Routing Server

DESCRIPTION

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

1 GENERAL

1.1 ROUTING SERVER

In a private network that consists of IP trunks that interconnect the nodes, the Routing Server feature provides the capability to store all the IP routing information and alternative routing information, for the entire network, in one central database. This information can then be retrieved, as required, by routing server enabled nodes in the MX-ONE network in order to route calls to the required destination.

This feature provides one central point at which all network routing management can be handled without the necessity of individually reconfiguring each node in the network whenever network changes are required.

The Routing Server feature can, in addition to providing IP routing information for the routing of calls within the private network, provide alternative routing information for the routing of calls over non-IP routes (for example, the public network) in the event of network failure or congestion.

The Routing Server feature has built in routines to verify the integrity of the stored IP routing information as well as providing a *self learning* feature whereby detailed destination information for the network only needs to be stored in the central database. This will then be distributed to all the other nodes in the network, 2.2.4 PNR Table Splitting in the Satellite on page 9 .

The Routing Server may also be replicated elsewhere in the network, for redundancy, in the event that access to the primary routing server is not possible.

1.2 GLOSSARY AND ACRONYMS

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

2 DESCRIPTION

The Routing Server feature has two constituent parts, each of which are separately licensed objects; the server and the satellite (or client).

The server stores the IP routing and alternative routing information on a permanent basis (in reload data) while the satellites store the information on a temporary basis, where the information is dynamically updated to reflect the changes and network status in the server.

The server, eight of which may be defined, can either be normal MX-ONE traffic carrying nodes in the network or MX-ONE nodes designated exclusively for the server functionality.

The satellites are normal traffic carrying MX-ONE nodes containing simplified routing data stored in the local Private Network Routing (PNR) table for the routing of calls in the network.

2.1 SERVER FUNCTIONS

2.1.1 SERVER DATA

The IP routing and alternative routing data, used by the Routing Server, is programmed in the PNR table database.The data in the PNR (TAB) table consist of:

- Destination number (ENTRY)

  ENTRY specifies the destination number to the node to be analyzed.

- Fictitious routing table (FRCT)

  FRCT specifies which fictitious routing choice table (RCT) entry that shall be used to reach the destination. This is used in the routing server for routing of locally originated calls and in the routine check to reach the destination to be checked. All entries in the table may use the same FRCT value since they will use the same outgoing IP route to reach the entire network. It should be noted that only **one** IP route needs to be programmed in the server; all calls and Routing Server functions will utilize this single route.

- Digits to prefix (PRE)

  PRE specifies the prefix digits to be added to the destination number if the call needs to be alternatively routed. This information is conveyed to the satellites for alternative routing.

- Digits to truncate (TRC)

  TRC specifies the number of digits to be truncated from the destination number if the call would need to be alternatively routed. This information is conveyed to the satellites for alternative routing.

- Digits to prefix 1 (PRE1)

  PRE1 specifies an alternative set of prefix digits to be added to the destination number if the call would need to be alternatively routed. This information is conveyed to the satellites for alternative routing.

- Digits to truncate 1 (TRC1)

TRC1 specifies an alternative number of digits to be truncated from the destination number if the call would need to be alternatively routed. This information is conveyed to the satellites for alternative routing.

- Routing server option (OPT) OPT specifies how the server should treat the data which it has stored with regard to the routine integrity check of the programmed data. It is not conveyed to the satellites.

  It can take one of three values:

  3 – This means that the data is valid and should be checked for integrity. If the integrity check fails, then the data will be marked as faulty and an alarm will be sent to the alarm log indicating which destination number and IP address is faulty.

  5 – This means that the data when initiated is potentially valid, but when the integrity check is made it will not be marked faulty nor will any alarm will be given if the check fails. However, the first integrity check is successful the server will change the option value to a 3. This value shall be used when upgrading a network with the routing server functionality: a node may be programmed with this value in the server, prior to upgrading. When the upgrading is completed the server will now treat t his node as a normal satellite node, that is, as for option 3.

  6 – This means that the data will never be checked for integrity. This is used for nodes in the network which will never support the routing server functionality and thus will never respond to an integrity check. that is, 3rd party switches.

