

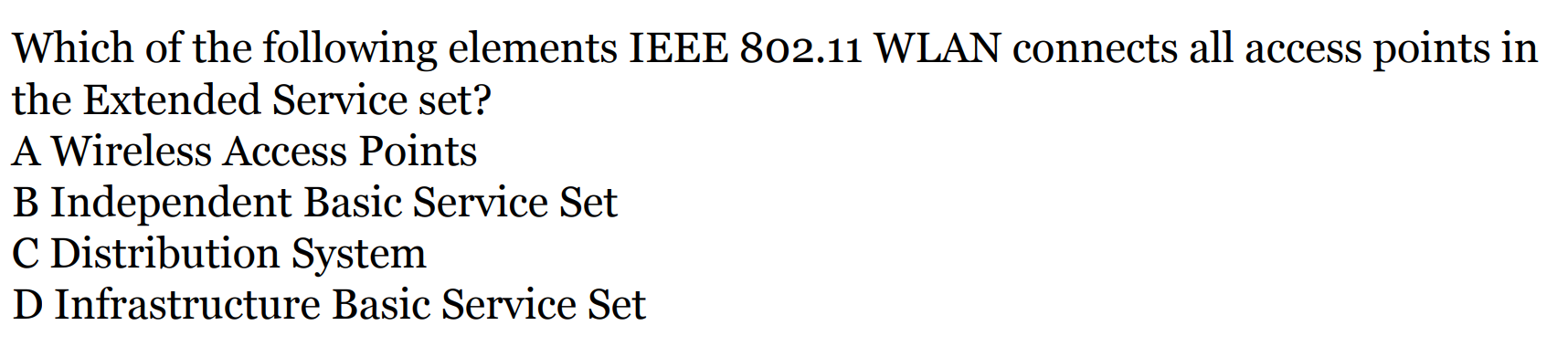
The correct hierarchical order of types of behavior for encryption viruses, from earliest to latest, is:

B. Oligo morphism, polymorphic, metamorphism

Let's break this down:

1. Oligomorphic viruses:
   * These were an early form of virus encryption.
   * They have a small set of decryption routines (typically 2-10) that they switch between.
   * This was an improvement over simple encrypted viruses but still relatively easy to detect.
2. Polymorphic viruses:
   * These came next as a more advanced form of encryption.
   * They can create an unlimited number of different encryption/decryption routines.
   * Each time the virus infects a new file, it encrypts itself differently.
   * This makes them much harder to detect than oligomorphic viruses.
3. Metamorphic viruses:
   * These are the most advanced and latest form of virus mutation.
   * They can rewrite their entire code each time they propagate, changing not just their encryption but their base code as well.
   * This makes them extremely difficult to detect as their core structure changes with each iteration.

The progression from oligomorphic to polymorphic to metamorphic represents an increase in complexity and sophistication in virus design, making each subsequent type more difficult to detect and combat than the last.



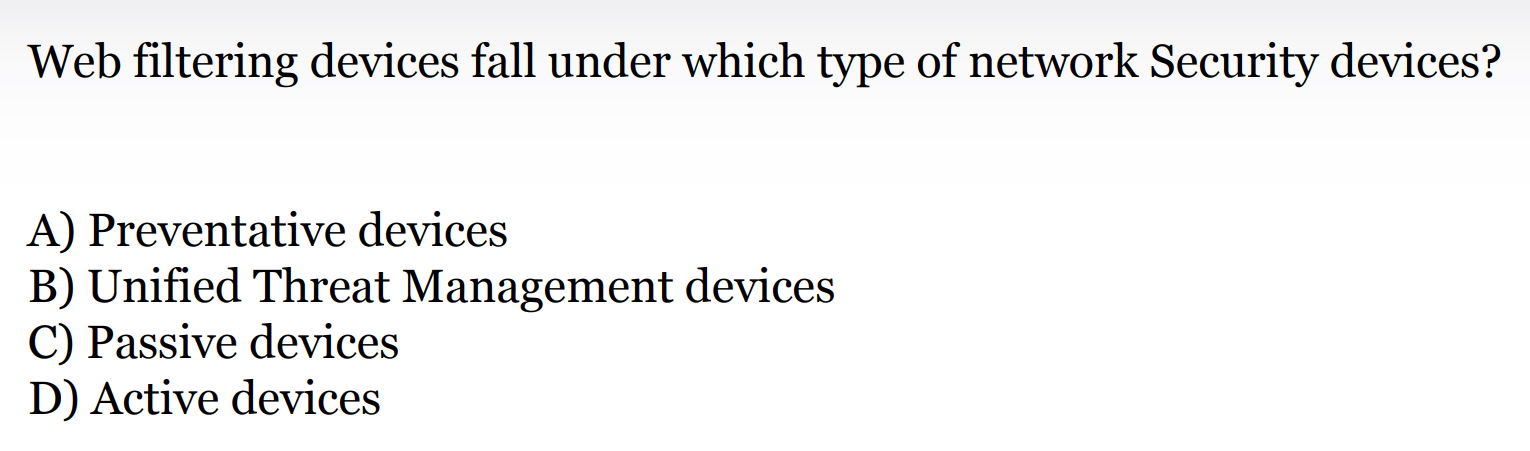
C. Distribution System

Let's break down the key elements of an IEEE 802.11 WLAN (Wireless Local Area Network) to understand why:

1. Basic Service Set (BSS): This is the basic building block of an 802.11 WLAN. It consists of a group of stations that communicate with each other.
2. Access Point (AP): This is a station that provides access to the distribution services via the wireless medium for associated stations.
3. Basic Service Area (BSA): The area covered by a Basic Service Set is called the Basic Service Area.
4. Independent Basic Service Set (IBSS): This is a type of BSS where stations communicate directly with each other without the use of an access point. It's also known as an ad-hoc network.
5. Infrastructure Basic Service Set: This is a BSS that includes an access point. Stations communicate through the AP rather than directly with each other.
6. Extended Service Set (ESS): This is a set of one or more interconnected Basic Service Sets and integrated Local Area Networks that appear as a single BSS to the Logical Link Control layer at any station associated with one of those BSSs.
7. Distribution System (DS): This is the system used to interconnect a set of Basic Service Sets and integrated Local Area Networks to create an Extended Service Set.

The Distribution System is the key element that connects all access points in an Extended Service Set. It allows multiple access points to work together to create a larger wireless network, enabling features like roaming between different BSS areas.

Therefore, the Distribution System (option C) is the correct answer, as it's the element that connects all access points in an Extended Service Set in an IEEE 802.11 WLAN.



The correct answer is:

B) Unified Threat Management devices

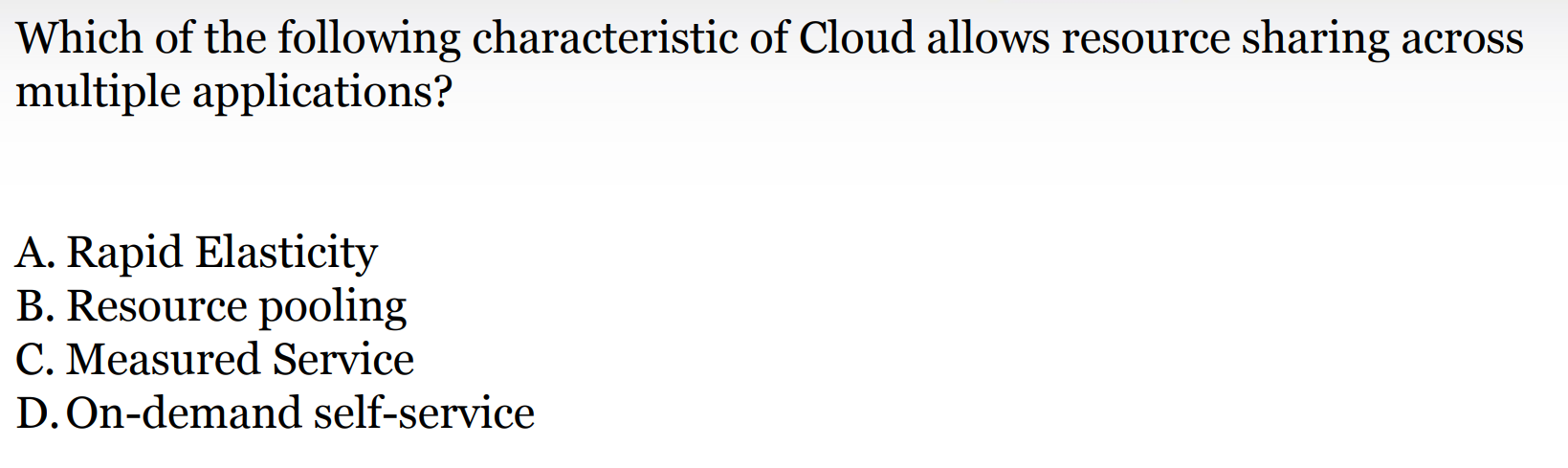
Let's break this down:

1. Preventative devices: These are designed to stop attacks before they occur. While web filtering can prevent access to malicious sites, this category is typically associated with firewalls and intrusion prevention systems.
2. Unified Threat Management (UTM) devices: These are comprehensive security solutions that combine multiple security features into a single device or service. Web filtering is often a key component of UTM solutions, along with firewalls, intrusion detection/prevention, antivirus, and more.
3. Passive devices: These monitor network traffic without actively intervening. Examples include network monitors and intrusion detection systems. Web filters actively block access, so they don't fall under this category.
4. Active devices: While web filters do actively intervene in network traffic, this term is too broad. Not all active devices are web filters, and this category doesn't specifically describe the multi-function nature of modern web filtering solutions.

