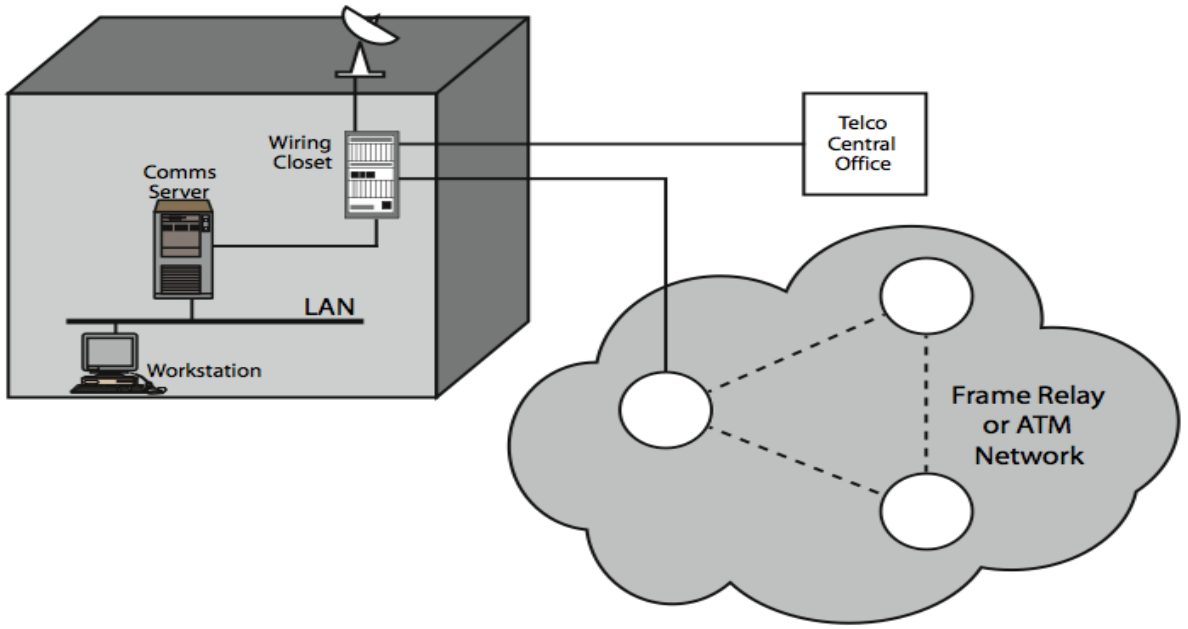
Confidentiality using Symmetric Encryption (CS-352)

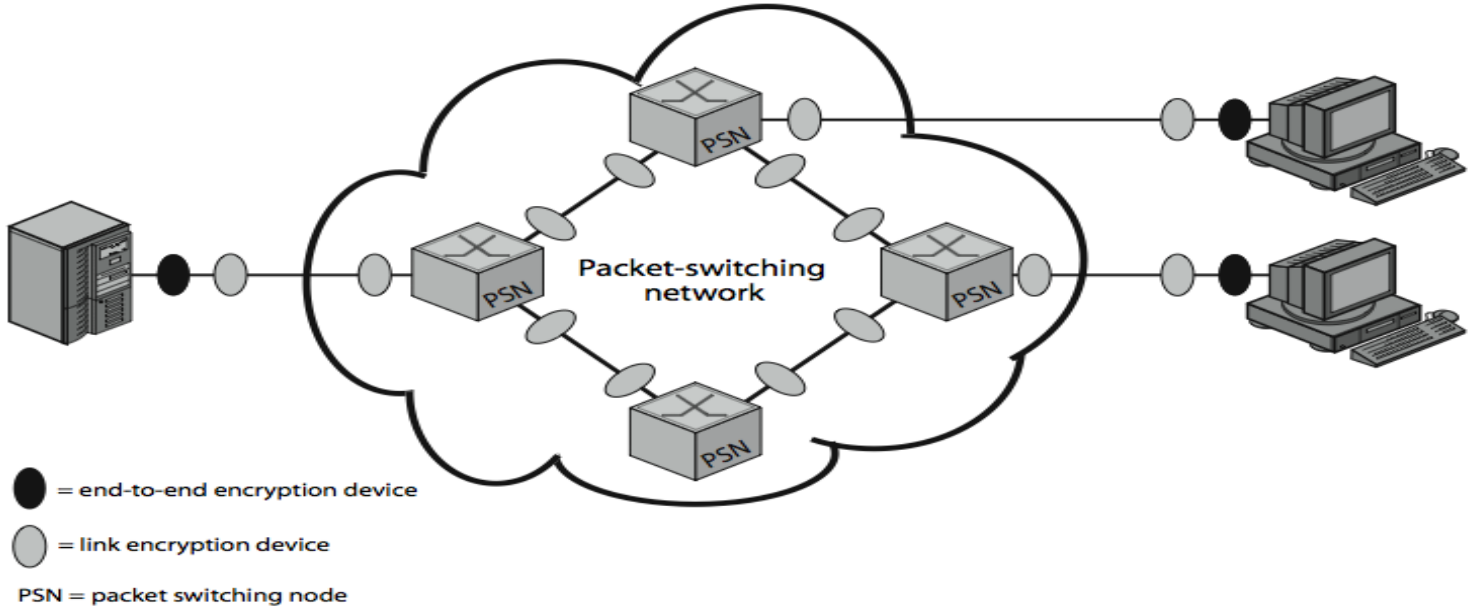
The Use of Symmetric Encryption to Provide Confidentiality

