
# High Availability

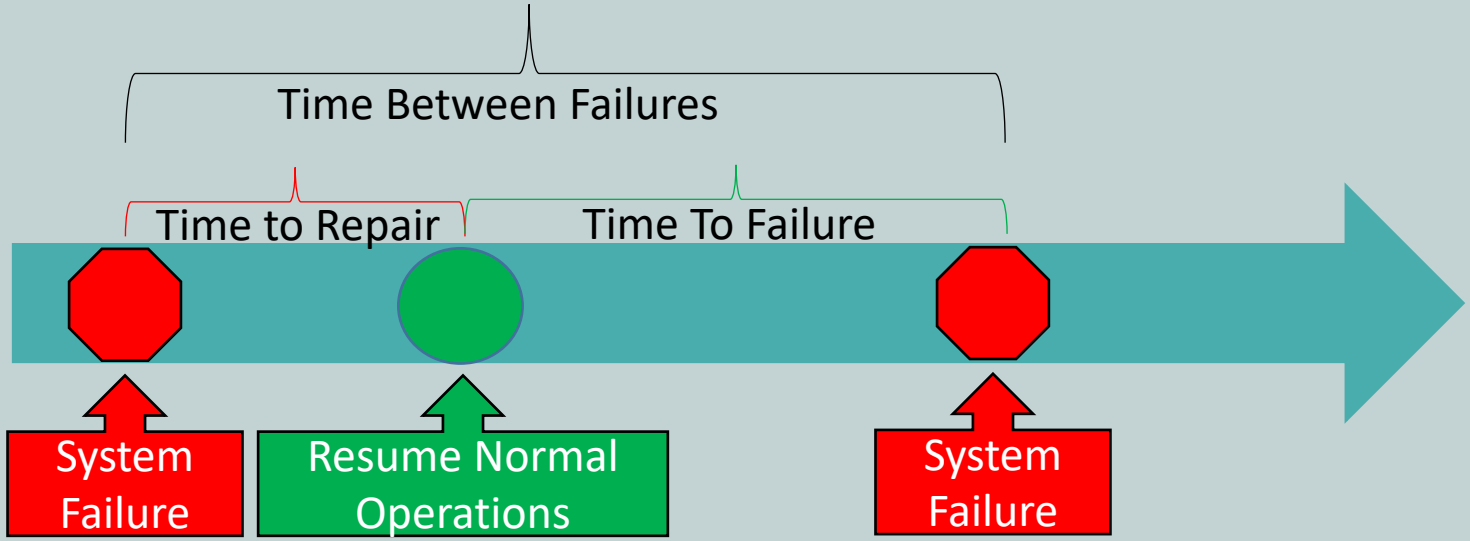
## CompTIA Network+ (N10-007)

# High Availability

- Availability is measured by uptime
- Five nines of availability (99.999%)
- Maximum of 5 minutes of downtime per year
- Availability
  - Concerned with being up and operational
- Reliability
  - Concerned with not dropping packets

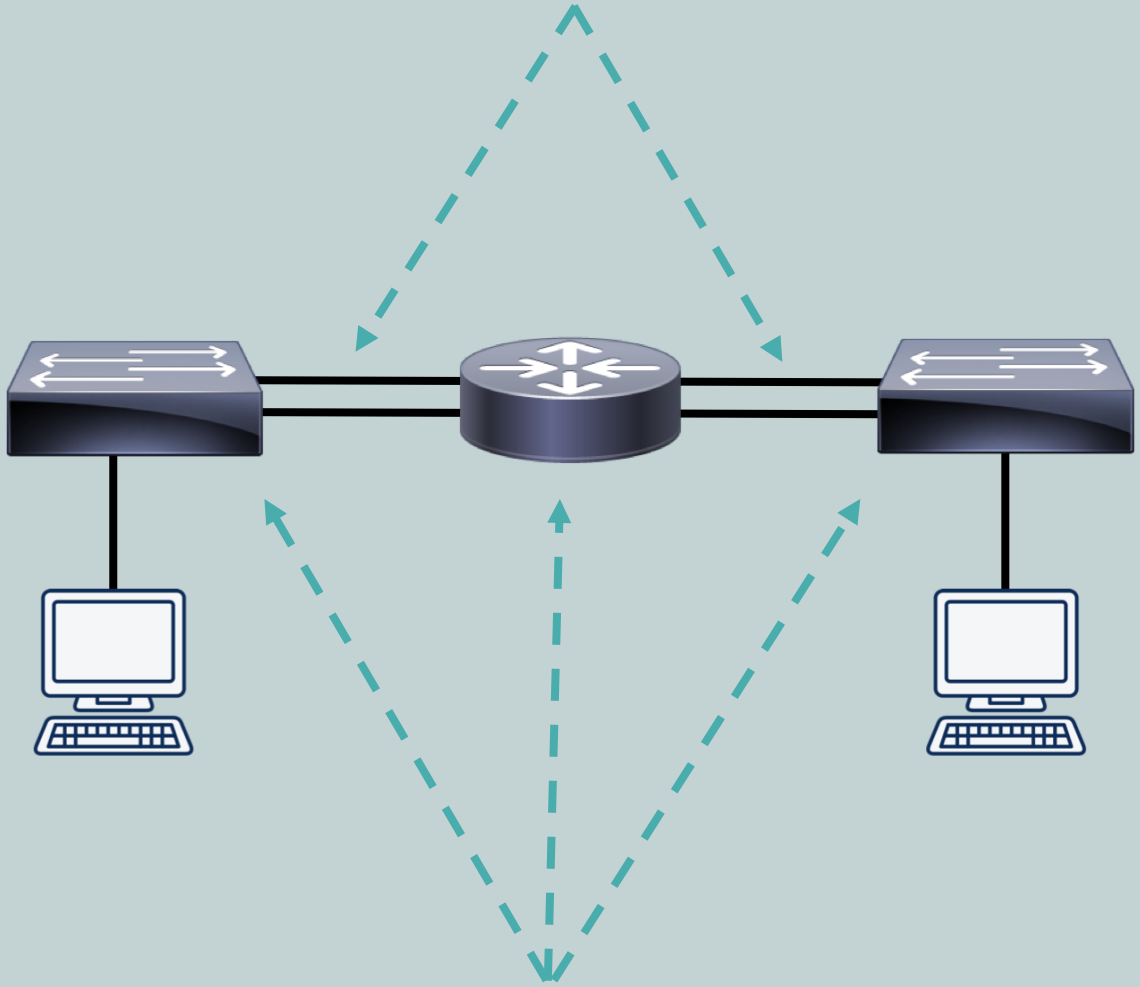
# High Availability

- Mean Time To Repair (MTTR)
  - Measures the average time it takes to repair a network device when it breaks
- Mean Time Between Failures (MTBF)
  - Measures the average time between failures of a device



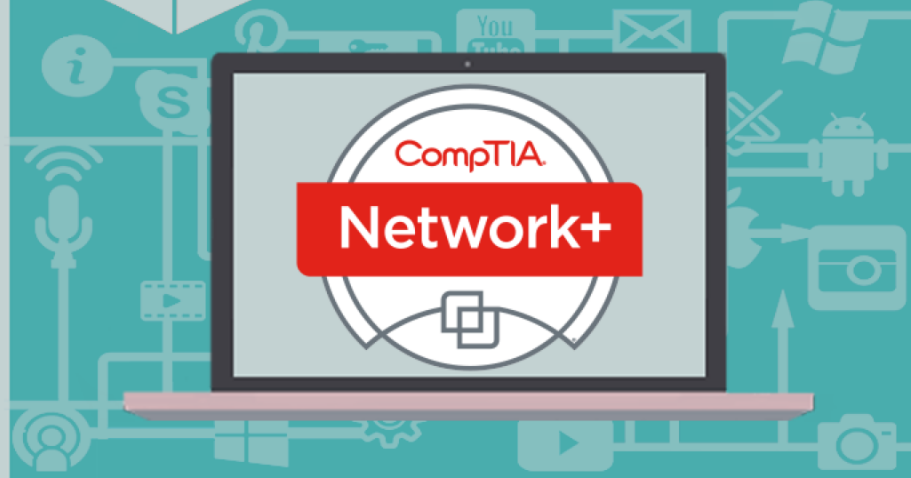
# Redundant Network with Single Points of Failure

