( 2 )

# code : 303404

BCA 4th Semester Exam., 2019

## INTRODUCTION TO STATISTICS

Time : 3 hours Full Marks : 60

Instructions :

1. The marks are indicated in the right-hand margin.
2. There are questions in this paper.

(üi) Attempt FIE questions in

(iv) Question Nos. 1 and 2 are compulsory.

1. Choose the correct answer (any six) :

1. The expected value or of a random variable is the center of its distribution.
   1. mode
   2. median

(iü) mean

(iv) Bayesian inference

1. Which of the following of a random variable is a measure of spread?
   1. Variance (ii) Standard deviation
   2. Empirical mean
   3. None of the above

( Turn Over )

AK9/800

1. A box contains 10 balls, of which 3 red, 2 are yellow and 5 are blue. balls are randomly selected replacement. Calculate the probabilfry that fewer than 2 of the bal!

are red.

* 1. 0•3601
  2. 06000
  3. 0-5282
  4. None of the above

 If two events (both with probability greater than O) are mutually exclusne, then

(i) they also must be complements (ii) they also could be complements

* 1. they cannot be complements
  2. None of the above

(e) A numerical value used as a summar measure for a sample, such as sample mean, is known as

* 1. population parameter
  2. sample parameter
  3. population mean
  4. None of the above

AK9/800 ( co—u

# ( 3 )

(f) A medical treatment has a success rate

|  |  |  |
| --- | --- | --- |
| of 0•8. Two patients will be treated with |  | If each observation of the dat |
| this treatment. Assuming the results |  | increased by 5, then what ha |
| are independent for the two patients, |  | its mean? |
| what is the probability that neither one |  | (i) It remains unchanged |
| of them will be successfully cured?  (i) 0-5 |  | (ii) It is increased by 5 |
| (ii) 0-36 |  | (iii) It is decreased by 5 |
| (iii) 02 |  | (iv) None of the above |

|  |  |
| --- | --- |
|  | (iii) 90 |
| (iv) the finite population correction factor is necessary | (iv) None of the above |
| (h) If | 2. Answer any three of the following |

(it)) 0-04

## C) In Statistics, out of 100, marks

(g) Whenever using the t-distribution instudents in final exams are as 90 ? estimation, we must assume that 95, 94, 90, 85, 84, 83, 85, 81, •

1. the sample size is at least 3082, 78, 79, 81, 80, 82, 85, 76, 85, ±
2. the sampling disüibution ismedian of data is approximately normal(i) 85
3. the population is approximately(ii) 95 normal https:/cwww.akubihar.com

two events are independent. then quesuo%

1. they must be mutually exclusive
2. the sum of their probabüities must (a) Let A and B be events in a sample be equal to one S such that
3. their intersection must be zero P(D) and 

(it,) None ofthese alternatives is correct '2

( a»er ) Find B C ).

AK9/800

## ( S )

1. Given set A {2, 3. 4, 5} and set B {I l, 12, 13, 14, 15}, two numbers are randomly selected, one from each set. What is probability that the sum of the two numbers equals 16?
2. Four fair six-sided dice are rolled. Find the probability that the sum of the results being 22.
3. Is the real-valued function

where O < p < 1 is parameter, a probability density function?

1. If HA) = 0-25 and P(B) = O. 8, then show that 0-05
2. Each of the nine words in the sentence "The quick brown fox, jumps over the lazy dog" is written on a separate piece of paper. These nine pieces of paper are kept in a box. One of the pieces is drawn at random from the box. Find the expected length of the word 12 drawn.
3. Let X and Y be two random variables. Then show that the sum of their expectation 12 f,ax + Y) - 

( Over )

AK9/800

S. What is correlation coefficient? Prove that the correlation coefficient between two variates x and y is zero, when they are independent.