- IP address 1 (IP1)

  IP1 specifies the primary IP address to reach the destination node. This information is conveyed to the satellites IP routing.

- IP address 2 (IP2)

  IP2 specifies an optional secondary IP address to reach the destination node. This information is conveyed to the satellites IP routing, 2.2.5 Load Balancing function in the Satellite on page 9.

- Remote route identity (RROUID)

  RROUID specifies the remote route identity of the destination node (and it is optional depending on whether the destination node has one specified). This information is conveyed to the satellites IP routing.

- Remote destination number (RDEST)

  RDEST specifies the destination number (the own exchange number) of the destination node. It is used by the integrity check routine (and is often the same as the destination number). This information is not conveyed to the satellites. (This is not applicable to OPT=6)

2.1.2 DISTRIBUTION OF DATA TO SATELLITES

When a satellite has no locally stored (temporary) IP routing information a virtual call request will be received by the server with the destination number for which data is required. The server will look up the data in its PNR table and attempt to locate the entry. This will return one of three possible results.

- An exact match is found. In this case the server will return the result together with all the data which it has stored for that entry.
- No match is found. In this case the server will return a negative result and the satellite will have to attempt to route the call locally.

- A partial match is found meaning that not enough digits have been received to be able to return any routing data, but potential data is available when, and if, more digits are received, 2.2.4 PNR Table Splitting in the Satellite on page 9 .

2.1.3 ROUTING OF CALLS ORIGINATING IN THE SERVER

When extensions within the server make calls to destinations in the network, the called number will be passed to PNR for routing (as for the normal PNR function). If an entry is found for which IP routing information exists then this will be used to route the call in the IP network together with the stored alternative routing information.

2.1.4 INTEGRITY (ROUTINE) CHECK

The server performs a time based routine check which will verify the integrity of the stored IP routing information (based on the option (OPT) value for that destination entry).

The routine check is started automatically after a reload or restart of the system or PNR program unit. The routine check may also be subsequently inhibited and enabled by command.

The routine check will set up a virtual call to each destination entry in the PNR table with a 5 second interval. The server will use the primary IP address (and remote route identity if specified) to establish the call. If a positive acknowledgment to the call setup is received the call will be released and the secondary IP address will be used to establish a call to the same destination in the same manner. The next destination entry will then be checked after a 5 s interval.

When option 3 is specified for a an entry and no positive acknowledgment is received for either of the IP addresses, then a second check will be made after 5 seconds. If no positive acknowledgment is received on the second check then the IP address will be fault marked and an alarm sent to the alarm log indicating which IP address is faulty and to which destination. The routine check will then continue to the next entry in the table. The routine check is cyclic and therefore the fault marked IP address w ill continue to be checked. If the check is subsequently successful, the fault marking will be removed and the alarm will be acknowledged.

While the IP address information is marked as faulty it will not be conveyed to the satellites. Only non fault marked IP addresses will be returned together with any alternative routing information.

2.2 SATELLITE (CLIENT) FUNCTIONS

2.2.1 SATELLITE DATA

The IP routing data in the satellite is programmed in the PNR table. The data programmed in the satellite in the PNR (TAB) table consist of:

- Destination number (ENTRY)

  ENTRY specifies the destination number to the node to be analyzed. However, it is not necessary to program complete destination numbers, 2.2.4 PNR Table Splitting in the Satellite on page 9 .

- Fictitious routing table (FRCT)

FRCT specifies which fictitious routing choice table (RCT) entry that shall be used to reach the destination. This is used in the satellite for routing of calls using the IP routing information received from the server. All entries in the table may use the same FRCT value since they will use the same outgoing IP route to reach the entire network. It should be noted that only **one** IP route needs to be programmed in the satellite. All calls and Routing Server functions will use this single route.

- Routing server option (OPT)

  OPT specifies how the satellite should handle the temporary data which it has received from the server.

  It can take one of three values:

  1 – The satellite PNR table contains IP data which can be used to route the call over the IP network.

