Welcome Back to CISSP Bootcamp Day 3

Michael J. Shannon

Class will begin at 10:00 am Central Standard Time

SITE AND FACILITY SECURITY

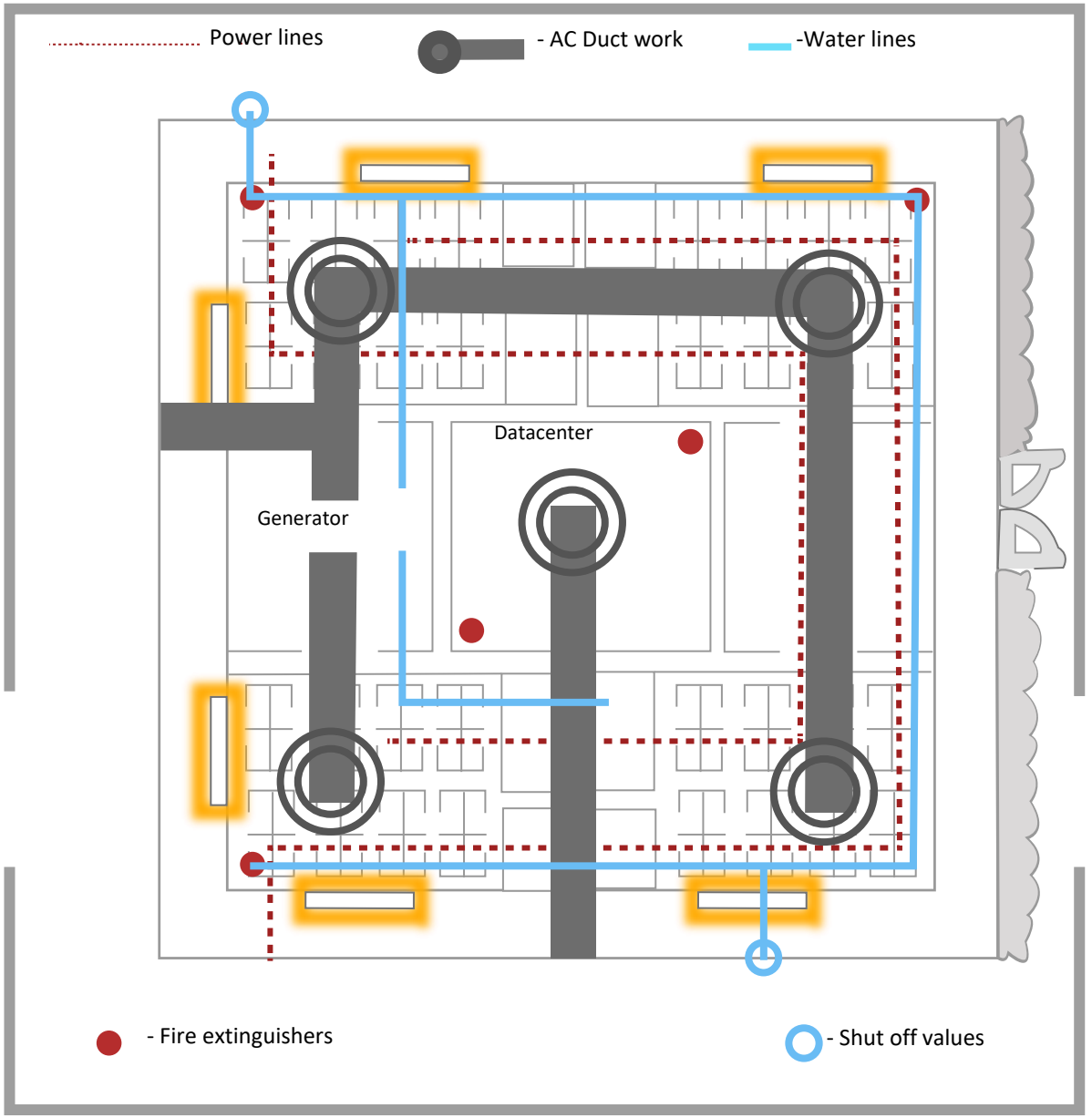
OBJECTIVES

- Describe site and facility security design principles, perimeter, and internal security controls
- Describe wiring closets, intermediate distribution frames, server rooms, and data centers
- Provide an overview of restricted and work areas, utilities, and heating, ventilation, and air conditioning (HVAC)
- Outline environmental and power issues, personnel safety, and security

SITE AND FACILITY SECURITY DESIGN PRINCIPLES

- When designing physical security controls, use a defense-in-depth approach:
  - Begin at the property or facility edge and work back to the most valuable assets
  - Begin at "the keep" of valuables and work your way out to the physical edge
- *This course will take an "outward-in" approach*
- Different sites will have varying demarcation points of physical and logical entry:
  - Strategy depends upon where the property line and demarcation points are