- In most organizations, workstations are attached to local area networks (LANs).
- Packets transmitted contain the source and destination address
- An eavesdropper can monitor the traffic on the LAN and capture any traffic desired on the basis of source and destination addresses.



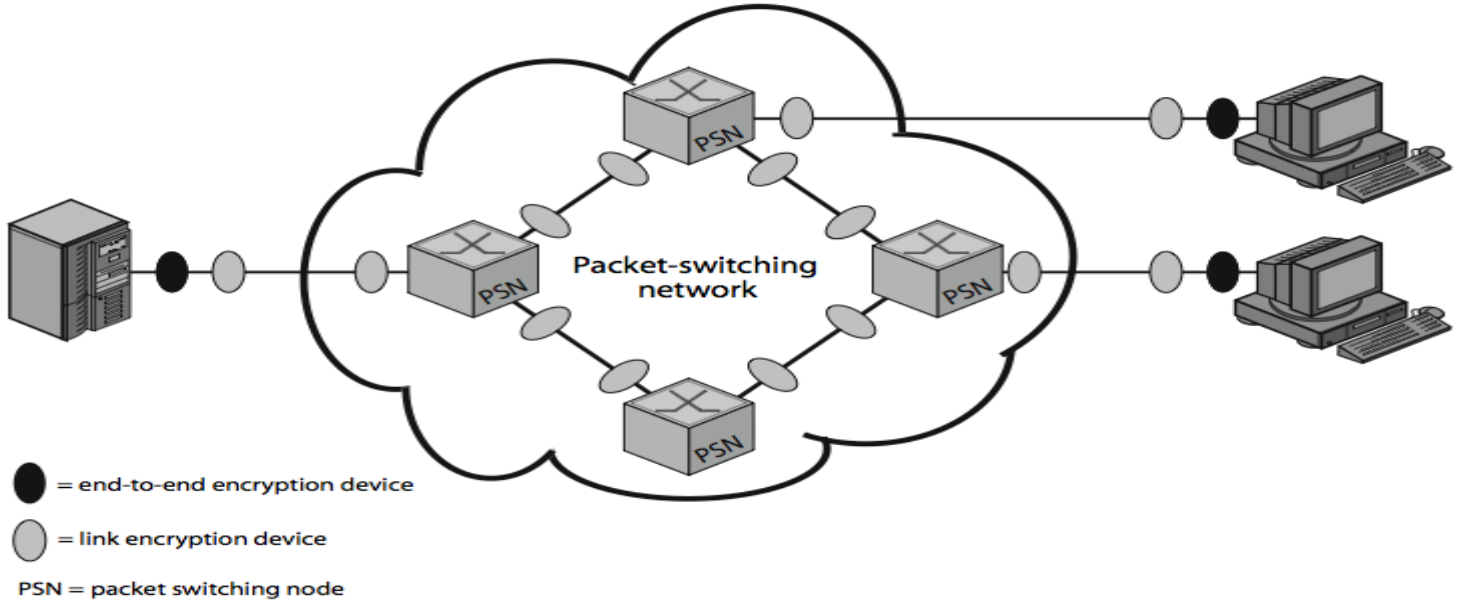
Placement of Encryption

- Link encryption
  - Encryption occurs independently on every link
  - Each vulnerable communications link is equipped on both ends with an encryption device.
  - Requires many encryption devices in a large network
  - Each pair of nodes that share a link should share a unique key – many keys must be provided



