IP Routing Frequently Asked Questions

Document ID: 28745

Contents

Introduction

This document provides answers to some of the more frequently asked questions about IP Routing.

Note: For information on document conventions, refer to Cisco Technical Tips Conventions.

Q. What does it mean to have fast or autonomous switching "enabled" and "disabled" on the same interface?

> **A.** Look at this example:

```
Ethernet 6 is up, line protocol is up
        Internet address is 192.192.15.1, subnet mask is 255.255.255.0
        Broadcast address is 192.192.15.255
        Address determined by non-volatile memory MTU is 1500 bytes
        Helper address is 192.192.12.5
        Outgoing access list is not set
        Proxy ARP is enabled
        Security level is default
        Split horizon is enabled
        ICMP redirects are always sent
        ICMP unreachables are always sent
        ICMP mask replies are never sent

        IP autonomous switching is enabled
        IP autonomous switching on the same interface is disabled
        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        Gateway Discovery is disabled
        IP accounting is disabled
        TCP/IP header compression is disabled
        Probe proxy name replies are disabled
```

> If you enable fast or autonomous switching on an interface, packets coming from any other interface on the router are fast−switched (or autonomous−switched) to that interface. If you enable same−interface fast or autonomous switching, packets whose source and destination address are the same are fast or autonomous switched.

> You can use same−interface fast or autonomous switching in cases where you have Frame Relay or Asynchronous Transfer Mode (ATM) WAN links configured as subinterfaces on the same main interface. Another situation is when you are using secondary networks on LAN interfaces, as during IP address migration. In order to enable same−interface fast switching, use the **ip route−cache same−interface** configuration command.

Q. How is the load shared between two parallel lines of equal capacity when these lines are configured for load balancing?

> **A.** For IP, if the router is fast switching, it load balances on a per−destination basis. If the router is process switching, it load balances on a per−packet basis. For more information, refer to How Does Load−Balancing Work? Cisco IOS® Software also supports both per packet and per destination load balancing with Cisco Express Forwarding (CEF). For more information, refer to Load Balancing with CEF and Troubleshooting Load Balancing Over

Parallel Links Using Cisco Express Forwarding.

Q. What does route summarization mean?

A. Summarization is the process by which we collapse many routes with a long mask to form another route with a shorter mask. Refer to OSPF and Route Summarization and the "Summarization" section of Enhanced Interior Gateway Routing Protocol for more information. The **auto−summary** command works only if you have contiguous subnets. If you work with discontiguous subnets, you need to use the **ip summary−address** interface configuration command on every interface that participates in the routing process where you want to configure summarization.

Q. When does a Cisco router generate a source quench?

A. Prior to Cisco IOS® Software Releases 11.3 and 12.0, a Cisco router generates a source quench only if it does not have the buffer space needed to queue the packet. If the router can't queue the routed packet onto the output interface's queue, it generates a source quench and registers an output drop against the output interface. If the router isn't congested, it won't generate a source quench.

You can look at the **show ip traffic** command output for source quenches sent. Also look at **show interface** to see if there are any drops. If there are none, then you should not see any source quench.

Cisco IOS Software Releases later than 11.3 and 12.0 do not include the source quench feature.

Q. When does a Cisco router initiate a routing request out its interfaces?

A. A Cisco router that runs a distance vector routing protocol initiates a routing request out its interfaces if any of these conditions are met:

- ◆ The interface goes down.
- ◆ There is any change to the **router** global configuration command.
- ◆ There is any change to the **metric** configuration command.
- ◆ The **clear ip route** EXEC command is used.
- ◆ The **shutdown** interface configuration command is used.
- ◆ The router is booted.
- ◆ There is any change to the **ip address** command.

The request is sent out to all interfaces configured for that particular protocol no matter which interface triggers the request. The request is sent out to one interface only if that is the only interface configured for the protocol.

When the **debug ip igrp events** or the **debug ip igrp transactions** command is enabled, you see this in any of these situations:

```
IGRP: broadcasting request on Ethernet0
IGRP: broadcasting request on Ethernet1
IGRP: broadcasting request on Ethernet2
IGRP: broadcasting request on Ethernet3
```

Q. What is the difference between the ip default–gateway, ip default–network, and ip route 0.0.0.0/0 commands?

A. The **ip default–gateway** command is used when IP routing is disabled on the router. However, **ip default–network** and **ip route 0.0.0.0/0** are effective when IP routing is enabled on the router and they are used to route any packets which do not have an exact route match in the routing table. Refer to Configuring a Gateway of Last Resort Using IP Command for more information.

