

# 第 1 章

## 静态路由专项

### 1.1 静态路由基础

静态路由是指网络管理员在路由器上**手工配置**的路由条目。通过静态路由，管理员可以简单、直观的方式，使路由器明确获知到达目的网络的转发路径。如图 1-1 所示，R1 去往 192.168.23.0/24 网段，下一跳为 192.168.12.2；R3 去往 192.168.12.0/24 网段，下一跳为 192.168.23.1。

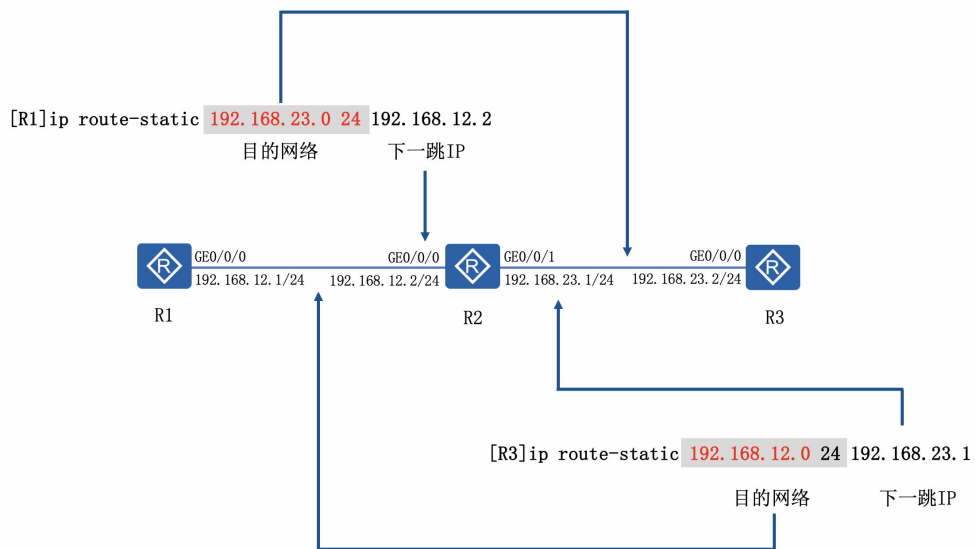


图 1-1 静态路由

配置完成后, 查看 R1 和 R3 的路由表, 可以看到对应优先级为 60 的静态路由条目。

```
[R1] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 8          Routes : 8

Destination/Mask    Proto    Pre    Cost    Flags    NextHop    Interface
192.168.12.0/24     Direct   0      0       D        192.168.12.1  GigabitEthernet0/0/0
192.168.12.1/32     Direct   0      0       D        127.0.0.1    GigabitEthernet0/0/0
192.168.12.255/32  Direct   0      0       D        127.0.0.1    GigabitEthernet0/0/0
192.168.23.0/24    Static   60     0       RD       192.168.12.2  GigabitEthernet0/0/0

[R3] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 8          Routes : 8

Destination/Mask    Proto    Pre    Cost    Flags    NextHop    Interface
192.168.12.0/24    Static   60     0       RD       192.168.23.1  GigabitEthernet0/0/0
192.168.23.0/24     Direct   0      0       D        192.168.23.2  GigabitEthernet0/0/0
192.168.23.2/32     Direct   0      0       D        127.0.0.1    GigabitEthernet0/0/0
192.168.23.255/32  Direct   0      0       D        127.0.0.1    GigabitEthernet0/0/0
```

在小规模网络中, 全网采用静态路由通常没有问题; 但在大型网络环境下, 若完全依赖静态路由实现互通, 不仅配置工作量巨大, 而且维护成本极高。由于网段数量众多, 管理员需要配置大量路由条目, 且静态路由无法随网络拓扑变化自动调整, 因此, 大规模网络通常采用动态路由协议, 或将静态路由与动态路由协议结合使用, 以实现高效、可靠的路由。

## 1.2 默认路由

### 1. 静态路由存在的问题

如图 1-2 所示, 路由器 R1 位于网络边缘, 其下行连接终端用户 (PC), 通过接口 GE0/0/0 上行接入核心路由器 R2。路由器 R2 后端连接着大量业务网段 (如 192.168.100.0/24 到 192.168.103.0/24 等)。PC 需要访问这些网段。如果使用传统的静态路由配置, 管理员需要在 R1 上为每一个目标网段逐一添加路由条目。例如:

```
[R1] ip route-static 192.168.100.0 24 192.168.12.2
[R1] ip route-static 192.168.101.0 24 192.168.12.2
[R1] ip route-static 192.168.102.0 24 192.168.12.2
[R1] ip route-static 192.168.103.0 24 192.168.12.2
...
```

该配置方式存在明显不足: R1 路由表中的路由条目过多, 不仅配置烦琐, 而且在实际场景中并无必要, 因为 R1 仅有一个网络出口。当网络规模进一步扩大时, 这种方式将带来较大的维护压力。

