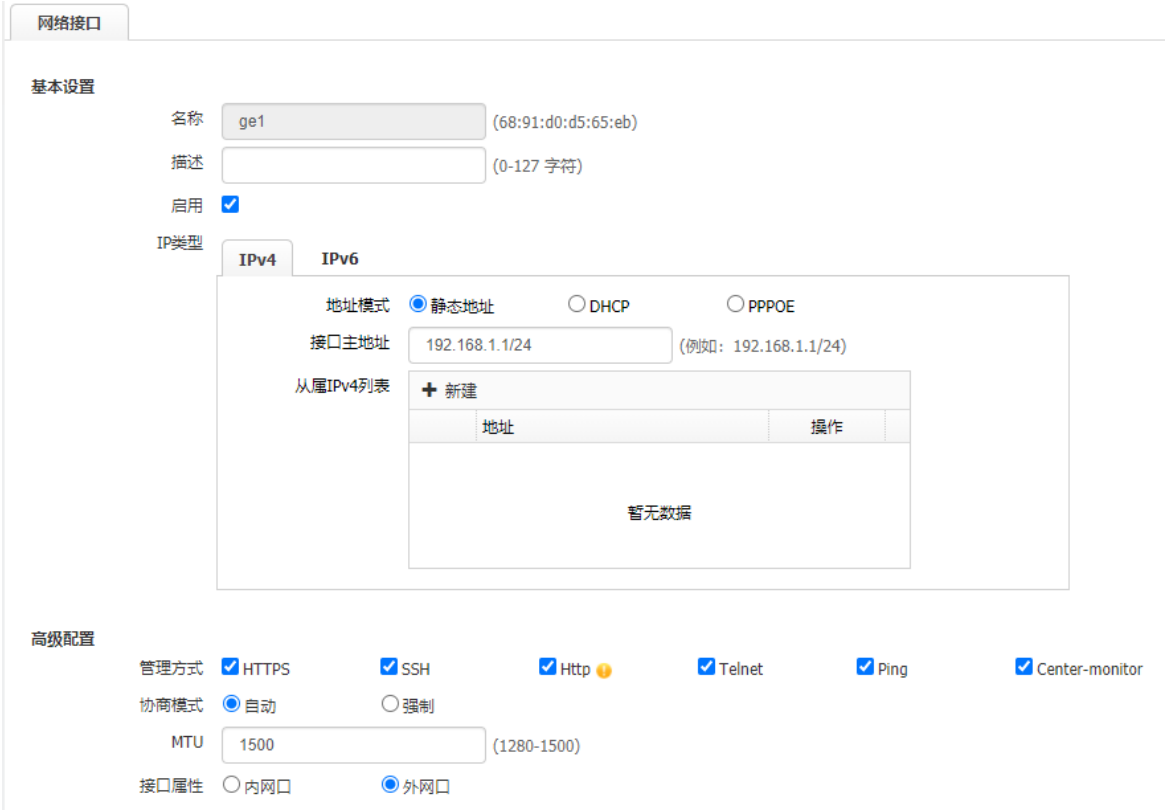


图4-18 ge2

(2)　配置地址对象

进入“策略配置>对象管理>地址对象>地址对象”，点击页面左上角的<新建>按钮，配置地址对象。名称为“上网网段”，地址节点选择子网地址，填写 192.168.2.0/24，点击<添加到列表>，点击提交。

图4-19 配置地址对象

(3)　配置 ISP 路由

进入“网络配置>路由管理>ISP 路由”，点击<新建>。

配置访问联通网络使用联通线路：

图4-20 配置 ISP 路由-联通线路

图4-21 配置 ISP 路由-电信线路

(4) 配置静态路由，进入“网络配置>路由管理>静态路由”，点击<新建>。

图4-22 配置静态路由-联通

图4-23 配置静态路由-电信

当某一接口 Down 掉后，ISP 路由会失效，切换到另一线路，当 ISP 未匹配时，会匹配默认路由。

(5)　配置源 NAT

在源地址处选择上网网段，转换类型为出接口，接口选择 ge0 和 ge1，配置完成后点击提交。

进入“策略配置>NAT 转换策略>源 NAT”，点击<新建>。

图4-24 配置 SNAT-ge0 口

图4-25 配置 SNAT-ge1

(6) 保存配置。

(7) 配置客户端 IP、网关以及 DNS。

将部门某电脑 IP 地址设置为 192.168.2.10/24,网关设置地为 192.168.2.1，DNS 配置为 8.8.8.8（一般设置为当地的 DNS 即可）。电脑可正常上网。

5. 注意事项

- 地址对象要与上网用户匹配。
- 源 NAT 要选择已配置的地址对象。
- 默认路由网关分别为 ISP 提供的 IP 地址。
- 安全策略按从上向下匹配的原则。状态为“ ”的上网策略才会生效。

4.6 版本升级

4.6.1 版本升级的内容

版本的升级包括软件、特征库文件及补丁升级。目的在于解决软件缺陷，更新最新的应用与 URL 特征。ACG 系统的软件需要解决软件缺陷或获取新软件特性，可通过 WEB 界面、命令行升级，当系统运行的主程序由于各种原因丢失或 WEB 界面和命令行均无法进入时，可进入底层 menuboot 程序进行主软件程序升级；通过升级加载热补丁可以在不影响系统运行的情况下，修复相关缺陷。

4.6.2 系统软件升级

在 WEB 界面下升级系统软件版本的步骤如下：

(1) 从官方网站获取新软件版本文件，版本文件必须是以.bin 为后缀。

(2) 进入 WEB 管理界面，进入“系统管理>系统维护>系统升级>手动升级”，点击系统软件后的<选择文件>按钮，选择本地存储的升级文件，点击上传。

图4-26 上传升级版本

(3) 点击上传后会显示文件上传进度条，WEB 界面显示如下提示则表示文件上传成功，可进行下一步操作。

图4-27 升级成功提示

(4) 点击 WEB 界面右上角<保存>按钮保存当前配置。

(5) 进入“系统管理>系统维护>系统重启”，选择系统重启提交后可重启设备。

(6) 点击提交后设备将进行重启，所有业务流量停止转发，同时页面停止响应，重启系统后再次 WEB 登录设备首页，检查首页版本信息是否升级成功。

 说明

升级前请先备份好配置文件。

4.6.3 特征库升级

ACG 系统在线运行时需要周期性的更新特征库，才能更好进行应用识别控制和流量控制。在设备无法正常与互联网进行通信的情况下，可通过 WEB 页面进行特征库手动升级。若设备可正常与互联网进行通信，则可通过设置定期自动从服务器更新最新的特征库 (特征库升级的前提是已经购买并导入授权升级许可，如未购买则无法进行升级，授权许可证查看可参考相关章节)。