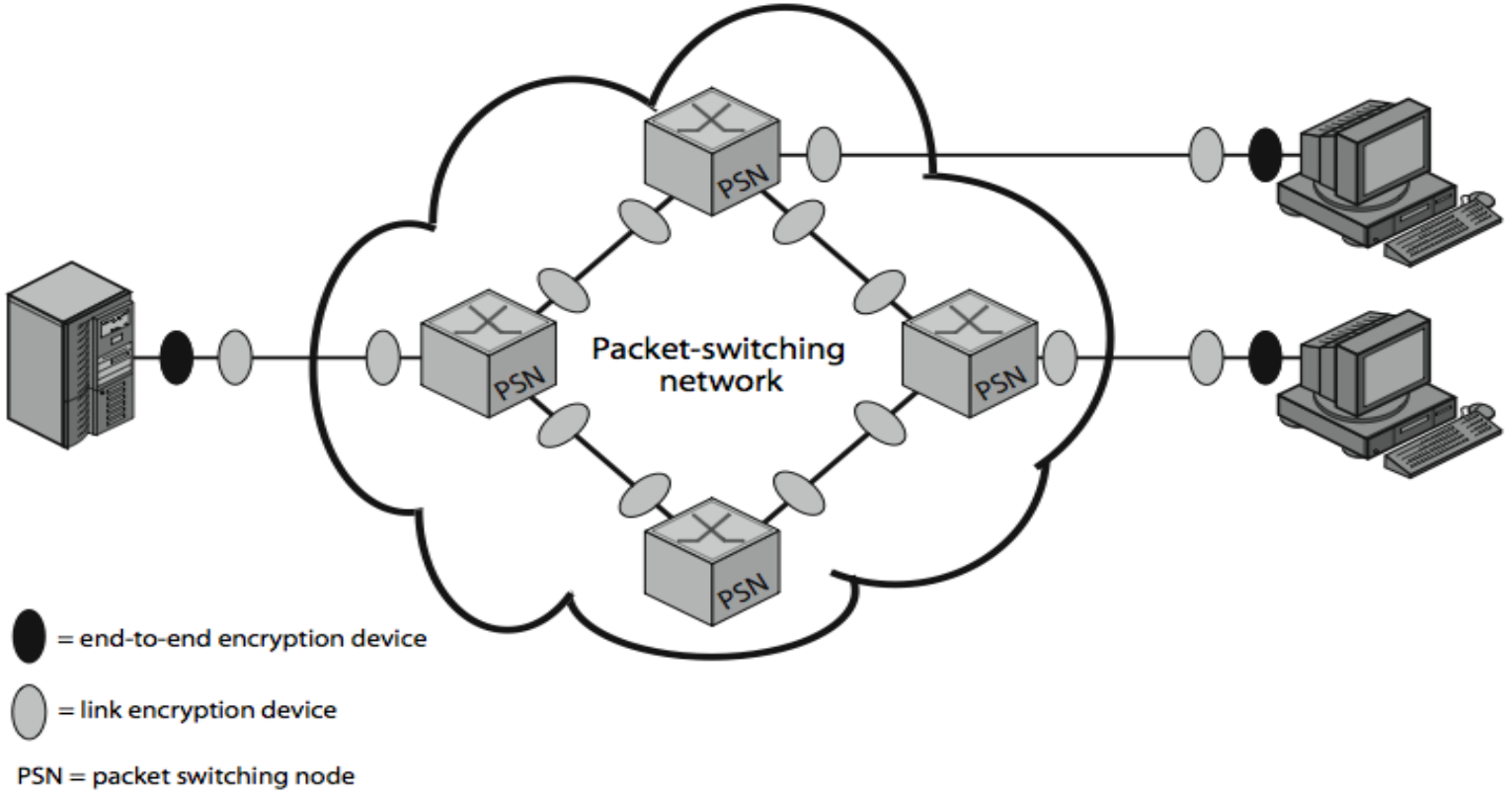
Placement of Encryption

- Link encryption
  - Encryption occurs independently on every link
  - Each vulnerable communications link is equipped on both ends with an encryption device.
  - Requires many encryption devices in a large network
  - Each pair of nodes that share a link should share a unique key – many keys must be provided



