TCP and UDP based ForCES Protocol TML over IP Networks

draft-wang-forces-iptml-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Abstract

This document defines ForCES Transport Mapping Layer (TML) over IP networks, the framework and the specifications to meet the ForCES TML requirements.

Table of Contents

Internet Draft ForCES TML over IP Mar. 2007

1. Introduction ..................................................... 2
2. Definitions ..................................................... 2
3. ForCES TML Overview ............................................ 3
   3.1. TML in ForCES Framework ................................. 3
   3.2. TML Requirements ....................................... 5
   3.3. PL-TML Service Primitives .............................. 6
1. Introduction

The Forwarding and Control Element Separation (ForCES), the requirements have been defined in RFC3654, and the framework in RFC3746. The ForCES protocol, which standardizes the information exchange method between Control Element (CE) and Forwarding Element (FE), is being defined in [ForCES-PL] by IETF.

Variant transport media (like IP, ATM, Ethernet, etc) may be applied to ForCES protocol for the interconnection between CE and FE. To make the ForCES protocol specification independent of these variant transport means, a Transport Mapping Layer (TML) is induced in the ForCES protocol. It is expected that different TML specifications be individually defined by IETF. A set of service primitives has been defined to provide standard interconnection between the ForCES Protocol Layer(PL) and the TML [TML-SP].

This document defines a TCP and UDP based ForCES Transport Mapping Layer (TML) over IP networks. It applies TCP and UDP protocols as the transport protocol for the ForCES protocol messages. Details are presented in this document for this TML to meet the ForCES TML requirements and the requirements of PL-TML service primitives defined in [TML-SP].

2. Definitions
Many definitions related to ForCES can be found in RFC3654, RFC3746 and the ForCES protocol [ForCES-PL], like:

ForCES Protocol Layer (ForCES PL) -- A layer in ForCES protocol architecture that defines the ForCES protocol messages, the protocol state transfer scheme, as well as the ForCES protocol architecture itself (including requirements of ForCES TML (see below)). Specifications of ForCES PL are defined by [ForCES-PL].

ForCES Protocol Transport Mapping Layer (ForCES TML) -- A layer in ForCES protocol architecture that uses the capabilities of existing transport protocols to specifically address protocol message transportation issues, such as how the protocol messages are mapped to different transport media (like TCP, IP, ATM, Ethernet, etc), and how to achieve and implement reliability, multicast, ordering, etc. The ForCES TML specifications are detailed in separate ForCES documents, one for each TML.

This document defines the following notions:

ForCES TML over IP networks -- TML for ForCES protocol that are applied to CE-FE interconnect networks, which run IP protocol at the Network Layer.

IP TML -- Specifically means ForCES TML over IP networks in this document, it uses TCP and UDP as the transport protocols.

Connection Manager Component (CMC) -- a component in IP TML that is responsible for all IP TML level connection management.

Arbiter Component (AC) -- a component in IP TML that is responsible for putting PL messages into IP TML level connections.

3.

ForCES TML Overview

3.1. TML in ForCES Framework

The ForCES protocol[ForCES-PL] has defined the relationship between ForCE PL and TML in the protocol framework, as shown in Figure 1. A TML always lies below a PL in the same ForCES NE and provides services to the PL. Semantic descriptions of the services are provided by the TML Service Primitives document [TML-SP].
During ForCES pre-association phase, a CE/FE TML is usually managed by CE Manager (CEM)/FE Manager (FEM), as shown in Figure 2, so as to be pre-configured with some initialization parameters, like IP addresses in this TCP/UDP based TML for establishment of the TML connections.

Note that although Figure 2 shows CEM/FEM being entities outside CE/FE, it is also possible CEM/FEM is physically embedded in CE/FE.

During ForCES post-association phase, ForCES PL is activated. TML is then associated to the local PL. From ForCES model point of view, to associate a CE/FE TML to the CE/FE PL is actually to associate the CE/FE TML to the CE/FE protocol entities in the CE/FE. In FE, the protocol entity is the FE protocol LFB. Note that at the same time, TMLs will have to still be associated to CEM/FEM. This actually infers that CEM/FEM will still be active during the post-association phase for TML management. Figure 3 shows the diagram for TML structure during post-association phase.
Figure 3 also indicates that:

1. TML properties (attributes, capabilities, events, etc) appearing at the PL level are actually part of the properties of CE/FE Protocol entities. Especially those TML properties that need to be accessible by CE must be appeared as FE Protocol properties.