Q. How do I use the ip helper–address command to forward Bootstrap Protocol (BOOTP) frames?

A. The **ip helper–address** command takes an argument of either the IP address of the BOOTP server or a directed broadcast address for the segment on which the BOOTP server resides. You can also have multiple instances of the command with different IP addresses if you have more than one BOOTP server. The ip helper–address command can also be used on individual sub interfaces.

Q. Enhanced Interior Gateway Routing Protocol (EIGRP) redistributes with the IGRP IP routing protocol automatically. Does EIGRP also interact with the Routing Information Protocol (RIP) IP routing protocol?

A. EIGRP can interact with RIP using the **redistribute** commands. Because RIP and EIGRP are so fundamentally different, automatic interaction would probably produce unpredictable and undesirable results. However, automatic interaction is possible between EIGRP and IGRP because of their architectural similarities. Refer to Redistributing Routing Protocols for more information.

Q. How do I configure my router to prefer an Open Shortest Path First (OSPF) route over an EIGRP route when the route is learned from both sources?

A. The short answer is to use the **distance** command under the routing process. OSPF has a default administrative distance of 110 and EIGRP has a default administrative distance of 90 for internal routes. If the same route prefixes are learned under both routing protocols, EIGRP–learned routes will be installed into the IP routing table because of the lower administrative distance (90 is less than 110). The key to having OSPF routes installed in the Routing Information Base (RIB), instead of EIGRP routes, is to make the administrative distance of OSPF less than that of EIGRP that uses the **distance ospf** command. To learn more about administrative distance, refer to What Is Administrative Distance?

Q. Does the use of extended IP access control lists (ACLs) filter regular routing updates (such as OSPF)? Do I need to explicitly permit the multicast IPs used by routing protocols (such as 224.0.0.5 and 224.0.0.6, in the case of OSPF) for updates to ensure the proper working of routing protocols?

A. Any IP ACL on an interface is applied to any IP traffic on that interface. All IP routing updates packets are handled as regular IP packets at the interface level, and, thus, they are matched with the ACL defined at the interface using the **access–list** command. To ensure that

the routing updates are not denied by ACLs, permit them using the following statements.

To permit RIP use:

```
access-list 102 permit udp any any eq rip
```

To permit IGRP use:

```
access-list 102 permit igrp any any
```

To permit EIGRP use:

```
access-list 102 permit eigrp any any
```

To permit OSPF use:

```
access-list 102 permit ospf any any
```

To permit Border Gateway Protocol (BGP) use:

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

For more information on ACLs, refer to Configuring IP Access Lists and Configuring Commonly Used IP ACLs.

Q. Does the interface subcommand no arp arpa disable the Address Resolution Protocol (ARP) function for a router interface?

A. By Advanced Research Projects Agency (ARPA) ARP, you mean "Ethernet interfaces" and, by default, ARP ARPA is set with **no arp snap**. This means that ARPA style ARPs are sent, but both ARPA and Subnetwork Access Protocol (SNAP) are answered. By setting **no arp arpa**, ARP requests are disabled, although null entries are created for every station to which an ARP request is attempted. You can enable SNAP alone, ARPA alone (the default), both SNAP and ARPA together (send two ARPs every time), or neither SNAP nor ARPA (which is what happens if you set **no arp arpa** without setting up any other ARP).

Q. Would it be possible to configure a router for a 255.255.254.0 Ethernet and a 255.255.252.0 serial subnet? Does IGRP/RIPv1 support variable subnetting?

A. Yes it is possible to configure these subnet masks. In order to subnet on a Cisco router, the subnet bits must be contiguous, so 255.255.253.0 would not be valid (11111111.11111111.11111101.00000000) while 225.255.252.0 would be valid (11111111.11111111.11111100.00000000). Subnetting by borrowing all but one bits from the host portion is not allowed. Also, traditionally, subnetting with a single bit was not allowed. The masks above satisfy these conditions. Refer to IP Addressing and Subnetting for New Users for more information.

IGRP RIP version 1 do not support variable length subnet masking (VLSM). A single router running any of these protocols would work fine with variable length subnetting. An incoming packet destined for one of the configured subnets would be routed properly and delivered to the correct destination interface. However, if the VLSM and discontiguous networks are configured across multiple routers in IGRP domain, then it will lead to routing problems.

