基本接口配置

本章介绍基本接口配置，包括以太网设置和巨帧配置。

注释 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。 要从情景更改到系统执行空间，请输入 **changeto system** 命令。

注释 对于平台模式中的 和上的 Firepower 4100/9300 机箱Firepower 2100 ，您可以在 FXOS 操作系统中配置基本接口设置。有关详细信息，请参阅机箱的配置或快速入门指南。

关于基本接口配置

本节介绍接口功能与特殊接口。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的

自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

管理接口

管理接口是一个仅用于管理流量的独立接口，具体情况视型号而定。

管理接口概览

可以通过连接至以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理插槽/端口接口（如果适用于所用的型号）

您可以需要根据管理访问来配置对接口的管理访问权限。

管理插槽/端口接口

下表列出了每个型号的管理接口。

表 *1:* 每个型号的管理接口

型号	**Management 0/0**	**Management 0/1**	**Management 1/0**	**Management 1/1**	可针对直通流量进行配置	允许子接口
Firepower 1000	-	-	-	支持	支持	支持

型号	Management 0/0	Management 0/1	Management 1/0	Management 1/1	可针对直通流量进行配置	允许子接口
Firepower 2100	-	-	-	支持	- 注释 技术上而言，您可以启用直通流量；但是，此接口的吞吐量不足以进行数据操作。	支持
Firepower 4100/9300	不适用 接口 ID 取决于分配给 ASA 逻辑设备的管理类型物理接口	-	-	-	-	支持
ASA 5506-X	-	-	-	支持	-	-
ASA 5508-X	-	-	-	支持	-	-
ASA 5516-X	-	-	-	支持	-	-
ISA 3000	-	-	-	支持	-	-
ASAv	支持	-	-	-	支持	-

注释 如果您安装了一个模块，则该模块的管理接口仅提供对该模块的管理访问。对于安装了软件模块的型号，软件模块与 ASA 使用相同的物理管理接口。

将任何接口用于管理专用流量

若想将任何接口（包括 EtherChannel 接口）用作管理专用接口，您只需将该接口配置为用于管理流量（请参阅 **management-only** 命令）。

透明模式下的管理接口

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口（物理接口、子接口[如果所用的型号支持]用作单独的仅管理接口。您不能将任何其他接口类型用作管理接口。对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要在 Firepower 型号 上为每个情景提供管理，您可以创建管理接口的子接口，然后向每个情景分配管理子接口。然而，不允许管理接口上有子接口，因此这些型号需要为了针对每个情景进行管理，您必须连接到数据接口。对于 Firepower 4100/9300 机箱，管理接口及其子接口不会被识别为情景中允许的特殊管理接口；您必须在这种情况下将管理子接口视为数据接口，并将其添加到 BVI。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注释 在透明防火墙模式下，管理接口以与数据接口相同的方式更新 MAC 地址表；因此不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，那么 ASA 会更新 MAC 地址表，以使用管理接口而非数据接口访问交换机。此操作会导致流量临时中断；出于安全考虑，ASA 在至少 30 秒的时间内不会为了从交换机传输至数据接口的数据包而再次更新 MAC 地址表。

不支持冗余管理接口

冗余接口不支持管理插槽/端口接口作为成员。但您可以将包含非管理接口的冗余接口设置为仅管理接口。

ASA 型号上的管理接口特性

ASA 5500-X 型号（）的管理接口具有以下特征：

- 不支持直通流量
- 不支持子接口
- 不支持优先级队列
- 不支持组播 MAC
- 软件模块共享管理接口。ASA 和该模块支持单独的 MAC 地址和 IP 地址。您必须在模块操作系统中执行模块 IP 地址的配置。但是，物理特性（例如启用接口）在 ASA 上配置。

基本接口配置的相关准则

透明防火墙模式

对于多情景透明模式，每个情景必须使用不同的接口；您不能在情景之间共享一个接口。

故障切换

您不能与数据接口共享一个故障切换接口或状态接口。

其他准则

有些管理相关服务在启用非管理接口和ASA实现“系统就绪”状态之前不可用。在“系统就绪”状态下，ASA 会生成以下系统日志消息：

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本接口配置的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，要使流量通过冗余接口，还必须启用成员物理接口。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- VXLAN VNI 接口 - 已启用。
- EtherChannel port-channel 接口（ASA 型号；ISA 3000）- 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel port-channel 接口（其他型号）- 已禁用。

注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和 ASA 上的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与ASA之间可能出现不匹配的情况。

默认速度和双工

- 默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。

默认连接器类型

有些型号包含两个连接器类型：铜缆 RJ-45 和光纤 SFP。RJ-45 是默认接口。您可以将 ASA 配置为使用光纤 SFP 连接器。

默认 MAC 地址

默认情况下，物理接口使用烧录MAC地址，物理接口的所有子接口均使用相同的烧录MAC地址。

启用物理接口和配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定的速度和双工（如有）
- 启用暂停帧以进行流量控制

开始之前

对于多情景模式，请在系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入**changeto system** 命令。

过程

步骤 1 指定要配置的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号，格式为 type[slot/]port。

物理接口类型包括：

- **gigabitethernet**
- **tengigabitethernet**
- **management**

依次输入类型和插槽/端口，例如 **gigabitethernet0/1**。类型与插槽/端口之间的空格是可选的。

步骤 2 （可选）设置速度：

speed {**auto** | **10** | **100** | **1000** | **10000** | **nonegotiate**}

示例：

```
ciscoasa(config-if)# speed 100
```

RJ-45 接口的默认设置为**自动**。

SFP 接口的默认设置为 **no speed nonegotiate**；此默认设置将速度设置为最大速度（最高达 1000 Mbps），并启用流量控制参数和远程故障信息的链路协商。对于 10 GB 接口，此选项将速度设置为 1000 Mbps。**nonegotiate** 关键字是唯一可用于 SFP 接口的关键字。**speed nonegotiate** 命令会禁用链路协商。

