Carrier Ethernet Services

White Paper

Ethernet Demarcation Devices

for managing

End-to-End Ethernet Service Delivery

July, 2012

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

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

Carrier Ethernet Services

Introduction

The use of Ethernet by Telecommunications Service Providers, for Corporate connectivity services, is growing rapidly and is set to dominate within just a few years.

'Layer 2' (i.e. of the OSI connection hierarchy model) Ethernet offers some attractive advantages to both Infrastructure Carriers and Telecoms Service Providers in terms of service provisioning, the inherent set-up complexities of Managed Router networks being largely eliminated. Nevertheless, challenges still exist in both the provisioning and ongoing management of Ethernet services, particularly since not only the quantity, but also the sophistication of services demanded by customers is rising. For example, until very recently even in the more advanced economies, the norm for Voice and Data services has been for two separate infrastructures. Now, co-incident with the rise of Ethernet as a transport vehicle, the emergence of SIP trunking for Voice over IP (VoIP) communications, and its associated need for tighter constraints in service quality than is required for most Data (e.g. simple Internet access) applications, is creating a need for greater management visibility to Ethernet service delivery on the part of the Service Provider.

Much effort, by both Carriers and Telecoms Equipment Manufacturers, principally under the auspices of the 'Metro Ethernet Forum' (MEF), has been put into the development of management tools for both Connectivity and, latterly, Performance Assurance for Ethernet services. Nevertheless, a reality today is that relatively few Infrastructure Carriers (by which we mean those with either Long-haul or local transport infrastructure, i.e. cable and/or fibre) make use of the capabilities now potentially available to them for management control and performance validation. Moreover, those which do generally choose to limit the extent of their 'manageable domain' to network segments bounded by their own Ethernet Demarcation Devices (EDDs). As National Telecommunications markets become increasingly de-regulated, there has been a corresponding growth in the number and diversity of Telecoms (in this case Ethernet) Service Providers, offering both a range of Value-Added Services (i.e. Data and/or Voice 'cloud' services) *and* Connectivity, some or all of which they typically secure under wholesale agreements from the Infrastructure Carriers.

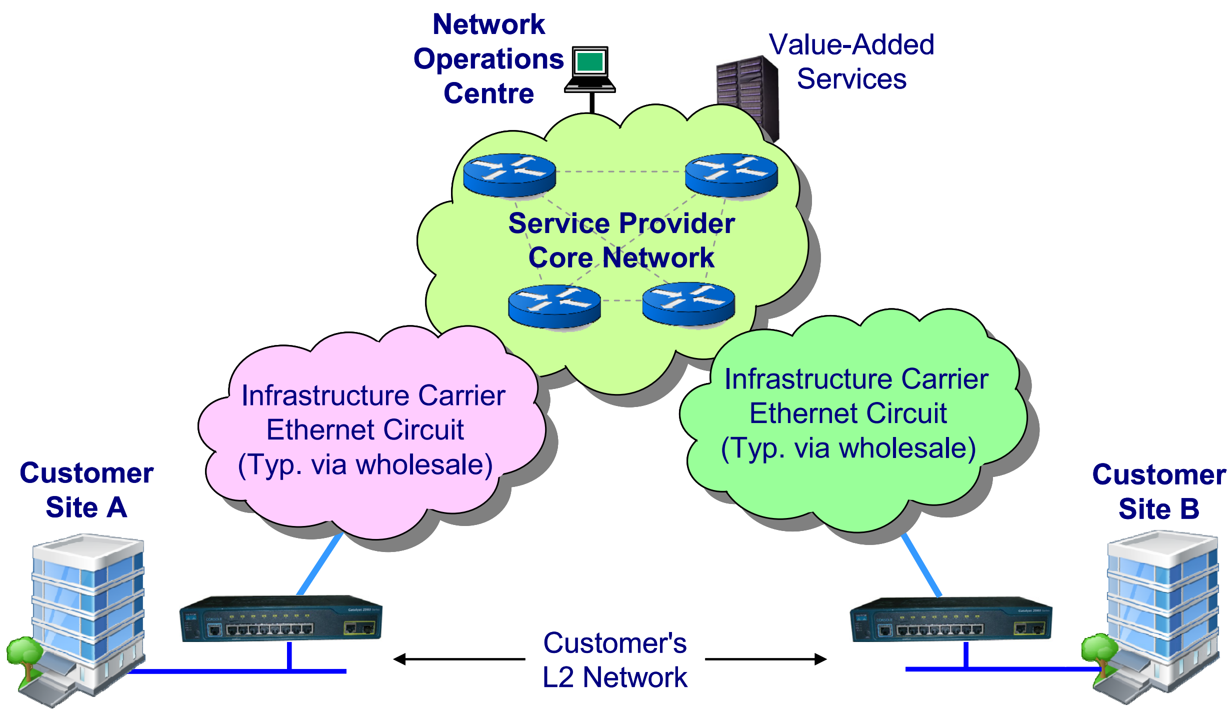


Fig. 1: Typical Ethernet Service Provision model, within which Service Providers may exist in separation from Infrastructure Carriers, from whom they acquire wholesale links

Carrier Ethernet Services

It is worth making a distinction between Ethernet Service Providers and Infrastructure Carriers, albeit that particularly in the case of the large National Providers, they may well be the same entity. The point here is that the Service Provider more often than not acts in the role of 'Aggregator', piecing together an end-to-end connectivity solution for their customers from elements of their own Core network, on which their value-adding services are based, and long or short-haul (i.e. 'tail') circuits from other Infrastructure Carriers.

This paper examines the challenges of Management of end-to-end network connections experienced by Ethernet Service Providers and looks at how the use of cost-effective, manageable Ethernet Demarcation Devices can help them to meet those challenges.

Backgrounder

It will not be a surprise to hear that much has changed over the past quarter century in the range and nature of the Telecommunications Services offered by Carriers to Corporate customers. In reality though, much of the change in Wide Area Networking (WAN) services has occurred in a rather compressed timescale relative to the evolution of the Local Area Networking (LAN) services used within customer premises, at least in terms of speed if not so much of the underlying technology.

With the advent of Ethernet in the mid 1980s, Corporates have (with a few distractions along the way) kept their faith with Ethernet in the LAN through a continual evolution process, which has seen Ethernet progress rapidly from a 'shared' 10Mbps bandwidth environment to the relatively common 'per-port' Switched 1Gbps and 10Gbps Ethernet services of today.

In contrast, Wide-Area Network (WAN) bandwidths and technologies remained relatively static for long periods over the past 25 years. Even as the relatively much faster Ethernet Corporate LAN environment progressed, WAN services, barriered by Routers, evolved independently and at a slower pace.

Over the past ten years, and in particular the past five, this picture has started to change dramatically. During the ten-year timeframe, there has been an inexorable evolution from SDH-based to so-called 'Next Generation' packet-based core switching in Carrier networks. Whilst SDH is still very much at the heart of many Carrier networks most, if not all, no longer invest in any development of their SDH infrastructure and look to their emerging Packet-based networks for development. In general, Next Generation packet networks have used IP/MPLS switching at the core and the choice of many Service Providers has been to offer 'Managed IP' network services across these platforms.

Over the past five years, the ubiquity of Ethernet in the LAN, driven not only by its connection speed but also by its relative simplicity, has led the Telecoms Carrier community to start to offer WAN services based on Layer-2 Ethernet connection, enabling Corporates to use largely the same familiar technologies in both LAN and WAN. Whilst 'Ethernet over SDH' services have emerged, extending the return of investment by the traditional infrastructure Carriers in their SDH core switched networks, for the majority of newer entrants, leveraging their MPLS switched core platforms to offer layer-2 point-to-point VPN and VPLS multi-point connectivity services has become an increasingly significant part of their service portfolio.

Coming right up to date, the diverse manner in which Ethernet WAN services are delivered today is something of a minefield of complexity, with several core network architectures being used, often championed by competing Network Equipment Manufacturers. A debate about the different WAN technologies underpinning the transport of Ethernet services today might invoke a deeply technical foray into the relative merits of;

- Ethernet over SDH / SONET, typically today via GFP encapsulation with VCAT
- Ethernet over MPLS, via Point-to-Point L2 VPN or VPLS Pseudowire tunnelling
- Ethernet over Carrier-Ethernet Transport (CET)

The last of these, and the most recent, might itself lead to a sub-debate over the merits of alternative approaches such as 'MPLS-TP' and 'PBB-TE' which is beyond the focus of this paper.

