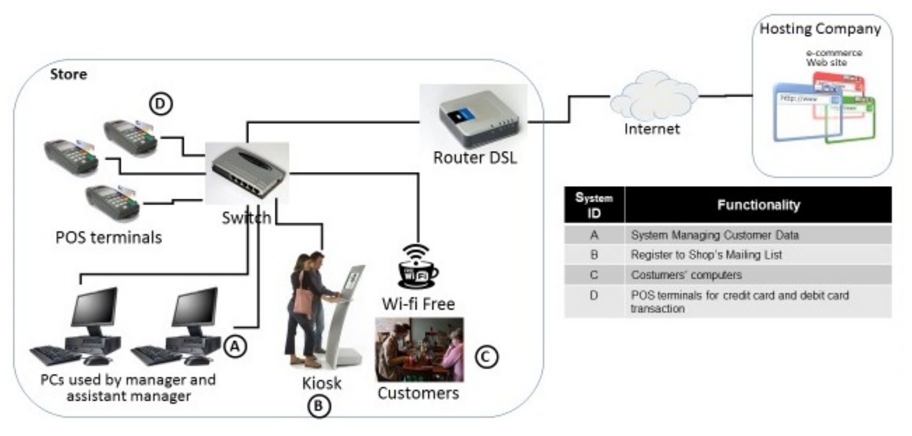
Flat Network

Network Description

> ”Joe’s Jumping Jerky Joint is a small company, it has four stores and an e-commerce Web site that accepts credit cards for payment. It was notified by one of his acquirers that it is now a Level 3 merchant and must demonstrate its compliance with the PCI DSS. Joes Jumping Jerky Joint stores use IP-based Point of Sale (POS) terminals. The POS terminals share infrastructure with some nonpayment machines. There are two PCs that are used by the manager and assistant manager of each store to browse the WEB, check e-mail, and access the order fulfillment screens from the online store. There is one kiosk in the store that allows customers to sign up for e-mail updates. The stores have free Wi-Fi to customers who come to the caf. There isn’t segmentation between wireless network and the wired infrastructure. Each store connects to the Internet via a business class Digital Subscriber Line (DSL) for his Internet service. The business class DSL came with an upgraded router that provides the capability to create a DMZ, but the company not used this functionality to date. For the Web site, the hosting facility needs ensuring that they are providing a PCI compliant solution.” [1, p. 7].

Figure 1 describes the scenario which was also complemented by textual description from the book.



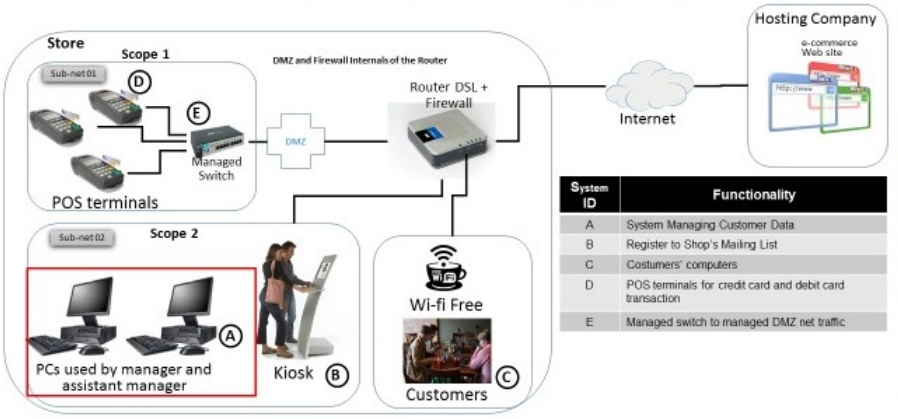
System ID	Functionality
A	System Managing Customer Data
B	Register to Shop's Mailing List
C	Costumers' computers
D	POS terminals for credit card and debit card transaction

ID	Description
A	PCs that are used by the manager and assistant manager of each store to browse the WEB, check e-mail, and access the order fulfillment screens from the online store.
B	There is one kiosk in the store that allows customers to sign up for e-mail updates. It is not fully up-to-date with PCI standards.
C	Free Wi-Fi to customers who come to the cafe.
D	POS are used by vendors to handle payment for purchases made by customers.

Fig. 1: Flat Network – Before Compliance with PCI DSS

> "Joe's Jumping Jerky Joint is a small company, it has four stores and an e-commerce Web site that accepts credit cards for payment. It was notified by one of his acquirers that it is now a Level 3 merchant and must demonstrate its compliance with the PCI DSS. Joes Jumping Jerky Joint stores use IP-based Point of Sale (POS) terminals. The POS terminals share infrastructure with some nonpayment machines. There are two PCs that are used by the manager and assistant manager of each store to browse the WEB, check e-mail, and access the order fulfillment screens from the online store. There is one kiosk in the store that allows customers to sign up for e-mail updates. The stores have free Wi-Fi to customers who come to the caf. There isn't segmentation between wireless network and the wired infrastructure. Each store connects to the Internet via a business class Digital Subscriber Line (DSL) for his Internet service. The business class DSL came with an upgraded router that provides the capability to create a DMZ, but the company not used this functionality to date. For the Web site, the hosting facility needs ensuring that they are providing a PCI compliant solution." [1, p. 76].

Figure 2 describes the scenario which was also complemented by textual description from the book.



System ID	Functionality
A	System Managing Customer Data
B	Register to Shop's Mailing List
C	Costumers' computers
D	POS terminals for credit card and debit card transaction
E	Managed switch to managed DMZ net traffic

Effects of changes in the infrastructure on each system.

ID	Description of changes to meet compliance requirements
A	This system is now under a separate subnet managed by the routers firewall. This prevents all other machines on the network to access the PoS systems.
B	This system is now under a separate subnet managed by the routers firewall. This prevents all other machines on the network to access the PoS systems.
C	The Wi-Fi service is now separated from the rest of the network.
D	The POS environment is separated from the rest of the network, and the managed switch manages the traffic of each POS terminal separately.
E	The Managed Ethernet switch permits separated the traffic for each POS terminal.

Fig. 2: Flat Network – After Compliance with PCI DSS

“The changes into flat network after compliance are described below and the DMZ functionality on the DSL router allows the owner to segment the POS devices onto their own network. The company needs to purchase a small managed Ethernet switch to accommodate the few POS devices per store. The configuration of his DSL router ensures that the firewall settings are done appropriately according to PCI DSS and do not allow access to the POS devices or the POS controller (if applicable) from the other systems on the network. For the Web site, the company must work with his hosting facility to ensure that they are providing a PCI compliant solution.” [2, p. 76].

References

1. CVSS-SIG. Common vulnerability scoring system v3.0: Specification document. Technical report, First.org, 2015.
2. B. R. Williams and A. Chuvakin. *PCI compliance: understand and implement effective PCI data security standard compliance.* Syngress, 2014.