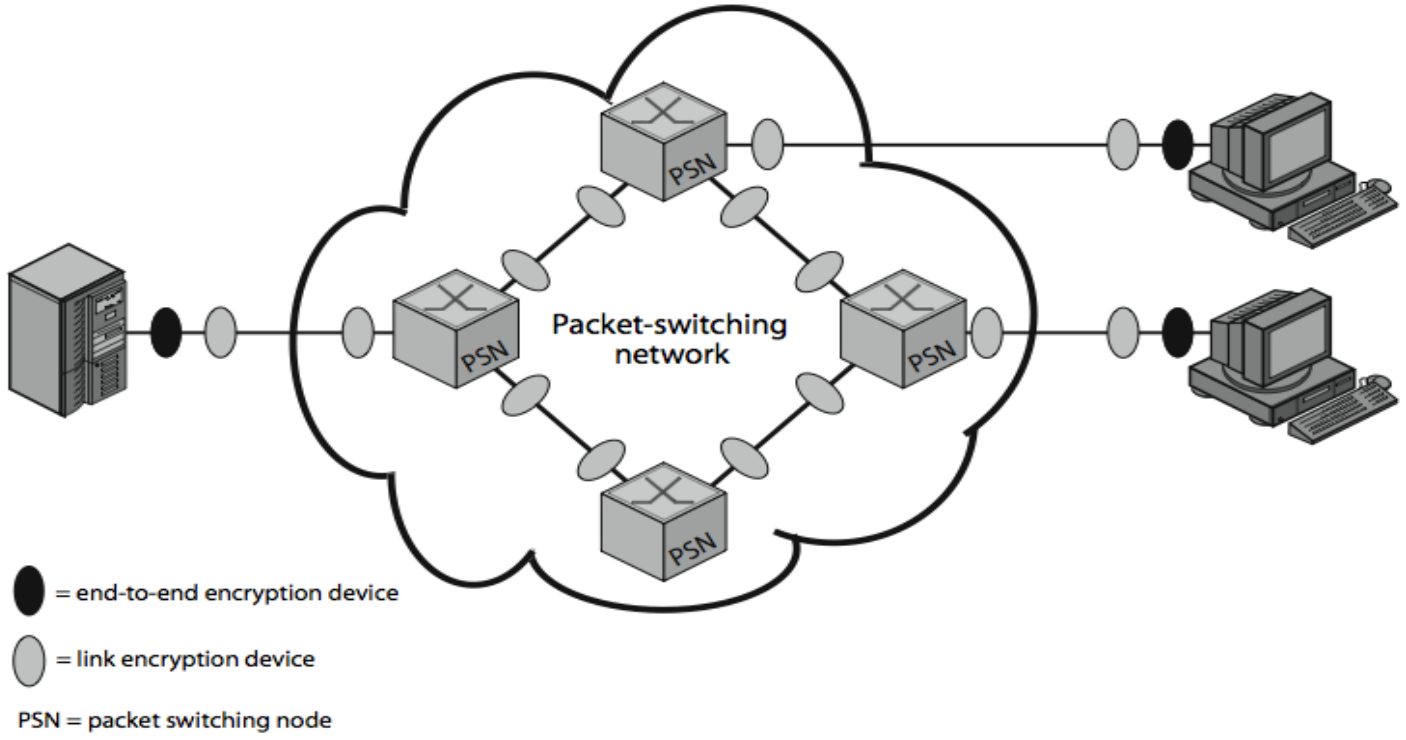
Placement of Encryption

- Disadvantage: the message must be decrypted each time it enters a switch because the switch must read the address in the packet header in order to route the message - the message is vulnerable at each switch.