  2 – This means that the data needs to be fetched from the server in order to be able to route the call. Whether or not it needs to be fetched for a particular call depends on whether temporary routing in formation has already been received and stored. It has also a special function; if the length of the destination number is shorter than that of the destination number stored in the server then it will invoke the PNR table splitting function.

  4 – This is the same as option 2 but the PNR splitting function will never be invoked. Therefore if the length of the destination number is shorter than that of the destination number in the server, then no temporary routing data will be stored and it will need to be fetched for every call.

- Remote destination number (RDEST)

  RDEST specifies the destination number (the own exchange number) of the server node. It is used for requesting the IP routing and alternative routing information from the server. It is also used for the updating check routine towards the server.

The IP routing data in the satellite which is not required to be programmed in the PNR table is that which is received from the server.

The data received from the server and stored in the satellite PNR table (TAB=PNR) consists of:

- Digits to prefix (PRE)

  PRE specifies prefix digits to be added to the destination number should the call need to be alternatively routed.

- Digits to truncate (TRC)

  TRC specifies the number of digits to be truncated from the destination number should the call need to be alternatively routed.

- Digits to prefix 1 (PRE1)

  PRE1 specifies an alternative set of prefix digits to be added to the destination number should the call need to be alternatively routed.

- Digits to truncate 1 (TRC1)

  TRC1 specifies an alternative number of digits to be truncated from the destination number should the call need to be alternatively routed.

- IP address 1 (IP1)

  IP1 is the primary IP address to reach the destination node.

- IP address 2 (IP2) – see load balancing function

  IP2 is a secondary IP address to reach the destination node.

- Remote route identity (RROUID)

  RROUID is the remote route identity of the destination node.

2.2.2 FETCHING OF IP ROUTING AND ALTERNATIVE ROUTING INFORMATION FROM THE SERVER

Whenever a call is made from a satellite to a destination for which no temporary information has already been stored the routing information must first be fetched from the server.

In order to do this, a destination number must have been programmed to reach the server. This destination is that which is specified in RDEST (described above) and uses the existing route destination initiation command RODDI. In this command the optional parameter IP (and if required RROUID) must be given, in order to define the IP address of the terminating route in the server. This is the **only** IP address which needs to be specified in any of the satellites. This destination number will use the same local IP route as for all other calls to the network.

When the dialled number is passed to PNR for analysis, a search is made in the PNR table to find the entry. When the entry is found, a virtual call is established to the server using the RDEST number to set up the call. The call contains a request to return the IP routing and alternative routing information for the destination number contained in the request message.

The server will respond with one of three possible results.

- An exact match is found. In this case the server will return the result together with all the data which it has stored for that entry.
- No match is found. In this case the server will return a negative result and the satellite will attempt to route the call locally.
- A partial match is found meaning that not enough digits have been received to be able to return any routing data, but potential data is available when, and if, more digits are received.

If an exact match has been found the satellite will store all the received data in PNR against that destination as temporary data and then proceed to establish the call using the received data.

If no match is found then the destination number will be passed to the normal routing handling routines to try to route the call.

If a partial match is found the system will wait for another digit to be received before making a new request to the server. This procedure will continue until one of the above two results are received. Depending on the option value of the destination entry, this may invoke the PNR table splitting function.

As described above, the mechanism to fetch the information from the server uses the existing routing functions of the RODDI command. Therefore it is possible to use the alternative routing function to be able to retrieve the information from alternative servers. Up to eight servers may be specified.

2.2.3 ROUTING OF CALLS IN THE SATELLITE

By using the temporary information stored in the PNR table for a destination, the satellite will attempt to route the call. The first attempt (and second if two IP addresses are

available) will use the IP information to route the call, if this attempt fails then the alternative routing procedures will be invoked. For alternative routing it is necessary to specify one or more alternative routes for the fictitious route from PNR, using the route destination initiate command RODDI. This can be used to specify an alternative route (for example, to the PSTN) in which the alternative routing information received from the server (PRE, TRC, PRE1, TRC1) will be used to reform the destination number into one which can be used by the alternative route to route the call (for example, from a private number to a public DID number).

