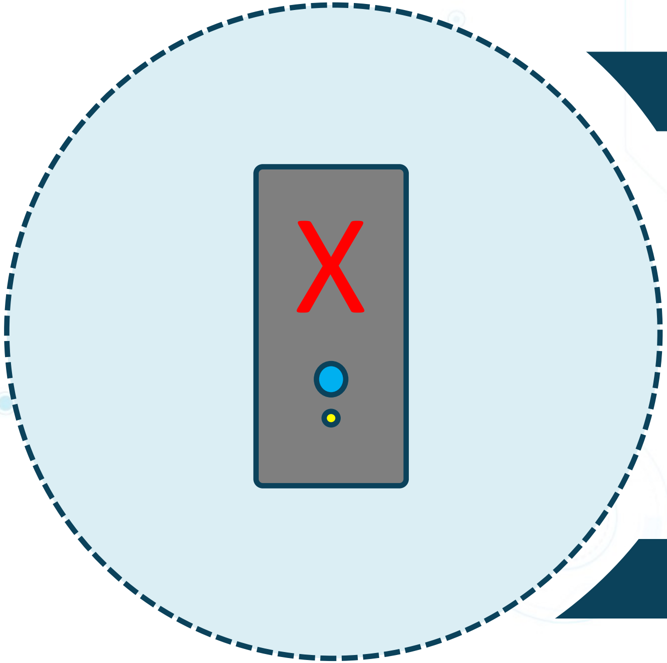
High Availability

- Reliability
  - Data processing systems
  - Data
  - Business processes

Unavailability



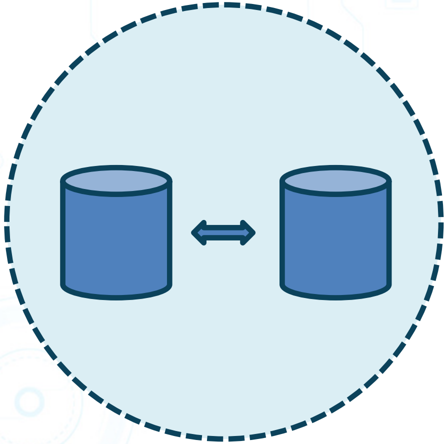
- Reputation loss
- Lack of compliance with laws and regulations
- Increased customer wait time
- Loss of revenue
- Personnel safety

High Availability

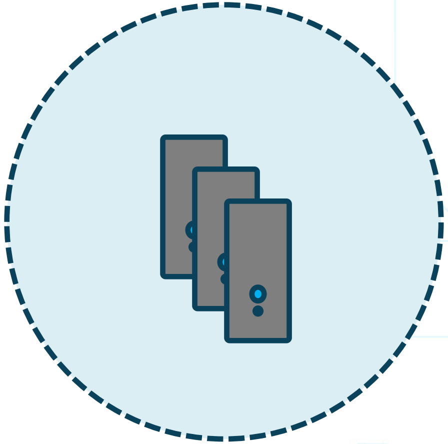
- Service Level Agreements (SLAs)
  - Contracts guaranteeing a level of service including availability
- IS availability auditing
  - Prioritize processes and systems data
  - Assess current availability implementations
    - This reveals risk

