

## Reliable Networks

### 1.6.1 Network Architecture

Have you ever been busy working online, only to have "the internet go down"? As you know by now, the Internet did not go down, you just lost your connection to it. It is very frustrating. With so many people in the world relying on network access to work and learn, it is imperative that networks are reliable. In this context, reliability means more than your connection to the Internet. This topic focuses on the four aspects of network reliability.

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment. For networks to function efficiently and grow in this type of environment, the network must be built upon a standard network architecture.

Networks also support a wide range of applications and services. They must operate over many different types of cables and devices, which make up the physical infrastructure. The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

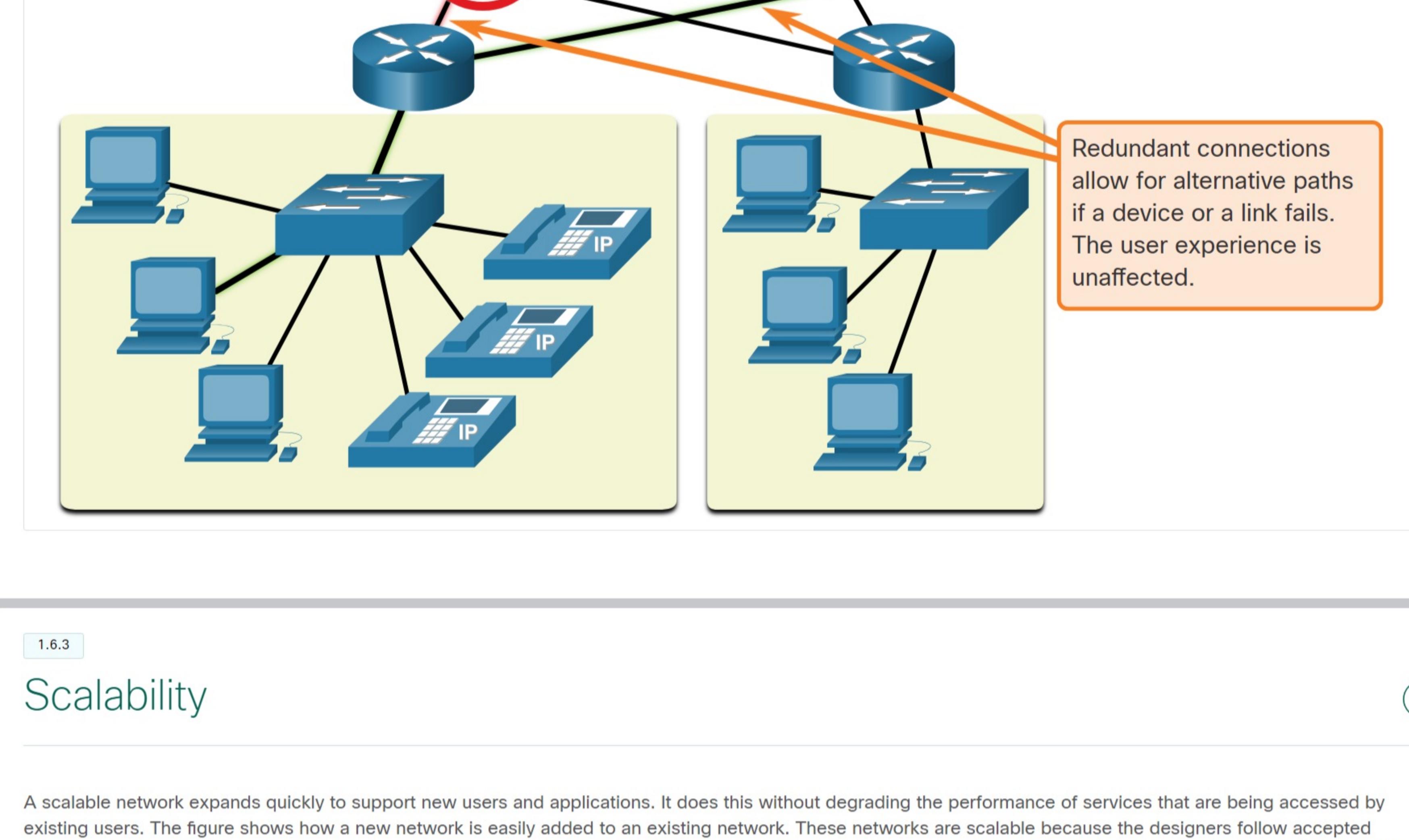
As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

