



Total Dynamic Routing Engine (TDRE)

Functional Description

Version 12.1.1 - March 2008

Table of Contents

Features and Benefits	3
Introduction	3
TDRE products	3
Features	3
<i>PPP encapsulation</i>	<i>3</i>
<i>Frame Relay encapsulation</i>	<i>4</i>
<i>ATM encapsulation</i>	<i>4</i>
<i>EFM encapsulation</i>	<i>5</i>
<i>Other WAN encapsulations</i>	<i>5</i>
<i>Interface characteristics</i>	<i>5</i>
<i>Dial-up interfaces</i>	<i>5</i>
<i>IP Address assignment and auto-provisioning</i>	<i>6</i>
<i>IP routing</i>	<i>6</i>
<i>IP filtering and firewall</i>	<i>8</i>
<i>Bridging and VLANs</i>	<i>9</i>
<i>Network address translation (NAT and PAT)</i>	<i>10</i>
<i>IP VPNs</i>	<i>10</i>
<i>Quality of Service (QoS)</i>	<i>12</i>
<i>Security</i>	<i>14</i>
<i>Maintenance and Management tools</i>	<i>15</i>
Features history	16
<i>New features in TDRE 11.0</i>	<i>16</i>
<i>New features in TDRE 11.1</i>	<i>17</i>
<i>New features in TDRE 11.2</i>	<i>18</i>
<i>New features in TDRE 11.3</i>	<i>18</i>
<i>New features in TDRE 11.4</i>	<i>19</i>
<i>New features in TDRE 11.5</i>	<i>20</i>
<i>New features in TDRE 12.0</i>	<i>20</i>
<i>New features in TDRE 12.1</i>	<i>22</i>
Product specific issues	25
<i>TDRE versions per product</i>	<i>25</i>
<i>WAN encapsulations</i>	<i>26</i>
<i>Other features</i>	<i>27</i>

Features and Benefits

- Uniform feature set for routers product range
- Uniform set of maintenance and management tools
- All features are standard included
- Including VPN and QoS functionality for layer 2 and layer 3 IP
- Free upgrades

Introduction

Available on a complete range of routing devices, the Total Dynamic Routing Engine (TDRE) software is a feature-rich operating system that provides a common IP and layer 2 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. OneAccess operates a policy of free upgrades and includes all functionality in a standard package.

This document describes all features in the TDRE 12.1 release. At the end of this document, one may find the list of new features per TDRE release. As some features are hardware dependent, at the end of this document one may find also a table with the hardware dependent feature set.

TDRE products

The following products are based on the TDRE:

- 1020 Router series
- 1030 Router series
- 1040 Router series
- 1061 Router
- 1221 ADSL Router
- 1421 SHDSL Router
- 1422 SHDSL Router
- 1423 SHDSL Router
- 1424 SHDSL Router
- 1431 SHDSL CPE
- 1432 SHDSL CPE
- 2400 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) , including Cisco's subnetmask extension
- BCP (Bridge Control Protocol, RFC 2878) including VLAN support
- CCP (Compression Control Protocol, RFC 1962) with support for the Predictor compression algorithm (RFC 1978)
- CHAP authentication with MD5 hashing (RFC 1994), unidirectional or bi-directional authentication
- MS-CHAP1 (RFC 2433) and MS-CHAP2 (RFC 2759) CHAP authentication protocol extensions
- PAP (PPP Authentication Protocols, RFC 1334), unidirectional or bi-directional authentication
- Multilink PPP (RFC 1990)(MLPPP) on devices with more than one interface of the same type
- The MLPPP bundle name or the MAC address can be exchanged
- Fragment interleaving with MLPPP
- PPP fragmentation (RFC 1990): enable to fixed size 200 bytes or disable
- Multi-class PPP (RFC 2686)
- Bandwidth Allocation Protocol (BAP) (RFC 2125) for ISDN interfaces

Frame Relay encapsulation

- Encapsulation compliant with RFCs 1490, 2427
- The equipment supports up to 200 DLCIs on a device
- CIR (Committed Information Rate) configurable per DLCI
- EIR (Excess Information Rate) configurable per DLCI
- Inverse ARP over Frame-Relay for automatic gateway configuration
- Different types of LMI (Local Management Interface):
 - revision 1 LMI
 - ANSI T1.617 D
 - ITU-T Q933 Annex A
 - FRF 1.2
- Frame-relay fragmentation (FRF 12)
- Multi-link Frame-Relay (FRF 16.1)(MLFR)
- Fragment interleaving with Frame Relay and MLFR

ATM encapsulation

- Higher layer protocols:
 - Classical IP according to RFC 2225 (formerly RFC 1577)
 - Ethernet or IP according to RFC 2684 (formerly RFC 1483)
 - PPPoA (PPP over ATM) according to RFC 2364
 - PPPoE (PPP over Ethernet) according to RFC 2516, 2684
 - auto PPP (in routing mode): an automatic selection is made between PPPoA and PPPoE
- Multiprotocol encapsulation using
 - LLC (Logical Link Control)
 - VC (Virtual Connection) multiplexing
- Reverse ARP for automatic IP address resolution
- Configuration of PCR (Peak Cell Rate) per PVC
- Service categories UBR, CBR, VBR-rt and VBR-nrt. The availability of CBR, VBR-rt and VBR-nrt service categories is hardware dependent.

- ATM cell format ITU-T I.311, I.321, I.361, I.432
- ATM forum UNI 3.1/4.0 PVCs
- ATM forum ILMI 3.1/4.0
- OAM F4 / F5 loop back response (ITU-T I.610)
- OAM F4 / F5 end-to-end loop back generation (ITU-T I.610)
- OAM F5 end-to-end RDI response
- OAM F4 /F5 segment and end-to-end CC (Continuity Check) (1431 only)
- OAM F4/F5 segment and end-to-end PM (Performance Monitoring)
- ATM IMA over E1 links (ATM Forum af -phy-0086.001 and ITU-T G.761) (on TIM 6E1 interface)

EFM encapsulation

- Compliance with IEEE 802.3 chapters 61 and 63 for SHDSL (2BASE -TL)
- Bonding in compliance with 802.3 chapter 61 (PAF) and ITU -T G.998.2
- OAM in compliance with 802.3 chapter 57 (802.3ah)

Other WAN encapsulations

- HDLC encapsulation in bridging mode (not interoperable with Cisco HDLC encapsulation)
- Error test encapsulation for end-to-end error tests over TDM networks between OneAccess devices.

