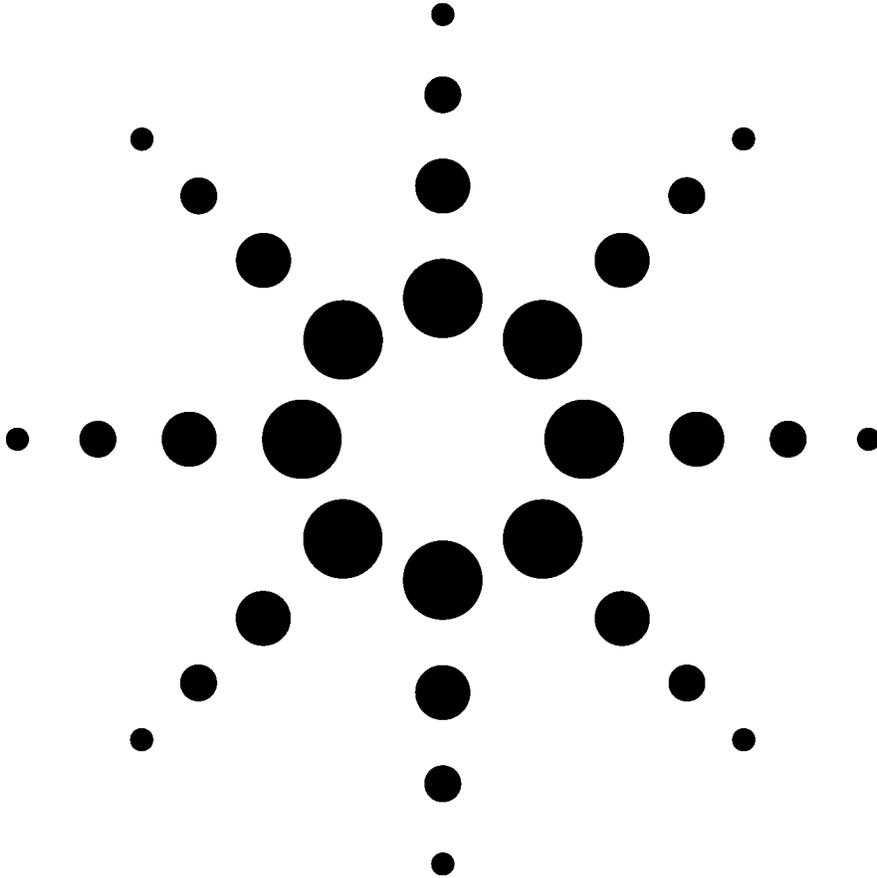


# **RFC 2544 Testing of Ethernet Services in Telecom Networks**

White Paper



**Nigel Burgess  
Agilent Technologies**



**Agilent Technologies**

## Introduction

The object of this paper is to discuss the use and testing of Ethernet services in telecommunications transmission networks, with the emphasis on the commissioning through to maintenance phases of network deployment and use. These phases are generally taken to be:

- Commissioning
- Acceptance testing
- Service turn-up/hand-over
- Network maintenance/troubleshooting

This paper will introduce Ethernet in its various forms and discuss its increasing use as a transport protocol in telecommunications networks. It will then discuss what testing should be done, and how that testing can be carried out, in order to ensure quality of service for the end user of an Ethernet service.

This paper is intended for telecommunications engineers and technicians involved in the deployment and use of Ethernet services. It will be of particular interest to those who are familiar with SONET/SDH services and who now find themselves deploying the "new" Ethernet services.

## The Need to Use Ethernet in Transmission

The need to transmit data on telecommunications networks is not new. In fact the very first telecommunications systems could only transmit "data", in the form of Morse code. The networks that have since been built around the world however were designed to carry only one type of traffic - voice. The telephony network is the biggest machine in the world, with many millions of interconnections. Until recently this network served its purpose well and it is only with the huge increase in the need for data transport, driven mostly by the Internet, that there has been any real need for change.

Until recently data traffic was carried on the telecommunication network by making it "look" like voice traffic, either by using a modem or, for higher bandwidth connections, packaging the data in such a way that it would fit into the standard 56/64 kbit/s channel structure of the telecoms network. However as the amount of data traffic in the network continues to grow, other means have to be found of carrying the new traffic that are more bandwidth efficient, less complex and less costly.