登录www.h3c.com官网，在首页 › 产品技术 › 企业级产品 › 信息安全 › 特征库服务专区 › 协议特征库版本(V5)，下载相应的特征库版本。ACG1000_APP_R3.1 对应的是ACG设备的特征库版本，其中-G对应的是R6611 及更新系列版本使用的特征库，不带-G的是R6609 及更早系列版本使用的特征库。

图4-28 官网下载特征库界面

1. 手动升级

通过 WEB 页面手动升级特征库的步骤如下：

(1) 通过在线客户或售后热线电话获取特征库离线文件。

(2) 使用 WEB 管理界面，进入系统管理>系统维护>系统升级>手动升级，点击应用控制特征库后的<选择文件>按钮选择本地存储的升级文件，点击上传。显示文件上传进度条，WEB 界面提示上传成功，可进行下一步操作。

(3) 进入主页>系统信息，查看系统信息，检查首页版本信息，升级成功。升级特征库文件无需重启设备系统即可生效。

2. 自动升级

设置自动从服务器升级特征库的步骤如下：

(1) 按拓扑设置默认路由使设备可访问互联网，进入“网络管理>基础网络>DNS 服务>DNS 透明代理”，设置主备 DNS。

(2) 点击提交设置完成，可在 WEB 界面进入“系统管理>系统维护>系统诊断工具”，通过 ping 百度测试 DNS 解析是否正常。

(3) 登录 WEB 管理界面，进入“系统管理>系统维护>系统升级>自动升级”，选择默认升级服务器，设定周期。设备会在设定的周期内自动从服务器更新最新特征库版本。

(4) 首次安装设备上线，可通过立即在线升级方式更新特征库至最新，进入“系统管理>系统维护>系统升级>自动升级”，点击<立刻升级>按钮。

(5) 进入“主页>系统信息”，查看统信息为升级的版本，升级成功。

4.6.4 注意事项

- 主程序升级需要重启设备，会造成断网，请避开业务高峰期升级。
- 主程序升级有一定风险，请务必保证升级过程中，设备供电稳定。
- 主程序升级前，请认真阅读相关文档。
- 升级不会导致配置、日志文件、库文件、license 丢失。
- 设备要连接互联网时才能升级库文件。
- 配置 DNS 才能检测库文件，自动更新。也可以手动方式检测最新库文件。
- 特征库在线升级过程中，设备需要从外网下载升级包，会占用一定网络带宽，且会影响设备的数据转发，所以建议将自动升级周期设置在业务低峰期。
- F6610 之前版本通过 web 管理页面无法直接升级 R6611P01 的-all 版本。由于 F6610 之前版本通过 web 管理页面升级版本时有 150M 大小的限制，超过 150M 的软件版本无法直接升级，而 R6611P01 的-all 版本超过了此大小，因此无法进行升级。可通过命令行进行升级或先升级为 F6610 及以上不带-all 的版本，再升级-all 的版本。
- 1G 及以下内存的设备，不建议升级到 6610 及以后版本，内存太小会导致 nmi 异常重启。

4.7 授权管理

4.7.1 获取设备信息（需在设备上操作）

设备信息用于在 H3C License 管理平台申请激活码/激活文件。您可通过 Web 页面获取设备信息，如下图所示。

H3C License 管理平台上的“H3C 设备 S/N”，就是设备 Web 页面上的“硬件 S/N”

图4-29 硬件设备信息示意图，在“主页 > 系统信息”页面

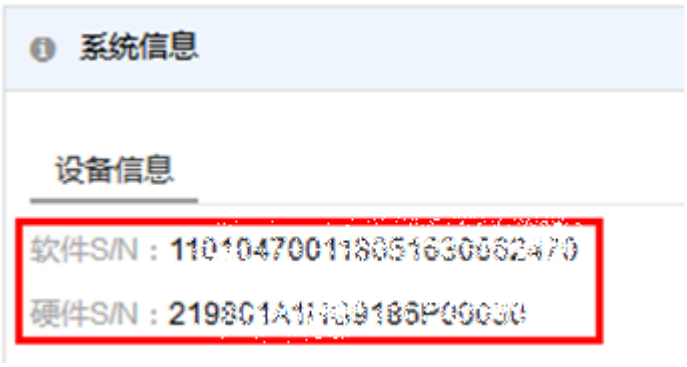


图4-30 ACG1000-V 虚拟产品设备信息示意图，在“监控统计 > 系统信息”页面（此截图适用于VACG E6451 版本）

图4-31 ACG1000-V 虚拟产品设备信息示意图，在“主页 > 系统信息”页面（此截图适用于 VACG E6453 版本及以后版本）

4.7.2 申请激活码/激活文件（需在H3C License管理平台上操作）

1. 功能简介

申请激活码/激活文件需要在 H3C License 管理平台上进行，H3C License 管理平台支持如下申请方式：

- 一次输入一个授权码，绑定一台设备，为一台设备申请一个授权。
- 一次输入多个授权码，您可以将不同授权码和同一设备绑定，也可以将不同授权码和不同设备绑定，从而为一台或多台设备申请授权。

2. 输入授权信息

(1) 在 PC 上启动浏览器，在浏览器地址栏中输入 H3C License 管理平台地址 http://www.h3c.com/cn/License 后按回车键，登录 H3C License 管理平台。

提示

建议使用浏览器：Chrome 62 及以上版本；IE 10 及以上版本；火狐 60 及以上版本。

(2) 单击“License激活申请”页签，进入“License激活申请”页面，如 图 4-32所示。

图4-32 License 激活申请页面

(3) 在输入授权信息页面中，输入授权信息。H3C License 管理平台支持通过以下方式输入授权码，请根据需要进行选择。

- 单个输入授权码

  在 图 4-32所示的授权码输入框中粘贴或手工输入完整的授权码字符串，然后单击<搜索&追加>按钮，H3C License管理平台会自动获取该授权码对应的授权信息。重复执行该操作可输入多个授权信息。

