Draft NICC ND 1611 V2.2.2 (2008-08)

NICC Document

Multi-Service NGN Interconnect Common Transport

Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London,
SE1 9HA.

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London SE1 9HA.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC.

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC.

Introduction

This specification forms part of the Next Generation Network, Multi-Service Interconnect Release Structure and should be read in conjunction with the associated releases of the standard Next Generation Networks, Release Definition [1].

1 Scope

The present document defines the common transport function for supporting multi-service interconnects between Next Generation Networks within the UK. This document defines the functional architecture for the common transport and specifies the protocols and interfaces that support TDM, ATM and managed IP type services on the same transmission.

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ND1610 Next Generation Networks, Release Definition

[2] SR 001 262 ETSI drafting rules Section 23:- Verbal Forms For The Expression Of Provisions

[3] ND1125 SDH INTERCONNECT BETWEEN UK LICENSED OPERATORS, TECHNICAL RECOMMENDATION

[4] ND1122 INTERCONNECT BETWEEN UK LICENSED OPERATORS, BASED UPON PERMANENT ATM CONNECTIONS, TECHNICAL RECOMMENDATION NICC

[5] IEE 802.1ah Provider Backbone Bridges, Draft

[6] IEE 802.3 Local and metropolitan area networks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 2002

[7] IEE 802.1Q Virtual Bridged Local Area Networks, 2003

[8] IEEE 802.3ad Aggregation of Multiple Link Segments (Now part of 802.3), 2002

[9] IEEE 802.1ad Draft Standard for Local and Metropolitan Area Networks-- Virtual Bridged Local Area Networks-- Amendment 4: Provider Bridges, 2005

[10] IEEE 802.1D Virtual Bridged Local Area Networks, 2003

[11] ITU-T G.811Timing characteristics of primary reference clocks, 1997-09

[12] IEEE 802.3ae Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 2005

[13] IEEE 802.1w Part 3: Media Access Control (MAC) Bridges: Rapid Configuration (Now part of 802.1d - Media Access Control (MAC) Bridges 2004), 2001

[14] IEEE 802.1ag Draft Standard “Connectivity Fault Management”, 2005

[15] ITU-T G.7041 Generic Framing Procedure, 2005-08

[16] ND1614 Management of the General Connectivity of PSTN/ISDN Service Interconnect for UK NGNs

[17] ND1612 Generic IP Connectivity for PSTN / ISDN Services between UK Next Generation Networks

[18] IETF draft-ietf-bfd-v4v6-1hop-08.txt BFD for IPv4 and IPv6 (Single Hop), Draft See Annex E

[19] IEEE 802.1Qay Provider Backbone Bridge Traffic Engineering, Draft

[20] IETF RFC792 INTERNET CONTROL MESSAGE PROTOCOL, Sep 1981

[21] ITU-T G.7042 Link capacity adjustment scheme (LCAS) for virtual concatenated signals, 2001-11

3 Definitions, symbols and abbreviations

The key words "**shall**", "**shall not**", "**must**", "**must not**", "**should**", "**should not**", "**may**", "**need not**", "**can**" and "**cannot**" in this document are to be interpreted as defined in the ETSI Drafting Rules [2].

3.1 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
CBR	Constant Bit Rate
CC	Connectivity Check
CFM	Connectivity Fault Management
CP	Communications Provider
CSFF	Client Signal Fail Frame
CTF	Common Transport Function
CTFI	Common Transport Function Interface
ETSI	European Telecommunication Standards Institute
FDI	Forward Defect Indicator
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical & Electronic Engineers
IP	Internet Protocol
IPG	Inter-Frame Gap
ITU-T	International Telecommunication Union - Telecoms
GFP	Generic Framing Procedure – ITU-T G.7041[15]
LCAS	Link Capacity Adjustment Scheme
LoS	Loss of Signal
MAC	Medium Access Control
MTU	Maximum Transfer Unit
NGN	Next Generation Network
OAM	Operations Administration and Maintenance
PCP	Priority Code Points
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SFD	Start of Frame Delimiter
TDM	Time Division Multiplex
VC	Virtual Circuit
VLAN	Virtual Local Area Network

4 Common Transport Function (CTF)

The NGN interconnect that supports multiple services is built around a common, multi-purpose transport function that provides a number of transport capabilities via two transmission technologies. This common NGN Interconnect transport function is represented in Figure 1 which shows the transport function (fB1) offering the following transport capabilities:

a) Internet Protocol transport
b) Ethernet transport
c) ATM transport
d) TDM transport

The transport function offers some or all of the above capabilities via the following transmission technologies:-

i) SDH (Figure 2)
ii) Ethernet Physical (Figure 3)

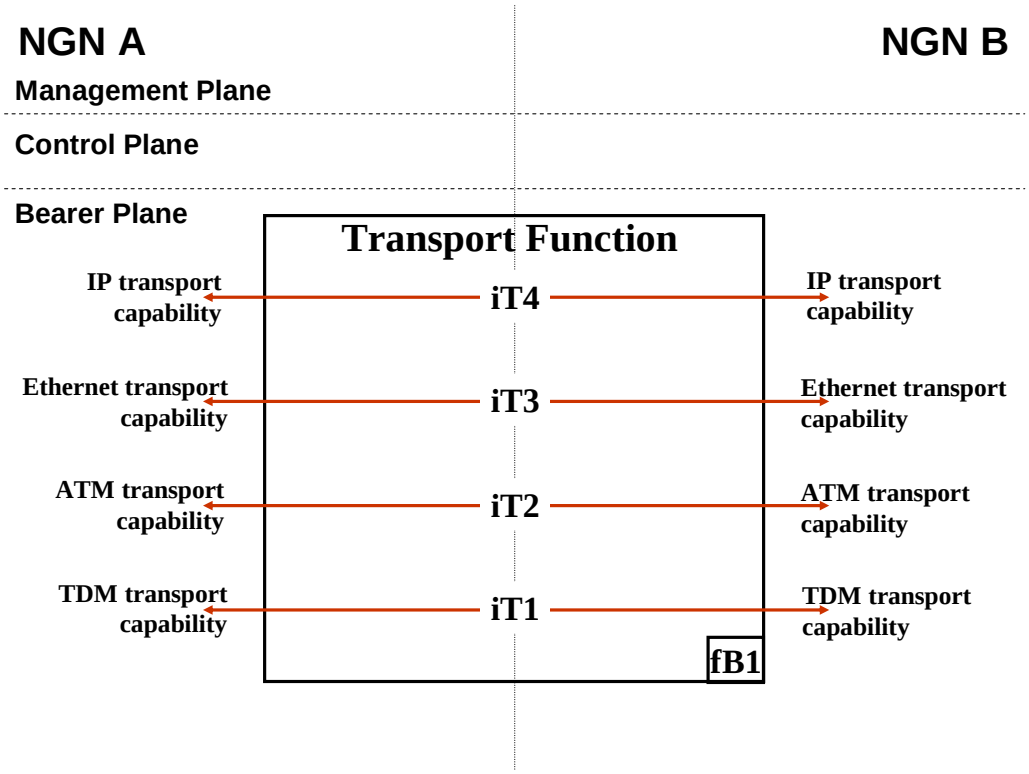

FIGURE 1: COMMON TRANSPORT FUNCTION

Table 1 gives the client network transport capability / server physical transmission technology compatibility matrix and the associated attributes.

Client Network Transport Capability	**Server Physical Transmission Technology**	**Capability Attributes**
TDM	SDH only	Bandwidth partitioned by SDH virtual container
ATM	SDH only	Bandwidth partitioned by SDH virtual container
Ethernet	SDH	Bandwidth partitioned by SDH 'n x virtual containers'. Ethernet encapsulated by GFP Ethernet VLANs each configured with fixed bandwidth, the total fitting within the underlying 'n x virtual containers' bandwidth.
Ethernet	Ethernet Physical	Ethernet VLANs each configured with fixed bandwidth, the total fitting within the underlying Ethernet physical bandwidth.
Internet Protocol	SDH or Ethernet Physical	IP service partitioned by underlying Ethernet VLAN and associated fixed bandwidth allowing IP services with overlapping IP addresses on separate VLANs.

TABLE 1: CLIENT NETWORK TRANSPORT CAPABILITY / SERVER PHYSICAL TRANSMISSION TECHNOLOGY COMPATIBILITY AND ATTRIBUTES

The transport function provides the physical termination of one or more of the transmission systems, to one or more NGNs. It also provides the framing of the transmission bit streams to provide separate virtual pipes called 'trails'.

A trail is a topological construct, which **shall** be monitored, that exists between a single (trail termination) source point and a single (trail termination) sink point, and follows a fixed network routing between these points over the lifetime of the trail (under failure-free conditions). Trails **shall** have resource (bandwidth) assigned to them. Strictly trails **shall** not reorder packets. Trails can only exist in either connection-oriented connection switched or connection-oriented packet switched mode networks. Trails do not exist in connectionless packet switched mode networks. Note that there is a 1:1 relationship between a connection and a trail in the point to point case.

From the service perspective the transport layer provides trails which have the following characteristics:-

a) Separacy at the IP protocol level, i.e. overlapping IP address spaces and packet marking schemes **may** be used on separate trails. Reachability isolation is provided by separate trails.
b) Separacy at the framing level, i.e. support of non-IP services e.g. ATM. Payload format isolation is provided by separate trails.
c) Static and policed bandwidth allocation to transport trails. Resource and performance isolation is provided by separate trails.

4.1 CTF Characteristics

The following are characteristics of the Common Transport Function (CTF) and its interfaces, as shown in Figure 1:-

a) The CTF supports multiple services. The services are clients of the CTF. The CTF **should** support multiple trails per Common Transport Function Interface (CTFI) physical port.
b) The CTF **need not** offer resilient transport.
    i. The physical transmission used by the CTF **may** offer protection.

ii. The service interconnect **may** offer a resilience mechanism e.g. the Service interconnect **may** use multiple CTFIs.

c) This Common Transport Function only provides point-to-point connectivity between communications providers.

d) The CTF **should** use one of two transport types:

Ethernet with associated bandwidth policy enforcement, where a VLAN tag can be used as a form of 'service instance identifier'. (Note - in its normal sense a VLAN is a restricted broadcast domain and is not a trail under the strictest definition of the term, but is functionally equivalent for the purposes of this interconnect on a point-to-point basis only if resource (bandwidth) is assigned to the VLAN and is monitored with OAM. A VLAN can therefore serve as an instance of a trail in the context of this interconnect specification.) The term “VLAN trail” will be used in this specification where the VLAN trail is a monitored point-to-point construct with reserved bandwidth.

SDH Virtual Containers.

e) The CTFI encapsulation and its labelling scheme **shall** transparently transport the services.

f) It **shall not** be possible for a communications provider to impersonate another communications provider by using incorrect labels.

g) Trails & labels (including VLAN tags) **must** be statically provisioned (i.e. not dynamically signalled). LCAS [21] **may** be used by the CTF by bilateral agreement to adjust the capacity of the SDH VCs.

4.2 Prohibited Connectivity

The following connectivity is specifically prohibited:-

a) Trails from the same physical port of the border function that go via different physical instances of the CTF **shall** be prohibited.

b) Border Functions **shall not** behave as intermediate CTF switches. That is trails **shall** start and terminate on a border function and **shall not** transit an intermediate border function.

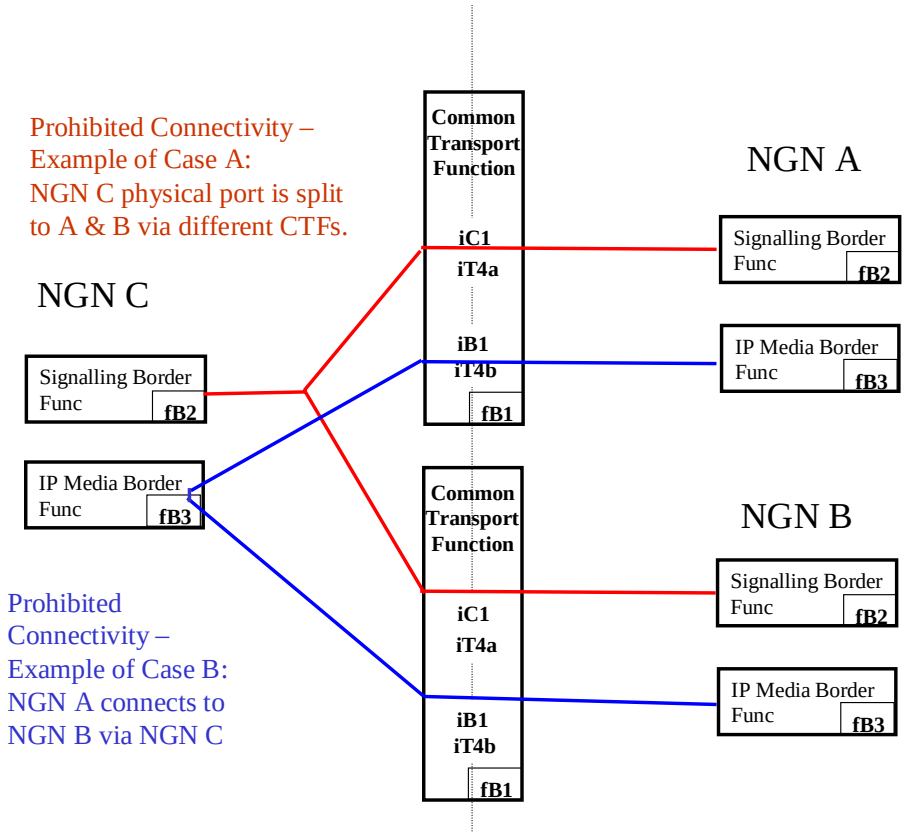

FIGURE 2: EXAMPLES OF PROHIBITED CONNECTIVITY CASES

4.3 Guaranteed Bandwidth and QoS for the Services

Each trail **shall** be constrained to a specified peak-rate to prevent contention for bandwidth (also known as bit-rate) between trails. Bandwidth sharing between trails **shall not** be permitted.