There are several options for dealing with this increase in data traffic and the various approaches all have advantages and disadvantages. For example, one option is to build an entirely new data-only network. The biggest disadvantage of this approach, and most of the other options, is the large amount of capital investment required. For this reason most network operators are integrating data services into their existing networks and they are doing this by utilizing the "next generation" of SONET/SDH network elements.

These new network elements carry all of the traditional T-carrier/PDH and SONET/SDH services but also allow the transport of data services in their native format, Ethernet. This reduces the complexity of the network for both the customer and the operator leading to a lower overall cost and more efficient use of bandwidth.

It is the use of these "next generation" elements that this paper addresses.

## Introduction to Ethernet

Ethernet is an asynchronous, frame-based protocol originally intended to provide a means of communication between more than two data devices, using shared media. Ethernet, fully defined by the IEEE 802.3 (2000) standard, has changed and evolved over time, increasing in speed and allowing the use of full-duplex transmission, rather than shared media.

The current version of the standard allows for many variations of speed and media type and these are described by the following notation:

<data rate in Mbit/s> <medium type> <Maximum segment length (x 100 m)>

For example, the standard contains a specification for a 10 Mbit/s, baseband system with a maximum segment length of 500 m. The notation for this would be 10BASE5. A media type identifier often replaces the segment length, for example the 'T' identifier is used for systems running on unshielded twisted pair cabling. All of the variations of Ethernet share the same basic frame structure, access/control method (MAC - Media Access Control) and, for systems using shared media, the same collision detection scheme (CSMA/CD - Carrier Sense Multiple Access / Collision Detect).

The most common Ethernet physical interfaces in current use are:

- 10BASE-T - 10 Mbit/s, baseband system, using category 3, 4 or 5 twisted pair cabling,
- 100BASE-TX - 100 Mbit/s, baseband system, using category 5 twisted pair cabling,
- 1000BASE-SX - 1000 Mbit/s, baseband system, using 850 nm, multi-mode optical fiber,
- 1000BASE-LX - 1000 Mbit/s, baseband system, using 1300 nm, single mode or multimode fiber.

Discussions in this paper refer to these physical interfaces, unless otherwise stated.

Figure 1 illustrates the structure of an Ethernet frame.

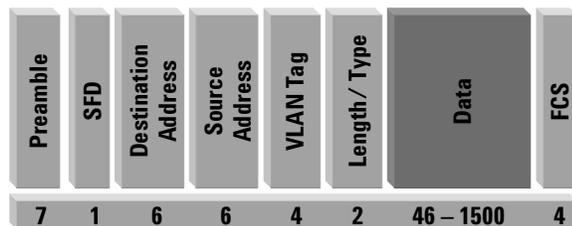


Figure 1: Structure of an Ethernet frame

The function of the various parts is as follows:

**Preamble/Start of Frame Delimiter, 8 Bytes** - Alternate ones and zeros for the preamble, 11010101 for the SFD (Start of Frame Delimiter). This allows for receiver synchronisation and marks the start of frame.

**Destination Address, 6 Bytes** - The MAC destination address of the frame, usually written in hex, is used to route frames between devices. Some MAC addresses are reserved, or have special functions. For example FF:FF:FF:FF:FF:FF is a broadcast address which would go to all stations.

**Sources Address, 6 Bytes** - The MAC address of the sending station, usually written in hex. The source address is usually built into a piece of equipment at manufacture. The first three bytes would identify the manufacturer and the second three bytes would be unique to the equipment. However there are some devices, test equipment for example, in which the address is changeable.

**VLAN Tag, 4 Bytes (optional)** - The VLAN tag is optional. If present it provides a means of separating data into “virtual” LANs, irrespective of MAC address. It also provides a “priority tag” which can be used to implement quality of service functions.

**Length/Type, 2 Bytes** - This field is used to give either the length of the frame or the type of data being carried in the data field. If the length/type value is less than 05DC hex then the value represents the length of the data field. If the value is greater than 0600 hex then it represents the type of protocol in the data field, for example 0800 hex would mean the frame was carrying IP. 809B hex would mean the frame was carrying AppleTalk.

**Data, 46 to 1500 Bytes** - The client data to be transported. This would normally include some higher layer protocol, such as IP or AppleTalk.

**Frame Check Sequence, 4 Bytes** - The check sequence is calculated over the whole frame by the transmitting device. The receiving device will re-calculate the checksum and ensure it matches the one inserted by the transmitter. Most types of Ethernet equipment will drop a frame with an incorrect or missing FCS.

