MetroCONNECT
Carrier Ethernet Demarcation

Solution Brief

End-to-End Circuit Performance Test and Monitoring
for
Ethernet Service Providers

Sept, 2016

Metrodata Ltd Laxton House, TW20 8RY U.K.

Tel: +44 (0)1784 744700 **www.metrodata.co.uk** **E-mail**: sales@metrodata.co.uk

Carrier Ethernet Demarcation

Introduction

The ubiquitous deployment by Telecommunications Companies of Packet Switched Networks, in replacement of long-standing SDH/PDH Circuit-Switched Infrastructures, has contributed to a rapid rise in the availability of high bandwidth Ethernet Services, increasingly delivered to Customer premises via fibre.

Packet Switched Services, offered to Corporate customers via Ethernet termination, tend to comprise one of two broad types; (i) 'Layer-3' Services, typically derived from 'MPLS' core switched networks, and most commonly delivered as IP-Virtual Private Network (IP-VPN) connections, terminated at the customer premises by IP 'Edge' Routers, or (ii) 'Layer-2' Services, often in the form of point-to-point Layer-2 VPN connections or multi-point Virtual Private LAN Services (VPLS), also derived from MPLS switched infrastructures. Such Layer-2 services are generally terminated at the customer premises by managed 'Ethernet Demarcation Devices'.

Within these broad service categories many variations exist and the breadth and diversity of Carrier Service offerings continues to increase. Some Carriers focus on Layer-2 infrastructure in the form of Switched Ethernet services, whilst others focus mainly on Layer-3 services. In the increasingly de-regulated world of Telecoms Services, Layer-2 Infrastructure Carriers may offer their services on a wholesale basis to Integrators or Layer-3 Service Providers. In this scenario, the Service Provider may regard the Layer-2 Carrier as simply a supplier of 'bandwidth', to which an IP-VPN offering, with associated Routers, is added to the switched Ethernet connectivity provisioned by the wholesale supplier. In an alternative approach, some end-user customers may contract with a Layer-3 Service Provider for IP infrastructure services, but on a 'wires only' basis, wishing to add their own on-site Routers, rather than having these supplied and managed by the Service Provider.

In either of these cases, it is likely that the Carriers offering either Layer-2 Wholesale services, or Layer-3 'wires only' services, will wish to deploy their own equipment at customer premises, to which Routers are connected, in order to achieve full end-to-end visibility and management of their own service offering. This is particularly important when, as is frequently the case, the infrastructure provider does not 'own' the physical connection media to every customer site, and must themselves rely on 3rd party provided 'tail circuits' to some locations in order to deliver their services (known generally as 'off-net' services). They will wish to have their own managed end-points right at the point of customer connection, in order to be able to configure, manage and monitor their services fully, end-to-end.

Only relatively recently have end-user customers come to fully appreciate that in the new packet-switched backbone era, not all services are the same in terms of real-world performance relative to expectation. Consequently, customers have started to be much more exacting in terms of the technical performance of the Wide-Area Network services that they contract for. Increasingly stringent 'Service Level Agreements' are being demanded, relating to such characteristics as traffic throughput, delay (a.k.a. latency), delay variation (a.k.a. jitter) and packet loss ratio. Attendant with such SLAs, pressure is being put on both Infrastructure Carriers and overlay Service Providers to be able to demonstrate, both at the time of initial provisioning, and during subsequent in-service usage, that services perform to specification. Providers are obliged to provide comprehensive 'Birth Certificate' reports for all newly commissioned circuits and, in some cases, on-going periodic performance reports during the term of a contract.

These requirements have led to the incorporation of a number of advanced testing and monitoring functions, typically requiring customised hardware to achieve the necessary performance for line rate testing, into the Ethernet Demarcation Devices deployed at the service edge. Such functions may include detailed 'Circuit Activation Testing' to standard profiles defined by RFC2544 and/or Y.1564, and In-Service Monitoring using Y.1731 (for Layer-2 services) and/or 'Two Way Active Measurement Protocol' (TWAMP) for Layer-3 services.

By deploying more sophisticated circuit termination devices, Carriers are not only able to supply their customers with evidence of their meeting defined specifications, but have been able to reduce their commissioning costs and can more effectively troubleshoot problems on behalf of their clients. This document looks specifically at the Test and Monitoring features of advanced Demarcation Devices, such as the 'MetroCONNECT' FCM family from Metrodata, considers why these features are important, and examines how Carriers and Service Providers typically use this functionality.