1. The probability that a machine produces a defective item is 002. Each item is checked as it is produced. Assuming that these are independent trials, what is the probability that at least 100 items must be checked to find one that is defective?
2. A sample of 900 members has a mean of 34 cm and SD of 2•61 cm. Is the sample from a large population of mean 305 cm and SD 2•61 cm? If the population is normal and its mean is unknown, find the 95% confidence limits of true mean. The value of Z at 5% significant level is IZu I •96.

https: www.akubihar.com Whatsapp @ 9300930012

Send your old paper & get 10/10 q-rü,

Paytm or Google Pay

[](https://www.spiceworks.com/user/about/ramya-mohanakrishnan) [Ramya Mohanakrishnan](https://www.spiceworks.com/user/about/ramya-mohanakrishnan) IT Specialist

Last Updated: May 17, 2023

**A computer network is defined as a system that connects two or more computing devices for transmitting and sharing information.** **This article explains computer network in detail, along with its types, components, and best practices for 2022.**

## Table of Contents

* [What Is a Computer Network?](https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_001)
* [Key Components of a Computer Network](https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_002)
* [Types of Computer Networks](https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_003)
* [Key Objectives of Creating and Deploying a Computer Network](https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_004)
* [Top 10 Best Practices for Computer Network Management in 2022](https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_005)

## **What Is a Computer Network?**

**A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.**

The first working network, called ARPANET, was created in the late 1960s and was funded by the U.S. Department of Defense. Government researchers used to share information at a time when computers were large and difficult to move. We have come a long way today from that basic kind of network. Today’s world revolves around the internet, which is a network of networks that connects billions of devices across the world. Organizations of all sizes use networks to connect their employees’ devices and shared resources such as printers.

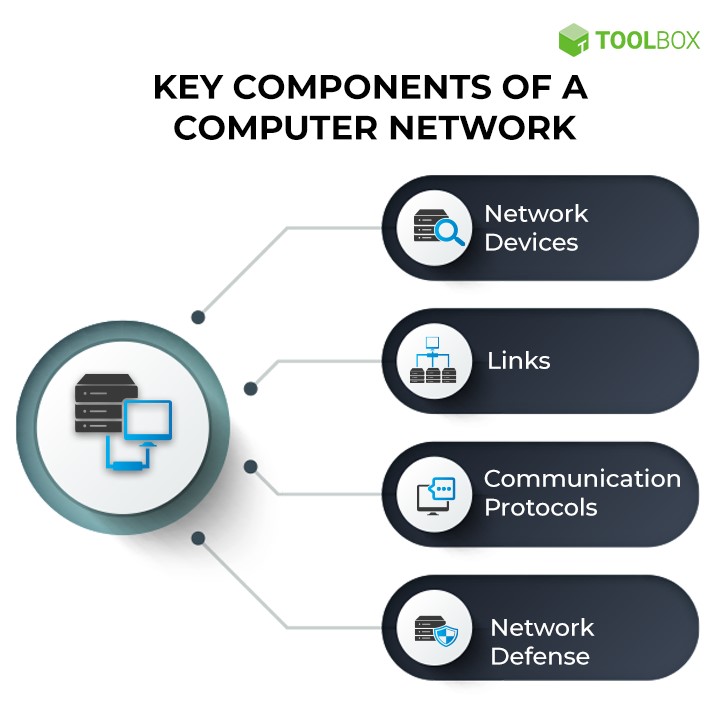
An example of a computer network at large is the traffic monitoring systems in urban cities. These systems alert officials and emergency responders with information about traffic flow and incidents. A simpler example is using [collaboration software](https://www.spiceworks.com/collaboration/content-collaboration/articles/top-collaboration-software-tools-for-teams/) such as Google Drive to share documents with colleagues who work remotely. Every time we connect via a video call, stream movies, share files, chat with instant messages, or just access something on the internet, a computer network is at work.

Computer networking is the branch of computer science that deals with the ideation, architecture, creation, maintenance, and security of computer networks. It is a combination of computer science, computer engineering, and telecommunication.

**See More:**[Building a Disaster Preparedness Strategy? Here’s How Leading Service Providers Can Help](https://www.spiceworks.com/tech/it-strategy/articles/building-disaster-preparedness-strategy-with-leading-service-providers/)

## **Key Components of a Computer Network**

From a broader lens, a computer network is built with two basic blocks: nodes or network devices and links. The links connect two or more nodes with each other. The way these links carry the information is defined by communication protocols. The communication endpoints, i.e., the origin and destination devices, are often called ports.