Interface characteristics

The definition of an “interface” 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. One can define up to 255 interfaces on a device.

Physical interface characteristics include:

- Configurable output queue length
- Configurable MRU (Maximum Receive Unit) on HDLC, PPP and Frame Relay interfaces up to a maximum value of 1650 bytes
- Fixed MRU of 2048 bytes on Ethernet interfaces

Dial-up interfaces

- Applicable to ISDN-BRI, ISDN-PRI, PSTN and AUX interfaces
- Dial-up pools if multiple dial-up interfaces are available
- Profiles for dial parameters:
 - Idle timeout and fast idle timeout
 - Number of packets buffered during call set-up
 - Interval between successive calls

- Call timeout
- Maximum outgoing call time over a 24 hours period
- Restriction on time frame within which outgoing calls are possible
- Maximum number of simultaneous ISDN channels for Multilink PPP
- Minimum number of ISDN channels to keep free for incoming calls
- PPP and Multilink PPP encapsulation for routed IP traffic
- Bandwidth Allocation Protocol (BAP) (RFC 2125) for ISDN interfaces
- Call filtering on incoming and / or outgoing calls, local and remote telephone number
- Channelised E1 interfaces can be used as an ISDN PRI interface (up to 30 simultaneous ISDN calls)
- ISDN callback for dial-out in compliance with the PPP LCP callback extension of RFC 1570. Operations 0, 1 and 3 are supported.
- Leased line operation on ISDN BRI interfaces (aka Standard Festverbindung (SFV))
- ISDN BRI internal and external loopback tests

IP Address assignment and auto-provisioning

- BOOTP/DHCP server (RFC 2131, RFC 2132) with static or dynamic address assignment
- IP address ranges in the DHCP server are configurable per interface
- If no gateway is configured in the DHCP server, the router gives its own address.
- DHCP relay agent (RFC 2131, RFC 2132)
- DNS relay
- Local DNS server
- Static IP address assignment
- Static ARP entries
- Automatic IP assignment through BootP client (RFC 951)
- Automatic IP assignment through DHCP client (RFC 2131, RFC 2132)
- DHCP client requests can be blocked from being transmitted on the LAN and from bridge groups
- Automatic IP assignment through PPP IPCP
- Possible assignment of secondary IP address on LAN interface
- Automatic IP gateway assignment through Inverse ARP (RFC 2390, in Frame -Relay and ATM)
- Numbered or unnumbered mode on WAN interfaces
- Automatic configuration file upload through DHCP client
- Automatic default route assignment on remotely learned IP address in PPP
- For deployment of many devices in a network, a pre-configuration file can be installed on the device's file system with the minimal configuration to connect to the servers for the auto-provisioning. A reset button allows returning to the pre-configuration (hardware dependent).

IP routing

The equipment complies with 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:

Static routing

Routing is based on 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 higher layer information. Traffic is routed to a certain interface or gateway based on one or more of the following parameters:

- Source and destination IP address range
- Type Of Service (TOS) value range (8 bits in the IP header, also called DSCP bits)
- IP protocol (examples are any (0), ICMP (1), IGMP (2), TCP (6), UDP (17))
- Source and destination port range for UDP / TCP packets

RIP

- RIP1 compliant with RFC 1058
- RIP2 compliant with RFC 2453
- Split horizon and selective router updates per interface
- Broadcasting of selective RIP updates limited to information on specific network subnets
- RIP2 authentication with MD5 hashing or clear text
- Triggered RIP for ISDN interfaces

OSPF

- Compliant with RFC 2328 (OSPF version 2)
- Import of statically configured routes including the default route
- Route summarization and route suppression through range definitions on areas
- Encryption through simple password or MD5 encryption chains
- Virtual links
- OSPF NSSA (RFC 3101)

BGP4

- Border Gateway Protocol version 4 (RFC 1771)

VRRP

- Virtual Router Redundancy Protocol in accordance with RFC 3768
- Critical interfaces list: whenever at least one critical interface is down, the router behaves for VRRP as if it were powered down.

ICMP

ICMP messages (RFC 792) are used to inform the originator of the packets about anomalies:

- "TTL exceeded" messages
- "destination unreachable" messages (configurable)

Multicasting and broadcasting

The TDRE equipment supports the handling of broadcasts and multicasts and include the following related functionalities:

- IGMPv2 (Internet Group Management protocol, RFC 2236), as the standard for IP multicasting
- IGMP proxy function

- Enabling or disabling the forwarding of directed broadcasts on an 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

IP MTU

- The IP MTU can be configured on the WAN and LAN interfaces (between 500 and 1650 bytes)

VRF

Virtual Routing and Forwarding (RFC 1771) allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. Each physical and logical interface belongs to one of the routing instances.

IP filtering and firewall

- Filtering of outgoing traffic on all interfaces based on extended access lists
- Filtering of incoming traffic on all interfaces based on extended access lists
- Filtering on incoming traffic on the IP protocol stack based on an extended access list
- IP extended access lists filter on the following parameters:
 - Source and destination IP address range
 - Type Of Service (TOS) value range (8 bits in the IP header, also called DSCP bits)
 - IP protocol (examples are any (0), ICMP (1), IGMP (2), TCP (6), UDP (17))
 - Source and destination port range for UDP / TCP packets
- Stateful inspection firewall with 3 zones (Internet, Corporate, DMZ) and Self (IP protocol stack)
- Outbound and inbound policies based on
 - Source and destination IP address range
 - Application (IP protocol and port range)
- PAT can be applied per outbound / inbound policy
- Outbound and inbound policies for the IP protocol stack
- Protection against attacks including
 - Denial of Service attacks (DoS): SYN flooding, winNuke, ICMP error messages, Ping of Death
 - Exploit attacks: IP unaligned timestamp, MIME flood, Sequence number out of range, IP option
 - Spoofing: FTP bounce, Sequence number prediction, IP Spoofing
 - Source Routing
- Firewall status and performance values
- Firewall logging with different priorities
 - Configurable per policy
 - Thresholds per attack type
- TCP MSS Adjustment. This feature enables the configuration of the maximum segment size (MSS) for transient TCP packets that traverse a router. When PPP over Ethernet (PPPoE) is being used in the network, PPPoE truncates the Ethernet maximum transmission unit (MTU) to 1492 bytes and no communication may be possible. Similarly when a tunnelling protocol such as GRE, L2TP or IPSEC is being used in the network, fragmentation may be required if the MSS is not adjusted, which slows down the communication.