Note:

- Suitable mechanisms for bandwidth limiting are policing or shaping. Shaping is useful as a mechanism to modify the traffic profile (i.e. bandwidth & burst characteristics) of a trail without necessarily imposing discard (i.e. smoothing out bursts), while policing maintains traffic within a specified bit-rate profile, dropping packets if necessary to do so.
- Both policers and shapers are generally characterised by both a sustainable mean bit-rate and burst (bytes) parameters. A token-bucket formulation is commonly used to describe and specify behaviour. The integration period for measuring the mean bit rate (token bucket size) **shall** be agreed on a bi-lateral basis.
- The approach of using a CBR profile across the CTFI greatly simplifies the QoS implementation, reduces the risk of error, and eases fault detection.
- The maximum MTU present within any trail has a bearing on worst-case delay and jitter experienced by other trails.
- The default maximum MTU size **shall** be 2000 bytes, excluding IFG, Preamble and SFD. (This aligns with proposals within IEEE Frame Expansion Task Force IEEE 802.3as.)

4.3.1 Management of Delay and Jitter for Critical Services

Delay and jitter management on the traffic egress point from one NGN to another NGN across the CTF **should** be the responsibility of the transmitting NGN. (It is an extension of overall responsibility for meeting performance requirements for each service, which covers the rest of the NGN.)

Note - Where stringent requirements exist for delay/jitter for particular services carried across the CTF, the approach described above of individually peak-rate limiting VLAN trails is not always sufficient. In some scenarios, transient contention between peak-rate limited VLAN trails on the CTF itself can give rise to levels of delay/jitter that may be deemed unacceptable. Aggravating combinations of factors are: (i) CTF aggregate speed below a certain level, (ii) mixture of services including jitter-sensitive and data-oriented services, (iii) large maximum MTU for data traffic, (iv) traffic carried on relatively large number of separate VLAN trails and (v) a desire to obtain high overall utilisation across the CTF.

In a mixed-services environment, prioritisation via multiple queues scheduling **may** be used to reduce jitter for a selected subset of the traffic. (Prioritisation is most effective when either the average packet-size or traffic-volume of the prioritised traffic is significantly smaller than for the other traffic.)

Each NGN CP **shall** consider applying prioritisation (or other multiple queues scheduling technique to achieve prioritisation) for traffic injected across CTF. QoS scheduling **may** be used without direct agreement or negotiation of details with the connecting NGN.

Refer to ND1613 [16] for guidance on prioritisation and scheduling.

4.3.2 Definitions and Parameters That Must Be Exchanged Between Connecting CPs Across the CTF

4.3.2.1 Bandwidth Definitions for Services Carried

Information on bandwidth definitions is contained in ND1613 [16].

4.3.2.1 Design Rules Constraining VLAN Trail Bandwidth Across CTF

No bandwidth contention exists between VLAN trails.

CPs **should** refer to the definition of bandwidth given in ND1613 [16]. Since the bandwidth definition does not include the Ethernet overheads associated with Preamble, SFD and IFG, an additional allowance **must** be made for these rather than simply ensuring the sum of VLAN trail sizes is less than the nominal CTF speed.

This amounts to the need to estimate the total bandwidth consumed by all VLAN trails on the CTF, including additional bandwidth equivalent to 20bytes per frame (For the IFG, Preamble and SFD,) and comparing this bandwidth to that available.

CPs **may** choose to limit the total bandwidth thus derived to a value somewhat less than make the upper limit lower than the available CTF bandwidth, for example, theoretical maximum as part of a delay/jitter management strategy. This is to accommodate correlation in traffic peaks with a specific service instance and between different service instances. Each CP NGN **must** provide clear information on how such constraining rules should be applied to the CTF.

If different connecting CPs implement different rules, the most stringent rule across the common CTF **should** be adopted.

Additional rules on VLAN usage may be applied on a per-service basis and are contained in service architecture documents and associated management guides, e.g. ND1612 [17] and ND1614 [16] for PSTN/ISDN services.

4.3.2.3 Parameters for Ingress Policing

Policing is commonly specified by means of a token-bucket formulation, i.e. a combination of a rate (bits/s) and a burst-size (bytes). CPs **may** apply policing on a per-VLAN trail basis at the ingress to their network, but if they do so, the police rate **must** be greater than or equal to the VLAN trail rate, properly taking into account precise bandwidth definitions. In addition, the maximum tolerable burst-size **should** be greater than that reasonably to be expected for the service carried, and **must** be specified.

Burst behaviour is a complex area that is not well understood, especially for interconnection involving multiple concatenated networks. Taking account of this, guidance for burst tolerance is given here, based on a generous assessment of what is likely to be sufficient in practice for any service:

Burst-tolerance (bytes) = 0.03(s) x VLAN-trail-rate (bits/s)/8

This does not preclude CPs choosing to specify a different burst-tolerance. This may be on a per-service basis if preferred.

4.3.2.4 Controlling the Egress Traffic Profile

CPs **must** ensure VLAN trail egress traffic conforms to the VLAN trail rate and agreed burst size parameter specified for ingress to networks to which they connect. Meeting this requirement for some services **may** require CPs to implement either policing or shaping, though it should be noted that shaping is likely to be preferable for many non-RT application traffic types. For other services this traffic-conformance requirement may be met naturally as a result of fundamental features of the service. An example of this is PSTN, where correctly-applied session-control limits the rate to within the police rate, while the burst-sizes which may be estimated by statistical queuing theory, should be significantly smaller than the values specified by the above formula. Even for such services CPs **may** apply policing or shaping as a precautionary measure, for example to protect other services or VLAN trails in event of a deviation from normally expected behaviour (such as due to a failure of session-control for PSTN).

CPs should be aware that unless the shaper itself has sufficient burst-tolerance, it may lead to the imposition of jitter on individual sessions carried on the VLAN trail, which may be significant for some services. As a consequence, where strict shaping is applied, a design rule is likely to be needed for the most jitter-critical services to constrain the maximum utilisation within a trail to less than 100%, so as to limit the magnitude of any imposed delay variation, refer to ND1614 [16].

4.3.3 Use of QoS Markings

Where all traffic within a trail requires the same QoS treatment across the CTF, it **shall not** be necessary for QOS markings to be part of the CTF specification.

Where each trail consists of only one traffic type, the use of QoS markings **may not** be necessary to achieve differentiation. Inspection of trail identifiers (VLAN ID) **may** be sufficient to identify two types of traffic.

Where the use of Prioritisation results in residual 802.1p or PCP markings being left on traffic egressing from an NGN, these markings **shall** be ignored in the ingress direction arriving from the CTF.

Note - It is recognised that future services may require support of multiple traffic types with different QoS requirements within the same trail, and in this case, consideration **may** be needed to providing some differentiation at packet-level

across the CTF by reference to 802.1p or PCP markings. Since a trail **shall** not re-order packets if packets within the trail are differentiated then such a construct should be called a “point to point flow”. This scenario is not considered any further in this document.

4.4 Transport Services Protocol Stacks

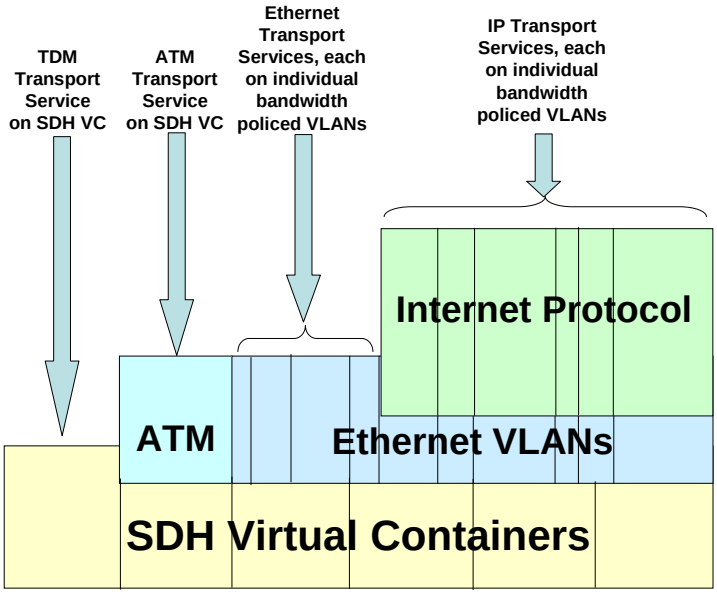

FIGURE 2: TRANSPORT SERVICES SUPPORTED BY SDH TRANSMISSION TECHNOLOGY

The dotted vertical lines in figures 2 & 3 represent the partitioning of the protocols into separate trails (including the use of VLAN trails in Ethernet in the context of this interconnect specification) by use of labels of different values.

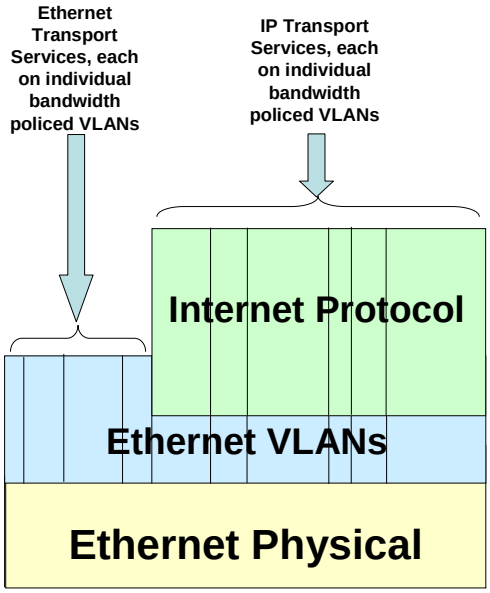

FIGURE 3: TRANSPORT SERVICES SUPPORTED BY ETHERNET TRANSMISSION TECHNOLOGY

4.5 Network Synchronisation

SDH transmission between networks **should not** provide network synchronisation**.** This is in line with the current SDH interconnect on legacy PSTNs in the UK.

For interconnects using Ethernet over fibre, there is currently no standard for conveying network synchronisation.

Unless deriving synchronisation via some other interconnect interface type, networks **should** synchronise against their own network clock that is compliant to ITU-T G.811 [11].

5 IP Transport Capability Specification – iT4

5.1 Physical Layer Options

5.1.1 Physical Interface Options

The layer 1 options for the IP transport capability are:

1. Ethernet mapped into SDH interconnect as per SDH INTERCONNECT BETWEEN UK LICENSED OPERATORS, TECHNICAL RECOMMENDATION [3] using ITU-T G.7041 [15] framed GFP.

2. 10 Gigabit Ethernet IEEE802.3ae [12] options (not mandatory):

Transceiver Type	**Wavelength**	**IEEE Standard**	**Maximum Distance/Cable Type**
10GBASE-SR	850 nm	802.3ae	300 m over 50-micron 2000 MHz*km multimode fibre
10GBASE-LR	1310 nm	802.3ae	10 km over single-mode fibre
10GBASE-ER	1550 nm	802.3ae	40 km over single-mode fibre
10GBASE-LW	1310 nm	802.3ae	(STM-64 variant WAN Phy) Single-mode fibre
10GBASE-EW	1550 nm	802.3ae	(STM-64 variant WAN Phy) Single-mode fibre

3. IEEE Gigabit Ethernet Options IEEE802.3 [6] (not mandatory):
    a. 1000BASE-SX: 62.5 um multimode fibre: up to 275 m
    b. 1000BASE-LX: 9/10 um single-mode fibre: up to 10 km
    c. 1000BASE-T: Category 5 cable: up to 100 m

5.1.2 Protection Mechanisms

When a Border Function detects or initiates a protection switching event the Border Function **shall** initiate an ARP announcement (also known as a “Gratuitous ARP”), after the protection switching event is complete, to update the ARP cache of its peers.

Note that Border Functions may not detect all protection switching events which may lead to a failure of IP connectivity of peer Border Functions until stale ARP entries have expired

SDH Multiplex Section Protection (MSP) **may** be used to provide "across the floor" protection for the SDH layer 1 interconnect option. Native Ethernet layer 1 options do not have equivalent protection mechanisms so IEEE 802.3ad [8] Link aggregation **may** be used.

5.1.3 GFP Client Signal Fail Frame (CSFF)

Where GFP is used CSFF **should** be used to indicate failure of the far-end Ethernet connectivity where:

Upon receiving a CSFF signal the SDH/GFP function **shall** "take down" (remove carrier or light) for the SDH section only if all VLANs connectivity on that section have failed.

5.1.4 Use of SDH LCAS

The SDH Link Capacity Adjustment Scheme (LCAS), standardized by the

ITU-T as G.7042 [21], is designed to manage the bandwidth allocation of

a Virtually Concatenated Group. SDH LCAS is recognised as a technique for varying the capacity of an SDH VC Group for an Ethernet client carried using GFP-F, without the need for an outage of the SDH VC Group. LCAS **may** be used across an MSI by bilateral agreement.

5.2 iT4 - Layer 2 for IP Transport Capability

"Ethernet" **shall** be the layer 2 used for IP services and the following Ethernet standards **shall** be followed:

1. IEEE 802.1Q [7] VLAN tagging. Different IP services will be placed in different VLANs. The VLAN ids **shall** be agreed on a bi-lateral basis between CPs.
2. IEEE 802.3ad [8] Link Aggregation **may** be used to provide load sharing and protection (which usually takes seconds to detect failure) (Note using 802.3ad to provide protection is not a standardised Ethernet feature.)
3. Rapid Spanning Tree Protocol (IEEE 802.1w) [13] **shall not** be used to provide protection as this is not a secure protocol to operate inter-CP.
4. IEEE 802.1p priority marking [10] **should not** be used. The CTF will be dimensioned to not drop or contend traffic at the point of interconnection. Individual operators **shall** be responsible for policing traffic onto the point to point interconnect to ensure it is not overloaded. Traffic **must** be policed per VLAN trail(i.e. per service) to ensure congestion/overload of a single service does not impact the performance of other services (assuming no overbooking). Per VLAN trail queuing **may** give the best performance isolation between services but is not a requirement.

5.3 iT4 – Failure Detection

The architecture for detection of failure of the IP transport function is shown in Figure 4. There are 3 key components to consider for failure detection:

- The physical trail. This includes the IEEE 802.3 functional components and may use SDH. The physical trail may use intermediate physical transport components of differing technologies.
- The VLAN trail. This includes the IEEE 802.1 functional components. The VLAN trail may cross intermediate Ethernet switches.
- The Service Level trail (for connection-oriented services) or monitored fragment (for connectionless services) between border functions. This is IP for iT4.

Each trail or monitored fragment **should** provide its own OAM protocol(s) to detect all the failures that are relevant to the trail or monitored fragment. The physical trail termination **may** pass proprietary Forward Defect Indicators to the VLAN trail termination and raise a management alarm signal. The VLAN trail termination **may** pass proprietary Forward Defect Indicators to the service trail termination or monitored fragment termination in the Border Function and raise a management alarm signal. The service level trail or monitored fragment termination in the Border Function may pass proprietary Forward Defect Indicators to the Application (if applicable to the application) and raise a management alarm signal. In general there are no guarantees that:

- The OAM protocol(s) will operate effectively end to end, especially in the case of the physical trail over multiple physical sections.
- That proprietary FDIs will be available.

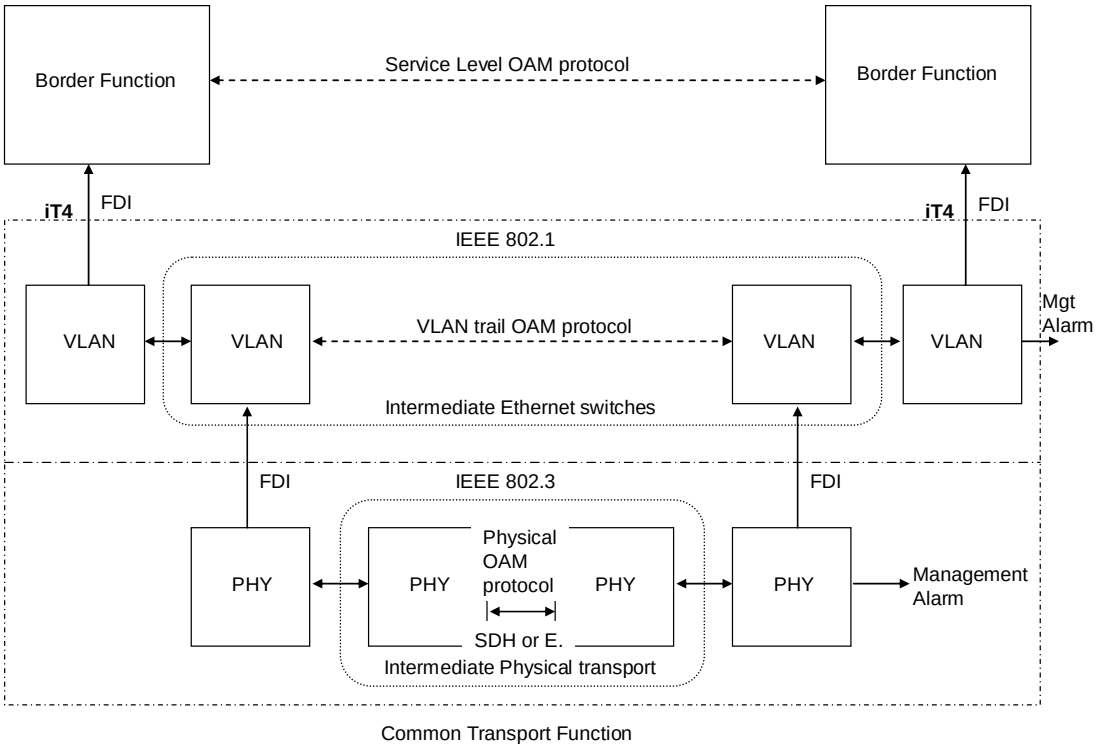

FIGURE 4: FAILURE DETECTION ARCHITECTURE

Figure 5 illustrates the recommended protocols for failure detection of iT4.

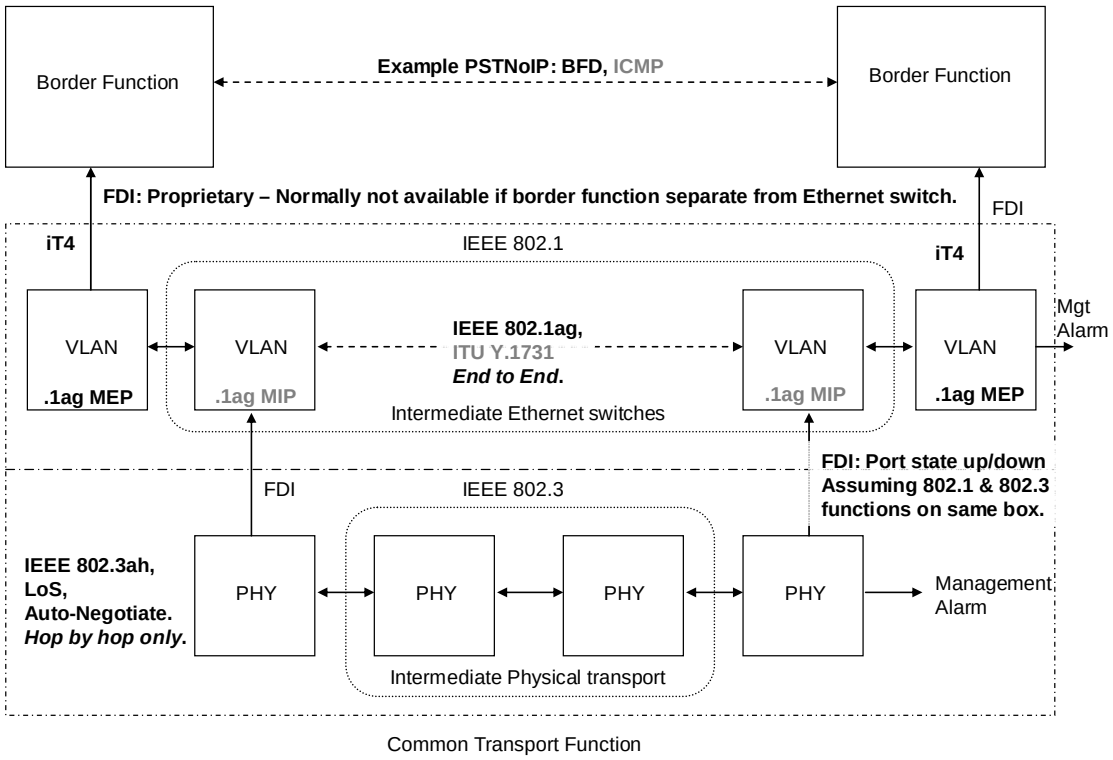

FIGURE 5: FAILURE DETECTION RECOMMENDATIONS

In order to check IP connectivity across iT4, the IP Border Functions using the IP CTF shall use BFD [18] or ICMP IP ping [20]. BFD should be used but ICMP IP ping may be used. If the Border Function is physically separate from the Ethernet switch then proprietary Forward Defect Indicators **should not** be available to the IP Border Functions from the VLAN trail functions. BFD CC rates and failure detection times **should** be determined based on the speed of any protection mechanisms implemented on the VLAN trails or physical trails i.e. client OAM **should** be slower than server layer OAM to give lower layer protection time to restore.

The VLAN trail functions **should** use IEEE 802.1ag CFM and **may** use ITU Y.1731 CC messages. The 802.1ag MEP function **should** be implemented at the VLAN trail terminations. The 802.1ag MIP functions **may** be implemented on intermediate Ethernet switches. The 802.1ag Maintenance Association Level to be used in the VLAN trail terminations **shall** be agreed on a bi-lateral basis. The VLAN trail OAM protocol **shall** provide detection of failure of the end to end VLAN trail. The CC rate per VLAN trail **shall** be negotiated on a bi-lateral basis. CC rates and failure detection times **shall** be determined based on the speed of any protection mechanisms implemented on the physical links. The VLAN trail termination function **should** raise an alarm to the management system on detection of failure. If the VLAN termination function is physically separate to the Border Function then proprietary Forward Defect Indicators **should not** be used. The VLAN trail failure detection mechanisms **may** be used to trigger VLAN trail protection when available in the future.

The physical trail functions **shall** use IEEE 802.3ah OAM and **should use** Loss of Signal and loss of IEEE 802.3 auto-negotiate signal to detect failure. Only if the intermediate physical transport is fully transparent to 802.3 signals then will the 802.3 auto-negotiate signal provide end to end detection of failure. Only if the intermediate physical transport is capable of link loss forwarding (e.g. Ethernet over SDH using GFP Client Signal Fail Frame) will Loss of Signal provide end to end detection of failure. The physical trail termination function **should** raise an alarm to the management system on detection of failure. CC rates and failure detection times **should** be determined based on the speed of any protection mechanisms implemented on the physical links.

Following the above recommendations the time taken to detect failure at a higher layer and invoke actions there will be bounded by:

- The speed of the underlying physical link OAM and protection mechanisms.
- The ability of the Border Functions to implement BFD [18].
- The ability of the management systems to trigger timely actions in the applications in response to alarms indicating failure of the transport function.

5.4 iT4 - SDH Transport Option Protocol Stack

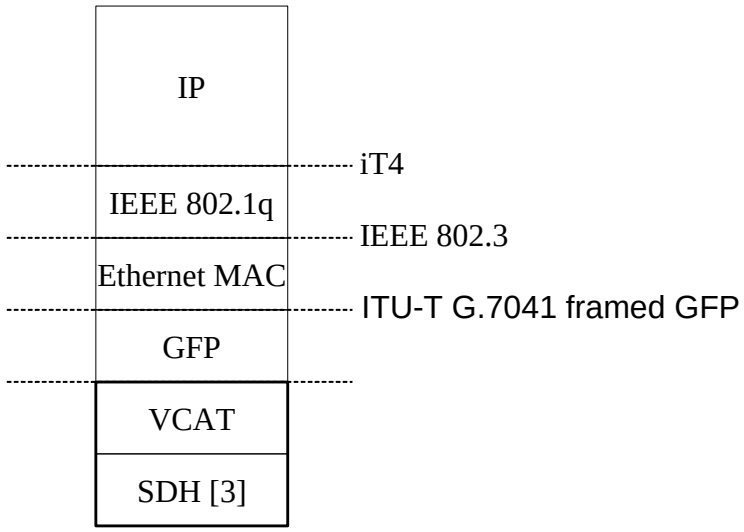

FIGURE 6: IT4 SDH TRANSPORT OPTION PROTOCOL STACK

5.5 iT4 - Ethernet Transport Option Protocol Stack

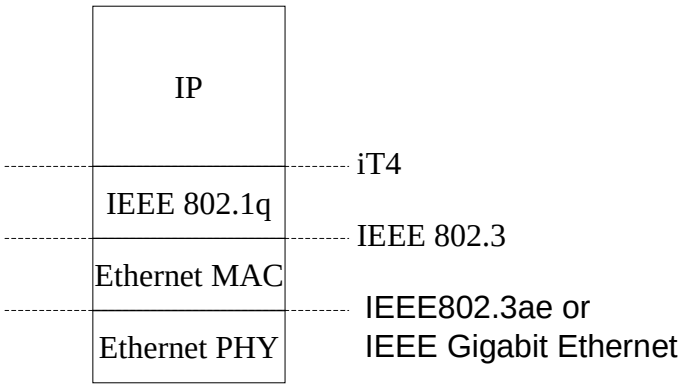

FIGURE 7: IT4 ETHERNET TRANSPORT OPTION PROTOCOL STACK

6 TDM Transport Capability– iT1

The mapping of TDM clients **shall** be as defined in SDH INTERCONNECT BETWEEN UK LICENSED OPERATORS, TECHNICAL RECOMMENDATION [3].

7 ATM Transport Capability– iT2

ATM **shall** be mapped as per INTERCONNECT BETWEEN UK LICENSED OPERATORS, BASED UPON PERMANENT ATM CONNECTIONS, TECHNICAL RECOMMENDATION [4].

8 Multi-Service Protocol Stacks

8.1 Multi-Service (iT1,2,4) over SDH Protocol Stack

Figure 8 shows the protocol stack for IP, ATM and SDH services over an SDH based transport function.