**Main Components of a Computer Network**

### 1. Network Devices

Network devices or nodes are computing devices that need to be linked in the network. Some network devices include:

* **Computers, mobiles, and other consumer devices**: These are end devices that users directly and frequently access. For example, an email originates from the mailing application on a laptop or mobile phone.
* **Servers**: These are application or storage servers where the main computation and data storage occur. All requests for specific tasks or data come to the servers.
* **Routers**: Routing is the process of selecting the network path through which the data packets traverse. Routers are devices that forward these packets between networks to ultimately reach the destination. They add efficiency to large networks.
* **Switches**: Repeaters are to networks what transformers are to electricity grids—they are electronic devices that receive network signals and clean or strengthen them. Hubs are repeaters with multiple ports in them. They pass on the data to whichever ports are available. Bridges are smarter hubs that only pass the data to the destination port. A switch is a multi-port bridge. Multiple data cables can be plugged into switches to enable communication with multiple network devices.
* **Gateways**: [Gateways](https://www.spiceworks.com/it-security/network-security/articles/what-is-secure-web-gateway/) are hardware devices that act as ‘gates’ between two distinct networks. They can be firewalls, routers, or servers.

**Learn More:** [Why a Network Management Card Is Essential to Secure Enterprise Networks from Cyber Threats](https://www.spiceworks.com/it-security/cyber-risk-management/articles/how-network-management-card-secures-networks)

### 2. Links

Links are the transmission media which can be of two types:

* **Wired**: Examples of wired technologies used in networks include coaxial cables, phone lines, twisted-pair cabling, and optical fibers. Optical fibers carry pulses of light to represent data.
* **Wireless**: Network connections can also be established through radio or other electromagnetic signals. This kind of transmission is called ‘wireless’. The most common examples of wireless links include communication satellites, [cellular networks](https://www.spiceworks.com/tech/innovation/articles/how-edge-and-5g-can-unlock-the-true-potential-of-ar-and-vr/), and radio and technology spread spectrums. Wireless LANs use spectrum technology to establish connections within a small area.

### 3. Communication protocols

A communication protocol is a set of rules followed by all nodes involved in the information transfer. Some common protocols include the internet protocol suite (TCP/IP), IEEE 802, Ethernet, wireless LAN, and cellular standards. TCP/IP is a conceptual model that standardizes communication in a modern network. It suggests four functional layers of these communication links:

* **Network access layer**: This layer defines how the data is physically transferred. It includes how hardware sends data bits through physical wires or fibers.
* **Internet layer**: This layer is responsible for packaging the data into understandable packets and allowing it to be sent and received.
* **Transport layer**: This layer enables devices to maintain a conversation by ensuring the connection is valid and stable.
* **Application layer**: This layer defines how high-level applications can access the network to initiate data transfer.

Most of the modern internet structure is based on the TCP/IP model, though there are still strong influences of the similar but seven-layered open systems interconnection (OSI) model.

IEEE802 is a family of IEEE standards that deals with local area networks (LAN) and metropolitan area networks (MAN). Wireless LAN is the most well-known member of the IEEE 802 family and is more widely known as WLAN or Wi-Fis.

### 4. Network Defense

While nodes, links, and protocols form the foundation of a network, a modern network cannot exist without its defenses. Security is critical when unprecedented amounts of data are generated, moved, and processed across networks. A few examples of network defense tools include [firewall](https://www.spiceworks.com/security/web-security/articles/what-is-firewall-definition-key-components-best-practices/), intrusion detection systems (IDS), intrusion prevention systems (IPS), network access control (NAC), content filters, proxy servers, anti-DDoS devices, and load balancers.