### 1.6.2 Fault Tolerance

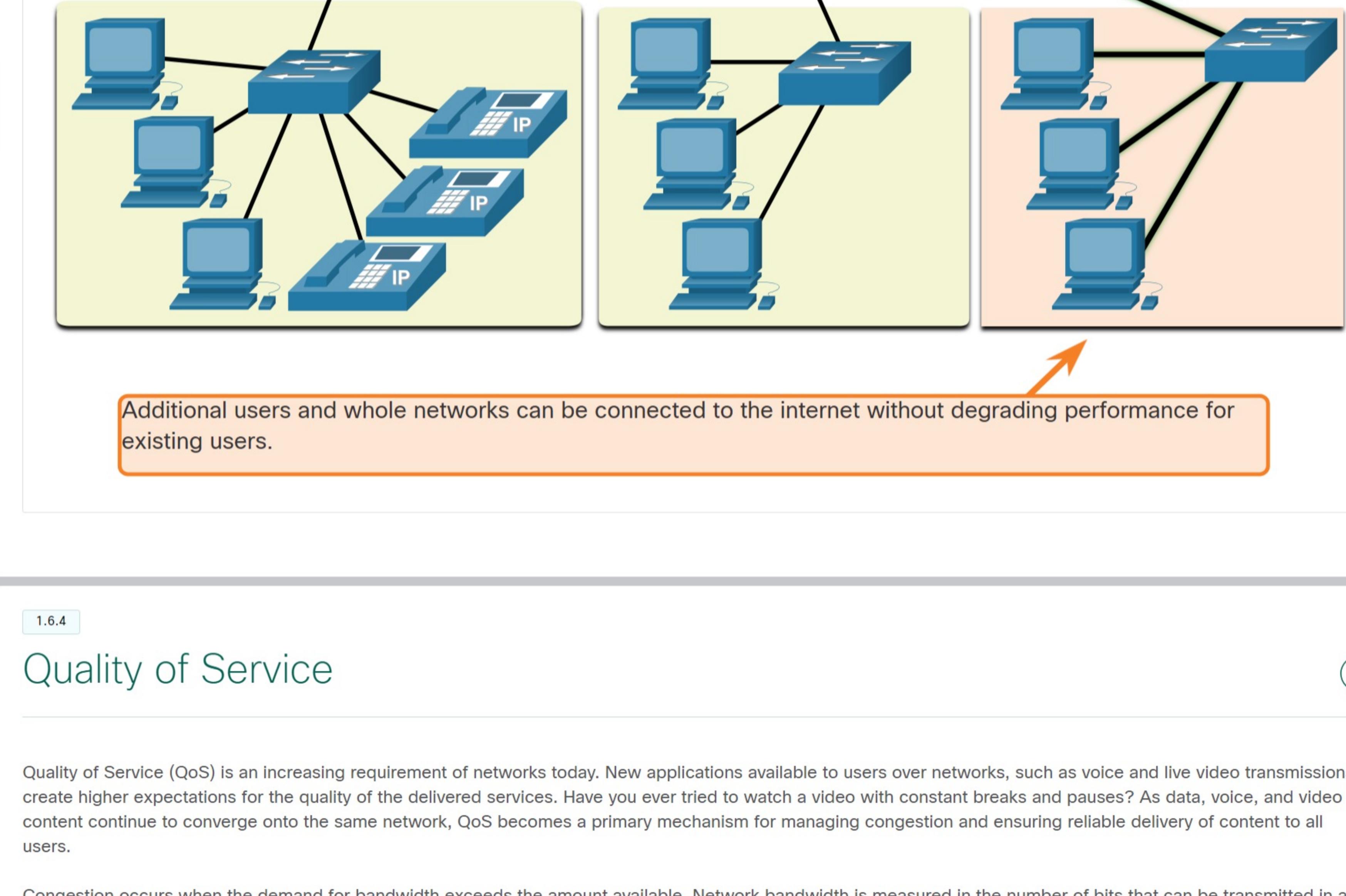
A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over a different link. Having multiple paths to a destination is known as redundancy.