Link Redundancy (Multiple connections between devices)



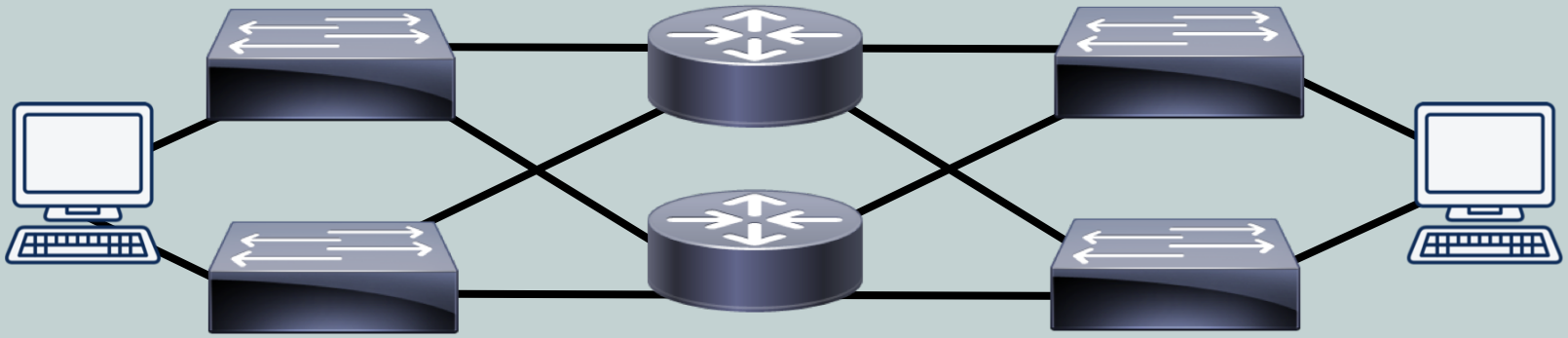
Internal Hardware Redundancy
(Power supplies and NICs)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



# Redundant Network with Now Single Points of Failure

Link Redundancy (Multiple connections between devices)



Redundancy of Components
(Switches and Routers)

# Hardware Redundancy

- Takes many forms

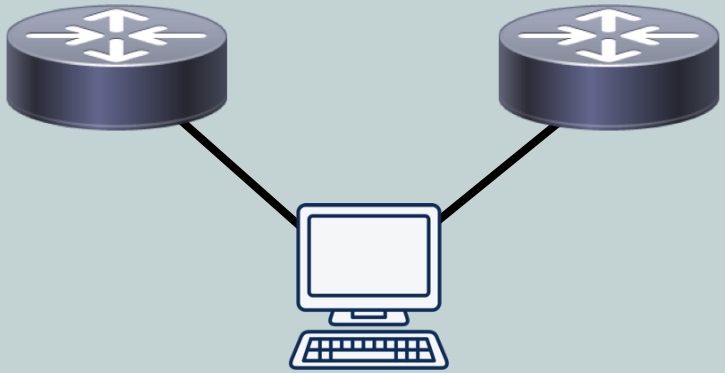
- Devices with two network interface cards (NICs), hard drives,  or internal power supplies

- Often found in strategic network devices
  - Routers, Switches, Firewalls, and Servers
  - Not often found in clients due to costs and administrative overhead involved in management

# Hardware Redundancy

- Active-Active
  - Multiple NICs are active at the same time
  - NICs have their own MAC address
  - Makes troubleshooting more complex

- Active-Standby
  - One NIC is active at a time
  - Client appears to have a single MAC address



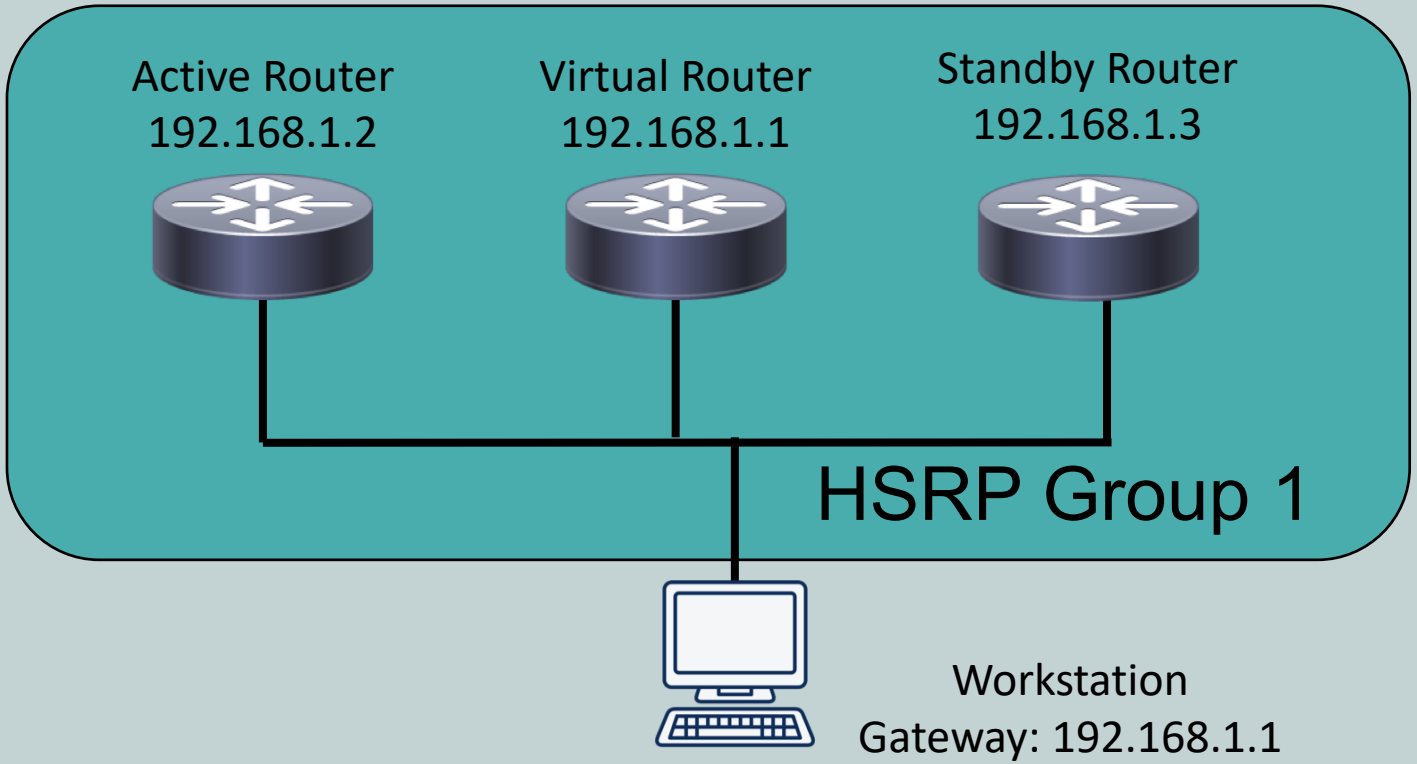
# Layer 3 Redundancy

- Clients are configured with a default gateway (router)
  - If the default gateway goes down, they cannot leave the subnet
  - Layer 3 Redundancy occurs with virtual gateways

- Layer 3 Redundancy Protocols
  - Hot Standby Router Protocol
  - Common Address Redundancy Protocol
  - Virtual Router Redundancy Protocol
  - Gateway Load Balancing Protocol
  - Link Aggregation Control Protocol