Availability Solutions

Data backup



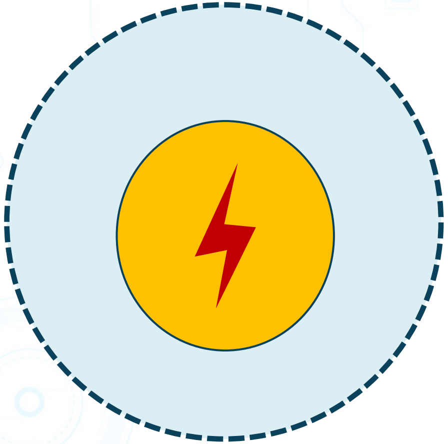
Replication to other regions



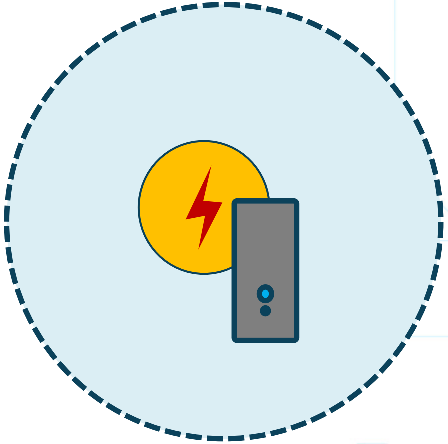
Clustering/load balancing

Availability Solutions

Redundant Internet connections

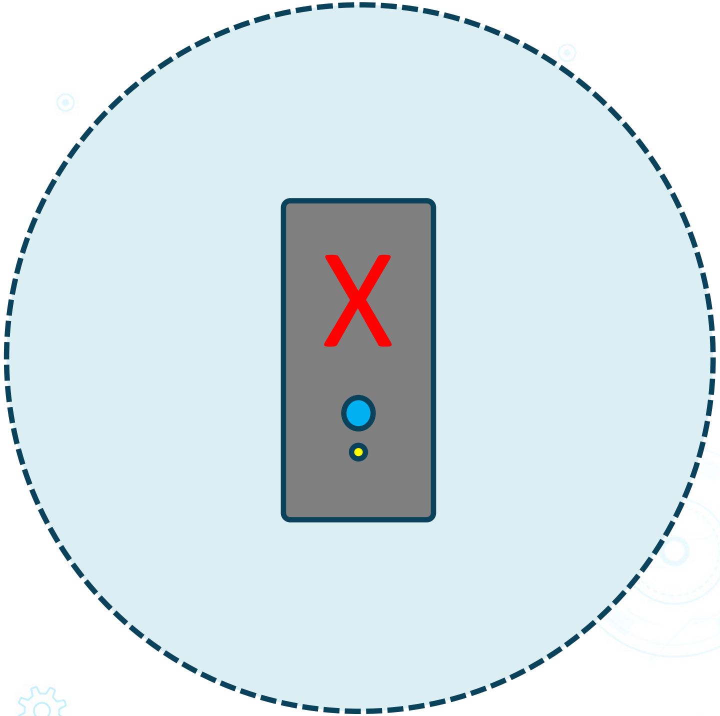


Backup power generators



Uninterruptible Power Supply (UPS)

Disaster Recovery Plan (DRP)



- Part of the overall Business Continuity Plan (BCP)
- Example problems
  - Crashed ecommerce website
  - Remote data center unreachable
  - Data corruption
  - Fire

Disaster Recovery Planning

Recovery Time Objective (RTO)

- Maximum tolerance for downtime
- Brings systems back online
- Data recovery time
- Time to move operations to an alternate site

Recovery Point Objective (RPO)

- Maximum tolerance for data loss
- How often backups should be taken
- Finance servers vs. file servers containing documentation

Disaster Recovery Planning

Mean time to repair (MTTR)

- Restoration time average
- Equipment reliability
- The more mature a system, the less time required for restoration

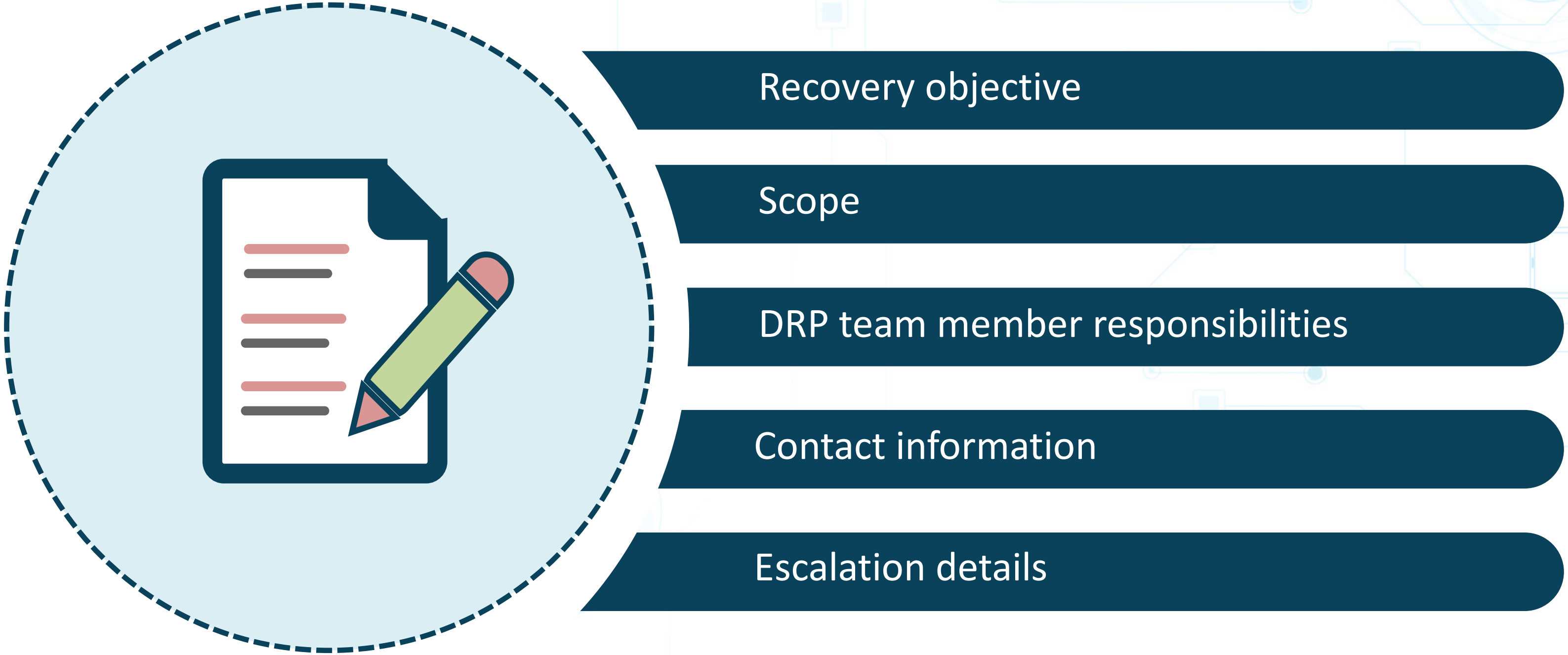
Mean time between failures (MTBF)