If the satellite fails to route the call using the temporary IP information received it will automatically erase that temporary data from the PNR table. The next call will therefore have to make a new request to the server for the data.

2.2.4 PNR TABLE SPLITTING IN THE SATELLITE

The Routing Server satellite has a special function which is useful when establishing a large network. Usually it is necessary to specify in all nodes the precise destination number of all other nodes in the network. Utilizing option 2 in the OPT parameter makes this unnecessary.

In the server, the destination numbers are precisely defined, as normal, together with the (new) IP routing and alternative routing information. In the satellites it is only required to specify a minimum of one digit which is defined an external destination number in number analysis.

As briefly described above, if the server returns a result with *partial match* then the satellite will initiate the PNR table split function. This will result in the destination entry in the PNR table being expanded by one digit. Subsequent calls will continue to expand the table by one digit until the server returns a result that an *exact match* is found. When this PNR split function has occurred an alarm is sent to the alarm log to notify the administrator that this has occurred. Since this will have changed reload data in the system the administrator should perform a system dump to preserve the data change.

2.2.5 LOAD BALANCING FUNCTION IN THE SATELLITE

In the server there is the possibility to specify two IP addresses for each destination in the PNR table. The second IP address is optional, but may be used to provide an alternative IP address which can be used to reach the destination in the case where there is a second IP trunk board in the destination node.

This serves two purposes:

- When the satellite receives two IP addresses from the server when attempting to establish a call, if the call attempt fails with the first IP address then a second attempt will be made using the second IP address. If both call attempts fail then the temporary information which has been stored will be erased.
- When a the satellite has received and stored two IP addresses it will use them on alternative calls to that destination in order to balance the load in the destination node. (Note that this has no connection to the Load Sharing function of the IP trunk in the MX-ONE).

2.2.6 UPDATING (ROUTINE) CHECK

Each satellite contains a time based updating check, which will request the IP routing and alternative routing information from the server. For destinations which do not have any temporary information stored in the satellite, this check will run every 10 hours with each destination being checked with a 5 s interval. For destinations which have infor-

mation stored, the check will only be made every 20 hours. Any existing stored information will be overwritten with the latest information received from the server.

The routine check is started automatically after a reload or restart of the system or PNR program unit. The routine check may also be subsequently inhibited and enabled by command. Enabling the check will initiate an immediate check.

2.2.7 ERASURE OF TEMPORARY STORED DATA IN THE SATELLITE

It is possible, to erase the temporary stored data for all destinations by command. When this command is given all temporary data which has been stored is erased and an update check is immediately started to retrieve the information from the server. This feature may be useful when many changes have been made in the server.

3 SCHEMATIC IMPLEMENTATION IN A NETWORK

Below you can see a schematic figure of the implementation in a network.