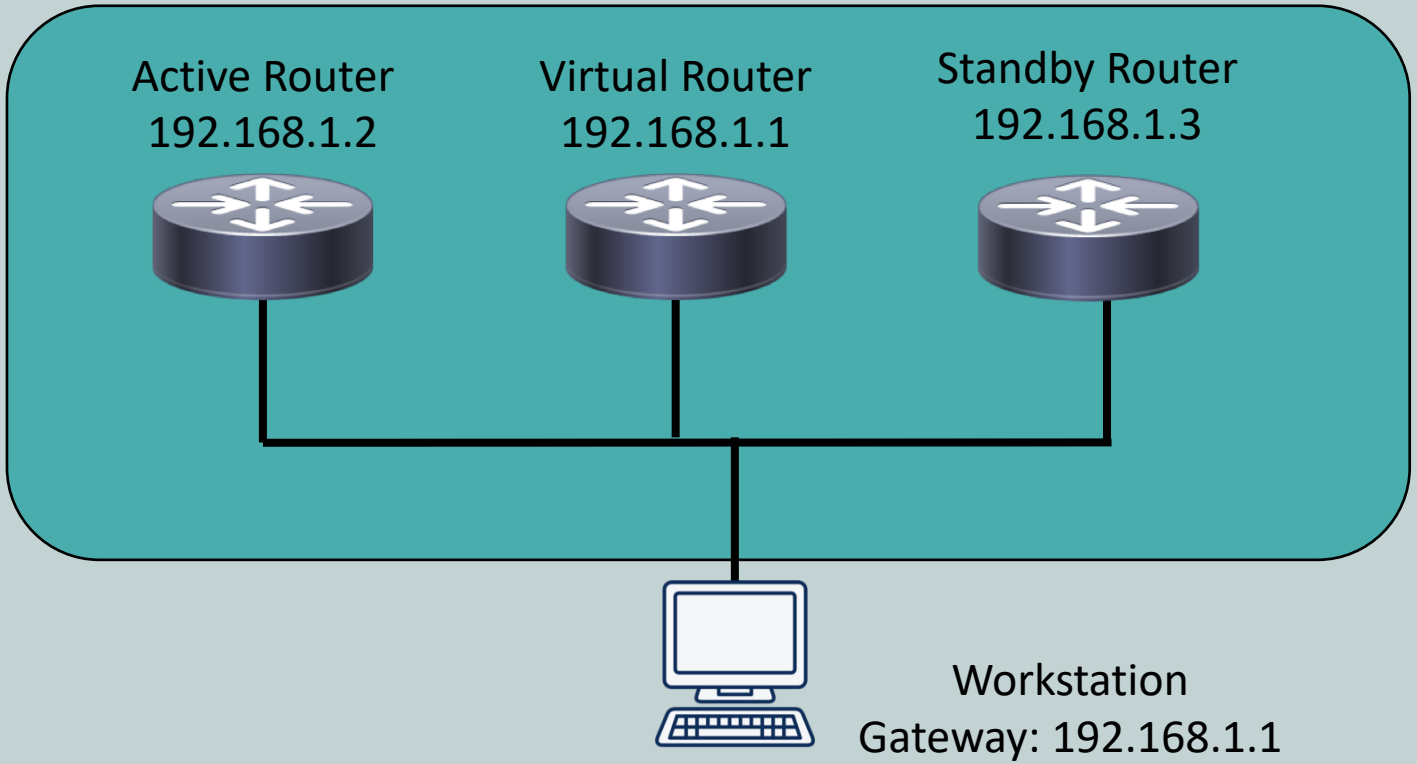
# Hot Standby Router Protocol (HSRP)

- Proprietary first-hop redundancy by Cisco
- Allows for active router and standby router
- Creates virtual router as the default gateway



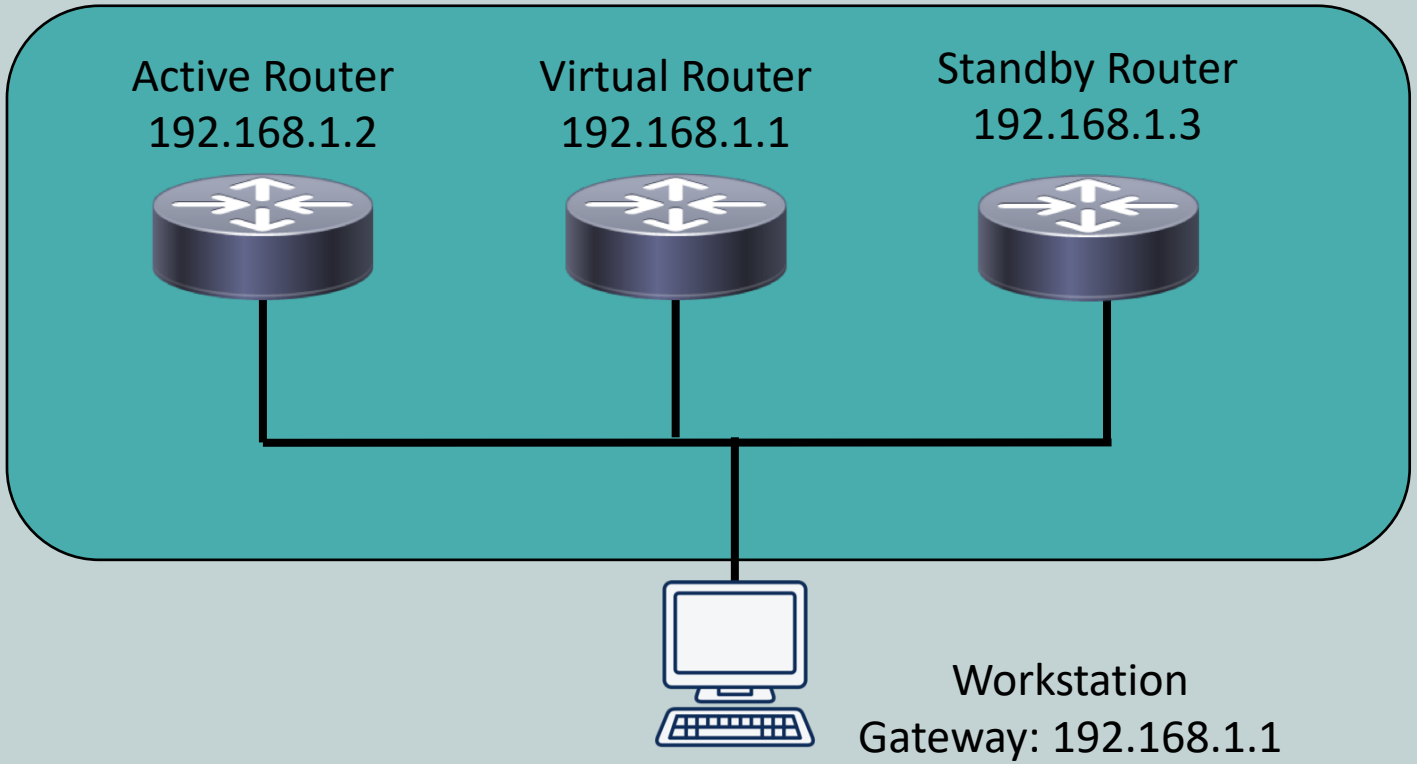
# Common Address Redundancy Protocol (CARP)

- Open-standard variant of HSRP
- Allows for active router and standby router
- Creates virtual router as the default gateway