- Failure rate average
- Availability percentage

MTBF/(MTBF + MTTR) x 100

6000/(6000 + 4) x 100 = 99.93%

Disaster Recovery Plan Document



- Recovery objective
- Scope
- DRP team member responsibilities
- Contact information
- Escalation details

Business Continuity

- Proactive planning for business disruptions
  - Natural disasters
  - Man-made disasters
- Employees must know their roles
  - Documentation accessibility

Business Impact Analysis (BIA)

- Identify and prioritize assets
- Consider loss of the asset, likelihood, and restoration time
    - Loss of revenue
    - Reputation loss
    - Non-compliance with laws and regulations
    - Reduced shareholder confidence

Business Continuity Plan (BCP)

- Identify critical business processes
- Specific disaster recovery plans
- Consider
  - Alternate business sites
  - Task outsourcing during a crisis
- Periodic review

Incident Response Plan (IRP)

- Incident response plan must be in effect before breaches
- Effects of inadequate incident response
  - Financial
  - Reputation
  - Business partnerships
- Annual review to keep up with changing threats

Incident Response Plan Details

- Procedures
- Data flow diagrams
- Network diagrams
- System configuration details
- Call list

Call List

- Incident response team contact information
- Chief Information Officer (CIO)
- System administrators
- Legal counsel
- Law enforcement
- Public Relations (PR) officer

Incident Response and Compliance

- Legal/regulatory requirements
  - Security breach notification requirement
  - Personally Identifiable Information (PII)
    - US HIPAA breach involving > 500 individuals
    - Canadian Digital Privacy Act
  - E.g. customer notification requirement for credit card data security breach

Alternate Recovery Sites

- Business continuity
- Physical facility
- Alternate network location for IT services

Cold Site

- Alternate business location
- Lacking
  - Hardware
  - Software
  - Data

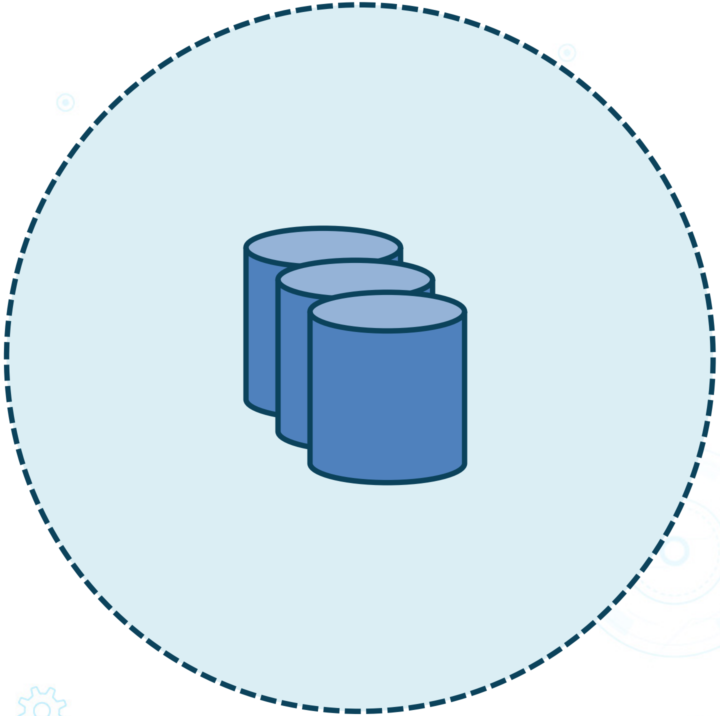
Warm Site

- Alternate business location
- Has hardware and software
- Data must be restored from backup

