Network Working Group
Request for Comments: 1242

S. Bradner, Editor
Harvard University

July 1991

Benchmarking Terminology for Network Interconnection Devices

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Abstract

This memo discusses and defines a number of terms that are used in describing performance benchmarking tests and the results of such tests. The terms defined in this memo will be used in additional memos to define specific benchmarking tests and the suggested format to be used in reporting the results of each of the tests. This memo is a product of the Benchmarking Methodology Working Group (BMWG) of the Internet Engineering Task Force (IETF).

1. Introduction

Vendors often engage in "specsmanship" in an attempt to give their products a better position in the marketplace. This usually involves much "smoke & mirrors" used to confuse the user. This memo and follow-up memos attempt to define a specific set of terminology and tests that vendors can use to measure and report the performance characteristics of network devices. This will provide the user comparable data from different vendors with which to evaluate these devices.

2. Definition format

Term to be defined. (e.g., Latency)

Definition:
The specific definition for the term.

Discussion:
A brief discussion about the term, it's application and any restrictions on measurement procedures.

Measurement units:
The units used to report measurements of this term, if applicable.

Issues:
List of issues or conditions that effect this term.

See Also:
List of other terms that are relevant to the discussion of this term.

3. Term definitions

3.1 Back-to-back

Definition:
Fixed length frames presented at a rate such that there is the minimum legal separation for a given medium between frames over a short to medium period of time, starting from an idle state.

Discussion:
A growing number of devices on a network can produce bursts of back-to-back frames. Remote disk servers using protocols like NFS, remote disk backup systems like rdump, and remote tape access systems can be configured such that a single request can result in a block of data being returned of as much as 64K octets. Over networks like ethernet with a relatively small MTU this results in many fragments to be transmitted. Since fragment reassembly will only be attempted if all fragments have been received, the loss of even one fragment because of the failure of some intermediate network device to process enough continuous frames can cause an endless loop as the sender repetitively attempts to send its large data block.

With the increasing size of the Internet, routing updates can span many frames, with modern routers able to transmit very quickly. Missing frames of routing information can produce false indications of unreachability. Tests of this parameter are intended to determine the extent of data buffering in the device.

Measurement units:
Number of N-octet frames in burst.

Issues:

See Also:

3.2 Bridge

Definition:
A system which forwards data frames based on information in the data link layer.

Discussion:

Measurement units:
n/a

Issues:

See Also:
bridge/router (3.3)
router (3.15)

3.3 bridge/router

Definition:
A bridge/router is a network device that can selectively function as a router and/or a bridge based on the protocol of a specific frame.

Discussion:

Measurement units:
n/a

Issues:

See Also:
bridge (3.2)
router (3.15)

3.4 Constant Load

Definition:
Fixed length frames at a fixed interval time.

Discussion:
Although it is rare, to say the least, to encounter a steady state load on a network device in the real world, measurement of steady state performance may be useful in evaluating competing devices. The frame size is specified and constant. All device parameters are constant. When there is a checksum in the frame, it must be verified.

Measurement units:
n/a

Issues:
unidirectional vs. bidirectional

See Also:

3.5 Data link frame size

Definition:
The number of octets in the frame from the first octet following the preamble to the end of the FCS, if present, or to the last octet of the data if there is no FCS.

Discussion:
There is much confusion in reporting the frame sizes used in testing network devices or network measurement. Some authors include the checksum, some do not. This is a specific definition for use in this and subsequent memos.

Measurement units:
octets

Issues:

See Also:

3.6 Frame Loss Rate

Definition:
Percentage of frames that should have been forwarded by a network device under steady state (constant) load that were not forwarded due to lack of resources.

Discussion:
This measurement can be used in reporting the performance of a network device in an overloaded state. This can be a useful indication of how a device would perform under pathological network conditions such as broadcast storms.

Measurement units:
Percentage of N-octet offered frames that are dropped. To be reported as a graph of offered load vs frame loss.