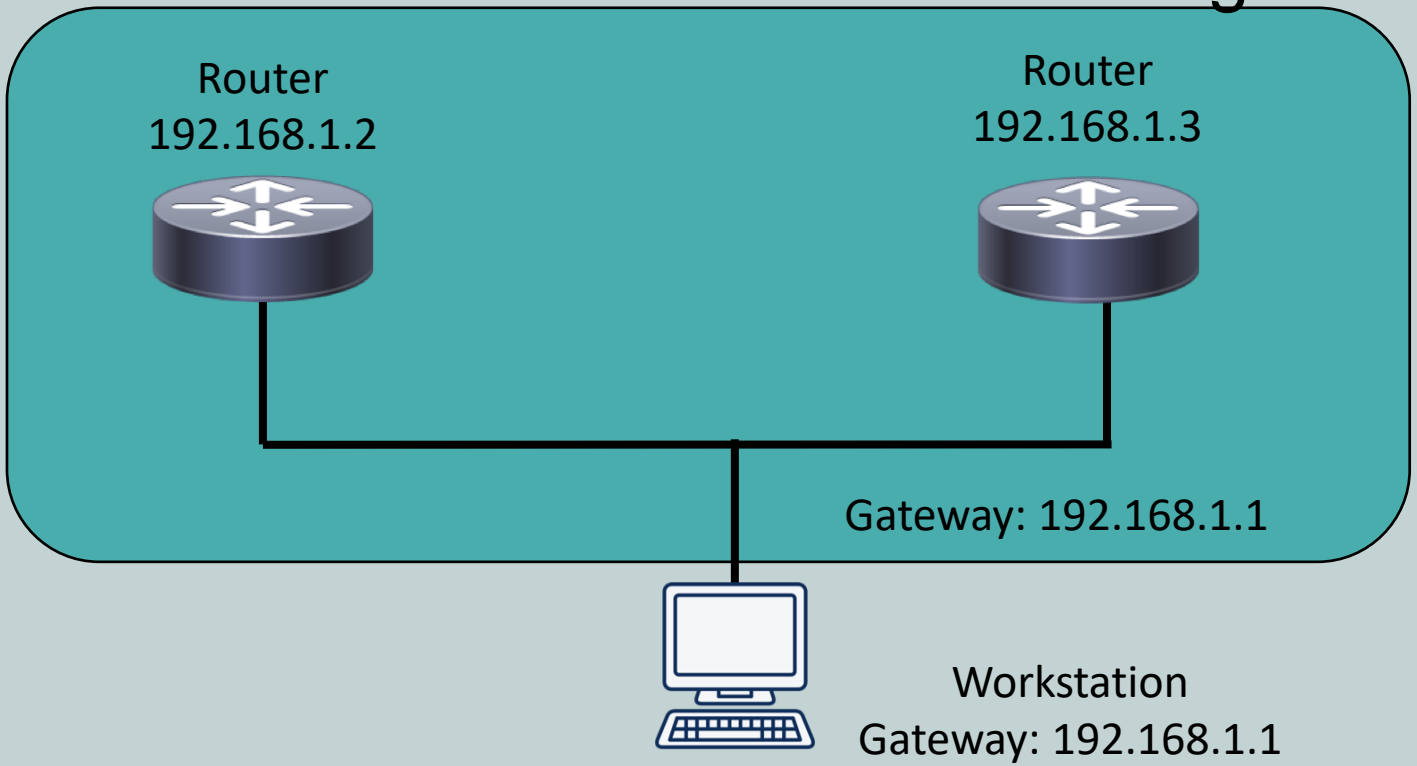
# Virtual Router Redundancy Protocol (VRRP)

- IETP open-standard variant of HSRP
- Allows for active router and standby router
- Creates virtual router as the default gateway



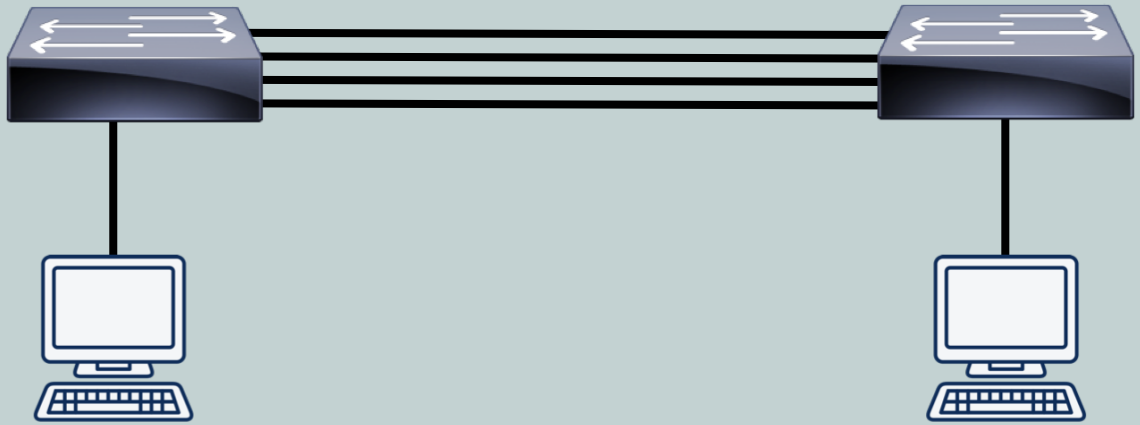
# Gateway Load Balancing Protocol (GLBP)

- Proprietary first-hop redundancy by Cisco
- Focuses on load balancing over redundancy
- Allows for active router and standby router
- Creates virtual router as the default gateway



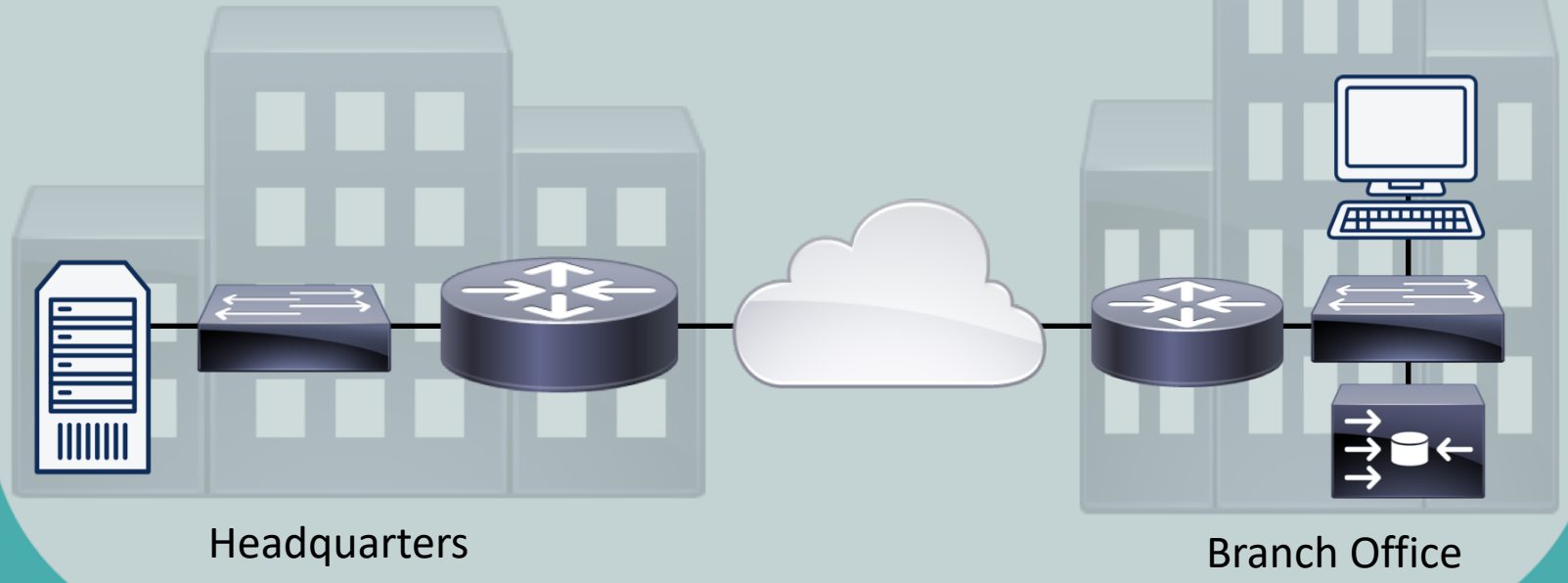
# Link Aggregation Control Protocol (LACP)

- Achieves redundancy by having multiple links between devices
- Load balancing occurs over multiple links
- Multiple links appear as single logical link