Bridging and VLANs

Bridging

- 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 interfaces on the router and may be combined with IP routing on the same interface.
- 10,000 MAC addresses cache
- Self-learning bridge may be disabled to operate it as a n interface convertor
- Maximum size of Ethernet frames depends on the device, but is guaranteed at least 1650 bytes
- VLAN support (802.1Q)
- Multiple bridge groups: a bridge group is a collection of interfaces that are connected through bridging. These interfaces may be physical or logical interfaces. In case a bridge-group is connected to a logical Ethernet VLAN interface, it is possible to forward or strip -off the VLAN ID (untagging) before sending the Ethernet packets to the other interfaces of the bridge group.
- Within a bridge group, an IP address can be defined for management purposes. Also secondary IP addresses can be configured.
- Integrated Routing and Bridging (IRB)
- MAC address configurable per bridge group
- Between different bridge-groups in the equipment, routing may be enabled.
- Multiple VLANs may be defined in the interface within a bridge group towards the IP router.
- IP TOS to 802.1P COS mapping and COS to TOS mapping are available on the LAN interface and the data sent between a bridge group and the IP router in order to maintain priority information when changing from IP to VLAN or vice versa.
- Up to 250 VLANs can be used per LAN interface. If tagging, untagging or filtering is used on port level within the built-in Ethernet switch, up to 16 different VLANs can be used.
- On the LAN interfaces and in bridge groups, MIB2 performance counters are available per VLAN

VLAN switching

- 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 802.1P priority tags.
- Switching may occur uniquely on the P-bits (agnostic to the VLAN tag)
- In VLAN switching mode, Q in Q is available.
- No practical limit on the number of VLANs in VLAN switching mode
- VLAN switching performance table
- VLAN switching mode can be combined with bridging mode for packets on the same interface.
- The switching rules can be bidirectionally or only in one direction

Filtering

- Simple filtering can be configured per interface for outbound traffic. These access lists filter on source MAC addresses.

- Advanced filtering can be configured per interface both in inbound and outbound directions. The filtering is based on source and destination MAC address ranges, the layer 3 protocol field, the number of TCP SYN packets per minute and VLAN tag and priority bits.
- Limit broadcasts in a bridge group selectively by interface. A proxy ARP cache avoids losing ARP requests.

Network address translation (NAT and PAT)

- Compliant with RFC 3022
- NAT mode for one-to-one private to public IP address translation
- PAT mode for many-to-one private to public IP address translation (also called port mapping, single address NAT or NAPT)
- NAT/PAT configurable on any interface (the interface with the public address(es))
- Up to 5 NAT/PAT interfaces
- List of UDP/TCP port numbers that should not be translated
- Reverse NAT or Port Forwarding (List of incoming UDP/TCP port numbers destined for a server)
- Easy NAT: CPE learns official IP address via PPP
- Application Layer Gateway (ALG) Support including:
 - General: FTP, ICMP (Echo, Echo response, Destination unreachable, time exceed & source quench), SQLNet
 - Microsoft Games
 - Video / Streaming applications: RTSP, QuickTime, Real Player (Real Audio / Real Video), H.323 (ASN1 PER encoding and decoding included), NetMeeting, Intel Video Phone, CuseeMe 5.0, SIP Audio
 - Communication: Internet Chat, IRC – MIRC, AOL Instant Messenger, AOL enhanced chat, ICQ2000b, Net2Phone, Microsoft Messenger
 - Security Related: PPTP, IPsec ESP (IPsec client from internal network), IKE, L2TP
- NAT has timed statistics showing the number of socket allocations / transferred data over a given interval

IP VPNs

PPPoE

- A PPPoE server is available on the LAN interfaces and in the bridge groups. Up to 100 PPPoE sessions can be terminated.
- PPPoE clients can be set-up on the LAN interface

L2TP tunneling

The Layer 2 Tunneling Protocol emulates a point-to-point connection over an IP network.

- Compliant with RFC 2661
- Available on WAN and LAN interfaces
- Tunnel authentication
- Available for IP and bridged PDUs
- Static and dynamic tunnels. Dynamic tunnels are set-up only if data is to be sent.
- One L2TP tunnel between each pair of IP addresses

TDRE

- One PPP session per L2TP tunnel
- L2TP tunnels can be set up from an interface running NAT/PAT
- L2TP backup tunnels
- RIP snapshot routing on L2TP tunnels
- L2TP counters: performance LCP events, authentication events, IPCP events, 'port'

GRE tunneling

- Generic Routing Encapsulation (GRE) (RFC 1701-1702)

IPsec security

- Compliant with RFCs 2401 and succeeding
- Lifetime option
- L2TP transport mode (RFC 3193)
- GRE transport mode
- IPsec tunnel mode (RFC2406) aka native IPsec
- ESP (Encapsulation Security Payload), allowing authentication of the sender and encryption of the data (RFC 2406)
- DES (56 bits; RFC 2405), 3DES (3 * 56 bits; RFC 2451) and NULL (RFC 2410) encryption. The availability of the different encryptions may be hardware dependent. See table at the end of this document.
- HMAC (Keyed-Hashing for Message Authentication) based on MD5 (RFC 2403) and SHA -1 (RFC 2404) for integrity and authentication
- Manual SAs (Security Association)
- IKE preshared SAs
- IKE certificate SAs; certificates manually installed or installed via Simple Certificate Enrollment Protocol (SCEP)
- Key management protocol framework compliant with
 - RFC 2408 "Internet Security Association and Key Management Protocol"
 - RFC 2407 "IP Security Domain of Interpretation for ISAKMP"
 - RFC 2409 "Internet Key Exchange" (IKE)
- IKE phase 1 main and aggressive negotiation modes
- IKE phase 2 Perfect Forward Secrecy (PFS)
- IKE Dead Peer Detection (RFC 3706)
- NAT Traversal (NAT-T) in compliance with RFC 3947 and 3948
- The MTU can be configured on the tunnels (L2TP, GRE and native IP sec). This MTU overrides the MTU on the outgoing interface if it is smaller.
- Proxy ID settings (for interoperability with Cisco or OneOS access -lists)

Note: On the standard equipment, the software handles the IPSEC encryption. 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 hardware accelerator chip. This chip takes care of the encryption / decryption, unburdening the software of this task.

