



**Feedback Resolution for Payload Loopback Discussion
from Sept2005 802.1 Meeting**


Linda Dunbar: ldunbar@futurewei.com

Bob Sultan: bsultan@futurewei.com

Steve Plote: steve.plote@lglass.net

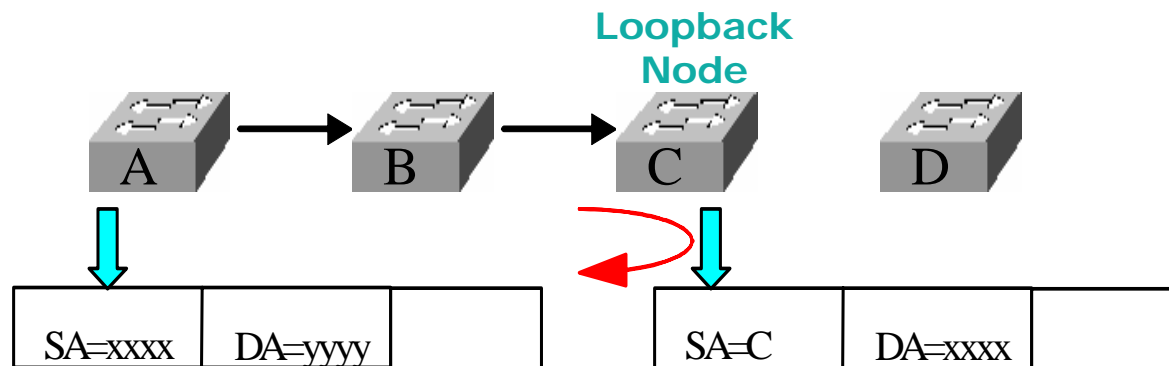
Lucy Yong: lucy.yong@wiltel.com

Nov, 2005


- 
- **Payload loopback was discussed at the IEEE802.1 Sept 2005 interim meeting. Here are the major feedback coming out of the discussion in Sept:**
 - **When the loopback node loops back the packets, it should use its own MAC address in the SA field to avoid messing up the MAC learning on the intermediate nodes.**
 - **Should consider 802.3ah's keep alive method to keep the payload loopback process on going.**
 - **Using SVID + MAC as identifier for flow of packets to be looped back**
 - **Comparison of Payload Loopback with the Y.17EtherOAM Test Msg**

Mechanism to avoid unwanted loops and avoid messing up MAC Learning in the network

- When the loopback node loops back the packets, it uses the original Source MAC as DA, and use its own MAC as SA



Reference: 802.3ah Payload Loopback

- 
- **802.3ah payload loopback is restricted to a single link**
 - **802.3ah Payload Loopback Protocol:**
 - **Loopback is initiated by sending Loopback Control OAMPDU with the loopback enabling command**
 - Receiving node is required within a second to send back Information OAMPDU after proper processing within the node is completed.
 - When contention occurs, i.e. both nodes send Loopback Control OAMPDU simultaneously: the higher source address takes precedence.
 - **During loopback:**
 - All “non OAMPDU” frames are looped back without altering any field.
 - Both DTEs are required to continuously send OAMPDU to keep the loopback alive. (no frequency is specified though)
 - **Exiting the loopback** by sending a loopback Control OAMPDU with the Disable OAM Remote Loopback command and receiving node sending back Information OAMPDU as confirmation