# Content Engine

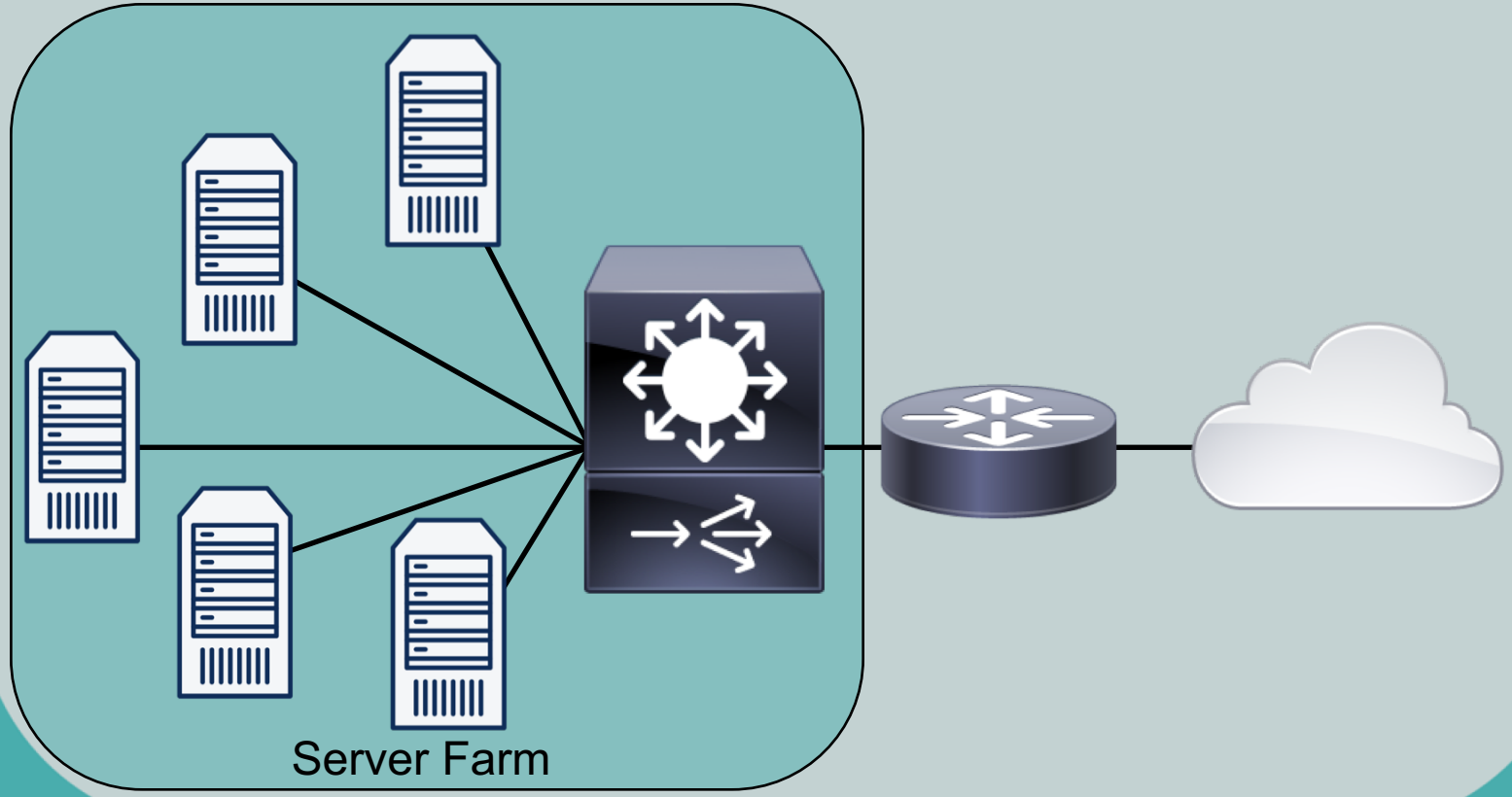
- Dedicated appliances that perform the caching functions of a proxy server
- Are more efficient than a proxy server
- Also called Caching Engines



# Content Switches

- Distributes incoming requests across the various servers in the server farm

- Also known as Load Balancers




# Designing Redundant Networks

## CompTIA Network+ (N10-007)

# Design Considerations

- Where will redundancy be used?
  - Module (or Parts) Redundancy
  - Chassis Redundancy
- What software redundancy features are appropriate?
- What protocol characteristics affect design requirements?

# Design Considerations

- What redundancy features should be used to provide power to an infrastructure device?

- What redundancy features should be used to maintain environmental conditions?

# Best Practices

- Examine the technical goals
- Identify the budget to fund high availability features
- Categorize business applications into profiles
  - Each requires a certain level of availability

# Best Practices

- Establish performance standards for high-availability solutions
  - Performance standards will drive how success if measured
- Define how to manage and measure the high-availability solution
  - Metrics help quantify success to decision makers

# Remember…

- Existing networks can be retrofitted, but it reduces the cost by integrating high availability practices and technologies into your initial designs


# Recovery

## CompTIA Network+ (N10-007)

# Recovery Sites

- In addition to hardware and software redundancy, sometimes you need site redundancy:
  - Cold Sites
  - Warm Sites
  - Hot Sites

# Cold Sites

- Building is available, but you may not have any hardware or software in place or configured
- You need to buy resources (or ship them in), and then configure/restore the network
- Recovery is possible, but slow and time consuming

# Warm Sites

- Building and equipment is available
- Software may not be installed and latest data is not available
- Recovery is fairly quick, but not everything from original site is available for employees

# Hot Sites

- Building, equipment, and data is available
- Software and hardware is configured
- Basically, people can just walk into the new facility and get to work
- Downtime is minimal with nearly identical service levels maintained

# Backup and Recovery

- Full
  - Complete backup is the safest and most comprehensive; Time consuming and costly
- Incremental
  - Backup only data changed since last backup
- Differential
  - Only backups data since the last full backup
- Snapshots
  - Read-only copy of data frozen in time (VMs)


# Quality of Service (QoS)

## CompTIA Network+ (N10-007)

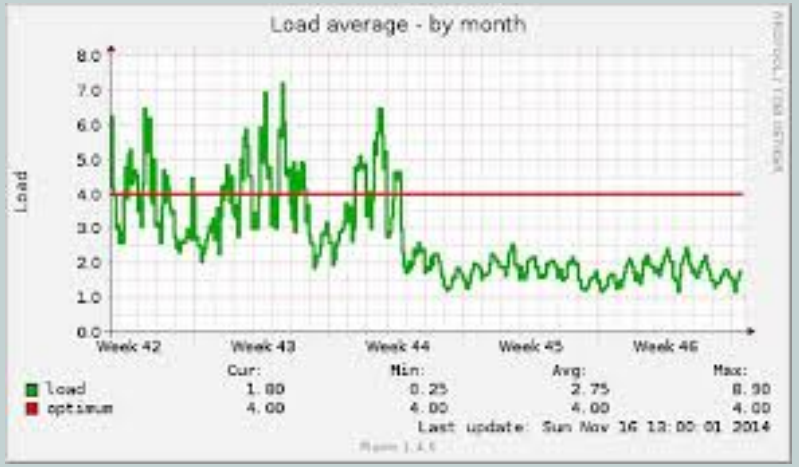
# Need for Quality of Service (QoS)

- Networks carry data, voice, and video content
- Convergence of media on the network requires high availability to ensure proper delivery
- Optimizing the network to efficiently utilize the bandwidth to deliver useful solutions to network users is crucial to success and cost savings


# Quality of Service (QoS)

- Enables strategic optimization of network performance for different types of traffic
  - Identifies types of traffic needing priority
  - Determines how much bandwidth required
  - Efficiently uses WAN link's bandwidth
  - Identifies types of traffic to drop during network congestion

- For example:
  - Voice (VoIP) and Video should have higher priority levels (less latency)



