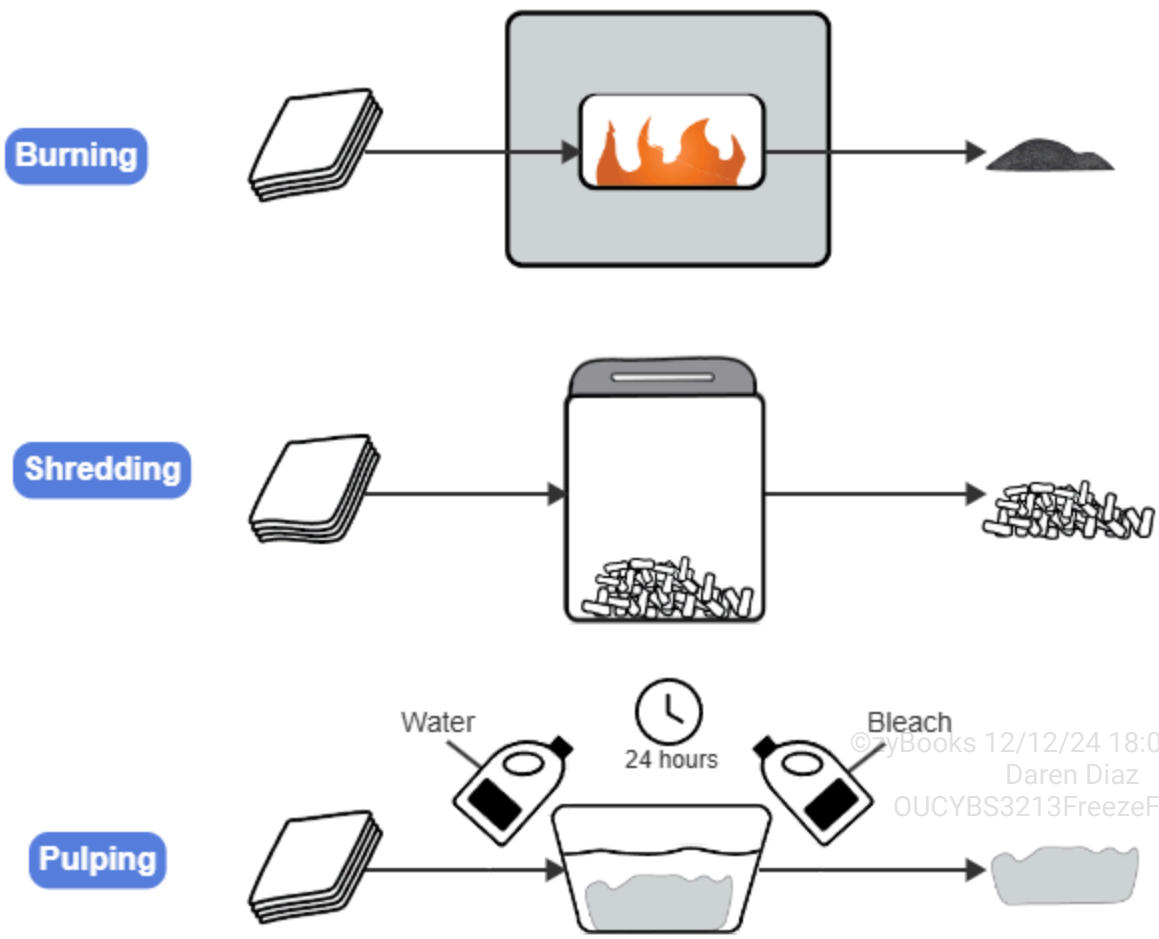
11.1 Secure data destruction

Data destruction: Paper documents

Paper documents with sensitive data must be destroyed to prevent data theft through dumpster diving. Document destruction methods include:

- ***Burning*** turns paper to ash in a high-temperature incinerator.
- ***Shredding*** turns paper into small confetti-like shreds using rotating blades.
- ***Pulping*** turns paper into a soft mush, called pulp, by soaking the paper in water and bleach.

PARTICIPATION ACTIVITY 11.1.1: Burning, shredding, and pulping.



Animation content:

Static image: Document destruction methods. The top section is labeled "Burning" and shows a stack of paper with an arrow pointing to the opening of an incinerator. Fire is shown in the opening. An arrow points from the opening to a pile of ashes. The middle section is labeled "Shredding" and shows a stack of paper with an arrow pointing to a shredder containing shreds of paper. An arrow points from the shredder to a pile of shreds. The bottom section is labeled "Pulping" and shows a stack of paper with an arrow pointing to a bucket containing liquid and a soft, mushy substance. Bottles labeled "Water" and "Bleach" are pouring into the bucket. Above the bucket, a clock is labeled "24 hours". An arrow is pointing from the bucket to a copy of the soft, mushy substance.
Step 1: Paper documents are burned in an incinerator. The fire turns the documents into ashes.
The label "Burning", a stack of paper, and an incinerator appear. The paper moves into the incinerator and disappears. A pile of ashes appears and moves to the right of the incinerator.
Step 2: When paper documents are fed into a shredder, rotating blades tear the paper into small pieces.
The label "Shredding", a stack of paper, and a shredder appear. The paper moves into the opening of the shredder. As the paper feeds through the opening, shreds appear inside of the shredder. When all of the paper is shredded into pieces, a copy of the shred pile moves to the right of the shredder.
Step 3: For pulping, water is used to break down the paper, and bleach is used to remove ink. After soaking for 24 hours, the result is a soft, mushy substance.
The label "Pulping", a stack of paper, and a bucket appear. The paper moves into the bucket. Bottles labeled "Water" and "Bleach" appear and pour into the bucket. A clock labeled "24 hours" appears above the bucket. The paper turns into a soft, mushy substance. A copy of the soft, mushy substance is moved to the right of the bucket.

Animation captions:

1. Paper documents are burned in an incinerator. The fire turns the documents into ashes.
2. When paper documents are fed into a shredder, rotating blades tear the paper into small pieces.
3. For pulping, water is used to break down the paper, and bleach is used to remove ink. After soaking for 24 hours, the result is a soft, mushy substance.

PARTICIPATION ACTIVITY 11.1.2: Document destruction.

Select the document destruction method described.

1) Produces ashes from paper documents.
   - ○ Burning
   - ○ Shredding

- Pulping

2) Uses water and bleach to break down paper documents.
   - Burning
   - Shredding
   - Pulping

3) The most practical method to destroy documents in an office.
   - Burning
   - Shredding
   - Pulping

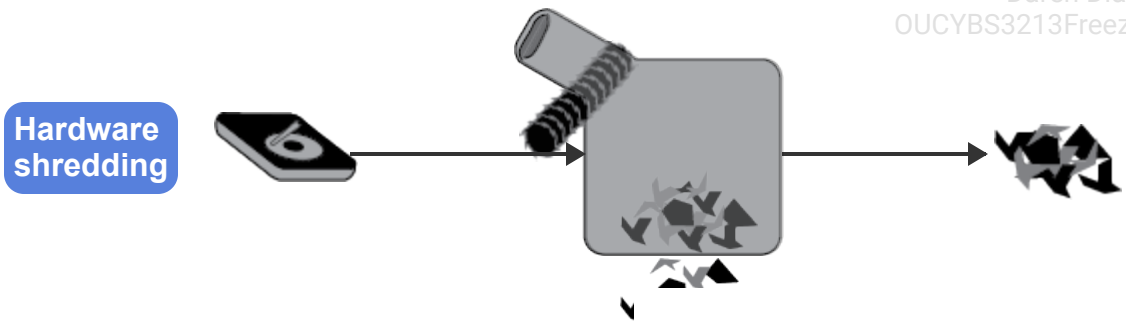
4) The least environmentally friendly method of document destruction.
   - Burning
   - Shredding
   - Pulping

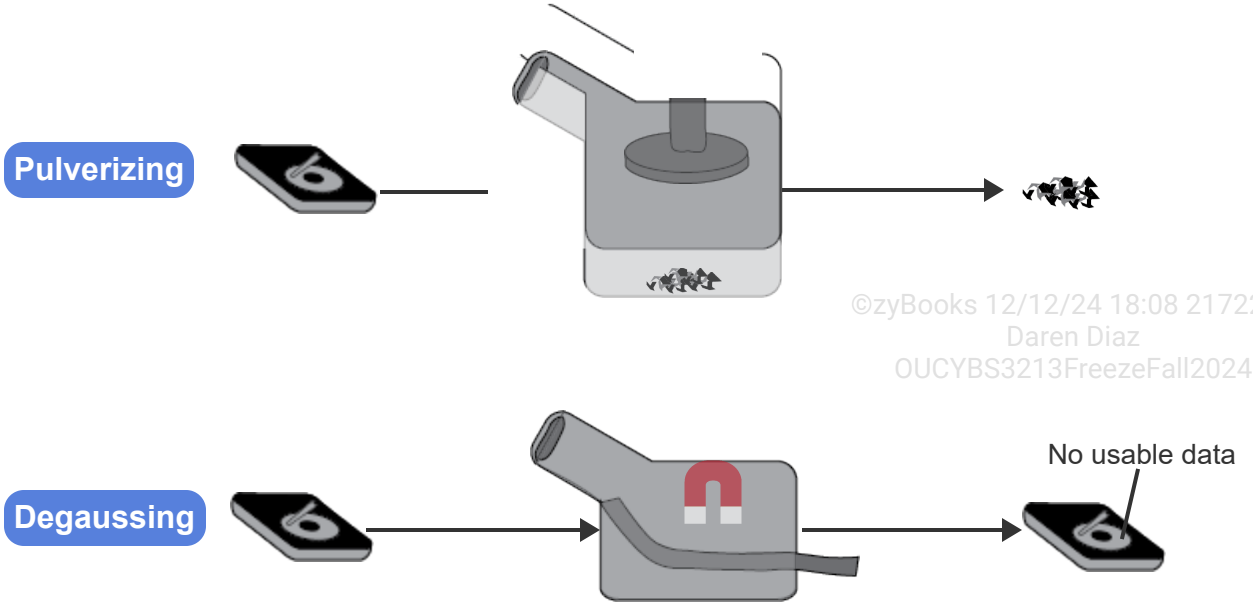
Data destruction: Digital data

When hardware containing data reaches end of life, digital data destruction procedures are used to prevent data theft. Digital data destruction methods include:

- ***Hardware shredding*** turns hardware into small metal pieces using specialized blades.
- ***Pulverizing*** turns hardware into tiny fragments or powder by crushing.
- ***Degaussing*** wipes data from magnetic media using strong magnetic fields.

PARTICIPATION ACTIVITY 11.1.3: Hardware shredding, pulverizing, and degaussing.





Animation content:

Static figure: Examples of hardware shredding, pulverizing, and degaussing of a hard disk drive.

Animation captions:

1. When a hard disk drive is fed into a hardware shredder, rotating blades break the drive into small metal pieces to prevent data recovery.
2. Pulverizing involves crushing the hard drive until the hard drive is broken into tiny fragments or dust.
3. For degaussing, a powerful magnet uses a controlled magnetic field to destroy data on the hard disk drive.

PARTICIPATION ACTIVITY | 11.1.4: Digital data destruction.

Select the digital data destruction method described.

1) Breaks hardware using rotating blades.

- ○ Hardware shredding
- ○ Pulverizing
- ○ Degaussing

2) Destroys data without physically breaking the hardware.

- ○ Hardware shredding

- Pulverizing
- Degaussing

3) The most effective way to destroy data on a solid state drive (SSD).

- Hardware shredding
- Pulverizing
- Degaussing

Third-party data destruction

Properly destroying data requires specialized equipment, so an organization may outsource data destruction to a third-party specialist. A third-party specialist destroys data and provides a certificate of destruction to the organization.

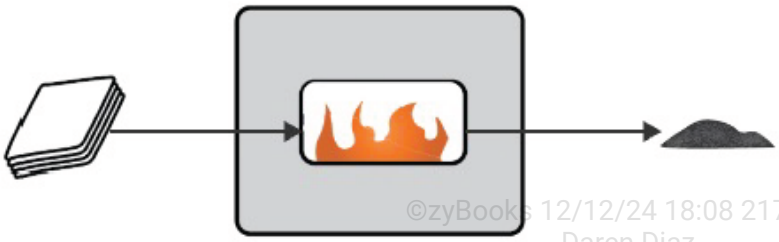
CHALLENGE ACTIVITY | 11.1.1: Secure data destruction.

581480.4344582.qx3zqy7

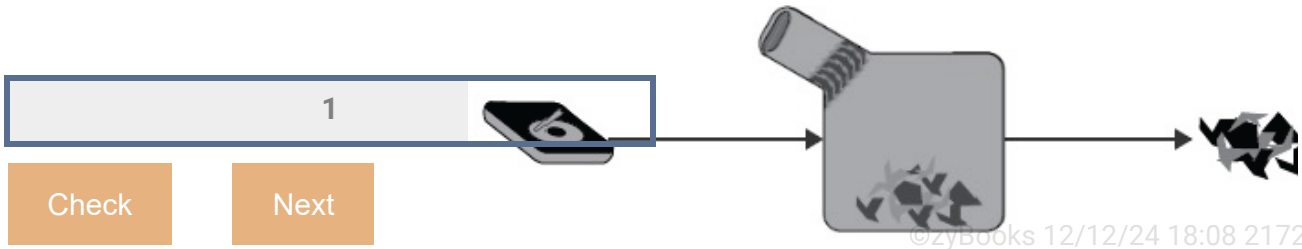
Start

Identify each data destruction method.