- 上传二维码自动识别授权码

  单击 图 4-32中所示的< ··· >按钮，H3C License管理平台会弹出“上传二维码的授权码图片”页面，如 图 4-33所示。在“上传二维码的授权码图片”页面上传授权码的二维码图片后，单击 图 4-32中所示的<搜索&追加>按钮，H3C License管理平台会自动获取二维码图片关联的授权信息。重复执行该操作可输入多个授权信息。

  提示

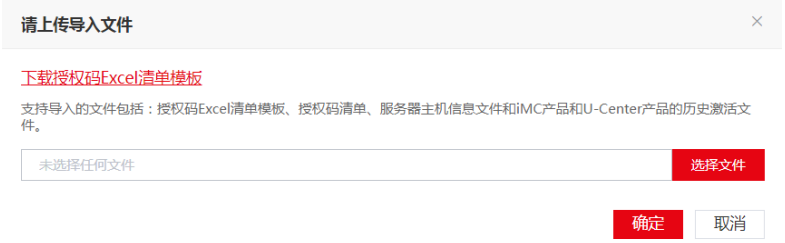
  请确保上传的授权码二维码图片完整、清晰，否则，H3C License 管理平台无法正确识别。

图4-33 上传二维码的授权码图片页面

- 批量导入授权码

  单击 图 4-32中所示的<导入&追加>按钮，H3C License管理平台会弹出“上传导入文件”页面，如 图 4-34所示。

图4-34 上传导入文件页面



H3C License管理平台支持通过授权码Excel清单文件的方式批量导入授权码，单击 图 4-34 中所示的“下载授权码Excel清单模板”链接，下载授权码Excel清单模板，Excel清单模板内容如 图 4-35所示。在模板中输入授权码，保存模板并上传该Excel文件，即可一次导入多个授权码，获取多个授权信息。

图4-35 授权码 Excel 清单模板内容

授权码（用于申请激活文件，必填）	备注：对应授权函上的授权序列号/License Key

(4) 授权信息输入完毕后，选中需要激活的授权码，如 图 4-36所示。单击<下一步>按钮，进入绑定硬件设备页面。

图4-36 授权信息输入完毕页面

说明

对于 SysScan-AE/ME/SE 三款设备首次激活系统功能或者扫描 IP 地址或域名时，这两个授权必须一起进行激活。

3. 绑定硬件设备

(1) 在绑定硬件设备页面中，确认上一步输入的授权码是否为您本次需要激活的授权码。

- 如需新增授权码，可参考 图 4-37进行如下操作：
  - 首先，在上面的工具栏中单击<增加>按钮。
  - 然后，在授权码输入框中粘贴或手工输入整个授权码字符串，或者单击授权码列的<···>按钮上传授权码的二维码图片。
  - 最后，单击<+>按钮，新增授权码信息。
- 如需移除授权码，选中授权码，在上面的工具栏中单击<移除>按钮，删除无需激活的授权码。

图4-37 在绑定硬件设备页面增加授权码

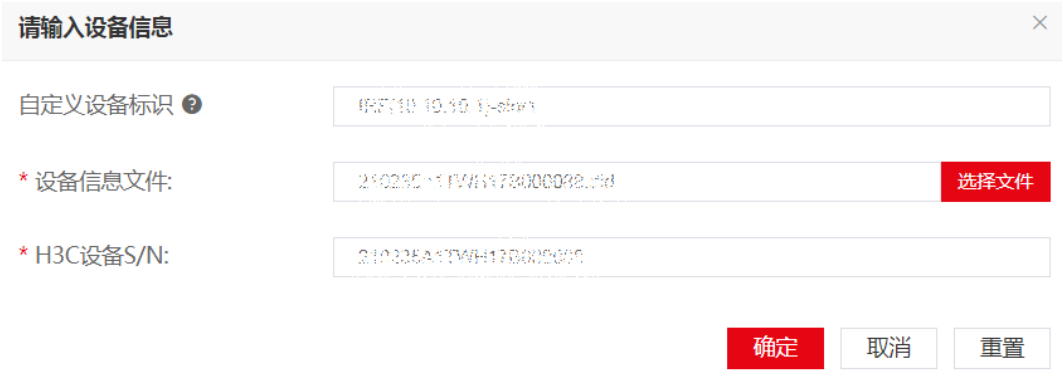
(2) 输入设备信息。

请根据H3C License管理平台页面的提示输入设备信息，设备信息的获取方法请参见“4.7.1 获取设备信息（需在设备上操作）”。H3C License管理平台支持通过以下方式输入设备信息，请根据需要进行选择。

- 一对一绑定

  单击 图 4-37所示列表中自定义设备标识列的<···>按钮，根据页面提示输入设备信息来分别将单个授权码和单台设备绑定，如 图 4-38所示。多次执行该步骤，可以将多个授权码和不同设备绑定。

图4-38 输入设备信息页面示意图



说明

图 4-38所示页面仅为示意图，不同产品此页面的显示信息可能不同，请以设备实际情况为准，并根据页面提示信息输入设备信息即可。

- 多对一绑定

  选中 图 4-37所示列表中需要绑定的授权码，在上面的工具栏中单击<批量录入设备>按钮将多个授权码和同一台设备绑定。

- 多对多绑定

  如 图 4-37所示，请按照以下步骤进行多对多绑定：

  – 首先，选中授权信息并在上面的工具栏中单击<导出>按钮，将所有选中的授权信息导出到一个 Excel 文件。
  – 然后，在导出的 Excel 文件中录入设备信息。
  – 最后，在上面的工具栏中单击<导入>按钮导入 Excel 文件，完成授权码和设备的批量绑定。

说明

- “自定义设备标识”为可选字段，它是用户可自定义的、用于标识一台设备的字符串。为方便您管理和记忆设备，建议您使用设备型号、IP 地址、设备所处地理位置等信息的组合作为自定义设备标识。该标识仅在本次 License 激活申请操作中生效，重新登录 License 激活申请页面后，该标识不再生效。如果您未定义该字段，设备会自动定义该字段。
- 部分产品不支持通过<导出>、<导入>按钮多对多绑定，例如绑定时需要上传设备信息文件的产品。产品是否支持多对多绑定，请以导出的 Excel 文档中的提示信息为准。