Web filtering devices are best categorized as Unified Threat Management devices because:

1. Modern web filters often do more than just filter web content. They may include malware scanning, application control, and data loss prevention features.
2. Web filtering is typically one feature among many in UTM solutions, integrated with other security functions for comprehensive protection.
3. UTM devices are designed to provide multiple security functions in a single, manageable platform, which aligns with the evolving role of web filtering in network security.
4. This categorization reflects the trend towards integrated, multi-function security solutions in modern network architectures.

Therefore, while web filters have preventative aspects and are active devices, they are most accurately classified as part of Unified Threat Management solutions in contemporary network security frameworks.



The correct answer is:

B. Resource pooling

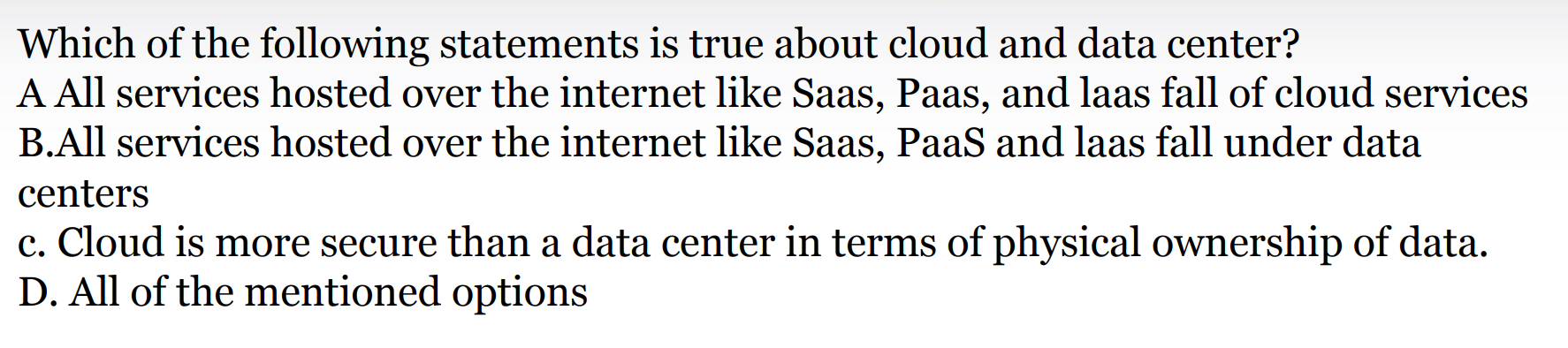
Let's break down each characteristic and explain why resource pooling is the most appropriate answer:

1. Rapid Elasticity: This refers to the ability to quickly scale resources up or down based on demand. While this is an important cloud characteristic, it doesn't specifically address resource sharing across multiple applications.
2. Resource pooling: This is the correct answer because it directly refers to the cloud provider's ability to serve multiple customers (multi-tenant model) from the same physical resources. These resources are dynamically assigned and reassigned according to consumer demand. This allows for efficient sharing of computing resources across multiple applications and customers.
3. Measured Service: This characteristic refers to the ability of cloud systems to automatically control and optimize resource use by leveraging a metering capability. While this helps in resource management, it doesn't specifically enable resource sharing across applications.
4. On-demand self-service: This allows users to provision computing capabilities as needed without requiring human interaction with each service provider. While this provides flexibility, it doesn't directly address resource sharing across applications.

Resource pooling is fundamental to cloud computing because:

1. It allows for efficient utilization of resources by sharing them among multiple users and applications.
2. It enables the cloud provider to achieve economies of scale by serving multiple customers from the same infrastructure.
3. It provides the foundation for other cloud characteristics like rapid elasticity and on-demand self-service.
4. It allows resources to be dynamically assigned and reassigned based on consumer demand, which is crucial for handling multiple applications with varying resource needs.

In summary, while all these characteristics are important aspects of cloud computing, resource pooling is the one that specifically enables resource sharing across multiple applications, making it the correct answer to this question.



The correct answer is:

A. All services hosted over the internet like SaaS, PaaS, and IaaS fall under cloud services

Let's analyze each statement:

A. This statement is correct. SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) are indeed the main service models of cloud computing. These services are delivered over the internet and are characterized by on-demand access, scalability, and pay-as-you-go pricing models.

B. This statement is incorrect. While data centers are the physical infrastructure that can host cloud services, not all services hosted over the internet are necessarily part of a data center. Cloud services can be distributed across multiple data centers and utilize virtualization technologies to abstract the physical infrastructure.

