# Instructor Materials
# Chapter 6: The Five Nines Concept

## Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

# Chapter 6:
# The Five Nines Concept

**Cybersecurity Essentials v1.1**

Cisco | Networking Academy®
Mind Wide Open™

# Chapter 6 - Sections & Objectives

## 6.1 High Availability

Explain the concept of high availability.

## 6.2 Measures to Improve Availability

Explain how high availability measures are used to improve availability.

## 6.3 Incident Response

Describe how an incident response plan improves high availability.

## 6.4 Disaster Recovery

Describe how disaster recovery planning plays an important role in implementing high availability.

# 2.1 High Availability

Cisco | Networking Academy®
Mind Wide Open™

# The Five Nines

## What is Five Nine?

- Five nines mean that systems and services are available 99.999% of the time. It also means that both planned and unplanned downtime is less than 5.26 minutes per year. High availability refers to a system or component that is continuously operational for a given length of time. To help ensure high availability:
- Eliminate single points of failure
- Design for reliability
- Detect failures as they occur

| Availability | Downtime per Year |
|---|---|
| 99% | 87 hours 36 mins |
| 99.5% | 43 hours 48 mins |
| 99.95% | 4 hours 23 mins |
| 99.99% | 53 mins |
| 99.999% | 5 mins |

# The Five Nines (Cont.)

## Environments That Require Five Nines

Although the cost of sustaining high availability may be too costly for some industries, several environments require five nines.

- The finance industry needs to main high availability for continuous trading, compliance, and customer trust.
- Healthcare facilities require high availability to provide around-the-clock care for patients.
- The public safety industry includes agencies that provide security and services to a community, state, or nation.
- The retail industry depends on efficient supply chains and the delivery of products to customers. Disruption can be devastating, especially during peak demand times such as holidays.

Finance Industry


Health Care Facilities


Public Safety

# The Five Nines (Cont.)

## Threats to Availability

There are many different types of threats to high availability, the threats can range from failure of a mission-critical application to severe storm such as a hurricane or tornado. Threats can also include catastrophic event such as a terrorist attack, building bombing, or building fires.

## Designing a High Availability System

High availability incorporates three major principles to achieve the goal of uninterrupted access to data and services:

- Elimination or reduction of single-points of failure
- System Resiliency
- Fault Tolerance

Finance Industry


Health Care Facilities


Public Safety

# 6.2 Measures to Improve Availability

Cisco | Networking Academy®
Mind Wide Open™

# Asset Management

An organization needs to know what hardware and software assets they have in order to protect them. Asset management includes a complete inventory of hardware and software. This means that the organization needs to know all of components that can be subject to security risks, including:

- Every hardware system
- Every operating system
- Every hardware network device
- Every network device operating system
- Every software application
- All firmware
- All language runtime environments
- All individual libraries

Many organizations may choose an automated solution to keep track of assets.

# Asset Management (Cont.)

- **Asset classification -** assigns all resources of an organization into a group based on common characteristics. An organization should apply an asset classification system to documents, data records, data files, and disks.
- **Asset Standardization -** as part of an IT asset management system, an organization specifies the acceptable IT assets that meet its objectives
- **Threat Identification -** The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of common vulnerabilities and exposure (CVE). The CVE identification contains a standard identifier number with a brief description, and references to related vulnerability reports and advisories.
- **Risk Analysis -** is the process of analyzing the dangers posed by natural and human-caused events to the assets of an organization. A user performs an asset identification to help determine which assets to protect.
- **Mitigation -** Mitigation involves reducing the severity of the loss or the likelihood of the loss from occurring. Many technical controls mitigate risk including authentication systems, file permissions, and firewalls.