Pick



Pick



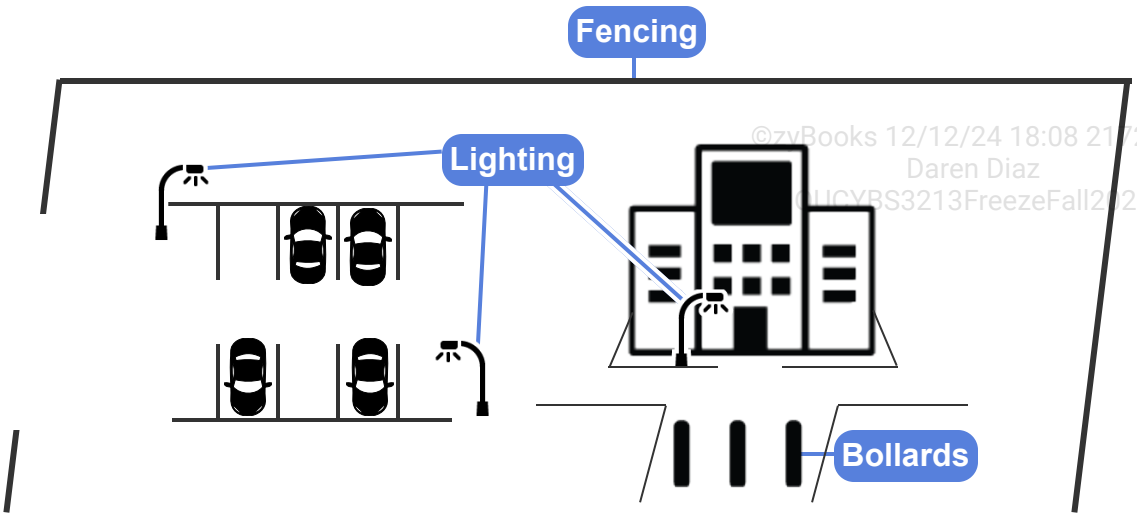
11.2 Physical access controls

Outside security

Outside security measures are used to prevent unauthorized access to a building or restricted area. Outside security measures include:

- A ***fence*** is a wood or wire barrier that encloses an area. Fencing acts as a deterrent because an intruder must climb the fence or enter through a gate.
- ***Lighting*** deters an intruder by eliminating dark areas. Lighting can be helpful in parking areas, along walkways, and near entrances.
- A ***bollard*** is a short post that prevents vehicle access to an area. A group of bollards is strategically placed to ensure openings are too small for a vehicle to drive through.
- ***Industrial camouflage*** is the act of obscuring a building's purpose. Ex: A call center is disguised as a warehouse to prevent angry customers from finding the call center.

PARTICIPATION ACTIVITY 11.2.1: Office building outside security.



Animation content:

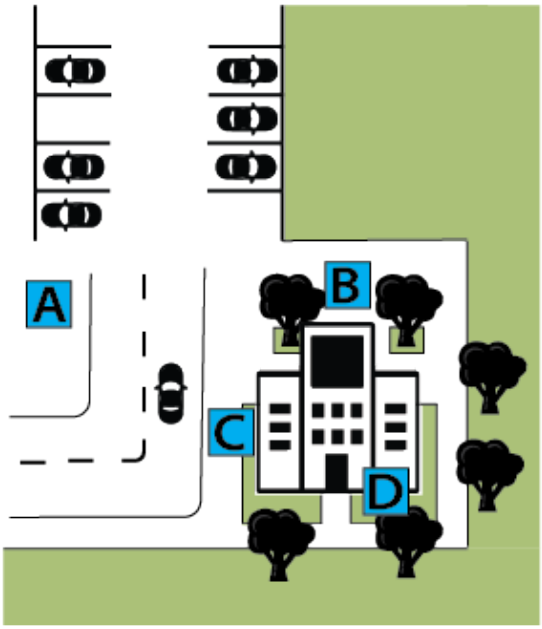
Static figure: A fence surrounding an office building and parking lot. Two street lamps are shown in the parking lot, and a third street lamp is next to the building's entrance. A wide walkway in front of the building's entrance has a line of three bollards evenly spaced across the walkway. A car is in front of the bollards. The car is too big to pass through the row of bollards.

Animation captions:

1. Fencing surrounds the office building to deter intruders. Monitoring a gate or opening is easier than monitoring all of the building's surrounding area.
2. Lighting is placed around the parking lot and at the building's entrance to eliminate dark areas.
3. Bollards are placed in a line across a walkway to prevent vehicle access.

PARTICIPATION ACTIVITY | 11.2.2: Outside security.

1)



Where should bollards be placed to increase building security?

- A
- B

- C
- D

2) An example of industrial camouflage is a data center _____.

- located in a secluded area of the desert
- placed in a nondescript building that looks like a warehouse
- surrounded by a barbed-wire fence

3) Highly secure areas like military bases add _____ to fencing to prevent unauthorized perimeter access.

- barbed wire
- cameras
- warning signs

Cameras

Cameras are used for indoor and outdoor security. A ***security camera*** is a camera designed to increase security by monitoring or recording an area. Ex: After a theft, recordings from a store's security cameras are used to identify the person responsible.

A security camera can include capabilities based on the camera's purpose. ***Object detection*** is a feature that detects the presence or movement of specific objects. Ex: Object detection can be used to detect the presence of a weapon or the movement of expensive equipment.

Motion recognition is a feature that activates the camera when movement is detected. Ex: A Ring doorbell notifies the homeowner and stores recordings when motion is detected.

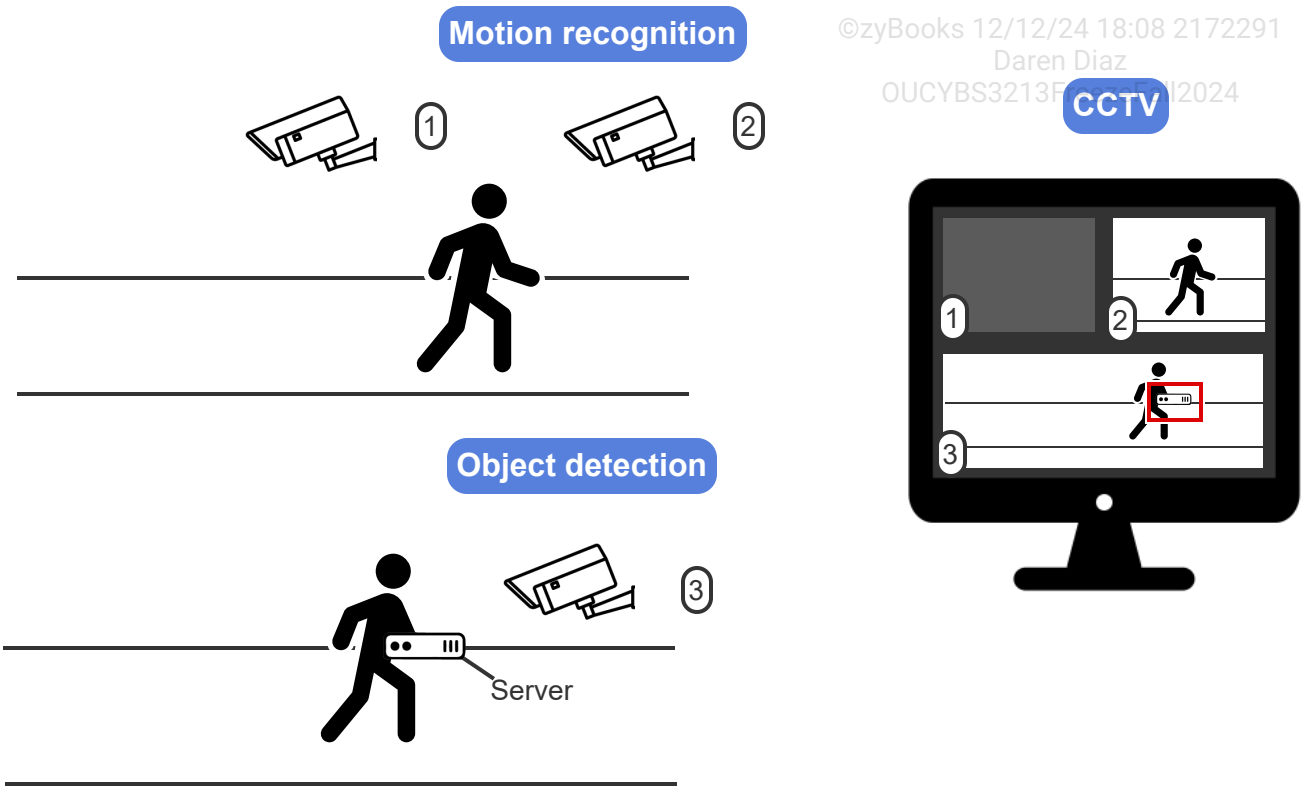
Three motion sensor technologies exist:

- An ***infrared (IR) sensor*** is a sensor that detects IR radiation, which is emitted by warm objects such as people.
- An ***ultrasonic sensor*** is a sensor that emits and receives high-frequency sound waves to detect objects. A change in the sound waves' return time indicates motion.
- A ***microwave sensor*** is a sensor that emits and receives electromagnetic microwave signals to detect objects. Since electromagnetic waves can travel through barriers, a microwave sensor can detect motion through walls.

Closed-circut television (CCTV) is a system that displays the camera's view on a screen. CCTV allows security personnel to monitor security cameras in real time. Ex: A security guard is assigned to watch

CCTV camera feeds showing all of a building's entrances.

PARTICIPATION ACTIVITY 11.2.3: Cameras as physical security.



Animation content:

Static image: A section labeled "Motion recognition" shows a hallway with two cameras, labeled 1 and 2. A person is walking near camera 2. Another section labeled "Object detection" shows a hallway with a camera labeled 3. A person holding a server is walking near camera 3. A monitor labeled "CCTV" is split into three sections labeled 1, 2, and 3. Section 1 is black. Section 2 shows the person walking in the Motion recognition section. Section 3 shows the person with the server in the Object detection section. The server is outlined in red.

Animation captions:

1. The CCTV shows camera 1's feed because camera 1 detects motion. Camera 2's feed is black because no motion is detected by camera 2.
2. The person leaves camera 1's view, so camera 1's CCTV feed goes black. The person enters camera 2's view, so camera 2's CCTV feed turns on.

3. Camera 3 detects specific types of expensive equipment like servers to prevent theft.
4. The camera recognizes the server, so the CCTV shows the server outlined in red.

PARTICIPATION ACTIVITY 11.2.4: Cameras.

1) To be notified when a package is delivered, Carey should install a camera with _____.
   - CCTV
   - motion recognition
   - object detection

2) Tatum wants a security camera that saves recordings but is concerned about storage space for the recordings. Tatum should choose a camera with _____ to conserve storage space.
   - CCTV
   - motion recognition
   - object detection

3) CCTV increases security by _____.
   - alerting security personnel to suspicious activity
   - enabling security personnel to monitor several areas at once
   - saving recordings for future reference

Locks

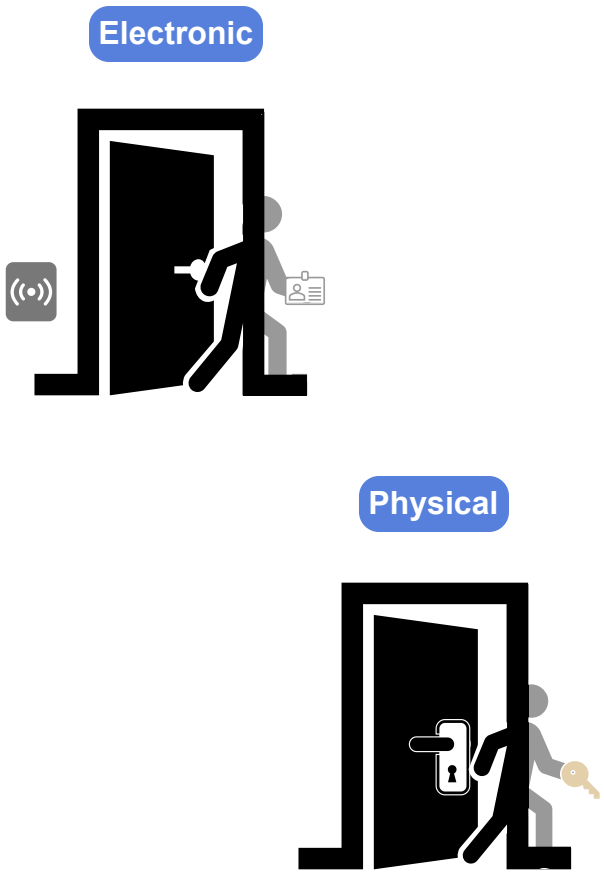
Locks are used to prevent unauthorized access to an area or object. Several lock types exist:

- An ***electronic lock*** is a lock that uses a computer system to authorize and allow entry. Ex: A door unlocks when an employee taps the employee's ID badge on a proximity card reader.
- A ***biometric lock*** is an electronic lock that uses a biometric identifier like a fingerprint to authorize access. Ex: An iPhone can be unlocked using facial recognition.
- A ***physical lock*** is a lock that uses a conventional locking mechanism. Ex: A deadbolt that unlocks with a traditional key.

