Link– end to end encryption
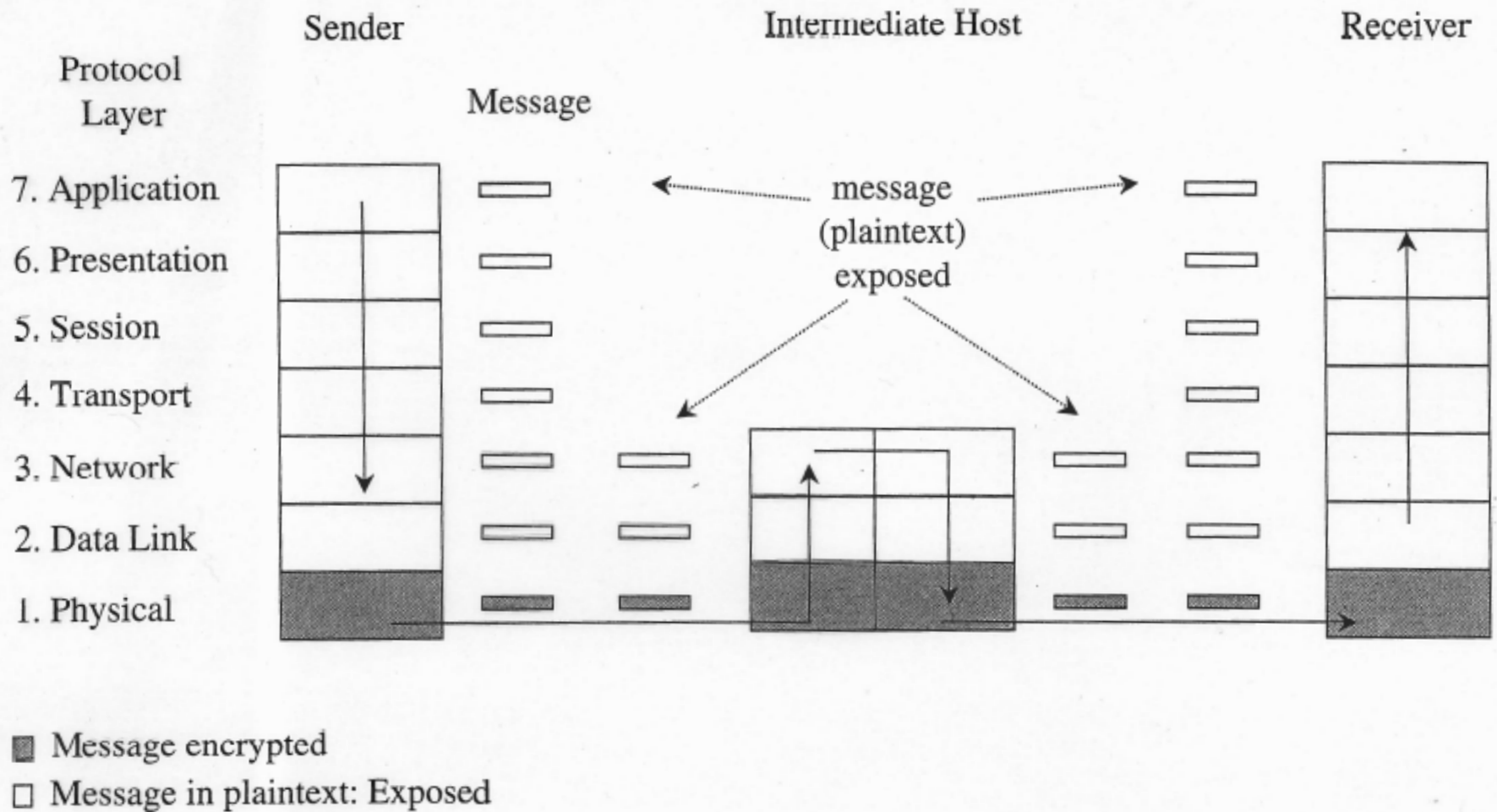
TABLE 7-5   Comparison of Link and End-to-End Encryption.
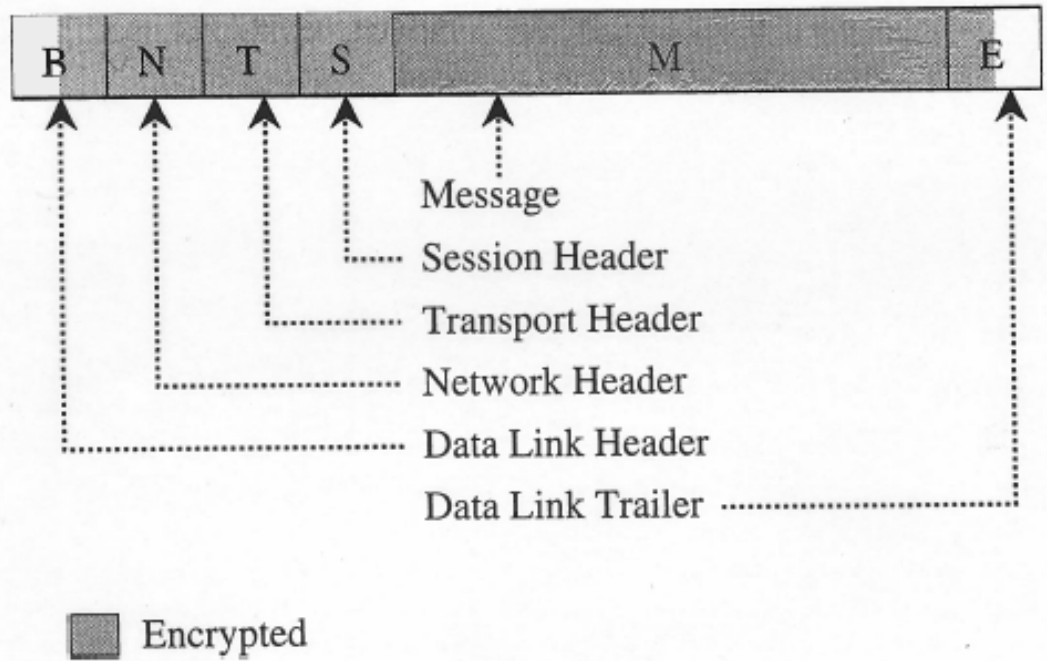
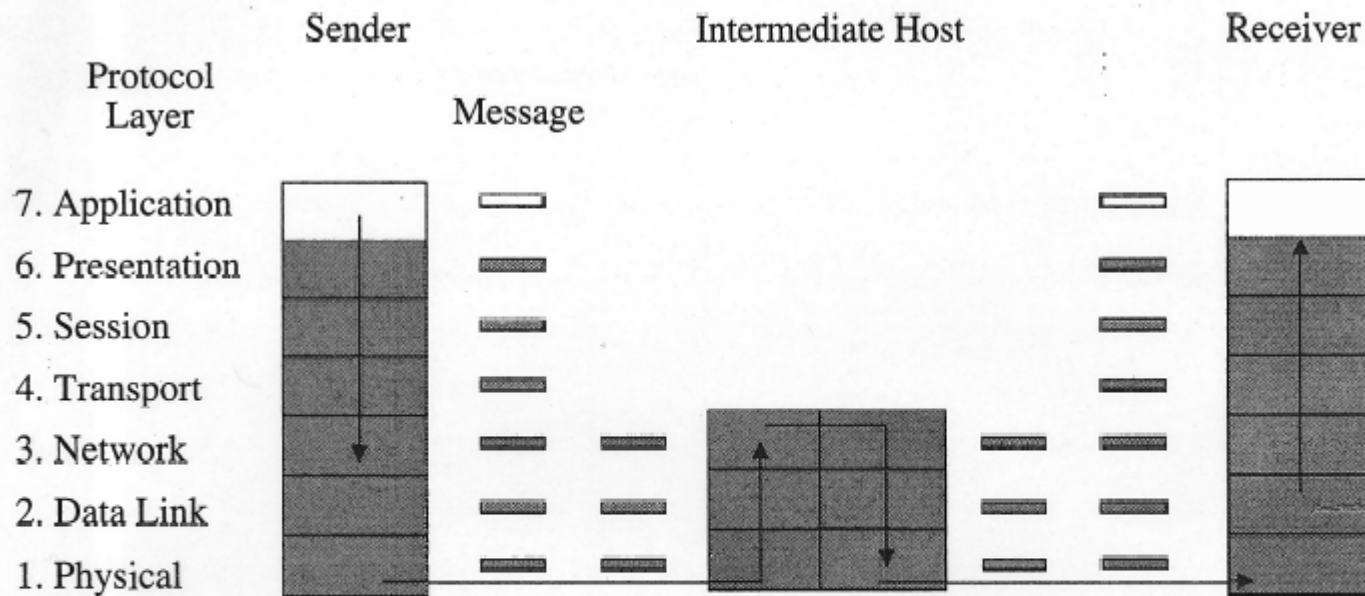| Link Encryption	End-to-End Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate nodes	Data encrypted in intermediate nodes
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One facility for all users	User selects encryption
Typically done in hardware	Either software or hardware implementation
All or no data encrypted	User chooses to encrypt or not, for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

