

HCIE-Security 备考指南

接口管理（NIP）



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 接口管理（NIP）需要掌握的知识点.....	1
接口配置.....	1
HCIE-Security 模拟面试问题及面试建议	13

HCIE-Security 接口管理（NIP）需要掌握的知识点

- 掌握 NIP 接口管理的配置

接口配置

设备接口分管理接口和业务接口两类。

查看接口状态图

接口状态图，展示了设备上当前接口的工作状态，以及固定接口主板和接口卡的面板指示灯。查看接口状态图，可帮助你了解当前设备的接口状态及其运行情况。

如果需要对各接口进行相关配置，单击接口图标，可进入该接口的配置界面进行相关配置。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口配置”页签。
3. 查看当前接口的工作状态。

如果需要了解接口状态是否为 Up，请参见接口状态图中的接口状态标识说明。

将鼠标光标停留在某接口上，可查看该接口的配置信息，例如，接口名称、接口别名、接口状态、IP 地址/掩码（只有管理接口可查看）、速率、双工模式、工作模式、输出/输入流量大小和输出/输入错包数等。单击“刷新”后能够查看到接口的最新信息。

4. 查看固定接口板面板指示灯和 ESP 板卡面板指示灯，有关指示灯的说明如[表 1](#)～[表 4](#)所示。

说明：

以下指示灯的含义是对 Web 上可能观察到的指示灯状态的解释，不包含设备启动等过程中指示灯的状态。如果需要了解指示灯的所有可能状态以及接口卡的面板指示灯状态，请参见产品光盘中的《硬件指南》。

设备暂不支持 Micro-SD 卡。

表 1 固定接口板面板指示灯说明

指示灯	颜色	含义
SYS	绿色	每 2 秒闪 1 次（0.5Hz）：系统处于正常运行状态。 熄灭：系统故障。
PWR	绿色	常亮：电源工作正常。 熄灭：电源故障。
TF CARD	绿色	常亮：Micro-SD 卡在位，但没有数据读写。 每秒闪 2 次（2Hz）：Micro-SD 卡正在进行数据读写。 每秒闪 2 次（2Hz）且 ALM 每 2 秒闪 1 次（0.5Hz）：Micro-SD 卡在读写中出现告警。 熄灭：Micro-SD 卡不在位。
ALM	红色	常亮：系统运行出现故障。 每 2 秒闪 1 次（0.5Hz）：升级异常、读写 Micro-SD 卡时出现异常。 熄灭：系统运行正常。
FAN	绿色	常亮：风扇工作正常。 熄灭：风扇故障。
MODE	绿色	常亮：主备模式双机热备中本设备工作在主模式下或设备未工作在主备模式双机热备。 熄灭：主备模式双机热备中本设备工作在备模式下。

表 2 ESP 卡指示灯说明

指示灯	颜色	含义
SYS	绿色	常亮：ESP 卡在位。
ALM	红色	常亮：ESP 卡业务处理出现故障。 熄灭：ESP 卡业务处理正常。

表 3 2×10GE 光口卡（DMIC）指示灯说明

指示灯	颜色	含义
0	绿色	常亮：接口 0 链路已经连通。 闪烁：接口 0 有数据收发。 熄灭：接口 0 链路没有连通。
1	绿色	常亮：接口 1 链路已经连通。 闪烁：接口 1 有数据收发。 熄灭：接口 1 链路没有连通。

表 4 SACC 卡指示灯说明

指示灯	颜色	含义
RUN	绿色	每 2 秒闪 1 次（0.5Hz）：SACC 加速卡工作正常。 熄灭：系统未上电或 SACC 加速卡工作异常。
ALM	红色	常亮：SACC 加速卡工作异常。