对于“非经 SDK 功能”授权的特殊说明：

- 对 ACG 设备进行除了“非经 SDK 功能”的其它功能授权时，请直接根据 H3C License 管理平台页面的提示输入设备信息即可。
- 对 ACG 设备进行“非经 SDK 功能”授权时，在 H3C License 管理平台输入设备信息的界面上，DID 项请选择“码”，如下图所示。

图4-39 设备信息 DID 选择示意图

选择 DID 类型为“码”后，输入 ACG 设备的“软件 S/N 码”，单击<确定>按钮，选择产品分类，如下图所示。

图4-40 产品分类选择示意图

在产品分类中，ACG 硬件设备选择“安全_ACG1000”产品分类；ACG1000-V 虚拟产品选择“安全_网络行为审计”产品分类。选择产品分类后，按照 H3C License 管理平台出现的内容输入设备信息即可。

(3) 将所有需要激活的授权码和设备绑定完毕后，请阅读并勾选“我已了解：授权码与硬件设备绑定后，对应的授权就与硬件设备进行了绑定。进行绑定操作时，请确保输入信息的准确，以免因授权码与硬件设备的错误绑定，导致目标设备没有获得正确的授权。”，如 图 4-41所示。单击<下一步>按钮，进入用户数据录入页面。

图4-41 绑定硬件设备完毕页面

4. 用户数据录入

请在用户数据录入页面中，根据 图 4-42所示要求输入用户信息，各参数的详细描述请参见 表 4-2。H3C License管理平台将根据您输入的信息来记录执行本次授权操作的用户信息。

输入用户信息后，单击<下一步>按钮，进入确认并激活页面。

图4-42 用户数据录入页面

表4-2 用户信息描述表

参数名称	参数描述	是否必须填写
最终客户单位名称	使用授权的最终用户的单位名称	必填
申请单位名称	您所在工作单位的名称	必填
申请联系人姓名	您的姓名	必填

参数名称	参数描述	是否必须填写
申请联系人电话	您的联系电话	必填
申请联系人E-mail	您的E-mail邮箱 注意 您的 E-mail 邮箱非常重要，用于接收 H3C License 管理平台生成的激活码/激活文件，请确保输入的邮箱地址正确并处于可用状态。	必填
申请联系人邮编	您所在位置的邮政编码	可选
申请联系人地址	您的联系地址	可选
项目名称	应用授权的项目名称	可选
验证码	网站显示的验证码，将网站显示的验证码直接输入即可，不需要区分大小写	必填

5. 确认并激活

(1) 请您核对授权信息和设备信息，确认无误后，阅读并勾选“已阅读并同意法律声明所述服务条款各项内容H3C授权服务门户法律声明”，如 图 4-43所示。单击<确认并激活License>按钮。

图4-43 确认并激活页面

(2) 再次核对授权信息和设备信息，在如 图 4-44所示页面中单击<确定>按钮。

图4-44 核对授权信息和设备信息页面

单击<确定>按钮后，H3C License 管理平台会自动生成激活码/激活文件，并将激活码/激活文件发送到“申请联系人 E-mail”对应的邮箱。

- 如果将一个授权码和一台设备绑定，H3C License管理平台会为该设备生成一个激活码/激活文件，并对应提供一个<获取激活信息>按钮来获取这个激活码/激活文件，如图 4-45所示。

图4-45 激活申请成功页面

- 如果将多个授权码和一台设备绑定，H3C License管理平台会为该设备的激活码/激活文件生成一个压缩文件，并多行共用一个<获取激活信息>按钮来获取相关激活信息，如图 4-46所示。

图4-46 激活申请成功页面

(3) 获取激活信息，您可以通过以下方式获取激活信息：

- 单击图 4-45中所示的<获取激活信息>按钮，可复制激活码或者将激活文件下载到登录PC。
- 单击图 4-45中所示的<批量获取激活信息>按钮，可一键获取本次申请激活操作申请到的所有激活码/激活文件（如 图 4-47所示）以及激活信息描述表（如 图 4-48所示）。

提示

推荐使用<批量获取激活信息>按钮方法，因为激活信息描述表能帮助您记录和管理激活文件。

图4-47 批量获取激活信息

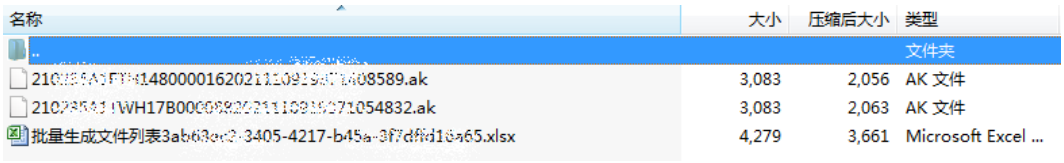
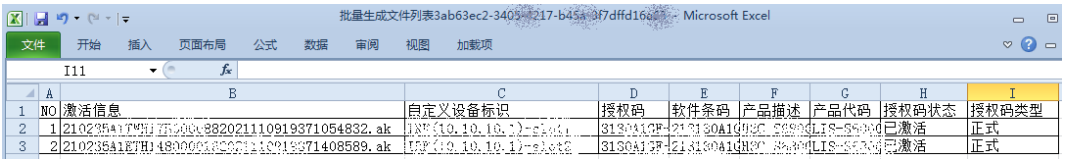


图4-48 激活信息描述表



- 登录“申请联系人 E-mail”对应的邮箱，查收激活码/激活文件。

提示

- 通常情况下，一个授权码会对应生成一个激活码/激活文件。
- 部分产品为简化激活码/激活文件的安装和管理，当您为同一台设备申请激活多个授权时，H3C License 管理平台会将多个授权码合并生成一个激活码/激活文件。
- 只要是 H3C License 管理平台成功生成的激活码/激活文件，不管生成的是一个还是多个激活码/激活文件，将这些激活码/激活文件安装到设备上后，您都会获得所有授权码中包含的授权，不会影响授权的使用。
- 当您申请多个激活文件时，网站需要一定时间来生成激活文件，请根据 H3C License 管理平台的提示信息，通过“申请联系人 E-mail”邮件获取激活文件，“确认并激活”页面将不再在 Web 页面上提供下载功能。
- 如果没有获取到激活码/激活文件，且使用授权码无法重新申请激活码/激活文件时，请联系 H3C 技术支持人员。