- A ***cable lock*** is a lock attached to a cable that can be looped through equipment. Ex: A bike lock is a cable lock that loops through a bike's frame and a bike rack to prevent theft.

All installed locks and surrounding material should be resistant to brute force entry attempts. Using solid door materials and reinforced door jambs enhances security by improving the effectiveness of installed locks.

PARTICIPATION ACTIVITY | 11.2.5: Locks as physical security.



Animation content:

Static image: Three open doors with an entering person. The first door is labeled "Electronic." A card reader is next to the door, and the entering person holds an ID badge. The second door is labeled "Biometric." A fingerprint reader is next to the door, and the entering person is not holding anything. The third door is labeled "Physical." The door has a deadbolt, and the entering person is holding a key.

Animation captions:

1. The electronic lock is connected to a proximity card reader. When an employee scans the employee's ID, the door unlocks.
2. The biometric lock is an electronic lock connected to a fingerprint reader. When an employee's fingerprint is scanned, the door unlocks.
3. The physical lock requires a key. When an employee inserts and turns the key, the door

PARTICIPATION ACTIVITY 11.2.6: Locks.

1) An ID badge can be used as authorization for a(n) _____ lock.
   - electronic
   - biometric
   - physical

2) A cable lock is used to _____.
   - control access to an area
   - prevent theft
   - protect important cables

3) Rene needs a lock that is unaffected by power loss. Rene should use a(n) _____ lock.
   - electronic
   - biometric
   - physical

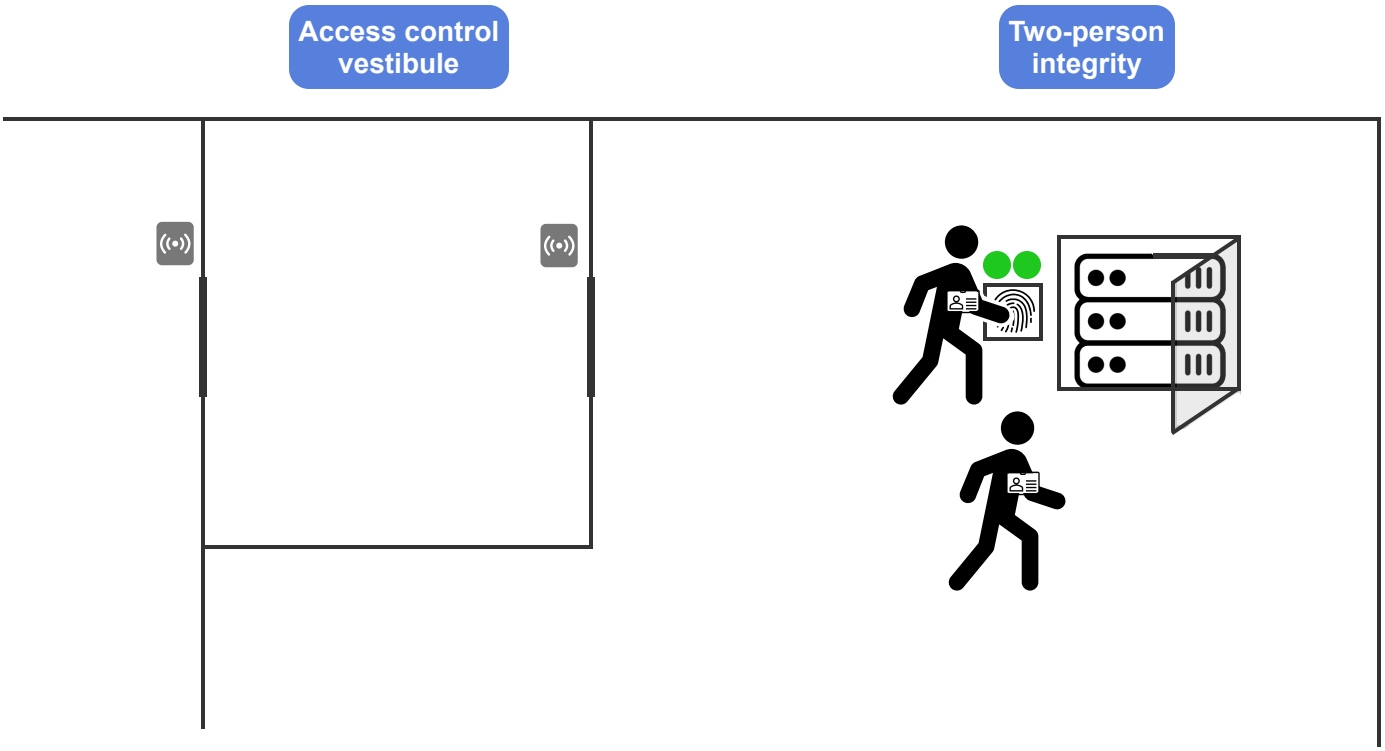
Additional access control

A reception area with visitor registration is used to control access at a building's entrance. ***Reception*** is an area between a building's entrance and the building's secure areas. A receptionist monitors employee access and grants or denies authorization to visitors. A ***visitor log*** is a record of visitors authorized to enter a secure area.

A ***guard*** is a security employee who monitors for suspicious activity. A guard patrols an area or monitors camera feeds through CCTV. A ***robot sentry*** is a robot that patrols an area and uses facial recognition to identify authorized individuals.

Sensitive areas or procedures require additional security measures. ***Two-person integrity*** is a control that requires authorization from two individuals to access a secure area or change an environment. An ***access control vestibule*** is a small room between a secure area and the outside unsecure area. To access the secure area, an individual must close the door to the outside unsecure area before opening the door to the secure area.

PARTICIPATION ACTIVITY | 11.2.7: Secure area access.



Animation content:

Static image: A building layout with three rooms. The middle room is small and labeled "Access control vestibule." The access control vestibule has doors opening into the other two rooms. The room on the right contains an open server cabinet and two employees. A fingerprint scanner is to the left of the server cabinet. Two green circles are above the fingerprint scanner. One of the employees is touching the fingerprint scanner. The label "Two-person integrity" is above the server cabinet.

Step 1: An employee needs to access the server room to fix a server. The employee must enter through an access control vestibule.

A building layout with three rooms. The middle room is small and labeled "Access control vestibule." The access control vestibule has doors opening into the other two rooms. The room on the right

contains a closed server cabinet. A fingerprint scanner is to the left of the server cabinet. Two red circles are above the fingerprint scanner. The label "Two-person integrity" is above the server cabinet. An employee holding a badge appears in the room on the left. The employee scans the badge on a card reader, and a door opens into the access control vestibule. The employee enters the access control vestibule, and the door closes.
Step 2: The first door must close before the second door opens to prevent tailgating.
The employee scans the badge on a scanner next to the door to the server room. The door opens. The employee enters, and the door closes.

Step 3: The server cabinet requires authentication from two employees to gain access. If a second employee does not authenticate within ten seconds, the lock resets.
The employee touches the fingerprint scanner next to the server cabinet. One of the circles above the fingerprint scanner turns green. The green circle then turns back to red.
Step 4: A second authorized employee enters the server room through the access control vestibule.
Step 5: When both employees authenticate, the server cabinet is unlocked.
The first employee touches the fingerprint scanner, and one of the circles turns green. The second employee touches the fingerprint scanner, and the second circle turns green. The server cabinet opens.

Animation captions:

1. An employee needs to access the server room to fix a server. The employee must enter through an access control vestibule.
2. The first door must close before the second door opens to prevent tailgating.
3. The server cabinet requires authentication from two employees to gain access. If a second employee does not authenticate within ten seconds, the lock resets.
4. A second authorized employee enters the server room through the access control vestibule.

PARTICIPATION ACTIVITY 11.2.8: Additional access control.

1) Access control at an office building's entrance should include _____.
   - an access control vestibule
   - reception
   - two-person integrity

2) Unlike a robot sentry, a guard can _____.
   - identify authorized individuals
   - patrol secure areas
   - respond to an incident

3) Many access control vestibules include a _____ for added security.

- security guard
- scale
- reception area

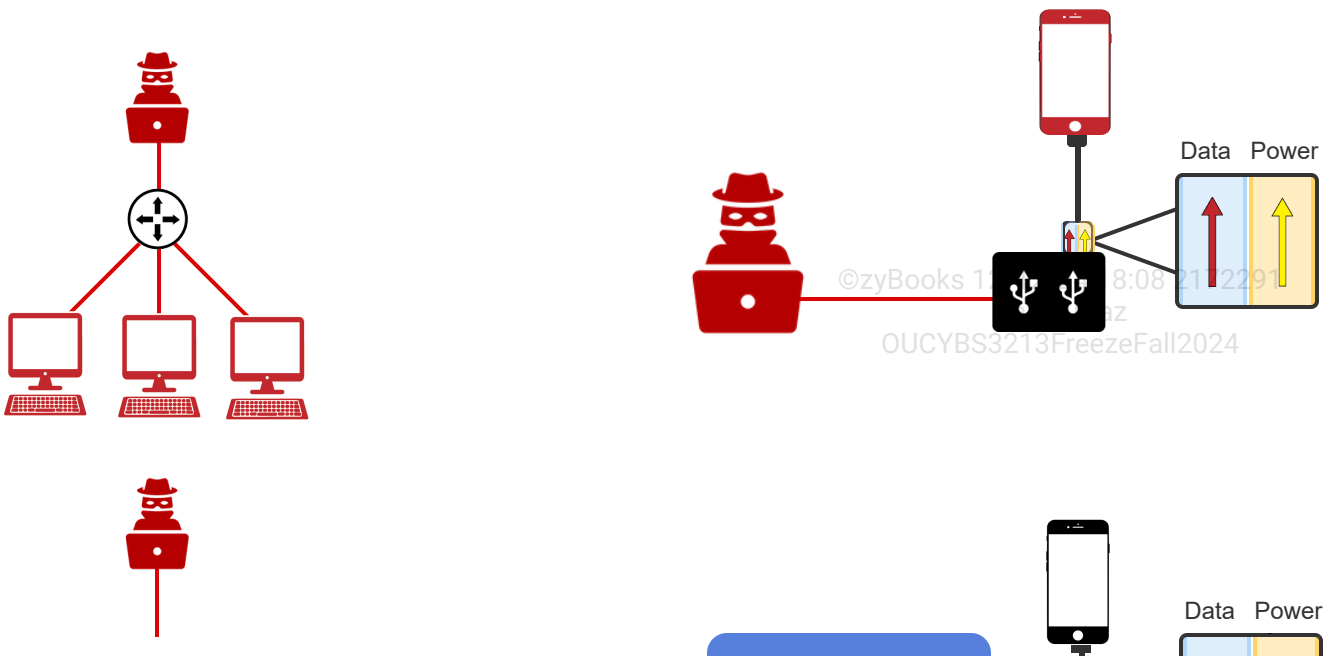
11.3 Equipment protection

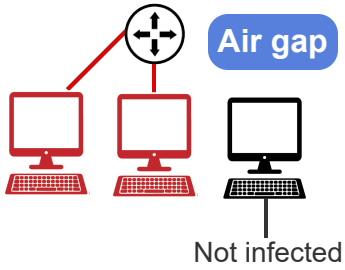
Physical device protection

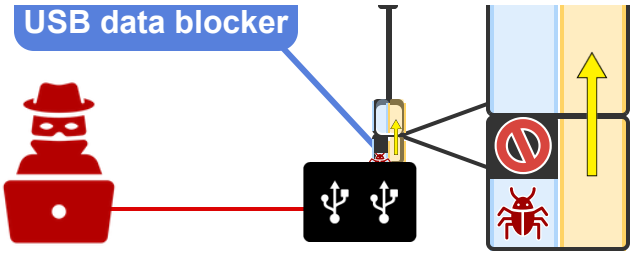
Physical mechanisms are used to protect devices from unauthorized access.

- An ***air gap*** is a deliberate lack of connection between a device and a network. Ex: A backup server is air-gapped to protect against a ransomware attack. If data on a network-connected server is encrypted by ransomware, the data can be restored from the air-gapped backup.
- A ***USB data blocker*** is a device placed between a USB connector and a power source that prevents data from traveling through the USB connector. Ex: When using a public charger at the airport, a user places a USB data blocker at the end of the user's phone charger to protect the phone from malicious data.

PARTICIPATION ACTIVITY 11.3.1: Air gap and USB data blocker.