表 3 2×10GE 光口卡（DMIC）指示灯说明		
指示灯	颜色	含义
		熄灭：SACC 加速卡工作正常。

配置管理接口

管理接口 MGMT 是设备上唯一的三层接口，提供单独的带外管理通道。通过管理接口，可实现以下功能：

- 管理员通过管理接口对设备进行配置、升级等管理操作。
- 设备通过管理接口向日志主机输出日志信息。
- 在双机热备组网环境下，使用管理接口作为心跳备份通道。



说明：

IDS 设备和工作在 IDS 模式下的 IPS 设备没有双机热备的应用场景，无须将管理接口作为心跳备份通道。

缺省情况下，管理接口的 IP 地址为 192.168.0.1/24。当管理接口的 IP 地址被修改后，当前所有在线用户需要使用修改后的 IP 地址重新登录。

当遗忘管理接口的 IP 地址时，请通过 Console 口方式登录设备（用户名为 admin，初始密码为 Admin@123），执行命令 **display manage-ip** 查看管理接口 IP 地址，或者执行命令 **manage-ip ip-address { mask | mask-length }** 修改管理接口 IP 地址。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口配置”页签。
3. 单击“接口状态图”中的 MGMT 接口图标（状态图中标识为 MGMT/HA）。
4. 依次输入或选择各项参数，如表 5 所示。
5. 单击“应用”。

界面显示操作成功，则表明管理接口已成功配置。

表 5 管理接口参数说明		
参数	说明	取值建议
IP 地址/掩码	接口的 IP 地址和掩码。	不能与网络内其他设备的 IP 地址冲突。

表 5 管理接口参数说明		
参数	说明	取值建议
默认网关	设备的默认网关地址。设备通过默认网关访问其他网段的设备，如 DNS 服务器等。	-
DNS 首选地址	负责接收设备提出的域名解析请求的首选 DNS 服务器地址。当设备通过域名访问网络时，设备通过默认网关向该 DNS 服务器发送域名解析请求。 当通过内网（升级服务器通过域名方式指定时）或外网方式升级应用控制知识库或威胁防护签名库时，必须配置 DNS 服务器地址。	-
DNS 备选地址	负责接收设备提出的域名解析请求的备选 DNS 服务器地址。当首选 DNS 服务器域名解析失败时，向备选 DNS 服务器发送域名解析请求。	-
速率	接口的工作速率。	<ul style="list-style-type: none"> 10M：表示配置接口的工作速率为 10Mbit/s。 100M：表示配置接口的工作速率为 100Mbit/s。 1000M：表示配置接口的工作速率为 1000Mbit/s。 自协商：表示配置接口工作在自动协商模式下。 <p>缺省情况下，接口的工作速率设置为自协商。</p> <p>接口的速率应确保与连接对端相同。</p>
双工模式	接口的双工模式。	<ul style="list-style-type: none"> 半双工：表示将接口配置为半双工模式。当希望接口同一时刻只能发送数据包或接收数据包时，可以将接口设置为半双工模式。 全双工：表示将接口配置为全双工模式。当希望接口在发送数据包的同时可以接收数据包，可以将接口设置为全双工模式。 自协商：表示配置接口工作在自动协商模式下。 <p>缺省情况下，接口的双工模式设置为自协商。</p> <p>接口的双工模式应确保与连接对端相同。</p>
ARP 欺骗攻击防御（IPS 设备）	攻击原理 攻击者为了改变网关设备上的 ARP 表项，会向网关设备发送虚假 ARP 请求报文。如	-
ARP 欺骗攻击检测		

表 5 管理接口参数说明		
参数	说明	取值建议
（IDS 设备）	<p>果设备将该报文中的 IP 地址与 MAC 地址对应关系学习至 ARP 表项，则会误将其他主机的报文转发给攻击源。</p> <p>防御原理</p> <p>开启 ARP 欺骗攻击防御或 ARP 欺骗攻击检测后，NIP 只在自己主动向其他主机发起 ARP 请求并得到回应的情况下才更改 ARP 表项，而不会学习主机主动发来的 ARP 请求报文。</p>	

配置业务接口属性

设备的固定接口板和扩展接口卡上的业务接口都划分为固定接口对。

在使用业务接口之前，需要根据网络组网情况，修改业务接口属性。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口配置”页签。
3. 单击“接口状态图”中的待配置的接口对的其中一个接口图标。
4. 依次输入或选择各项参数，如表 6 所示。
5. 单击“应用”。

