



[LoopTelecom.com](http://LoopTelecom.com)

# **Migration of a Secure TDM Network to a Packet-based Network**

## **Introduction**

In a traditional TDM network, when secure communications are required, users often use link encryption technology, which requires no change on terminal devices. Rapid development of IP-based technologies with their low-cost nature leads migration of TDM to IP technology. During the transition, the planner has to preserve interoperability of the two networking technologies and maintain security of the communications. This white paper proposes a solution that uses a centralized packet processing for the transition.

## **Legacy Secure TDM Network**

The traditional TDM network provides secure communication with two possible technologies, the end-to-end encryption and link encryption. The end-to-end technology does data encryption inside the terminal equipments that allows per-user based encryption policy. This method ensures only authorized user can see plain text. The network maintainer must carefully configure the equipments and educate users, or user errors can compromise security.

Another technology, link encryption (shown as Figure 1), does encryption on the outgoing TDM wire, so any terminal equipment can gain same level of communication security without any change. Because of the central nature, a network maintainer only needs to pay attention on the setting of the encryption device. (Users are usually not aware of existence of the encryption.)

Because the link encryption does the encryption on external wire, when a network is transiting from TDM to IP, users have choices to integrate the original secure TDM channel with the new IP network. This offers more flexibility.

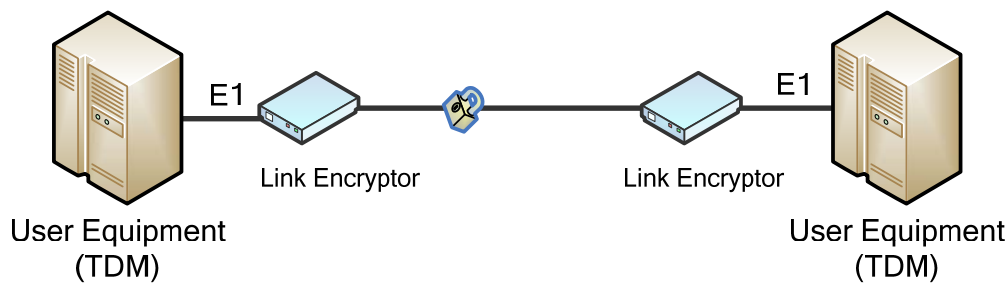


Figure 1 TDM link encryption

## Transition Options

When a network is moving from TDM-based technology to packet-based technology, an indispensable issue is how to keep legacy TDM devices in operation. TDM over IP that packetizes TDM bit stream and transports it over a packet network is considered a good solution, shown in Figure 2.

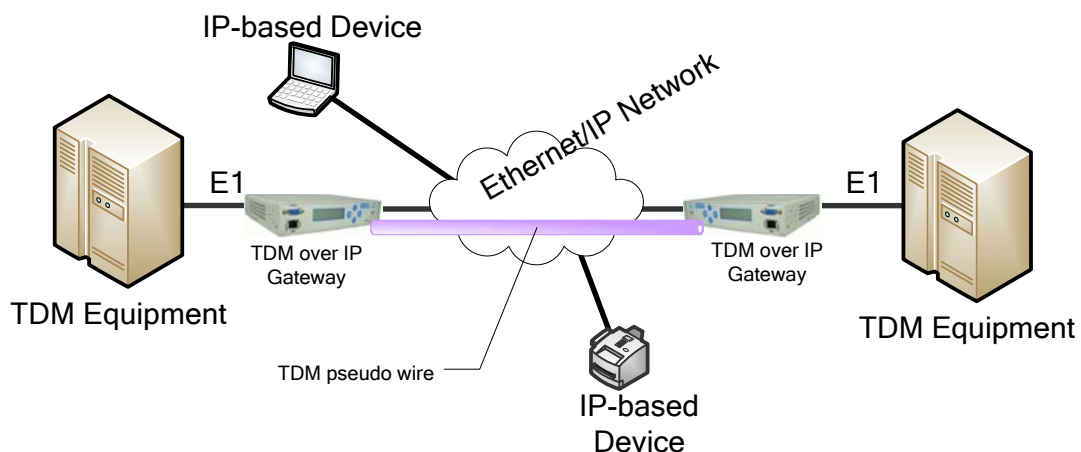


Figure 2 Merging TDM with a packet network

In such mixed network, users can implement their secure communications with two options:

- Keeping the original TDM link encryptor for the TDM bit stream and adding another packet encryptor for packet traffics.
- Introducing only a packet encryptor that encrypts both packetized TDM data and other native IP traffics (shown as Figure 3).

A design of a TDM over IP network must consider two important factors, packet transmission delay and packet loss. TDM latency is affected by TDM packetization



[LoopTelecom.com](http://LoopTelecom.com)

delay and packet transmission delay. In most of cases, the packet transmission delay can contribute significant TDM latency because of routing (switching) delay and its variation. To minimize the TDM latency, network devices should service the TDM packets with high priority to minimize routing/switch delay and the variation. Additionally, the TDM packets must also have low drop eligibility, so when network congestion happens, the TDM traffic can still gain service without packet loss.

With the single packet encryptor solution, the central controlled packet processing allows the encryptor to provide better packet classification and prioritization that enables easier traffic engineering. This simplifies network setting.

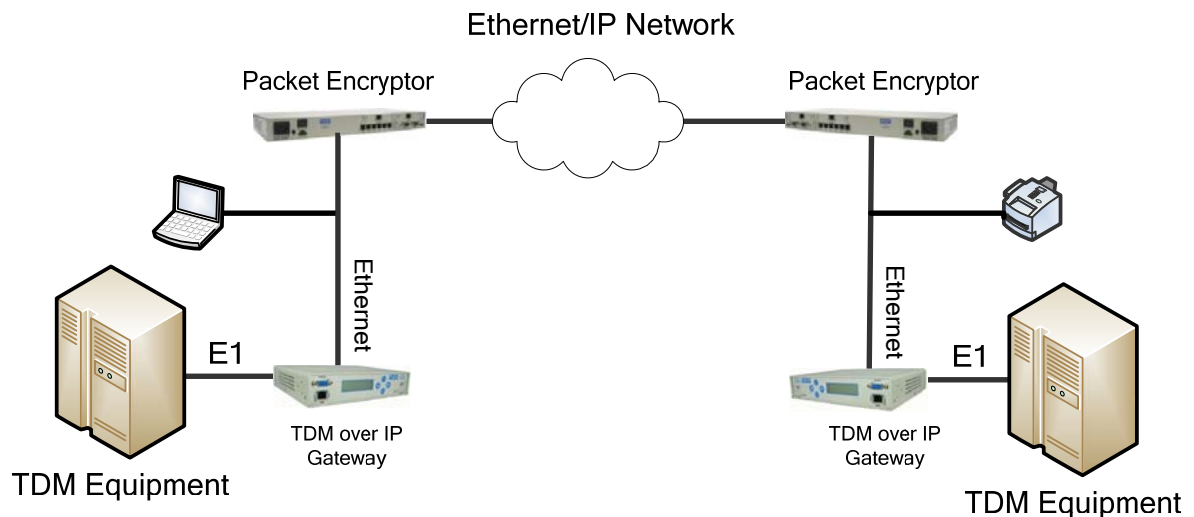


Figure 3 Single packet encryption device

## A Pure Packet-based Network

Once users successfully replace all TDM equipments with IP-based devices, the users can remove the TDM over Ethernet gateways from the transition network.

During this stage, the user only needs to re-set policies in the encryptor for encrypting classes of traffics accordingly.

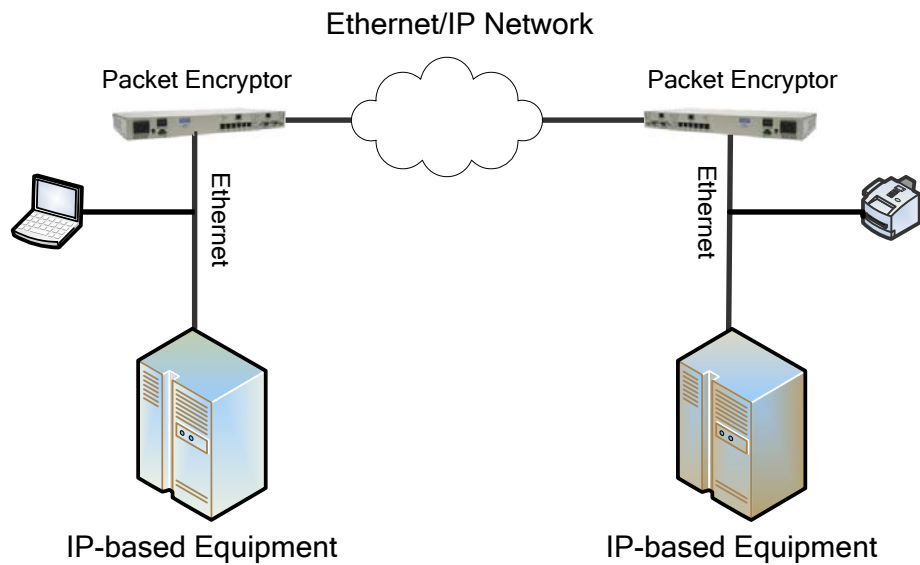


Figure 4 Final packet network

## Conclusion

The white paper presents an approach that allows a smooth transition of TDM to IP. The approach does integrated encryption, traffic classification and engineering with a single device. For some special security applications, like military and government communications, users may require replaceable encryption module with specialized encryption algorithms, which usually has higher investment cost. In such cases, users need a gradual transition solution that maximizes reusability of the encryption devices to lower the migration cost.