Implementing a packet-switched network is one way that reliable networks provide redundancy. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the same destination. In the figure, the user is unaware and unaffected by the router that is dynamically changing the route when a link fails.



### 1.6.3 Scalability

A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

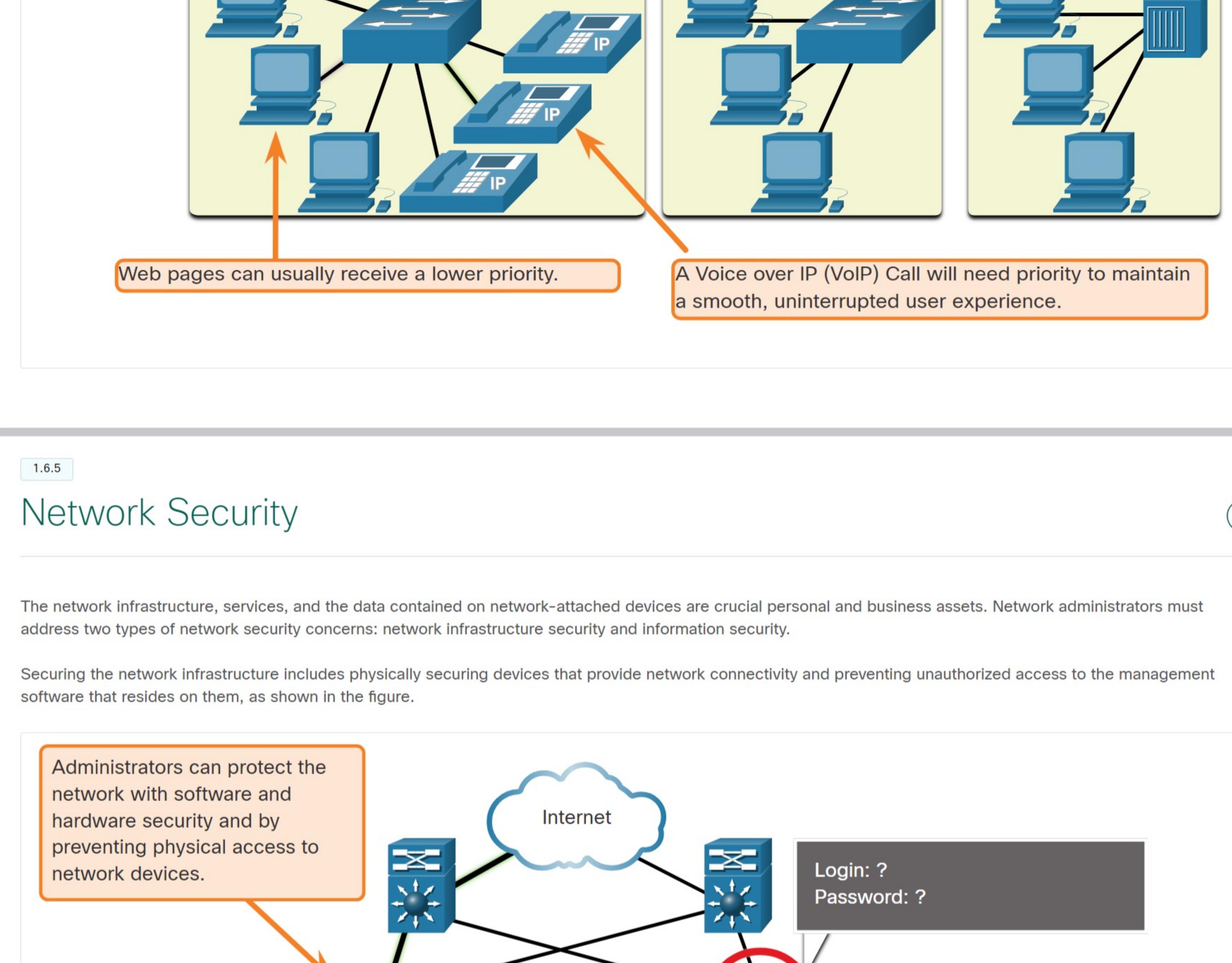


### 1.6.4 Quality of Service

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

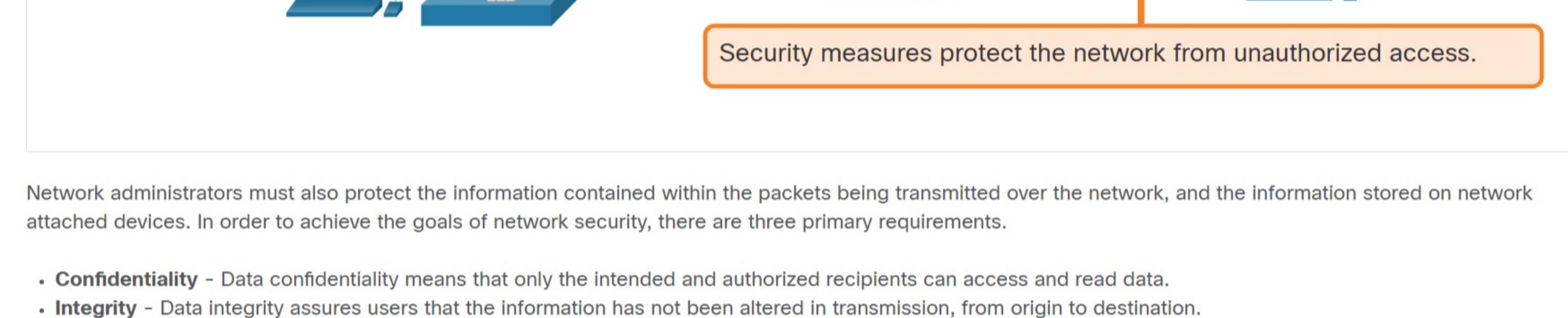
When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. In the figure, one user is requesting a web page, and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.



### 1.6.5 Network Security

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. Network administrators must address two types of network security concerns: network infrastructure security and information security.

Securing the network infrastructure includes physically securing devices that provide network connectivity and preventing unauthorized access to the management software that resides on them, as shown in the figure.



Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network-attached devices. In order to achieve the goals of network security, there are three primary requirements.

- Confidentiality - Data confidentiality means that only the intended and authorized recipients can access and read data.
- Integrity - Data integrity assures users that the information has not been altered in transmission, from origin to destination.
- Availability - Data availability assures users of timely and reliable access to data services for authorized users.

### 1.6.6 Check Your Understanding - Reliable Networks

Check your understanding of reliable networks by choosing the correct answer to the following questions.

1. When designers follow accepted standards and protocols, which of the four basic characteristics of network architecture is achieved?

- fault tolerance
- Scalability
- QoS
- Security

2. Confidentiality, integrity, and availability are requirements of which of the four basic characteristics of network architecture?

- fault tolerance
- Scalability
- QoS
- Security

3. With which type of policy, a router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion?

- fault tolerance
- Scalability
- QoS
- Security

4. Having multiple paths to a destination is known as redundancy. This is an example of which characteristic of network architecture?

- fault tolerance
- Scalability
- QoS
- Security

[Check](#)

[Show Me](#)

[Reset](#)