If this may sound a little bewildering, there is a similarly varied approach to the so-called 'last-mile' delivery of Ethernet services, i.e. between 'local' Carrier exchanges and customer premises.

In this area, amongst the transport mechanisms in regular deployment are;

- Ethernet over both Passive (i.e. PON) and Active Fibre
- Ethernet over TDM services, including single or multiple 'bonded' SDH/PDH circuits
- Ethernet over multiple bonded 'telephony' grade copper wiring
- Ethernet over cable-modem (Co-ax) infrastructure

Increasingly, these Ethernet services are being used not only for Data, but also for Voice, i.e. for the delivery of VoIP 'SIP' Trunks directly to the modern generation of Corporate IP-PBX Servers.

One of the main challenges to Ethernet as a delivery vehicle for Corporate Voice and Data services is that, unlike its SDH predecessor, Ethernet is not intrinsically deterministic, nor does it carry, at least by default, clock synchronisation signalling for Voice and other services, so it is not sufficient simply to provision an end-to-end Ethernet network connection safe in the knowledge that any underlying architecture will assure the performance of the link for a given customer application. Verification of the integrity of the circuit is set to become an important aspect of Carrier Ethernet implementation.

Ethernet Demarcation Devices, otherwise known as Network interface Devices (NIDs) are being deployed by Carriers as a manageable interface between the edge of their network and their customers' switched Ethernet LANs.

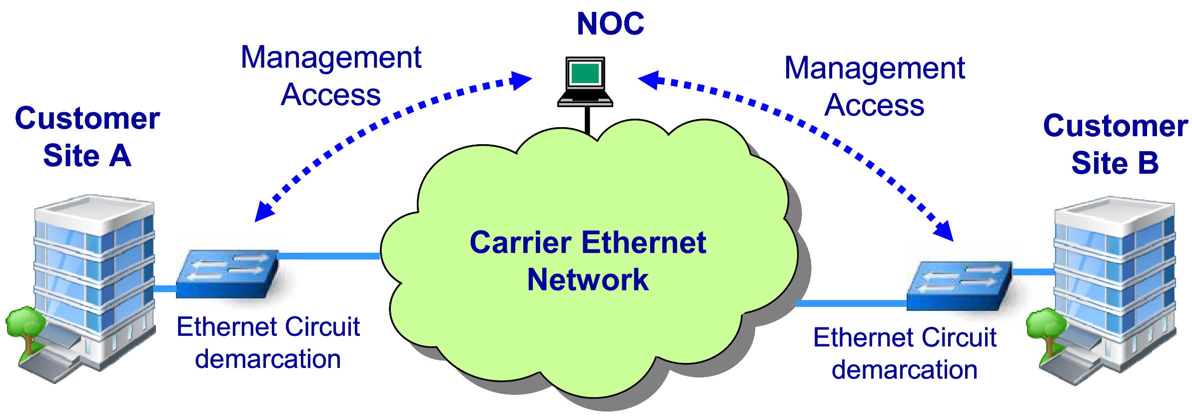


Fig. 2: Deployment of Ethernet Demarcation Devices (EDDs) for end-point management

Increasingly, Corporate clients are asking of their Ethernet Service Provider not just that they provide a certain bandwidth of connection, but that they demonstrate, both at the time of network provisioning and on an ongoing basis during in-service use, that they are meeting specific 'Service Level Agreement' (SLA) conditions. To add further complexity, the customer SLA may not relate to the singular 'pipe' of the Ethernet connection, but may indeed relate to a number of distinct service 'flows' within the pipe, such as VoIP, Video or Internet Data traffic, for which markedly different service parameters may apply.

Management Challenges for the Ethernet Service Provider

For the Ethernet Service Provider, the management of customer end-points may be a challenge. As National Telecommunications Services worldwide undergo deregulation, opening up to an ever-increasing number of Service Providers, more and more often a Customer's Service Provider is not itself, either wholly or partially, an Infrastructure Carrier, but acts as an 'Aggregator', deploying Infrastructure Networks acquired on a wholesale basis for either for long-haul circuits, local 'last mile' access, or both.

Typically, although Infrastructure Carriers may have their own manageable circuit end-points, they do not typically grant management access to these devices to wholesale customers. Unless the Service Provider has their own manageable entities at the customer premises they may not be able, without sending an Engineer to site, to be certain either that an effective connection is made to the customer network, or that the Infrastructure Carrier's circuit is fully configured and operational. In short, they have little or no customer premise or 'end-to-end' circuit visibility. This scenario is illustrated in fig. 3 below.