2. PL-TML Service Primitives are used by cores of CE/FE Protocol entities to access the TML properties, as well as to send/receive PL messages via TML.

From Figure 3, it is also shown that TML receives configurations from both PL layer and CEM/FEM during the post-association phase. It is important to note the difference of the two types of management. CEM/FEM management for TML at post-association phase is a consistent management from pre-association phase, which is mainly for TML connection management, while PL level management for TML is for the management that is independent of actual TML media and only based on the uniformly defined TML service primitives.

### 3.2. TML Requirements

The ForCES protocol[ForCES-PL] has defined the general requirements to all types of ForCES TMLs, as below:

1. **Reliability**
   As defined by RFC 3654, section 6 #6.

2. **Security**
   TML provides security services to the ForCES PL. TML layer should support the following security services and describe how they are achieved.
* Endpoint authentication of FE and CE.
* Message Authentication
* Confidentiality service

3. Congestion Control
The congestion control scheme used needs to be defined. The congestion control mechanism defined by the TML should prevent the FE from being overloaded by the CE or the CE from being overwhelmed by traffic from the FE. Additionally, the circumstances under which notification is sent to the PL to notify it of congestion must be defined.

4. Uni/multi/broadcast addressing/delivery if any
If there is any mapping between PL and TML level Uni/Multi/Broadcast addressing it needs to be defined.

5. HA decisions
It is expected that availability of transport links is the TML’s responsibility. However, on config basis, the PL layer may wish to participate in link failover schemes and therefore the TML must support this capability.

6. Encapsulations used.
Different types of TMLs will encapsulate the PL messages on different types of headers. The TML needs to specify the encapsulation used.

7. Prioritization
It is expected that the TML will be able to handle up to 8 priority levels needed by the PL layer and will provide preferential treatment. TML needs to define how this is achieved. The requirement for supporting up to 8 priority levels does not mean that the underlying TML MUST be capable of handling up to 8 priority levels. In such an event the priority levels should be divided between the available TML priority levels. For example, if the TML only supports 2 priority levels, the 0-3 could go in one TML priority level, while 4-7 could go in the other.

8. Protection against DoS attacks
As described in RFC 3654, section 6

3.3. PL-TML Service Primitives

PL-TML service primitives are standard interfaces between PL and TML for the information exchanges. The following service primitives are defined in [TML-SP]:

    TMLopen()
    TMLclose()
Refer to [TML-SP] for more details.

4. IP TML Framework

We define the architectural framework of a TCP and UDP based ForCES TML over IP networks (IP TML) as in Figure 4. This framework applies to both CE TML and FE TML over IP networks.
IP TML as showed in Figure 4 uses a "TCP-UDP pair connection" for interconnection between CE TMLs and FE TMLs. A TCP-UDP pair connection contains a TCP connection and a UDP connection, which MUST have the same source and destination IP addresses and port numbers.

We define that IP TML connections should always be established in the form of TCP-UDP pair connection format, i.e., whenever a TCP connection is established, a UDP connection with the same source and destination addresses should also be available for this IP TML.

Note that, a UDP in a TCP-UDP pair is capable of multicast with the support from IP multicast protocols.

The TCP-UDP pair connections are managed by a component called "Connection Manager Component (CMC)". The CMC is responsible to all TML connections for the establishment and release, security of the connections, TML level High Availability (HA) management. Usually CMC fulfills these tasks by receiving configuration information from CE/FE Managers as described in Figure 2 and Figure 3. CMC also receives configuration information from local PL layer by means of the PL running TML Configure service primitive.

Section 4.1 describes the CMC component in details.

Interfaces between PL and TML in this IP TML framework shall comply with the defined PL-TML service primitives [TML-SP].

Once PL messages are generated by PL layer, they are sent to TML layer by the TMLsend service primitive. IP TML receives the PL messages and put the messages into two separate message queues according to the types of the PL messages. PL messages with Redirect Message type are put in a redirect message queue, while all other messages that are called control messages are put in a control message queue.

PL messages are put into TML level connections via a component called "Arbiter Component (AC)". The AC decides when and to which TML connections a PL message in the two queues should be injected into. Usually IP TML uses TCP/UDP socket interfaces to put the messages in the IP TML connections.

The AC also receives PL messages from peer TML via the TML connections, and makes them ready for local PL layer to fetch by means of the PL using TML Receive service primitive.
The AC may also generate TML events according to the TML connection state and notifies local PL layer of the events. The TML events should comply with the TML event specifications defined in the PL-TML service primitives [TML-SP].

The AC has to receive configuration information from PL layer via TML configure service primitive.