EDD Test and Monitoring Basics

Over the past few years, each of three Industry standards bodies, namely the Institute of Electrical and Electronic Engineers (IEEE), the International Telecommunications Union (ITU) and the recently re-named MEF (formerly the 'Metro Ethernet Forum') have been active in developing and promoting both capabilities and standards in relation to Carrier (i.e. WAN) Ethernet Services. Initially, a number of 'Operations, Administration and Management' (OAM) protocols were developed relating to Ethernet WAN deployments.

Relatively simple visibility and connectivity checking of single segment Ethernet connections is supported by the 'Link OAM', or 'Ethernet First Mile' (EFM) protocol, formalised initially as IEEE 802.3ah, by which it is still generally best known, albeit that this functionality has now been fully incorporated into the core of the 802.3 standard itself.

An additional level of connectivity assurance is offered by those Demarcation Devices supporting the 'Connectivity Fault Management' (CFM) protocol, formalised under the standard IEEE 802.1ag. CFM offers the ability for a number of end-point devices to establish and monitor a 'community' of reachable mid- and end-points across a customer's network, which can offer some degree of pro-activity to the Service Provider with regard to connectivity fault detection.

Consider the rather simplified Infrastructure diagram below.

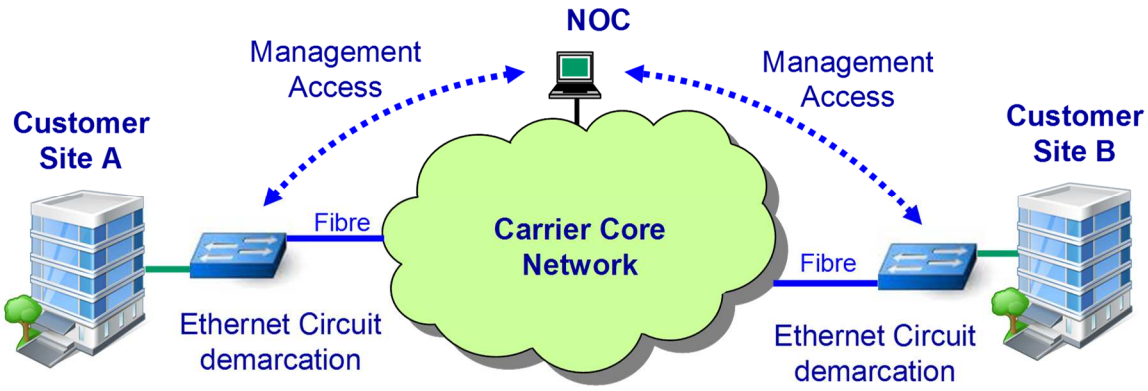

Fig 1. Simplified end-to-end Ethernet WAN Circuit model

In this example, a Telecoms Carrier provides an Ethernet service between two customer sites, A and B. In order to facilitate full manageability, right up to the point of connectivity to the customer's equipment at each site, the Carrier installs manageable Ethernet Demarcation Devices as Customer Premises Equipment (CPE), between the fibre WAN connection and the customer's LAN equipment.

Above and beyond simple connectivity management, customers may ask of their Service Providers that they provision multiple traffic streams across their Ethernet 'pipe' connections, to which potentially different criteria may apply for key network performance parameters, including acceptable frame loss ratio, 'latency' (i.e. traffic delay) and 'jitter' (delay variation), together with comprehensive traffic throughput 'policing'. Providers may then be faced with the challenge of proving to their customers, at the time of provisioning, that such performance parameters are complied with for each individual Service data stream within a given end-to-end Ethernet connection. Such parameters may be detailed within a tightly defined 'Service Level Agreement' (SLA), to which compliance needs to be demonstrated.

Furthermore, Service Providers may not only need to demonstrate SLA compliance at the time of commissioning, but they may be required subsequently to monitor 'in-service' traffic and take pro-active remedial steps with regard to any potential breach of SLA.

Ethernet Demarcation Devices, equipped with advanced packet processing capabilities, can offer a very effective tool to Service Providers in this regard. For example if a Service Provider, from a Network Operations Centre, can interact with an EDD in such a manner as to configure this device to issue one or more test traffic streams across the network to a corresponding remote end-point, at which traffic may be 'looped' and returned, then this can be highly beneficial. Such test streams can facilitate accurate reporting of throughput, packet loss, latency and jitter, for the end-to-end network link. Demarcation Devices with such capabilities are now readily available. Necessarily, such devices contain more than simple switch and management processing functionality. Dedicated packet processing hardware is required in order to ensure accurate time-stamping, test collation and reporting in real-time for line rates up to 1Gbps and beyond.

Another of the OAM protocols, this time the ITU-T's Y.1731 suite, operating at Layer-2 (via Ethernet MAC addressing), offers the potential for in-service monitoring of SLA compliance. More recently, the 'Two-Way Active Measurement Protocol' suite, or TWAMP, offers similar monitoring functionality but using IP-addressed packets, enabling monitoring of latency and jitter, for instance, to much greater precision than traditional simple, software-based 'PING' tests, across Layer-3 Routed infrastructures. This can be important to Service Providers in hybrid environments, for which customer site edge-devices may be connected via Layer-2 local tails, whilst some elements of an end-to-end path under test may comprise IP-Routed infrastructure, from which simple Ethernet MAC-addressed test packets would be blocked.

All of these capabilities, incorporated within the most recent generation of advanced Ethernet Demarcation Devices, ensure that Service Providers' customers experience strength and depth in support.

Circuit Activation Testing (CAT) & 'Birth Certificate' Reporting

At the time of contracting for a new WAN connection, it is now common for a set of 'Service Level Agreement' (SLA) parameters to be established between the Service Provider and their customer. Typical parameters will include Throughput, Packet Loss Ratio, Delay (Latency), Delay Variation (Jitter) and an overall metric for 'availability' as a percentage of total commissioned lifetime of the service.

On commissioning of the service, the Enterprise customer will wish to establish that the contracted criteria are being met, at least with regard initially to the first four of the above parameters, since the availability metric necessarily takes some elapsed time to become meaningful.

In the absence of Ethernet Demarcation Devices equipped with integrated circuit testing capabilities, testing of this type would normally require dedicated Ethernet test sets, featuring comprehensive controls for configuration of all the appropriate parameters to match the SLA required of the network under test. Such devices are excellent but expensive, and testing might typically involve a specific trip to site by a well-trained resource, to connect the test set at the demarcation point of the Service Provider's connection and run the test. Moreover, this type of equipment will launch test traffic into the network which requires to be looped or 'reflected' back at the far end of the WAN link, in order to enable evaluation and for report compilation back at the tester, so it may additionally be necessary to have a suitable resource at the destination point for the network link under test, to facilitate this.

It is important to note at this point that it is not normally suitable to create a simple physical network loop at the remote end of the circuit under test, since in Ethernet and/or IP terms this would appear, to the WAN infrastructure, as though two devices with the same Ethernet and/or IP address were transmitting from different points within the network, not normally an allowable condition. Instead, the loop-back point must more closely replicate a regular device, which can be achieved by Source Address / Destination Address 'swapping' of test packets reflected back to the Tester. Dedicated hardware would normally be required for such a task, since this may need to be conducted at full line rate up to 1Gbps or more.

The most common current profiles for performance testing of Ethernet networks are known respectively as RFC2544 and Y.1564. The former is arguably most appropriate for situations in which the boundaries of network performance are unknown, or for which no clear SLA has already been defined. The test typically involves the transmission of packets in a pre-determined sequence of sizes, perhaps from the

Ethernet minimum of 64 bytes (excluding overheads due to VLAN tagging etc.) in steps up to the maximum packet size supported across the Service Providers equipment, or likely to be used by the Enterprise. The test will attempt to flood the network at maximum line rate, and if errors are detected, for instance by a level of packet loss due to the WAN not supporting the transmitted rate, then the test will follow an algorithm to progressively back-off and then steadily increase traffic flow until the maximum sustainable rate is determined. Once this rate is determined for each of the range of packet sizes specified within the test, then key metrics are measured and recorded at the maximum rate. One part of a typical Layer-2 RFC2544 test summary, actually generated from one of Metrodata's Ethernet Demarcation Devices, is illustrated in Fig. 2.

```
test regime: RFC2544
unit node name: "FCM9005_CO"
unit mac address: 00:c0:81:00:14:d5
start time: 12:13:33 Tue 01/03/2016
---
testing Flow1 "CustomerData"

[Results Summary View]

RFC2544 Throughput Test result summary:

          media     max          measured                                  information
 packet   speed     throughput   throughput   utilisation   utilisation    rate
 size     (Mbps)    (fps)        (fps)        (Mbps)        (%)            (Mbps)
 ------------------------------------------------------------------------------
 68       100       142045       142045       100.00        100.000        77.27
 128      100       84459        84459        100.00        100.000        86.49
 256      100       45290        45290        100.00        100.000        92.75
 512      100       23496        23496        100.00        100.000        96.24
 1024     100       11973        11974        100.00        100.000        98.09
 1280     100       9615         9616         100.00        100.000        98.47
 1518     100       8127         8128         100.00        100.000        98.71

RFC2544 Round-Trip Latency Test:

 frame   time   rate     utilisa-   latency (us)           variation (us)
 size    (s)    (fps)    tion (%)   min     max     ave    max     ave
 ---------------------------------------------------------------------
 68      10     127812   89.980     18.7    29.0    18.8   10.1    0.0
 128     10     76034    90.020     29.3    39.3    29.4   9.8     0.0
 256     10     40756    89.990     51.8    61.8    51.9   9.9     0.0
 512     10     21147    90.000     96.8    106.4   96.9   9.5     0.0
 1024    10     10776    90.000     187.0   193.9   187.0  6.8     0.0
 1280    10     8654     90.000     232.0   239.4   232.1  7.3     0.0
 1518    10     7315     90.000     273.9   284.3   274.0  10.3    0.0
---
```

Fig. 2: RFC2544 Test report example (single flow summary only)

In contrast, the Y.1564 profile test can be an excellent choice for testing against a pre-defined 'Committed Information Rate' (or 'CIR', typically part of an SLA definition). Typically the test sequence involves traffic generation increasing over a minimal number of increments up to the CIR, for a given packet size. Provided that the CIR is met, the test proceeds to record characteristics similar to those of the RFC2544 test. This is repeated for different packet sizes in order to provide a full qualification of the Network service.

Both RFC2544 and Y.1564 tests are 'agnostic' to packet type and addressing. Consequently, by using a tester capable of supporting both Ethernet MAC addressing and IP addressing, then these tests can be conducted across either Layer-2 or layer-3 infrastructures.

Metrodata's MetroCONNECT 'FCM' family of Advanced Ethernet Demarcation Devices, supporting service data rates up to 10Gbps, incorporate custom traffic generation and loop-back hardware, and can

perform comprehensive RFC2544 and Y.1564 profile testing, for each of Layer-2 (Ethernet MAC-addressed) and Layer-3 (IP-addressed) traffic. In the latter case, the FCM products transmit UDP test packets of specific (user selectable) Port Number, in order to ensure differentiation from regular user application traffic throughout the network. Each family member also supports loop-back of test traffic using Source Address/Destination Address (SA/DA) packet-swapping at line rate, in each of the following modes:

(i) Pure Ethernet MAC-addressed packets
(ii) IP-addressed packets of user selectable protocol type (also underlying Ethernet MAC addresses)
(iii) Specific UDP Port number (also underlying IP and Ethernet MAC addresses)

Having this range of loop-back mode flexibility enables Metrodata's devices to inter-operate with a wide range of 3rd party Network testers, should this be necessary.

In operation, through either local connection or more usually via network login from a Network Management Platform, an operator sets up the test type and parameters on a particular EDD and runs testing against a remote loop-back device, either at the far end of a cross-network point-to-point link, or perhaps at an intermediary Carrier POP location, if testing is only required for a particular network segment. In the case of Layer-2 (Ethernet MAC) testing, Metrodata has implemented a generic loop-back MAC address into all of its devices, which is used as the default Layer-2 packet address for generated test traffic. Whenever a remote Metrodata FCM device sees packets destined for this (Metrodata-specific) address, then such packets will automatically be SA/DA swapped and looped back to the originating EDD. This provides a convenient, minimal configuration approach to test operation, although it is possible to substitute the generic test address for a unique, device-specific secondary MAC address for any given EDD when required. Alternatively, Metrodata EDDs can generate test traffic to any other address should some other 3rd party loop-back device be deployed.

Once a test has run, the instigating EDD stores the test result as a report file, which can be subsequently uploaded by File Transfer to a Network Management Platform, for incorporation directly into a Carrier's Birth Certificate report for the service. It is alternatively possible to automate the upload of the report to a Management Console (sent as a simple 'flat' text file for maximum flexibility). The whole CAT process is illustrated in Fig. 3 below, showing a combination of MetroCONNECT FCM9003 and FCM9005 EDD units.

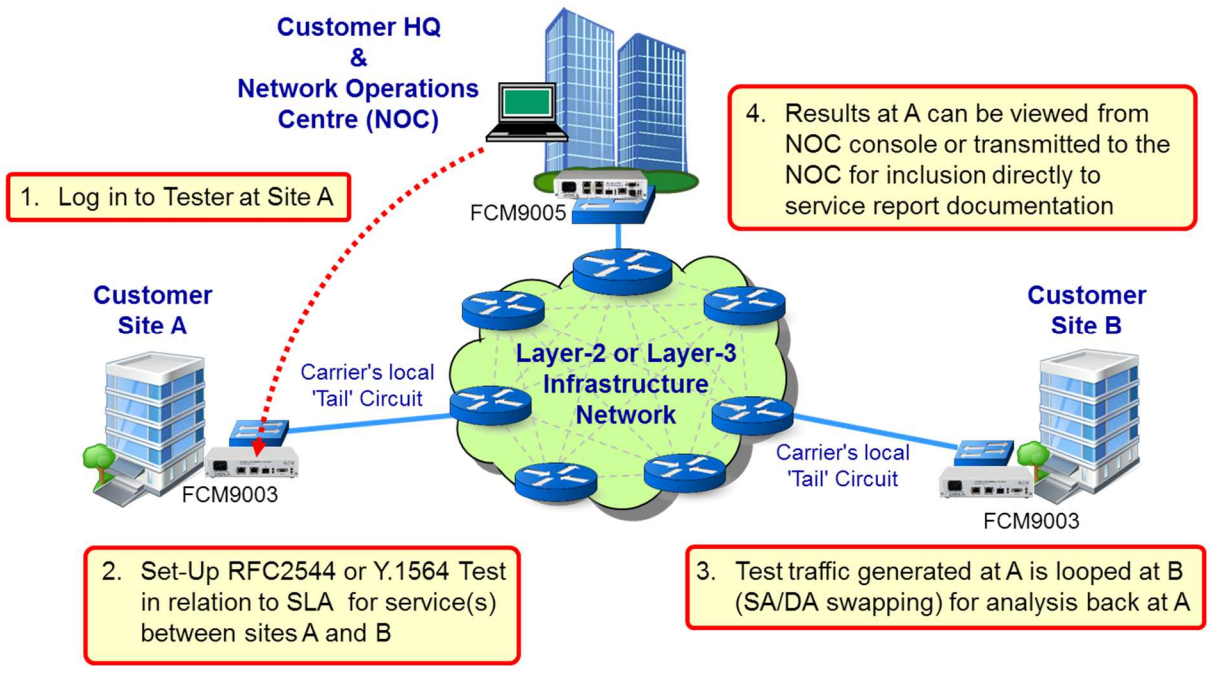

Fig. 3: Metrodata EDDs used for Circuit Activation Testing

In-service Performance Monitoring

During subsequent 'in-service' usage, the challenge for the Carrier becomes one of monitoring actual performance of the network under 'real load' conditions. For pure Layer-2 (Ethernet) networks, the ITU-T Y.1731 protocol provides mechanisms for enabling periodic test packets to be inserted into live data-streams, which can then be used to monitor latency and jitter characteristics for each service defined across a Layer-2 circuit. The size and frequency of such test packets are low, hence they are 'minimally invasive' and do not appreciably impact the performance or characteristics of customers' services.

Recently, the more advanced Demarcation Devices, such as those within Metrodata's MetroCONNECT FCM family, have started to include an additional protocol suite, the Two-Way Active Measurement protocol' (TWAMP), which performs a similar job, but for IP-addressed traffic. TWAMP is also somewhat less complex in set-up and operation than Y.1731, so is seen both as more simple to use and more flexible, since it can be used just as readily for layer-2 networks as it can for networks comprising partial or complete Layer-3 (IP Routed) infrastructure.

In operation, for one or more distinct services or 'flows' defined for customer traffic within a Carrier's network, an 'SLA profile' may be established between pairs or numbers of EDDs at different customer locations. Such profile may include the following:

Service throughput
Maximum allowable latency
Maximum allowable delay variation/jitter
Maximum allowable traffic frame loss ratio
Minimum allowable 'availability' percentage

Against each of these parameters, it is possible to assign alarm criteria such that, for example, the Carrier's Network Operations Centre might be alerted if the latency of one of a customer's services, perhaps representing only a single virtual pathway within an overall Ethernet 'pipe', rises above a certain threshold defined within the customer's SLA. The monitoring and alarming mechanism is outlined below:

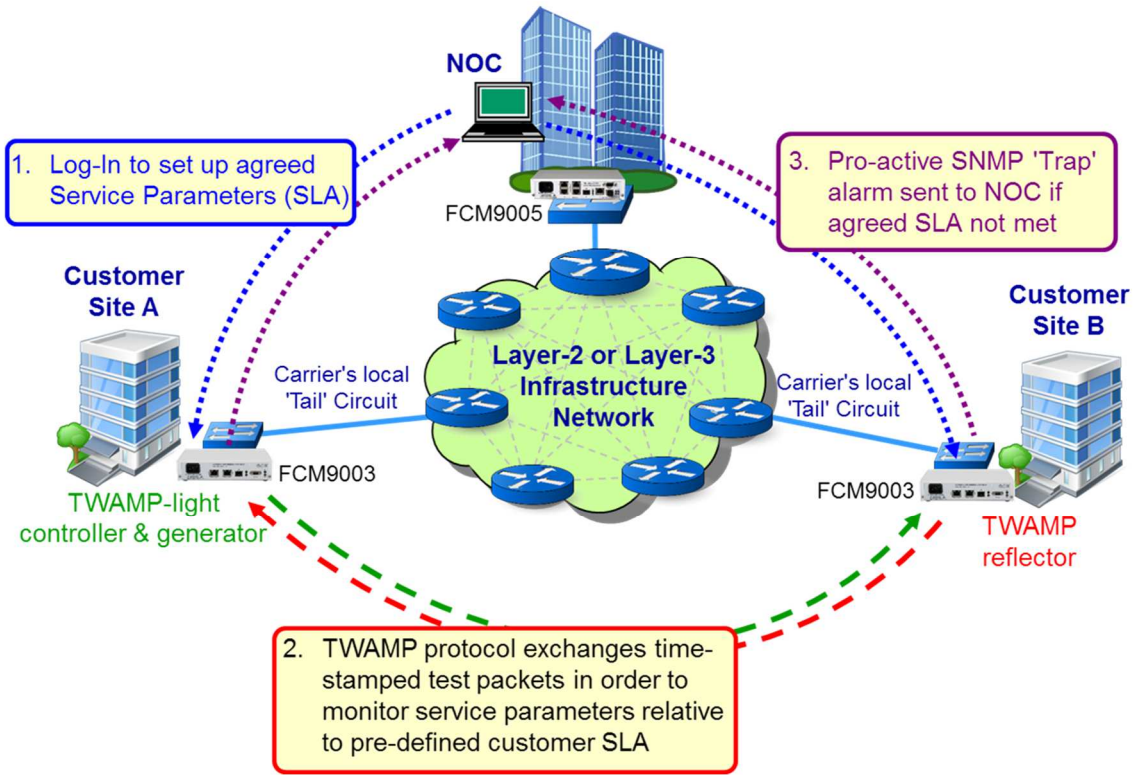

Fig. 4: Metrodata EDDs used for In-Service Performance Monitoring & Alarming

Whilst alarming in the event of specific threshold criteria being breached is clearly important, a Service Provider may wish alternatively to view trends in key performance criteria, for example the variation of traffic delay during a one day or one month period.

Metrodata's FCM family of Demarcation Devices offer great flexibility in the viewing and retrieval of such data. in the first instance, real-time characteristics are stored in a format which can be readily accessed by SNMP-based network Management Applications. Management console operatives can readily set up an enquiry to interrogate key data on a regular basis, say every 15 minutes, thereby building up a table, or graph, of any service performance variable which may be of concern. Alternatively, the products themselves store an appreciable amount of historical data, filed within 15-minute, 1 hour and 24 hour logs for up to 30 days, available to view dynamically by log-in under management control to any Demarcation Device.