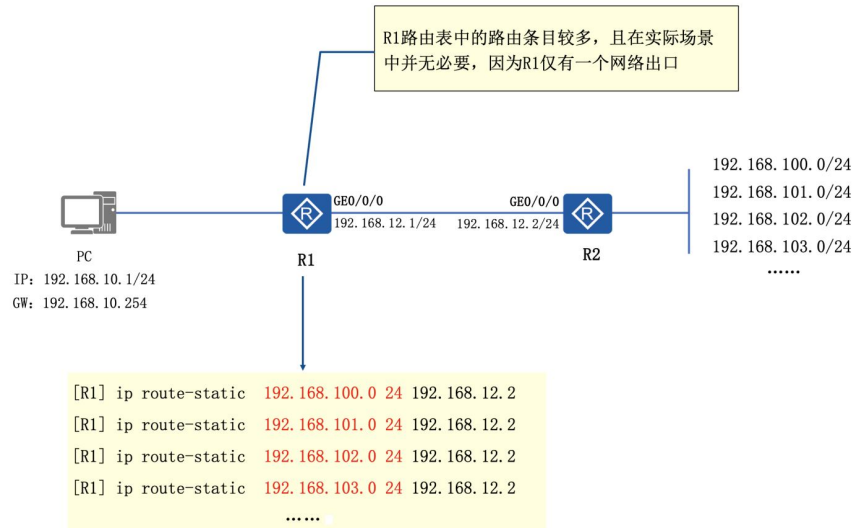


图 1-2 静态路由存在的问题

## 2. 优化方案：部署默认路由

为解决边缘路由器路由表臃肿的问题，可引入默认路由作为优化手段。默认路由是一种特殊的静态路由，其目的网络和子网掩码均为 **0.0.0.0**，可匹配所有未被精确路由命中的目的地址。在路由匹配过程中，根据最长匹配原则，**由于默认路由掩码为 0**，默认路由通常作为“无更精确路由可选”时的兜底转发路径。

如图 1-3 所示，在路由器 R1 上，仅需配置一条指向网络出口（下一跳地址为 192.168.12.2）的默认路由，即可替代所有指向 R2 的精确静态路由。

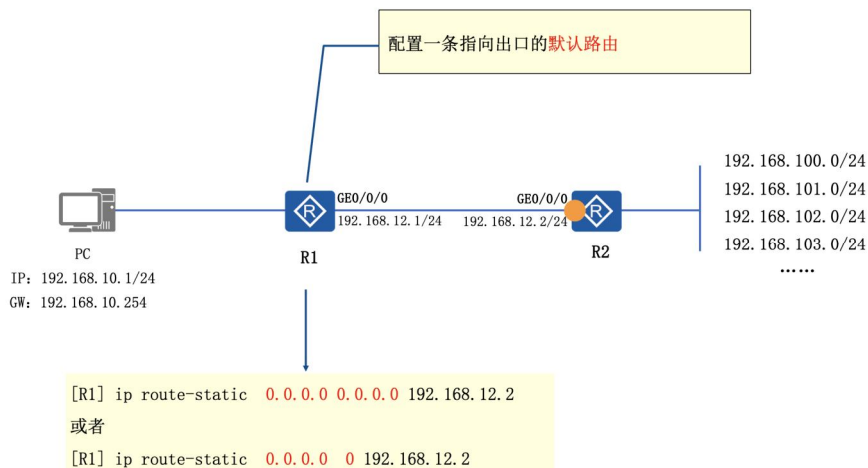


图 1-3 默认路由

```
[R1] ip route-static 0.0.0.0 0.0.0.0 192.168.12.2
```

也可采用如下简写形式:

```
[R1] ip route-static 0.0.0.0 0 192.168.12.2
```

通过上述配置, R1 会将所有未命中精确路由的流量统一转发至 R2, 由 R2 负责后续选路处理, 从而显著简化配置并降低运维复杂度。

### 3. 静态路由与默认路由对比

在实际工程中, 静态路由与默认路由并非对立关系, 而是需要根据网络规模、设备角色和运维需求进行合理取舍。两者对比见表 1-1。

表 1-1 静态路由和默认路由对比

路由类型	优势	缺点	典型适用场景
静态路由	<ul style="list-style-type: none"> <li>配置直观: 逻辑清晰, 便于理解和排错。</li> <li>路径可控性强: 管理员可以精确指定每一条流量的转发方向。</li> <li>带宽占用小: 不依赖动态路由协议, 不产生额外协议报文</li> </ul>	<ul style="list-style-type: none"> <li>扩展性较差: 随着网络规模扩大, 配置和维护成本迅速上升。</li> <li>缺乏自适应能力: 当链路或节点发生故障时, 无法自动调整, 需要人工介入</li> </ul>	通常用于拓扑简单或需要精细控制路径的网络
默认路由	<ul style="list-style-type: none"> <li>配置极其简洁: 可避免维护大量明细路由表项。</li> <li>节省资源: 缩小路由表规模, 降低设备 CPU 与内存资源消耗, 提高转发表查找效率</li> </ul>	匹配精度低, 配置不当容易形成环路	通常部署在网络边界或汇聚位置, 例如: <ul style="list-style-type: none"> <li>网络出口路由器。</li> <li>防火墙设备。</li> <li>具备单一或明确上联出口的核心交换机或汇聚交换机</li> </ul>

## 1.3 等价路由和浮动路由

### 1. 等价路由

等价路由 (Equal Cost Multi-Path, ECMP), 是指路由设备在转发数据报文时, 如果路由表中存在到达同一目的网段且具有相同路由优先级 (Preference) 和开销值 (Cost) 的多条路径, 路由器会将这些路径看作“等价”的。

此时, 这些路径会被同时加入到路由表中, 数据流量将按照特定的负载分担算法在这些有效接口和下一跳之间进行分流转发。这种机制不仅充分利用了网络带宽资源, 提高了传输效率, 还在一定程度上提供了链路级的冗余保护。