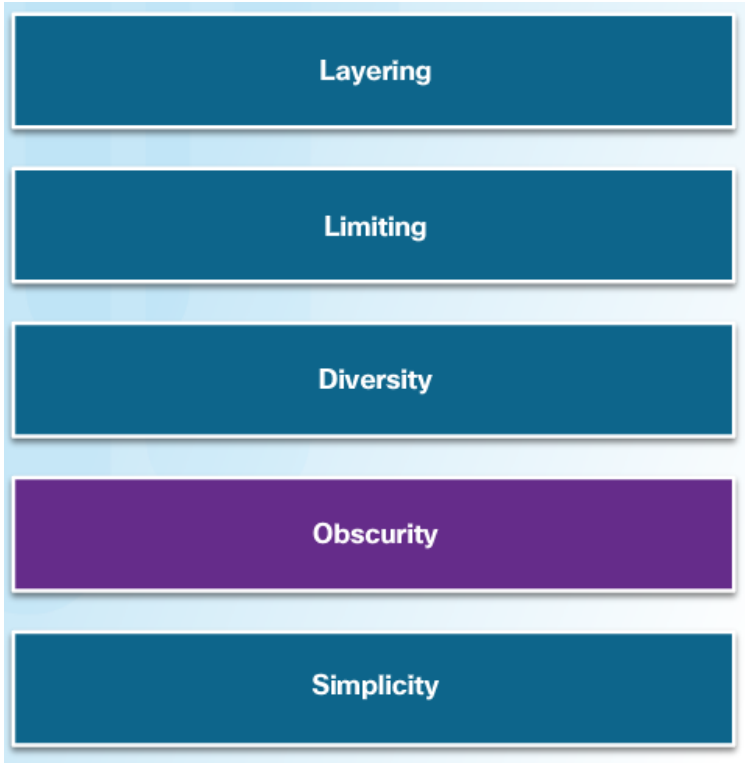
# Defense in Depth

Defense in depth will not provide an impenetrable cyber shield, but it will help an organization minimize risk by keeping it one step ahead of cyber criminals. To make sure data and information remains available, an organization must create different layers of protection:

- A **layered** approach provides the most comprehensive protection. If cyber criminals penetrate one layer, they still have to contend with several more layers with each layer being more complicated than the previous one. Layering is creating a barrier of multiple defenses that coordinate together to prevent attacks.
- **Limiting** access to data and information reduces the possibility of a threat. An organization should restrict access so that users only have the level of access required to do their job.

# Defense in Depth

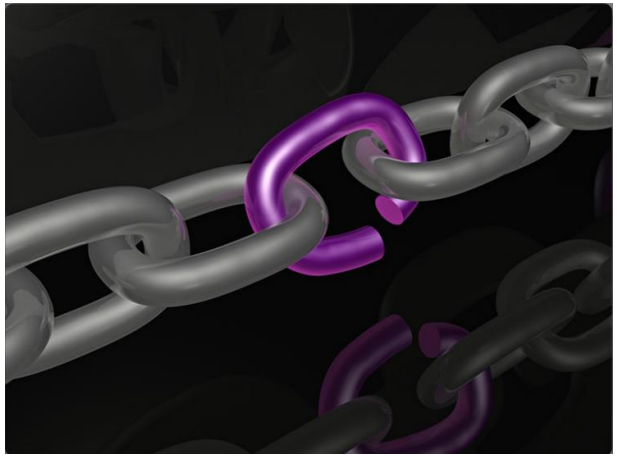
- **Diversity** refers to changing the controls and procedures at different layers. Breaching one layer of security does not compromise the whole system. An organization may use different encryption algorithms or authentication systems to protect data in different states.
- **Obscuring** information can also protect data and information. An organization should not reveal any information that cyber criminals can use to figure out what version of the operating system a server is running or the type of equipment it uses.
- Complexity does not necessarily guarantee security. If the process or technology are too complex, misconfigurations or failure to comply can result. **Simplicity** can actually improve availability.