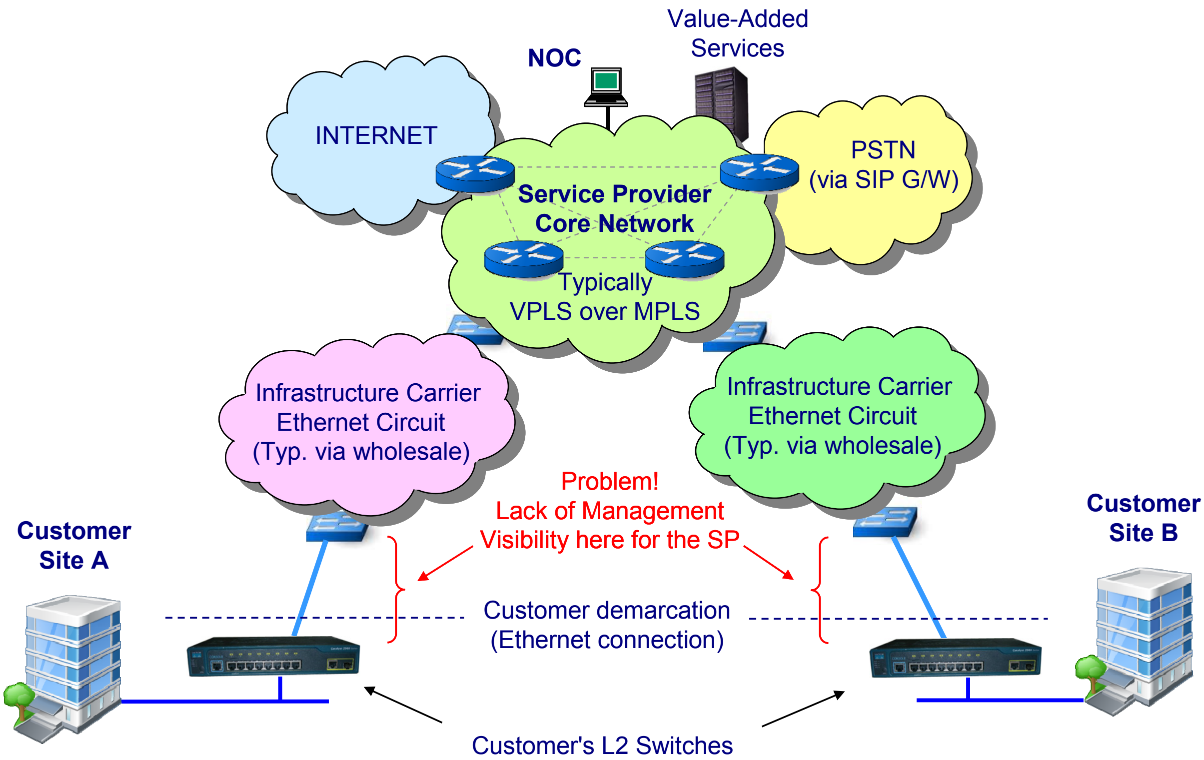


Fig. 3: The Ethernet Service Provider may only have visibility to customer connections and the end-to-end network path by deployment of their own managed Ethernet Demarcation Devices

By introducing their own manageable Ethernet Demarcation Devices, the Service Provider gains management visibility to the end-points of the network, between Carrier 'tail' circuits and the Customer LAN.

One requirement for the Service Provider is to keep their own management traffic separated from that of their Customer(s). This is normally achieved via the use of a dedicated VLAN for Network Management, within which typically resides the management tools and platforms associated with the Service Provider's Operations Centre (NOC). It should be possible to terminate a given management VLAN within the Demarcation Device at the customer premises, in such a manner that management traffic does not propagate through the customer facing network port(s) of the device. The management VLAN itself may be designated either via a dedicated 'carrier-class' Q-in-Q S-Tag or alternatively, for less convoluted multi-Carrier networks, via a more conventional customer C-Tag designation, which requires the Service Provider to ensure that the customer itself does not use the same VLAN designation for their own traffic separation and/or prioritisation purposes.

Management visibility Vs. Performance assurance

In order to provide a degree of Management visibility at the customer premise, only a limited capability is required for Ethernet Demarcation Device functionality. The Service Provider requires to 'see' beyond any demarcation device deployed by their 'tail circuit' infrastructure carrier, with the ability both to report on connectivity both towards the network and similarly towards the customer's switched LAN environment. In general, switch-based demarcation devices, supporting VLAN/prioritisation and software-based management functionality, accessible via SNMP and/or a command-line interface via Telnet, can be sufficient. This scenario is illustrated in Fig. 4 below:

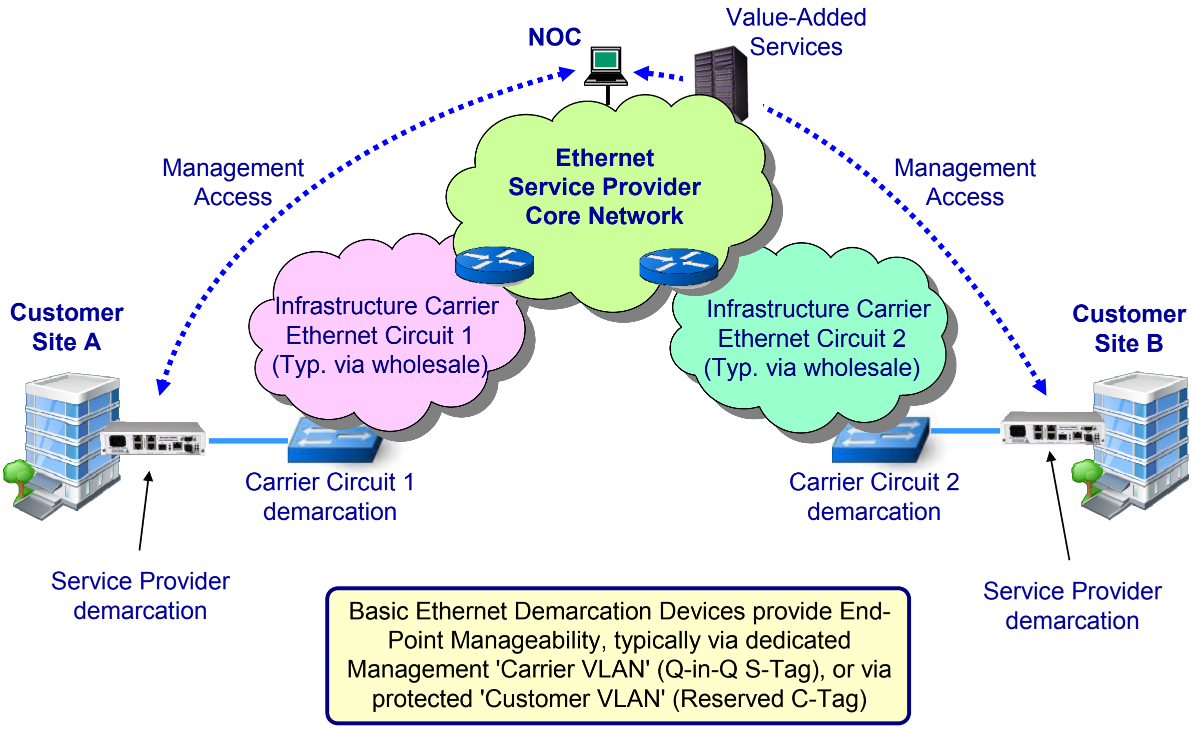


Fig. 4: Basic end-point management via cost-effective Ethernet Demarcation Devices such as the Metrodata FCM8000

In recent times, support for various degrees of Carrier Ethernet 'Operations, Administration and Management' (OAM) protocols has been promoted, mostly via the auspices of the 'Metro Ethernet Forum' (MEF), which is active in the promotion of Carrier Ethernet Services.

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 to the core of the 802.3 standard itself.

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

Above and beyond connectivity management though, customers are increasingly asking 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 parameter, including latency and delay variation (a.k.a. 'jitter').

In a more advanced deployment, a Service Provider may need to provision multiple services per physical Ethernet connection. They may then be faced with the challenge to demonstrate to their customer, at the time of provisioning, that specific 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 should be verified.

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

Ethernet Demarcation Devices equipped with more 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 Management console, 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, this can be highly beneficial. Such test stream(s) can enable accurate reporting of throughput, packet loss, latency and delay variation, for the end-to-end network link. Demarcation Devices with such capabilities are now emerging. 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 Service-OAM protocols, this time the ITU-T's Y.1731 suite, relates to the ability to provide in-service testing and reporting of SLA compliance, which a number of vendors refer to as 'Performance Assured Ethernet' (PAE). Fig. 5 below, indicates the use of advanced Ethernet Demarcation Devices, such as the Metrodata FCM9004, for SLA verification:

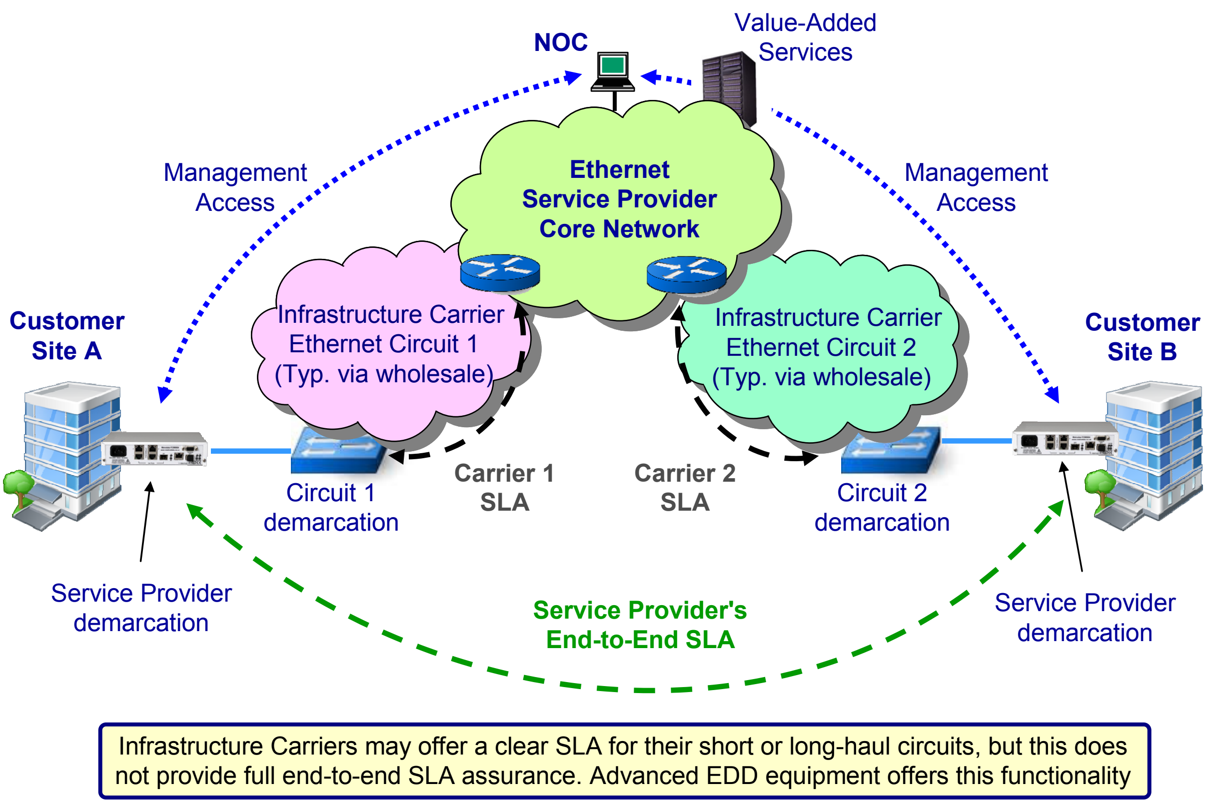


Fig. 5: Performance Assured Ethernet with Customer SLA verification via Advanced Ethernet Demarcation Devices, such as the Metrodata FCM9004.

Metrodata Ltd Ethernet Demarcation Devices

For basic managed Demarcation applications, Metrodata offers the FCM8000 & FCM9000 products, members of the popular family of 'MetroCONNECT' Ethernet Service Access and LAN Extension solutions.