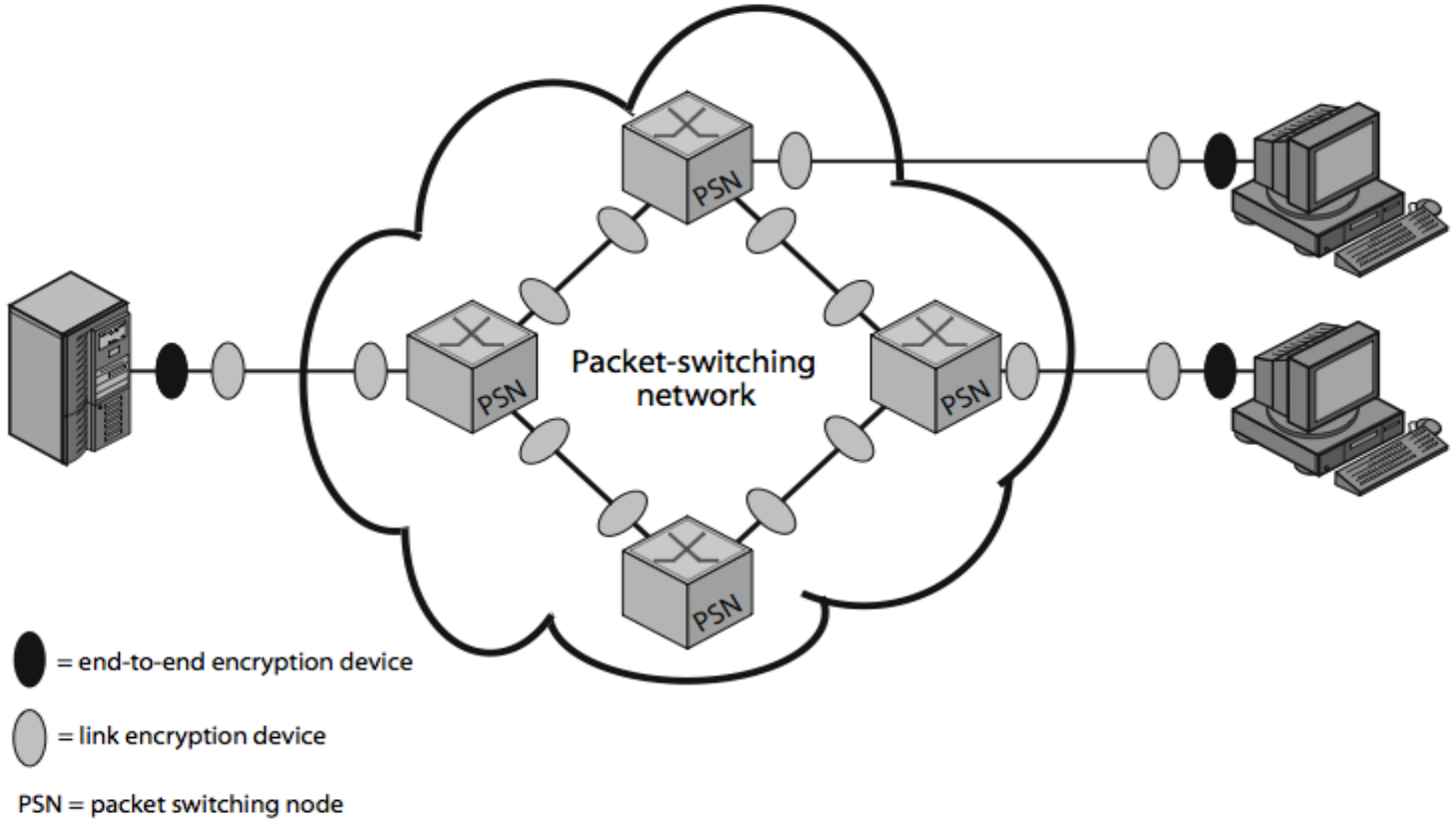
Placement of Encryption

- End-to-end encryption
  - Encryption occurs between original source and final destination.
  - The data in encrypted form are transmitted across the network to the destination terminal or host.