Issues:

See Also:
overhead behavior (3.11)
policy based filtering (3.13)
MTU mismatch behavior (3.10)

3.7 Inter Frame Gap

Definition:
The delay from the end of a data link frame as defined in section 3.5, to the start of the preamble of the next data link frame.

Discussion:
There is much confusion in reporting the between frame time used in testing network devices. This is a specific definition for use in this and subsequent memos.

Measurement units:
Time with fine enough units to distinguish between 2 events.

Issues:
Link data rate.

See Also:

3.8 Latency

Definition:
For store and forward devices:
The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port.

For bit forwarding devices:
The time interval starting when the end of the first bit of the input frame reaches the input port and ending when the start of the first bit of the output frame is seen on the output port.

Discussion:
Variability of latency can be a problem.
Some protocols are timing dependent (e.g., LAT and IPX).
Future applications are likely to be sensitive to

network latency. Increased device delay can reduce the useful diameter of net. It is desired to eliminate the effect of the data rate on the latency measurement. This measurement should only reflect the actual within device latency. Measurements should be taken for a spectrum of frame sizes without changing the device setup.

Ideally, the measurements for all devices would be from the first actual bit of the frame after the preamble. Theoretically a vendor could design a device that normally would be considered a store and forward device, a bridge for example, that begins transmitting a frame before it is fully received. This type of device is known as a "cut through" device. The assumption is that the device would somehow invalidate the partially transmitted frame if in receiving the remainder of the input frame, something came up that the frame or this specific forwarding of it was in error. For example, a bad checksum. In this case, the device would still be considered a store and forward device and the latency would still be from last bit in to first bit out, even though the value would be negative. The intent is to treat the device as a unit without regard to the internal structure.

Measurement units:
Time with fine enough units to distinguish between 2 events.

Issues:

See Also:
link speed mismatch (3.9)
constant load (3.4)
back-to-back (3.1)
policy based filtering (3.13)
single frame behavior (3.16)

3.9 Link Speed Mismatch

Definition:
Speed mismatch between input and output data rates.

Discussion:
This does not refer to frame rate per se, it refers to the actual data rate of the data path. For example,

an Ethernet on one side and a 56KB serial link on the other. This is has also been referred to as the "fire hose effect". Networks that make use of serial links between local high speed networks will usually have link speed mismatch at each end of the serial links.

Measurement units:
Ratio of input and output data rates.

Issues:

See Also:
constant load (3.4)
back-to-back (3.1)

3.10 MTU-mismatch behavior

Definition:
The network MTU (Maximum Transmission Unit) of the output network is smaller than the MTU of the input network, this results in fragmentation.

Discussion:
The performance of network devices can be significantly affected by having to fragment frames.

Measurement units:
Description of behavior.

Issues:

See Also:

3.11 Overhead behavior

Definition:
Processing done other than that for normal data frames.

Discussion:
Network devices perform many functions in addition to forwarding frames. These tasks range from internal hardware testing to the processing of routing information and responding to network management requests. It is useful to know what the effect of these sorts of tasks is on the device performance. An example would be if a router were to suspend forwarding or accepting frames during the processing of large routing update for a complex protocol like

OSPF. It would be good to know of this sort of behavior.

Measurement units:
Any quantitative understanding of this behavior is by the determination of its effect on other measurements.

Issues:
bridging and routing protocols
control processing
icmp
ip options processing
fragmentation
error processing
event logging/statistics collection
arp

See Also:
policy based filtering (3.13)

3.12 Overloaded behavior

Definition:
When demand exceeds available system resources.

Discussion:
Devices in an overloaded state will lose frames. The device might lose frames that contain routing or configuration information. An overloaded state is assumed when there is any frame loss.

Measurement units:
Description of behavior of device in any overloaded states for both input and output overload conditions.

Issues:
How well does the device recover from overloaded state?
How does source quench production effect device?
What does device do when its resources are exhausted?
What is response to system management in overloaded state?