Quality of Service (QoS)

Traffic classes

The Quality of Service mechanism is based on total of 7 forwarding queues per interface . Queues are numbered 1 to 7 with 1 the lowest priority and 7 the highest. Six of them are for user data, while the last one is a system queue:

Queue	Queue type	Description
1 – 5	configurable queue	Standard queues
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.

IP traffic classification and policing

The classification and policing of the traffic between the different queues occurs through an IP Traffic Policy. The following variants of traffic policy are available:

'Traffic shaping'

Based on a variety of TCP/IP protocol parameters, a complete customised policy may be set. The elements that define how the traffic is forwarded to a certain priority queue are the following:

- Source and destination IP address range
- Type Of Service (TOS) value range (8 bits in the IP header, also called DSCP bits)
- IP protocol (examples are any (0), ICMP (1), IGMP (2), TCP (6), UDP (17))
- Source and destination port range for UDP / TCP packets
- Existing priority colour (suitable for outbound traffic policies)

Traffic that meets an entry in the traffic policy can get be remarked with a different TOS/DSCP value or the priority can be coloured for further processing (independent of the TOS/DSCP setting).

The maximum queue length in packets (before packets are dropped) is configurable.

Performance information is available on classified traffic: discarded packets and usage of each line in the traffic-shaping table

'TosDiffServ'

The data is redirected to the queues based on *DiffServ* (RFCs 2474, 2475) 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.

TDRE

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	packets are dropped if
00 and 01	the queue length exceeds a configurable maxLength1
10	the queue length exceeds a configurable maxLength2
11	the queue length exceeds a configurable maxLen gth3

'TosMapped'

This simple and flexible policy allows classifying the traffic based on a user-defined range of the TOS field into one of the queues. The maximum queue length in packets (before packets are dropped) is configurable.

'QueueMapped'

This outbound policy maps the colour of packets that have passed an inbound traffic policy to a priority queue. This allows grouping differently coloured packets to a single priority queue.

Bridge traffic classification and policing

Classification can be configured per physical and logical interface both in inbound and outbound directions. The filtering is based on source and destination MAC address ranges, the layer 3 protocol field, VLAN tag and priority bits.

Traffic that meets an advanced access list entry can get an additional action. Possible actions are:

- Limit TCP SYNs
- Jump over or jump to another entry (stacked filtering)
- Colour the packet with a priority, map COS to TOS or set TOS and COS bits
- Apply an IP traffic policy

Traffic shaping

- On the Ethernet interfaces, a maximum outbound bandwidth can be configured. This allows limiting the traffic sent out on the Ethernet interface below the physical bandwidth.
- Per queue, a committed information rate (cir) is configurable. Per queue the bandwidth is measured over a period of time. Traffic that exceeds the cir value is no longer serviced conform the selected priority policy but is queued until there are no other queues with traffic below their cir value. If the maximum queue length is meanwhile reached, additional packets are dropped. This is also called Committed Access Rate (CAR).
- The traffic shaping on outbound packets is extended with an eir value (Excess Information Rate) per queue. Traffic above the cir value is accepted up to a maximum rate cir + eir if there is sufficient bandwidth available, e.g. because there is currently no higher priority traffic on this outbound interface.

- CIR and EIR statistics are available. The statistics include the number of packets that could be directly transmitted, the number of packets that were first queued before they were sent, the number of packets dropped, the total number of packets sent conform the CIR value and the total number of packets sent conform the EIR value. The same statistics are also available expressed in bytes.

Priority scheduling

The way that the *configurable queues* are transmitting data can be selected according to different algorithms. It is also called Priority Queuing (PQ). Each queue has a quatum and a weight parameter. The quatum defines how many data are taken from the queue each time. The quatum is expressed in bytes or packets. The weight parameter defines the relative number of times this queue is emptied. Following algorithms are implemented:

- FIFO (first in first out): no separate priority queues are in use
- Round Robin: the configurable queues all have equal weight
- Absolute Priority: the queues have no weight nor a quatum. A lower priority queue is emptied only if all higher priority queues are empty.
- Weighted Fair Queuing: weights are configurable per configurable queue . If the traffic classification is based on DSCP (tosDiffServ) bits, this is commonly called WFQ. If the traffic classification is using traffic shaping, this is commonly called Class Based Weighted Fair Queuing (CBWFQ).
- Low delay Weighted Fair Queuing: weights are configurable per configurable queue. Data in the low delay queue is always emptied prior to any data in the user configurable queues. This is commonly called Low Latency Queuing (LLC).

IP SLA (traffic quality monitoring)

- Measurement of roundtrip delay, jitter and loss
- configurable destinations
- Measurements are based on ICMP echo packets (ping)
- Configurable DSCP bits for different quality service classes
- Sliding window of up to 2000 packets with a configurable time interval
- Returns number of packets sent and received, the number of lost packets, the minimum, average and maximum delay and the average, maximum negative and maximum positive jitter
- Alarms with configurable thresholds for the average delay, the maximum delay , the difference between the minimum and the maximum delay , the average jitter, the maximum jitter and percentage loss. Jitter is defined as the differential delay between two consecutive packets.
- Logging of the quality monitoring results per time interval

Security

The equipment is password protected for access through the different maintenance and management tools. For each router one can define a variety 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 (configuration, firmware files...)

The unit also features a Radius client (RFC 2865), that can be used for authentication, authorisation and accounting (AAA) of network maintenance sessions, or for PPP sessions initiated by remote devices.

Per interface one can enable/disable all access to the device for traffic coming from this interface. Overall access with specific management tools can be prohibited (telnet – HTTP, SNMP, TFTP, FTP).