Reference: Loopback Code Defined by IEEE802.3ah

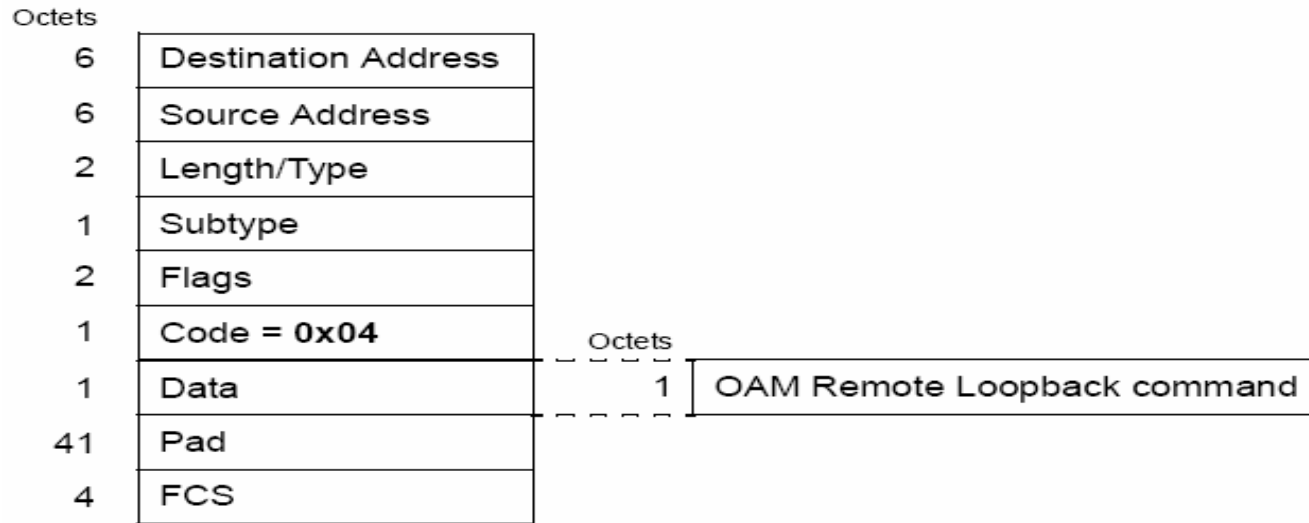


Figure 57–14—Loopback Control OAMPDU frame structure

Table 57–5—OAM remote loopback commands

Command	Description
0x00	<i>Reserved - shall not be transmitted, should be ignored on reception by OAM client</i>
0x01	Enable OAM Remote Loopback
0x02	Disable OAM Remote Loopback
0x03-0xFF	<i>Reserved - shall not be transmitted, should be ignored on reception by OAM client</i>



Extra Steps for Payload Loopback In Bridged Network

- **To make sure that only one payload loopback can be enabled within a maintenance domain:** (Achieved by Loopback Reservation)
 - To prevent network overload caused by multiple loopback being initiated within the same time period
 - To prevent unwanted loopback initiated by 3rd party which is not agreed by the source.
 - 802.3ah's contention scheme of using MAC address order is not enough
- **Loopback node needs to change DA and SA when looping back packets.**
 - Shown in the previous page
- **Flow based loopback, where flow is identified by SVID + Source MAC**

Protocol for the Payload Loopback in Bridged Network



Payload Loopback reservation:

- To make sure that there is only one loopback to be activated within one maintenance domain.

Starting Payload Loopback (Handshake Process)

- To make sure that both source and loopback nodes agree upon the loopback term and confirm the loopback

During Payload Loopback:

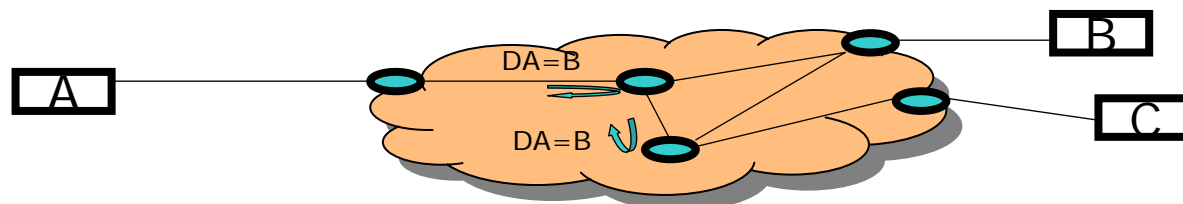
- Both Source and the Loopback Node exchange periodic Loopback request command to keep the Payload Loopback status alive
- The Loopback Node will alter DA and SA before sending back all the “Non-OAMP” packets with the specified S-VID and Source MAC :


Exiting Payload Loopback

- Explicit request from the Source node to terminate the Loopback action
- Timeout