The minimum legal frame size, including the FCS but excluding the preamble, is 64 bytes. Frames below the minimum size are known as “runts” and would be discarded by most Ethernet equipment.

The maximum standard frame size is 1522 bytes if VLAN tagging is being used and 1518 bytes if VLAN is not being used. It is possible to use frames larger than the maximum size. Such frames are called “Jumbo Frames” and are supported by some manufacturer’s equipment in various sizes up to 64 Kbyte. Jumbo frames are identical in form to standard frames but with a bigger data field. This produces a better ratio of “overhead” bytes to data bytes and hence more efficient transmission. Jumbos are non-standard and manufacturer specific and therefore interoperability cannot be guaranteed.

The frames are transmitted from left to right, least significant bit first. The frames are separated by an “inter-packet gap”. The minimum length of the inter-packet gap is 12 bytes. The inter-packet gap exists because in a half duplex system time is needed for the medium to go quiet before the next frame starts transmission. The inter-packet gap is not really needed for full duplex operation but is still used for consistency.

## Auto-Negotiation

Most Ethernet devices support auto-negotiation. When two devices are first connected together they will send information to each other to “advertise” their capabilities. The devices will then configure themselves to the highest common setting. The capabilities negotiated are speed, full or half duplex operation and the use of flow control.

## Introduction to the OSI Seven Layer Model.

The OSI seven layer model presents a means of describing the functions of the various sections, or layers, of a data communication system.

Ethernet covers the bottom two layers of this model, layer 1, the physical medium (UTP, Coaxial cable, Fibre) over which the data is transferred and layer 2 (Data Link Layer), the control mechanism for transmitting data onto the medium and receiving data from the medium.

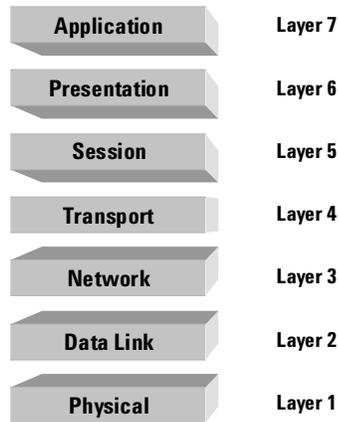


Figure 2: OSI Seven Layer Model

Layer 3 is the network Layer and this function is most commonly carried out by IP, but could also be AppleTalk, IPX or other such protocols.

The purpose of Ethernet is to ensure data is transferred over a link in a communications network, while the layer 3 protocol has the job of ensuring the data is transferred over the whole network, from the original source to the ultimate destination. This may use any number of separate Ethernet links. The simplified network diagram in Figure 3 illustrates this.

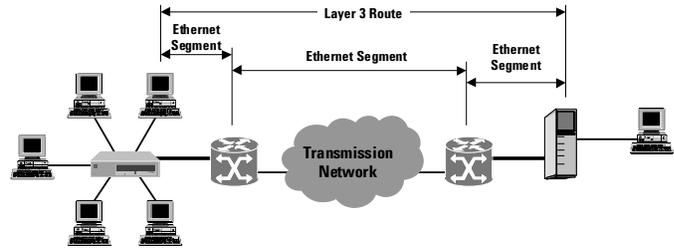


Figure 3: Simplified network diagram

The higher layer protocols, layers 4 and above, have the task of ensuring the integrity of transmitted data and presenting the data to the user or application. The function of these higher layer protocols is of little interest in a transmission environment. A detailed description of the function of all seven layers of the model, and the advantages and disadvantages of the various protocols used in each layer can be found in any good text on data networking.

## Testing Ethernet Services

The Ethernet connections mentioned above must be tested to ensure that they are operating correctly and also they are performing to the required levels.

This is done by testing the bandwidth, the delay and the loss of frames in the connection. In Ethernet terms these are called Throughput, Latency and Frame Loss.

## Throughput

Data throughput is simply the maximum amount of data, that can be transported from source to destination. However the definition and measuring of throughput is complicated by the need to define an acceptable level of quality. For example, if 10% errored or lost frames were deemed to be acceptable then the throughput would be measured at 10% error rate. This document shall use the generally accepted definition that throughput should be measured with zero errors or lost frames.