All accesses (successful and failed logins) are logged.

Maintenance and Management tools

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

- TMA (Total 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 port 1728).
- TMA CLI: stand-alone command line console software
- TMA for HP OpenView: management integration in HP Openview NNM
- TMA Element Management: stand-alone Element Management
- Local console: a standard VT100 connection with command line or interactive menu -driven user interface
- TELNET server with command line or interactive menu -driven user interface (RFC 854)
- TELNET client from the console port and from within another telnet session.
- HTTP interactive menu -driven web user interface (RFC 2616)
- HTTP interface available on ports 80 and 8080
- Customisable JAVA based web interface
- 5 simultaneous TMA, TMA CLI, local console, telnet and HTTP sessions
- PING (RFC 792) request and reply with extended options . Multiple pings can be sent simultaneously.
- Traceroute command with extended options
- TFTP configuration and software download (RFC 1350)
- FTP configuration and software download (RFC 414)
- TML: Total Memory Loader for the download of configuration or software through the serial console port
- SNMP version 1 (RFC 1157)
- SNMP version 2 (RFCs 3416-3418). The release of SNMPv2 involves SNMP private MIB files that are different from the ones before TDRE 12.0. Both versions may co -exist in a network.
- SNMP version 3 (RFCs 3413-3415) (without the use of a RADIUS server)
- 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
- Timed statistics for many performance attributes (e.g. MIB2 interface values):
 - Values per 15 minutes during the last 2 hours
 - Values per 2 hours during the last 24 hours
 - Values per day during the last 7 days

- Timed statistics can be synchronised to the real-time clock. This means e.g. for the 24 hours statistics that every 2 hours interval starts at exactly an even hour of the day. For the 7 days statistics each day interval starts at exactly midnight. For the 2 hours statistics each 15 minutes interval starts at exactly an hour or 15, 30 or 45 minutes after the hour.
- Timed statistics can be automatically exported to the file system. A selection of statistics can be configured for export. Per configurable period a new file is created. Using FTP/TFTP one can upload these files to a PC or server for further processing or analysis.
- The absolute performance counters can be cleared overall or per object
- Dual software image allows secure firmware upgrades
- Mode to automatically boot up from the most recent stored software version
- Compressed software image allows fast transfer and compact storage in Flash memory

Features history

New features in TDRE 11.0

PPP encapsulation

- MS-CHAP1 (RFC 2433) and MS-CHAP2 (RFC 2759) CHAP authentication protocol extensions
- Multi-class PPP (RFC 2686)
- Bandwidth Allocation Protocol (BAP) (RFC 2125) for ISDN interfaces

Frame Relay encapsulation

- Frame-relay fragmentation (FRF 12)
- Multi-link Frame-Relay (FRF 16.1)
- Improved algorithm for the CIR/EIR calculation
- The total number of DLCIs on a device is increased from 40 to 200

ATM encapsulation

- OAM F4 /F5 segment and end-to-end CC (Continuity Cells) (1431 only)

Other WAN encapsulations

- Error test encapsulation for end-to-end error tests over TDM networks between OneAccess devices
- Leased line operation on ISDN BRI interfaces (aka Standard Festverbindung (SFV))

Interface characteristics

- Configurable MRU (Maximum Receive Unit) on HDLC, PPP and Frame Relay interfaces up to a maximum value of 1650 bytes (default 1560 bytes)

Routing

- Policy based routing can also be used on interfaces with NAT and/or PAT
- Triggered RIP for ISDN interfaces
- OSPF routing protocol
- The IP MTU can be configured on the WAN and LAN interfaces (between 500 and 1650 bytes)

IP filtering and firewall

- Filtering of incoming traffic on all interfaces based on extended access lists
- Filtering on incoming traffic on the IP protocol stack based on an extended access list

Bridging and VLANs

- MAC address configurable per bridge group
- IP TOS to 802.1P COS mapping and COS to TOS mapping are available on the LAN interface to maintain priority information when changing from IP to VLAN or vice versa.
- In VLAN switching mode, Q in Q as defined in IEEE 802.1ad is available.
- Limit broadcasts in a bridge group selectively by interface. A proxy ARP cache avoids losing ARP requests.

Network Address translation (NAT and PAT)

- Up to 5 NAT/PAT interfaces

Tunneling and VPNs

- L2TP tunnels can be set up from an interface running NAT/PAT

Quality of Service

- Per queue, a committed information rate (cir) is configurable. Per queue the bandwidth is measured over a period of time. Traffic that exceeds the cir value is no longer serviced conform the selected priority policy but is queued until there are no other queues with traffic below their cir value. If the maximum queue length is meanwhile reached, additional packets are dropped.

New features in TDRE 11.1

ATM encapsulation

- In routing mode, auto PPP is available on ATM PVCs: an automatic selection is made between PPPoA and PPPoE.

IP Address assignment and auto-provisioning

- DNS proxy:
 - If the router has a static DNS server address is configured or it has received a DNS server address via a DHCP request (as a DHCP client), the router uses that address in DHCP replies (as a DHCP server).
 - If the router has not yet a DNS server address, it uses its own address as a DNS server address in DHCP replies with a short lease time.
- The router relays DNS requests to configured or learned DNS servers.
- DHCP client requests can be blocked from being transmitted on the LAN and from bridge groups.

Bridging and VLANs

- Multiple VLANs may be defined in the interface within a bridge group towards the IP router.
- IP TOS to 802.1P COS mapping and COS to TOS mapping are available on the data sent between a bridge group and the IP router to maintain priority information when changing from IP to VLAN or vice versa.

Tunneling and VPNs

- A PPPoE server is available on the LAN interfaces and in the bridge groups. Up to 100 PPPoE sessions can be terminated. This feature is only available on 1061 Router and 2400 Series.

Quality of Service

- Performance information is available on routed traffic shaped data: number of discards and usage of each line in the traffic-shaping table.

Maintenance and management tools

- Customisable JAVA based web interface

New features in TDRE 11.2

Routing

- The OSPF status information has been extended with
 - the received netmask in the network LSAs table, the summary LSA table and the external LSA table
 - the imported type in the table of external routes
- Default metrics can be configured for importing RIP and static routes into OSPF.
- The import of external routes into OSPF can be filtered.
- Virtual Router Redundancy Protocol in accordance with RFC 3768
- Critical interfaces list: whenever at least one critical interface is down, the router behaves for VRRP as if it were powered down.