如图 1-4 所示, 路由器 R1 到达 10.1.1.0/24 网段存在两条路径, 可以配置两条静态路由到达该网段, 配置命令如下:

```
[R1] ip route-static 10.1.1.0 24 20.1.1.2 //到达 10.1.1.0/24 下一跳为 20.1.1.2
```

```
[R1] ip route-static 10.1.1.0 24 30.1.1.2 //到达 10.1.1.0/24 下一跳为 30.1.1.2
```

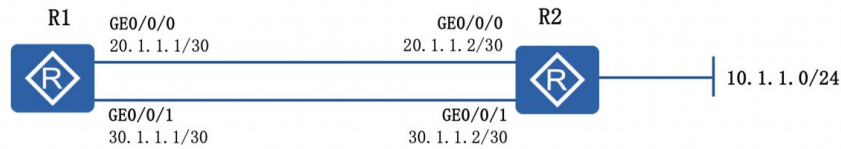


图 1-4 等价路由

由于两条静态路由均未手工指定优先级，其优先级均为华为设备静态路由的默认值 60。同时，两条路由的开销均为 0（静态路由默认开销），因此可同时进入 R1 的路由表。访问 10.1.1.0/24 的流量将在 GE0/0/0 和 GE0/0/1 两条链路上实现负载分担。此时在 R1 查看路由表，可以看到已形成两条等价路由。

```
[R1] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 11          Routes : 12

Destination/Mask    Proto    Pre  Cost   Flags     NextHop     Interface
10.1.1.0/24        Static   60   0      RD        20.1.1.2    GigabitEthernet0/0/0
                   Static   60   0      RD        30.1.1.2    GigabitEthernet0/0/1
```

ECMP 负载分担方式常见为**基于流与基于包**两种。华为设备在缺省情况下采用基于流的负载分担方式，即同一数据流始终沿同一路径转发。部分设备可通过命令 `ip load-balance packet`，将负载方式调整为基于包的逐包转发。但当报文较大需要分片，且多条链路时延差异较大时，逐包转发可能导致报文乱序，从而影响数据重组和业务质量。

当路由器或三层交换机检测到存在多条到达同一目的地的等价路径时，会通过哈希算法将业务流量分配到不同的下一跳接口。`load-balance` 命令用于指定哈希计算所依据的报文字段，不同的负载分担方式对应不同的哈希依据，其对比关系见表 1-2，相关配置如下：

```
[R1] load-balance ?
  dst-ip      According to destination IP hash arithmetic
  dst-mac     According to destination MAC hash arithmetic
  src-dst-ip  According to source/destination IP hash arithmetic
  src-dst-mac According to source/destination MAC hash arithmetic
  src-ip      According to source IP hash arithmetic
  src-mac     According to source MAC hash arithmetic
[R1] load-balance src-dst-ip //配置为基于源目 IP 进行流量负载分担
```

表 1-2 不同负载分担方式对比

模式	基于要素	工作原理	应用场景
dst-ip	目的 IP 地址	仅根据接收方 IP 进行哈希。去往同一个目的 IP 的所有数据，会走同一个下一跳	少量客户端访问很多服务器，或者在使用由目的地址决定的缓存服务器集群时，保证去往特定网站的流量总是命中特定的链路

续表

模式	基于要素	工作原理	应用场景
dst-mac	目的 MAC 地址	仅根据入接口的目的 MAC 哈希	几乎不用于 ECMP。对于三层接口，目的 MAC 通常就是接口本身的 MAC，这意味着所有流量的哈希值都一样，流量将只走一条路（易导致单链路拥塞）
src-ip	源 IP 地址	仅根据发起方 IP 进行哈希。来自同一个源 IP 的所有数据（无论去往哪里），均会被强制走同一个下一跳	很多客户端访问少量服务器。例如，园区网出口。你需要确保同一个员工的所有上网流量都从同一个 ISP 出口出去，以便于审计或策略控制
src-dst-ip	源 IP+目的 IP	（最推荐/默认）设备提取数据包的源 IP 和目的 IP 进行异或运算。只要源和目的 IP 不变，该数据流就始终走同一个下一跳	绝大多数三层网络环境。它能保证同一个会话（Session）的包序不乱，同时利用了源和目的两个维度的随机性，流量分担最均匀
src-dst-mac	源 MAC+目的 MAC	（ECMP 中较少使用）提取数据帧的源 MAC 和目的 MAC 进行哈希。因三层转发时源/目 MAC 地址会在每跳重写，入接口看到的源 MAC 通常固定为上一跳设备的 MAC，导致哈希结果单一，故不推荐在三层接口使用	特殊场景：当设备承担“透传”角色或上一跳设备数量极多且 IP 极度离散，但希望降低芯片解析 IP 头部的开销时使用（现代设备极少需要这样省性能）
src-mac	源 MAC 地址	仅根据上一跳设备的 MAC 地址哈希	不推荐用于 ECMP——除非你的上一跳连接了大量不同的二层设备，否则容易导致负载极度不均（哈希极化）

## 2. 浮动路由

浮动路由是一种利用路由优先级机制实现的链路备份技术，通过为到达同一目的地的多条静态路由设置不同优先级，实现主备路由切换。

- 主路由（Primary Route）：配置较小的优先级数值（优先级高），该路由会被优选并加入路由表，承担正常的的数据转发任务。
- 备用路由（Backup Route）：配置较大的优先级数值（优先级低），在主路由正常时，它不会出现在路由表中，而是“隐藏”在后台。