# Redundancy

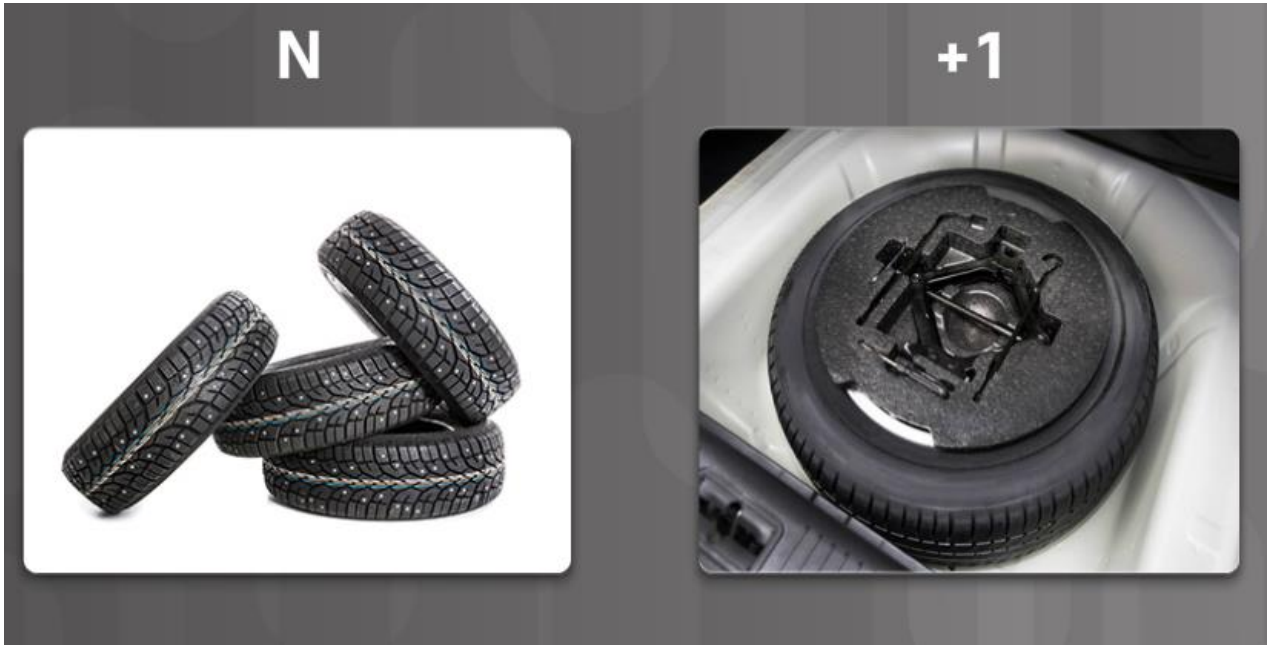
A **single point of failure** must be identified and addressed. A single point of failure can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility.

- Single points of failure are the weak links in the chain that can cause disruption of the organization's operations.
- Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on a single element.
- The organization can also build redundant components into the critical operation to take over the process should one of these points fail.



# Redundancy (Cont.)

- **N+1 redundancy** ensures system availability in the event of a component failure.
- Components (N) need to have at least one backup component (+1).
- For example, a car has four tires (N) and a spare tire in the trunk in case of a flat (+1).



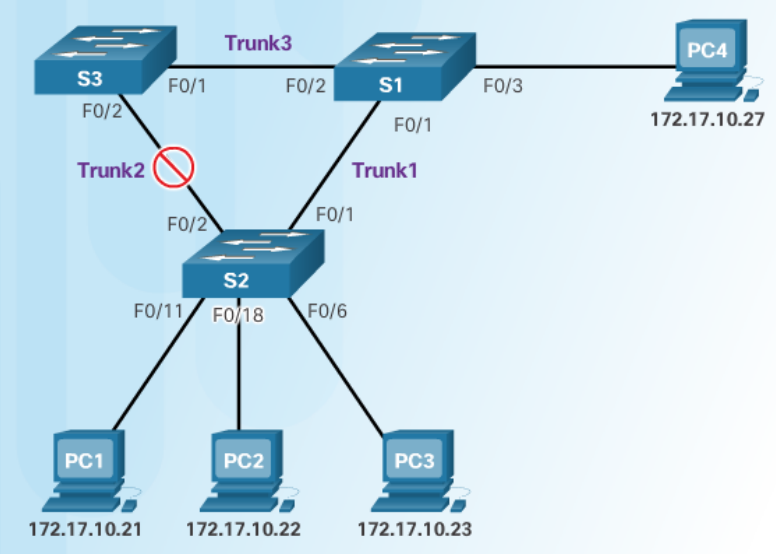
# Redundancy (Cont.)