Hot Site

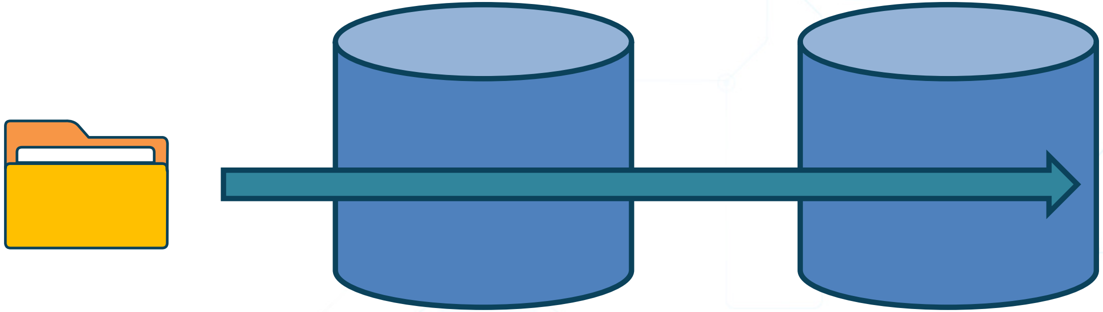
- Alternate business location
- Shortest RPO compared to cold and warm sites
- Has hardware, software, and up-to-date data
  - Data replication from primary site

Redundant Array of Independent Disks (RAID)



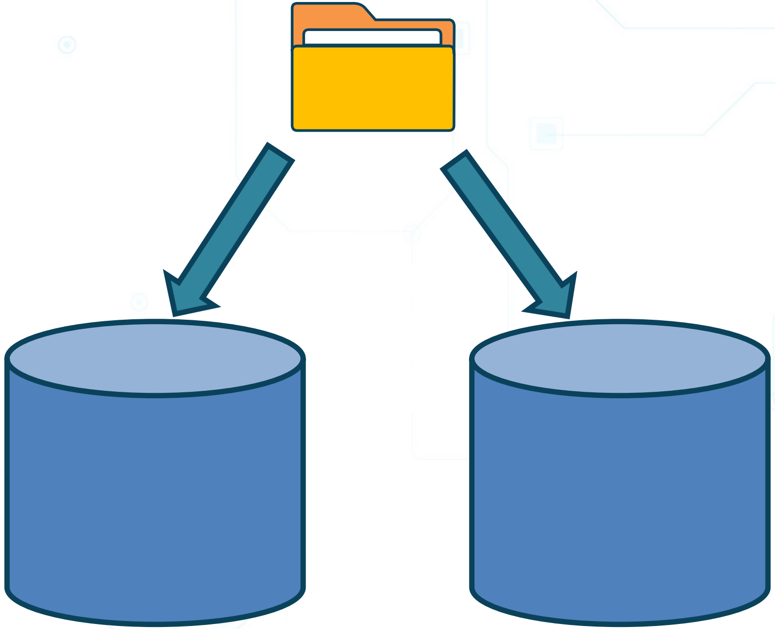
- Multiple physical storage devices working together as a single logical drive
- Hardware RAID controller
- Software RAID

RAID 0 - Disk Striping



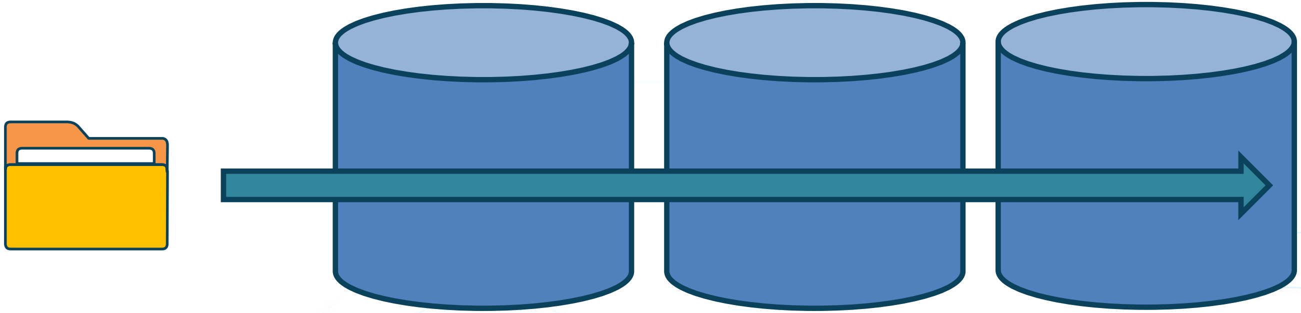
Data is written across all disks in the array

RAID 1 - Disk Mirroring



The same data is written to both disks

RAID 5 - Disk Striping with Distributed Parity



- Data is written across all disks in the array
- Parity information is written on a different disk than the related data