界面显示操作成功，则表明接口已成功配置。

表 6 业务接口属性参数说明		
参数	说明	取值建议
接口别名	对接口设置的其他名称，方便用户记忆和识别接口的用途。	<p>缺省情况下，根据接口对编号先后顺序，接口别名取值为 a0x 和 b0x，x 从 1 开始，依次累加。例如，接口对 GE0/0/1 和 GE0/0/2，其默认接口别名分别为 a01 和 b01。</p> <p>您可以根据实际网络情况自定义接口别名。例如，为了能够让管理员更加直观看 IPS 接口对的部署位置，可以通过根据 IPS 接口对应网络的不同位置定义接口别名。如：</p> <ul style="list-style-type: none"> 接口对中接口 a01 连接外网，可以定义 a01 的接口别名为 External。

表 6 业务接口属性参数说明

参数	说明	取值建议
		<ul style="list-style-type: none"> 接口对中接口 b01 连接内网，可以定义 b01 的接口别名为 Internal。 <p>例如，为了能够让管理员更加直观看看到 IDS 接口所监听的网络，可以通过根据 IDS 接口所连接的网络位置定义接口别名。如：IDS 接口 a02 监听交换机 A 的端口，可以定义 a02 的接口别名为 Monitor_SW_A。</p>
防御模式	流量型攻击防御功能需要在接口上配置相应的防御模式才生效。	<p>DNS 信誉学习功能需要在接口上配置防御模式为服务器流量防御，其他的流量型攻击防御需要在接口上配置防御模式为客户端流量防御。</p> <p>一般情况下，在攻击流量的入接口上配置防御模式为客户端流量防御，在连接服务器的接口上配置防御模式为服务器流量防御。</p>
光电切换	<p>每对光电互斥口由一个光接口和一个电接口组成，同一时刻只能使用一种接口。通过“光电切换”，管理员可根据网络线缆连接情况决定光电互斥口工作在光接口还是电接口状态。</p> <p>缺省情况下，光电互斥口工作在电接口状态。</p> <p>接口对 a03-b03 和 a04-b04 是两个光电互斥接口对，需要配置该参数。</p> <p>对于 IPS 接口对，两个接口的光电状态应一致。</p> <p>对于 IPS 接口对组合，允许流量入口和出口的光电状态不一致，例如，入口均为电口，出口均为光口。</p>	<ul style="list-style-type: none"> 光口：光电互斥口工作在光接口状态。 电口：光电互斥口工作在电接口状态。
速率	<p>接口的工作速率。</p> <p>当接口为以太网电接口时，需要配置该参数。</p>	<ul style="list-style-type: none"> 10M：表示配置接口的工作速率为 10Mbit/s。 100M：表示配置接口的工作速率为 100Mbit/s。 1000M：表示配置接口的工作速率为 1000Mbit/s。 自协商：表示配置接口工作在自动协商模式下。 <p>缺省情况下，接口的工作速率设置为自协商。</p> <p>接口的速率应确保与连接对端相同。</p>
双工模式	<p>接口的双工模式。</p> <p>当接口为以太网电接口时，需要配置该参</p>	<ul style="list-style-type: none"> 半双工：表示将接口配置为半双工模式。当希望接口同一时刻只能发送数

表 6 业务接口属性参数说明

参数	说明	取值建议
	数。	<p>据包或接收数据包时，可以将接口设置为半双工模式。</p> <ul style="list-style-type: none"> 全双工：表示将接口配置为全双工模式。当希望接口在发送数据包的同时可以接收数据包，可以将接口设置为全双工模式。 自协商：表示配置接口工作在自动协商模式下。 <p>缺省情况下，接口的双工模式设置为自协商。</p> <p>接口的双工模式应确保与连接对端相同。</p>
禁止接口	选中“启用”前的复选框，表示关闭接口。在数据传输过程中关闭接口，将造成数据帧丢失，请慎重使用。	-