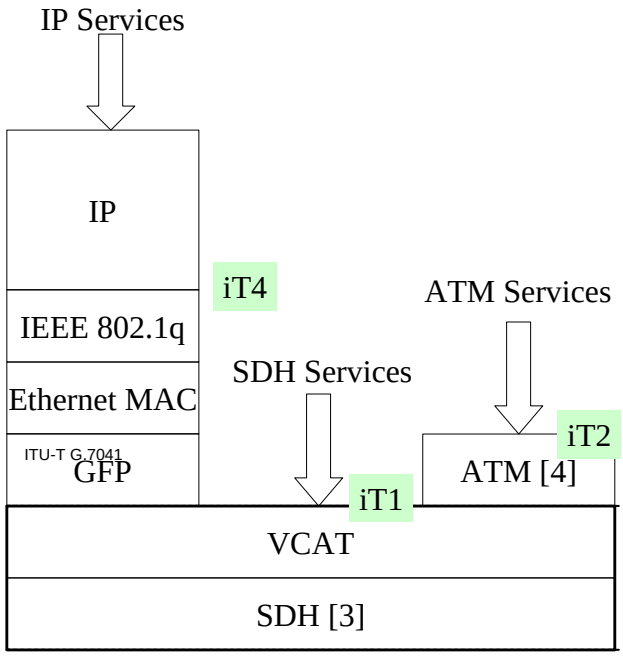

FIGURE 8: MULTI-SERVICE PROTOCOL STACK

8.2 Multi-Service (iT1,2,3,4) over Ethernet Protocol Stack

Since Ethernet standards do not yet support SDH and ATM there is no option to implement SDH or ATM over Ethernet. Only IP services **shall** be supported over the Ethernet transport function.

9 Ethernet Transport capability – iT3

This release of the NGN Interconnect common transport **shall not** support an Ethernet transport capability for Ethernet services. Later releases of this specification **may** support Ethernet services using IEEE 802.1ah [5] “Provider Backbone Bridging” or IEEE 802.1Qay [19] “Provider Backbone Bridge Traffic Engineering”.

For IP transport single tagged Ethernet frame with Ethertype 0x8100 **should** be used. For Ethernet transport double tagged IEEE 802.1ad or 802.1ah Ethernet frames **should** be used with Ethertype 0x88a8. This **may** necessitate the use of double tags and the 0x88a8 Ethertype to support IP transport on multi-service (IP & Ethernet) transport interfaces in the future.

Note that due to GFP’s limitation of an 8 bit multiplexer field it **may not** be a suitable mechanism to support future Ethernet services interconnection where each SDH VC **may** be supporting thousands of customers.

10 Security

The CTF **cannot** provide authentication or privacy for its clients (services). It is recommended that clients (services) using the CTF **should** provide their own authentication and privacy functions.

MAC filtering **shall** be implemented to prevent infinitely circulating Ethernet packets, e.g. CP A **cannot** receive CP's B Ethernet packets from CP C and CP B **cannot** route Ethernet packets to CP C via CP A.

The following protocols **shall not** be used between CPs:

1. Ethernet Spanning Tree Protocols

11 Naming, Numbering and Addressing

11.1 IP Transport Capability

11.1.1 IP Addressing

The IP addresses used by the IP client of the IP transport capability is a service specific issue which will be described in the service specific documents.

11.1.2 Ethernet VLANs Used to Provide IP Transport Capability

VLAN Tag addressing
The VLAN tag **shall** be identified by the VLAN ID (VID). Per IEEE 802.1Q, this has 12 bits, allowing the identification of 4096 VLANs within a given Ethernet network. VID values 0 and 4095 (FFF) **shall** be reserved. The maximum possible VLAN configurations **shall** be 4,094.

There **shall** be no centrally-administered VLAN-tag space for the UK, and the addressing of VLANs **shall** be done through bilateral agreement. Each interconnect point **shall** represent a separate VLAN-space, although network operators **should** give due consideration to how the VLAN separation will be maintained within their network, particularly between the Border Functions and Common Transport Function. This **may** be achieved via tag switching or physical separation.

The assignment of VLANs to interconnect relationships **shall** be service specific, with a given service requiring one or more VLANs. For example, a voice interconnection **shall** require two VLANs, one for control and one for media; if the commercial arrangements were such that each network operator owned their own capacity, this would imply that up to four VLANs could be required for the interconnect as a whole.

Annex (informative): Connectivity Examples

Figure 9 shows examples of permitted connectivity where the square boxes represent IP border functions that combine the adaptation and trail termination functions. The small circles on the square boxes represent physical ports.

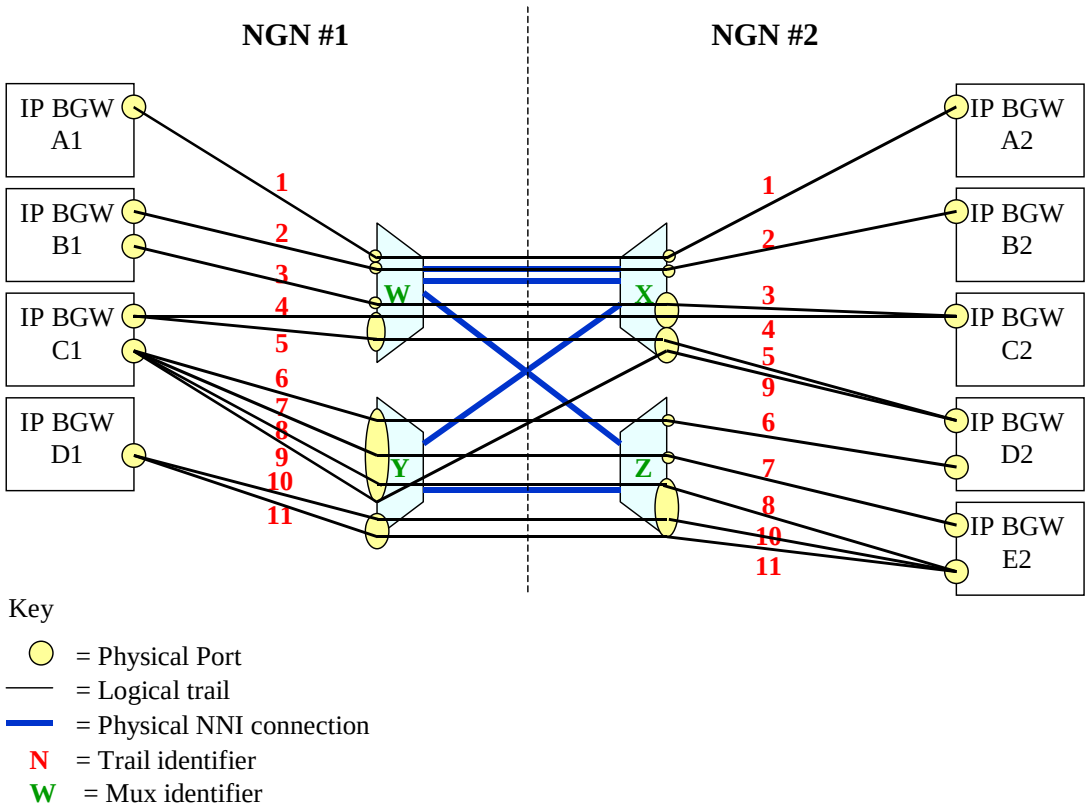

FIGURE 9: TRANSPORT FUNCTION CONNECTIVITY EXAMPLES

Annex B (informative):
iT4 - SDH Transport Option Multiplexing Hierarchy

Figure 10 shows the multiplexing hierarchy for the iB1 SDH transport Option. This shows there **may** be many IP services supported by many VLANs supported by many GFP flows etc.