Network Attacks

Wired

Wireless

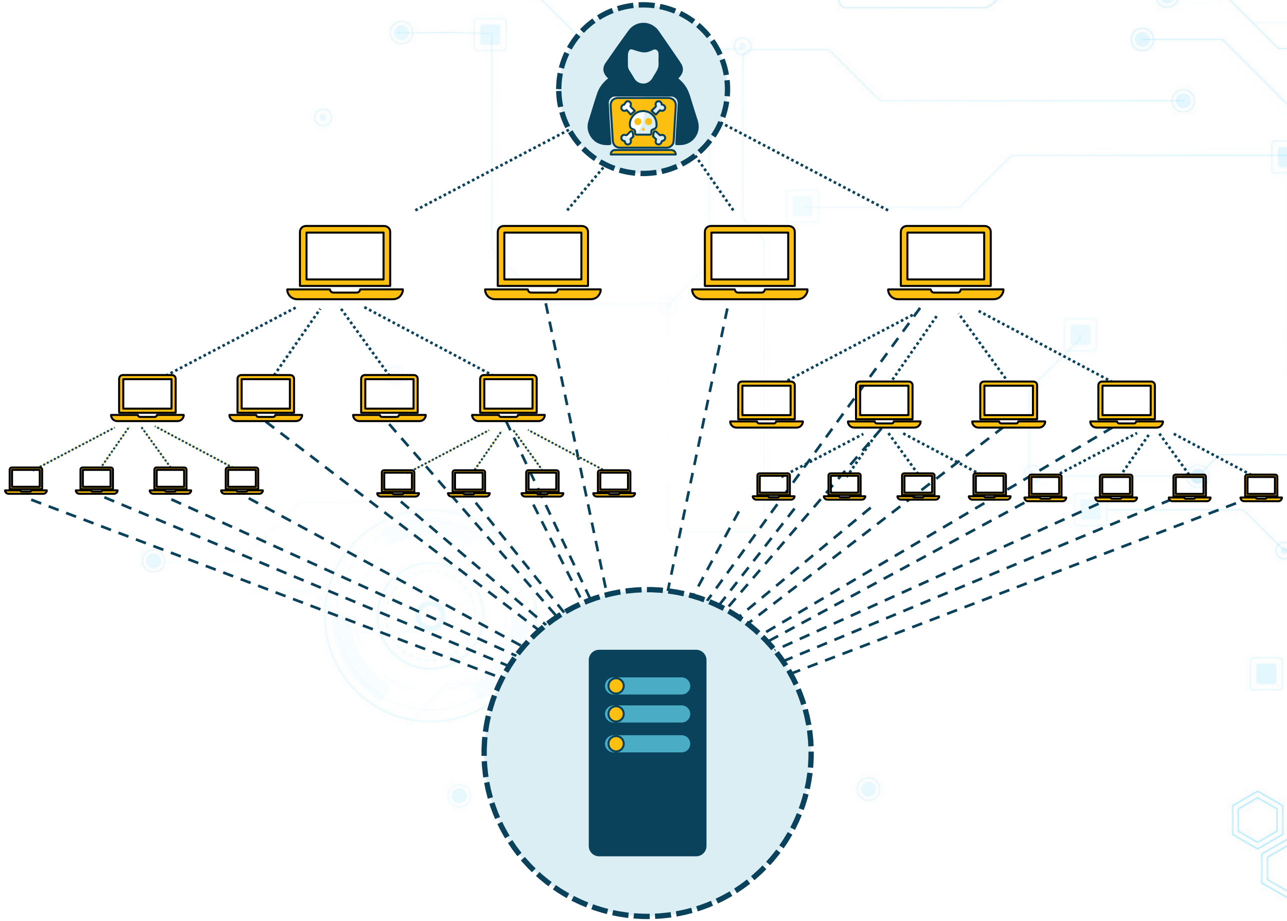
Wired Networks

- Twisted pair cabling
  - Copper wires that transmit electrical signals
  - Relatively easy to wire tap
- Fiber optic
  - Tiny fibers that transmit light
  - Longer transmission range than twisted pair
  - Difficult to tap into

