

1. **Identify the main components of the system.**
- Hardware components: CPU, Memory, Storage, Network Interface Card (NIC), Operating System (OS), Applications.
 - Software components: OS, Applications, Drivers, Firmware.
 - Network components: Router, Switch, Modem, Firewall, VPN, DNS, DHCP, IP Addressing.
 - Security components: Antivirus, Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Security Policies, Access Control Lists (ACLs).
 - Management components: Network Management System (NMS), Configuration Management System (CMS), Monitoring Tools, Logging Tools, Backup and Recovery Tools.

2. **Describe the architecture of the system.**

The architecture of the system is designed to be modular and scalable. It consists of several layers: the hardware layer at the base, followed by the operating system layer, then the application layer, and finally the network layer. The network layer is further divided into sub-layers for network management, security, and data transport. The architecture is designed to support a wide range of devices and applications, and to be able to adapt to changing requirements.

3. **Explain the data flow and storage within the system.**

The data flow and storage within the system are as follows:

1. **Data Flow:** Data is typically generated by applications and stored in a database. The database is connected to the network, and data is transferred between the database and the network. The network then distributes the data to the appropriate devices and applications.

2. **Storage:** Data is stored in a database, which is typically located on a server. The database is connected to the network, and data is transferred between the database and the network. The network then distributes the data to the appropriate devices and applications.

3. **Security:** Data is protected by a variety of security measures, including encryption, access control, and intrusion detection. The security measures are designed to prevent unauthorized access to the data and to detect and prevent any attempts to compromise the data.

4. **Discuss the security measures implemented in the system.**

The security measures implemented in the system are as follows:

1. **Encryption:** Data is encrypted using a strong encryption algorithm, such as AES, to protect it from unauthorized access. The encryption key is stored securely and is only used when the data is being transmitted or stored.

2. **Access Control:** Access to the data is controlled using a variety of access control mechanisms, including user authentication, role-based access control (RBAC), and attribute-based access control (ABAC). The access control mechanisms are designed to ensure that only authorized users and applications can access the data.

3. **Intrusion Detection and Prevention:** The system is equipped with intrusion detection and prevention (IDP) tools that monitor the network for any signs of unauthorized activity. If any suspicious activity is detected, the IDP tools will alert the system administrators and will take steps to prevent the activity from continuing.

4. **Security Policies:** The system is governed by a set of security policies that define the rules for how data should be handled. The security policies are designed to ensure that the data is protected from unauthorized access and that the system is able to detect and prevent any attempts to compromise the data.

5. **Network Management:** The network is managed using a variety of network management tools, including network management systems (NMS), configuration management systems (CMS), and monitoring tools. The network management tools are designed to ensure that the network is operating correctly and to detect and prevent any problems that may arise.

6. **Configuration Management:** The system is configured using a variety of configuration management tools, including configuration management systems (CMS) and configuration management databases (CMDB). The configuration management tools are designed to ensure that the system is configured correctly and to detect and prevent any changes that may be made without proper authorization.

7. **Monitoring:** The system is monitored using a variety of monitoring tools, including monitoring tools and logging tools. The monitoring tools are designed to ensure that the system is operating correctly and to detect and prevent any problems that may arise.

8. **Logging:** The system is logged using a variety of logging tools, including logging tools and security information and event management (SIEM) tools. The logging tools are designed to ensure that the system is operating correctly and to detect and prevent any problems that may arise.

© 2000 Blackwell Science Ltd
Journal of Internal Medicine 247: 105–112

1000

[illegible]

1000

Year	1990	1995	2000
Population (Million)	1.2	1.5	1.8
Urban population (Million)	0.4	0.6	0.8
Urban population (%)	33	40	44

1000

	2014	2013
Operating income	\$1,000,000	\$1,000,000
Depreciation and amortization	200,000	200,000
Change in accounts receivable	(50,000)	(50,000)
Change in accounts payable	100,000	100,000
Change in inventory	(100,000)	(100,000)
Change in other assets and liabilities	0	0
Net cash provided by operating activities	\$1,150,000	\$1,150,000

[illegible]

	2014	2013
Revenues		
Operating revenues	\$ 1,074,715	\$ 1,074,715
Other revenues	\$ 1,074,715	\$ 1,074,715
Expenses		
Operating expenses	\$ 1,074,715	\$ 1,074,715
Other expenses	\$ 1,074,715	\$ 1,074,715
Net income	\$ 0	\$ 0

Background

Healthcare providers (HCPs) are responsible for the safe and effective use of medicines.

• **Medication safety** is a key component of patient safety.

• **Medication safety** is the prevention of harm to patients from the use of medicines.