Bridging and VLANs

- Secondary IP addresses can be configured on the bridge group
- On the LAN interfaces and in bridge groups, MIB2 performance counters are available per VLAN

New features in TDRE 11.3

Dial-up interfaces

- Channelised E1 interfaces can also be used as an ISDN PRI interface. On this interface up to 30 simultaneous ISDN calls can be terminated and / or initiated.
- ISDN callback for dial-out is available in compliance with the PPP LCP callback extension as defined in RFC 1570. Operations 0, 1 and 3 are supported.

IP Address assignment and auto-provisioning

- IP address ranges in the DHCP server are configurable per interface
- The DHCP server collects the DNS names of all DHCP clients and acts as a local DNS server for these names

Bridging and VLANs

- VLAN switching performance table
- The number of entries in the VLAN table on the LAN interface or bridge group is no longer restricted to 25. The total number of interfaces however remains restricted to a maximum 255.

- VLAN switching mode can be combined with bridging mode for packets on the same interface.

Maintenance and management tools

- The WEB interface is also available on port 8080: this allows connecting the web interface in case a NAT service is defined at port 80.

Tunneling and VPNs

- L2TP tunnel discard: allows resetting the main tunnel and closing the routes to the main tunnel when the tunnel is no more available. This ensures that the routes over the tunnel are down instead of spoofing.
- RIP snapshot routing possible on L2TP tunnels

New features in TDRE 11.4

IP filtering and firewall

- Firewall with 3 zones (Internet, Corporate, DMZ) and Self (IP protocol stack)
- Outbound and inbound policies based on
 - Source and destination IP address range
 - Application (IP protocol and port range)
- PAT can be applied per outbound / inbound policy
- Outbound and inbound policies for the IP protocol stack
- Protection against attacks: SYN flooding, Source routing, winNuke, FTP bounce, IP unaligned timestamp, MIME flood, Sequence number prediction, Sequence number out of range, URL filtering, ICMP error messages
- Firewall status and performance values
- Firewall logging with different priorities
 - Configurable per policy
 - Thresholds per attack type

Network address translation (NAT and PAT)

- Application Layer Gateway (ALG) Support including:
 - General: FTP, ICMP (Echo, Echo response, Destination unreachable, time exceed & source quench), SQLNet
 - Microsoft Games
 - Video / Streaming applications: RTSP, QuickTime, Real Player (Real Audio / Real Video), H.323 (ASN1 PER encoding and decoding included), NetMeeting, Intel Video Phone, CuseeMe 5.0, SIP Audio
 - Communication: Internet Chat, IRC – MIRC, AOL Instant Messenger, AOL enhanced chat, ICQ2000b, Net2Phone, Microsoft Messenger
 - Security Related: PPTP, IPSec ESP (IPSec client from internal network), IKE, L2TP

Tunneling and VPNs

- IPSec Key management protocol framework compliant with
 - RFC 2408 "Internet Security Association and Key Management Protocol"
 - RFC 2407 "IP Security Domain of Interpretation for ISAKMP"
 - RFC 2409 "Internet Key Exchange" (IKE)

TDRE

- IKE with preshared SAs

New features in TDRE 11.5

ATM encapsulation

- Service categories VBR-rt and VBR-nrt. The availability of VBR-rt and VBR-nrt service categories is hardware dependent.

IP Address assignment and auto-provisioning

- For deployment of many devices in a network, a pre-configuration file can be installed on the device's file system with the minimal configuration to connect to the servers for the auto-provisioning. A reset button allows to return to the pre-configuration (hardware dependent).

IP routing

- OSPF NSSA (RFC 3101)
- Default route import into OSPF

PPP

- The MLPPP bundle name or the MAC address can be exchanged
- Fragmentation can be disabled in MLPPP

Dial-up interfaces

- The AUX port can be used as a dial-out interface (to connect e.g. a PSTN modem)
- ISDN BRI internal and external loopback tests

Tunneling and VPNs

- IKE with certificate SAs on devices with TDRE 11.4 features
- Certificates manually installed or installed via Simple Certificate Enrollment Protocol (SCEP) on devices with TDRE 11.4 features
- NAT Traversal (NAT-T) in compliance with RFC 3947 and 3948. NAT-T is an add-on to the IKE and Ipsec protocols that make them work when going through NAT.

Access security

- Access logging (successful and failed logins)

Maintenance and Management tools

- Traceroute command with options like DSN name resolution, source IP address, packet length, TOS value and timeouts
- FTP supports Windows XP SP2
- The absolute performance counters can be cleared overall or per object

New features in TDRE 12.0

Kernel

- The Operating System has been adapted with an improved buffer management. This has an impact on the overall performance and in particular with some software modules like the firewall.

- There is a common driver for all physical interfaces .
- The use of general RAM memory and of Dual Port RAM memory has been optimised.

PPP encapsulation

- VLAN 802.1Q support within BCP

ATM encapsulation

- ATM OAM F4/F5 segment and end-to-end PM (Performance Monitoring)

Interfaces

- The status attributes ifDropLevelExceeded and QLength have been added on the LAN interfaces.
- There is an additional configuration attribute to enable/disable automatic retrain of the line interface if the layer 2 on the line interface becomes down (attribute layer2Check).
- Timed statistics (2h, 24h, 7d) are now available per port on an Ethernet switch.

Dial-up interfaces

- The no-traffic timer is now separate for the incoming and outgoing traffic on ISDN & PSTN connections. This corrects backup issues where the backup link remains open due to data traffic flowing in a single direction on the main and the backup link.

IP address assignment and auto-provisioning

- Static ARP entries

IP routing

- Border Gateway Protocol version 4 (RFC 1771). It has been tested for 1000 prefixes and 10 simultaneous sessions to other routers.
- New RIP attribute clearNextHop; when this attribute is enabled, the nextHop parameter in an advertised RIP route is set to zero. The default value is disabled.
- Static routes that are reachable via an Ethernet interface can be configured without a gateway attribute. This simplifies configuration.
- Configuration attribute 'sendHostUnreachable' with options enable/disable added (default enabled)

Bridging and VLANs

- Advanced access lists in bridged mode. The filtering is based on source and destination MAC address ranges, the layer 3 protocol field, the number of TCP SYN packets per minute and VLAN tag and priority bits. This advanced filtering can be configured per interface both in inbound and outbound directions.