The FCM8000 and FCM9000 provide the following common features:

- 10/100Mbps or 1Gbps Service Delivery:
- Copper or Fibre network port, Copper or Fibre user port
- VLAN tag-switching (802.1q) & prioritisation (802.1p) with Q-in-Q support
- IEEE 802.3ad with LACP support and RSTP for link resilience
- Per port traffic Policing/Shaping
- Jumbo Frame Support (10k byte)
- Management via Console port, Telnet, SNMP & Carrier E'net OAM (802.3ah, 802.1ag CFM)
- Service Provider's Management traffic isolation via designated VLAN
- Link loss forwarding
- Zero-touch provisioning in association with other MetroCONNECT family members
- TACACS+ & SSH for secure authentication & access

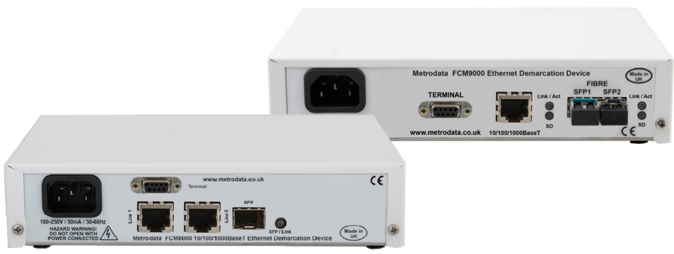


Fig. 6: Metrodata FCM8000 (front) and FCM9000 (rear) Managed Ethernet Demarcation Devices

For advanced applications, enabling the Service provider to provision and validate end-to-end Ethernet Performance, Metrodata offers the FCM9004 product. This product offers Copper (RJ45) or Fibre (SFP) Network Connection up to 1Gbps and up to 4x RJ45 & 1x SFP/Fibre LAN Connections up to 1Gbps.

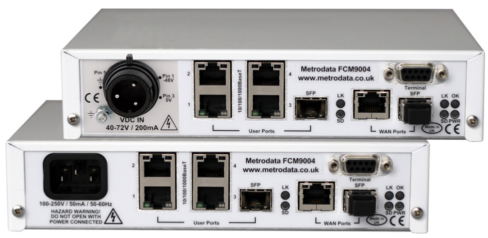


Fig. 7: Metrodata FCM9004 Advanced Managed Ethernet Demarcation Device

In addition to the features of the more basic managed devices, the FCM9004 offers:

- Advanced VLAN Traffic Mapping & Q-in-Q handling
- ITU-T Y.1731 for in-service performance monitoring
- Core-Edge and End-End Network SLA verification capabilities, including:
- Embedded wirespeed test traffic generator with packet time-stamping
- Layer 2/3 SA/DA Loopback for assurance measurement over extended networks
- Embedded wirespeed SLA calculation & reporting tools

- Dedicated hardware Service Assurance Module, 'MetroSAM', ensuring effective SLA measurements for wire-speed applications to 1Gbps, including:
- Sophisticated provisioning and in-service measurement tools
- Throughput, Frame Loss, Frame Delay and Frame Delay Variation analysis
- Multiple traffic flow characterisation

A typical (simplified) scenario for deployment of the FCM9004, illustrating test-traffic generation and loop-back during initial circuit provisioning, is represented in Fig. 8 below:

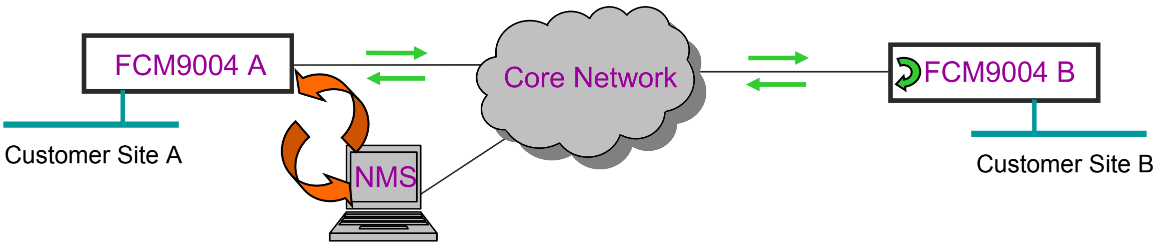
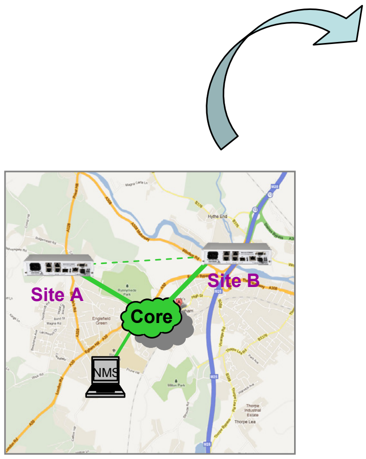