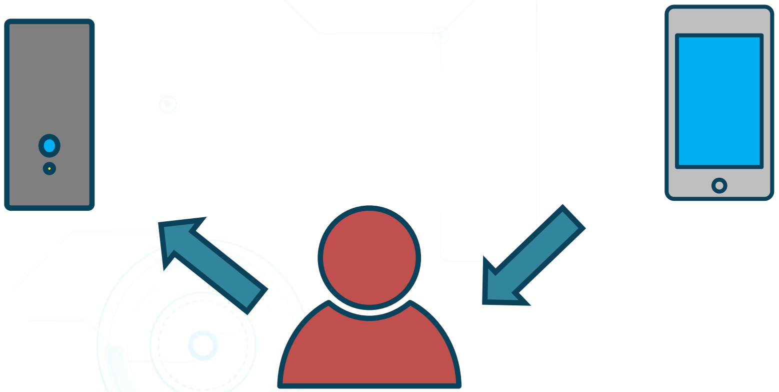
Wireless Networks

- Near field communication (NFC)
- Bluetooth
- Wi-Fi
- Cellular
- Satellite

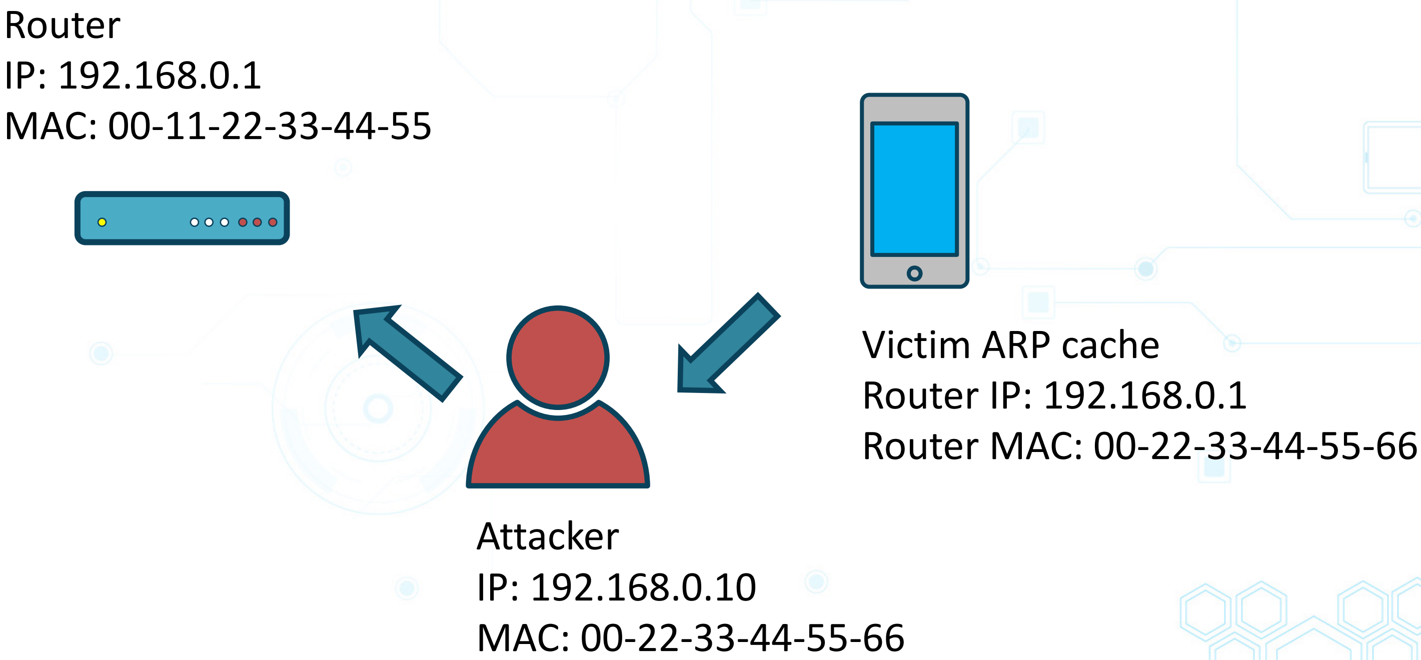
Distributed Denial of Service (DDoS)



Man in the Middle (MiTM)



ARP Poisoning



Router
IP: 192.168.0.1
MAC: 00-11-22-33-44-55

Victim ARP cache
Router IP: 192.168.0.1
Router MAC: 00-22-33-44-55-66

Attacker
IP: 192.168.0.10
MAC: 00-22-33-44-55-66

DNS Spoofing

- Attacker compromises a DNS server or client DNS resolver cache
- Valid DNS names return fake IP addresses
- Fake IP addresses point to malicious sites

Network Threat Mitigation

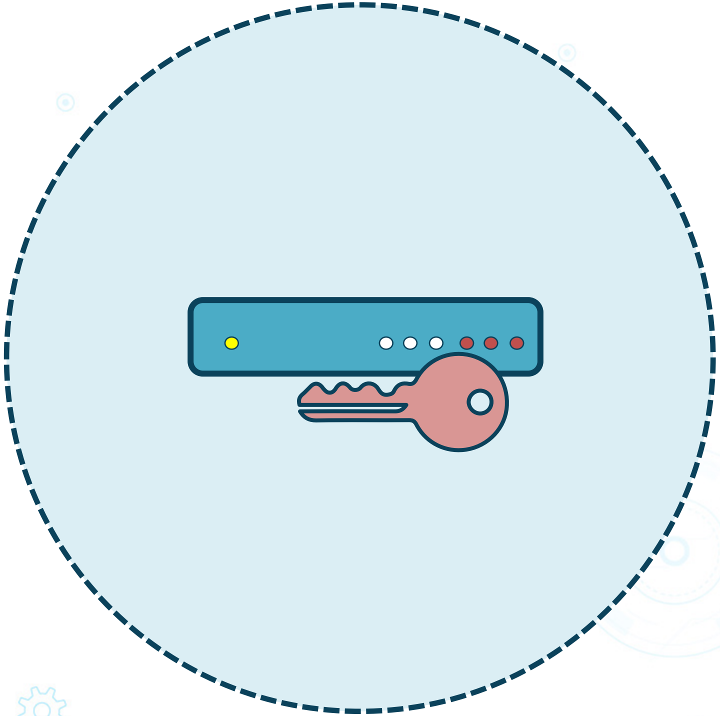
Wired

- Limit access to wiring closets
- Disable unused switch ports
- Switch port static MAC addresses