Animation content:

Static figure: Representations of an air gap and a USB data blocker.
Step 1: An attacker spreads malware to all devices through the network's router.
A router is connected to three desktop computers. An attacker appears and connects to the router. The attacker sends malware to the three desktop computers through the router.
Step 2: An air gap prevents malware from infecting a device through a network connection.
A new router and three new desktop computers appear. Two of the computers are connected to the router. The space between the third computer and the router is labeled "Air gap". A new attacker appears and connects to the router. The attacker sends malware to the two connected computers. The third computer is labeled "Not infected".
Step 3: A smartphone charges using a public USB charging station. The USB connector has a power tunnel and a data tunnel. Power travels through the power tunnel.
A smartphone, a charging cable, and a USB charging station appear. The charging cable connects to the smartphone and USB charging station. The charging cable's USB connector connected to the USB charging station is shown with the left half labeled "Data" and the right half labeled "Power". A lightning bolt travels through the "Power" side and through the cable to the smartphone.
Step 4: An attacker connects to the USB charging station to spread malware to connected devices. The malware travels through the USB connector's data tunnel and infects the smartphone.
An attacker appears and connects to the USB charging station. The attacker sends a bug to the USB charging station. The bug travels through the "Data" side of the USB connector and then through the cable to infect the smartphone.
Step 5: A USB data blocker is placed between the USB charging station and the smartphone. Power travels through the USB data blocker and the USB connector's power tunnel.
A new smartphone, a new charging cable, and a new USB charging station appear. A USB data blocker appears between the USB connector and the USB charging station. The charging cable connects to the smartphone and the USB data blocker. The USB data blocker connects to the USB charging station. The USB connector and USB data blocker are shown with the left half labeled "Data" and the right half labeled "Power". A black box is shown across the "Data" side of the USB data blocker. A lightning bolt travels through the "Power" side of the USB data blocker and USB connector and then through the cable to the smartphone.
Step 6: The attacker attempts to spread malware through the USB charging station, but the USB

data blocker prevents the data from traveling through the USB connector.
An attacker appears and connects to the USB charging station. The attacker sends a bug to the USB charging station. The bug is stopped in the "Data" side of the USB data blocker.

Animation captions:

1. An attacker spreads malware to all devices through the network's router.
2. An air gap prevents malware from infecting a device through a network connection.
3. A smartphone charges using a public USB charging station. The USB connector has a power tunnel and a data tunnel. Power travels through the power tunnel.
4. An attacker connects to the USB charging station to spread malware to connected devices. The malware travels through the USB connector's data tunnel and infects the smartphone.
5. A USB data blocker is placed between the USB charging station and the smartphone. Power travels through the USB data blocker and the USB connector's power tunnel.
6. The attacker attempts to spread malware through the USB charging station, but the USB data blocker prevents the data from traveling through the USB connector.

PARTICIPATION ACTIVITY 11.3.2: Physical device protection.

1) An air gap protects a device from malware by _____.
   - blocking suspicious data
   - monitoring incoming data
   - separating the device from the network

2) To transfer data to an air-gapped device, the data is _____.
   - physically transported using removable media
   - transmitted through a wired network connection
   - transmitted through a wireless network connection

3) A USB data blocker stops data transmission by _____.
   - blocking unknown senders
   - disconnecting the data transfer pins

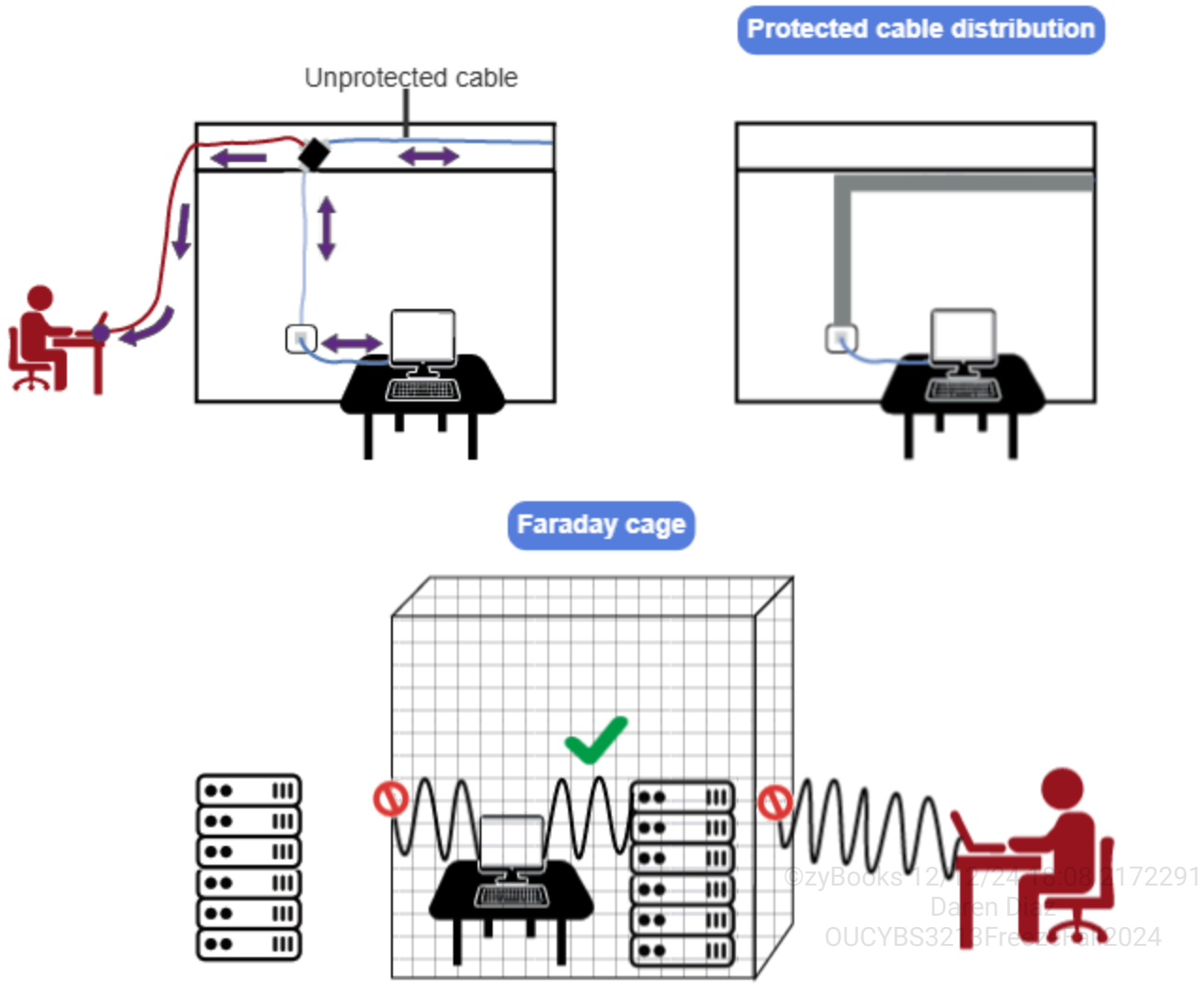
requiring authentication

Physical network protection

Physical mechanisms are used to prevent unauthorized access to a wired or wireless network.

- ***Protected cable distribution*** is a strategy that secures network cables against unauthorized access or harm. Ex: A network cable is mounted inside a metal enclosure to prevent tampering.
- A ***Faraday cage*** is a mesh enclosure that blocks electromagnetic fields like wifi signals. Ex: A Faraday cage is built into a server rack to protect the servers from outside eavesdropping.

PARTICIPATION ACTIVITY 11.3.3: Protected cable distribution and Faraday cage.



Animation content:

Static figure: A desktop computer connected to a cable that runs behind the wall and through the ceiling. The cable is labeled "Unprotected cable". A cable tap is attached to the cable in the ceiling, and an attacker has a laptop with another cable attached to the cable tap. Another desktop computer is connected to a cable that runs through a metal enclosure mounted to the wall. The enclosure is labeled "Protected cable distribution". A mesh cage labeled "Faraday cage" contains a desktop computer and a server. A wireless signal wave between the desktop computer and the server is labeled with a green checkmark. A wireless signal travels from the desktop computer towards a server outside of the Faraday cage. The wireless signal stops at the edge of the Faraday cage. An attacker with a laptop sits outside of the Faraday cage. A wireless signal travels from the attacker's laptop towards the server inside the Faraday cage. The wireless signal stops at the edge of the Faraday cage.

Animation captions:

1. A workstation is connected to the local network through a wired Ethernet connection. Data travels through unprotected cables running through the ceiling and behind the wall.
2. An attacker places an Ethernet tap on the Ethernet cable in the ceiling. The tap allows the attacker to eavesdrop on data sent over the cable.
3. To increase security, cables are placed in wall-mounted metal casing. The casing acts as a deterrent because the cable is harder to access. Mounting the cable on the wall allows for visual checks.
4. A Faraday cage blocks wireless signals. Within the Faraday cage, the desktop computer can wirelessly communicate with the servers.
5. The desktop cannot wirelessly communicate with a server outside the Faraday cage because the Faraday cage blocks the signal.
6. Similarly, an attacker cannot wirelessly communicate with any devices inside the Faraday cage.

PARTICIPATION ACTIVITY 11.3.4: Physical network protection.

1) _____ is used to protect a wired network from tampering and unauthorized access.

   - ○ A Faraday cage
   - ○ Protected cable distribution

2) Amari needs to protect a piece of sensitive equipment from wireless signal interference. Amari should use _____ to protect the equipment.

   - ○ a Faraday cage

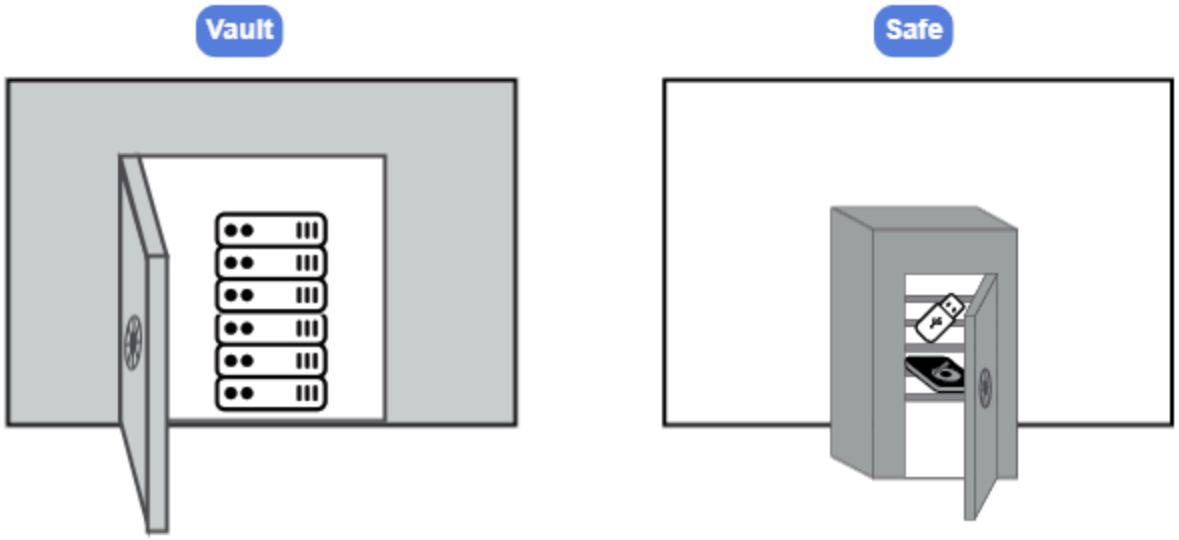
- protected cable distribution

Secure areas

Critical equipment is placed in a secure area that requires authentication for access.

- A ***vault*** is a secure room used to store critical equipment like servers. A vault may store unused equipment or contain operational equipment. Ex: A secure server room is a type of vault.
- A ***safe*** is a separate, movable secure area used to store small critical equipment like backups. Ex: An organization may provide a small safe to each employee to safely store removable media like USB drives.

PARTICIPATION ACTIVITY | 11.3.5: Secure areas.



Animation content:

Static figure: An open vault containing a server rack and an open safe containing a USB drive and a hard disk drive.

Animation captions:

1. A vault is permanently built into the building's construction. The vault contains critical servers.
2. A safe is separate from the building and moveable. The safe contains storage media containing sensitive information.

PARTICIPATION ACTIVITY 11.3.6: Secure areas.

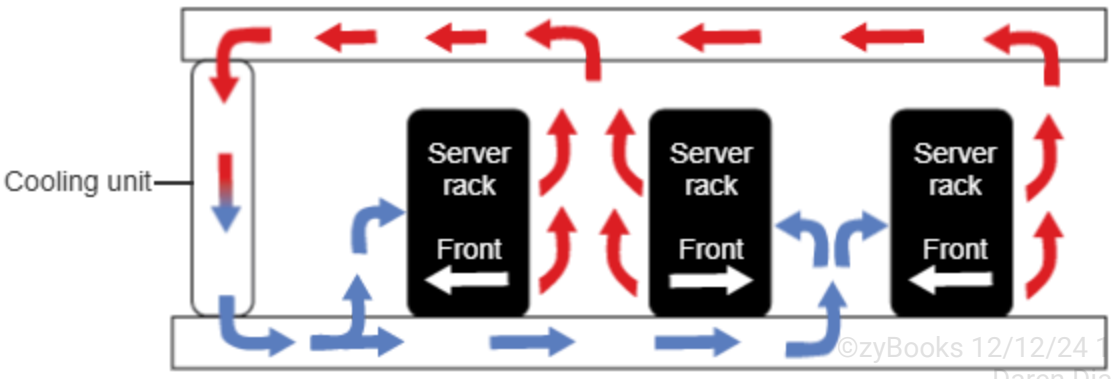
1) A _____ is difficult to add after an office's initial construction is complete.
   - safe
   - vault

2) A vault or safe physically protects equipment by _____.
   - blocking wireless signals
   - requiring authentication

Equipment cooling

Equipment protection includes environmental controls to prevent damage. Servers create heat while operating. When several servers are housed in a server rack, the excessive heat can damage the servers. A ***hot aisle/cold aisle*** system uses alternating hot and cold aisles in a server room to manage the heat and cool the servers.