仅当主路由的下一跳不可达或物理链路发生故障（Down），导致主路由失效时，备用路由才会“浮动”出来并被激活，加入路由表接管数据转发，从而保证业务连续性。如图 1-4 所示，R1 与 R2 之间若改用主备链路设计，则配置命令如下：

```
[R1] ip route-static 10.1.1.0 24 20.1.1.2 preference 50 //优先级调整为 50，成为主路由
[R1] ip route-static 10.1.1.0 24 30.1.1.2 //默认优先级 60，成为备用路由
```

管理员将下一跳为 20.1.1.2 的静态路由优先级手动设置为 50，低于默认值 60（在华为 VRP 系统中，数值越小表示路由由优先级越高）。正常情况下，R1 仅将优先级为 50 的主路由写入路由表，业务流量统一通过 R2 的 GE0/0/0 接口转发，优先级为 60 的备用路由不参与转发。当该 GE0/0/0

接口发生故障时，由于主路由的下一跳或出接口失效，该路由将从路由表中被撤销。此时，优先级为 60、经由 R2 的 GE0/0/1 的备用静态路由自动生效并写入路由表，接管业务流量，从而实现了无须人工干预的自动切换。等价路由和浮动路由对比见表 1-3。

表 1-3 等价路由和浮动路由对比

特性	等价路由 (ECMP)	浮动路由 (Floating Route)
工作模式	Active-Active (双活/多活)	Active-Standby (主备)
路由表状态	所有等价路径同时存在于路由表中	仅最优路径存在于路由表中，次优路径隐藏
优先级设置	必须相同	必须不同
核心优势	增加带宽，提升吞吐量	提供高可靠性，作为容灾备份
适用场景	链路带宽相近，追求传输效率	主备链路带宽差异大或按流量计费的备线场景

## 1.4 静态路由和 BFD 联动

### 1. 静态路由的“盲区”

静态路由配置简单且不占用设备计算资源，但其缺点在于故障感知能力较弱。默认情况下，静态路由是否生效仅取决于本地出接口的物理状态 (Up/Down)，只能感知直连链路故障，无法感知非直连链路故障。

**直连故障：**当直连链路发生故障（如网线断开）时，本地接口物理状态变为 Down，设备能够立即感知异常，相关静态路由会自动从路由表中撤销，业务流量可切换至备用路径，对网络影响较小。

**非直连故障：**这是静态路由应用中的主要问题。当两台路由器之间存在二层交换设备或传输设备时，即使远端路由器发生故障，本地接口物理状态仍可能保持 Up，静态路由依然存在于路由表中，数据包被持续转发至不可达的下一跳，形成“黑洞”，最终导致业务中断。

如图 1-5 所示，在 R1 上配置默认路由 `ip route-static 0.0.0.0 0 12.1.1.2`。当 R2 的 GE0/0/0 接口发生故障时，由于该接口为直连接口，R1 能够及时感知接口状态变化，并迅速将对应的默认路由从路由表中撤销。同时，在 R1 上配置另一条默认路由 `ip route-static 0.0.0.0 0 13.1.1.2`。当 R3 的 GE0/0/0 接口发生故障时，由于 R1 与 R3 之间仍存在一台二层交换机，R1 无法直接感知 R3 接口的失效状态，因此该默认路由仍会保留在 R1 的路由表中，但其下一跳实际上已不可达。

针对这类非直连链路故障无法及时感知的问题，引入了双向转发检测 (Bidirectional Forwarding Detection, BFD) 技术。该技术通过快速的双向检测机制，实现对链路和转发路径状态的实时感知，从而提高路由收敛速度与网络可靠性。

### 2. BFD

BFD 是一种用于快速检测链路或 IP 连通性的机制。相比路由协议依赖的 Hello 报文故障检测

机制（通常为秒级），BFD 可实现**毫秒级故障感知**。通过将 BFD 会话与静态路由或动态路由协议联动，由 BFD 负责实时监测转发可达性，路由协议负责转发决策，一旦链路中断，BFD 立即触发路由失效并切换至备份路径，从而显著**提升网络收敛速度与可靠性**。

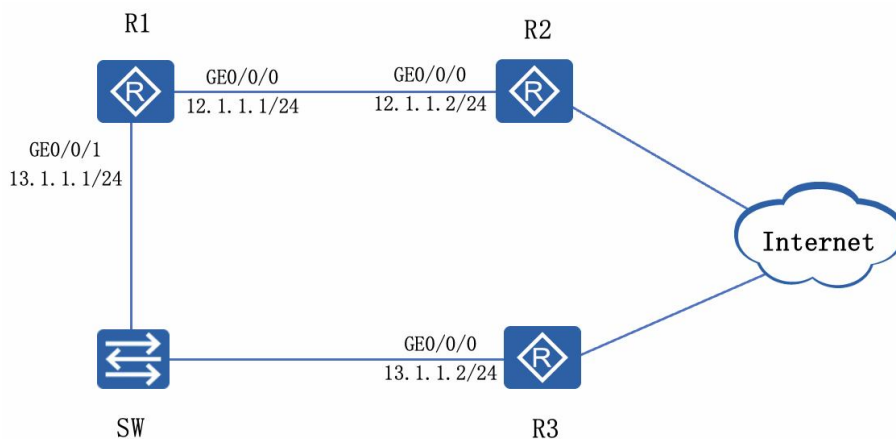


图 1-5 静态路由“盲区”