The AC will also share information about TML connections with CMC. The TML Connection Table in the CMC can also be accessed by AC. AC will then use the table to arbitrate PL messages and to put them in TML connections.

PL messages are encapsulated to TCP/UDP packets in AC before they are put in IP TML connections. PL messages are de-encapsulated in AC when received from peering TML and made ready to output to local PL.

Section 4.2 describes in details the AC component.

4.1. Connection Manager Component (CMC)

The Connection Manager Component (CMC) receives configuration information from CE manager (if it is a CE TML) or FE manager (if a FE TML), as well as from local PL layer.

There is only one kind of TML connections defined in this IP TML: TCP-UDP pair connection(s). A recommendation for the assignment of the TCP-UDP pairs is as below:

1. A base TCP-UDP pair connection between every CE and every FE MUST be applied.
2. Multiple TCP-UDP pair connections between one same CE and one same FE MAY be applied for the sake of TML requirements like prioritization.
3. PL control messages always use TCP in the TCP-UDP pair connection(s) for transportation.
4. PL redirect messages always use UDP in the TCP-UDP pair connection(s) for transportation.

The following steps may be adopted to establish a TCP-UDP pair connection between a CE and a FE:

1. CMC in a CE acts as a server and waits for a TCP connection from FEs
2. CMC in a FE acts as a client, and it should get information from the FE manager for connecting to peering CE TML, which usually includes the IP address and the port number for the CE TML.
3. CMC in the FE makes a TCP connection to the CE TML.
4. A UDP connection with the same source and destination addresses is then simultaneously and implicitly established.
CMC maintains a table called "TML Connection Table". This table contains information about all TCP-UDP pair connections that have been established. For every TCP-UDP pair connection, the table usually contains the following information:

- Connection destination CE/FE ID
- Connection destination IP address and port number
- PL Message type(s) the connection applies for
- PL Message priority(s) the connection applies for

The TML connections establishment process usually occurs once TML receives TML open service primitives from local PL. When a new FE is up and is going to associate itself to a CE, the FE PL usually needs to open the TML first, then to send a FE Association Message to join in the ForCES NE.

All active TML connections will be closed and shutdown if a TML close service primitive is received from local PL by a TML. When a FE is going to leave a CE, it will send a FE teardown message to CE first, then the PL will send a TML close primitive to local TML to close all TML connections.

After a TML is opened, the TML connections can be modified or released. Some new connections can be added. All newly modified connection information will immediately trigger CMC to change the connection state.

CMC generates TML events and notify local PL of the events. How it is notified to PL is an implementation detail and depends upon individual OS platforms the IP TML and the PL adopts. For instance, in several OS platforms, a callback mechanism may be adopted for this purpose.

The TML events generated by CMC include:

- TML error event

This event will happen once the TML TCP-UDP pair connections have encountered some failure.

<table>
<thead>
<tr>
<th>TML error code</th>
<th>TML error</th>
<th>Associated Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>all local TML link failure i.e., there is no one TML connection available owing to local problem</td>
<td>none</td>
</tr>
<tr>
<td>2</td>
<td>some local TML link failure peer TML CE/FE ID(s)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>peer TML unavailable peer TML CE/FE ID(s)</td>
<td></td>
</tr>
</tbody>
</table>
4.2. Arbiter Component (AC)

Arbiter Component (AC) should fulfill the following tasks:

1. To decide when and at what rate to inject PL messages into TML connections

By AC fulfilling this task, it is expected the IP TML meet the TML requirements for prioritization, congestion control, and in some way, protection against DoS attacks from redirect data.

2. To decide which connection(s) a PL message to be injected into.

AC does this work by use of the "TML Connection Table" generated by CMC as described above. AC will use the "Destination ID", "Message type" and "Message priority", which are associated with every message received from PL, to match the table to find out the corresponding IP TML connection(s).

3. To encapsulate PL messages to packets of TML connections or to de-encapsulate PL messages from packets of TML connections.

4. To receive PL messages from TML connections and send them to local PL by use of TML service primitives.

On receiving packets coming from peer TML, the IP TML just de-encapsulates them to get PDU of PL messages, then to put the messages in a receive queue waiting for PL to to fetch.

5. To generate TML events and to notify local PL of the events if the events have been subscribed by the PL.

The TML events generated by AC include:

-.TML message arrival event
-.TML congestion alert event
This event includes the following cases:
1. Control message congestion alert
The conditions invoking this alert is defined as below:

(TBD)

2. Redirect message congestion alert
The conditions invoking this alert is defined as below:

(TBD)

3. Alert for redirect DoS attack
The conditions invoking this alert is defined as below:

(TBD)

5. IP TML to meet TML Requirements

This section defines how the ForCES IP TML is specified to meet ForCES TML requirements as defined by [ForCES-PL].