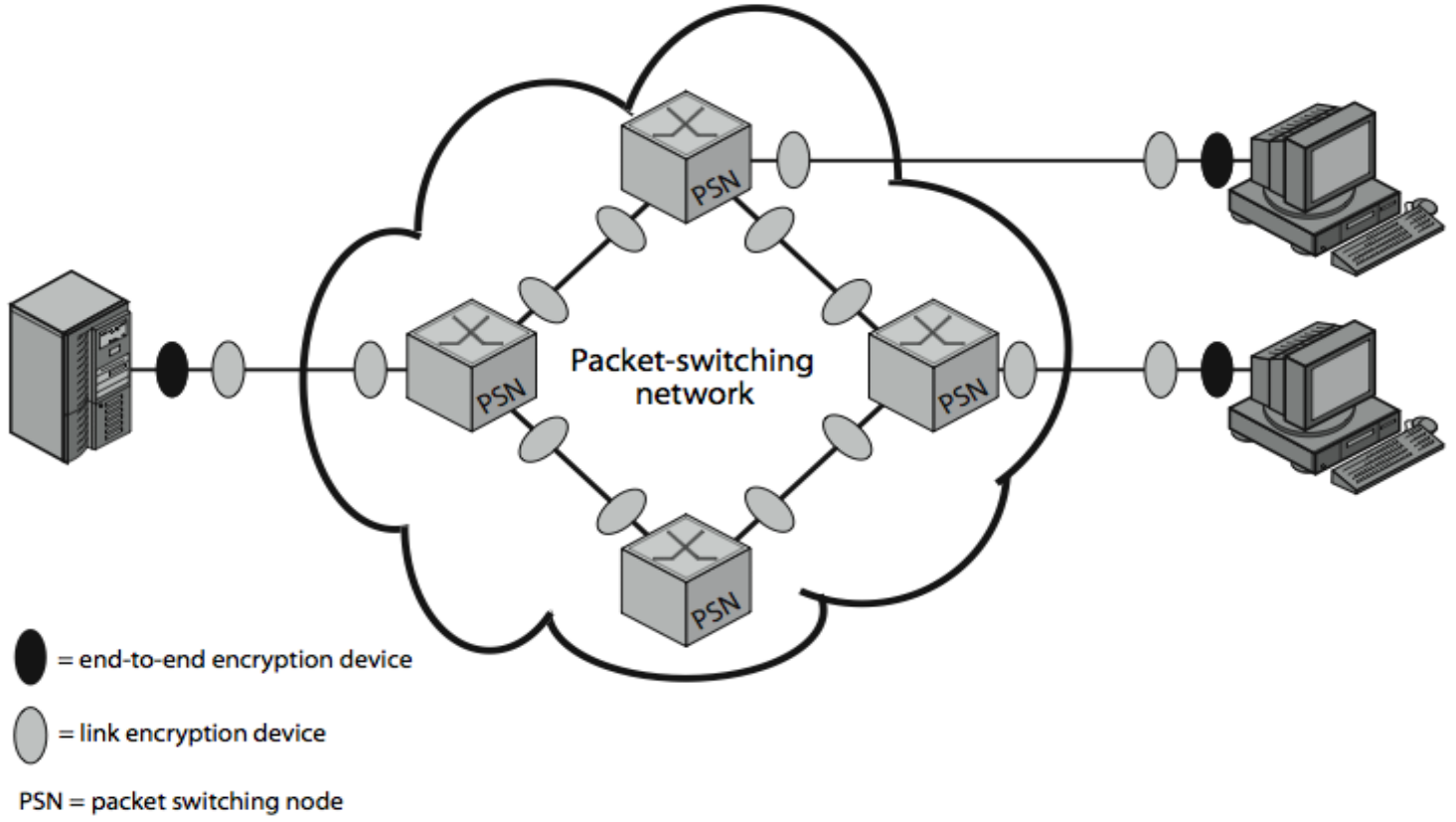
Placement of Encryption

- End-to-end encryption
  - The destination shares a key with the source and hence is able to decrypt the data.



Placement of Encryption

- End-to-end encryption
  - The destination shares a key with the source and hence is able to decrypt the data.