4.7.3 安装激活码/激活文件（需在设备上操作）

注意

在安装激活码/激活文件前，请备份并妥善保管您获取的激活码/激活文件。当误操作将激活码/激活文件删除，或者设备故障授权不可用时，可使用备份的激活码/激活文件恢复授权。

请您将从 H3C License 管理平台申请到的激活码/激活文件安装到设备上，以便获得授权。

- 如果您从 H3C License 管理平台申请到的是激活码，请在设备上安装激活码。
- 如果您从 H3C License 管理平台申请到的是激活文件，请在设备上安装激活文件。

请通过 Web 页面登录设备，执行以下操作安装激活码/激活文件：

选择“系统管理 > 系统维护 > 授权管理”，进入授权管理页面，单击<导入许可证>按钮进行导入，在授权管理页面输入获取的激活码。如下图所示。

图4-49 安装激活码示意图

说明

使用多个授权码生成的多个激活码，需要分别导入设备进行授权。

4.7.4 注意事项

- 授权码仅可以完成绑定一次，绑定成功后授权码失效不能再次被绑定。
- 激活码只能导入与其绑定的软件 S/N 设备和设备 S/N 中，无法导入其他设备系统中。
- 激活码导入设备后，设备端开始生效。

4.8 策略配置

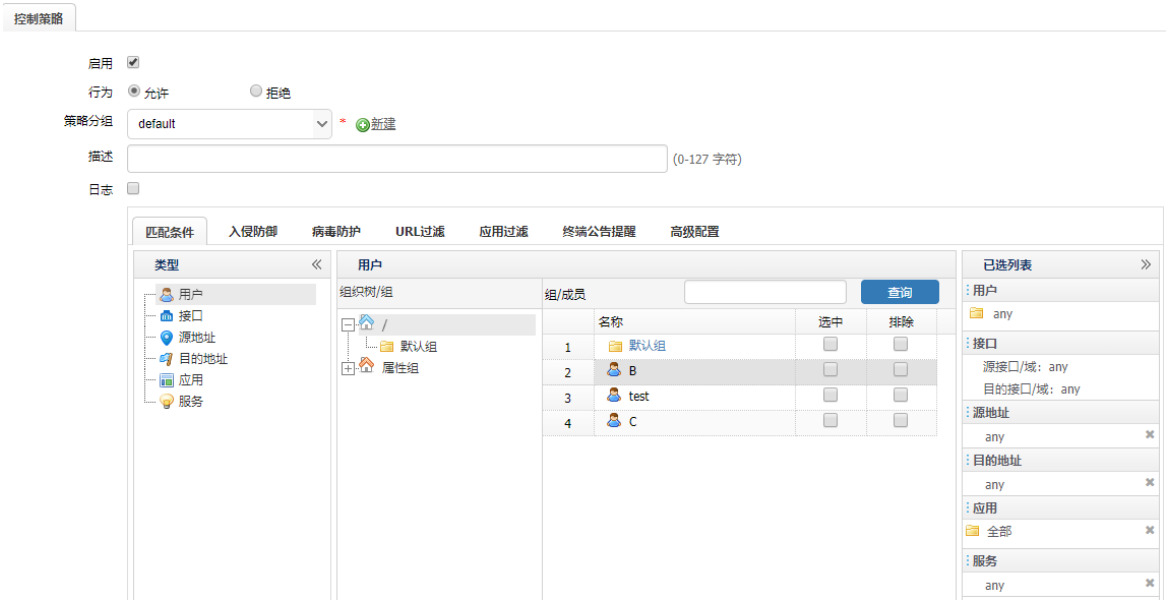
4.8.1 配置控制策略

1. 控制策略说明

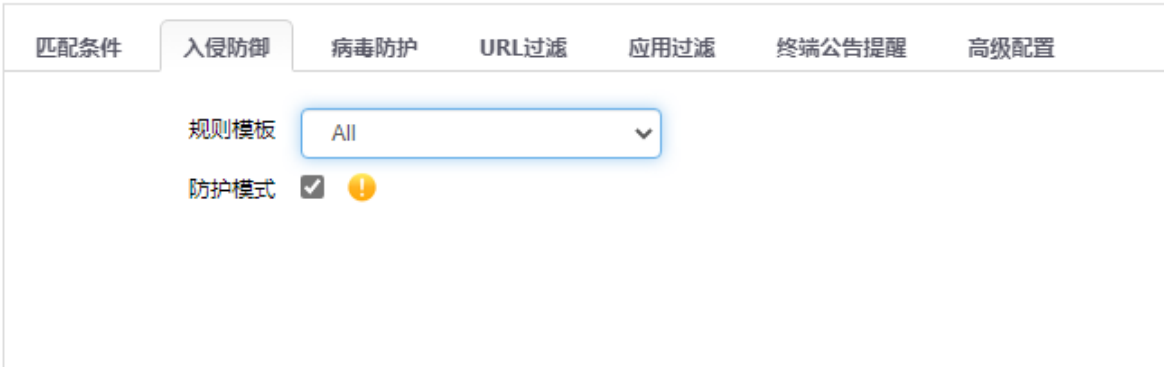
设备通过一体化策略实现对用户行为进行控制或审计。用户可以通过控制策略实现对内网用户或者安全域之间的访问控制，同时支持对匹配策略的流量进行入侵检测、病毒检测以及恶意 URL 检测，保障用户上网时的安全。

2. 配置步骤

(1) 新建控制策略设置策略动作，并配置匹配条件，只有符合匹配条件的流量才会进入后续的策略控制（入侵检测等）流程。



(2) （选配）选择入侵防御规则模板，默认有 All、Windows、Unix-like 和 Webserver 四种，包含相应场景下的 IPS 规则，如果默认规则的动作无法满足实际需求，可以引用派生修改后的规则模板。