FIGURE 7-21 Link Encryption.

Courtesy of Pfleeger & Pfleeger: "Security in Computing"

| B | N | T | S | M | E |

Message
Session Header
Transport Header
Network Header
Data Link Header
Data Link Trailer

FIGURE 7-22 Message Under Link Encryption.

▨ Encrypted

FIGURE 7-23   End-to-End Encryption.

Message

Session Header

Transport Header

Network Header

Data Link Header

Data Link Trailer
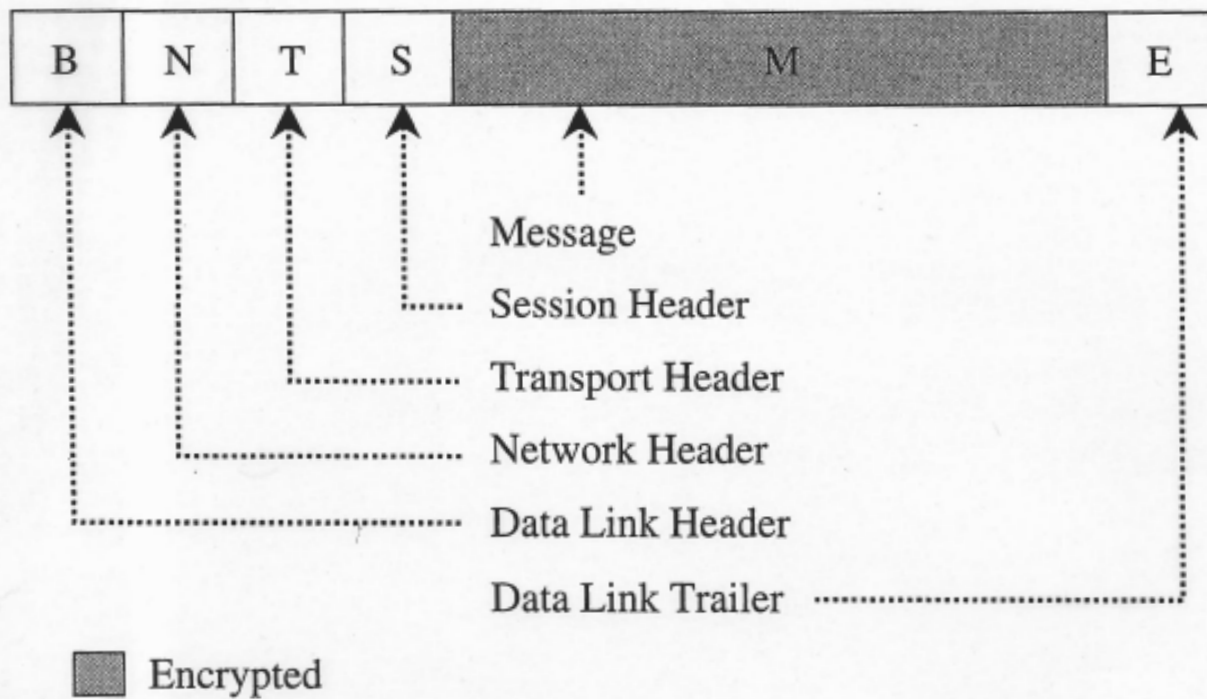
Encrypted

FIGURE 7-24 End-to-End Encrypted Message.

TABLE 7-5   Comparison of Link and End-to-End Encryption.

Link Encryption	End-to-End Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate nodes	Data encrypted in intermediate nodes
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One facility for all users	User selects encryption
Typically done in hardware	Either software or hardware implementation
All or no data encrypted	User chooses to encrypt or not, for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication