ICMP 协议

一、基本功能

全称： Internet 控制消息协议(Internet Control Message Protocol)

作用： 通过传递 ICMP 报文，进行差错检查，错误报告以及控制功能。

1. 控制功能（重定向）

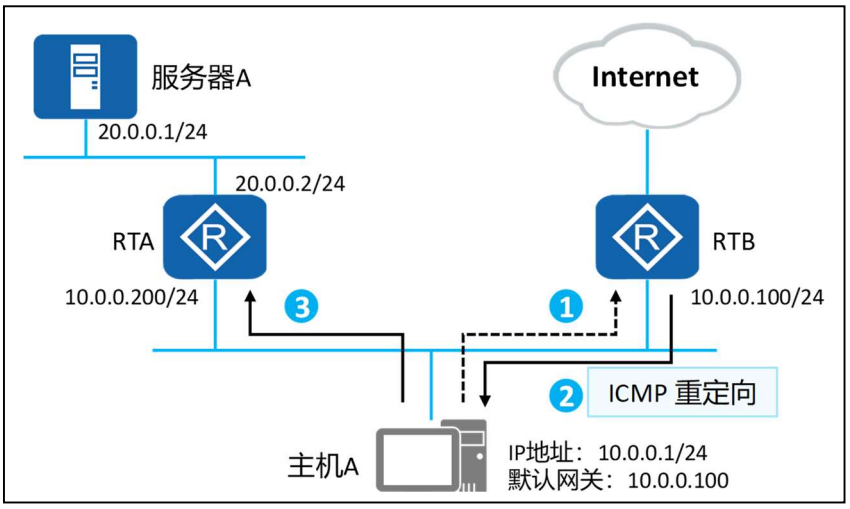

图 1. 控制功能（重定向）场景图

如上图场景中：当主机 A(10.0.0.1)想要访问服务器 A(20.0.0.1)时，由于主机和服务器处于不同网段，主机 A 需要将访问信息发送给网关路由 RTB，RTB 再将访问信息发送给服务器 A，这种情况下就会出现：次优路径。

ICMP 重定向的解决方法：主机在进行不同网段访问时，数据会交给网关（路由器），当路由器从接口收到该数据包时，进行查找路由表条目，发现数据包发出的接口和收到的接口一致时，会触发重定向报文。

重定向报文包含：访问的目的地址+最优下一跳。

回到上图场景：网关路由器收到主机 A 要访问服务器 A 的信息后，会将重定向报文发送给主机 A，主机 A 收到后，产生主机路由，主机后续访问服务器 A 直接通过重定向报文中的下一跳进行访问，也就是直接将访问信息直接发送给

RTA，不需要再通过网关路由器进行转发，从而解决次优路径。

2. 差错检测与错误报告功能

ICMP 定义了各种错误消息，用于诊断网络连接性问题；根据这些错误消息，源设备可以判断出数据传输失败的原因。

1） 超时

如果网络中发生了环路，导致报文在网络中循环，且最终 TTL 超时，这种情况下网络设备会发送 TTL 超时消息给发送端设备。

2） 目的地不可达

如果目的地不可达，则中间的网络设备会发送目的不可达消息给发送端设备。目的不可达的情况有多种，如果是网络设备无法找到目的网络，则发送目的网络不可达消息；如果网络设备无法找到目的网络中的目的主机，则发送目的主机不可达消息。

二、ICMP 数据包格式

Type	Code	Checksum
ICMP的报文内容		

Type	Code	描述
0	0	Echo Reply
3	0	网络不可达
3	1	主机不可达
3	2	协议不可达
3	3	端口不可达
5	0	重定向
8	0	Echo Request
11	0	Time out

图 2. ICMP 报文格式图

ICMP 报文封装在 IP 报文中，IP 报文头部 Protocol 值为 1 时表示 ICMP 协议。

字段解释：

1. Type 和 Code 字段：ICMP 消息的格式取决于 Type 和 Code 字段，其中 Type 字段为消息类型，Code 字段包含该消息类型的具体参数。常见的类型与代码关系如图 2 所示，完整的类型与代码对应关系如表 1 所示，蓝色标出部分是常用 ICMP 报文。

注意：type 为 3 的都是目的不可达信息，也称为差错报文。

2. 校验和字段：用于检查消息是否完整。
3. 报文内容中包含 32 bit 的可变参数，这个字段一般不使用，通常设置为 0。

- 在 ICMP 重定向消息中，这个报文内容字段用来指定网关 IP 地址，主机根据这个地址将报文重定向到指定网关。
- 在 Echo 请求消息中，报文内容字段包含标识符和序号，源端根据这两个参数将收到的回复消息与本端发送的 Echo 请求消息进行关联。尤其是当源端向目的端发送了多个 Echo 请求消息时，需要根据标识符和序号将 Echo 请求和回复消息进行一一对应。

表 1. ICMP 报文类型与代码

类型 TYPE	代码 CODE	用途|描述 Description	查询类 Query	差错类 Error
0	0	Echo Reply——回显应答（Ping 应答）	x	
3	0	Network Unreachable——网络不可达		x
3	1	Host Unreachable——主机不可达		x
3	2	Protocol Unreachable——协议不可达		x
3	3	Port Unreachable——端口不可达		x
3	4	Fragmentation needed but no frag. bit set——需要进行分片但设置不分片比特		x
3	5	Source routing failed——源站选路失败		x

类型 TYPE	代码 CODE	用途|描述 Description	查询类 Query	差错类 Error
3	6	Destination network unknown——目的网络未知		x
3	7	Destination host unknown——目的主机未知		x
3	8	Source host isolated (obsolete)——源主机被隔离（作废不用）		x
3	9	Destination network administratively prohibited——目的网络被强制禁止		x
3	10	Destination host administratively prohibited——目的主机被强制禁止		x
3	11	Network unreachable for TOS——由于服务类型 TOS，网络不可达		x
3	12	Host unreachable for TOS——由于服务类型 TOS，主机不可达		x
3	13	Communication administratively prohibited by filtering——由于过滤，通信被强制禁止		x
3	14	Host precedence violation——主机越权		x
3	15	Precedence cutoff in effect——优先中止生效		x
4	0	Source quench——源端被关闭（基本流控制）		x
5	0	Redirect for network——对网络重定向		x
5	1	Redirect for host——对主机重定向		x
5	2	Redirect for TOS and network——对服务类型和网络重定向		x
5	3	Redirect for TOS and host——对服务类型和主机重定向		x
8	0	Echo request——回显请求（Ping 请求）	x	
9	0	Router advertisement——路由器通告	x	
10	0	Route solicitation——路由器请求	x	

类型 TYPE	代码 CODE	用途|描述 Description	查询类 Query	差错类 Error
11	0	TTL equals 0 during transit——传输期间生存时间为 0		x
11	1	TTL equals 0 during reassembly——在数据报组装期间生存时间为 0		x
12	0	IP header bad (catchall error)——坏的 IP 首部（包括各种差错）		x
12	1	Required options missing——缺少必需的选项		x
13	0	Timestamp request (obsolete)——时间戳请求（作废不用）	x	
14		Timestamp reply (obsolete)——时间戳应答（作废不用）	x	
15	0	Information request (obsolete)——信息请求（作废不用）	x	
16	0	Information reply (obsolete)——信息应答（作废不用）	x	
17	0	Address mask request——地址掩码请求	x	
18	0	Address mask reply——地址掩码应答	x	

三、ICMP 的两大应用

1. Ping 命令

ICMP 差错检测与错误报告的典型应用是 Ping。Ping 是检测网络连通性的常用工具，同时也能够收集其他相关信息。用户可以在 Ping 命令中指定不同参数，如 ICMP 报文长度、发送的 ICMP 报文个数、等待回复响应的超时时间等，设备根据配置的参数来构造并发送 ICMP 报文，进行 Ping 测试。

Ping 命令通过查询(request)和响应(reply)进行实现。

使用功能：差错检测。

作用：测试网络连通性。

1） 路由与交换设备上 Ping 命令参数说明

ping + 目的 IP(域名) + 选项（-a、-c 等等)

- ping -a：指定报文的源 IP，默认为出接口 IP 地址
- ping -c：指定报文发送的数量，默认为 5
- ping -t：持续发送报文
- ping -h：指定 TTL 的值，默认值为 255
- ping -i：指定发送 ICMP 报文的接口

2) Windows 系统中的 Ping 命令参数说明

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [-j computer-list] | [-k computer-list] [-w timeout] destination-list

- -t Ping 指定的计算机直到中断。
- -a 将地址解析为计算机名。
- -n count 发送 count 指定的 ECHO 数据包数。默认值为 4。
- -l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节;最大值是 65,527。
- -f 在数据包中发送"不要分段"标志。数据包就不会被路由上的网关分段。
- -i ttl 将"生存时间"字段设置为 ttl 指定的值。
- -v tos 将"服务类型"字段设置为 tos 指定的值。
- -r count 在"记录路由"字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。
- -s count 指定 count 指定的跃点数的时间戳。
- -j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)IP 允许的最大数量为 9。
- -k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)IP 允许的最大数量为 9。
- -w timeout 指定超时间隔，单位为毫秒。

- destination-list 指定要 ping 的远程计算机。

2. Tracert 命令

ICMP 的另一个典型应用是 Tracert。

Tracert 基于报文头中的 TTL 值来逐跳跟踪报文的转发路径。为了跟踪到达某特定目的地址的路径，源端首先将报文的 TTL 值设置为 1。该报文到达第一个节点后，TTL 超时，于是该节点向源端发送 TTL 超时消息，消息中携带时间戳。然后源端将报文的 TTL 值设置为 2，报文到达第二个节点后超时，该节点同样返回 TTL 超时消息，以此类推，直到报文到达目的地。这样，源端根据返回的报文中的信息可以跟踪到报文经过的每一个节点，并根据时间戳信息计算往返时间。

设备无法访问时，会自动会送相应的 ICMP 差错报文，可用于排障。用以跟踪数据包经过的**三层设备。**

使用功能：错误报告

作用：用于跟踪数据包的转发路径。一般用于排障。

1） 路由与交换设备上 tracert 命令参数说明

tracert + 选项（-a、-f、-m 等等） + 目的 IP 地址

- tracert -a 指定源 IP
- tracert -f 指定初次 TTL 的值
- tracert -q 指定发送单个报文的次数，默认为 3
- tracert -m 最大的 TTL 值，默认为 30

2） Windows 系统中的 Tracert 命令参数说明

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

- -d 不将地址解析成主机名。
- -h maximum_hops 搜索目标的最大跃点数。
- -j host-list 与主机列表一起的松散源路由(仅适用于 IPv4)。

- -w timeout　　等待每个回复的超时时间(以毫秒为单位)。
- -R　　跟踪往返行程路径(仅适用于 IPv6)。
- -S srcaddr　　要使用的源地址(仅适用于 IPv6)。
- -4　　强制使用 IPv4。
- -6　　强制使用 IPv6。