Fig. 8: FCM9004 SLA Verification during initial circuit provisioning

In this scenario, under control from the Service Provider's Network Management console, FCM9004-A is instructed to instigate loop-back at corresponding end-point FCM9004-B and then to generate and launch a test traffic stream (or streams) towards FCM9004-B. Using accurate time-stamping and wire-speed computation, FCM9004-A can provide a detailed analysis of traffic compliance Vs. the customer's required SLA with respect to throughput, packet loss, circuit latency and latency variation (jitter) per traffic flow for the A-B connection, as illustrated in fig. 9 below. Thereafter, during in-service use, 'background' test-packets are exchanged (using mechanisms of the Y.1731 S-OAM protocol) to continually monitor SLA adherence, alerting the Management Console to any potential breach of required performance levels.



Typical Management Screen Presentation

SLA Verification Testing / Circuit Provisioning

A-end: "Site A" **B-end:** "Site B" **Test Traffic Type:** L2, MAC Addr Loop-back

Traffic Parameters	**Stream 1**	**Stream 2**	**Stream 3**	**Stream 4**
Traffic Category:	Real-Time	High Priority	Best-Effort	Best-Effort
EVC Number (S-Tag):	100	100	100	100
VLAN Number (C-Tag):	101	102	103	104
Frame Size (Byte):	250	250	1000	10000
Committed SLA				
CIR (Mbps):	100	10	0	0
CBS (Bytes):				
EIR (Mbps):				
EBS (Bytes):				
Colour Mode:	Blind	Blind	Blind	Blind
Frame loss (%):	<0.05	<0.001	N/A	N/A
Frame delay (µs):	<300	<5000	N/A	N/A
Frame delay variation (µs):	<100	<2000	N/A	N/A
Test Results				
Throughput (Mbps):	100	10	10	80
Lost frames (%):	0.0250	0.0005	0.0100	0.0250
Average frame delay (µs):	100	1000	5000	10000
Frame delay variation (µs):	10	100	250	1000
Pass/Fail	**Pass**	**Pass**	**Pass**	**Pass**

Fig. 9: FCM9004 SLA verification report for end-to-end circuit Site A - Site B

Carrier Ethernet Services

Summary

Infrastructure Carriers and Telecoms Service Providers alike see advantages in the provision of end-to-end Layer-2 Ethernet connectivity as a solution to their clients' connectivity needs. Some of the advantages of Ethernet, Vs. the current generation of largely 'Managed Router' services are:

- Lower provisioning complexity, no need for IP address schema
- Lower costs: Fewer Routers, lower cost CPE & lower complexity
- Lower network latency
- Protocol-agnostic network
- More rigorous QoS with precise end-to-end service levels in terms of throughput, loss, latency and jitter
- Scalable bandwidth
- Evolution flexibility: Core network may transition from MPLS/VLPS to pure Ethernet Transport (e.g. PBB-TE, MPLS-TP) with little or no impact on customer connection configuration

Whilst Infrastructure Carriers utilise their own manageable end-points for the link-services which they provide, Service Providers generally require their own manageable Demarcation devices if they are to be able to ensure even the most basic of management visibility, both towards their customers' LAN connection point and towards their Wide-Area network infrastructure provider's termination point.

By using advanced, and increasingly cost-effective Demarcation Devices, such as the FCM9004 from Metrodata, the Service Provider is potentially able to gain a high degree of Performance Assurance in relation to their customers' end-to-end Ethernet networks. By deployment of Demarcation Devices based on architectures incorporating custom packet-processing hardware for the generation of test-traffic, loop-back and data collation, the Service Provider can verify, both at the time of circuit provisioning and subsequently in-service, that their service meets stringent SLAs increasingly being demanded by their customers. Such SLAs may relate not only to the Ethernet service 'pipe' between sites, but to multiple traffic streams, of different types and potentially demanding different levels of performance in relation to the key parameters of throughput, packet loss, latency and jitter, contained within the service pipe.