**See More:**[What Is Local Area Network (LAN)? Definition, Types, Architecture and Best Practices](https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network/)

## **Types of Computer Networks**

Computer networks can be classified based on several criteria, such as the transmission medium, the network size, the topology, and organizational intent. Based on a geographical scale, the different types of networks are:

1. **Nanoscale networks**: These networks enable communication between minuscule sensors and actuators.
2. **Personal area network (PAN)**: PAN refers to a network used by just one person to connect multiple devices, such as laptops to scanners, etc.
3. **Local area network (LAN)**: The [local area network](https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network/) connects devices within a limited geographical area, such as schools, hospitals, or office buildings.
4. **Storage area network (SAN)**: SAN is a dedicated network that facilitates block-level data storage. This is used in storage devices such as disk arrays and tape libraries.
5. **Campus area network (CAN)**: Campus area networks are a collection of interconnected LANs. They are used by larger entities such as universities and governments.
6. **Metropolitan area network (MAN)**: MAN is a large computer network that spans across a city.
7. **Wide area network (WAN)**: [Wide area networks](https://www.spiceworks.com/tech/networking/articles/what-is-wide-area-network/) cover larger areas such as large cities, states, and even countries.
8. **Enterprise private network (EPN):** An enterprise private network is a single network that a large organization uses to connect its multiple office locations.
9. **Virtual private network (VPN)**: [VPN](https://www.spiceworks.com/collaboration/remote-support/articles/what-is-a-virtual-private-network/) is an overlay private network stretched on top of a public network.
10. **Cloud network**: Technically, a cloud network is a WAN whose infrastructure is delivered via cloud services.

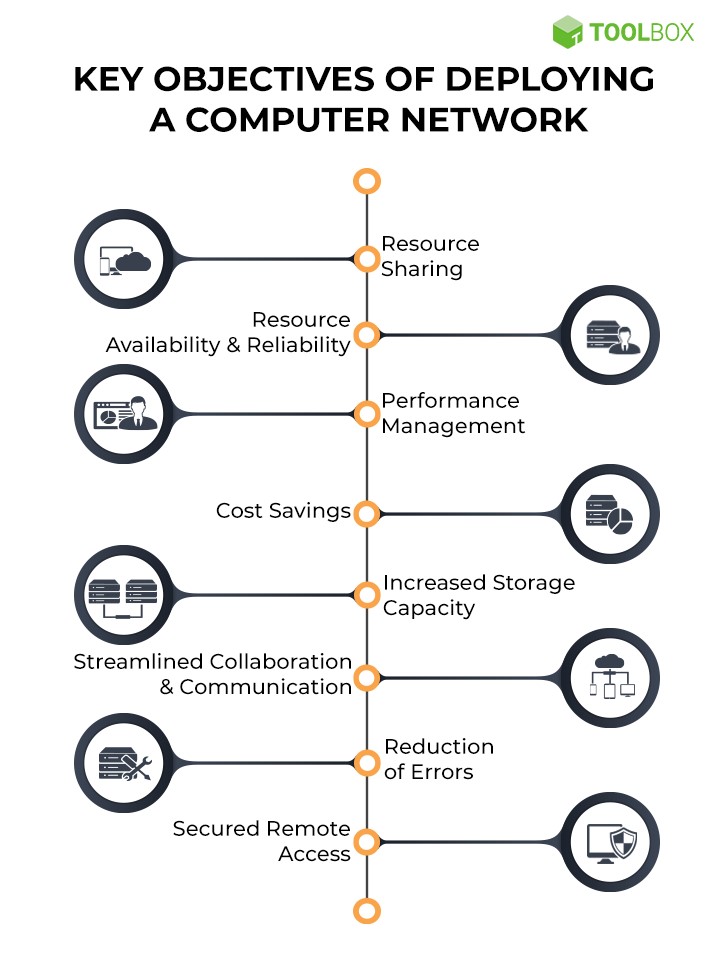
Based on organizational intent, networks can be classified as:

1. **Intranet**: Intranet is a set of networks that is maintained and controlled by a single entity. It is generally the most secure type of network, with access to authorized users alone. An intranet usually exists behind the router in a local area network.
2. **Internet**: The internet (or the internetwork) is a collection of multiple networks connected by routers and layered by networking software. This is a global system that connects governments, researchers, corporates, the public, and individual computer networks.
3. **Extranet**: An extranet is similar to the intranet but with connections to particular external networks. It is generally used to share resources with partners, customers, or remote employees.
4. **Darknet**: The [darknet](https://www.spiceworks.com/tech/security/blogs/dark-web-deep-web-and-how-is-it-used-090319/) is an overlay network that runs on the internet and can only be accessed by specialized software. It uses unique, customized communication protocols.