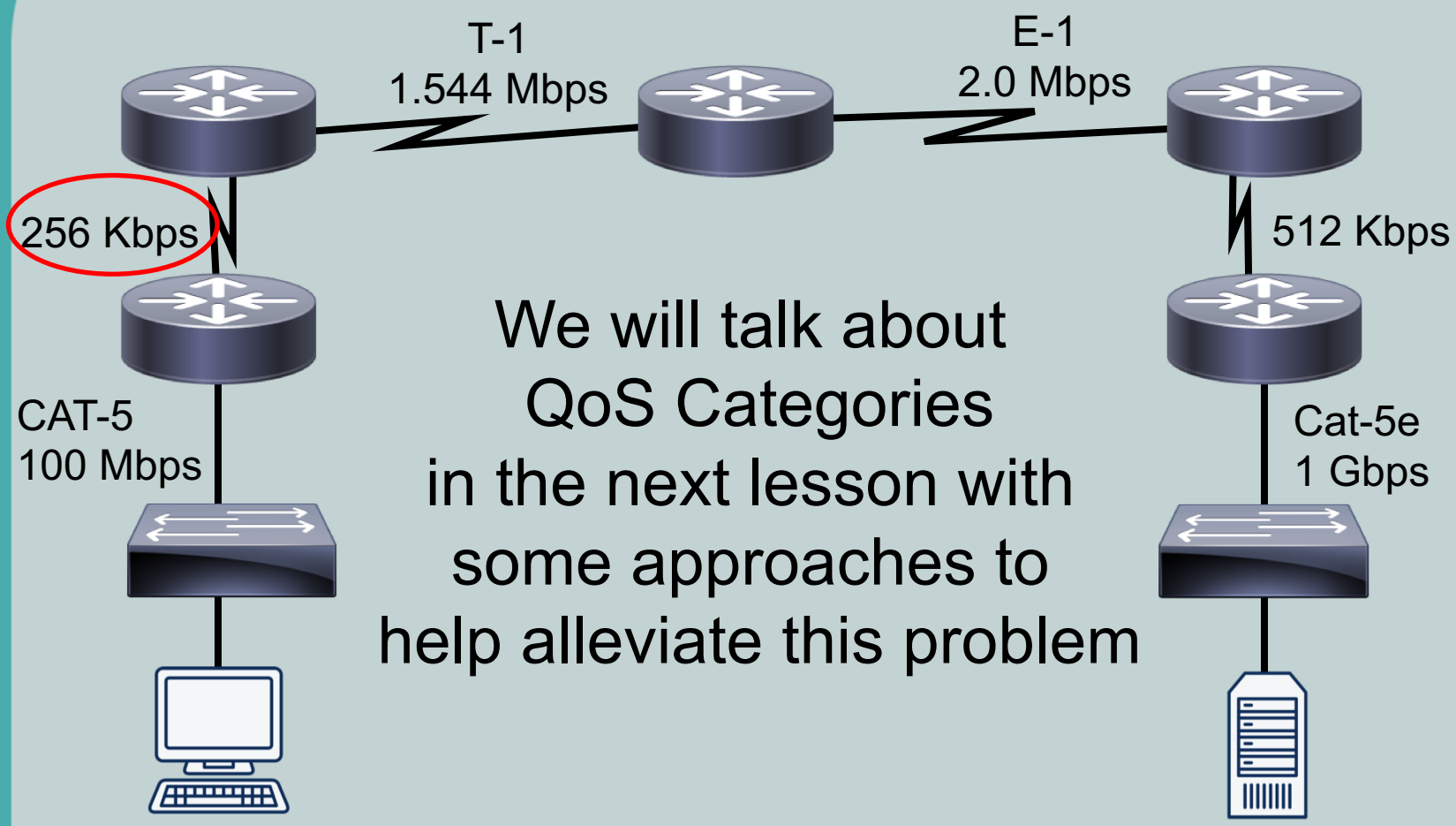

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

# Categories of QoS

- Delay
  - Time a packet travels from source to destination
  - Measured in milliseconds (ms)
- Jitter
  - Uneven arrival of packets
  - Especially harmful in VoIP
- Drops
  - Occurs during link congestion
  - Router's interface queue overflows and causes packet loss

# "Effective" Bandwidth



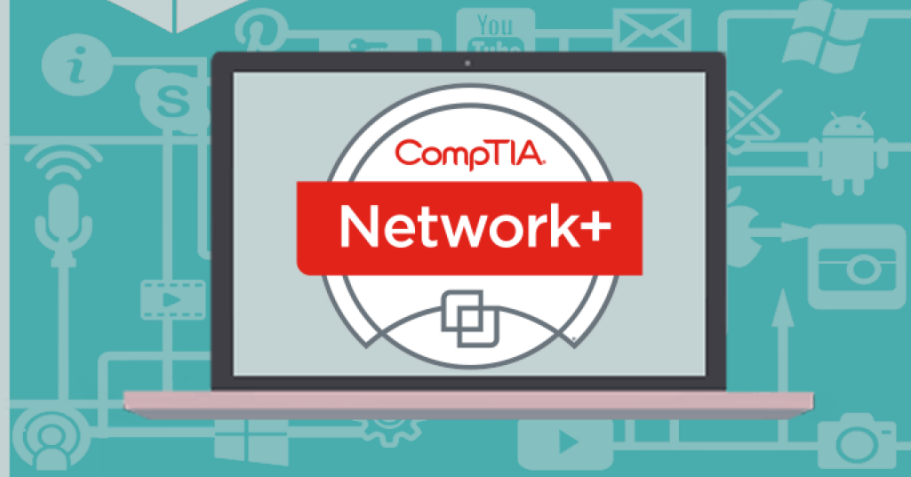

We will talk about QoS Categories in the next lesson with some approaches to help alleviate this problem

***So, how do we increase the available bandwidth, then?***

*Like water flowing through pipes of various sizes,*

*the flow rate is limited to the smallest pipe*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE




# QoS Categorization

## CompTIA Network+ (N10-007)

# Purpose of QoS

- To categorize traffic, apply a policy to those traffic categories, and prioritize them in accordance with a QoS policy

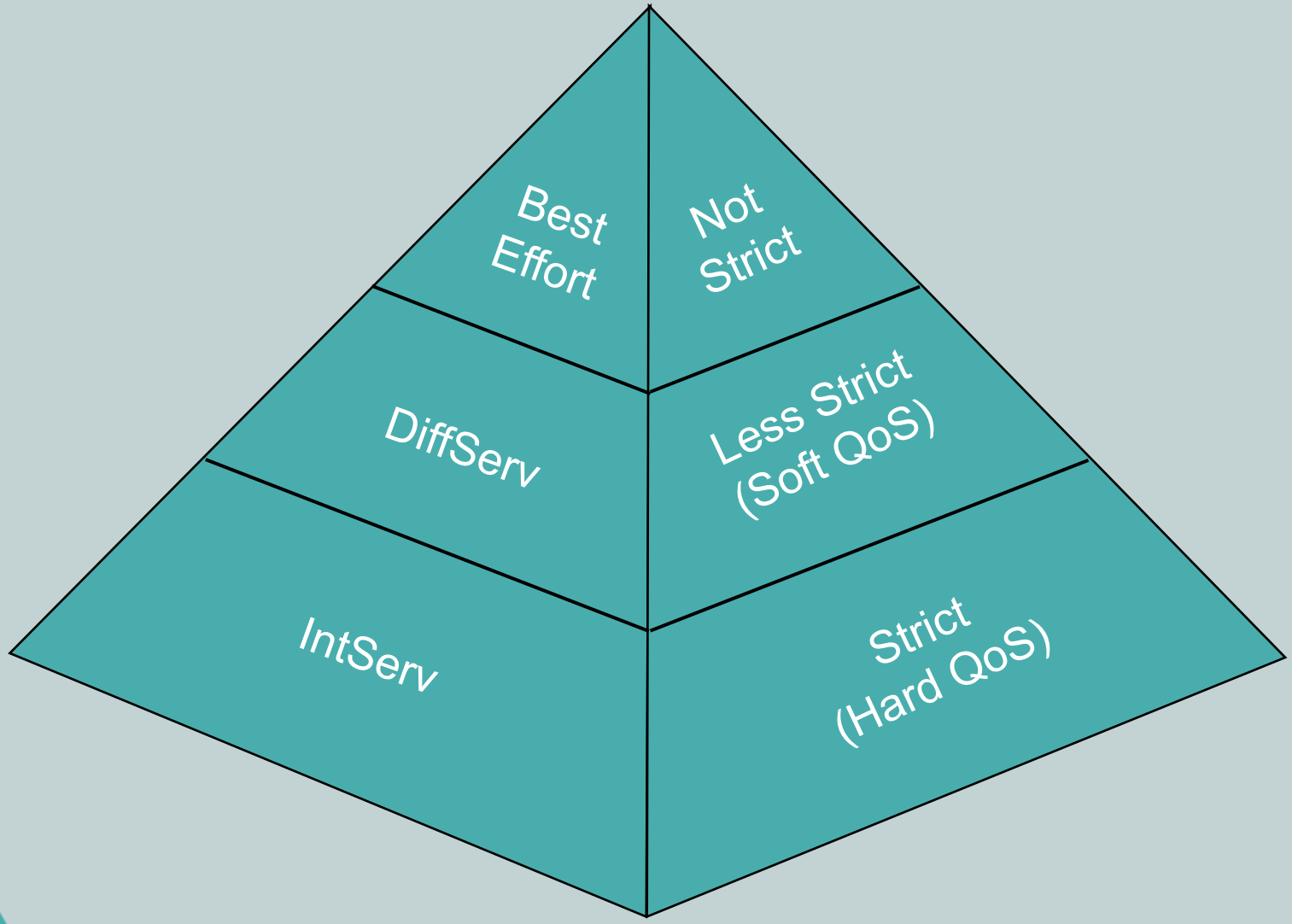
# Categorization of Traffic

- Determine network performance requirements for various traffic types (Voice, Video, Data)
- Categorize traffic into specific categories:
  - Low delay
    - Voice
    - Streaming Video
  - Low priority
    - Web browsing
    - Non-mission critical data
- Document your QoS policy and make it available to your users