修改接口对工作模式（IPS 设备）



说明：

IDS 设备的接口对始终工作在 IDS 模式下，无须进行工作模式的切换。

IPS 设备的固定接口板和扩展接口卡上的业务接口都划分为固定接口对，支持三种工作模式：

- 直路 IPS 模式

当设备通过接口对直路透明接入网络时，需要将接口对配置为直路 IPS 模式。

每个 IPS 接口对的两个接口分别用来连接上下行设备形成一条业务链路。设备对流经该链路的数据流进行深度分析，能精确、实时地识别、阻断、限制各种网络威胁。

- 单臂 IPS 模式

当 IPS 设备单臂旁挂在交换机的 trunk 链路上，要检测多个 VLAN 对之间的流量时，需要将接口对配置为单臂 IPS 模式。

当接口对工作在单臂 IPS 模式时，设备检测交换机上送的流量，对匹配 VLAN 对的数据流进行深度分析，对命中策略的数据进行处理。对处理完毕后的数据包，根据 VLAN 对的映射关系进行 VLAN 转换，并通过原接口将流量返回交换机。

- IDS 模式

当设备通过接口旁路接入网络时，需要将接口配置为 IDS 模式。


工作在 IDS 模式的接口对，可以将接口对中的任意一个接口旁挂到链路交换机的监听端口。设备通过接收流量镜像、探测复制报文的方式捕获数据报文，然后对镜像流量进行检测分析，从而对所在网络起到监控作用。

IPS 设备支持部分接口工作在直路 IPS 模式下，部分接口工作在 IDS 或单臂 IPS 模式下，实现多链路、混合接入。



注意：

- 缺省情况下，所有的接口对工作在 IPS 模式下。
- 修改接口对的工作模式之前，请确保业务接口属性已根据实际组网情况调整。
- 修改接口对的工作模式之后，接口对下已配置的策略将全部被清除，仅应用了缺省的安全策略。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口对配置”页签。
3. 单击“接口对列表”中需要修改工作模式的接口对所在行的 .
4. 依次输入或选择各项参数，如表 7 所示。
5. 单击“应用”。
6. 在弹出的确认提示框中，单击“是”。

界面显示操作成功，且“工作模式”列已显示切换后的模式。

表 7 接口对参数说明

参数	说明	取值建议
工作模式	根据设备在网络中的部署情况，选择接口对的工作模式。	<ul style="list-style-type: none"> • 直路 IPS：设备通过接口对直路透明接入网络，即设备直接处于数据转发的链路上。 • 单臂 IPS：设备通过接口旁挂在交换机上，根据 VLAN 对表项进行数据的转发。 • IDS：设备通过接口旁路接入网络，即设备不在数据转发的链路上。

表 7 接口对参数说明

参数	说明	取值建议
VLAN 对	当接口对工作在单臂 IPS 模式时，需要配置该参数。	VLAN 对由两个 VLAN ID 组成，例如“1-100”。 当 IPS 设备的接口对工作在单臂 IPS 模式时，IPS 设备会根据 VLAN 对的映射关系，将进入接口数据包的 VLAN 字段进行转换，并通过原接口将数据包返回。 例如：单臂 IPS 模式下的接口检测到数据包的 VLAN 字段为“1”，根据 VLAN 对“1-100”的映射关系，将数据包的 VLAN 字段转换为“100”，再将数据包从原接口发出。

组合接口对（IPS 设备）

接口对组合是高级部署选项，主要用于存在非对称流量的场景。接口对组合是将多个接口对合并成一个逻辑上的组，从而将多条链路的流量作为整体进行监控和分析。

在链路聚合和负载分担的组网下都可能出现流量不对称的情况，此时需要使用 NIP 的多个接口对进行接入并使用接口对组合功能，使 NIP 可以整体处理多个链路的报文。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口对配置”页签。
3. 选择“接口对列表”中待组合的接口对表项前的复选框。
4. 单击“组合”。
5. 依次输入或选择各项参数，如表 8 所示。
6. 单击“应用”。
7. 在弹出的确认提示框中，单击“是”。

界面显示操作成功，且“接口对列表”中将出现组合后的接口信息。

表 8 接口对组合参数说明

参数	说明	取值建议
工作模式	根据设备在网络中的部署情况，选择接口对组合后的工作模式。	<ul style="list-style-type: none"> 直路 IPS：设备通过接口对直路透明接入网络，即设备直接处于数据转发的链路上。

表 8 接口对组合参数说明		
参数	说明	取值建议
		<ul style="list-style-type: none"> 单臂 IPS：设备通过接口旁挂在交换机上，根据 VLAN 对表项进行数据的转发。 IDS：设备通过接口旁路接入网络，即设备不在数据转发的链路上。
转发模式	<p>根据设备在网络中的部署情况，选择接口对组合后的转发模式。</p> <p>当接口对组合后工作在 IPS 模式时，需要配置该参数。</p>	<ul style="list-style-type: none"> 接口对模式：报文根据接口对对应关系进行转发。例如将接口对“a01-b01”和接口对“a02-b02”组合后，从接口“a01”接收的报文始终由接口“b01”进行转发，不会由接口“b02”进行转发。 交换模式：设备根据报文的目的 MAC 地址，从接口对组合的对端接口选择出接口。例如将接口对“a01-b01”和接口对“a02-b02”组合，从接口“a01”接收到报文时，设备根据报文的目的 MAC 地址，选择“b01”或“b02”为出接口。
别名	在文本框中输入接口对组合后的别名，方便识别组合后接口的用途。针对 IPS 接口对组，其两端的别名不能相同。	-
成员	待组合的接口对。	-
VLAN 对	当接口对组合后工作在单臂 IPS 模式时，需要配置该参数。	<p>VLAN 对由两个 VLAN ID 组成，例如“1-100”。</p> <p>当 IPS 设备的接口对组合后工作在单臂 IPS 模式时，IPS 设备会根据 VLAN 对的映射关系，将进入接口数据包的 VLAN 字段进行转换，并通过原接口将数据包返回。</p> <p>例如：单臂 IPS 模式下的接口检测到数据包的 VLAN 字段为“1”，根据 VLAN 对“1-100”的映射关系，将数据包的 VLAN 字段转换为“100”，再将数据包从原接口发出。</p>

组合接口对（IDS 设备）

接口对组合是高级部署选项，主要用于存在非对称流量的场景。接口对组合是将多个接口对合并成一个逻辑上的组，从而将多条链路的流量作为整体进行监控和分析。

对于 IDS 设备使用接口对组合的典型场景是存在非对称流量的负载分担组网，当需要通过多个接口对复制不同链路的流量时需要将多个接口对组合在一起进行整体流量分析。

1. 选择“系统 > 配置 > 接口”。
2. 选择“接口对配置”页签。
3. 选择“接口对列表”中待组合的接口对表项前的复选框。
4. 单击“组合”。
5. 在“别名”中输入接口对组合后的别名，方便识别组合后接口的用途。
6. 单击“应用”。
7. 在弹出的确认提示框中，单击“是”。

界面显示操作成功，且“接口对列表”中将出现组合后的接口信息。

启用接口对状态同步（IPS 设备）



说明：

IDS 设备和旁路部署的 IPS 设备不支持接口对状态同步功能，没有该功能的应用场景。

网络中，相邻两设备在中间接入 NIP 后，从一个接口进入的流量将从该接口所属的 IPS 接口对的另一个接口发出。如果接口对中两个接口状态不一致，而 NIP 的上下游设备又不能及时感知，将导致部分业务中断。

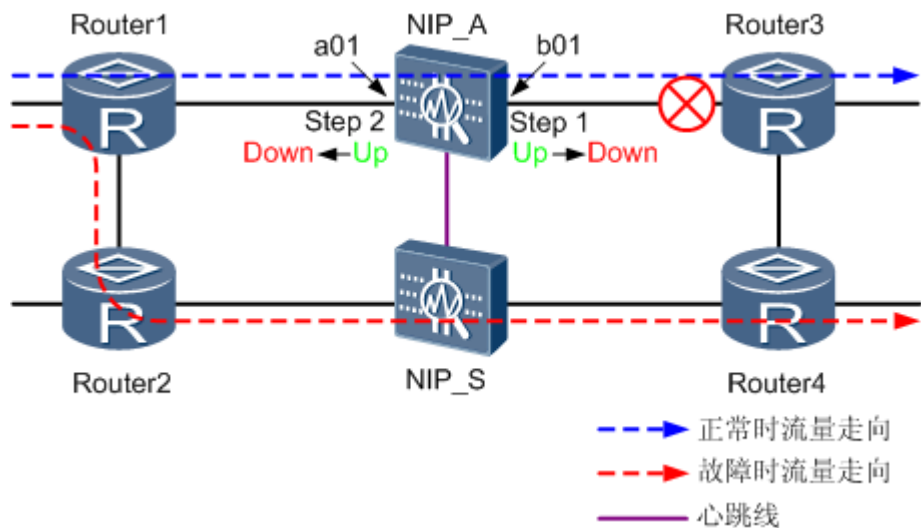
为解决这一问题，引入接口对状态同步功能。启用接口对状态同步后，NIP 的 IPS 接口对的两个接口状态将自动保持一致。当接口对的一端接口的状态由 Up 变为 Down 时，其对端接口的状态由 Up 变为 Down。当两端接口状态均恢复正常后，该接口对才能恢复工作。在以下场景下，通过接口对状态同步功能，可大大提高可靠性：