PARTICIPATION ACTIVITY 11.3.7: Hot and cold aisles.



Animation content:

Static figure: A server room showing hot and cold air flow.
Step 1: The servers in the server racks produce heat. The heat is released from the backs of the server racks in alternating aisles and enters vents in the ceiling to travel to the cooling unit.
Three server racks are shown. The first server rack faces to the left, the second server rack faces to the right, and the third server rack faces to the left. Hot air moves from the back of the server racks, up into the ceiling, and toward a cooling unit.
Step 2: The cooling unit cools the hot air and returns the cool air through a floor vent.
The hot air turns to cool air as the air travels through the cooling unit.
Step 3: The cold air is pushed to the aisles with the fronts of the server racks to cool the servers and maintain optimal operating temperatures.
The cool air travels through the floor to the fronts of the server racks.

Animation captions:

1. The servers in the server racks produce heat. The heat is released from the backs of the server racks in alternating aisles and enters vents in the ceiling to travel to the cooling unit.
2. The cooling unit cools the hot air and returns the cool air through a floor vent.
3. The cold air is pushed to the aisles with the fronts of the server racks to cool the servers and maintain optimal operating temperatures.

PARTICIPATION ACTIVITY 11.3.8: Hot and cold aisles.

1) A hot/cold aisle system is used in a server room to _____.
   - keep half of the servers hot and half of the servers cold
   - maintain optimum temperatures for operational servers
   - make the server room comfortable for employees

2) If Robin is standing in a cold aisle of a server room, Robin has access to the _____ of the server racks.
   - back
   - front

CHALLENGE ACTIVITY 11.3.1: Equipment protection.

Start

Company K implements an air gap for a critical backup.

Select all that apply to the air-gapped backup.

- [ ] Can perform automatic backups
- [ ] Receives data via removable media
- [ ] Is not connected to a wired network
- [ ] Is not connected to a wireless network

1 2 3

Check Next

11.4 High availability and restoration

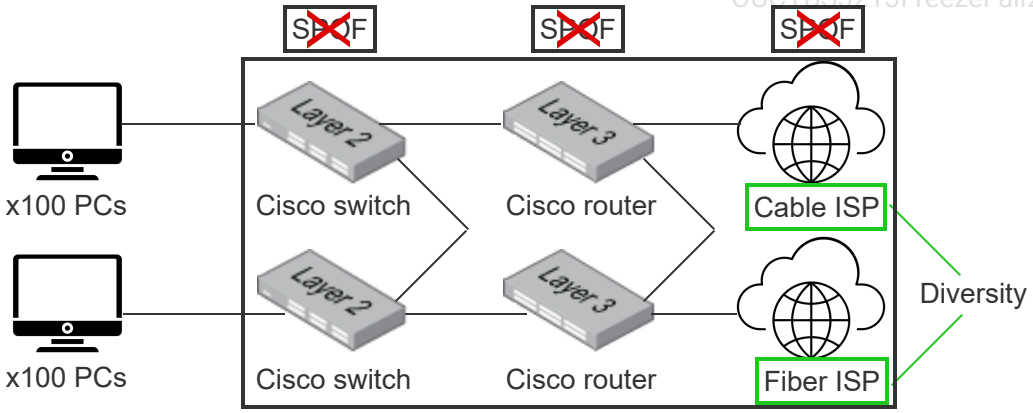
HA concepts

High availability (HA) is a business resource's ability to remain available for use even in the event of failure, disaster, or peak use. HA aims to eliminate a single point of failure. A ***single point of failure (SPOF)*** is a critical business resource without redundancy and diversity. HA relies on four concepts to eliminate a SPOF:

- ***Resilience*** is a computing infrastructure's ability to remain functional during a service degradation or disruption.
- ***Redundancy*** is the duplication of a business resource to eliminate a SPOF.

- ***Diversity*** is the use of different technologies, vendors, cryptographies, and other controls to eliminate a SPOF.
- ***Scalability*** is the measure of a system's ability to handle increased demands.

PARTICIPATION ACTIVITY | 11.4.1: HA concepts.



Redundancy and scalability

Animation content:

Static figure: A LAN consisting of 200 computers, two switches, two routers, and two ISPs is displayed.
Step 1:A SPOF negatively impacts operations. HA aims to eliminate a SPOF through redundancy and diversity. A network segment consisting of 100 computers, one Cisco switch, one Cisco router, and one cable ISP is displayed. SPOF labels appear above the switch, router, and ISP because no backup options exist.
Step 2: HA depends on resource redundancy. Redundancy contributes to SPOF elimination. Ex: Multiple switches, routers, and ISPs provide network resource redundancy. A second Cisco switch, Cisco router, and cable ISP are added. The switch and router are no longer a SPOF. However, the ISP SPOF remains because both ISPs use cable.
Step 3: HA utilizes diversity along with redundancy to eliminate a SPOF. Ex: An organization using a cable ISP and a fiber ISP eliminates a SPOF for internet services. The cable ISPs are highlighted to show a lack of diversity. The second cable ISP is replaced with a fiber ISP to provide both redundancy and diversity. The ISP SPOF is now eliminated.
Step 4: HA also contributes to scalability by increasing the amount of available network resources. Ex: Multiple switches, routers, and ISPs serving more users. Another 100 computers are added to the network. The additional switch, router, and ISP are able to accommodate the additional computers because HA provides redundancy and scalability.

Animation captions:

1. A SPOF negatively impacts operations. HA aims to eliminate a SPOF through redundancy and diversity.
2. HA depends on resource redundancy. Redundancy contributes to SPOF elimination. Ex: Multiple switches, routers, and ISPs provide network resource redundancy.
3. HA utilizes diversity along with redundancy to eliminate a SPOF. Ex: An organization using a cable ISP and a fiber ISP eliminates a SPOF for internet services.
4. HA also contributes to scalability by increasing the amount of available network resources. Ex: Multiple switches, routers, and ISPs serving more users.

PARTICIPATION ACTIVITY 11.4.2: HA.

1) Which network ability ensures a resource's availability during peak use?
   - BC
   - DR
   - HA

2) What is the deployment of a single router for hundreds of users an example of?
   - SPOF
   - Redundancy
   - Diversity

3) What is the deployment of two routers from the same vendor for hundreds of users an example of?
   - SPOF
   - Redundancy
   - Diversity

4) What is the deployment of two routers from different vendors for hundreds of users an example of?
   - SDN
   - Change management
   - Diversity

HA configurations

Two HA configuration categories exist:

- ***Load balancing*** is the act of distributing network traffic among multiple devices to improve performance and prevent overload.
- ***Failover*** is the automatic switching from a failed device to another non-failed device to prevent service disruption.

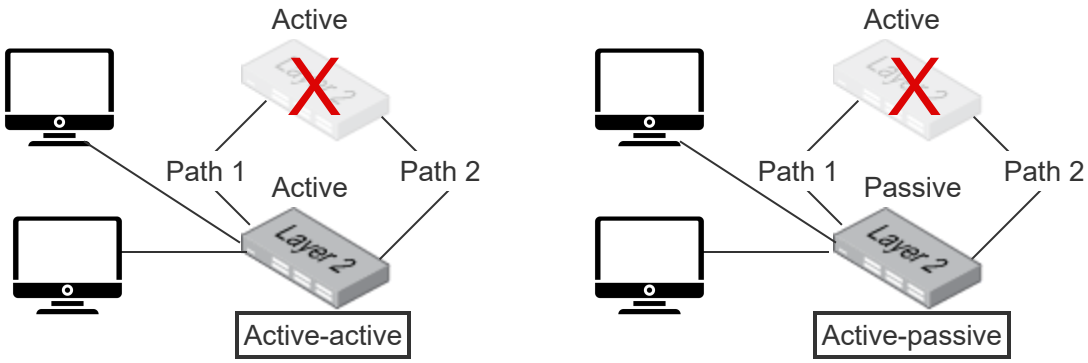
A device used for HA is configured as active or passive:

- An ***active device*** is a device actively providing a service or function.
- A ***passive device*** is a dormant device only providing a service or function when an active device fails.

Two HA device configuration options exist:

- ***Active-active*** is a HA configuration where paired devices are both active devices.
- ***Active-passive*** is a HA configuration with one active device and one passive device.

PARTICIPATION ACTIVITY 11.4.3: HA configurations.



Animation content:

HA configuration categories include load balancing, failover, and multipathing. A HA device is configured as an active device or a passive device.

Animation captions:

1. Networking devices are paired together to provide HA. Ex: Two pairs of switches.
2. An active-active configuration leverages load balancing, failover, and multipathing because each switch transmits network traffic evenly.
3. Each switch can handle a full workload if one switch fails because of the active-active failover configuration and the multipath between switches.

4. An active-passive configuration leverages failover because one HA resource is active while another HA resource is dormant.
5. A passive switch becomes an active switch when the active switch fails because of the active-passive failover configuration

PARTICIPATION ACTIVITY 11.4.4: High availability configurations.

1) Which HA configuration category evenly distributes network's workload among multiple devices?
   - Load balancing
   - Failover
   - Multipathing

2) Which HA configuration category prevents service disruption?
   - Load balancing
   - Failover
   - Multipathing

3) Which HA configuration option leverages all three HA configuration categories?
   - Active-active
   - Active-passive
   - Passive-passive

4) Which HA configuration option includes a dormant device?
   - Active-active
   - Active-passive
   - Passive-active

Scalability HA

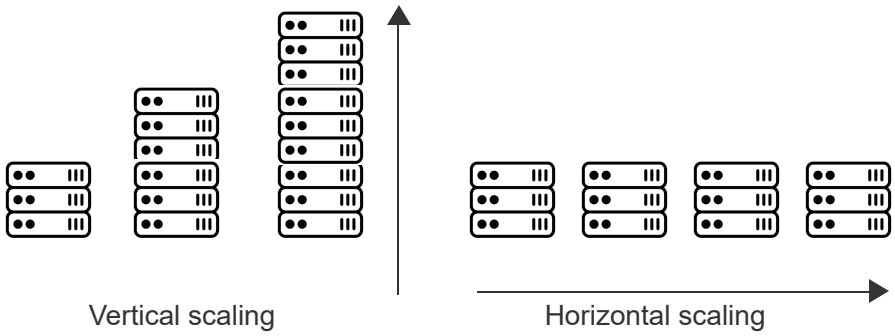
When loads on systems and services become high or when components in an infrastructure fail, organizations need a way to respond. Scalability is a common design element and a useful response control for many systems in modern environments where services are designed to scale across many servers instead of requiring a larger server to handle a larger workload.

Two major categories of scalability:

- Vertical scalability requires a larger system or device. ***Vertical scalability*** is used when all tasks need to be run on the same system. Vertical scalability can be more expensive than horizontal scaling and is required for every large memory footprint application that cannot be run on a smaller system.
- Horizontal scalability grows by adding smaller systems or devices. ***Horizontally scalability*** is used to add or remove resources, adjusting for growth or downsizing. This approach also provides opportunities for upgrades and incident responses.

Moves to the cloud and virtualization have allowed scaling to be done more easily. Many environments support horizontal scaling with software-defined services and systems that can scale at need to meet demand, while also allowing safer patching capabilities and the ability to handle failed systems by simply replacing the system with another identical replacement as needed.

PARTICIPATION ACTIVITY 11.4.5: Vertical and horizontal scaling.



Animation content:

Static figure: A blank screen.
Step 1: Vertical scaling upgrades current servers. Vertical scaling is less expensive and complex compared to horizontal scaling. Three columns of servers appear. Each column from left to right has another server stacked on top.
Step 2: Horizontal scaling adds new servers to support existing servers. Horizontal scaling requires less downtime and increases resilience compared to vertical scaling. To the right of the three Vertical columns of servers are four columns of servers all the same size with an arrow below the server pointing to the right.

Animation captions:

1. Vertical scaling upgrades current servers. Vertical scaling is less expensive and complex compared to horizontal scaling.

2. Horizontal scaling adds new servers to support existing servers. Horizontal scaling requires less downtime and increases resilience compared to vertical scaling.

PARTICIPATION ACTIVITY 11.4.6: Scaling.