### 3. BFD 配置

第 1 步：启用 BFD 功能。

```

[R1] bfd           //系统视图下全局启用 BFD
[R1-bfd] quit     //退出当前配置视图
[R3] bfd           //系统视图下全局启用 BFD
[R3-bfd] quit
  
```

第 2 步：创建 BFD 会话。

```

[R1] bfd R1toR3 bind peer-ip 13.1.1.2 interface GigabitEthernet0/0/1 //创建名为 R1toR3 的 BFD 会话，并将其绑定到本地接口 GigabitEthernet0/0/1，对端 IP 地址为 13.1.1.2
[R1-bfd-session-R1toR3] discriminator local 10 //R1 的本地标识符设为 10
[R1-bfd-session-R1toR3] discriminator remote 20 //R2 的远端标识符设为 20
[R1-bfd-session-R1toR3] commit //提交当前 BFD 会话配置，使上述参数正式生效
[R1-bfd-session-R1toR3] quit

[R3] bfd
[R3-bfd] quit
[R3] bfd R3toR1 bind peer-ip 13.1.1.1 interface GigabitEthernet0/0/0 //创建名为 R3toR1 的 BFD 会话，并将其绑定到本地接口 GigabitEthernet0/0/0，对端 IP 地址为 13.1.1.1
[R3-bfd-session-R3toR1] discriminator local 20 //R3 的本地标识符设为 20
[R3-bfd-session-R3toR1] discriminator remote 10 //R3 的本地标识符设为 10
[R3-bfd-session-R3toR1] commit
  
```

第 3 步：配置浮动路由并绑定 BFD。

```

[R1] ip route-static 0.0.0.0 0.0.0.0 13.1.1.2 track bfd-session R1toR3 //配置主路由，绑定 BFD 会话“R1toR3”，即当 BFD 会话状态为 up，该路由生效
[R1] ip route-static 0.0.0.0 0.0.0.0 12.1.1.2 preference 100 //配置备份路由（浮动路由），优先级大于默认值 60 即可
  
```

第 4 步：结果验证与现象分析。

(1) 在 R1 上查看 BFD 会话状态，可以看到 State 为 Up，说明 BFD 会话已正常建立。

```
[R1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
10	20	13.1.1.2	Up	S_IP_IF	GigabitEthernet0/0/1

```
Total UP/DOWN Session Number : 1/0
```

(2) 查看 R1 的路由表，可以看到当前生效的是优先级为 60 的缺省路由（默认优先级），下一跳为 13.1.1.2。

```
[R1] display ip routing-table
```

```
Route Flags: R - relay, D - download to fib
```

```
Routing Tables: Public
```

```
Destinations : 11 Routes : 11
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
<b>0.0.0/0</b>	<b>Static</b>	<b>60</b>	<b>0</b>	<b>RD</b>	<b>13.1.1.2</b>	<b>GigabitEthernet0/0/1</b>
12.1.1.0/24	Direct	0	0	D	12.1.1.1	GigabitEthernet0/0/0
12.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
12.1.1.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
13.1.1.0/24	Direct	0	0	D	13.1.1.1	GigabitEthernet0/0/1
13.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
13.1.1.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1

(3) 模拟故障操作。通过关闭路由器 R3 的 GE0/0/0 接口，或拔掉该接口网线，模拟 R3 设备宕机或链路中断。当故障发生后，R1 上的 BFD 会话状态会迅速由 Up 切换为 Down，表明链路连通性已丧失。

```
[R3] interface g0/0/0
```

```
[R3-GigabitEthernet0/0/0] shutdown //关闭 R3 的 GE0/0/0 接口，模拟线路故障
```

```
[R1] display bfd session all
```

```
//查看 R1 的 BFD 状态，已经切换为 Down
```

Local Remote	PeerIpAddr	State	Type	InterfaceName
10 20	13.1.1.2	Down	S_IP_IF	GigabitEthernet0/0/1

```
Total UP/DOWN Session Number : 0/1
```

在 BFD 的快速检测机制作用下，R1 会立即将与该 BFD 会话绑定的主用静态路由撤销，使其不再参与选路。此时再次查看 R1 路由表，可以看到缺省路由的下一跳已自动由原主链路切换为备份链路的 12.1.1.2，业务流量随之转移至备用线路，实现了快速、自动的故障切换。

```
[R1] display ip routing-table
```

```
Route Flags: R - relay, D - download to fib
```

```
Routing Tables: Public
```

Destinations : 12		Routes : 11				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
<b>0.0.0.0/0</b>	<b>Static</b>	<b>100</b>	<b>0</b>	<b>RD</b>	<b>12.1.1.2</b>	<b>GigabitEthernet0/0/0</b>
12.1.1.0/24	Direct	0	0	D	12.1.1.1	GigabitEthernet0/0/0
12.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
12.1.1.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
13.1.1.0/24	Direct	0	0	D	13.1.1.1	GigabitEthernet0/0/1
13.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
13.1.1.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1

#### 4. BFD 单臂回声

当对端设备不支持 BFD 功能（如部分老旧防火墙或无法配置 BFD 的设备）时，可在本端启用 BFD 单臂回声机制。本端主动发送 BFD 检测报文，对端仅在网络层进行环回转发，无须参与 BFD 会话的建立与维护，仍可实现对转发路径连通性的检测。