# Ways of Categorizing Traffic

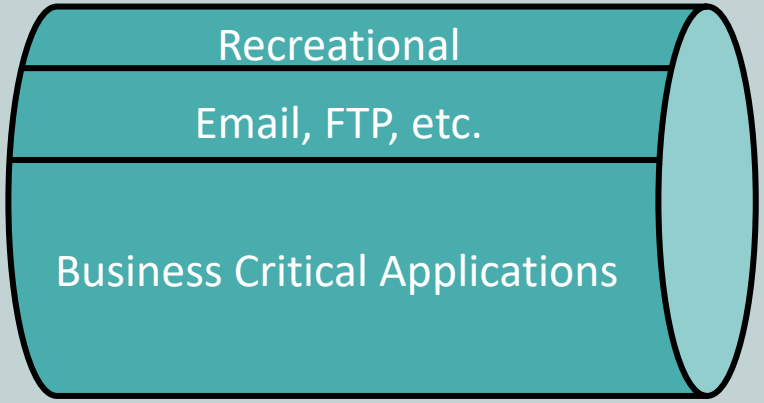
- Best Effort
  - Does not truly provide QoS to that traffic
  - No reordering of packets
  - Uses FIFO (first in, first out) queuing
- Integrated Services (IntServ or Hard QoS)
  - Makes strict bandwidth reservations
  - Reserves bandwidth by signaling devices
- Differentiated Services (DiffServ or Soft QoS)
  - Differentiates between multiple traffic flows
  - Packets are “marked”
  - Routers and switches make decisions based on those markings

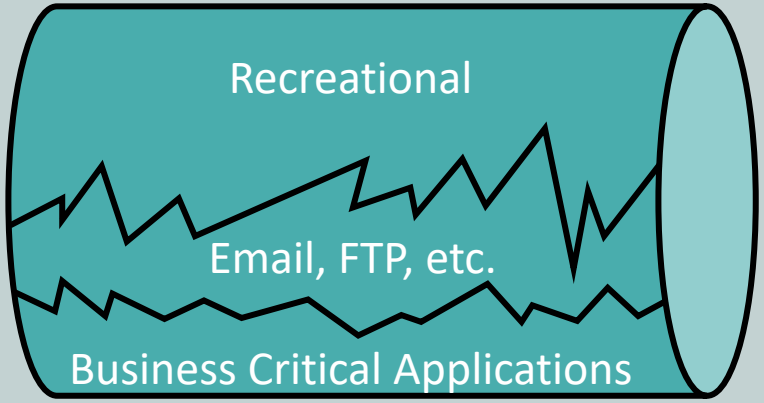
# Ways of Categorizing Traffic



# Methods of Categorizing Traffic

- Classification
- Marking
- Congestion management
- Congestion avoidance
- Policing and shaping
- Link efficiency



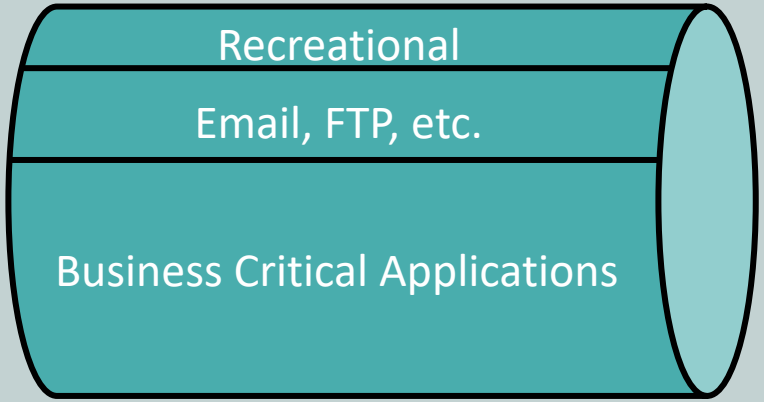

(We will cover these in the next lecture in depth)

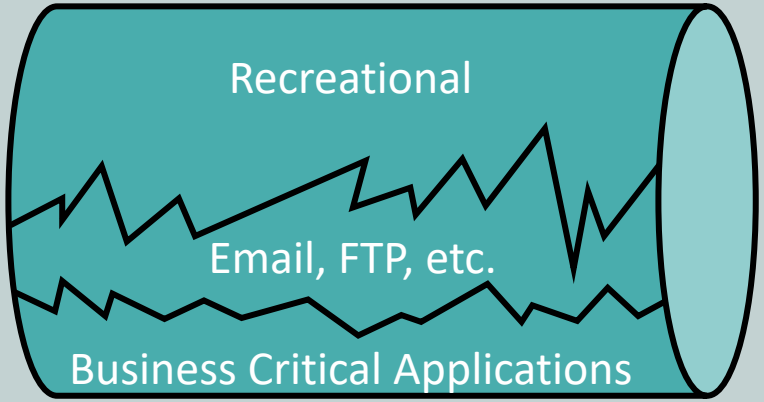

# QoS Mechanisms

## CompTIA Network+ (N10-007)

# Ways of Categorizing Traffic

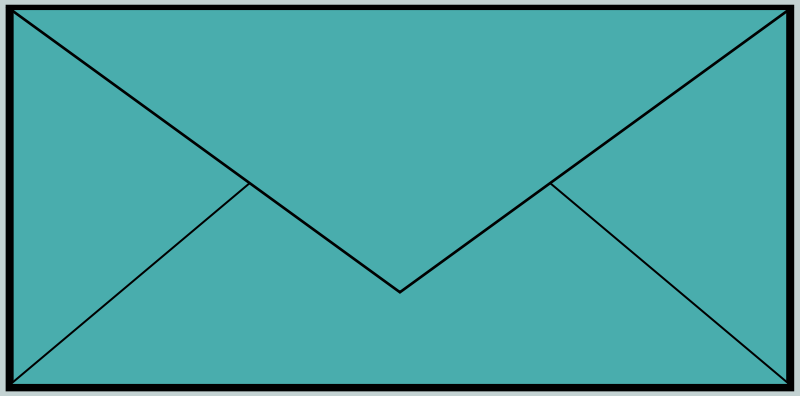
- Classification
- Marking
- Congestion management
- Congestion avoidance
- Policing and shaping
- Link efficiency




# Classification of Traffic

- Traffic is placed into different categories
- For example, the E-mail class might contain various types of traffic
  - POP3
  - IMAP
  - SMTP
  - Exchange

