

# Telindus Dynamic Routing Engine (TDRE)

<b>FEATURES AND BENEFITS .....</b>	<b>2</b>
<b>INTRODUCTION .....</b>	<b>2</b>
<b>PRODUCT LINES SUPPORTED BY TDRE.....</b>	<b>2</b>
<b>FEATURES.....</b>	<b>2</b>
PPP ENCAPSULATION .....	2
FRAME-RELAY ENCAPSULATION .....	2
ATM ENCAPSULATION .....	3
INTERFACE DEFINITION .....	3
IP ADDRESS ASSIGNMENT .....	3
IP ROUTING .....	4
<i>Standard static routing:</i> .....	4
<i>Policy based static routing:</i> .....	4
<i>RIP1 (RFC 1058)</i> .....	5
<i>RIP2 (RFC 2453)</i> .....	5
<i>OSPF (RFC2328) *</i> .....	5
<i>Support for ICMP</i> .....	5
BRIDGING AND VLAN SUPPORT .....	5
MULTICASTING AND BROADCASTING .....	7
NETWORK ADDRESS TRANSLATION (NAT AND PAT) .....	7
TUNNELING AND VPN SUPPORT.....	7
FIREWALL FUNCTIONALITY AND ACCESS LISTS .....	7
QUALITY OF SERVICE (QOS) .....	8
ACCESS SECURITY .....	11
MAINTENANCE AND MANAGEMENT TOOLS .....	11

## Features and Benefits

- Uniform feature set for Telindus IP product range
- Uniform set of maintenance and management tools
- All features are standard included
- Including VPN and QoS functionality
- Free upgrades

## Introduction

Available on an extensive range of Telindus platforms, the Telindus Dynamic Routing Engine (TDRE) software is a feature-rich operating system that provides a common IP fabric, functionality and maintenance interface across your network. The TDRE guarantees a common feature set across the different product lines and a uniform support by maintenance and management tools. Telindus operates a policy of free upgrades and includes all functionality in a standard package.

## Product lines supported by TDRE

Following products are based on the TDRE:

- 103x Desktop Access Router series
- 106x Desktop Access Router series
- 122x ADSL Router series
- 142x SHDSL Router series
- 1431 SHDSL CPE series
- 24xx Access concentrator series
- Crocus Router 10M modular interface

## Features

### ***PPP encapsulation***

- Encapsulation compliant with RFC 1661, 1662
- LCP (Link Control Protocol)
- IPCP (IP Control Protocol, RFC 1332)
- BCP (Bridge Control Protocol, RFC 2878)
- CCP (Compression Control Protocol, RFC 1962) with support for the Predictor compression algorithm (RFC 1978)
- Support of CHAP authentication with MD5 hashing (RFC 1994), unidirectional or bi-directional authentication
- Support of PAP (PPP Authentication Protocols, RFC 1334), unidirectional or bi-directional authentication
- Support of MS-CHAP en MS-CHAP v2 Authentication
- Support for multi-link PPP (RFC 1990)
- Support for PPP fragmentation (RFC 1990)

### ***Frame-Relay encapsulation***

- Encapsulation compliant with RFC 1490, 2427

- The equipment supports multiple DLCI's (PVC) on each WAN interface. The number of DLCIs per WAN interface is only limited by the amount of available memory. As (for example on a channelised E1 interface) the number of WAN ports on a router may be quite high, the total number of DLCIs in the router may become quite important.
- CIR (Committed Information Rate) configurable per DLCI
- EIR (Excess Information Rate) configurable per DLCI
- Support of Inverse ARP over Frame-Relay for automatic gateway configuration
- Support of different types of LMI (Local Management Interface):
  - revision 1 LMI
  - ANSI T1.617 D
  - ITU-T Q933 Annex A
  - FRF 1.2
- Support for Frame-relay fragmentation (FRF 12)
- Support for Multi-link Frame-Relay (FRF 16.1)

### **ATM encapsulation**

- Supported higher layer protocols:
  - Classical IP according to RFC 1577
  - Ethernet or IP according to RFC 2684
  - PPPoA (PPP over ATM) according to RFC 2364
  - PPPoE (PPP over Ethernet) according to RFC 2516, 2684
- Multiprotocol encapsulation using
  - LLC (Logical Link Control)
  - VC (Virtual Connection) multiplexing
- Support of Reverse ARP for automatic IP address resolution
- Configuration of PCR (Peak Cell Rate) per PVC
- ATM cell format ITU-T I.361
- ATM forum UNI 3.1/4.0 PVCs
- ATM forum ILMI 3.1/4.0
- OAM F4 loop back support (ITU-T I.610)
- OAM F5 loop back support (ITU-T I.610)

### **Interface definition**

The definition of an "interface" on equipment entirely depends on the configuration of the unit and can correspond to the following:

- A physical interface, e.g. an Ethernet interface, a serial interface,...
- A Frame-Relay DLCI
- An ATM PVC
- An L2TP Tunnel
- A VLAN

Logical interfaces behave similarly as physical interfaces, except that they don't send interface alarms.