步骤 3 （可选）设置 RJ-45 接口的双工：

duplex {**auto** | **full** | **half**}

示例：

```
ciscoasa(config-if)# duplex full
```

auto 设置是默认设置。EtherChannel 接口的双工设置必须为 **full** 或 **auto**。

步骤 4 （可选）启用暂停 (XOFF) 帧可对千兆以太网接口和 10 千兆以太网接口进行流量控制：

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

示例：

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```

如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。根据FIFO缓冲区的使用率，NIC硬件会自动生成暂停 (XOFF) 和 XON 帧。如果缓冲区的使用率超过高水位标记，系统会发送暂停帧。默认的 *high_water* 值为 128 KB（10 千兆以太网）和 24 KB（千兆以太网）；您可以将此值设置为介于 0 到 511（10 千兆以太网）或介于 0 到 47 KB（千兆以太网）之间的值。发送暂停后，如果缓冲区使用率降低至低于最低限的水平，则可发送 XON 帧。默认的 *low_water* 值为 64 KB（10 千兆以太网）和 16 KB（千兆以太网）；您可以将此值设置为介于 0 到 511（10 千兆以太网）或介于 0 到 47 KB（千兆以太网）之间的值。链路伙伴可能会在接收 XON 后或 XOFF 到期后恢复流量，具体由暂停帧中的计时器值控制。默认的 *pause_time* 值为 26624；您可以将此值设置为介于 0 到 65535 之间的值。如果缓冲区使用率持续高于高水位标记，则将重复发送暂停帧，但受暂停刷新阈值控制。

使用此命令时，系统会显示以下警告：

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

要在没有提示的情况下更改参数，请使用 **noconfirm** 关键字。

注释　系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 5 启用接口：

no shutdown

示例：

```
ciscoasa(config-if)# no shutdown
```

要显示接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

启用巨帧支持（ASA 型号）

巨帧是指大于标准最大值 1518 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨帧支持。为巨帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。请注意，ASA MTU 设置的负载大小不包括第 2 层（14 字节）和 VLAN 报头（4 字节），因此最大 MTU 是 9198，具体取决于您的型号。

注释　此程序仅适用于 ASA 硬件型号和 ASAv。Firepower 型号默认支持巨帧。

开始之前

- 在多情景模式下，请在系统执行空间中设置此选项。
- 此设置的更改要求您重新加载 ASA。
- 确保要将需要传送巨帧的每个接口的 MTU 设置为大于默认值 1500 的值；例如使用 **mtu** 命令将该值设置为 9198。在多情景模式下，请在每个情景中设置 MTU。
- 请务必调整 TCP MSS，以对非 IPsec 流量禁用此功能（使用 **sysopt connection tcpmss 0** 命令），或者根据 MTU 增加 TCP MSS 的值。

过程

启用巨帧支持：

jumbo-frame reservation

示例

以下示例将启用巨帧预留、保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

监控接口

请参阅以下命令。

注释 对于平台模式和的 Firepower 2100 和Firepower 4100/9300，某些统计信息未使用ASA命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。这些命令对于设备模式下的 Firepower 1000 和 2100 也很有用。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

对于平台模式下的 Firepower 2100，另请参阅以下 FXOS connect local-mgmt 命令：

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

有关详细信息，请参阅 FXOS 故障排除指南。

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

基本接口示例

请参阅以下配置示例。

物理接口参数示例

以下示例在单模式下配置物理接口的参数：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

多情景模式示例

以下示例在多情景模式下配置用于系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配到 contextA：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本接口配置历史

表 *2:* 接口历史

功能名称	版本	功能信息
在 Firepower 1100 和 2100 的 SFP 光纤接口上可禁用速度自动协商	9.14(1)	现在，您可以配置 Firepower 1100 或 2100 SFP 接口以禁用自动协商。对于 10GB 接口，您可以将速度配置为 1GB 而无需自动协商；无法对速度设置为 10GB 的接口禁用自动协商。 新增/修改的命令：**speed nonegotiate**
ASAv 的管理 0/0 接口上支持通过流量	9.6(2)	现在，您可以在 ASAv 的管理 0/0 接口上允许通过流量。过去，仅 Microsoft Azure 上的 ASAv 支持通过流量；现在所有 ASAv 都支持通过流量。您可以选择将此接口配置为仅管理接口，但默认情况下，没有进行此配置。 修改了以下命令：**management-only**
在千兆以太网接口上支持暂停帧以进行流量控制	8.2(5)/8.4(2)	您现在可以在所有型号的千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制。 修改了以下命令：**flowcontrol**。
在 ASA 5580 的 10 千兆以太网接口上支持暂停帧以进行流量控制	8.2(2)	您现在可以为流量控制启用暂停 (XOFF) 帧。 ASA 5585-X 也支持此功能。 引入了以下命令：**flowcontrol**。
对 ASA 5580 的巨型数据包支持	8.1(1)	思科 ASA 5580 支持巨帧。巨帧是指大于标准最大字节数（1518 字节）的以太网数据包（包括第 2 层报头和 FCS），最大可达 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨帧支持。为巨帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。 ASA 5585-X 也支持此功能。 引入了以下命令：**jumbo-frame reservation**。

功能名称	版本	功能信息
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	现在，ASA 5510 通过增强型安全许可证为端口 0 和 1 提供 GE（千兆以太网）支持。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。