- 双机热备组网

如[图 1](#)所示，NIP_A 和 NIP_S 直路部署在网络中，上、下行业务接口与路由器相连。正常情况下，NIP_A 为主用设备，处理业务报文，NIP_S 为备用设备，不处理业务报文。

在该组网环境下，当 NIP_A 与 Router3 之间的链路发生故障时，Router1 不能快速感知链路故障，继续向该链路传送报文，直到路由收敛才将链路进行切换，这将导致部分报文被丢弃。在 NIP_A 的 IPS 接口对上启用接口对状态同步功能后，当 b01 接口状态变为 Down 时，NIP_A 将 a01 的接口状态也置为 Down，Router1 快速感知主链路故障，及时将流量切到备份链路上。

图 1 双机热备组网



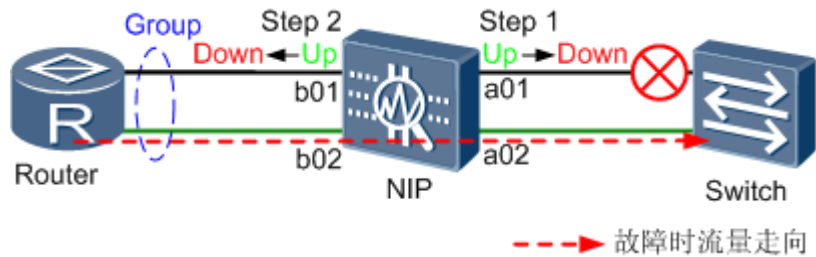
• 接口对组合组网

如图2所示，Router 和 Switch 之间是链路聚合组网，各通过两个接口形成 2 条链路的聚合。NIP 将两个 IPS 接口对（a01-b01、a02-b02）组合，接入网络。正常情况下，流量分担在两条链路上进行传输。

当 NIP 的 a01 接口与 Switch 之间的链路发生故障时，Router 不能快速感知链路故障，继续向该链路传送报文，这将导致部分报文被丢弃。在 NIP 的 IPS 接口对组合上启用接口对状态同步功能后，当 a01 接口状态变为 Down 时，NIP 将 b01 的接口状态也置为 Down，Router 快速感知 a01-b01 所在链路故障，及时将流量切到 a02-b02 所在链路上。

对于接口对组合中的每对接口对，其状态完全独立互不影响。例如，图2中 a01 接口状态变化后，只会影响到 b01 接口状态的变化，对 a02 或 b02 接口不影响。

图2 接口对组合组网



1. 选择“系统 > 配置 > 接口”。
2. 选择“接口对配置”页签。
3. 在“接口对列表”中，选中待配置的接口对或接口对组合的对应“接口对状态同步”列的复选框。

界面显示操作成功，则表明接口对状态同步功能已成功启用。

其他操作

操作	说明
修改接口对的组合	对于 IPS 设备，修改组合接口对的工作模式将导致组上已应用的策略全部被清除。
拆除接口对的组合	拆除接口对的组合后，该组的成员接口将恢复为缺省状态。其中，对于 IPS 设备，将恢复成 IPS 接口对，并应用缺省的安全策略；而 IDS 设备，将恢复成 IDS 接口对，并应用缺省的安全策略。

HCIE-Security 模拟面试问题及面试建议

1. NIP 设备上接口对有那几种工作模式？