The below is a screen capture of a 15-minute data store relating to performance characteristics of an IP traffic stream, as measured via periodic packet exchange using the TWAMP protocol, between two peering points, i.e. the EDD from which this report is being generated, and a remote 'peer' location within the network, with a defined IP address. This may well be a corresponding EDD at the remote end of a customer's point-to-point link across a Carrier's network, or could alternatively be any intermediate point along such a path. The screen illustrates both the 'SLA' which has been pre-defined for this particular link in terms of key performance criteria, alongside the measured characteristics for this particular 15-minute window. In this instance, no SLA thresholds have been breached and no alarms raised.

TWAMP Performance Report

Peer2 "Egham" 10.10.10.2

Start: 15Sep 15:15	2-way/			
Logged time: 480s	Outbound	Inbound	SLA	Alarms
Sent Frames	480			NP 0s
Received Frames	480			SLA 0s
Lost Frames	0			MON 0s
Unavailable	0s			
Availability	100%		99.9%	
Frame Loss Ratio	0%		0.01%	
Min Delay	0.0021ms			
Average Delay	0.0101ms			
Max Delay	0.0320ms		10ms	
Good Delays	100%		95%	
Average Delay Var	0.0074ms	0.0066ms		
Max Delay Variation	0.0163ms	0.0163ms	10ms	
Good Delay Vars	100%	100%	95%	

Fig. 5: Metrodata EDDs used for In-Service Performance Monitoring & Alarming

Through the combination of detailed and flexible Circuit Activation Testing at the time of initial provisioning, or whenever required as an aid to troubleshooting, together with comprehensive in-service monitoring, Ethernet Demarcation Devices offer a low-cost, always-on mechanism for Carriers and Service Providers both to ensure the integrity of their services, and bring differentiating value to their customers in terms of assured performance reporting.

About Metrodata Ltd.

Metrodata is a leading vendor of Telecoms Equipment focused on Network Access and Interface Conversion Applications. The company's products are designed and manufactured in the UK and Metrodata has been a supplier to Telecoms Service Providers, Corporates and Governmental organisations worldwide since 1989.

Major current product ranges include the 'MetroCONNECT' family of Managed Ethernet Extension and Demarcation solutions, 'NetTESTER' family of Embedded Enterprise Testing equipment and 'MetroWAVE' family of passive CWDM & DWDM Optical Multiplexers.

About MetroCONNECT FCM Family Demarcation Devices

Metrodata's family of Ethernet Demarcation Devices currently include the FCM9003, FCM9005 and (by late 2016) the FCM10G05. Developed to the Carrier-quality criteria born of over 25 years of supply to the Telecoms Industry, the wider MetroCONNECT family includes products for Managed Ethernet Extension and Service Delivery over SDH/PDH and Serial Media, as well as regular Ethernet Copper and Fibre demarcation applications. Within the MetroCONNECT family, the FCM range of Ethernet Demarcation Devices are cost-effective and yet offer advanced custom-hardware based facilities for comprehensive test and monitoring for both Layer-2 (Ethernet Switched) and Layer-3 (IP Routed) network infrastructures.

FCM9003

Low in cost and yet feature-rich, the FCM9003 has two Ethernet RJ45 ports and one flexible-media SFP port supporting service connections up to 1Gbps, each of which can be defined for LAN or WAN usage. Both 'auto-sensing' AC and DC PSU variants are available.

The FCM90003 includes Metrodata's custom 'MetroSAM' Service Assurance Module hardware, supporting both Layer-2 (Ethernet MAC addressed) and Layer-3 (IP addressed) Test-traffic generation, loop-back and analysis, enabling RFC2544 and/or ITU-T Y.1564 profile testing. The product additionally supports both ITU-T Y.1731 and TWAMP functionality for in-service performance monitoring.

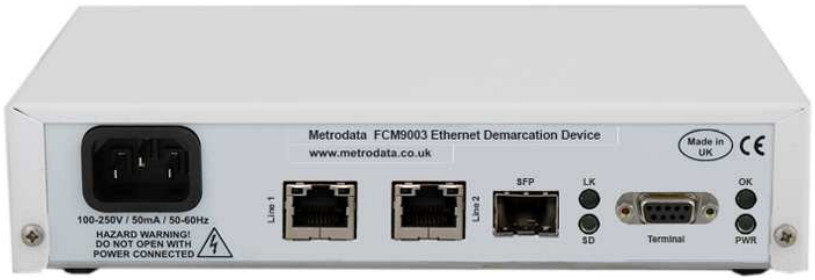

Fig. 6: MetroCONNECT FCM9003 Ethernet Demarcation Device
(AC PSU variant shown)

Full details and the product datasheet are available at:

http://www.metrodata.co.uk/products/Carrier-Ethernet-Service-Delivery/fcm9003-ethernet-demarcation-device.htm

FCM9005

Advanced Demarcation Device featuring multiple LAN and/or WAN ports, for connection either via copper (RJ45) or fibre (SFP).