End-to-End Encryption

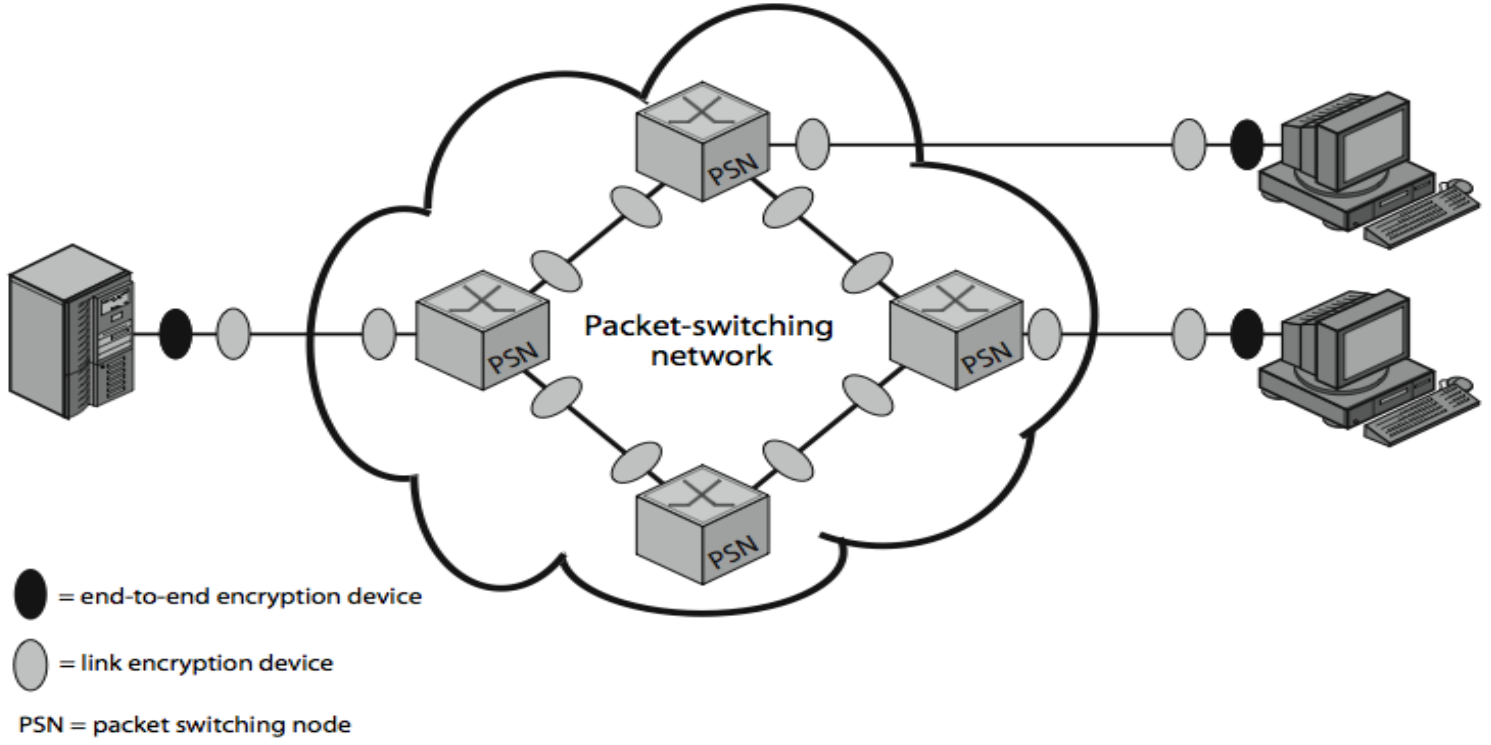
- Can we encrypt the entire message?

End-to-End Encryption

- Can we encrypt the entire message?
  - Does not work
  - Packet: a header and some user data.
  - The switch will receive an encrypted packet and be unable to read the header - must leave headers in clear
  - Contents protected, traffic pattern flows are not

Ideally, Want Both

- Ideally want both at once
  - End-to-end protects data contents over entire path and provides authentication
  - Link protects traffic flows from monitoring



Solution

- The host encrypts the user data portion of a packet using an end-to-end encryption key
- The entire packet is then encrypted using a link encryption key
- As the packet traverses the network, each switch
  - Decrypts the packet
  - Uses a link encryption key to read the header
  - Encrypts the entire packet again for sending it out on the next link

Traffic Analysis

- Still possible for an attacker to access the amount of traffic on a network and to observe the amount of traffic entering and leaving each end system.