5.1. Reliability

This IP TML meets the reliability requirement by defining that PL control messages must be transported by TCP, while PL redirect messages must be transported by UDP.

TCP reliability features like no packet loss, no reordering, and no corruption then maps to the reliability of PL control message transportation, but note that TCP does not guarantee a timely transportation, therefore timeliness is not guaranteed in the IP TML.

The reason to mandate UDP for PL redirect messages is that:

1. UDP provides relatively raw data transportation performance, which fits well in the cases where the application level of which may further be embedded with some Internet protocols like IP, UDP and even congestion awareness protocols like TCP protocol. Usually, redirect data contain data that may load other Internet protocols like TCP, UDP, and IP.
2. UDP provides multicast/broadcast mechanisms. This provides efficient support for PL layer multicast/broadcast.

5.2. Security

(TBD)

5.3. Congestion Control and Protection against DoS Attacks

Although PL control messages and redirect messages are transmitted separately over TCP and UDP, such separation itself does not provide congestion control and protection against DoS attacks from redirect data [GRMP-TEST]. Therefore, IP TML using the framework as Figure 4 may still face the danger of control messages being congested or even DoS attacked.
This specification does not specify any detailed implementation on how the IP TML meets the Congestion and DoS attack protection requirement. This specification also does not require that an IP TML implementation must provide a pure IP TML layer mechanism for congestion control and protection against DoS attacks, although individual implementations may apply such mechanism. Instead, this specification just specifies that an IP TML must provide a congestion alert event notification as defined in Section 4.2 to PL, so that PL may use the signal to construct a PL level congestion control and DoS attack protection.

5.4. High Availability

ForCES protocol has provided Heartbeat Messages specifically for CE/FE availability detection at PL layer, therefore TML layer does not need to take care of CE/FE level availability.

TML may take care of High Availability on TML connections.

In this IP TML, every TML connection is a TCP-UDP pair connection. A TCP connection is connection-oriented and has provided connection management. Although UDP does not provide such connection management, the UDP is defined to have associated to a TCP and formed a TCP-UDP pair. As a result, IP TML connections with TCP-UDP pairs does not need to take extra means to detect its connection availability.

5.5. Multicast

PL level Multicast for ForCES messages must map to IP TML level multicast by the following specifications:

1. Multicast control messages from a CE to FEs or from a FE to CEs must map to multiple unicast TCPs at IP TML
2. Multicast redirect messages from a CE to FEs or from a FE to CEs must map to UDP multicast at IP TML

Definition of a Multicast list data structure used for IP TML complies with that specified in [TML-SP].

To fulfill a UDP multicast at the IP TML level, a special parameter shall further be defined. The purpose of the parameter is to associate a PL level multicast ID to an IP level IP multicast address, in order for UDP to use the IP multicast address to multicast PL level messages. This parameter is to be defined as an TML media specific TML attribute as defined in [TML-SP], so that it can be set by CE PL layer. We call the attribute a "UDP multicast address for PL" attribute. The attribute therefore has the following element format:

UDP multicast address for PL =
Internet Draft  ForCES TML over IP  Mar. 2007

{multicast id, IP(UDP) multicast address}

Where, multicast id is the PL level destination ID for multicast, IP multicast address is a multicast IP address.

IP TML multicast can further be classified with four cases, according to the multicast message types and the transmission directions, as below:

1. Multicast control messages from a CE to FEs
2. Multicast redirect messages from a CE to FEs
3. Multicast control messages from a FE to CEs
4. Multicast redirect messages from a FE to CEs

They are described in details as below.

1. Multicast control messages from a CE to FEs

As described above, this case is mapped to IP TML with IP TML multiple unicast TCPs, and by the following steps:

a. CE PL (or its application layer) forms a PL level multicast list. TML Service Primitive has defined such multicast list as an TML attribute of TML [TML-SP] as below:

   multicast list = {multicast id, member1, member2, ... memberN}

   Where, multicast id is the PL level destination id for multicast, followed are the members of the multicast, including this CE ID and several FE IDs that are in the multicast group.

b. CE PL sends the PL multicast list to the CE TML by TMLconfig service primitive.

c. CE PL also use unicast to send the PL multicast list to all FE members by use of ForCES protocol configure messages. In every FE, the PL multicast list has been defined as an attribute of its FE protocol LFB.