Comparison of Payload Loopback with Y.17EtherOAM Test Msg

- **Payload represents a special traffic pattern which are unique in diagnosing intermittent network problems**
- **Y.17 Test Msg are for different trouble shooting purpose than Payload loopback.**
 - The destination address of the bi-directional Test Msg is the node to loop back the packets.
 - Y.17 Test Msg can't trouble shoot network segments with packets destined towards a customer MAC
 - Transport Network has both PRBS testing and Payload Loopback diagnostic tools for many years. Both diagnostic tools are needed by operators for different purposes
- **Payload loopback can apply to flows with MAC address from customer domain and an unique SVID**
- **Y.17 Test Msg doesn't have the mechanism defined to avoid network overload with multiple test streams from multiple nodes simultaneously.**
- **Payload loopback not only can be used to diagnose payload performance of nodes on the expected route, it can also be used to test if unexpected nodes are traversed by the specified payload.**

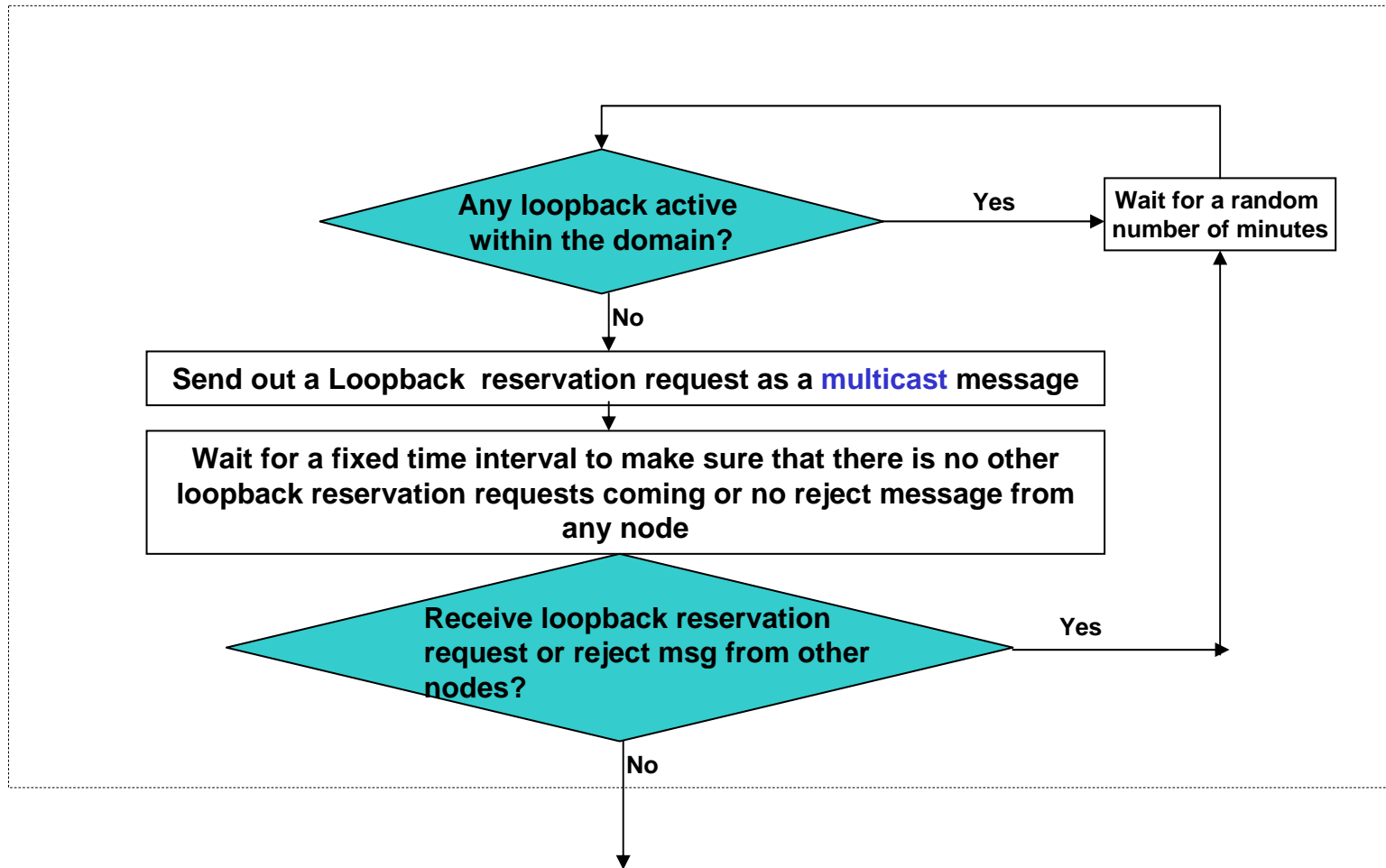


- 
- **Reserve a section in 802.1ag for payload loopback**
 - **Define a code to enable/disable protocol triggered payload loopback**