Network address translation (NAT and PAT)

- A flood ping over standard NAT is supported.

Tunneling and VPNs

- Generic Routing Encapsulation (GRE) (RFC 1701-1702)
- IPSec tunnel mode or Native IPSec (RFC2406)
- PPPoE clients can be set-up on the LAN interface
- IKE Dead Peer Detection (RFC 3706)

Quality of Service

- In bridged mode any IP packet inside and Ethernet packet can be classified based on its DSCP (TOS) bits.

Maintenance and Management tools

- SNMP version 2. The release of SNMPv2 involves SNMP private MIB files that are different from the ones before TDRE 12.0. Both versions may co-exist in a network.
- SNMP version 3 (without the use of a RADIUS server)
- Wherever 2 hours and 24 hours statistics are available, also 7 days statistics are available now.
- TELNET client from the console port and from within another telnet session.

New features in TDRE 12.1

EFM encapsulation

- Compliance with IEEE 802.3 chapters 61 and 63 for SHDSL (2BASE -TL)
- Bonding in compliance with 802.3 chapter 6 1 (PAF) and ITU-T G.998.2
- OAM in compliance with 802.3 chapter 57 (802.3ah)

IP routing

- Virtual Routing and Forwarding (VRF) (RFC 1771). This technology allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. Each physical and logical interface belongs to one of the routing instances.

IP filtering and firewall

- TCP MSS Adjustment. This feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router. When a TCP session is established the MSS value in the set -up is adapted to the configured value in order to reduce the maximum size of TCP segments. When PPP over Ethernet (PPPoE) is being used in the network, PPPoE truncates the Ethernet maximum transmission unit (MTU) to 1492 bytes and no communication may be possible. Similarly when a tunnelling protocol such as GRE, L2TP or IPSEC is being used in the network, fragmentation may be required if the MSS is not adjusted, which slows down the communication.

Bridging and VLANs

- Traffic that meets an extended bridge access list entry can get an additional action. Possible actions are:
 - Limit TCP SYNs
 - Jump over or jump to another entry (stacked filtering)
 - Colour the packet for a priority, map COS to TOS or set TOS and COS bits
 - Apply an IP traffic policy
- In VLAN switching mode, switching may occur also uniquely on the P-bits
- In VLAN switching mode, rules can now be bidirectionally or only in one direction

Network Address Translation (NAT and PAT)

- NAT has timed statistics showing the number of socket allocations / transferred data over a given interval.

IP VPN

- The MTU can be configured on the tunnels (L2TP, GRE and native IPsec). This MTU overrides the MTU on the outgoing interface if it is smaller. This feature is handy if the tunnel passes over a PPPoE link which requires an MTU of 1492. The other (non tunnelled) traffic uses the standard MTU on the outgoing interface.
- To allow a better analysis of L2TP related network problems a number of counters have been added to the L2TP tunnel: performance LCP events, authentication events and IPCP events. Also a parameter 'port' was added (= ifIndex).
- Proxy ID settings have been added to GRE and L2TP IPsec tunnels. They were already available for native IPsec. The proxy settings must be used when TDRE is used in combination with Cisco or OneOS access-lists. They should be the same on both sides (mirror).

Quality of Service

- IP traffic quality monitoring (IP SLA): end-to-end roundtrip delay, jitter and loss can be measured to configurable destinations. The measurement is based on ICMP echo packets (ping). The DSCP bits can be configured in order to obtain results for different quality service classes. Using a sliding window of up to 2000 packets with a configurable time interval, values are returned for the number of packets sent and received, the number of lost packets, the minimum, average and maximum delay and the average, maximum negative and maximum positive jitter. Alarms are available with configurable thresholds for the average delay, the maximum delay, the difference between the minimum and the maximum delay, the average jitter, the maximum jitter and percentage loss. Jitter is defined as the differential delay between two consecutive packets. Logging is also available of the quality monitoring results per time interval.
- On the Ethernet interfaces, a maximum outbound bandwidth can be configured. This allows limiting the traffic sent out on the Ethernet interface below the physical bandwidth. This is suitable when using the Ethernet interface as the network interface with another NTU device behind with limited WAN bandwidth. A new bandwidth configuration attribute is present on the LAN interfaces, with CIR bandwidth limit, maxQueueLength and bandwidth calculation correction parameters.
- The traffic shaping on outbound packets is extended with a n EIR value (Excess Information Rate) per queue. Traffic above the CIR value is accepted up to a maximum rate CIR + EIR if there is sufficient bandwidth available, e.g. because there is currently no higher priority traffic on this outbound interface.
- CIR and EIR statistics are available. The statistics include the number of packets that could be directly transmitted, the number of packets that were first queued before they were sent, the number of packets dropped, the total number of packets sent conform the CIR value and the total number of packets sent conform the EIR value. The same statistics are also available expressed in bytes.
- The traffic policy supports now filtering on the current colouring (= priority) of the packet buffer. This colouring can be set on the packet buffer by an inbound traffic policy and afterwards be used on an outbound traffic policy. IP traffic policies for outbound traffic have got an additional classification method queueMapped where packets previously coloured (e.g. by an inbound policy) can be mapped to a priority queue. This allows grouping differently coloured packets to a single priority queue.

Maintenance and Management tools

- Timed statistics are now available per port on an Ethernet switch and per ATM PVC.

- Timed statistics can be synchronised to the real-time clock. This means e.g. for the 24 hours statistics that every 2 hours interval starts at exactly an even hour of the day. For the 7 days statistics each day interval starts at exactly midnight. For the 2 hours statistics each 15 minutes interval starts at exactly an hour or 15, 30 or 45 minutes after the hour.
- Timed statistics can be automatically exported to the file system. A selection of statistics can be configured for export. Per configurable period a new file is created. Using FTP/TFTP one can upload these files to a PC or server for further processing or analysis.
- Multiple simultaneous pings can be sent now .
- A new attribute userInfo has been added to the management object. It's a table where the user can put free text information. Its main purpose is to copy values of certain attributes that have a snmp OID that is higher than $2^{31}-1$. Some SNMP platforms cannot handle such high OID's (e.g. IBM Proviso).