Refer to Why Doesn't RIP or IGRP Support Discontiguous Networks? for more information.

The newer IP routing protocols, EIGRP, ISIS, and OSPF, as well as RIP version 2, support VLSM, and they should be preferred in your network design. Refer to IP Routing Protocols Technical Support Page for more information on all IP routing Protocols.

Q. Can an interface have more than one ip access–group statement in its configuration?

A. In Cisco IOS versions 10.0 and later, you can have two **ip access–group** commands per interface (one for each direction):

```
interface ethernet 0
        ip access-group 1 in
        ip access-group 2 out
```

One **access–group** is used for inbound traffic and one for outbound traffic. Refer to Configuring Commonly Used IP ACLs and Configuring IP Access Lists for more information on ACLs.

Q. Can I configure two interfaces in the same subnet (t0 = 142.10.46.250/24 and t1 142.10.46.251/24)?

A. No. For the routing to work, each interface should be on a different subnet. However, if you are only bridging, and not doing IP routing, then you can configure the two interfaces on the same subnet.

Q. Is it possible to have duplicate ip addresses for two serial interfaces that belong to the same router?

A. Yes, duplicate ip addresses are allowed on serial interfaces. It is a more efficient way of bundling links together (ie. MLPPP) and also a better way to preserve address space. Change the encapsulation from the default HDLC to PPP in order to assign duplicate ip addresses.

Q. I have primary and secondary IP addresses configured on an Ethernet interface and my router is running RIP (a distance vector routing protocol). How does split–horizon affect the routing updates?

A. Refer to How Split Horizon Effects RIP/IGRP Routing Updates when Secondary Addresses Are Involved.

Q. Is there a performance advantage when using the the IP access list keyword *established* on an extended ACL? Does using "established" make the access list more vulnerable? Do you have specific examples of the usage?

A. There is no real performance advantage. The keyword *established* simply means that packets with the acknowledgment (ACK) or reset (RST) bits set are let through. To learn more about ACLs in general, refer to Configuring IP Access Lists.

The *established* keyword allows the internal hosts to make external TCP connections and to receive the return control traffic. In most scenarios, this type of ACL would be essential on a firewall configuration. The same result can also be achieved either by using Reflexive ACLs or Context−Based Access Control. Refer to Configuring Commonly Used IP ACLs for some sample configurations.

Q. I have four equal cost parallel paths to the same destination. I am doing fast switching on two links and process switching on the other two. How will the packets be routed in this situation?

A. Assume that we have four equal cost paths to some set of IP networks. Interfaces 1 and 2 fast switch (**ip route−cache** enabled on the interface) , 3 and 4 do not (**no ip route−cache**). The router first establishes the four equal cost paths in a list (path 1, 2, 3, and 4). When you do a **show ip route x.x.x.x**, the four "next hops" to x.x.x.x display.

The pointer is called interface_pointer on interface 1. Interface_pointer cycles through the interfaces and routes in some orderly deterministic fashion such as 1−2−3−4−1−2−3−4−1 and so on. The output of **show ip route x.x.x.x** has a "*" to the left of the "next hop" that interface_pointer uses for a destination address not found in the cache. Each time that interface_pointer is used, it advances to the next interface or route.

To illustrate the point better, consider this repeating loop:

♦ A packet comes in, destined for a network serviced by the four parallel paths.
♦ The router checks to see if it is in the cache. (The cache starts off empty.)
♦ If it is in the cache, the router sends it to the interface stored in the cache. Otherwise, the router sends it to the interface where the interface_pointer is and moves interface_pointer to the next interface in the list.
♦ If the interface over which the router just sent the packet is running route−cache, the router populates the cache with that interface ID and the destination IP address. All subsequent packets to the same destination are then switched using the route−cache entry (thus they are fast−switched).

If there are two route−cache and two non−route−cache interfaces, there is a 50 percent probability that a uncached entry will hit an interface that caches entries, caching that destination to that interface. Over time, the interfaces running fast switching (route−cache) carry all the traffic except destinations not in the cache. This happens because once a packet to a destination is process−switched over an interface, the interface_pointer moves and points to the next interface in the list. If this interface is also process−switched, then the second packet is process−switched over the interface and the interface_pointer moves on to point to the next interface. Since there are only two process−switched interfaces, the third packet will route to fast−switched interface, which, in turn, will cache. Once cached in the IP route−cache, all the packets to the same destination will be fast−switched. Thus, there is a 50 percent probability that a uncached entry will hit an interface that caches entries, caching that destination to that interface.

In case of a failure of a process−switched interface, the routing table is updated and you would have three equal cost paths (two fast−switched and one process−switched). Over time, the interfaces running fast switching (route−cache) carry all the traffic except destinations not in the cache. With two route−cache and one non−route−cache interfaces, there is a 66 percent probability that a uncached entry will hit an interface that caches entries, caching that destination to that interface. You can expect that the two fast switched interfaces will carry all the traffic over time.

Similarly when a fast switched interface fails, you would have three equal cost paths, one fast–switched and two process–switched. Over time the interface running fast switching (route–cache) carries all the traffic except destinations not in cache. There is 33 percent probability that a uncached entry would hit an interface that cached entries, caching that destination to that interface. You can expect that the single interface with caching enabled will carry all of the traffic over time in this case.

If *no* interface is running route–cache, the router round–robins the traffic on a packet–by–packet basis.

In conclusion, if multiple equal paths to a destination exist, some are process–switched while others are fast switched, then over time most of the traffic will be carried by the fast–switched interfaces only. The load balancing thus attained is not optimum and might in some cases lower the performance. Therefore, it is recommended that you do one of the following:

- ♦ Either have all route–cache or no route–cache on all interfaces in parallel paths.

  or
- ♦ Expect that the interfaces with caching enabled will carry all of the traffic over time.

Q. What is Unicast Reverse Path Forwarding (uRPF)? Can a default route 0.0.0.0/0 be used to perform a uRPF check?

A. Unicast Reverse Path Forwarding, used for preventing source address spoofing, is a "look backward" ability which allows the router to check and see if any IP packet received at a router interface arrives on the best return path (return route) to the source address of the packet. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, the packet is dropped or forwarded, depending on whether an access control list (ACL) is specified in the **ip verify unicast reverse–path list interface** configuration command. For more information, refer to the Configuring Unicast Reverse Path Forwarding chapter of the *Cisco IOS Security Configuration Guide, Release 12.2* .

Default route 0.0.0.0/0 can not be used to perform a uRPF check. For example, if a packet with source address 10.10.10.1 comes on Serial 0 interface and the only route matching 10.10.10.1 is the default route 0.0.0.0/0 pointing out Serial 0 on the router, the uRPF check fails and it drops that packet.

Q. Who does load–balancing when there are multiple links to a destination, Cisco Express Forwarding (CEF), or the routing protocol?

A. CEF does the switching of the packet based on the routing table which is being populated by the routing protocols such as EIGRP, RIP, Open Shortest Path First (OSPF), and so forth. CEF does the load–balancing once the routing protocol table has been calculated. For more details on load balancing, refer to How does load–balancing work?

Q. What are the maximum number of secondary IP addesses that can be configured on a router interface?

A. There are no limits on configuring secondary IP addresses on a router interface. For more information, refer to Configuring IP Addressing.

Q. What is the Pause control counter?

A. The Pause control counter indicates the number of times the router requests another router to slow the traffic. For example, two routers, Router A and Router B, are connected through a link with flow control enabled. If Router B faces a traffic burst, Router B sends a Pause output packet to inform Router A to slow the traffic because the link is oversubscribed. At that time, Router A receives a Pause input packet that informs it of the request sent by Router B. Pause output / input packets are not a problem or an error. They are simply flow control packets between two devices.

Q. Can a VLAN interface and a tunnel interface have the same IP address?

A. No. Bridging over tunnel is not supported, as the tunnel requires IP traffic to be encapsulated in a GRE header, and you cannot encapsulate the layer 2 traffic.

Q. What is Virtual Routing and Forwarding (VRF)?

A. Virtual Routing and Forwarding (VRF) is a technology included in IP network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality because it allows network paths to be segmented without the use of multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication. Internet Service Providers (ISPs) often take advantage of VRF in order to create separate Virtual Private Networks (VPNs) for customers. Therefore the technology is also referred to as VPN routing and forwarding.

VRF acts like a logical router, but while a logical router can include many routing tables, a VRF instance uses only a single routing table. In addition, VRF requires a forwarding table that designates the next hop for each data packet, a list of devices that can be called upon to forward the packet, and a set of rules and routing protocols that govern how the packet is forwarded. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that must remain outside the VRF path.

Q. How do I connect two different ISPs and route different traffic to different ISPs?

A. Policy based routing (PBR) is the feature that allows you to route the traffic to different ISPs based on the source address.

Q. What is the difference between the two methods to create static routes?

A. There are two methods to create static routes:

- The **ip route 10.1.1.1 255.255.255.0 eth 0/0** command generates an ARP broadcast that looks for the next–hop IP address.
- The **ip route 10.1.1.1 255.255.255.0 172.16.1.1** command does not generate an ARP request. It keeps Layer 2 out of the routing process.

Q. What is the purpose of ports 2228 and 56506?

A. Ports 2228 and 56506 are not registered port numbers. They can be used by any application. Some applications initiate a connection with these port numbers. Because of this, the port numbers are shown in the output of the **show ip sockets** command. If the port numbers need to be blocked, configure an access–list in order to block the ports.

Q. What is the difference between point–to–point subinterfaces and multi–point subinterfaces?

A. Point–to–point interfaces are used in serial communication. These types of connections are assumed to transmit solely to the station at the opposite end. The examples of Point–to–point are EIA/TIA 232, EIA/TIA 449, X.25, Frame Relay, T–carrier, and OC3 – OC192.

Point–to–multipoint connects one station to several other stations. Point–to–multipoint are of two types

- ♦ Point–to–multipoint Non–Broadcast
- ♦ Point–to–multipoint Broadcast

In Point–to–multipoint Non–broadcast, the communication is replicated to all the remote stations. Only specific, selected stations hear the replicated communication. The examples are Frame Relay and ATM.

Point–to–multipoint Broadcast are characterized by a physical medum that connects to all machines and where all communication is heard by all stations.

Q. Can you configure different MTU for subinterfaces under the same main interface? How do 7500/GSR/ESR routers behave in this scenario?

A. You can configure different IP MTU with the **ip mtu** command on different subinterfaces. When you change the MTU on a subinterface, the router checks the MTU from the main interface. If the main interface MTU is set to a lower value than the one configured on the subinterface, the router changes the MTU on the main interface to match with the subinterface. Thus, the physical MTU configured with the **mtu** command on the main interface needs to be higher than the IP MTU configured on the sub interfaces.

Packet memory is carved based on the highest MTU configured on 75000/GSR. There is one exception to this; the Engine 4+ linecard does not require to carve buffers on MTU change. On ESR, the packet memory is carved at boot time and is not affected by MTU settings. So if you change the MTU, you should not have any impact on ESR.

Q. How do you limit the number of sessions when a customer accesses the network?

A. If the customers use the same IP address, then use the **ppp ipcp address unique** command in order to reduce the number of sessions that the customer uses.

Q. How is accounting data age calculated?

A. The accounting data age increments its value in a 1 minute basis since the time IP accounting was enabled. This continues until the **clear ip accounting** command is issued,

which resets it from 0.

Q. What does the term threshold and timeout in IP SLA operation mean?

A. Threshold sets the rising threshold that generates a reaction event and stores history information for an IP SLAs operation.

Timeout sets the amount of time an IP SLAs operation waits for a response from its request packet.

Q. What is the significance of Time mentioned in the routing table entry?

A. This is the age of the route in the routing table. It is the time period for which the route is present in the routing table.

Q. What is Network Descriptor Block (NDB)?

A. It is the network information, which is stored in "Routing table" with Routing Descriptor Block (RDB). The memory to hold the IP routing table learned prefixes is divided into NDB and RDB. Each route in Routing information Base (RIB) requires one NDB and one RDB for each path. If the route is subnetted, additional memory is required in order to maintain the NDB, and the direct memory use for IP RIB can be shown with the **show ip route summary** command.

Related Information

- **BGP: Frequently Asked Questions**
- **MPLS FAQ For Beginners**
- **NAT Frequently Asked Questions**
- **OSPF: Frequently Asked Questions**
- **EIGRP Frequently Asked Questions**
- **QoS Frequently Asked Questions**
- **BGP Support Page**
- **MPLS Support Page**
- **IGRP Support Page**
- **EIGRP Support Page**
- **IP Routing Proctocols Support Page**
- **IP Routed Protocols Support Page**
- **IS–IS Support Page**
- **NAT Support Page**
- **OSPF Support Page**
- **RIP Support Page**
- **QoS Support Page**
- **Technical Support & Documentation – Cisco Systems**