Backup Slides

Details of Payload Loopback Reservation Stage



Next Stage

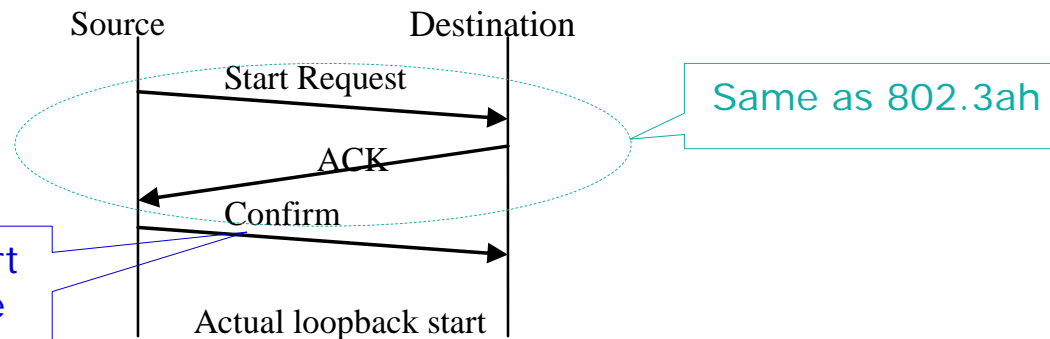
Loopback Reservation Reject

- 
- **Loopback Reservation request can be rejected by the following conditions:**
 - There is already an active payload loopback in the administrative domain
 - The source or destination node specified by the Loopback Reservation request don't want to proceed with the loopback
 - In case the loopback is initiated by the 3rd party which is not agreed by the source.
 - **Loopback Reservation Reject should be sent to both originating node and the node which is to perform the loopback**
 - The reason that the loopback node has to be informed of the rejection is to make sure that the loopback node will not perform any loopback which is rejected.
 - This step is to prevent any node from requesting a loopback without the proper reservation being granted.

Handshake to Start the Payload Loopback Stage

○ Handshake between Source and Destination

- To reach agreement on the loopback term and confirm the loopback
- To make sure that the destination node will not acknowledge any loopback request without prior reservation
- To mark the START and END of the loopback




Extra step to formally start the loopback to make the process more robust

Same as 802.3ah


○ Time to Live:

- To prevent free run loopback (i.e. never stop) caused by network node or link failure
- To let all the other nodes keep track of on-going loopback which might be active in the administrative domain.

Why Payload Loopback?

- 
- **For fault localization and performance testing with the original payload traffic over a fixed period of time.**
 - **Actual payload traffic are needed over a period of time for diagnosing special performance issues in the network!**
 - When customer encounters packets drops or bandwidth between two end points (A and B) not meeting the SLA, customer and provider need to trouble shoot where the packet drops occur and where the bottleneck is for the bandwidth drop.
 - Ping like message is not enough.

Why need protocol triggered payload loopback?

- 
- **To verify if a particular flow over a service instance (specified by S-VID) of payload can reach an immediate node with full bandwidth within a specified time span, without operator's intervention**
 - **Easy, convenient, and can be performed without provider's intervention**
 - Whenever a user needs to trouble shoot intermittent network problems, he can initiate the loopback independently, without service provider's assistance, which greatly reduce service provider's maintenance cost.
 - **No need for interoperable network management systems**
 - The loopback can be triggered and go through 3rd party vendor networks without interoperable network management interface
 - As being proven in reality, it is extremely difficult to have interoperable network management systems to manage end to end operations for network with multiple vendors' equipment
 - **To verify if a particular packet flow over a service instance traverse through the specified nodes, either expected or unexpected.**