- A **redundant array of independent disks (RAID)** combines multiple physical hard drives into a single logical unit to provide data redundancy and improve performance.
- RAID takes data that is normally stored on a single disk and spreads it out among several drives. If any single disk is lost, the user can recover data from the other disks where the data also resides.
- RAID can also increase the speed of data recovery.
- Using multiple drives makes retrieving requested data faster, instead of relying on just one disk to do the work.
- A RAID solution can be either hardware-based or software-based. The following terms describe how RAID stores data on the various disks:
  - **Parity** - Detects data errors.
  - **Striping** - Writes data across multiple drives.
  - **Mirroring** - Stores duplicate data on a second drive.

# Redundancy (Cont.)

**Spanning Tree** is a network protocol that provides for redundancy:

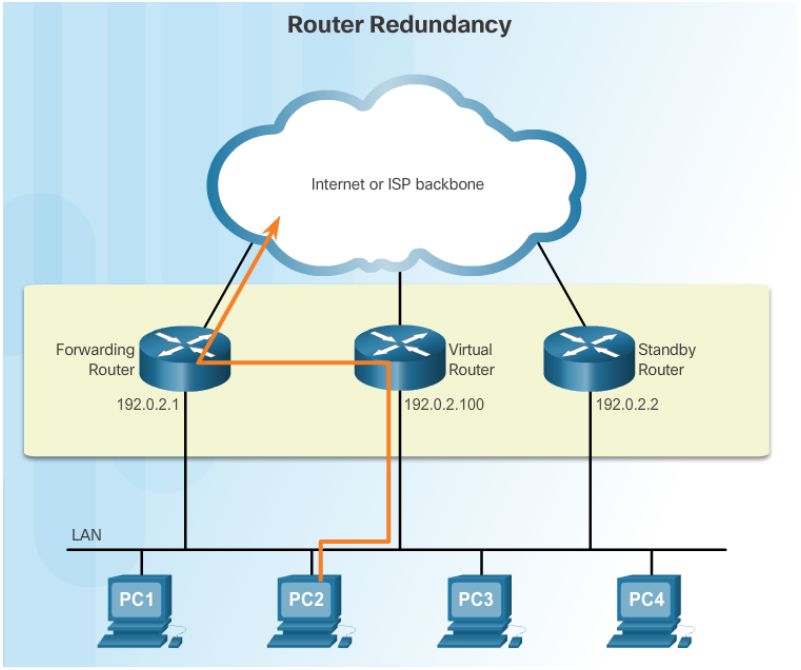
- The basic function of STP is to prevent loops on a network when switches interconnect via multiple paths.
- STP ensures that redundant physical links are loop-free. It ensures that there is only one logical path between all destinations on the network.
- STP intentionally blocks redundant paths that could cause a loop.



# Redundancy (Cont.)

The default gateway is typically the router that provides devices access to the rest of the network or to the Internet. If there is only one router serving as the default gateway, it is a single point of failure. Router redundancy involves:

- Choosing to install an additional standby router.
- The ability of a network to dynamically recover from the failure of a router acting as a default gateway is known as first-hop redundancy.



# Redundancy (Cont.)

**Router Redundancy Options -** options available for router redundancy include:

- **Hot Standby Router Protocol (HSRP)** - HSRP provides high network availability by providing first-hop routing redundancy.
- **Virtual Router Redundancy Protocol (VRRP)** - A VRRP router runs the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, the elected router is the virtual router master, and the other routers act as backups, in case the virtual router master fails.
- **Gateway Load Balancing Protocol (GLBP)** - GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.

# Redundancy (Cont.)

**Location Redundancy -** An organization may need to consider location redundancy depending on its needs. The following outlines three forms of location redundancy:

- **Synchronous -** Synchronizes both locations in real time, requires high bandwidth and locations must be close together to reduce latency.
- **Asynchronous Replication -** Not synchronized in real time but close to it, requires less bandwidth and sites can be further apart because latency is less of an issue.
- **Point-in-time-Replicatio**n - Updates the backup data location periodically and is the most bandwidth conservative option because it does not require a constant connection.