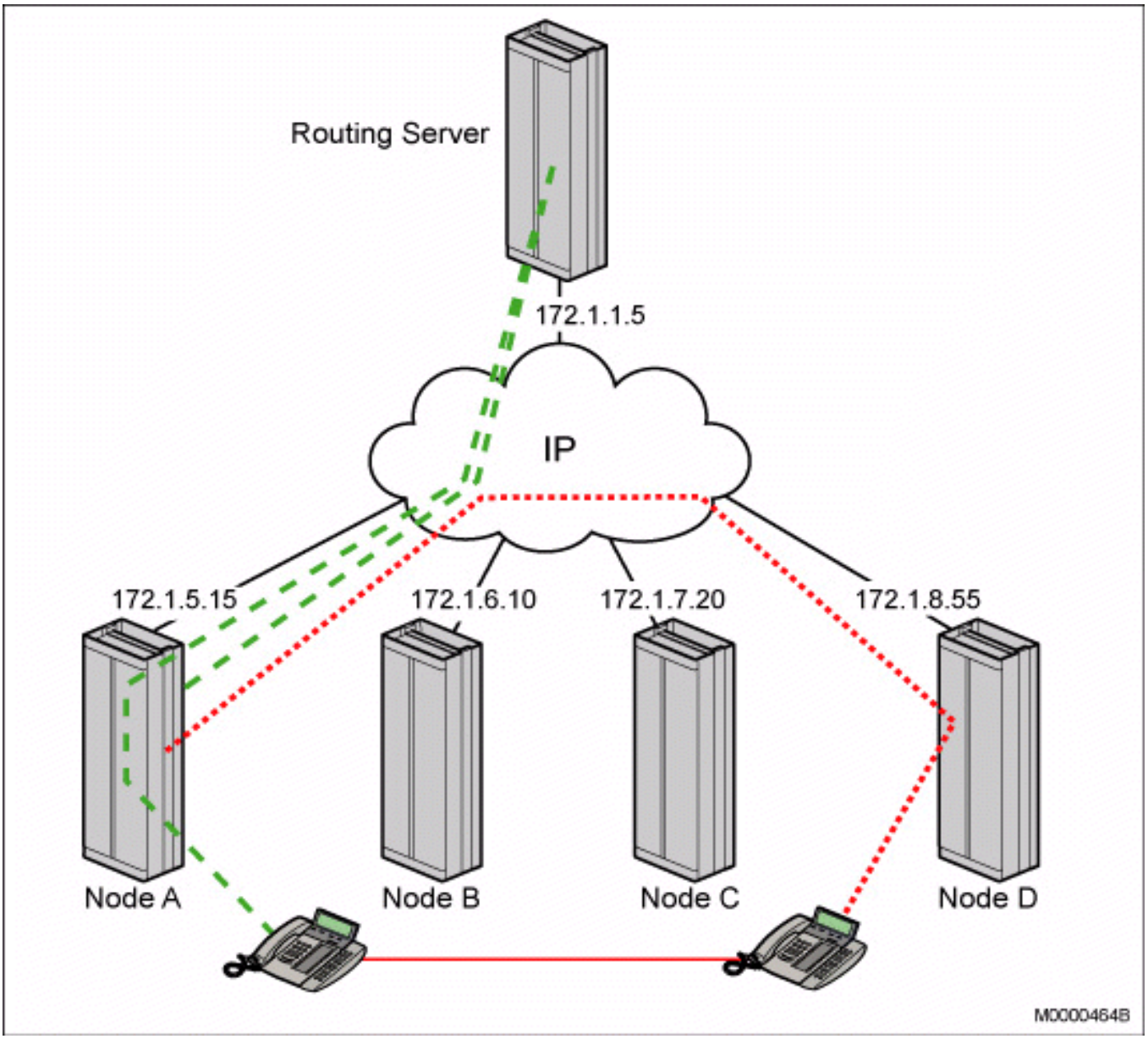

Figure 1: Schematic implementation of a Routing Server in a network.

4 BENEFITS AND ADVANTAGES OF THE ROUTING SERVER

Traditional TDM based networks have always been built with a hierarchical structure. The primary reason for building in this fashion was the cost for long distance leased lines, traffic to and from exchanges in a region or country to another region or country needed to be concentrated via transit exchanges.

A secondary effect was the ease of administration as only the transit exchanges needed information about other exchanges in the network.

With IP-networking, once an exchange is connected to the wide area IP-infrastructure, all exchanges can be reached directly which improves call set up times and avoids the use of resources in other exchanges (transits). Unfortunately, to utilize these benefits of IP networking, all exchanges in the complete network needs access to information about all other exchanges. A rough calculation of the management effort for a real customer case landed at some 1 million command line entries (MML commands) for the whole network. This is simply an impossible task.

The purpose of the Routing Server is to allow the configuration of an optimal network solution which utilizes the advantages of IP-networking.

With the Routing Server application, only one exchange in the network needs to be programmed with all data (or a few, if loadsharing and redundancy is required).

For the customer case mentioned above, the Routing Server needed roughly 4000 command line entries.

An additional benefit with the Routing Server application, compared with our competitors centralized gatekeeper solutions, is the fact that all routing data is automatically downloaded to each exchange in the network, thus providing full autonomy with possibility to reroute failed calls over alternate networks, for example, a PSTN, in situations where an exchange is isolated due to failed access to the IP network.