Wireless

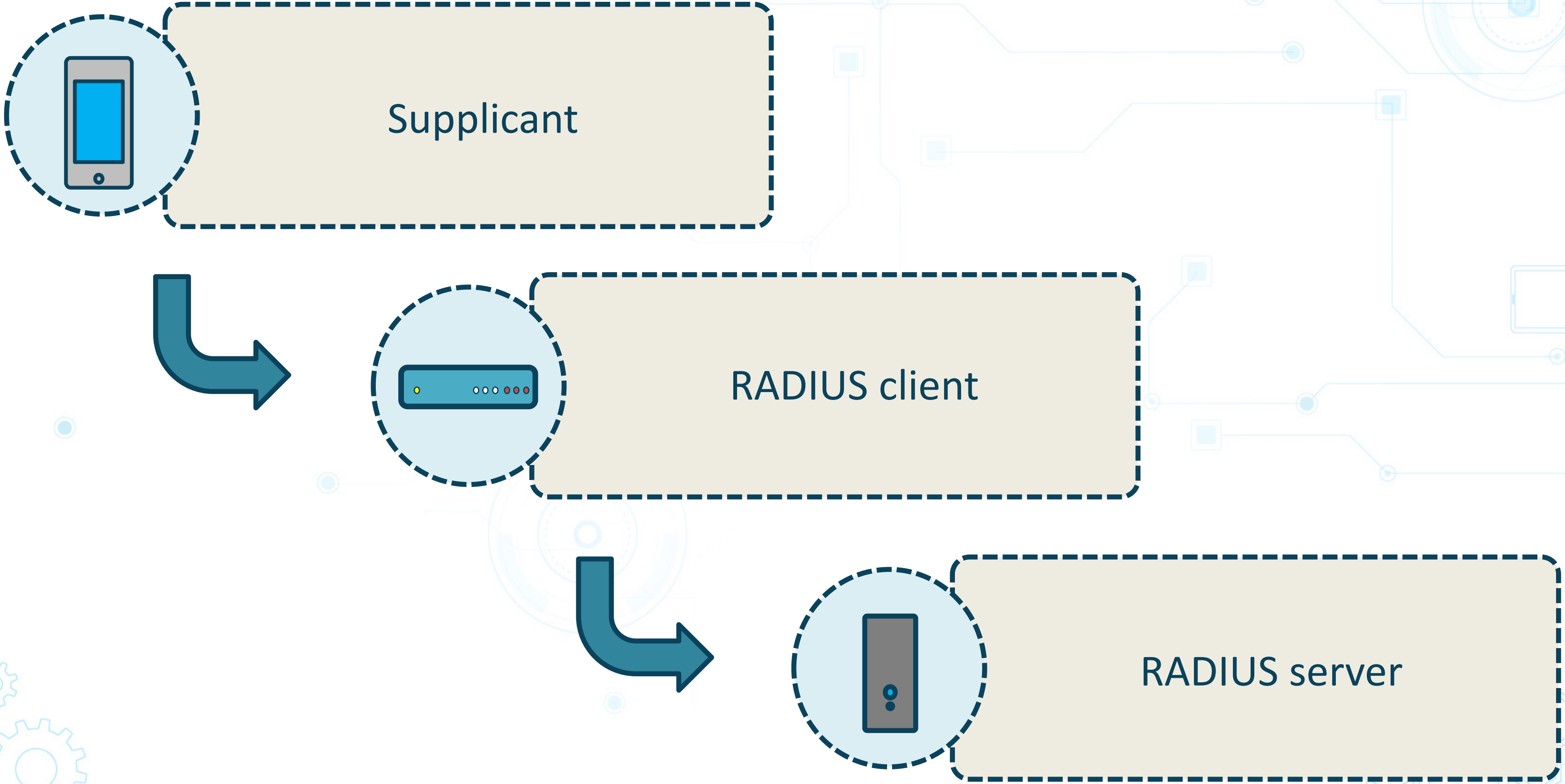
- Disable SSID broadcasting
- MAC address filtering
- WPA2
- RADIUS authentication
- Guest network
- AP isolation mode

Network Access Control (NAC)



- IEEE 802.1X
- Connectivity points
  - Network switch
  - Wireless router
  - VPN
  - Dial-in