As a full-featured EDD, the FCM9005 is compliant with the requirements for MEF CE 2.0 Certification. Like the FCM9003, the FCM9005 includes Metrodata's 'MetroSAM' Service Assurance Module hardware, facilitating comprehensive Circuit Activation Testing and In-Service Monitoring. The product is also available in a dual-redundant Power Supply (AC) variant, for additional service resilience.

Regular EDD features for this product include single or double VLAN Tag push/pop, multi-point & multi-level CFM, Full Traffic flow Policing (including for colour-aware WAN implementations) and full 8-level COS-based flow definition, in line with the requirements of CE2.0 Certification.

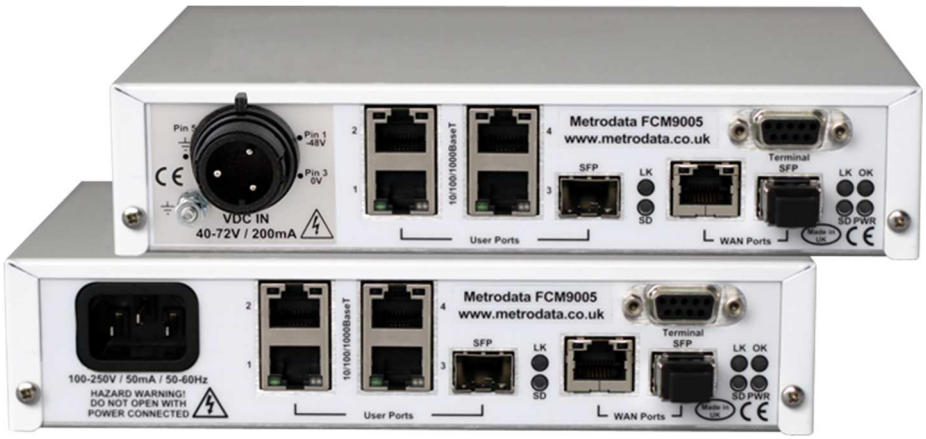

Fig. 7: MetroCONNECT FCM9005 Ethernet Demarcation Device
(Single AC and -48V DC PSU variants shown)

Full details and the product datasheet are available at:

http://www.metrodata.co.uk/products/Carrier-Ethernet-Service-Delivery/fcm9005-advanced-ethernet-demarcation-device.htm

FCM10G05

Due for full customer launch before the end of 2016, the FCM10G05 is Metrodata's Ethernet Demarcation Device for deployments with 10Gbps Ethernet circuits. Featuring a number of 1Gbps ports, as well as a single 10Gbps LAN port, the product supports 10Gbps WAN connectivity via an SFP+ port. Like the FCM9005, the FCM10G05 is compliant with the requirements for MEF CE 2.0 Certification and includes Metrodata's 'MetroSAM' Service Assurance Module hardware.

Fig. 8: MetroCONNECT FCM10G05 Ethernet Demarcation Device
(Single AC PSU variant shown)

Carrier Ethernet Demarcation

All FCM family products provide full Network Management Access, via local terminal and/or remote connection using Telnet/SSH, SNMP and Web-Browser applications. Rack-mounting kits are available for all variants. A ‘zero-touch provisioning’ facility is provided for all products within the range, in order to minimise the installation & configuration actions required on initial deployment.

Metrodata is committed to support for the FCM9005 and FCM10G05 platforms via SDN Orchestration platforms, via the incorporation of support for both management via NetCONF and a set of YANG-based models for key port and flow-based configuration actions. Such support will be facilitated via a software release currently scheduled for the send half of 2017.

Metrodata Ltd.
Laxton House, Eversley Way
EGHAM, Surrey, TW20 8RY U.K.

☎ +44 (0)1784 744700
sales@metrodata.co.uk
www.metrodata.co.uk