以下为 R1 单臂回声的配置示例，仅需在 R1 侧进行配置，R3 无须任何配置，即可完成对 R1 与 R3 之间链路连通性的检测。

```
[R1] bfd //首先需要全局下开启 bfd
[R1-bfd] quit //退出 bfd 配置视图
[R1] bfd R1toR3_echo bind peer-ip 13.1.1.2 interface g0/0/1 one-arm-echo //创建 bfd 单臂回声会话
[R1-bfd-session-r1tor3_echo] discriminator local 1000 //配置本地标识符 (单臂回声不需要配置 discriminator remote id)
[R1-bfd-session-r1tor3_echo] min-echo-rx-interval 300 // (可选) 调整发包时间为 300ms
[R1-bfd-session-r1tor3_echo] detect-multiplier 3 // (可选) 设置检测超时时间为 3 倍
[R1-bfd-session-r1tor3_echo] commit //提交配置
[R1-bfd-session-r1tor3_echo] quit //退出当前视图
```

查看 BFD 状态，状态已经处于 up，表示对端 IP 地址 13.1.1.2 处于连通状态。

```
[R1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
1000	-	13.1.1.2	Up	S_IP_IF	GigabitEthernet0/0/1

Total UP/DOWN Session Number : 1/0

## 1.5 静态路由和 NQA 联动

### 1. NQA 原理

网络质量分析 (Network Quality Analysis, NQA) 是一种由网络设备主动发起的网络性能探测与统计技术，可对**时延、抖动、丢包率等**关键性能指标进行实时测量。通过 NQA，设备能够持续监视网络服务质量 (QoS)，并在网络发生异常时为故障诊断与定位提供依据。

在网络运维中，为使网络服务质量可视化，通常需要采集大量性能数据，传统方式往往依赖专用探针设备或额外监测系统，增加了建设和运维成本。引入 NQA 功能后，无须部署独立探针，即可在现有设备上完成网络质量检测，从而有效降低投入成本。

NQA 支持对多种协议和业务性能进行监测，可**实时获取 HTTP 总时延、TCP 连接时延、DNS 解析时延与错误率、文件传输速率、FTP 连接时延等**运行指标，为网络质量评估、性能优化和故障排查提供可靠的数据支撑。

## 2. NQA 配置

NQA 配置逻辑比 BFD 稍复杂，分为“配置测试实例”和“关联路由”两步。

第 1 步：配置 NQA 测试实例。

```
[R1] nqa test-instance admin icmp_probe //创建管理员为 admin，名称为 icmp_probe 的实例
[R1-nqa-admin-icmp_probe] test-type icmp //指定测试类型为 ICMP（即 Ping）
[R1-nqa-admin-icmp_probe] destination-address ipv4 13.1.1.2 //探测目标的 IP（ISP 网关）
[R1-nqa-admin-icmp_probe] frequency 10 //每隔 10 秒探测一次
[R1-nqa-admin-icmp_probe] probe-count 2 //配置 NQA 测试探针数目为 2
[R1-nqa-admin-icmp_probe] start now //立即启动探测
[R1-nqa-admin-icmp_probe] quit
```

第 2 步：默认路由关联 NQA。

```
[R1] ip route-static 0.0.0.0 0.0.0.0 13.1.1.2 track nqa admin icmp_probe
//当 nqa 状态正常时（即 13.1.1.2 可以 ping 通），该默认路由生效，否则失效
```

## 3. BFD 和 NQA 对比

BFD 侧重于“快”，能以极小的协议开销实现毫秒级的链路及转发路径故障检测，仅用于判断连通性，主要为静态路由或动态路由协议提供快速失效触发机制。NQA 侧重于“全”和“活”，不仅可检测连通性，还可模拟真实业务流量，对时延、抖动、丢包率等性能指标进行主动探测，更适用于网络质量评估、故障定位和业务感知。两者对比见表 1-4。

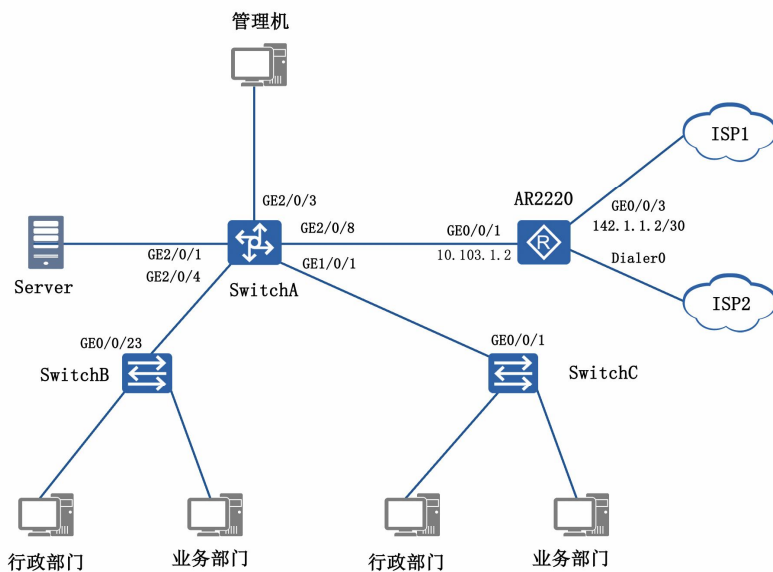
表 1-4 BFD 和 NQA 对比

维度	BFD（双向转发检测）	NQA（网络质量分析）
检测速度	极快（毫秒级），故障切换几乎无感	较慢（秒级），默认通常为秒级探测，探测频率过高将显著增加 CPU 负载
部署条件	双边协商，两端设备都支持并配置 BFD（除单臂回声外）	单边部署，仅需本端配置，对端只需具备基础 IP 转发功能即可
检测层次	网络层/链路层，仅检测连通性（能否 ping 通）	多层次（L2~L7），不仅能 ping，还能测 TCP 端口、DNS 解析、HTTP 网页打开速度等
资源消耗	硬件辅助，大多由线卡芯片处理，CPU 占用低	软件处理，主要由主控 CPU 模拟发包，大量部署会消耗 CPU
应用场景	核心骨干网、数据中心互联、直连设备高可用	互联网出口检测（探测 ISP）、服务可用性检测（如 Web 服务器检测）

## 1.6 考前冲刺精华习题

### 试题 1 (6 分)

根据下图所示, 公司采用两条链路接入 Internet, 其中, ISP2 是 (1) 链路。



路由器 AR2220 的部分配置如下:

```
detect-group 1
detect-list 1 ip address 142.1.1.1
timer loop 5
ip route-static 0.0.0.0 0.0.0.0 Dialer 0 preference 100
ip route-static 0.0.0.0 0.0.0.0 142.1.1.1 preference 60 detect-group 1
```

由以上配置可知, 用户默认通过 (2) 访问 Internet, 该配置片段实现的网络功能是 (3)。

- (1) 备选答案: A. 以太网            B. PPPoE  
 (2) 备选答案: A. ISP1            B. ISP2

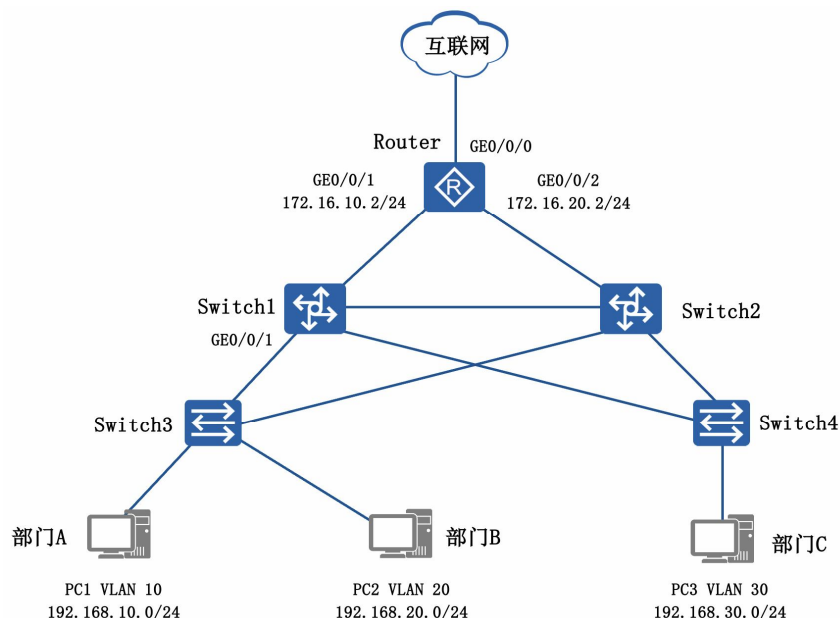
#### 【参考答案】

- (1) B    (2) A    (3) 网络冗余备份 (或出口主备路由)

**【summer 解析】** 根据浮动路由的选路规则, 优先级为 60 的路由将作为主路由; 当其下一跳失效时, PPPoE 拨号线路对应的备份路由被激活并投入使用。

### 试题 2 (4 分)

某园区组网方案如下图所示, 数据规划见下表。



操作	准备项	数据	说明
配置接口和 VLAN	Eth-Trunk 类型	静态 LACP	Eth-Trunk 链路支持手工负载分担和静态 LACP 两种工作模式
	端口类型	连接交换机的端口设置为 trunk; 连接 PC 的端口设置为 access	交换机互联端口采用 trunk 模式, 终端接入端口采用 access 模式
	VLAN ID	Switch3: VLAN 10、20 Switch1: VLAN 10、20、30、100、300	交换机有缺省 VLAN 1, 为二层隔离部门 A 和 B, 将部门 A 划到 VLAN 10, 部门 B 划到 VLAN 20, Switch1 通过 Vlanif100 连接到出口路由器
配置核心交换机路由	IP 地址	Switch1: Vlanif100 172.16.10.1/24 Vlanif300 172.16.30.1/24 Vlanif10 192.168.10.1/24 Vlanif20 192.168.20.1/24	Vlanif 100 用于 Switch1 与出口路由器对接, VLAN 300 用于 Switch1 与 Switch2 对接。Switch1 上配置 VLAN 10、VLAN 20 的 IP 地址后, 部门 A 与部门 B 之间可通过 Switch1 互通 Switch1 上需要配置一条缺省路由, 下一跳指向出口路由器; 配置一条备用路由, 下一跳指向 Switch2
配置出口路由器	公网接口 IP 地址	GE0/0/0 202.101.111.2/30	GE0/0/0 为出口路由器连接 Internet 的接口, 一般称为公网接口
	公网网关	202.101.111.1/30	该地址是与出口路由器对接的运营商设备 IP 地址, 出口路由器上需要配置一条缺省路由, 用于将内网流量转发到 Internet

续表

操作	准备项	数据	说明
配置出口路由器	内网接口 IP 地址	GE0/0/1:172.16.10.2/24 GE0/0/2:172.16.20.2/24	GE0/0/1、GE0/0/2 为出口路由器连接内网的接口，GE0/0/1 用于连接主设备，GE0/0/2 用于连接备份设备

如果配置静态路由实现网络互通，补充在 Switch1 和 Router 上配置的命令片段。

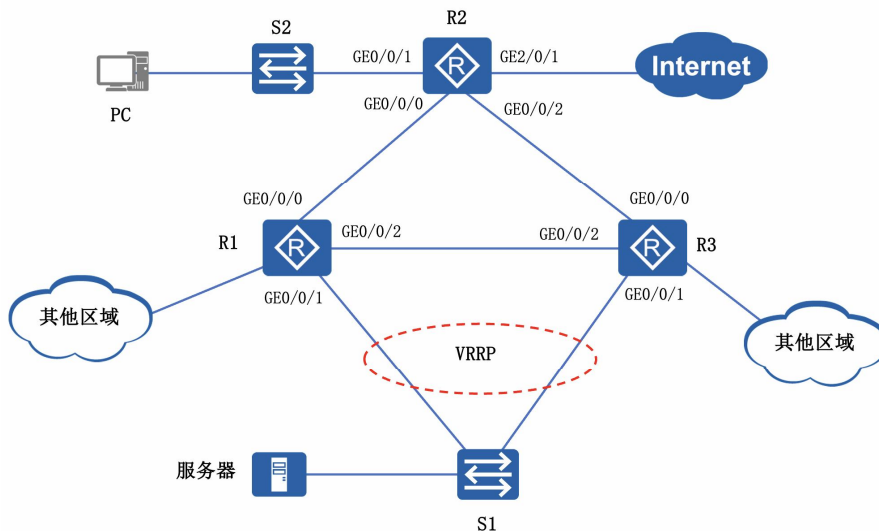
```
[Switch1] ip route-static (1) //默认优先级
[Switch1] ip route-static 0.0.0.0 0.0.0.0 172.16.30.2 preference 70
[Router] ip route-static (2) //默认优先级
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.10.1
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.20.1 preference70
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.10.1
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.20.1 preference70
```

【参考答案】(1) 0.0.0.0 0.0.0.0 172.16.10.2 (2) 0.0.0.0 0.0.0.0 202.101.111.1

【summer 解析】掌握静态路由配置。理解拓扑图和表格数据的对应关系，从表格可以看出 Switch1 和 Router 对接的 VLAN 为 100，主用默认路由器下一跳为 Router 的 GE0/0/1，即 IP 地址 172.16.10.2。出口路由器需要配置指向互联网（即公网关）的默认路由，下一跳为 202.101.111.1。

试题 3 (6 分)

某公司网络拓扑如下图所示，其中出口路由器 R2 连接 Internet，PC 所在网段为 10.1.1.0/24，服务器 IP 地址为 10.2.2.22/24，R2 连接的 Internet 出口网关地址为 110.125.0.1/28。各路由器端口及所对应的 IP 地址信息如下表所示。假设各个路由器和主机均已完成各个接口 IP 地址的配置。



路由器	端口	IP 地址
R1	GigabitEthernet0/0/0	10.12.0.1/29
	GigabitEthernet0/0/1	10.2.2.1/24
	GigabitEthernet0/0/2	10.13.1.1/29
R2	GigabitEthernet0/0/0	10.12.0.2/29
	GigabitEthernet0/0/1	10.1.1.1/24
	GigabitEthernet0/0/2	10.23.0.2/29
	GigabitEthernet2/0/1	110.125.0.2/28
R3	GigabitEthernet0/0/0	10.23.0.3/29
	GigabitEthernet0/0/1	10.2.2.3/24
	GigabitEthernet0/0/2	10.13.1.3/29

通过静态路由配置使路由器 R1 经过路由器 R2 作为主链路连接 Internet, R1→R3→R2→Internet 作为备份链路; 路由器 R3 经过路由器 R2 作为主链路连接 Internet, R3→R1→R2→Internet 作为备份链路。

请按要求补全命令或回答问题。

R1 上的配置片段:

```
[R1] ip route-static 0.0.0.0 0.0.0.0 (1)
[R1] ip route-static 0.0.0.0 0.0.0.0 (2) preference 100
```

R2 上的配置片段:

```
[R2] ip route-static (3) 110.125.0.1
```

以下两条命令的作用是 (4)。

```
[R2] ip route-static 10.2.2.0 255.255.255.0 10.12.0.1
[R2] ip route-static 10.2.2.0 255.255.255.0 10.23.0.3 preference 100
```

**【参考答案】** (1) 10.12.0.2 (2) 10.13.1.3 (3) 0.0.0.0 0.0.0.0 (4) 配置去往服务器网段的浮动路由, 优先走 R1 路由器, 把经 R3 的链路作为备份。

**【summer 解析】** 掌握浮动路由配置, 并能通过文字进行描述。

#### 试题 4 (20 分)

某公司网络拓扑如下图所示, 从 R1 到 R2 有两条转发路径, 下一跳分别为 R2 和 R3。由于 R1 和 R2 之间的物理距离较远, 通过一个二层交换机 SW1 作为中继。假设所有设备均已完成接口 IP 地址配置。

**【问题 1】** (4 分)

从 PC1 发出的目的地址为 ISP1 的 IP 报文, 将默认发到 R2 的 GE2/0/1。PC1 构造帧时, 是否需要获得该接口的 MAC 地址? 为什么?