Network Authentication Process



Supplicant

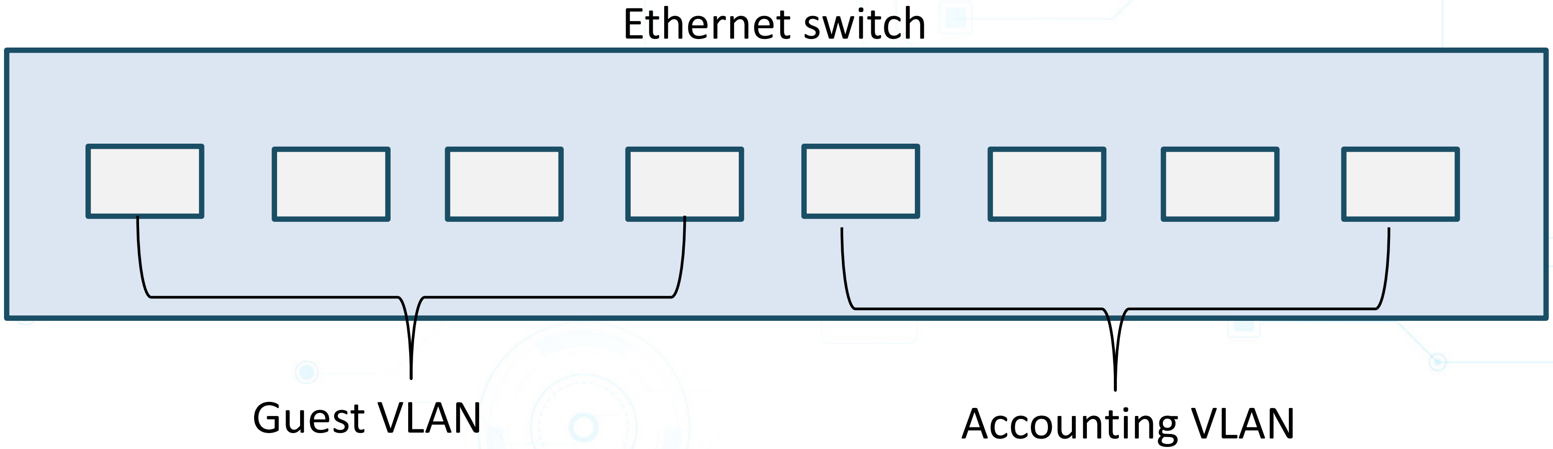
RADIUS client

RADIUS server

Network Access Control

- Client (supplicant) health checks
  - Some configurations can be auto-remediated
  - Malware scanner
  - Firewall
  - Updates applied
  - Correct hardware peripherals exist

Virtual Local Area Network (VLAN)



Firewalls

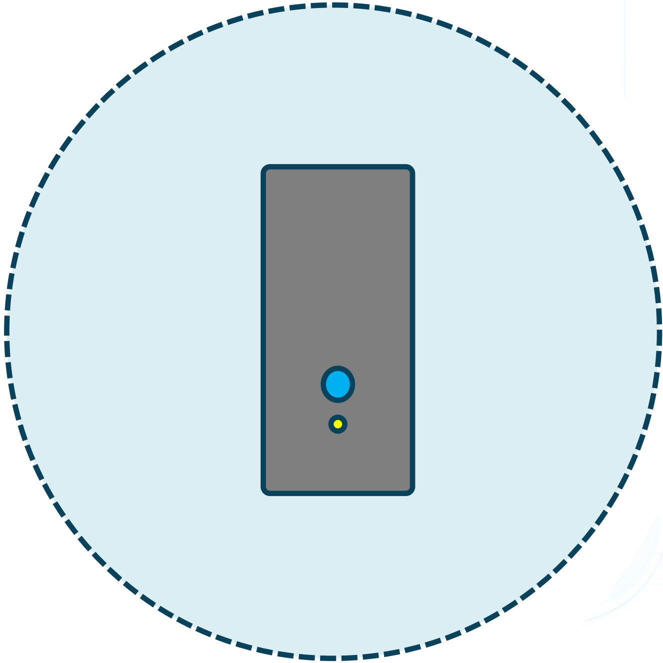
Hardware

Software

Packet Filtering Firewalls

- IP addresses and port numbers
- Protocol type
- Incoming and outgoing interface
- Placement

Forward Proxy Servers



- Sits between user and Internet (DMZ)
- Fetches content on behalf of user
- Content can be cached

Web Application Firewall (WAF)

- Specific to HTTP/S connectivity to web applications
- Protection against common web app attacks
  - SQL injection
  - Cross-site scripting
  - Directory traversal

In this exercise, you will

- Differentiate between RPO and RTO
- Describe when RAID 0 vs. RAID 5 should be used
- List network security options
- Configure software RAID 1 using a Windows Server virtual machine

RPO and RTO

- Recovery point objective (RPO)
  - Maximum tolerable amount of data loss
- Recovery time objective (RTO)
  - Maximum tolerable amount of downtime

RAID

- RAID 0 - Striping
  - Improves performance
  - Minimum of 2 disks
- RAID 5 - Striping with distributed parity
  - Improves performance and availability
  - Minimum of three disks

Network Security

- Fiber optic vs. twisted pair
- Encrypt data in transit
- Network access control
- Wi-Fi
  - Disable SSID broadcasting
  - MAC address filtering