1) Horizontal scaling increases the number of servers to provide scalability.
   - True
   - False

2) Horizontal scaling requires less downtime compared to vertical scaling.
   - True
   - False

3) Horizontal scaling is used for large memory footprint applications.
   - True
   - False

4) Horizontal scaling is more resilient than vertical scaling.
   - True
   - False

Replication and recovery concepts

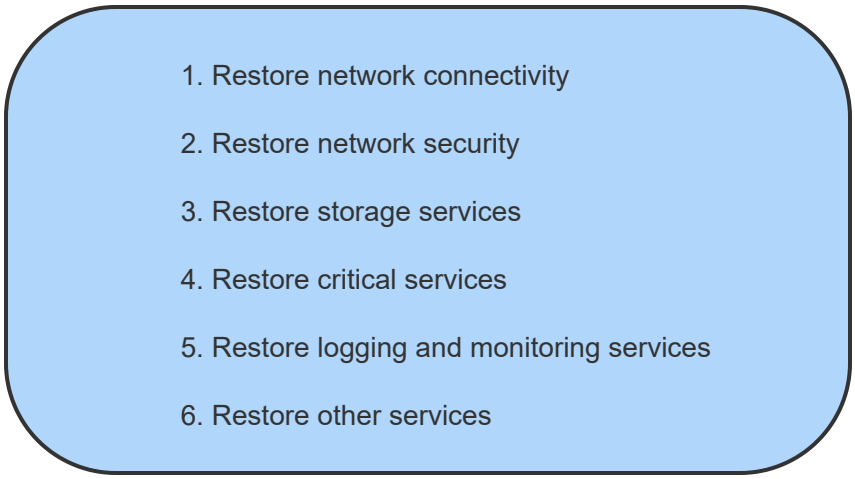
An organization uses various network operations to protect data integrity and resource availability from incidents and disasters. Three network operations maintain data integrity and resource availability:

- ***Replication*** is the process of maintaining at least one data copy or configuration copy, known as a ***backup***.
- ***Recovery*** is the ability to use a backup to recover from an event.
- ***Restoration*** is the process of returning network operations to normal functionality following an event.

Many organizations use geographic dispersity as a part of replication. ***Geographic dispersity*** is the use of multiple geographic locations for replication, recovery, and restoration resources like backups.

A ***functional recovery plan (FRP)*** is a set of processes detailing an organization's recovery and restoration efforts. A ***restoration order*** is an FRP process determining a network service's restoration priority.

PARTICIPATION ACTIVITY | 11.4.7: Restoration order.



Animation content:

Static figure: An example six-step restoration order is displayed.
Step 1: Restoration starts with network connectivity for a shell host so the shell host can restore subsequent network resources. The restore network connectivity restoration step appears.
Step 2: Security devices are restored next to ensure subsequent network resources are properly protected. The restore network security restoration step appears.
Step 3: Storage devices and critical services are restored next to provide user access. The restore storage services and restore critical services restoration steps appear.
Step 4: Logging and monitoring is restored after user access to evaluate the restoration process. The restore logging and monitoring restoration step appears.
Step 5: Non-critical services are restored last. The restore other services restoration step appears.

Animation captions:

1. Restoration starts with network connectivity for a shell host so the shell host can restore subsequent network resources.
2. Security devices are restored next to ensure subsequent network resources are properly protected.
3. Storage services and critical services are restored next to provide user access.
4. Logging and monitoring is restored after user access to evaluate the restoration process.
5. Non-critical services are restored last.

PARTICIPATION ACTIVITY 11.4.8: Replication and recovery concepts.

1) Which network operation ensures a backup is available?
   - Replication
   - Recovery
   - Restoration

2) Which replication process ensures backups are stored in multiple locations?
   - Restoration order
   - HA
   - Geographic dispersity

3) Which plan details how a network service returns to normal functionality after an event?
   - FRP
   - IRP
   - BCP

4) Which process determines why a firewall is restored before a workstation is restored?
   - Load balancing
   - Restoration order
   - Failover

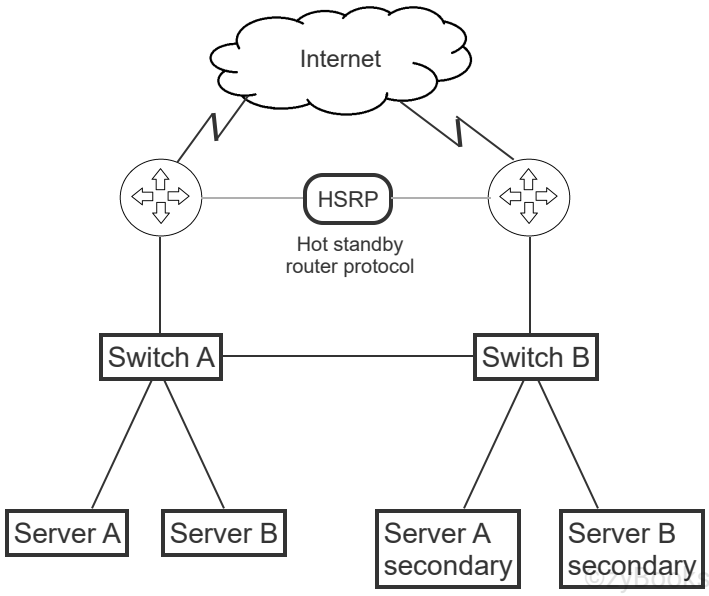
11.5 Redundancy

Network redundancy and resilience

Common elements in designs for redundancy and resilience are:

- Geographic dispersal of systems ensures that a single disaster, attack, or failure cannot disable or destroy the systems. A distance of 90 miles between systems is suggested for geographical dispersal.
- Separation of servers and other devices in data centers.
- Use of multiple network paths (multipath) solutions ensures that a severed cable or failed device will not cause a loss of connectivity.
- Redundant network devices, including multiple routers, security devices like firewalls and intrusion prevention systems, or other security appliances, are also commonly implemented to prevent a single point of failure.
- Protection of power, using uninterruptible power supply (UPS) systems that provide battery or other backup power options for short periods of time.
- Systems and storage redundancy helps ensure that failed disks, servers, or other devices do not cause an outage.
- Diversity of technologies is another way to build resilience into an infrastructure.

PARTICIPATION ACTIVITY 11.5.1: Network redundancy.



Animation content:

Static figure: Two similar network segments are shown. Each network segment consists of two servers connected to a switch, the switches are connected to routers, and the routers are connected to the internet.
Step 1: A network segment includes two servers connected to a switch with a router connected to

the internet. Server A, server B, switch A, a router, and a cloud representing the internet appear. Lines represent the connections between the servers, switch, router, and the internet.
Step 2: A second network segment with secondary servers is deployed. Switches A and B are connected to create multipath. Server A, server B, switch B, and a router appear. A line representing a connection between switch A and B appears.
Step 3: HSRP is configured between the routers to provide redundancy. HSRP allows for transparent failover at the first-hop IP router. An HSRP text box appears between the two routers representing an HSRP configuration between the routers.

Animation captions:

1. A network segment includes two servers connected to a switch with a router connected to the internet.
2. A second network segment with secondary servers is deployed. Switches A and B are connected to create multipath.
3. HSRP is configured between the routers to provide redundancy. HSRP allows for transparent failover at the first-hop IP router.

PARTICIPATION ACTIVITY 11.5.2: Redundancy and resilience.

1) Which solution ensures a severed cable does not cause a loss of connectivity?
   - Separation
   - Replication
   - Multipath

2) Which design element is achieved by using different technologies?
   - Diversity
   - Redundancy
   - Multipath

3) Which design element is achieved by using multiple network devices to eliminate a SPOF?
   - Resilience
   - Redundancy
   - Multipath

NIC teaming

HA for network resources includes multipath and path diversity configurations. ***Path diversity***, or ***path diversification***, is a multipath configuration used to select the most optimal path for data flow reliability. Multipath and path diversification typically rely on network resources with multiple network adapters. ***NIC bonding***, or ***NIC teaming***, is a configuration combining, or aggregating, multiple physical NICs into a logical NIC.

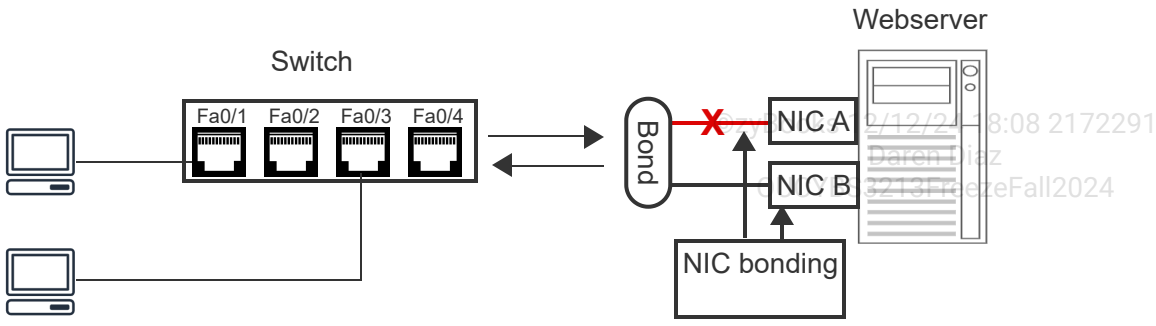
Routers provide default gateway HA by using a first hop redundancy protocol (FHRP). ***First hop redundancy protocol (FHRP)*** is a protocol used to increase a default gateway's availability by aggregating multiple routers into a single virtual router. Two FHRP types exist:

- ***Virtual router redundancy protocol (VRRP)*** is a non-proprietary FHRP type available for various routers.
- ***Hot standby router protocol (HSRP)*** is a Cisco-proprietary FHRP type available for Cisco routers.

NIC teaming or bonding?

NIC teaming, or NIC bonding, is a term used by many vendors to describe a pair of NICs configured to operate as a single NIC. Some vendors consider teaming and bonding to be two different configurations. Ex: Red Hat Enterprise Linux (RHEL) offers NIC teaming or NIC bonding. Both team and bond configurations aggregate two NICs to provide redundancy, resilience, and scalability. NIC teaming offers features not offered by NIC bonding and vice-versa.

PARTICIPATION ACTIVITY 11.5.3: NIC bonding.



Animation captions:

1. PCs and a web server with multiple NICs are connected to a switch. The server's physical NICs, NIC A and NIC B, are bonded for HA.
2. NIC A and NIC B work together to provide load balancing. NIC B maintains connectivity if NIC A fails and vice-versa.

PARTICIPATION ACTIVITY 11.5.4: HA for network resources.

1) What can a server use to provide HA?
   - Bonded media
   - Unbonded media
   - NIC teaming

2) Which routing protocol increases a default gateway's availability?
   - OSPF
   - FHRP
   - RIP

3) Which FHRP type is non-proprietary?
   - VRRP
   - HSRP
   - IGRP

4) Which FHRP type is only available for a Cisco router?
   - VRRP
   - HSRP
   - IGP

Power redundancy

Network redundancy provides multiple paths for traffic, so that data keeps flowing, even in the event of a network failure. Organizations need to also address the concerns of power failures on network devices or environmental controls. Consistent power is critical to keep a business operational. Equipment providing redundant power systems keeps businesses operational during power outages. Equipment used with HA includes:

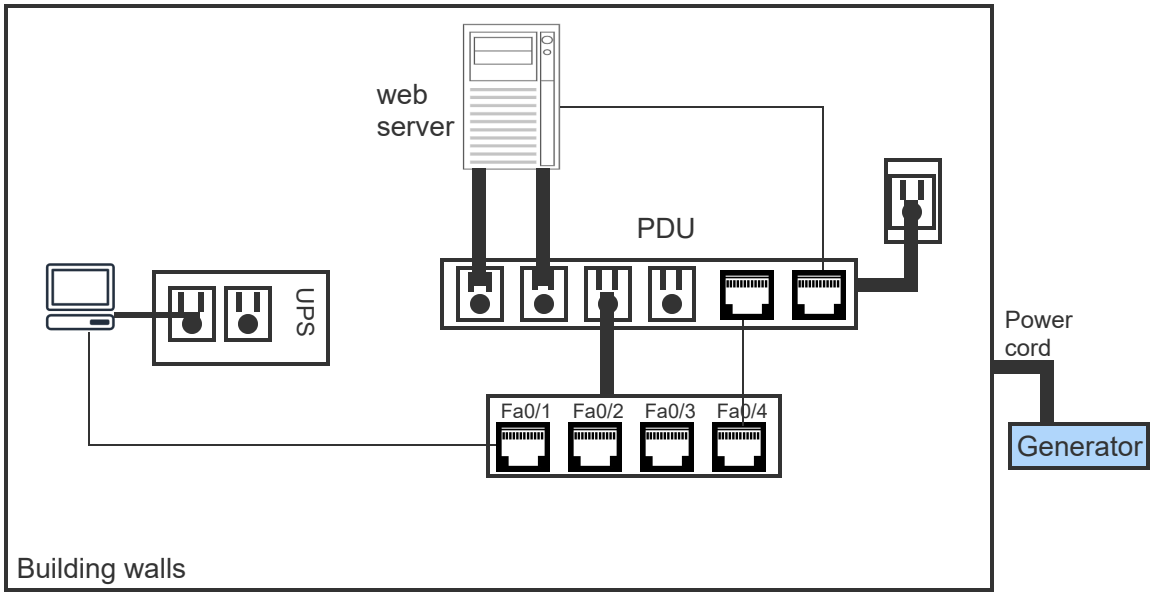
- A ***power supply unit (PSU)***, or ***power supply***, is hardware used to convert and supply received electrical power to other computing hardware.