**See More:**[Wide Area Network (WAN) vs. Local Area Network (LAN): Key Differences and Similarities](https://www.spiceworks.com/tech/networking/articles/wan-vs-lan)

## **Key Objectives of Creating and Deploying a Computer Network**

There is no industry—education, retail, finance, tech, government, or healthcare—that can survive without well-designed computer networks. The bigger an organization, the more complex the network becomes. Before taking on the onerous task of creating and deploying a computer network, here are some key objectives that must be considered.



**Objectives of Deploying a Computer Network**

### 1. Resource sharing

Today’s enterprises are spread across the globe, with critical assets being shared across departments, geographies, and time zones. Clients are no more bound by location. A network allows data and hardware to be accessible to every pertinent user. This also helps with interdepartmental data processing. For example, the marketing team analyzes customer data and product development cycles to enable executive decisions at the top level.

### 2. Resource availability & reliability

A network ensures that resources are not present in inaccessible silos and are available from multiple points. The high reliability comes from the fact that there are usually different supply authorities. Important resources must be [backed up](https://www.spiceworks.com/tech/cloud/articles/network-attached-storage-nas-vs-cloud-backup-which-suits-your-organization-the-best/) across multiple machines to be accessible in case of incidents such as hardware outages.

### 3. Performance management

A company’s workload only increases as it grows. When one or more processors are added to the network, it improves the system’s overall performance and accommodates this growth. Saving data in well-architected databases can drastically improve lookup and fetch times.

### 4.Cost savings

Huge [mainframe](https://www.spiceworks.com/tech/hardware/articles/mainframes-in-hyperscale-era/) computers are an expensive investment, and it makes more sense to add processors at strategic points in the system. This not only improves performance but also saves money. Since it enables employees to access information in seconds, networks save operational time, and subsequently, costs. Centralized network administration also means that fewer investments need to be made for IT support.

### 5. Increased storage capacity

Network-attached storage devices are a boon for employees who work with high volumes of data. For example, every member in the [data science team](https://www.spiceworks.com/tech/big-data/articles/9-skills-you-need-to-become-a-freelance-data-scientist-in-2021/) does not need individual data stores for the huge number of records they crunch. Centralized repositories get the job done in an even more efficient way. With businesses seeing record levels of customer data flowing into their systems, the ability to increase storage capacity is necessary in today’s world.

### 6. Streamlined collaboration & communication

Networks have a major impact on the day-to-day functioning of a company. Employees can share files, view each other’s work, sync their calendars, and exchange ideas more effectively. Every modern enterprise runs on internal messaging systems such as Slack for the uninhibited flow of information and conversations. However, emails are still the formal mode of communication with clients, partners, and vendors.

### 7. Reduction of errors

Networks reduce errors by ensuring that all involved parties acquire information from a single source, even if they are viewing it from different locations. Backed-up data provides consistency and continuity. Standard versions of customer and employee manuals can be made available to a large number of people without much hassle.