In any given Ethernet system the absolute maximum throughput will be equal to the data rate, e.g. 10 Mbit/s 100 Mbit/s or 1000 Mbit/s. In practice these figures cannot be achieved because of the effect of frame size. The smaller size frames have a lower effective throughput than the larger sizes because of the addition of the pre-amble and the interpacket gap bytes, which do not count as data. The maximum achievable throughput for various frame sizes is given in the following tables:

**Table 1: 10 Mbit/s System**

Frame Size	Data Throughput	Preamble & IGP	Frames per sec
64 byte	7.62 Mbit/s	2.38 Mbit/s	14,880
128 byte	8.65 Mbit/s	1.35 Mbit/s	8,445
256 byte	9.27 Mbit/s	0.72 Mbit/s	4,528
512 byte	9.62 Mbit/s	0.38 Mbit/s	2,349
1024 byte	9.81 Mbit/s	0.19 Mbit/s	1,197
1280 byte	9.84 Mbit/s	0.15 Mbit/s	961
1518 byte	9.87 Mbit/s	0.13 Mbit/s	812
1522 byte (includes VLAN)	9.87 Mbit/s	0.13 Mbit/s	810

**Table 2: 100 Mbit/s System**

Frame Size	Data Throughput	Preamble & IGP	Frames per sec
64 byte	76.19 Mbit/s	23.81 Mbit/s	148,809
128 byte	86.49 Mbit/s	13.51 Mbit/s	84,459
256 byte	92.75 Mbit/s	7.25 Mbit/s	45,289
512 byte	96.24 Mbit/s	3.76 Mbit/s	23,496
1024 byte	98.08 Mbit/s	1.92 Mbit/s	11,973
1280 byte	98.46 Mbit/s	1.54 Mbit/s	9,615
1518 byte	98.69 Mbit/s	1.30 Mbit/s	8,127
1522 byte (includes VLAN)	98.70 Mbit/s	1.30 Mbit/s	8,106

**Table 3: 1000 Mbit/s System**

Frame Size	Data Throughput	Preamble & IGP	Frames per sec
64 byte	761.90 Mbit/s	238.10 Mbit/s	1,488,095
128 byte	864.86 Mbit/s	135.14 Mbit/s	844,594
256 byte	927.54 Mbit/s	72.46 Mbit/s	452,898
512 byte	962.40 Mbit/s	37.59 Mbit/s	234,962
1024 byte	980.84 Mbit/s	19.16 Mbit/s	119,731
1280 byte	984.61 Mbit/s	15.38 Mbit/s	96,153
1518 byte	986.99 Mbit/s	13.00 Mbit/s	81,274
1522 byte (includes VLAN)	987.02 Mbit/s	12.97 Mbit/s	81,063

## Latency

Latency is the total time taken for a frame to travel from source to destination. This total time is the sum of both the processing delays in the network elements and the propagation delay along the transmission medium.

In order to measure latency a test frame containing a time stamp is transmitted through the network. The time stamp is then checked when the frame is received. In order for this to happen the test frame needs to return to the original test set by means of a loopback (round-trip delay).

## Frame Loss

Frame loss is simply the number of frames that were transmitted successfully from the source but were never received at the destination. It is usually referred to as frame loss rate and is expressed as a percentage of the total frames transmitted. For example if 1000 frames were transmitted but only 900 were received the frame loss rate would be:  $(1000 - 900) / 1000 \times 100\% = 10\%$  Frames can be lost, or dropped, for a number of reasons including errors, over-subscription and excessive delay.

**Errors** - most layer 2 devices will drop a frame with an incorrect FCS. This means that a single bit error in transmission will result in the entire frame being dropped. For this reason BER, the most fundamental measure of a SONET/SDH service, has no meaning in Ethernet since the ratio of good to errored bits cannot be ascertained.

**Oversubscription** - the most common reason for frame loss is oversubscription of the available bandwidth. For example, if two 1000 Mbit/s Ethernet services are mapped into a single 622 Mbit/s SONET/SDH pipe (a common scenario) then the bandwidth limit is quickly reached as the two gigabit Ethernet services are loaded. When the limit is reached, frames may be dropped.

**Excessive Delay** - The nature of Ethernet networks means that it is possible for frames to be delayed for considerable periods of time. This is important when testing as the tester is "waiting" for all of the transmitted frames to be received and counted. At some point the tester has to decide that a transmitted frame will not be received and count the frame as lost. The most common time period used to make this decision is the RFC specification of two seconds. Thus any frame received more than two seconds after it is transmitted would be counted as lost.

## Customer Requirements

### Service Level Agreements

In many cases Ethernet services are being set-up under Service Level Agreements (SLA) with customers. Often Quality Of Service (QoS) issues are raised and this is one of the most discussed topics currently in the Ethernet services industry.