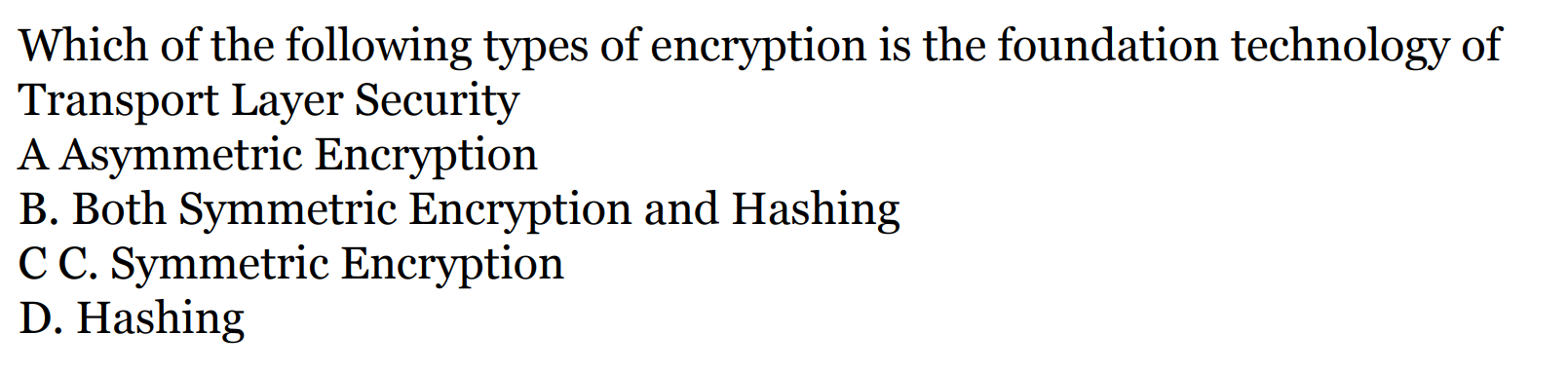
C. This statement is incorrect. The security of cloud vs. data center depends on various factors and can't be generalized. While cloud providers often have robust security measures, physical ownership of data in a private data center can provide certain security advantages in some cases. The security level depends on implementation, policies, and practices rather than the model itself.

D. This option is incorrect because not all of the mentioned options are true.

To elaborate on why A is correct:

1. SaaS (Software as a Service): Applications are hosted and managed by the service provider and accessed by users via the internet. Examples include Gmail, Salesforce, and Microsoft Office 365.
2. PaaS (Platform as a Service): This provides a platform allowing customers to develop, run, and manage applications without the complexity of maintaining the infrastructure. Examples include Google App Engine and Heroku.
3. IaaS (Infrastructure as a Service): This provides virtualized computing resources over the internet. Users have direct access to the underlying infrastructure through virtual machines. Examples include Amazon EC2 and Microsoft Azure Virtual Machines.

These services are fundamental to cloud computing and are delivered over the internet, making statement A the correct choice. They leverage the cloud's characteristics of on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.



The correct answer is:

A. Asymmetric Encryption

Let's break down why asymmetric encryption is the foundation technology of Transport Layer Security (TLS) and explain the roles of the other types of encryption:

1. Asymmetric Encryption (Correct Answer):
   * Also known as public-key cryptography
   * Used in the initial handshake phase of TLS
   * Allows for secure key exchange without prior shared secrets
   * Provides the basis for authenticating the server (and optionally the client)
   * Examples include RSA, Diffie-Hellman, and Elliptic Curve cryptography
2. Symmetric Encryption:
   * Used for bulk data encryption after the handshake
   * Faster than asymmetric encryption for large amounts of data
   * The keys for symmetric encryption are securely exchanged using asymmetric encryption during the handshake
   * Examples include AES, ChaCha20
3. Hashing:
   * Used for integrity checks and in the creation of digital signatures
   * Not used for encryption, but for verifying that data hasn't been tampered with
   * Examples include SHA-256, SHA-3

While TLS uses all of these cryptographic techniques, asymmetric encryption is considered the foundation because:

1. It enables the secure establishment of a shared secret over an insecure channel, which is crucial for the initial handshake.
2. It provides a way to authenticate the server (and optionally the client) through digital certificates, which is essential for preventing man-in-the-middle attacks.
3. Without asymmetric encryption, the other security mechanisms in TLS would be vulnerable to interception and tampering.

The TLS protocol typically works as follows:

1. Use asymmetric encryption for the initial handshake and key exchange
2. Use the exchanged keys to set up symmetric encryption for the bulk of the data transfer
3. Use hashing for integrity checks throughout the process

While symmetric encryption and hashing play crucial roles in TLS, asymmetric encryption provides the foundational security that makes the rest of the protocol possible. Therefore, asymmetric encryption is considered the foundation technology of TLS