(3) （选配）配置防病毒策略。支持 http、ftp、imap、pop3、smtp 协议，病毒文件类型需要在防病毒设定中进行设置。

(4) （选配）配置 URL 过滤策略。设备内置部分恶意 URL 特征，可以通过此设置过滤这部分恶意 URL。

(5) （选配）配置应用过滤策略。应用过滤可以根据不同应用设置规则。

(6) （选配）配置终端公告。用于给内网终端提示或者警告。例如发现有访问恶意 URL 地址，可以将相关的公告页面推送给用户。

(7) 完成高级配置。配置规则生效时间以及限制的终端类型等。完成后，单击“提交”完成配置。

4.8.2 配置审计策略

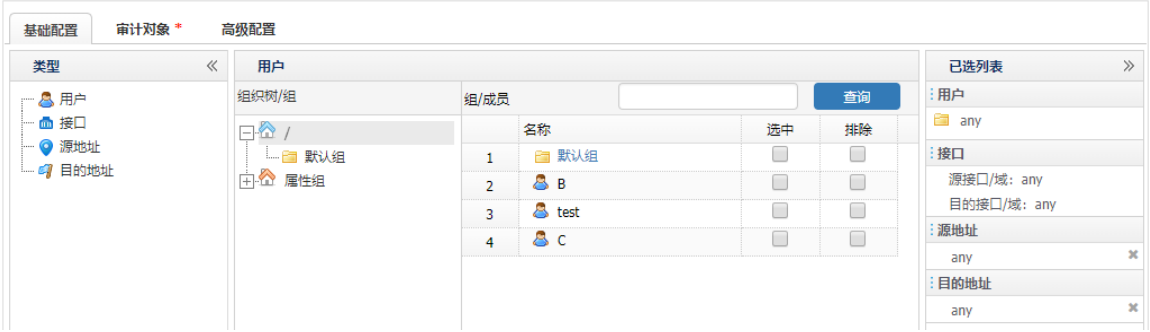
1. 审计策略说明

通过配置审计策略，可以对内网用户访问外网进行审计控制，并记录相关的审计日志。

当前支持的应用主要包括：IM 类、社区类、搜索引擎类、邮件类、文件传输类、股票娱乐类及其它应用类等。

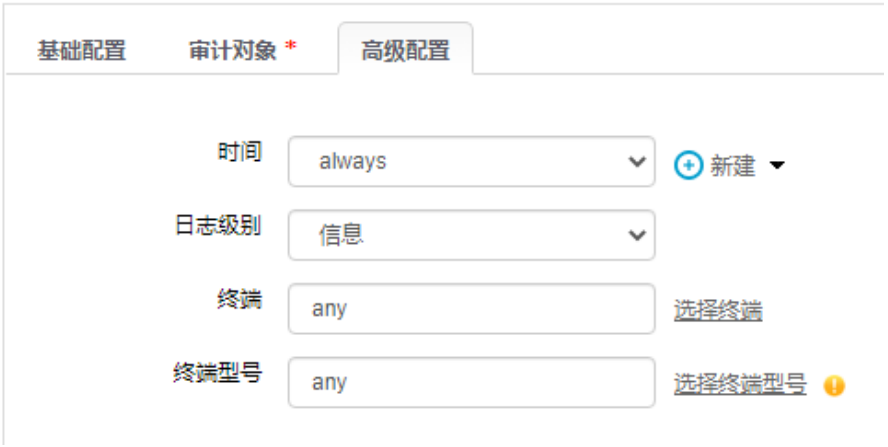
2. 审计日志配置步骤

(1) 新建审计策略，配置基础配置，即需要审计的流量的匹配条件。



(2) 配置审计对象，勾选需要审计的类型以及详细内容。

(3) 完成高级配置，并提交配置。



4.9 完成配置

完成配置后，请在主页面的右上角的快捷工具栏中单击保存配置。至此，您已经完成了设备的快速上线配置。

5 高级功能

5.1 用户认证

5.1.1 用户认证简介

用户认证是一种身份验证机制，通过认证可以验证访问者的身份，同时可以获取用户和 IP 地址的对应关系，用户认证是基于用户配置策略的基础。主要作用如下：

- 进行权限管理，只有具有相应权限的用户才能访问特定网络资源；
- 通常终端的 IP 地址是动态变化的，给针对终端的上网行为管理、统计分析等带来了不便。用户认证将网络流量的 IP 地址识别为具体的用户，可以基于用户维度进行精细化的管理。

ACG 支持本地 WEB 认证、微信认证、短信认证、Portal 认证、免认证、单点登录、访客二维码认证、IC 卡认证、APP 认证、POP3 认证、钉钉认证、混合认证等多种认证方式。

通过 ACG 设备配置用户认证的流程如下：

(1) 配置认证服务器（可选）。

(2) 设置认证方式。

(3) 设置认证模板。

(4) 配置认证策略。

5.1.2 应用场景

本地认证既可以由设备完成，也可以通过第三方认证服务器完成，如果用户和密码存储在设备本地，则认证过程在设备上进行；如果用户和密码存储在第三方认证服务器，则认证通过第三方认证服务器完成（如 Radius/LDAP），称为第三方认证。

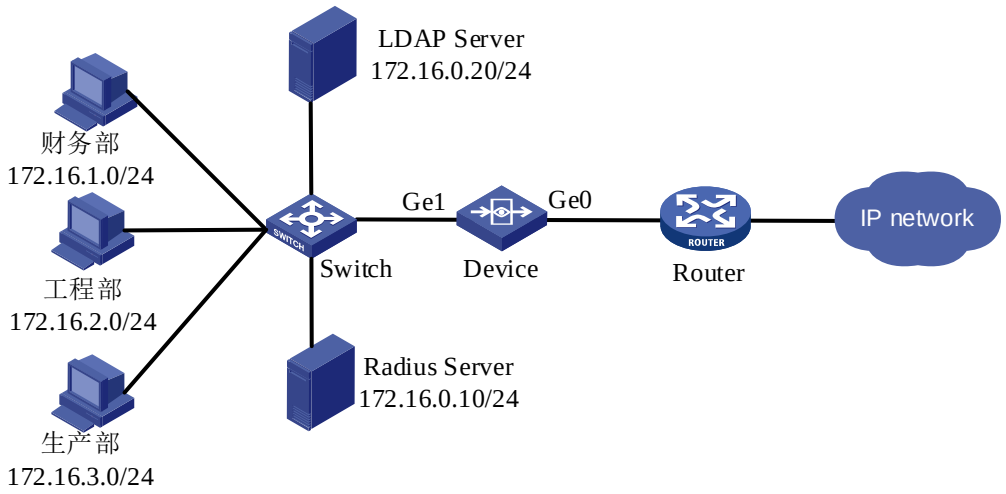
- 用户和密码存储在设备本地

管理员在设备上创建用户/密码，内网终端在访问网络资源之前，需要经过设备的认证。完成认证后，终端 IP 关联上认证用户。终端在访问网络资源时，设备根据基于该用户的策略，决定是否放通流量。

- 第三方认证：

如果网络中已经部署了第三方认证服务器（Radius/LDAP），那么管理员不需要再在设备上配置用户的账号和密码等属性。可借助第三方认证服务器完成对用户的认证，从而实现用户的统一管理，减少配置及维护的工作量。

图5-1 用户认证功能组网图



如图 5-1所示，财务部进行Web认证上网，用户名和密码存储在设备的本地；工程部进行Web认证上网，用户名和密码存储在Radius服务器上；生产部进行Web认证上网，用户名和密码存储在LDAP服务器上。

5.1.3 配置方法

用户认证功能的配置详情，请参见《H3C SecPath ACG1000 系列应用控制网关 典型配置举例》中“用户认证功能典型配置举例”。

5.1.4 配置注意事项

- 设备的配置 Web 认证时，允许用户的 TCP 三次握手报文、DNS 报文以及 ICMP 报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。
- 如果需要实现访问某些资源时免 Web 认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的目的 IP 地址排除即可。

5.2 流控

5.2.1 流控简介

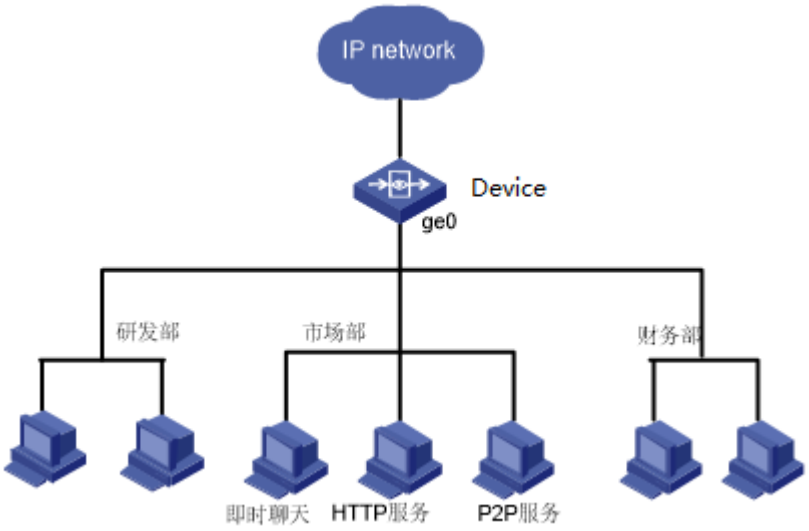
流量管理是通过流量分析，对各种上网流量大小进行精细控制的一种方法。传统的流量管理功能仅仅是对带宽进行限制，无法根据应用、服务、用户进行带宽限制，设备的流量管理具有如下特点：

- 使用虚拟线路和管道，实现层次化的流量管理
- 支持优先级，确保高优先级的应用能够获得带宽
- 支持保障带宽和最大带宽
- 支持弹性带宽或带宽借用，充分利用网络资源
- 能够根据应用、服务、用户、IP 地址组进行流量控制
- 能够分别对 Ingress/Egress 流量进行控制

- 能够保障用户公平使用带宽
- 能够自动分辨低时延的特殊应用，避免上行拖垮下载的特殊情况。

5.3 应用场景

图5-2 流控组网图



- 通过最大带宽、保障带宽和连接数限制，对企业实施带宽管理

在企业日常办公环境中，Email、ERP 等流量可以认为是关键业务流量；而 P2P、在线视频等流量可以认为是非关键业务流量。管理员经常面临企业的有限带宽长时间被非关键业务流量占据，而关键业务的流量却无法得到保证，导致正常业务受到影响，引起投诉。

设备提供的整体最大带宽限制和整体带宽保障功能，可以有效限制企业非关键业务流量占用的带宽，而且可以针对关键业务的流量进行保证，确保可以在流量高峰时段正常转发。

- 通过每 IP/每用户最大带宽，对内网的每 IP 地址或每用户实施带宽管理

企业内网员工通过源 NAT 方式访问互联网，同时企业内网服务器使用 NAT Server 方式对外提供访问服务。由于企业出口带宽有限，而少数用户却占用了大多数的带宽资源，对外提供服务的某些内网服务器也占用了较大的带宽，这些问题都严重影响了企业正常运作。

设备提供的带宽管理功能，在源 NAT 或者服务器映射（NAT Server）场景下，可以配置每个员工能够使用的最大带宽资源或者每服务器对外可提供的最大带宽资源，从而实现细粒度的带宽管控。

5.3.2 配置方法

流控功能的配置详情，请参见《H3C SecPath ACG1000 系列应用控制网关 典型配置举例》中“QoS 通道限速功能典型配置举例”。

5.4 日志

5.4.1 日志简介

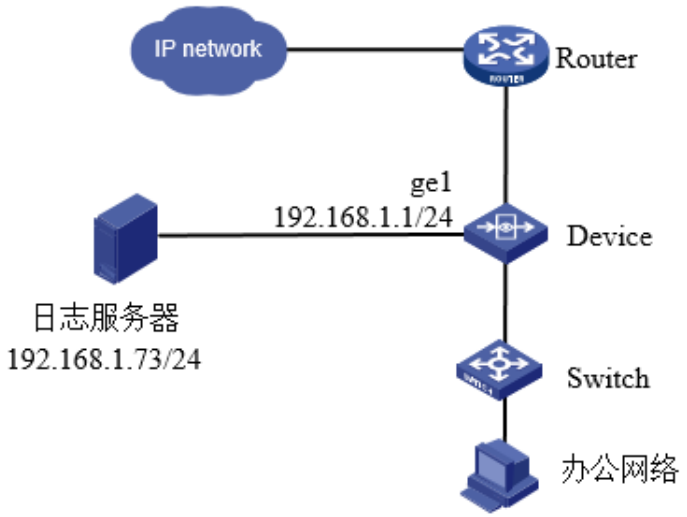
设备拥有日志管理功能，可以记录并输出各种日志信息，当前支持的日志主要有如下几种：