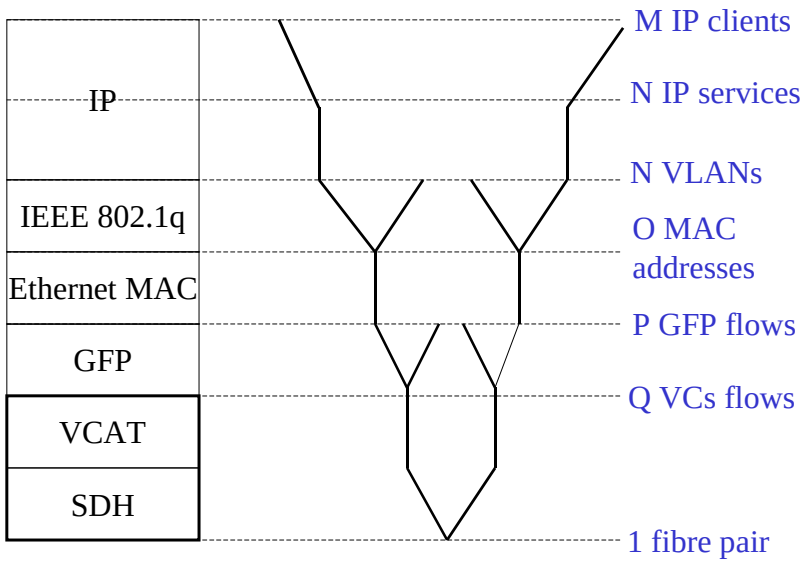

FIGURE 10: IT4 SDH TRANSPORT OPTION MULTIPLEXING HIERARCHY

Annex C (informative):
iT4 - Ethernet Transport Option Multiplexing Hierarchy

Figure 11 shows the multiplexing hierarchy for the iB1 Ethernet transport Option.

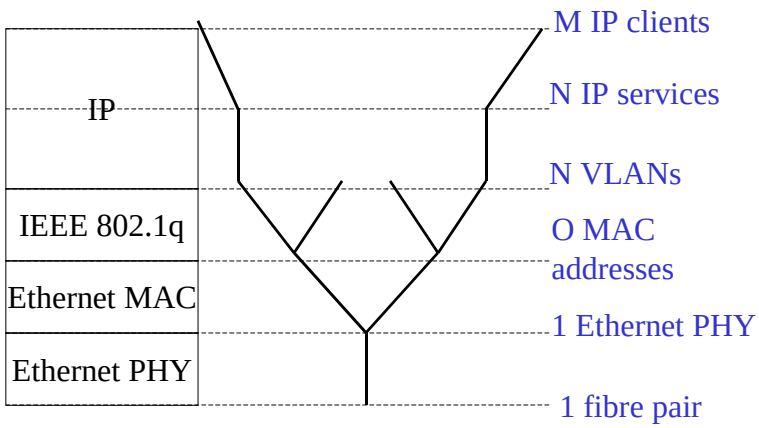

FIGURE 11: IT4 ETHERNET TRANSPORT OPTION MULTIPLEXING HIERARCHY

Annex D (innormative):
Multiplexing Hierarchy For The Multi-Service Protocol Stack

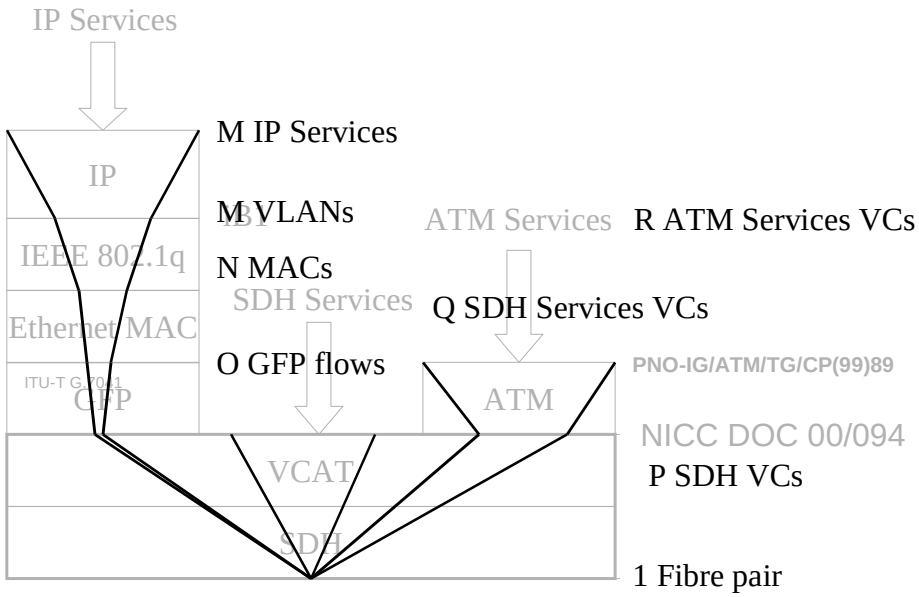

FIGURE 12: MULTIPLEXING HIERARCHY FOR THE MULTI-SERVICE SDH PROTOCOL STACK.

Annex E (informative):
BFD for IPv4 and IPv6 (Single Hop) Draft


draft-ietf-bfd-v4v6-1hop-08.txt


draft-ietf-bfd-generic-04.txt


draft-ietf-bfd-base-08.txt

History

Document history		
Issue 1	02/05/2006	Authorised for publication on the Ofcom web site at TSG07 and NICC55.
Issue 2	11/10/2007	On TSG 28-day approval completing 9th November 2007, when the correct version numbering will be inserted.
V1.2.1	06/12/2007	Converted unedited from Issue 2 to V1.2.1 to comply with the new ND numbering rules, for publication on the NICC web site.
V2.2.1	25/06/2008	Change requests A&R 001 and A&R 002 implemented.
V2.2.2	19/08/2008	BFD “shall” to “should” editorial change and BFD reference & Annex E updated. Converted to new template.