The FEs further send the PL multicast list to the FE TMLs by means of TML service primitive.

d. When a CE PL use a TML send service primitive to send CE TML a control message with its destination ID being the multicast id as in the multicast list TML attribute, the CE TML distributes the messages to individual TCP connections according to the FE member IDs and the connection information in TML connection tables.
e. At the FE side, when such CE PL message arrives at individual FE TML in the multicast group, the FE TMLs just accept the message and deliver it to the FE PLs, for the FE TMLs know it is a member of the multicast from the multicast list TML attribute just configured.

3. Multicast redirect messages from a CE to FEs

As defined above, this multicast is mapped to IP TML with UDP multicast, and by the following steps:

a. CE PL (or its application layer) forms a PL multicast list and a UDP multicast address for PL. The UDP multicast list address for PL is defined as above.

b. CE PL then sends the PL multicast list and the UDP multicast address for PL to the CE TML by TML configuration service primitives.

c. When the CE TML receives the UDP multicast address for PL, it triggers some IP layer multicast protocol, like IGMP, to let the CE TML join in the IP multicast group designated by the IP multicast address in the UDP multicast address for PL.

d. CE PL also send the PL multicast list and the UDP multicast address for PL to all the multicast FE members by use of ForCES protocol configure messages. The FE members further send the lists to their TMLs.

e. When an FE TML has received the UDP multicast address for PL, it triggers some IP layer multicast protocol, like IGMP, to let the FE TML join in the IP multicast group.

f. When a CE generates and sends to the CE TML a PL redirect message with its destination ID being the multicast id, the CE TML will transmit the message by means of a UDP protocol with its IP address assigned with the IP multicast address designated by the UDP multicast address for PL.

g. At the FE side, because the TMLs of all multicast FE members have already joined in the IP multicast group, any of the FE TMLs can receive the packet transported by step f). The TML further deliver the redirect message to its PL layer, finishing the transportation of ForCES redirect messages from CE to FEs by means of UDP multicast.

3. Multicast control messages from a FE to CEs

(TBD)

4. Multicast redirect messages from a FE to CEs
5.6. Prioritization

This IP TML can meet the different prioritization from PL level by use of several TCP-UDP pair connections between one same CE and one same FE.

5.7. Encapsulation

1. TCP Encapsulation

When ForCES PL messages are transported over TCP, a TCP port number or port numbers (if multiple TCP connections are established) that are specifically assigned for ForCES protocol should be adopted.

The encapsulation format is as below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  TCP header with the port number for the ForCES protocol                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                      |
|                                                      |
|                                                      |
|                                                      |
|                                                      |
~                    ForCES PL Message                          ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2. UDP Encapsulation

When ForCES PL messages are transported over UDP protocol, a UDP port number that is specifically assigned to ForCES protocol should be used.

The encapsulation format is as below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  UDP header with the port number for the ForCES protocol                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                      |
|                                                      |
|                                                      |
|                                                      |
|                                                      |
~                    ForCES PL Message                          ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
6. Security Considerations
   (TBD)

7. IANA Considerations
   The Following Assigned Numbers are considered:
   TCP Port Number(s) for ForCES Protocol
   UDP Port Number for ForCES protocol

8. References
   [RFC3654] H. Khosravi, et al., Requirements for Separation of IP
             Control and Forwarding, RFC 3654, November 2003.
   [RFC3746] L. Yang, et al., Forwarding and Control Element Separation
             (ForCES) Framework, RFC 3746, April 2004.
   [ForCES-PL] A. Doria, et al., ForCES protocol specifications, draft-
   [ForCES-Model] J. Halpern, E. Deleganes, ForCES Forwarding Element
   [TML-SP] W. M. Wang, J. Hadi, et al., ForCES TML Service Primitives,
            work-in-progress, draft-ietf-forces-tmlsp-01.txt, Feb., 2007
               Proceedings of 59th IETF Meeting, 2004, Feb.29-Mar.4, Seoul, Korea,

9. Author’s Address

Weiming Wang
Zhejiang Gongshang University
149 Jiaogong Road
Hangzhou  310035
P.R.China
Phone: +86-571-28877721
EMail: wmwang@mail.zjgsu.edu.cn

Ligang Dong
Zhejiang Gongshang University
149 Jiaogong Road
Hangzhou  310035
P.R.China
Phone: +86-571-28877751
EMail: donglg@mail.zjgsu.edu.cn

Bin Zhuge
Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.