

## Chapter 18



# Network Operations

CompTIA Network+



# Episode 18.01

Episode title: **What are Network Operations?**

Objective: **4.1 Explain common security concepts**

# Key Terms



- Security risks
- Business risks
- Documentation
- Nondisclosure agreement (NDA), memorandum of understanding (MOU), bring your own device (BYOD), statement of work (SOW)
- Change management

# Key Terms



- Disaster planning
- Forensics
- Incident response
- High availability

## Quick Review



- Network operations is a broad term that describes the actions needed to be taken to protect the network and organization
- Two main risks are security and business
- High availability ensures that your network doesn't go down



# Episode 18.02

Episode title: **Security Policies**

Objective: **3.2 Explain the purpose of organizational documents and policies**

# Acceptable Use Policy



- Define ownership
- Web site access
- Access time

# Remote Access Policy



- VPN
- Authentication



# Password Policy



- Complexity
- Lockout

# IT Safety Policy



- Lifting equipment
- Equipment handling
- Spills
- Procedures

# License Restriction



- Usage
- Transfer
- Renewal

# International Export Control



- Military information
- Nuclear information
- License keys

# Key Terms



- Nondisclosure agreement (NDA)

## Quick Review



- Security policies document to users how to access system resources and what is allowable and acceptable
- Safety policies apply to the IT department too!
- NDAs, software licensing, and data restrictions need to be considered to protect an organization



# Episode 18.03

Episode title: **Change Management**

Objective: **3.2 Explain the purpose of organizational documents and policies**

## Key Terms



- Change management... here we go!
- Change management team... action figures!
- Some are even human
- Strategic change vs. infrastructure change
- Documentation is the last step in change management process



## Quick Review



- The change management team handles infrastructure-level changes
- The change process includes requests, types of changes, configuration procedures, rollback and more
- The end game is documentation of all the changes made



# Episode 18.04

Episode title: **Patching and Updating**

Objective: **4.3 Given a scenario, apply network hardening techniques**

# Key Terms



- Patching
- Operating system updates
- Driver updates
- Firmware updates
- Research
- Test
- Configuration backups

## Quick Review



- Operating system updates are the most common type of update
- Firmware updates are necessary, but they depend on the device
- Before patching, be sure to research, test, and configure backups



# Episode 18.05

Episode title: **Security Risk Management**

Objective: **4.1 Explain common security concepts**

# Key Terms



- Asset
- Threat assessment
- External threats
- Internal threats
- Natural events
- Natural disasters
- Vulnerability assessment
- Penetration (pen) testing

# Key Terms



- Posture assessment
- Business risk assessment
- Vendor assessment
- Process assessment

## Quick Review



- A vulnerability assessment can point out potential weaknesses in your organization
- Pen testing is used to examine the strength of your network security
- A risk posture is an overall look at security in the organization





# Episode 18.06

Episode title: **Points of Failure**

Objective: **3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution**

# Key Terms



- Critical assets
- High availability (HA)
- Virtual IP
- Redundancy
- Fault tolerance
- Clustering
- Load balancing

## Quick Review



- A single point of failure is one system that, if it fails, will bring down an entire process, workflow, or the whole organization
- Critical assets are the systems needed to maintain production
- Critical nodes are the devices needed to maintain the network
- The key to maintaining production on the network is to avoid a single point of failure



# Episode 18.07

Episode title: **Standard Business Documentation**

Objective: **3.2 Explain the purpose of organizational documents and policies**

# Key Terms



- Service Level Agreement (SLA)
- Memorandum of Understanding (MOU)
- Multi-Source Agreement (MSA)
- Statement of Work (SOW)

## Service Level Agreement (SLA)



- Between a customer and service provider
- Scope, quality, and terms of service to be provided
  - Definition of service provided
  - Equipment
  - Technical support

## Memorandum of Understanding (MOU)



- Defines an agreement between two parties
- Used where a legally binding contract is inappropriate
  - Definition of agreed duties
  - Time frame
  - ???????????

# City of Houston Hospital Patient Exchange Disaster MOU



- Cost
- Logistics



# Statement of Work (SOW)



- Legal contract between two parties (vendor and customer)
  - Defines services to be performed/supplied
  - Defines time frame/deliverables
  - Defines milestones/defines progress

## Quick Review



- Standard business documentation is common in networking
- Standards on the exam include SLA, MOU, MSA, and SOW
- These are real-world standards



# Episode 18.08

Episode title: **Incident Response and Forensics**

Objective: **4.1 Explain common security concepts**

# Key Terms



- Forensics
- First responder
- Secure the area
- Document the scene
- Collect evidence
- Chain of custody
- Forensics report
- Legal hold
- Electronic discovery (e-discovery)

## Quick Review



- The first responder is the person who must report an incident as soon as it happens
- If the first responder faces a serious threat, they must escalate it to the proper people
- The four-step process of forensics is secure the area, document the scene, collect evidence, and interface with authorities (submit forensics report)



# Episode 18.09

Episode title: **Disaster Recovery and Backups**

Objective: **3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution**

# Key Terms



- Backup plan assessment
- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Configuration data
- State data
- Mean time to repair (MTTR)
- Mean time to failure (MTTF)
- Mean time between failures (MTBF)

# Key Terms



- Snapshots
- Local backups
- Offsite backups
- Cloud backups



## Quick Review



- A single point of failure is one system that, if it fails, will bring down an entire process, workflow, or the whole organization
- Critical assets are the systems needed to maintain production
- Critical nodes are the devices needed to maintain the network
- The key to maintaining production on the network is to avoid a single point of failure



# Episode 18.10

Episode title: **Business Continuity**

Objective: **3.2 Explain the purpose of organizational documents and policies**  
**3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution**

# Key Terms



- Business continuity plan (BCP)
- Disaster recovery
- Business continuity
- Distance and location
- Internet requirements
- Housing and entertainment

# Key Terms



- Legal issues
- Annual exercises
- Failover
- Alternative processing sites
- Alternative business practices
- After action reports

## Quick Review



- Contingency planning (business continuity planning) attempts to mitigate incidents to preserve business functionality
- Understand the pros and cons of the offsite options available: cold site, warm site, hot site, cloud site
- Thorough planning and practice is what makes recovery plans successful when disasters occur



# Episode 18.11

Episode title: **Deployment Models**

Objective: **3.2 Explain the purpose of organizational documents and policies**  
**5.5 Given a scenario, troubleshoot general networking issues**

# Key Terms



- Bring your own device (BYOD)
- BYOD policy
- Acceptable use policy (AUP)
- Onboarding policy
- Offboarding policy
- Mobile Device Manager (MDM)
- BYOD challenges

## Key Terms



- Corporate-owned, business only (COBO)
- Corporate-owned, personally enabled (COPE)
- Choose your own device (CYOD)



## Quick Review



- A bring your own device (BYOD) policy enables employees to use their own device on the network
- The Mobile Device Manager (MDM) can manage mobile devices brought by employees
- The organization should establish which data is controlled by the user and which is controlled by the organization