See Also:

3.13 Policy based filtering

Definition:
Filtering is the process of discarding received

frames by administrative decision where normal operation would be to forward them.

Discussion:
Many network devices have the ability to be configured to discard frames based on a number of criteria. These criteria can range from simple source or destination addresses to examining specific fields in the data frame itself. Configuring many network devices to perform filtering operations impacts the throughput of the device.

Measurement units:
n/a

Issues:
flexibility of filter options
number of filter conditions

See Also:

3.14 Restart behavior

Definition:
Reinitialization of system causing data loss.

Discussion:
During a period of time after a power up or reset, network devices do not accept and forward frames. The duration of this period of unavailability can be useful in evaluating devices. In addition, some network devices require some form of reset when specific setup variables are modified. If the reset period were long it might discourage network managers from modifying these variables on production networks.

Measurement units:
Description of device behavior under various restart conditions.

Issues:
Types:
power on
reload software image
flush port, reset buffers
restart current code image, without reconfuration

Under what conditions is a restart required?
Does the device know when restart needed (i.e., hung state timeout)?
Does the device recognize condition of too frequent auto-restart?
Does the device run diagnostics on all or some resets?
How may restart be initiated?
physical intervention
remote via terminal line or login over network

See Also:

3.15 Router

Definition:
A system which forwards data frames based on information in the network layer.

Discussion:
This implies "running" the network level protocol routing algorithm and performing whatever actions that the protocol requires. For example, decrementing the TTL field in the TCP/IP header.

Measurement units:
n/a

Issues:

See Also:
bridge (3.2)
bridge/router (3.3)

3.16 Single frame behavior

Definition:
One frame received on the input to a device.

Discussion:
A data "stream" consisting of a single frame can require a network device to do a lot of processing. Figuring routes, performing ARPs, checking permissions etc., in general, setting up cache entries. Devices will often take much more time to process a single frame presented in isolation than it would if the same frame were part of a steady stream. There is a worry that some devices would even discard a single frame as part of the cache setup procedure under the

assumption that the frame is only the first of many.

Measurement units:
Description of the behavior of the device.

Issues:

See Also:
policy based filtering (3.13)

3.17 Throughput

Definition:
The maximum rate at which none of the offered frames are dropped by the device.

Discussion:
The throughput figure allows vendors to report a single value which has proven to have use in the marketplace. Since even the loss of one frame in a data stream can cause significant delays while waiting for the higher level protocols to time out, it is useful to know the actual maximum data rate that the device can support. Measurements should be taken over a assortment of frame sizes. Separate measurements for routed and bridged data in those devices that can support both. If there is a checksum in the received frame, full checksum processing must be done.

Measurement units:
N-octet input frames per second
input bits per second

Issues:
single path vs. aggregate
load
unidirectional vs bidirectional
checksum processing required on some protocols

See Also:
frame loss rate (3.6)
constant load (3.4)
back-to-back (3.1)

4. Acknowledgements

This memo is a product of the IETF BMWG working group:

Chet Birger, Coral Networks
Scott Bradner, Harvard University (chair)
Steve Butterfield, independant consultant
Frank Chui, TRW
Phill Gross, CNRI
Stev Knowles, FTP Software, Inc.
Mat Lew, TRW
Gary Malkin, FTP Software, Inc.
K.K. Ramakrishnan, Digital Equipment Corp.
Mick Scully, Ungerman Bass
William M. Seifert, Wellfleet Communications Corp.
John Shriver, Proteon, Inc.
Dick Sterry, Microcom
Geof Stone, Network Systems Corp.
Geoff Thompson, SynOptics
Mary Youssef, IBM

Security Considerations

Security issues are not discussed in this memo.

Author's Address

Scott Bradner
Harvard University
William James Hall 1232
33 Kirkland Street
Cambridge, MA 02138

Phone: (617) 495-3864

EMail: SOB@HARVARD.HARVARD.EDU
Or, send comments to: bmwg@harvisr.harvard.edu.