- ***Dual PSU***, or ***dual supply***, is a pair of PSUs used to ensure the failure of one PSU does not cause an outage or service disruption.
- A ***power distribution unit (PDU)*** is an electrical power strip able to distribute received electrical power to multiple devices and PSUs.
- A ***managed power distribution unit (PDU)*** is a PDU with additional features like remote electrical power monitoring and configuration.
- An ***uninterruptible power supply (UPS)*** is a PDU with a battery backup.
- A ***generator*** is equipment providing long-term electrical power during utility power failure.

Additional equipment ensures an environmental factor or a disaster does not affect HA:

- ***Heating, ventilation, and air conditioning (HVAC)*** is equipment controlling environmental factors like temperature and humidity.
- ***Fire suppression*** is fire detection and extinguishing, or suppressing, equipment.

PARTICIPATION ACTIVITY 11.5.5: Electrical power protection.



Animation content:

Equipment used with HA ensures an electrical power event, a disaster, or environmental factors do not affect HA.

Animation captions:

1. A UPS provides short-term power during utility power failure. A UPS provides backup power to one or multiple devices.

2. Dual power supplies installed in a server keeps the server running if one power supply fails.
3. A managed PDU can provide intelligent power management to a device, a server rack, or an entire data center.
4. A generator is used to provide long-term power during utility power failure. A generator can provide backup power to an entire facility.

PARTICIPATION ACTIVITY 11.5.6: HA equipment.

Select the described equipment.

1) Two power supplies installed in a server.
   - PDU
   - UPS
   - Dual PSU

2) An electric power strip with remote monitoring capabilities.
   - PDU
   - Managed PDU
   - PSU

3) Equipment providing long-term power during a disaster.
   - UPS
   - Generator
   - Dual PSU

4) Data center temperature and humidity control.
   - Fire suppression
   - Managed PDU
   - HVAC

11.6 Data protection

Onsite and offsite replication

Replication involves creating and maintaining one or more identical copies of data or configurations to ensure data redundancy and availability. Two primary replication methods exist:

- ***Onsite***, or ***on-premises (on-prem) replication***, involves creating duplicate copies of data or configurations within the same physical location, such as a server room or data center, to ensure local redundancy.
- ***Offsite***, or ***off-premises (off-prem) replication***, involves creating duplicate copies of data or configurations in a separate physical location, such as a remote data center, public cloud, or disaster recovery site, to ensure geographic redundancy.

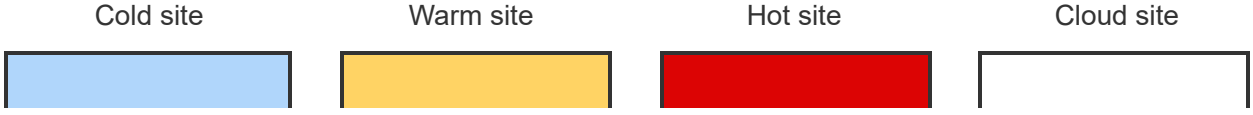
Offsite replication ensures data availability and business continuity in the event of local disasters, system failures, or primary site outages. Four types of disaster recovery sites exist:

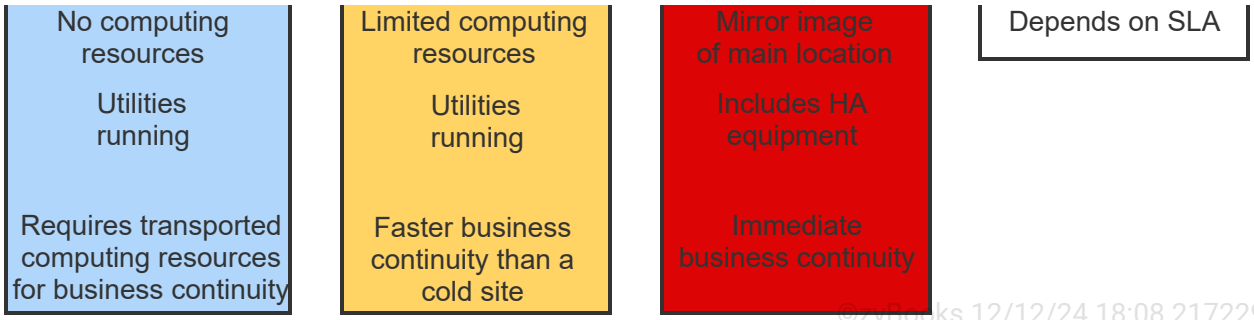
- A ***cold site*** is an empty facility where an organization can transport business continuity resources. A cold site is equipped and prepared in advance, demanding planning regarding human resources needed for activation and operation.
- A ***warm site*** is a facility with some, but not all, business continuity resources. A warm site has technology and infrastructure that can be quickly scaled up with minimal resources.
- A ***hot site*** is a facility with all necessary business continuity resources, requiring continuous management of technology and infrastructure to ensure immediate operational takeover.
- A ***cloud site*** uses a cloud service provider's resources as a disaster recovery site. Service level agreements (SLAs) with the cloud provider ensures that the provider's capabilities align with the organization's needs for availability, scalability, and data security.

Capacity planning is critical for managing disruptions effectively. ***Capacity planning*** involves estimating and preparing the necessary resources across disaster recovery sites to handle emergencies. The planning aligns resources at each disaster recovery site with the demands of various disaster scenarios, ensuring efficient operational transitions and minimal downtime.

Continuity of operations planning (COOP) is a strategy designed to ensure that critical business functions continue during emergencies. COOP aims to maintain or rapidly reinstate critical business functions following a disruption. Properly planned and adequately resourced disaster recovery sites enable the seamless continuation or restoration of operations. The strategy encompasses the integration of physical and technological resources and emphasizes training personnel to execute recovery protocols effectively.

PARTICIPATION ACTIVITY 11.6.1: Disaster recovery sites.





Animation content:

Static figure: The details of a cold, warm, hot, and cloud site are displayed.
Step 1: A cold site is an empty facility where an organization can transport business continuity resources to. Distance is an important consideration when using an offsite location. The cold site's characteristics are displayed and include: no computing resources; utilities running; and requires transported computing resources for business continuity.
Step 2: A warm site includes some, but not all business continuity resources. A warm site provides faster restoration than a cold site. The warm site's characteristics are displayed and include: limited computing resources; utilities running; and faster business continuity than a cold site.
Step 3: A hot site mirrors an organization's primary location. A hot site is immediately functional as an alternative site for an organization. The hot site's characteristics are displayed and include: mirror image of main location; includes HA equipment; and immediate business continuity.
Step 4: An organization must consult the SLA with a cloud service provider to determine the business continuity resources the organization can use in a cloud site. The cloud site's characteristics are displayed and include: depends on SLA.

Animation captions:

1. A cold site is an empty facility where an organization can transport business continuity resources to. Distance is an important consideration when using an offsite location.
2. A warm site includes some, but not all business continuity resources. A warm site provides faster restoration than a cold site.
3. A hot site mirrors an organization's primary location. A hot site is immediately functional as an alternative site for an organization.
4. An organization must consult the SLA with a cloud service provider to determine the business continuity resources the organization can use in a cloud site.

PARTICIPATION ACTIVITY 11.6.2: Replication storage locations.

Identify if a replication storage location is onsite or offsite based on the description provided.

1) A tape drive located in a server room at an organization's headquarters.

- Onsite
- Offsite

2) A NAS located in the basement of a building an organization operates from.

- Onsite
- Offsite

3) Replication to storage located in a public cloud.

- Onsite
- Offsite

4) A remote facility with current backups of all organizational computing resources.

- Onsite
- Offsite

Full, differential, and incremental backups

A ***data backup*** is the process of copying data from a primary to a secondary location, protecting the data from malicious action or disaster. A data backup is an excellent example of preventive control. Three data backup options exist:

- A ***full backup*** is data replication for all data.
- A ***differential backup*** is data replication for all data created or changed since the last full backup.
- An ***incremental backup*** is data replication for all data created or changed since the last full or incremental backup.

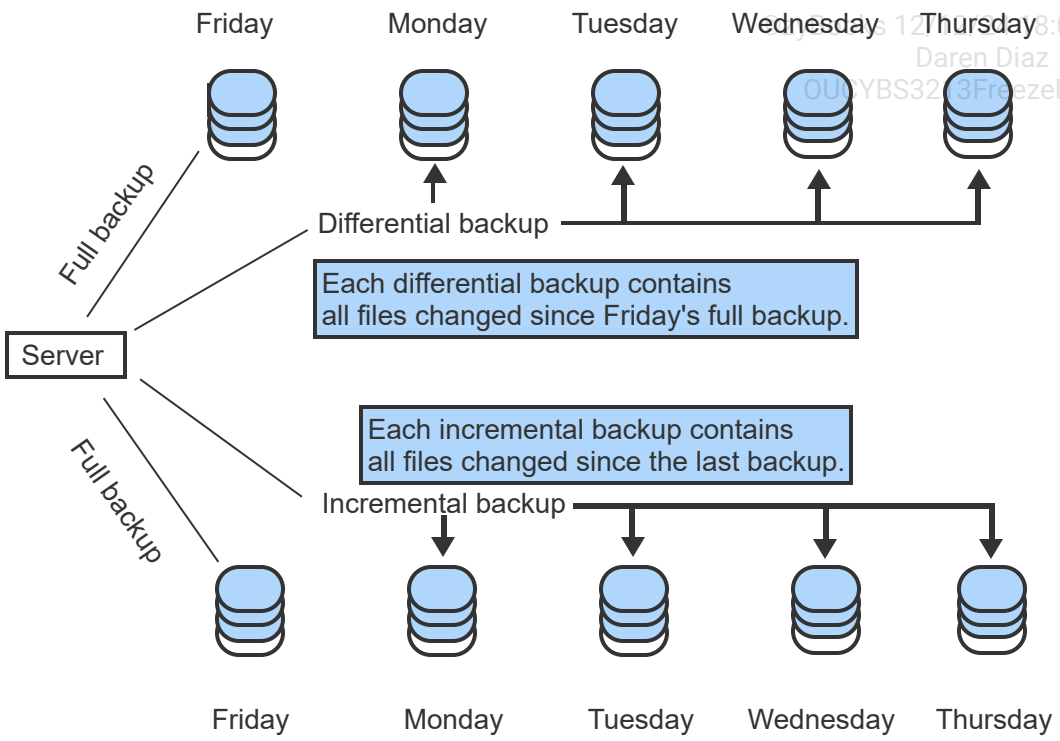
To further enhance data integrity and facilitate a robust recovery process, backup journaling can be employed. ***Backup journaling*** involves recording and tracking every change made to data during backup operations. The journal enables for reverting to a previous state in the event of system failure or data corruption, ensuring data consistency and reducing recovery time.

A data replication strategy typically uses all three data backup options:

- A full backup is created during system deployment to replicate all initial data.
- A daily incremental backup is scheduled to run automatically during off-hours.
- A weekly differential backup is scheduled to run automatically during off-hours.

- A monthly full backup replaces the initial full backup or the previous month's full backup.

PARTICIPATION ACTIVITY | 11.6.3: Replication options.



Animation content:

Static figure: A server's backup schedule is displayed.
Step 1: A full backup replicates all data in a single operation. A full backup is commonly scheduled on a weekly or a monthly basis. The server performs a full backup on a Friday.
Step 2: A differential backup replicates all created or changed data since the last full backup. A differential backup is usually faster than a full backup. The server performs a differential backup on Monday, Tuesday, Wednesday, and Thursday. Each differential backup contains all files changed since Friday's full backup.
Step 3: A daily incremental backup replicates data files created or changed since the last full or incremental backup. The server performs another full backup on a Friday. The server performs an incremental backup on Monday, Tuesday, Wednesday, and Thursday. Each incremental backup contains all files changed since the last backup.

Animation captions:

1. A full backup replicates all data in a single operation. A full backup is commonly scheduled on a weekly or a monthly basis.

2. A differential backup replicates all created or changed data since the last full backup. A differential backup is usually faster than a full backup.
3. A daily incremental backup replicates data files created or changed since the last full or incremental backup.

PARTICIPATION ACTIVITY 11.6.4: Data replication.

1) Which replication option captures all data regardless of the data's backup status?
   - Full backup
   - Differential backup
   - Incremental backup

2) Which replication option is typically scheduled on a daily basis?
   - Full backup
   - Differential backup
   - Incremental backup

3) A differential backup executes only after which other replication option?
   - Full backup
   - Incremental backup
   - Restoration

4) Which replication option is used during a system's deployment?
   - Full backup
   - Differential backup
   - Incremental backup

5) What does the ability to revert to a previous state imply about a backup journal's functionality?
   - The journal increases data transfer rates across the network

- The journal records changes in chronological order
- The journal maintains a real-time backup of all transactions and changes

Backup media

Data backup is essential for organizations to perform their core business functions and to keep the business running in the event of hardware failures or natural disasters. Choosing the storage devices or backup media to use for backups is a step in creating a backup process. Backup storage options:

- A ***disk*** is a data storage device using either platters in a ***hard disk drive (HDD)*** or integrated memory modules in a ***solid-state drive (SSD)***.
- An ***optical disc*** is a data storage device using either a ***digital video disc (DVD)*** or ***Blu-ray disc (BD)***.
- A ***tape drive***, or ***tape***, is a data storage device using magnetic tape.
- A ***boot disk***, or ***live boot media***, is a portable disk or optical disc containing a bootable operating system.