# System Resilience

Resiliency defines the methods and configurations used to make a system or network tolerant of failure. Routing protocols provide resiliency. Resilient design is more than just adding redundancy. Resiliency is critical to understand the business needs of the organization, and then incorporate redundancy to create a resilient network.

# 6.3 Incident Response Phases

Cisco | Networking Academy®
Mind Wide Open™

# Incident Response Phases

Incident response defines the procedures that an organization follows after an event occurs outside the normal range. When an incident occurs, the organization must know how to respond. Organizations needs to develop an incident response plan and put together a Computer Security Incident Response Team (CSIRT) to manage the response. Incident response has consist of four phases:

1. **Preparation** – planning for potential incidents
2. **Detection and Analysis** - discovering the incident
3. **Containment and Eradication, and Recovery** - efforts to immediately contain or eradicate the threat and begin recovery efforts
4. **Post-Incident Follow-Up** – investigate the cause of the incident and ask questions to better understand the nature of the threat

# Incident Response Technologies

There are many technologies that are used to implement an incident response:

- **Network Admission Control (NAC)** - allows network access for authorized users with compliant systems. A compliant system meets all of the policy requirements of the organization.
- **Intrusion Detection Systems (IDSs)** - monitor the traffic on a network. IDS systems are passive.
- **Intrusion Prevention Systems** - operates in inline mode. It can detect and immediately address a network problem.
- **NetFlow and IPFIX** - NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. The Internet Engineering Task Force (IETF) used Cisco's NetFlow Version 9 as the basis for IP Flow Information Export (IPFIX).
- **Advanced Threat Intelligence** - can help organizations detect attacks during one of the stages of the cyberattack (and sometimes before with the right information).

# 6.4 Disaster Recovery

Cisco | Networking Academy®
Mind Wide Open™

# Disaster Recovery Planning

**Types of Disasters** - It is critical to keep an organization functioning when a disaster occurs. A disaster includes any natural or human-caused event that damages assets or property and impairs the ability for the organization to continue operating.

- **Natural Disasters -** geological disasters (earthquakes, landslides, volcanoes, and tsunamis), meteorological disasters (hurricanes, tornadoes, snow storms, lightning, and hail), health disasters (widespread illnesses, quarantines, and pandemics) and miscellaneous disasters (fires, floods, solar storms, and avalanches).
- **Human-caused Disasters -** Human-caused disasters - labor events (strikes, walkouts, and slowdowns), social-political events (vandalism, blockades, protests, sabotage, terrorism, and war), materials events (hazardous spills and fires) and utilities disruptions (power failures, communication outages, fuel shortages, and radioactive fallout)

# Business Continuity Planning

**Need for Business Continuity -** Business continuity is one of the most important concepts in computer security. Even though companies do whatever they can to prevent disasters and loss of data, it is impossible to predict every scenario. It is important for companies to have plans in place that ensure business continuity regardless of what may occur.

**Business Continuity Considerations -** Business continuity controls are more than just backing up data and providing redundant hardware. Business Continuity Considerations should include:

- Documenting configurations
- Establishing alternate communications channels
- Providing power
- Identifying all dependencies for applications and processes
- Understanding how to carry out automated tasks manually

# Business Continuity Planning

## Business Continuity Best Practices

1. Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Identify critical systems and processes, and prioritize them based on necessity.
3. Identify vulnerabilities, threats, and calculate risks.
4. Identify and implement controls and countermeasures to reduce risk.
5. Devise methods to bring back critical systems quickly.
6. Write procedures to keep the organization functioning when in a chaotic state.
7. Test the plan.
8. Update the plan regularly.

# 6.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

# Summary

- This chapter began by explaining the concept of five nines, a high availability standard that allows for 5.26 minutes of downtime per year.
- The chapter discussed the various approaches that organizations take to ensure system availability.
- Solid system design includes accommodating measures that provide redundancy and resiliency so that an organization can recover quickly and continue operation.
- The chapter also discussed how an organization responds to an incident by establishing procedures that it follows after an event occurs.
- The chapter concluded with a discussion of disaster recovery and business continuity planning.