There are three main areas that are involved in determining what type of service to offer; bandwidth, delay and loss of data.

Bandwidth is a key factor as more and more of it is required. Data transfer, email, web based seminars and discussions and voice-over-IP are demanding more bandwidth from service providers. In order to support these services an agreed bandwidth is usually set in the SLA and proof is commonly required that the bandwidth will be available in the connection given by the service provider.

Delay is another key factor in an SLA especially when real time services are being used. These services can range from web based seminars and presentations though to Voice-over-IP (VoIP). Long delay times in the network can cause these services to be disrupted or have a reduced quality. When VoIP is in place, long delay times can interfere heavily in a normal telephone conversation which is unacceptable to an end user. The other attribute for delay is that it should be constant. If the delay is fairly small but it varies considerably during the transmission, problems will still occur in the use of real time service.

Loss of data is obviously unwanted in any network. A service provider will need to make sure that the Ethernet service being provided will not lose frames and packets when they are transmitted through the network.

### RFC 2544 Benchmark Testing

This paper has so far discussed what tests can be done on an Ethernet service connection and what a customer often requires, but how does a service provider perform tests that the customer will understand and will accept? How long do the tests last and what results mean anything?

The answer is *Request For Comments 2544* (RFC 2544). This is a benchmark test that specifies certain test criteria that allow both service provider and customer to meet an agreement.

RFC 2544 requires the standard frame sizes (64, 128, 256, 512, 1024, 1280 and 1518 byte) to be tested for a certain length of time and a certain number of times. This is because all these frame sizes are used in the network and so the results for each must be known.

The tests that are mentioned in RFC 2544 are Throughput, Latency, Frame Loss and Back-to-back frames. The first three are mentioned previously in this paper.

Back-to-back frame testing involves sending a burst of frames with minimum inter-frame gaps to the DUT and count the number of frames forwarded by the DUT. If the count of transmitted frames is equal to the number of frames forwarded the length of the burst is increased and the test is rerun.

If the number of forwarded frames is less than the number transmitted, the length of the burst is reduced and the test is rerun. The back-to-back value is the number of frames in the longest burst that the DUT will handle without the loss of any frames.

The RFC 2544 test asks for the results of all these tests to be recorded both in text and graphical formats. The results can then give accurate performance data for both service provider and customer.

### How to test RFC 2544

The tests performed in an RFC 2544 test can be manual but this is tedious, time consuming and susceptible to errors in the test method. The easiest way is to have a fully automated test feature which allows the user to simply enter a few details about the test scenario and then start the test. The test equipment will then run through all the requirements for the RFC 2544 test and will display the results for the user.

Page intentionally left blank

## **Agilent Computing and Networking Solutions**

### **Enabling service and device innovation for computing and communications**

Agilent Technologies is a worldwide leader in testing computer and communications devices, elements, systems and services that enable high-speed computation and communications. The test portfolio includes:

- multiservices test solutions for converging network infrastructure enabling component, network elements manufacturers and service providers to accelerate the delivery of next-generation devices for applications from backbone, metro, enterprise, access, to backplanes.
- digital microwave solutions for high-speed communications busses and backplanes that allow more complete characterization of new devices and designs with easy, accurate and repeatable BER, jitter and protocol performance measurements.
- a broad range of optical test solutions used by component and equipment manufacturers, aerospace & defense companies, universities and service providers to characterize the latest in high performance and low cost photonic devices and networks.

**[www.agilent.com](http://www.agilent.com)**

**[www.framescope.com](http://www.framescope.com)**  
**[www.wirescope.com](http://www.wirescope.com)**

### **Sales, Service and Support**

#### **United States**

1 800 829 4444  
1 800 829 4433 (FAX)

#### **Canada**

1 877 894 4414  
1 888 900 8921 (FAX)

#### **Europe**

(31) (0) 20 547 2111  
(31) (0) 20 547 2190 (FAX)

#### **Japan**

0120 421 345  
0120 421 678 (FAX)

#### **Latin America**

(55) 11 4197 3600  
(55) 11 4197 3800 (FAX)

#### **Australia**

1 800 629 485  
1 800 142 134 (FAX)

#### **Asia-Pacific**

(852) 800 930 871  
(852) 800 908 476 (FAX)

This information is subject to change without notice.

Copyright © 2004 Agilent Technologies  
November 15, 2004

**5989-1927EN**



**Agilent Technologies**