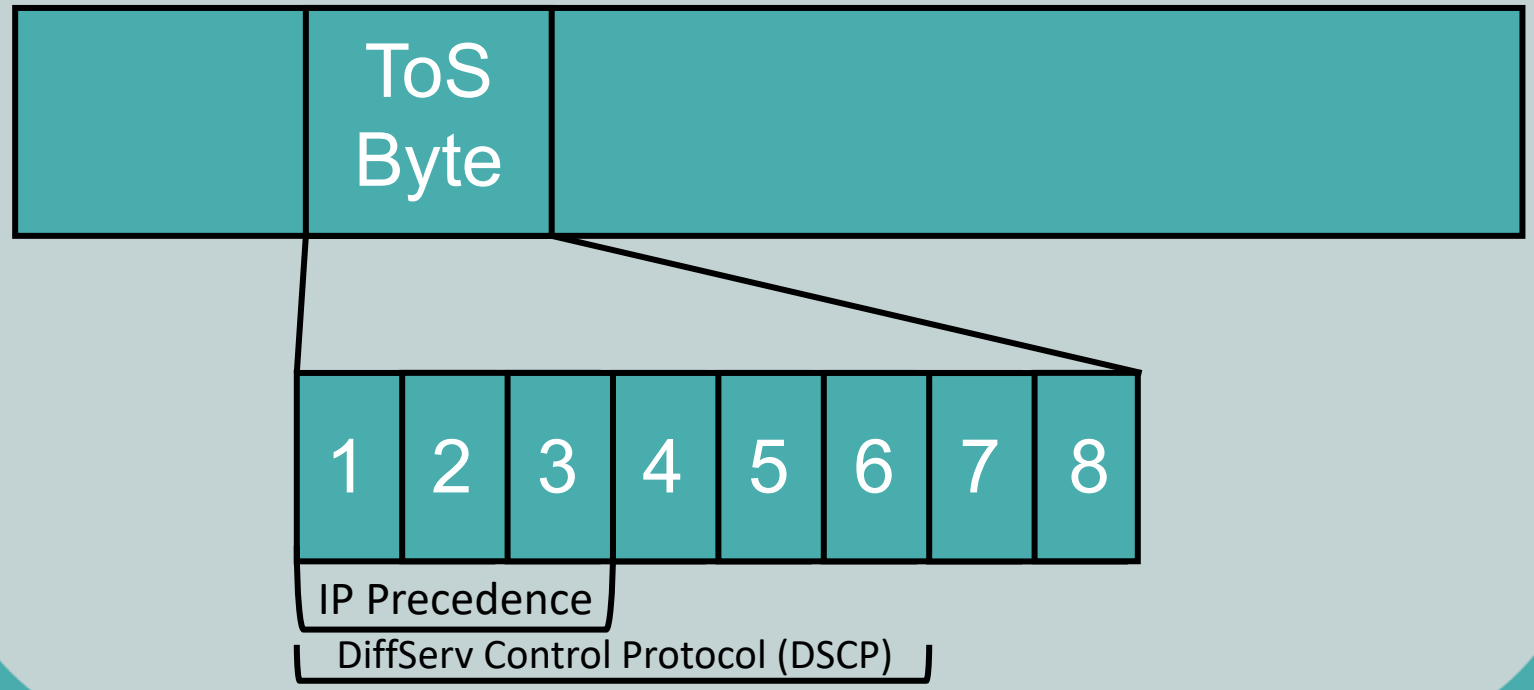


- Classification does not alter any bits in the frame or packet

# Marking of Traffic

- Alters bits within a frame, cell, or packet indicates handling of traffic

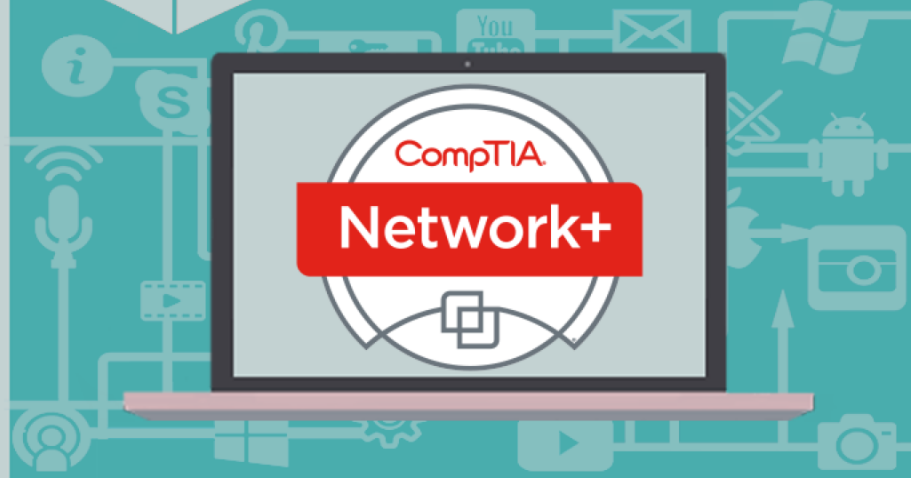
- Network tools make decisions based on markings



# Congestion Management

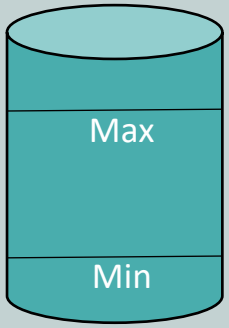
- When a device receives traffic faster than it can be transmitted, it buffers the extra traffic until bandwidth becomes available
  - Called *queuing*
- Queuing algorithm empties the packets in specified sequence and amount
- Queuing algorithms types
  - Weighted fair queuing
  - Low-latency queuing
  - Weighted round-robin



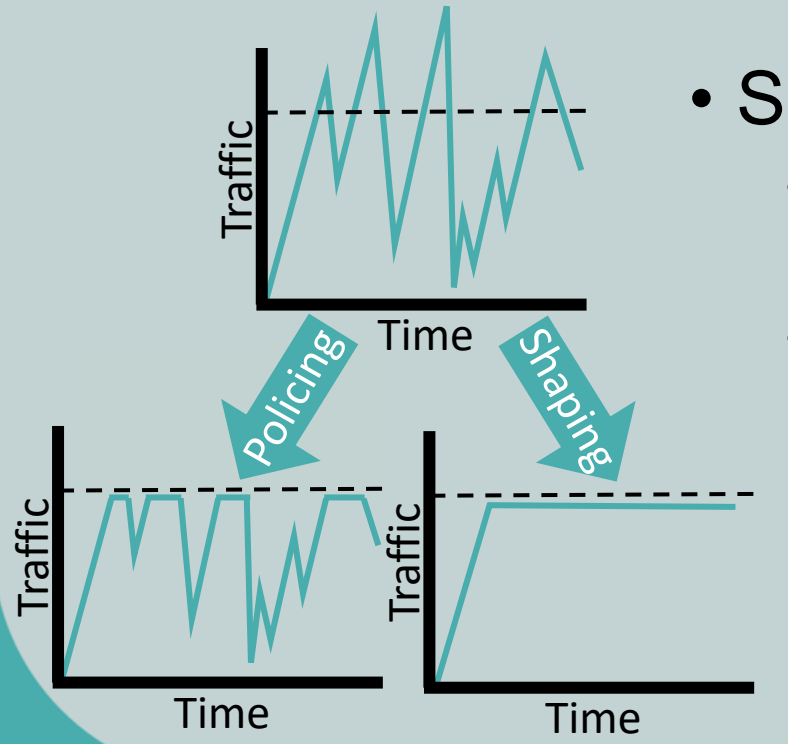
# Congestion Avoidance

- Newly arriving packets would be discarded if the device's output queue fills to capacity
- *Random Early Detection* (RED) is used to prevent this from occurring
  - As the queue fills, the possibility of a discard increases until it reaches 100%
  - If at 100%, all traffic of that type is dropped
  - RED instead drops packets from selected queues based on defined limits
- If TCP traffic, it will be retransmitted
- If UDP, it will simply be dropped




# Policing and Shaping

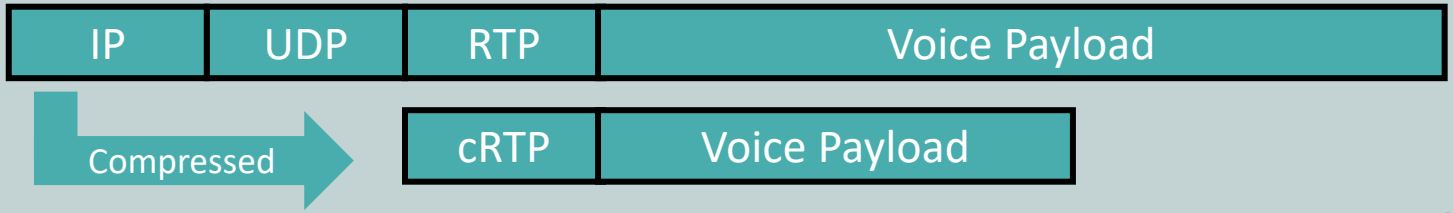
- Policing
  - Typically discards packets that exceed a configured rate limit (*speed limit*)
  - Dropped packets result in retransmissions
  - Recommended for higher-speed interfaces




- Shaping
  - Buffers (delays) traffic exceeding configured rate
  - Recommended for slower-speed interfaces

# Link Efficiency: Compression

- Packet payload is compressed to conserve bandwidth
- VoIP payload can be reduced by 50%
  - Payload size from 40 bytes to 20 bytes
- VoIP header can be reduced by 90-95%
  - Uses RTP header compression (cRTP)
  - Header size goes from 40 bytes to 2 to 4 bytes




- Utilized on slower-speed links to make most of limited bandwidth

# Link Efficiency: LFI

- Link Fragmentation & Interleaving (LFI)
- Fragments large data packets and interleaves smaller data packets between the fragments
- Utilized on slower-speed links to make the most of limited bandwidth