### **IP Address assignment**

- BOOTP/DHCP server (RFC 2131, RFC 2132)
  - Static or dynamic address assignment
- DHCP relay agent (RFC 2131, RFC 2132)

- Static IP address assignment
- Automatic IP assignment through BootP client (RFC 951)
- Automatic IP assignment through DHCP client (RFC 2131, RFC 2132)
- Automatic IP assignment through IPCP
- Possible assignment of secondary IP address on LAN interface
- Automatic IP gateway assignment through Inverse ARP (RFC 2390, supported on Frame-Relay, PPP, ATM or L2TP)
- Numbered or unnumbered mode

## **IP routing**

The equipment complies to the router requirements as stated in RFC 1812 and supports the routing of standard IP packets (RFC 791) between the different interfaces on the equipment according to following routing protocols:

### **Standard static routing:**

Routing is done through static routing entries in the routing table. Alternate routing is possible through the use of different preferences for different routes to the same destination.

### **Policy based static routing:**

Normal routing is based on the destination IP address. Policy based routing offers the possibility to define different routing entries based on additional information. Traffic is routed to a certain interface or gateway based on following parameters:

sourceIpStartAddress sourceIpEndAddress	These elements set the range for the IP source address as specified in the IP header. Packets that fall within the specified range and fulfil the other conditions are using this route
destinationIpStartAddress destinationIpEndAddress	These elements set the range for the IP destination address as specified in the IP header. Packets that fall within the specified range and fulfil the other conditions are using this route
TosStartValue TosEndValue	These elements set the range for the Type Of Service field value. Packets that fall within the specified range are forwarded
IpProtocol	Use this element to set the protocol field from the IP header. Packets that have the specified protocol field are forwarded You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
SourcePortStart sourcePortEnd	These elements set the range for the source port as specified in the UDP / TCP headers. Packets that fall within the specified range and fulfil the other conditions are using this route You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514),

	router (520), socks (1080), l2tp (1701), telindus (1728).
DestinationPortStart destinationPortEnd	These elements set the range for the destination port as specified in the UDP / TCP headers. Packets that fall within the specified range and fulfil the other conditions are using this route You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.

### **RIP1 (RFC 1058)**

- Support of SplitHorizon and selective router updates per interface
- Support for broadcasting of selective RIP updates limited to information on specific network subnets

### **RIP2 (RFC 2453)**

- Support of SplitHorizon and selective router updates per interface
- Support for broadcasting of selective RIP updates limited to information on specific on specific network subnets
- Support for authentication with MD5 hashing or clear text

### **OSPF (RFC2328) \***

#### **Support for ICMP**

to inform the originator of the packets about possible shorter routes

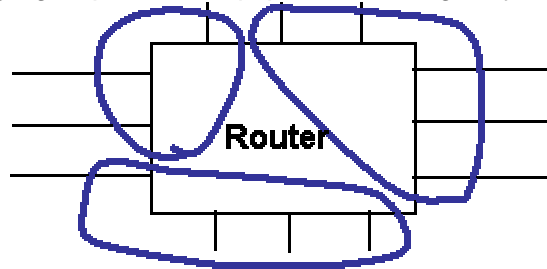
- "TTL exceeded" messages
- "destination unreachable: port unreachable" messages
- "destination unreachable: communication with destination is administratively prohibited" messages

## **Bridging and VLAN support**

The equipment supports Bridging with support of the spanning tree protocol (IEEE 802.1D). The spanning tree protocol allows having multiple paths between two sites, building redundancy in the connection. Bridging may be enabled or disabled for each of the available ports on the router and may be combined with IP routing on the same interface. The bridging foresees also the blocking of certain MAC-addresses on outgoing traffic based on a bridge access list. There is no hard-coded limitation on the number of MAC addresses that can be stored in the unit. A minimum of 10.000 MAC addresses is guaranteed on all products. It is possible to disable the self-learning functionality of the bridge and operate it as a repeater.

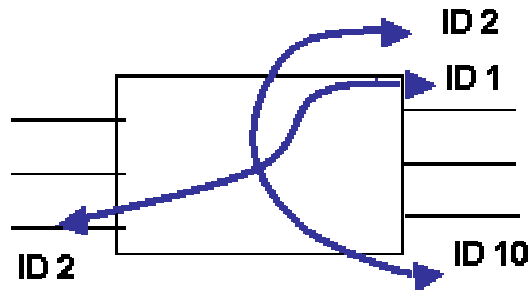
The equipment offers the possibility to create multiple bridge groups. A bridge group is a collection of interfaces that are connected through bridging. In case a bridge-group is connected to a virtual Ethernet VLAN interface, it is possible to forward or strip-off the VLAN ID before sending the Ethernet packets to the other interfaces of the bridge group. Within a bridge group, the equipment can monitor a predefined VLAN for management purposes. As described in the section on QoS (Quality of Service), the equipment can also take into account the 802.1P tag for setting the priority when forwarding the packet.

Between different bridge-groups in the equipment, routing may be enabled.



*multiple bridge groups in a multiport device*

A bridge-group can also be configured as a "VLAN switch" In this case, a mapping is done between a VLAN ID on one interface and a VLAN ID on another interface. For this purpose, a VLAN switching table is used. This table can also be used for "tagging" or "untagging" VLAN tags and for changing the priority tags.



*acting as a "VLAN switch"*

### ***Multicasting and broadcasting***

The Telindus equipment supports the handling of broadcasts and multicasts and includes following related functionalities:

- Support for IGMPV2 (Internet Group Management protocol, RFC 2236), as the standard for IP multicasting.
- Enabling or disabling the forwarding of directed broadcasts on a certain interface
- Setting of helper address for broadcasts, in order to replace the general broadcast address by the address of specific host(s) in the network.

### ***Network address translation (NAT and PAT)***

**NAT** allows the use of private IP addresses on the local Ethernet, while still having access via the WAN interface to the Internet (official IP addresses). Each Ethernet IP address that needs Internet access is translated into an official IP address before sending traffic on the WAN interface. The number of simultaneous users with Internet access is limited to the number of official IP addresses. This may be a static or a dynamic (automatic) process.

**PAT** (RFC 3022) uses only one single official IP address on the WAN network. The Telindus 1032 Router translates all private IP addresses on the local Ethernet to the single official IP address. The PAT implementation also supports incoming traffic from the public network through the use of a service-mapping table.

You can combine both translation methods (NAT and PAT) and tune them to specific needs.

### ***Tunneling and VPN support***

#### **L2TP tunnelling (Layer 2 Tunnelling Protocol RFC 2661)**

This protocol is used to emulate a point-to-point connection over IP, which can be used to set-up a PPP session between the two access routers. The implementation includes the possibility to configure tunnel authentication prior to the setup of L2TP.

- Supported on WAN and LAN interfaces
- Each equipment can be configured as a LAC (L2TP Access Concentrator) or as a LNS (L2TP Network Server)

#### **IPSec security (RFCs 2401-2411)**

- Support of L2TP transport mode (RFC 3193)
- Support of ESP (Encapsulation Security Payload), allowing authentication of the sender and encryption of the data
- Support of DES or 3DES encryption (56 bit or 3x 56bit)
- Support for HMAC (Keyed-Hashing for Message Authentication) based on MD5 or SHA-1 for integrity and authentication.
- Support of Manual SA (Security Association)

Note: On the standard equipment, encryption in IPSEC is handled by the software. As this is a processor-consuming task, the forwarding performance of the equipment decreases. Therefore, some equipment is also available in a version with a 3DES encryption chip. This chip takes care of the DES and 3DES encryption / decryption, unburdening the software of this task.

### ***Firewall functionality and access lists***

The equipment allows the filtering of traffic on outgoing traffic on LAN or WAN interfaces based on extended access lists. These lists allow the filtering of the traffic based on following parameters:

sourceIpStartAddress sourceIpEndAddress	These elements set the range for the IP source address as specified in the IP header. Packets that fall within the specified range are forwarded
destinationIpStartAddress destinationIpEndAddress	These elements set the range for the IP destination address as specified in the IP header. Packets that fall within the specified range are forwarded
TosStartValue TosEndtValue	These elements set the range for the Type Of Service field value. Packets that fall within the specified range are forwarded
IpProtocol	Use this element to set the protocol field from the IP header. Packets that have the specified protocol field are forwarded You can specify the protocol by typing the rotocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
SourcePortStart sourcePortEnd	These elements set the range for the source port as specified in the UDP / TCP headers. Packets that fall within the specified range are forwarded You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
DestinationPortStart destinationPortEnd	These elements set the range for the destination port as specified in the UDP / TCP headers. Packets that fall within the specified range are forwarded You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.

An additional access list can be activated for the traffic towards to the protocol stack used for the network management and remote control of the router. In this case, incoming traffic can be blocked based on the address-range of the IP source.

### **Quality of Service (QoS)**

The QoS mechanism is implemented based on different forwarding queues. The Telindus routers implement for every interface on the equipment a total of 7 different queues, of which 6 are actually used by user data.

The implementation of the queues is as follows:

Queue	Queue type	Description
1 - 5	configurable queue	The user can decide which data goes into which queue.
6	low delay queue	This queue is always addressed between every user configurable queue and should be used by delay sensitive traffic.
7	system queue	This queue is filled with link monitoring messages etc. and has priority over all other queues.

The way that the *configurable queues* are transmitting data can be selected according to different algorithms. Following algorithms are implemented:

- Fifo (first in first out)
- Round Robin (each configurable queue has equal weight)
- Absolute Priority
- Weighted Fair Queuing
- Low delay Weighted Fair Queuing

The distribution of the traffic between the different queues can occur according to following QoS Traffic Policies:

The QoS Traffic Policy defines the ways in which the router will distribute the traffic over the different forwarding queues in the equipment. A total of 6 queues is available for user data.

Following policies for distributing the traffic over the queues are defined:

#### **A: Trafficshaping**

Based on a table, a complete customised policy may be set. The elements that define how the traffic is forwarded to a certain priority queue are the following:

sourceIpStartAddress sourceIpEndAddress	These elements set the range for the IP source address as specified in the IP header. Packets that fall within the specified range are forwarded and queued if applicable.
destinationIpStartAddress destinationIpEndAddress	These elements set the range for the IP destination address as specified in the IP header. Packets that fall within the specified range are forwarded and queued if applicable.
TosStartValue TosEndtValue	These elements set the range for the Type Of Service field value. Packets that fall within the specified range are forwarded and queued if applicable.
IpProtocol	Use this element to set the protocol field from the IP header. Packets that have the specified protocol field are forwarded and queued if applicable. You can specify the protocol by typing the rotocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
SourcePortStart	These elements set the range for the source port as

sourcePortEnd	specified in the UDP / TCP headers. Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
DestinationPortStart destinationPortEnd	These elements set the range for the destination port as specified in the UDP / TCP headers. Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
newTosValue	Use this element to set the new TOS field value. When you select a new TOS field value, then a packet that matches an entry in the trafficShaping table its TOS field value is changed. Selecting unchanged, leaves the TOS field value as it is.
priority	Use this element to set the destination queue for a packet matching an entry in the trafficShaping table. In case an overload condition occurs, then a packet that matches an entry in the trafficShaping table is sent to the specified queue. The priority element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

### B: TosDiffServ

The data is redirected to the queues based on *DiffServ* (refer to RFC2597) regarding class and drop precedence. This means that, depending on their Type Of Service (TOS) field, some packets are moved to other queues and/or dropped sooner than other packets in case the queue is full.

The highest 3 bits of the TOS field are mapped as follows:

Bit values	correspond with
000 up to 100	queues 1 up to 5, respectively
101 and higher	the low delay queue

The next 2 bits define the drop precedence:

Bit values	correspond with
00 and 01	maxLength1
10	MaxLength2
11	MaxLength3

---

Where `mawlength1`, `Maxlength2`, `Maxklength3` correspond to the number of data packets that may be present in a queue before a packet is dropped. These values may be different for each of the queues.

**C: TosMapped**

This simple and flexible policy allows to queue the traffic based on a user defined range of the TOS field.

In case of **VLAN tagged Ethernet traffic**, the 802.1P tag can be used to map the traffic to any of the priority queues described above.

## **Access Security**

The equipment is password protected for access through the different maintenance and management tools. For each router one can define an unlimited number of users, where each user can be given a customised access-right to the equipment. The access-right is based on a combination of following elements:

- Read-access: read all parameters except security parameters
- Write-access: write all parameters except security parameters
- Security-access: read and change security parameters
- Filesystem-access: access to the file system (for advanced users)

The unit also features a Radius client functionality (RFC 2865), that can be used for authentication Authorisation and Accounting (AAA) of network maintenance sessions, or for PPP sessions initiated by remote end-users.

## **Maintenance and Management tools**

The equipment is supported by a wide set of local and remote maintenance and management tools. These tools include:

- TMA (Telindus Maintenance Application): A free graphical maintenance application delivered with the equipment. It can be used to access the device through a local serial connection or through an IP connection (UDP socket 1728).
- TMA CLI stand-alone command line console software
- TMA for HP OV management integration in HP Openview
- TMA elementview stand-alone element management
- Local console: a standard VT100 connection with command line interface or interactive menu-driven interface
- TELNET with command line interface or interactive menu-driven interface (RFC 854)
- HTTP web interface with interactive menu-driven interface (RFC 2616)
- PING (RFC 792)
- TFTP configuration and software download (RFC 1350)
- FTP configuration and software download (RFC 414)
- TML: Telindus Memory Loader for the donload of configuration or software through the serial console port.
- SNMP (RFC 1157)
- SNMP MIB2 (RFC 1213), private MIB
- SNMP traps (RFC 1215)
- SYSLOG event logging generation (RFC 3164)
- Simple Network Time Protocol (SNTP) (RFC 2030)
- IP loop back address

\* Under development. Please check availability.