Product specific issues

TDRE versions per product

The table below indicates per product and per TDRE version whether these TDRE features are available in the latest firmware. When available, the latest firmware version matching this TDRE version is listed.

Feature	1021	1022 1023	1030 Series	1040 Series	1061	1221
TDRE 11.0			T2802/01700		T2410/00800	
TDRE 11.1			T2802/01900		T2410/01100	T2858/00400 ; T2861/00400
TDRE 11.2	T2858/00500		T2802/02000			T2858/00500 ; T2861/00500
TDRE 11.3			T2802/02300		T2410/01500	
TDRE 11.4	T2858/00700					T2858/00700 ; T2861/00700
TDRE 11.5	T2858/01400		T2802/02900		T2410/02000	T2858/01400 ; T2861/01400
TDRE 12.0	T2858/02000	T2865/00500	T2802/03400	T2866/00400	T2410/02200	T2858/02100 ; T2861/02100
TDRE 12.1	(1)	(1)	(1)	(1)	(1)	(1)

Feature	1421 1422 Crocus Router 10M Intf	1423	1424	1431	1432	2400 Series
TDRE 11.0	T2852/02400			T2855/01400		T2402/00800 ; T2403/00800 ; T2404/00800
TDRE 11.1	T2852/02600			T2855/01800		T2402/01400 ; T2403/01200 ; T2404/01200
TDRE 11.2	T2852/02700					
TDRE 11.3	T2852/02900					T2402/01700 ; T2403/01500 ; T2404/01500
TDRE 11.4						
TDRE 11.5	T2852/03200	T2863/00700		T2855/02200		T2402/02000 ; T2403/02000 ; T2404/02000
TDRE 12.0	T2852/04100	T2863/01200		T2855/02600	T2860/00400	T2402/02200 ; T2403/02200 ; T2404/02200
TDRE 12.1	(1)	(1)	(1)	(1)	(1)	(1)

(1) See the product documentation on the OneAccess website <http://www.oneaccess.com> to find the latest firmware version

WAN encapsulations

Products	1022 1030 1042	1023 1030 1043	1021 1030 1221 1423	1021 1030 1221 1423	1221	1030 1040	1421 1423 ¹	1221 1422 1431 1432 2400	1424	1061 2400	1061 2400	1061 2400	Cr Rtr 10M Intf
Interface type	G703	RS530	ISDN-BRI	ISDN-BRI LL	PSTN	AUX	DSL	DSL	DSL	TIM 6E1	TIM E3/T3	TIM STM1	Basic Unit interface
PPP										2			
Multilink PPP										2			
Multi-class PPP										2			
Frame Relay										2			
Multilink Frame Relay										2			
HDLC													
Error test													
ATM	3												
ATM IMA													
EFM													

¹ The 1423 versions support the additional HDLC based WAN encapsulations (starting from a minimal hardware version), except the version with ISDN backup, which only supports ATM encapsulation on its SHDSL link.

² In PPP and Frame Relay modes, the E1 interfaces operate in framed mode, possibly in fractional E1 mode

³ ATM on the E1 interface of the 1031 and the first E1 interface of the 1032 and 1042.

Other features

Feature	1021	1022 1023	1030 Series	1040 Series	1061	1221
Hardware accelerator (HWA)		⁴				⁴
DES encryption						
3DES encryption		⁴				
Routing and bridging performance (Kpps)	90	50	45	90	175	45 / 80 ⁵
Routing performance with IPSec (Kpps) ⁶	24		4,2	24		21
# Bridge groups	13	13	13	13	25	13
# IP VPN tunnels (IPSEC, L2TP, GRE)	25	25	25	25	25	25
# ATM PVCs	-	-	31	31	200	31
ATM CBR service category	-	-	-			
ATM VBR-rt & VBR-nrt service	-	-	-			
ATM OAM Performance Management (PM)		-	-			
Statefull inspection firewall & application layer gateway					-	
ISAKMP, IKE & IPSEC certificates					-	
BGP4, GRE, native IPSEC						
PPPoE client on the LAN		-	-		-	
PPPoE server	-		-	-		-
Flash memory (M Byte)	8	8	16	16	64	8
RAM memory (MByte)	16	16	16 ⁷	64	256	16
Customisable JAVA web interface						
Reset button		⁸		⁸		

⁴ Available on specific versions with indication HWA

⁵ Highest values for versions with built-in hardware accelerator

⁶ With 3DES encryption and using the hardware accelerator

⁷ 64MByte on the 1035

⁸ The 1022, 1041 and 1042 have a reset button

Feature	1421 1422	1423	1424	1431	1432	2400 Series	Crocus Router 10M Interface
Hardware accelerator (HWA)		⁴					
DES encryption							
3DES encryption							
Routing and bridging performance (Kpps)	40	50 / 90 ⁵	250	40	40	175	45
Routing performance with IPSec (Kpps) ⁶		24	TBD				
# Bridge groups	13	13	13	13	13	25	13
# IP VPN tunnels (IPSEC, L2TP, GRE)	10	25	25	10	10	25	10
# ATM PVCs	31	31	31	30 ⁹	30 ⁹	200	
ATM CBR service category	-						-
ATM VBR-rt & VBR-nrt service	-						-
ATM OAM Performance Management (PM)	-						-
Statefull inspection firewall & application layer gateway	-			-		-	-
ISAKMP, IKE & IPSEC certificates	-			-		-	-
BGP4, GRE, native IPSEC	-			-			-
PPPoE client on the LAN	-			-	-	-	-
PPPoE server	-	-	-	-	-		-
Flash memory (M Byte)	8	8	32	8	8	16	8
RAM memory (MByte)	8	16	64	16	16	32	16
Customisable JAVA web interface							
Reset button							

⁹ This includes up to 5 CES PVCs + 1 low speed management PVC and/or any mix of other PVCs (for IP/Ethernet, FRF or ATM switching).