### 8. Secured remote access

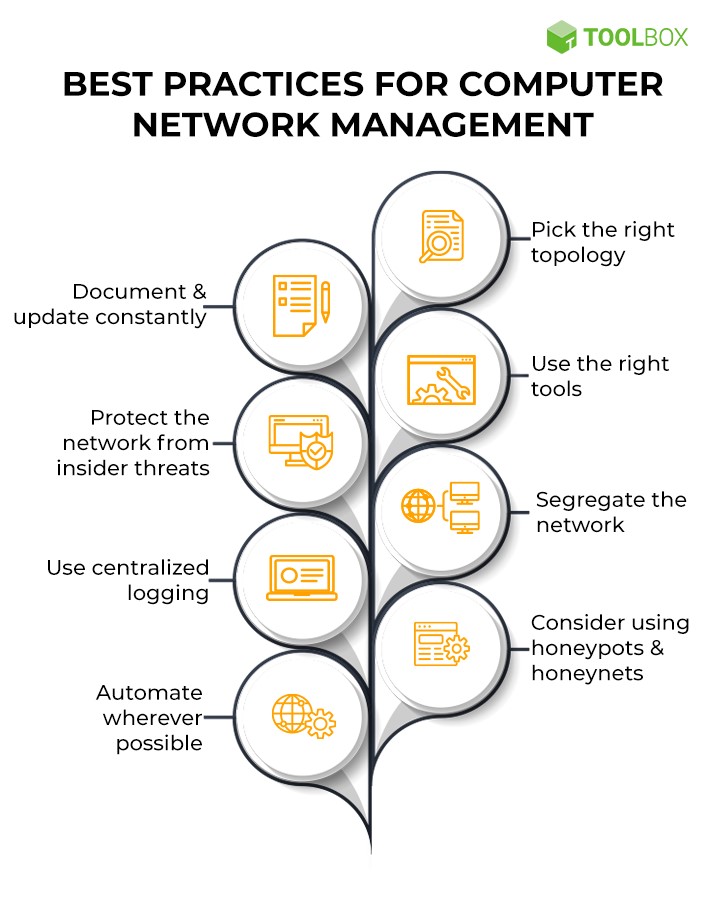
Computer networks promote flexibility, which is important in uncertain times like now when natural disasters and pandemics are ravaging the world. A secure network ensures that users have a safe way of accessing and working on sensitive data, even when they’re away from the company premises. Mobile handheld devices registered to the network even enable [multiple layers of authentication](https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-multi-factor-authentication/) to ensure that no bad actors can access the system.

**See More:**[What Is Wide Area Network (WAN)? Definition, Types, Architecture, and Best Practices](https://www.spiceworks.com/tech/networking/articles/what-is-wide-area-network/)

## **Top 10 Best Practices for Computer Network Management in 2022**

Network management is the process of configuring, monitoring, and troubleshooting everything that pertains to a network, be it hardware, software, or connections. The five functional areas of network management are fault management, configuration management, performance management, security management, and (user) accounting management.

Computer networks can quickly become unruly mammoths if not designed and maintained from the beginning. Here are the top 10 practices for proper computer network management.



**Network Management Best Practices**

### 1. Pick the right topology

Network topology is the pattern or hierarchy in which nodes are connected to each other. The topology can speed up, slow down, or even break the network based on the company’s infrastructure and requirements. Before setting up a network from scratch, network architects must choose the right one. Some common topologies include:

* **Bus network**: Each node is linked to only one other node.
* **Ring network**: Each node is linked to two other nodes, thus forming a ring.
* **Mesh network**: Each node must strive to be connected to every other node in the system.
* **Star network**: A central node server is linked to multiple other nodes. This is faster since data doesn’t have to travel through each node.
* **Tree network**: Here, nodes are arranged in hierarchies.

### 2. Document & update constantly

Documentation of the network is vital since it is the backbone of operations. The documentation must include:

* Technical specifications of equipment, including wires, cables, and connectors
* Hardware
* The software used to enable the hardware and the smooth and secure flow of data
* Firmware
* A formal record of policies and procedures with respect to network operators and users

This must be audited at scheduled intervals or during rehauls. Not only does this make network management easier, but it also allows for smoother compliance audits.

### 3. Use the right tools

The network topology is just the first step toward building a robust network. To manage a highly available and reliant network, the appropriate tools must be placed at the right locations. Must-have tools in a network are:

* **Network monitoring solutions**: A network monitoring solution gives complete visibility into the network. Visual maps help gauge network performance. It can track packets, provide a granular look into network traffic, and help spot anomalies. Newer monitoring systems leverage [artificial intelligence](https://www.spiceworks.com/tech/artificial-intelligence/tech-101/what-is-artificial-intelligence-history-types-applications-benefits-challenges-and-future-of-ai/) to predict scaling requirements and cyber threats using historic and real-time data.
* **Configuration management tools**: A network contains many components that interface with each other. This results in a lot of configuration parameters to keep track of. Configuration management tools resolve this by providing configuration tools that span across the entire network. They also allow network managers to ensure that all compliance requirements have been fulfilled.
* **IP address managers**: Bigger networks need to have an IP address manager (IPAM) to plan, track, and manage information associated with a network’s IP addresses.
* **Security solutions**: [Firewalls](https://www.spiceworks.com/it-security/network-security/top-10-firewall-security-software/), [content filtering systems](https://www.spiceworks.com/it-security/network-security/articles/what-is-content-filtering-definition-types-and-best-practices/), intrusion detection and prevention systems—these are all tools that safeguard networks that are carrying increasingly sensitive loads. No network is complete without them. However, just acquiring these tools is not enough. They must also be properly placed within the network. For example, a [firewall](https://www.spiceworks.com/it-security/network-security/articles/top-10-firewall-hardware-devices/) must be placed at every network junction. Anti-DDoS devices must be placed at the perimeters of the network. Load balancers need to be placed at strategic locations based on the infrastructure, such as before a cluster of database servers. This must be an explicit part of the network architecture.

### 4. Establish baseline network & abnormal behavior

A baseline allows admins to know how the network normally behaves in terms of traffic, user accesses, etc. With an established baseline, alerts can be set up in appropriate places to flag anomalies immediately. The normal range of behavior must be documented at both, user and organizational levels. Data required for the baseline can be acquired from routers, switches, firewalls, wireless APs, sniffers, and dedicated collectors.

### 5. Protect the network from insider threats

Firewalls and intrusion prevention systems ensure that bad actors remain out of the network. However, insider threats need to be addressed as well, particularly with cybercriminals targeting those with access to the network using various [social engineering](https://www.spiceworks.com/security/vulnerability-management/articles/what-is-social-engineering/) ploys. One way of doing this is to operate on a least-privilege model for access management and control. Another is to use stronger authentication mechanisms such as [single sign-on (SSO)](https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-single-sign-on/) and [two-factor authentication (2FA)](https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-two-factor-authentication/). Besides this, employees also need to undergo regular training to deal with security threats. Proper escalation processes must be documented and circulated widely.

### 6. Use multiple vendors for added security

While it makes sense to stick to one hardware vendor, a diverse range of network security tools is a major plus for a large network. Security is a dynamic and ever-involving landscape. Hardware advancements are rapid and cyber threats also evolve with them. It is impossible for one vendor to be up to date on all threats. Additionally, different intrusion detection solutions use different detection algorithms. A good mix of these tools strengthens security; however, you must ensure that they are compatible and allow for common logging and interfacing.

### 7. Segregate the network

Enterprise networks can become large and clunky. Segregation allows them to be divided into logical or functional units, called zones. Segregation is usually done using switches, routers, and virtual LAN solutions. One advantage of a segregated network is that it reduces potential damage from a cyberattack and keeps critical resources out of harm’s way. Another plus is that it allows for more functional classification of networks, such as separating programmer needs from human resources needs.

### 8. Use centralized logging

Centralized logs are key to capturing an overall view of the network. Immediate log analysis can help the security team flag suspicious logins and IT admin teams to spot overwhelmed systems in the network.

### 9. Consider using honeypots & honeynets

Honeypots are separate systems that appear to have legitimate processes and data but are actually a decoy for insider and outsider threats. Any breach of this system does not cause the loss of any real data. A honeynet is a fake network segment for the same cause. While this may come at an additional cost to the network, it allows the security team to keep an eye out for malicious players and make appropriate adjustments.

### 10. Automate wherever possible

New devices are added to systems regularly, and old ones are retired. Users and access controls keep changing frequently. All of these must be automated to ensure that human error does not occur and there are no vulnerable zombie systems in the network, costing money and security. Automation with respect to security is also crucial. It is a good practice to automate responses to attacks, including blocking IP addresses, terminating connections, and gathering additional information about attacks.

**See More:**[What Is Network Security? Definition, Types, and Best Practices](https://www.spiceworks.com/security/network-security/articles/what-is-network-security/)