Traffic Analysis

- Traffic analysis is the process of monitoring communications flows in order to deduce information from patterns in communication.
- Following types of information can be derived from a traffic analysis attack:
  - Identities of partners
  - Message length
  - How frequently the partners are communicating
    - Frequent communications — can denote planning
    - A lack of communication — can indicate a lack of activity
- Useful both in military & commercial spheres

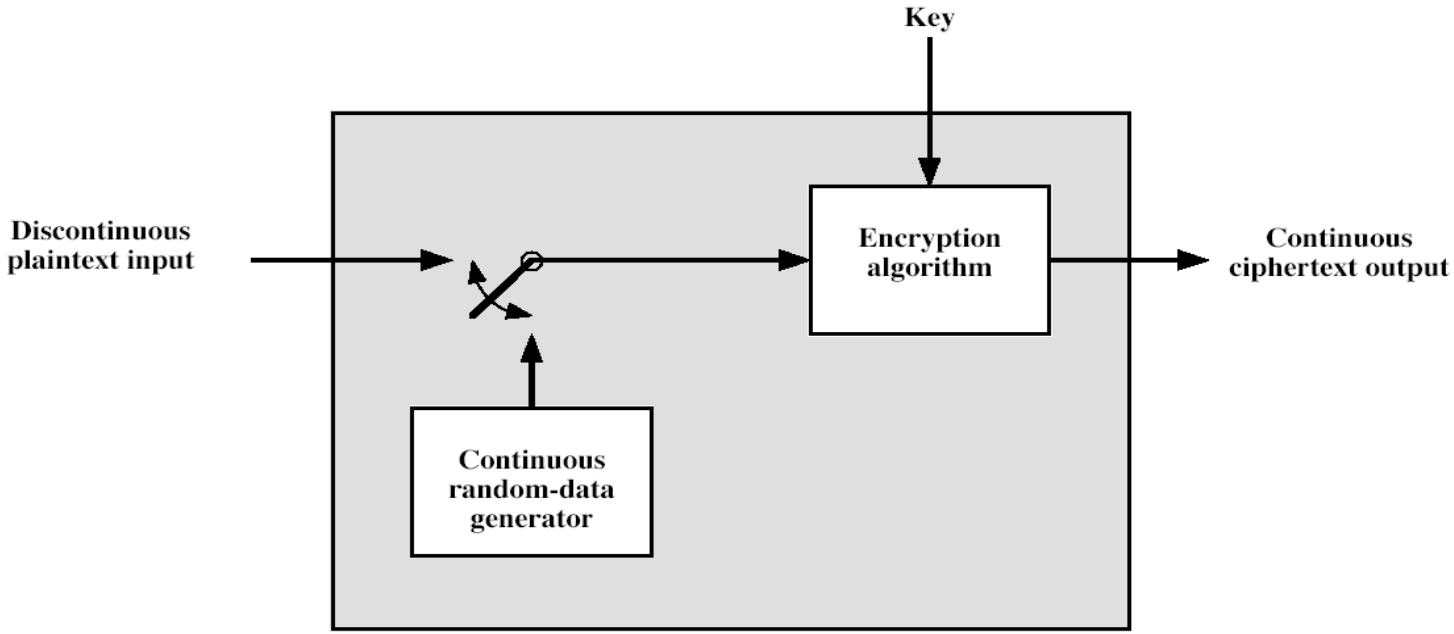
Traffic Analysis

- Can also be used to create a covert channel
  - Covert channel: a means of communication in a fashion unintended by the designers of the communications facility.
  - The channel is used to transfer information in a way that violates a security policy
  - Example:
    - The employee may wish to communicate information to an outsider in a way that is not detected by management.
    - The two participants could set up a code in which a legitimate message of a less than a certain length represents binary 0, whereas a longer message represents a binary 1.

Countermeasures: Traffic Analysis

Countermeasures: Traffic Analysis

- Traffic padding can further obscure flows
  - Produces ciphertext continuously, even in the absence of plaintext. A continuous random data stream is generated
    - When plaintext is available, it is encrypted and transmitted.
    - Otherwise, random data are encrypted and transmitted.
  - At cost of continuous traffic



Credits

- Many slides borrowed from Dr. Ping Yang from State University of New York at Binghamton