Policy-Based Routing

Teldat-DM 745-I

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents. 1

Chapter 1 Policy-Based Routing Technology 2

1.1 Introduction 2

1.2 The Benefits of Policy-Based Routing 2

1.3 Policy-Based Routing Data Forwarding 2

1.3.1 Tagging Network Traffic 2

1.4 Applying Policy-Based Routing 3

1.4.1 Policy Route Maps 3

1.4.2 Match Clauses / Defining the Criteria 3

1.4.3 Set Clauses / Defining the Route 3

1.4.4 Management Implications 4

Chapter 2 Policy Routing Configuration 5

2.1 Introduction 5

2.2 Enabling Policy Routing 5

2.2.1 IP POLICY ROUTE-MAP 6

2.2.2 NO IP POLICY ROUTE-MAP. 6

2.2.3 LIST POLICY 6

2.2.4 LOCAL POLICY ROUTE-MAP 6

2.2.5 NO LOCAL POLICY ROUTE-MAP 6

Chapter 3 Policy Routing Monitoring 8

3.1 Monitoring tools 8

I Related Documents

Teldat-Dm 752-I Access Control

Teldat-Dm 764-I Route Mapping

Chapter 1 Policy-Based Routing Technology

1.1 Introduction

In today's high performance internetworks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. Where administrative issues dictate that traffic be routed through specific paths, policy-based routing, introduced in Teldat Routing Software Release 10.1, can provide the solution. By using policy-based routing, customers can implement policies that selectively cause packets to take different paths.

Policy routing also provides a mechanism to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques. These queuing techniques provide an extremely powerful, simple, and flexible tool to network managers who implement routing policies in their networks.

This chapter discusses the Teldat routing software policy-based routing feature and addresses policy-based routing and its functionality. In addition, the issues related to managing an internetwork with policy-based routing implemented are described. And finally, the applications of policy-based routing in internetworks are presented.

1.2 The Benefits of Policy-Based Routing

The benefits that can be achieved by implementing policy-based routing in the networks include:

- Source-Based Transit Provider Selection — Internet service providers and other organizations can use policy-based routing to route traffic originating from different sets of users through different Internet connections across the policy routers.
- Quality of Service (QOS) — Organizations can provide QOS to differentiated traffic by setting the precedence or type of service (TOS) values in the IP packet headers at the periphery of the network and leveraging queuing mechanisms to prioritize traffic in the core or backbone of the network.
- Cost Savings — Organizations can achieve cost savings by distributing interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost, switched paths.
- Load Sharing — In addition to the dynamic load-sharing capabilities offered by destination-based routing that the Teldat routing software has always supported, network managers can now implement policies to distribute traffic among multiple paths based on the traffic characteristics.

1.3 Policy-Based Routing Data Forwarding

Policy-based routing (PBR) provides a mechanism for expressing and implementing forwarding/routing of data packets based on the policies defined by the network administrators. It provides a more flexible mechanism for routing packets through routers, complementing the existing mechanism provided by routing protocols.

Routers forward packets to the destination addresses based on information from static routes or dynamic routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF), or BGP (Border Gateway Protocol). Instead of routing by the destination address, policy-based routing allows network administrators to determine and implement routing policies to allow or deny paths. These policies can be based on the following:

- Identity of a particular end system
- Application
- Protocol
- Size of packets

Policies can be defined as simply as "my network will not carry traffic from the engineering department" or as complex as "traffic originating within my network with the following characteristics will take path A, while other traffic will take path B."

1.3.1 Tagging Network Traffic

Policy-based routing allows network administrators to classify traffic using access control lists (ACLs) and then set the DSCP, IP precedence, TOS or the DF bit values, thereby tagging the packets with the defined classification.

Classification of traffic through policy-based routing allows the network administrator to identify traffic for different classes of service at the perimeter of the network and then implement QOS defined for each class of service in the core of the network using priority, custom, or weighted fair queuing techniques. This process saves having to classify the traffic explicitly at each WAN interface in the core/backbone network.

1.4 Applying Policy-Based Routing

Policy-based routing is applied to incoming packets. All unicast packets received on an interface with policy-based routing enabled are considered for policy-based routing. The router passes the packets through enhanced packet filters called route maps. Based on the criteria defined in the route maps, packets are forwarded/routed to the appropriate next hop.

1.4.1 Policy Route Maps

Each entry in a route map statement contains a combination of match and set clauses/commands. The match clauses define the criteria for whether appropriate packets meet the particular policy (that is, the conditions to be met). The set clauses explain how the packets should be routed once they have met the match criteria.

For each combination of match and set commands in a route map statement, all sequential match clauses must be met simultaneously by the packet for the set clauses to be applied. There may be multiple sets of combinations of match and set commands in a full route map statement.

The route map statements can also be marked as permit or deny. If the statement is marked as a deny, the packets meeting the match criteria are sent back through the normal forwarding channels (in other words, destination-based routing is performed). Only if the statement is marked as permit and the packets meet the match criteria are all the set clauses applied. If the statement is marked as permit and the packets do not meet the match criteria, then those packets are also forwarded through the normal routing channel.

Note

Policy routing is specified on the interface that receives the packets, not on the interface from which the packets are sent.

1.4.2 Match Clauses / Defining the Criteria

The IP standard or extended ACLs can be used to establish the match criteria. The standard IP access lists can be used to specify the match criteria for source address; extended access lists can be used to specify the match criteria based on application, protocol type, TOS, and precedence.

The match clause feature has been extended to include matching packet length between specified minimum and maximum values. The network administrator can then use the match length as the criterion that distinguishes between interactive and bulk traffic (bulk traffic usually has larger packet sizes).

The policy routing process proceeds through the route map until a match is found. If no match is found in the route map, or the route map entry is made a deny instead of a permit, then normal destination-based routing of the traffic ensues.

Note

There is an implicit deny at the end of the list of match statements.

1.4.3 Set Clauses / Defining the Route

If the match clauses are satisfied, one of the following set clauses can be used to specify the criteria for forwarding packets through the router; they are evaluated in the order listed:

(1) List of specified IP addresses and/or interfaces through which the packets can be routed — The IP address can specify the adjacent next hop router in the path towards the destination to which the packets should be forwarded. In order to sent the packets, you use the first one of the following conditions that is active: the first IP address associated to a currently connected interface, or the first specified interface that is ‘up’ or the *local* clause.

(2) List of default IP addresses and/or interfaces — Route to the interface or the next hop specified by this set clause only if there is no explicit route for the destination address of the packet in the routing table. In order to sent the packets, you use the first one of the following conditions that is active: the first IP address associated to a currently connected interface, or the first specified interface that is ‘up’ or the *local* clause.

(3) IP TOS — A value or keyword can be specified to set the type of service in the IP packets.

(4) IP precedence — A value or keyword can be specified to set the precedence in the IP packets.

(5) DSCP (Differentiated Services Code Point) value — You can specify a code from 0 to 63.

(6) DF (Don’t Fragment) bit — You can establish the IP header DF bit value.

The set commands can be used in conjunction with each other.

If the packets do not meet any of the defined match criteria (that is, if the packets fall off the end of a route map), then those packets are routed through the normal destination-based routing process. If it is desired not to revert to normal forwarding and to drop the packets that do not match the specified criteria, then a Loopback interface should be specified as the last interface in the list by using the set clause.

1.4.4 Management Implications

The route specified by configured policies might differ from the best route as determined by the routing protocols, enabling packets to take different routes depending on their source, length, and content. As a result, packet forwarding based on configured policies will override packet forwarding based on the routing entries in the routing tables to the same destination. For example, the management applications might discover a path that will pertain to the path discovered by a dynamic routing protocol or specified by static route mapping, whereas the actual traffic might not follow that path, based on the configured policies.

Similarly, the “traceroute” command might generate a path that is a different from the route used by the packets generated by the user application.

Because the added flexibility to route traffic on user-defined paths rather than the paths determined by routing protocols may make the environment more difficult to manage and might cause routing loops, policies should be defined in a deterministic manner to keep the environment simple and manageable.

Chapter 2 Policy Routing Configuration

2.1 Introduction

To enable policy routing, you must identify which route map to use for policy routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met. These steps are described in the Teldat-Dm764-I Route Mapping Manual.

To define the route map to be used for policy routing, use the following command in global configuration mode:

Command	Aim
Config>**feature route-map**	Enters route map configuration mode.
Route map config>**route-map** *map-tag*	Defines a route map controlling where the packets are transmitted.

Then configure the match and set clauses to define the criteria by which packets are examined to learn if they will be policy-routed, and to set the actions to be taken on matching packets.

To enable policy routing on an interface, indicate which route map the router should use by using the following command in IP protocol configuration menu and in the IP parameters configuration from the configuration menus of the interfaces where these are applied.

Command	Aim
<ifc> config>**ip policy route-map***map-tag*	Identifies the route map to use for packets arriving on an interface. All packets received through this interface are subject to policy routing.
IP config>**local policy route-map***map-tag*	Identifies the route map to use for locally generated packets.

2.2 Enabling Policy Routing

Policy Routing is independently enabled in each interface so that all packets entering through an interface are affected by the policy routing configuration for the said interface.

To configure Policy Routing in an interface, you first need to access the configuration menu for the interface in question:

```
*config
Config>network <interface_name>
<interface_name> config>
```

Commands relative to Policy Routing in an interface are as follows:

Command	Aim
ip policy route-map *map-tag*	Enables Policy Routing for packets received on this interface.
no ip policy route-map	Disables Policy Routing for packets received on this interface.

You can also enable Policy Routing for locally generated packets i.e. in the device itself (packets that have not entered through an interface).

In order to configure Policy Routing, access the general configuration menu:

To do this, access the ip protocol configuration menu from the general configuration menu:

```
*config
Config>protocol ip

-- Internet protocol user configuration --
IP config>
```

The commands used to enable Policy Routing for locally generated packets are as follows:

Command	Aim
local policy route-map *map-tag*	Enables Policy Routing for locally generated packets.
no local policy route-map	Disables Policy Routing for locally generated packets.

To check the policy routing configuration, use the **list policy** command.

These commands are explained in the following paragraphs.

2.2.1 IP POLICY ROUTE-MAP

This command enables Policy Routing for packets received on the interface which is being configured. This also defines the route map to use with the said packets.

Syntax:

```
<interface_name> config>ip policy routemap <maptag>
```

map-tag	Name of the route map to use.

Example:

```
ethernet0/0 config>ip policy route-map office
ethernet0/0 config>
```

2.2.2 NO IP POLICY ROUTE-MAP

This command disables Policy Routing for packets received on a specified interface.

Syntax:

```
<interface_name> config>no ip policy routemap
```

Example:

```
ethernet0/0 config>no ip policy route-map
ethernet0/0 config>
```

2.2.3 LIST POLICY

This command displays the policy routing configuration in those interfaces where this is enabled.

Syntax:

```
<interface_name> config>list policy
```

Example:

```
IP config> list policy
Ip policy routing:
  Interface      Route map
  ethernet0/0    office
  serial0/0      extern
  local          admin
IP config>
```

2.2.4 LOCAL POLICY ROUTE-MAP

This command enables Policy Routing for locally generated packets i.e. those packets that have not been received through an interface. This also defines the route map to be used with the said packets.

Syntax:

```
<interface_name> config>local policy route-map <map-tag>
```

map-tag	Name of the route map to be used.

Example:

```
IP config>local policy route-map office
IP config>
```

2.2.5 NO LOCAL POLICY ROUTE-MAP

This command disables Policy Routing for locally generated packets i.e. packets that have not been received through an interface.

Syntax:

```
<interface_name> config>no local policy route-map
```

Example:

```
IP config>no local policy route-map
IP config>
```

Chapter 3 Policy Routing Monitoring

3.1 Monitoring tools

Policy Routing functionality has the following monitoring mechanisms available:

(1) Access lists statistics

(2) POLR subsystem events.

The access lists statistics used in the route maps provide information on how many packets have matched each access list entry (and therefore with the route map). These also offer information on the last packet that matched each entry.

Example:

```
*monitor
+feature access
-- Access Lists user console --
Access Lists+list all all-access-lists

Standard Access List 1, assigned to Route map
 ACCESS LIST ENTRIES
1     PERMIT  SRC=172.24.51.104/32
        Hits: 277
  (172.24.51.104 <-> 172.24.78.116  :0x0  ICMP  TYPE=8 CODE=0  ECHO  DCSP:0)
Access Lists+
```

For further information on the access lists monitoring commands, please see manual Teldat-Dm752-I Access Control.

You can obtain detailed information on the actions carried out by the Policy Routing subsystem through the POLR subsystem events.

Example:

```
*monitor
+event
-- ELS Monitor --
ELS+enable trace subsystem polr all
ELS+view
ELS+03/24/03 10:27:27 *POLR.006 mis 172.24.77.253 -> 172.24.255.255 len 78 prt 17
int ethernet0/0 rtmap myhost
03/24/03 10:27:27  POLR.008 mch 172.24.51.104 -> 172.24.78.116 len 60 prt 1 int
ethernet0/0 rtmap myhost entry 25
03/24/03 10:27:27  POLR.009 set 172.24.51.104 -> 172.24.78.116 tos 0x00 to 0x10
03/24/03 10:27:27  POLR.012 fwd 172.24.51.104 -> 172.24.78.116 rt tbl
```

For further information on the POLR subsystem events, please see the events document *els.rtf* which is attached in the software distribution.