- 系统日志：记录系统的状态信息。
- 操作日志：记录系统操作信息等。
- 控制日志：主要是应用控制日志和恶意 URL 日志。
- 审计日志：主要包括访问网站日志、IM 聊天软件日志、社区日志、搜索引擎日志、邮件日志、文件传输日志、娱乐/股票日志、协议审计日志及其它应用日志。
- 安全日志：主要是入侵防御日志、病毒防护日志、安全防护日志、WEB 防护日志、防暴力破解日志、弱密码防护日志等。
- 终端日志：包括用户上下线日志、共享接入日志、移动终端日志、流量限额日志、DDI 终端用户日志及用户自注册日志。

5.4.2 应用场景

设备系列支持本地日志及第三方日志两种日志记录方式。

- 本地日志：可以通过配置日志模块中的日志过滤部分，将产生的日志记录在本地数据库中。
- 第三方日志：可以通过配置日志模块中的日志服务器及日志过滤部分，将日志发送到远程日志服务器在日志服务器上查看日志信息，或者将日志发送到日志分析与管理平台，通过日志分析与管理平台对设备的日志进行分析、留存。



5.4.3 配置方法

流控功能的配置详情，请参见《H3C SecPath ACG1000 系列应用控制网关 典型配置举例》中“日志功能典型配置举例”。

5.5 HA

5.5.1 HA特性

HA 是 High Availability 缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

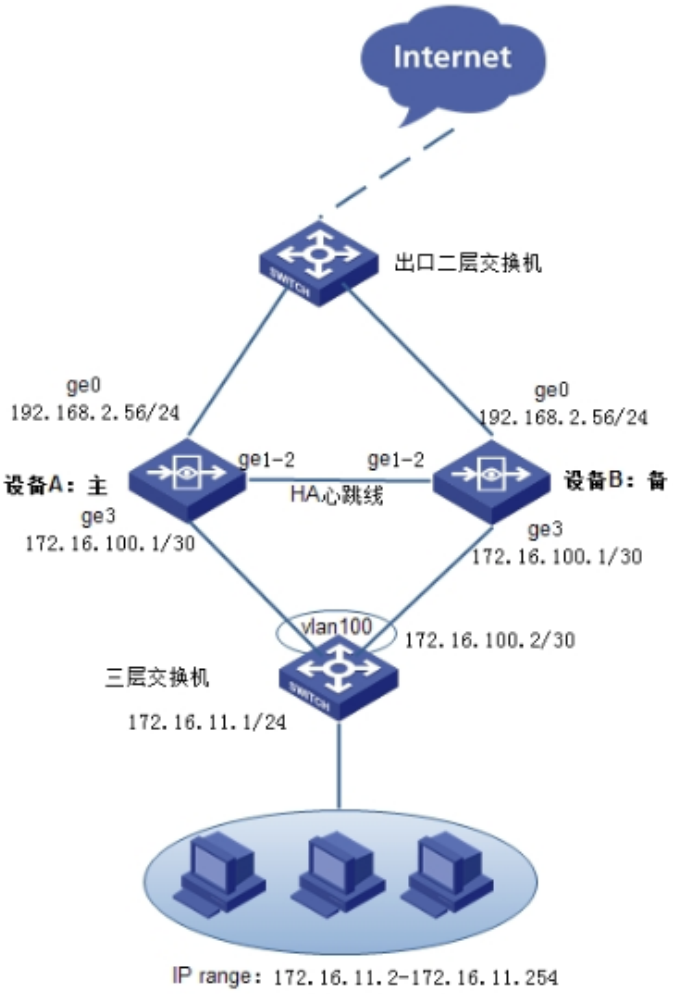
在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

本产品通过双机热备来实现 HA。

5.5.2 应用场景

设备 A 和设备 B 工作在路由+NAT 模式，并以 HA 主备模式部署，实现热备份，接入网络，两台设备开启本地 web 认证，主设备 A 上的业务配置会实时同步给备设备 B，当设备 A 发生故障后，备设备 B 切换为主，继续转发数据。

图5-3 HA 主备路由模式三层组网图



5.5.3 配置方法

流控功能的配置详情，请参见《H3C SecPath ACG1000 系列应用控制网关 典型配置举例》中“HA 主备典型配置举例”。

6 更多参考信息

至此，您已了解和掌握了防火墙的基本功能和部分常用的高级功能。后续您可以登录 H3C 官网，访问“文档中心”或“知了社区”获取更多的产品知识。

图6-1 文档中心二维码

产品资料的具体获取方法请参考 图 6-2。

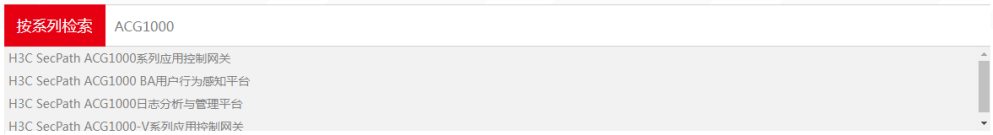
图6-2 产品资料获取方法示意图

按产品检索 ➡ 选择 [安全]

各产品栏目中的资料根据款型系列划分，您可以在清单中直接点击进入具体产品的资料栏目。

快速检索 ➡ 输入产品系列名称的关键字 ➡ 从关键字匹配结果中选择其一

快速检索功能为您提供了在产品栏目中快速定位到具体产品资料入口的便捷操作。



常见资料栏目

全部文档	显示本产品栏目下全部文档
文档合集	资料书架　CHM文档包
快速系列	快速安装　快速配置　产品FAQ
视频专区	安装视频　产品介绍视频　技术介绍视频　配置视频
了解产品	产品介绍　安全和兼容性手册
了解技术	技术白皮书　技术介绍
安装升级	安装指导　可插拔部件手册　升级指南　License指南　Visio模具
配置调测	配置指导　典型配置举例　高危操作手册　安全加固手册
参考指南	命令参考　日志参考　MIB参考
诊断维护	故障处理手册
二次开发	开发指南　API参考
工　　具	命令查询　日志查询　H3C个人资料库

说明：安全产品系列众多，针对不同产品系列配套的资料栏目和手册稍有差异，请以网站显示为准。