Multiple disks are commonly used to provide replication for a PC or server. ***Redundant array of inexpensive disks (RAID)*** is a logical combination of multiple disks to provide redundancy and replication.

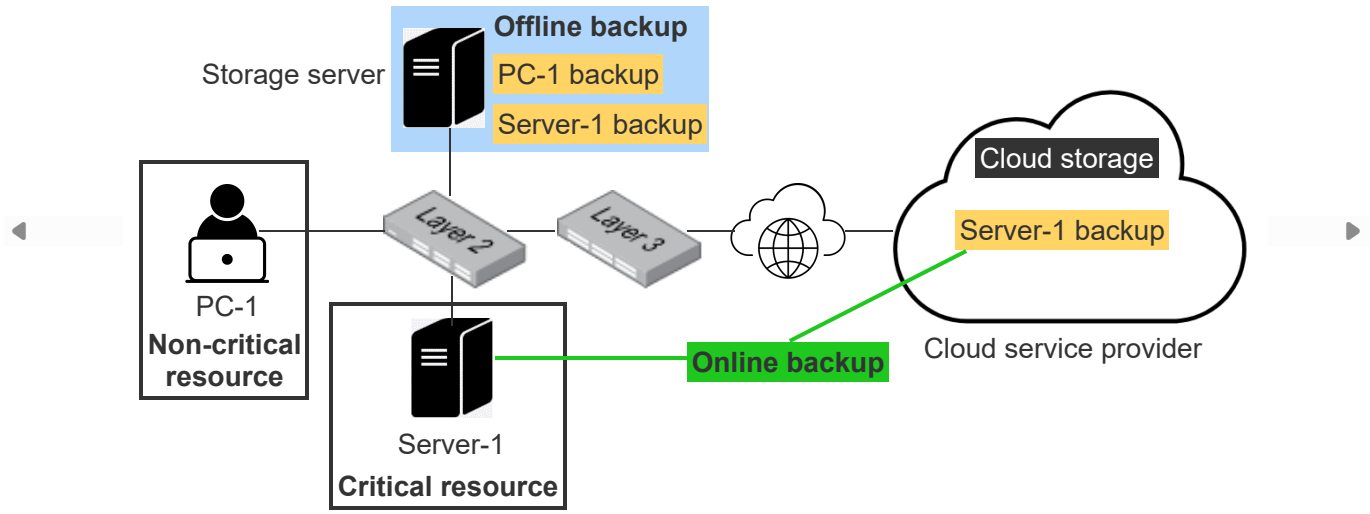
Table 11.6.1: RAID levels.

Level	Name	Minimum disks required	Description
0	Striping	2	Data is spread, or striped, to other drive(s)
1	Mirroring	2	Data is replicated, or mirrored, to other drive(s)
5	Striping with parity	3	Striping with one drive providing error detection, or parity
6	Striping with double parity	4	RAID 5 with two parity drives
10	Mirroring and striping	4	Combination of RAID 1 and 0

Two storage strategies are used for backups:

- An ***online backup*** is an always updated and accessible backup to a third-party or cloud service provider.
- An ***offline backup*** is a regularly updated and readily available backup to on-premise storage.

PARTICIPATION ACTIVITY 11.6.5: Online vs. offline backup storage.



Animation content:

Static figure: The online and offline backup options are displayed for a network consisting of a PC, two servers, a switch, a router, an internet connection, and a cloud service provider.
Step 1: Online and offline backups are commonly used together to meet organizational needs. The network appears with options for online and offline backups. An online backup uses a green label with black text. An offline backup uses a blue label with black text.
Step 2: An online backup is used with a mission critical resource to provide the fastest recovery and restoration possible. Server-1 is labeled as a critical resource. A backup of Server-1 is created and sent to the cloud storage with the cloud service provider. The online backup label is applied to Server-1's backup.
Step 3: An offline backup is used with a non-critical resource to provide slower, but equally reliable recovery and restoration. PC-1 is labeled as a non-critical resource. A backup of PC-1 is created and sent to the storage storage located on the local network. The offline backup label is applied to PC-1's backup.
Step 4: An offline backup can serve as a backup to an online backup. Ex: Server-1 can store an online and offline backup for redundancy and diversity. A second backup is created for Server-1 and sent to the storage server located on the local network.

Animation captions:

1. Online and offline backups are commonly used together to meet organizational needs.
2. An online backup is used with a mission critical resource to provide the fastest recovery and restoration possible.
3. An offline backup is used with a non-critical resource to provide slower, but equally reliable recovery and restoration.
4. An offline backup can serve as a backup to an online backup. Ex: Server-1 can store an online and offline backup for redundancy and diversity.

PARTICIPATION ACTIVITY 11.6.6: Backup storage.

Match each storage backup option to the correct description.

How to use this tool

Disk **Live boot media** **RAID** **Optical disk**

	An SSD used to store a backup.
	Multiple disks configured for replication.
	A BD used to store a backup.
	A HDD with a bootable operating system.

Reset

Storage

While traditional backup methods have used onsite storage options like tape drives, storage area networks (SANs), and network attached storage (NAS) devices, cloud and third-party offsite backup options have continued to become increasingly common.

A few important considerations come into play with cloud and offsite third-party backup options:

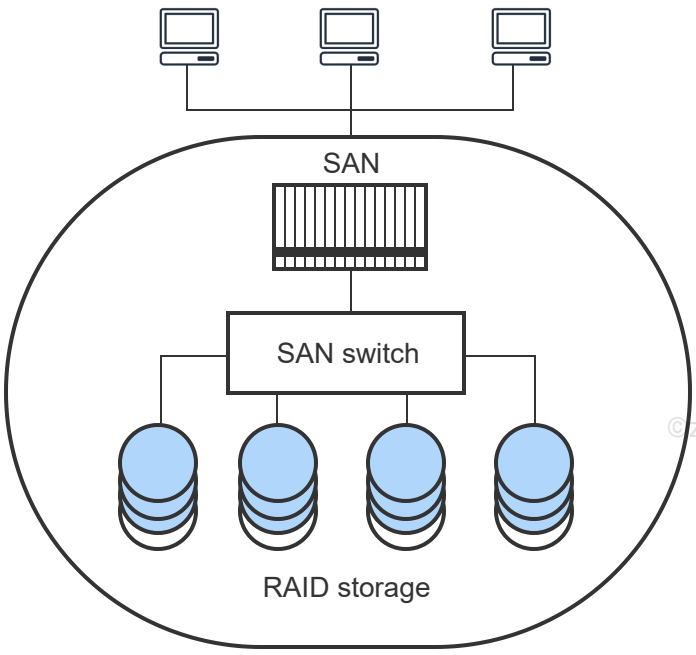
- Bandwidth requirements for both the backups themselves and restoration time if the backup must be restored partially or fully. Organizations with limited bandwidth or locations with low

bandwidth are unlikely to be able to perform a timely restoration. This fact makes offsite options less attractive if quick restoration is required, but remains attractive from a disaster recovery perspective to ensure that data is not lost completely.

- Time to retrieve files and cost to retrieve files. Solutions like Amazon's Glacier storage focus on low-cost storage but have higher costs for retrieval, as well as slower retrieval times. Administrators need to understand storage tiering for speed, cost, and other factors, but must also take these costs and technical capabilities into account when planning for the use of third-party and cloud backup capabilities.
- Reliability. Many cloud providers have extremely high advertised reliability rates for their backup and storage services, and these rates may beat the expected durability of local tape or disk options.
- New security models are required for backups. Separation of accounts, additional controls, and encryption of data in the remote storage location are all common considerations for use of third-party services.

A SAN typically provides block-level access, looking like a physical drive. NAS devices usually present data as files. This line is increasingly blurring since SAN and NAS devices may be able to do both. Organizations may simply use SAN and NAS to describe big (SAN) or smaller (NAS) devices. SANs are typically more expensive, have faster access times, and higher bandwidth than a NAS.

PARTICIPATION ACTIVITY | 11.6.7: SAN.



Animation content:

Step 1: Three computers connect to a network containing a SAN. A SAN is a multilocation network built to share storage resources with an authorized entity. Step 2: A SAN switch and RAID storage appears in the network. A SAN enhances storage devices, like disk arrays and tape libraries, making the drives appear as external hard drives on their local system.

Animation captions:

1. A SAN is a multilocation network built to share storage resources with an authorized entity.
2. A SAN enhances storage devices, like disk arrays and tape libraries, making the drives appear as external hard drives on their local system.

PARTICIPATION ACTIVITY 11.6.8: Storage.

1) Which network characteristic must an organization consider for an offsite backup?
   - Bandwidth
   - Time to retrieve file
   - Reliability

2) Which storage solution device normally accesses and transfers data the quickest?
   - NAS
   - SAN
   - Tape

3) Which storage characteristic measures the quality of a backup?
   - Multipath
   - Bandwidth
   - Reliability

Device configuration

A device's configuration is stored in two different storage locations:

- ***Non-persistent storage*** is a temporary storage location where stored data does not survive a power loss.
- ***Persistent storage*** is a permanent storage location where stored data survives a power loss.

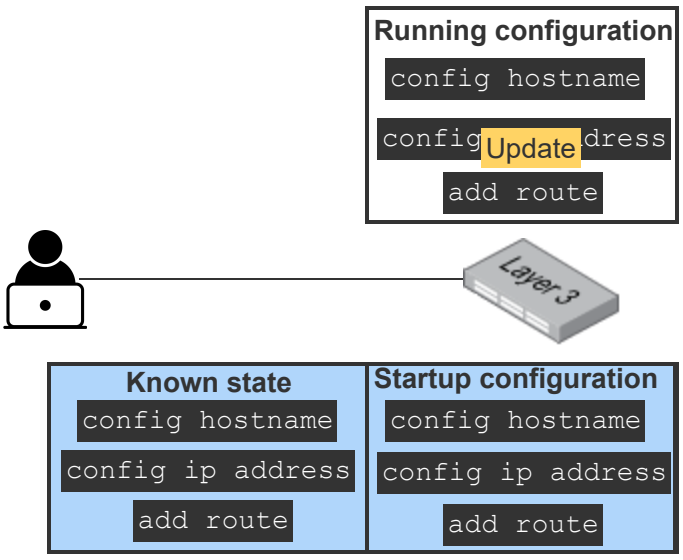
A device has multiple configurations depending on which storage location is used:

- A ***startup configuration*** is a device configuration located in persistent storage.
- A ***running configuration*** is a device configuration located in non-persistent storage.

A running configuration can be saved to persistent storage to become the new startup configuration or be saved as a device state. A ***device state*** is used to provide configuration replication through a persistent point-in-time device configuration. A device state providing a guaranteed operational configuration is considered a ***known state*** or a ***known-good configuration***. Three known-good configurations exist:

- A ***last known good configuration*** is a known-good configuration created automatically by Microsoft Windows.
- A ***snapshot*** is a manually created known-good configuration commonly used for a VM.
- An ***image*** is a manually created known-good configuration commonly used for a PC or server.

PARTICIPATION ACTIVITY 11.6.9: Configuration replication.



Animation content:

Static figure: None. Step 1:A network administrator deploys and configures a new router. Saving the initial baseline configuration to persistent storage creates the startup configuration. A user connected to a router appears. A box title running configure appears above the router with the commands config hostname and config ip sent to the router appears in the box. A box titled startup config appears below the router. When the user sends the command copy running-config startup-config the information in the running config box is copied to the running config box. Step 2: The network administrator adds a new route to the router's routing table during runtime. The routing

table entry becomes part of the router's running configuration. The add route command appears in the running config. Step 3: Saving the running configuration to persistent storage creates a new startup configuration. The user issues a copy running-config startup-config command the information in the running config is copied to the startup config. Step 4: The router requires an update. A last known state is saved to persistent storage before installing the update. The update is pushed to the router. The user issues an update command to the router and the running config is copied to persistent storage as the last Known state.

Animation captions:

1. A network administrator deploys and configures a new router. Saving the initial baseline configuration to persistent storage creates the startup configuration.
2. The network administrator adds a new route to the router's routing table during runtime. The routing table entry becomes part of the router's running configuration.
3. Saving the running configuration to persistent storage creates a new startup configuration.
4. The router requires an update. A last known state is saved to persistent storage before installing the update. The update is pushed to the router.

PARTICIPATION ACTIVITY 11.6.10: Configuration replication.

1) Where is a startup configuration stored?
   - Non-persistent storage
   - Persistent storage
   - A storage area network

2) Which changed configuration is stored in non-persistent storage?
   - Running configuration
   - Startup configuration
   - Baseline configuration

3) Which configuration is guaranteed to be operational?
   - Known-bad
   - Known-good
   - Non-persistent configuration

4) Which device state is manually saved to persistent storage?

- Last known good configuration
- Active-active
- Snapshot

11.7 LAB: Backup and restore (Walkthrough)

IT-Labs are not printable at this time.

11.8 LAB: Redundant Array of Independent Disks (RAID) (Walkthrough)

IT-Labs are not printable at this time.

11.9 LAB: Securing data at rest (Scenario)

IT-Labs are not printable at this time.