KNOW ALL PROPERTY AND FACILITY INGRESS/EGRESS POINTS



FACILITY SECURITY PLAN LIFE CYCLE

01 Facility profile

02 Roles and responsibilities

03 Risk management strategy

04 Security countermeasures

05 Maintenance, repair, and testing procedures

06 Incident response management and procedures

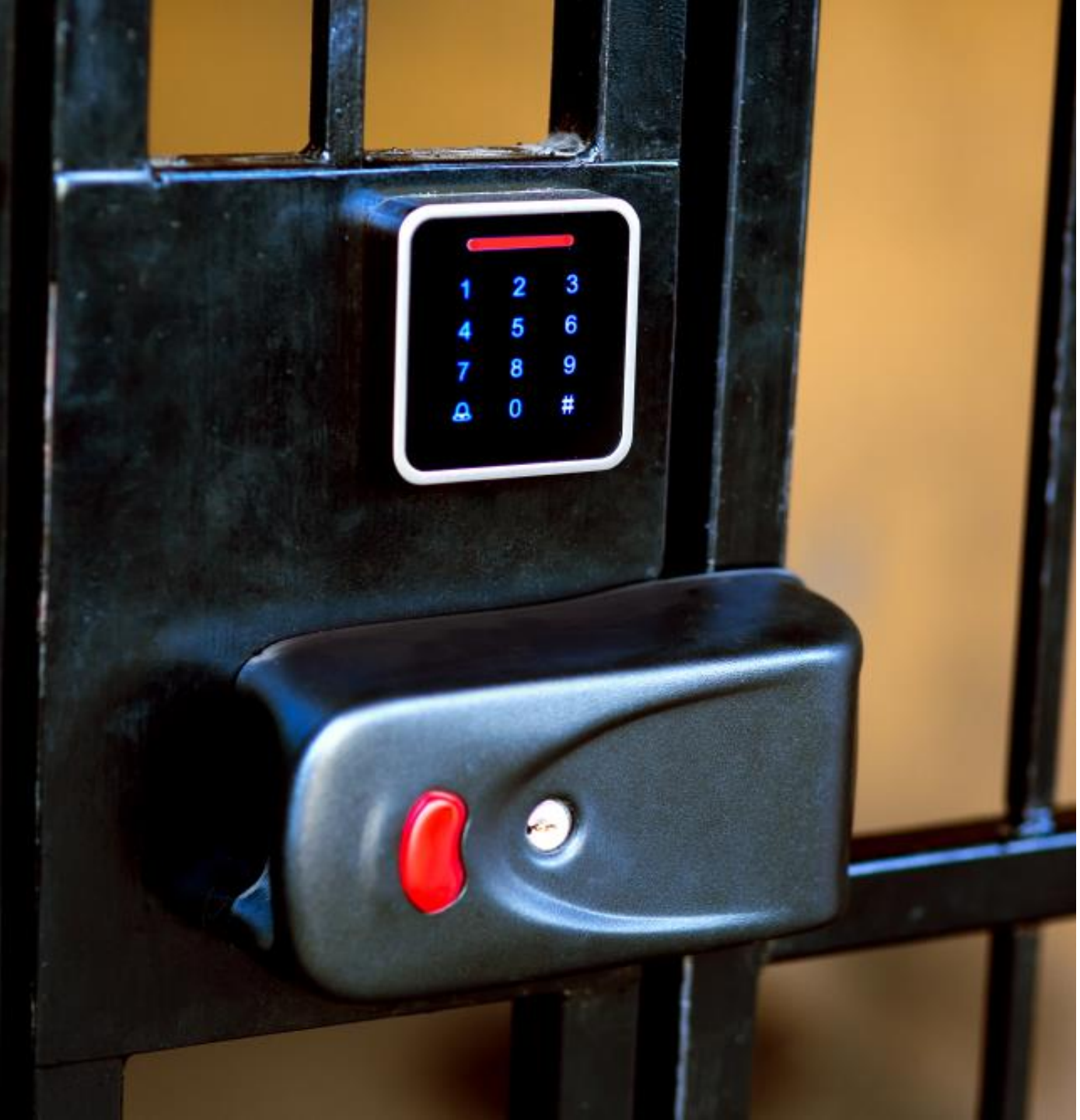
07 Employee training

08 Program review

PERIMETER SECURITY CONTROLS

Perimeter barriers:

- Landscaping such as hedgerows and trees
- Fences (with barbs, electrified)
- Tire shredders (one-way only)
- Bollards (permanent and temporary)
- Moats or ponds
- Gates (wooden and metal)
- Guard gates (armed and unarmed sentries)



FENCE BARRIERS

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- High security areas will use barbed wire and/or electric fences combined with warning signs every 6-8 feet
- Fences are combined with entry/exit gates of varying strength:
  - Barricade gates
  - Tire shredders

GATES SEPARATED INTO CLASSES

- Class I: Residential gate operation
- Class II: Commercial, like parking lot or garage
- Class III: Industrial/limited access (warehouse, factory, loading dock, etc.)
- Class IV: Restricted access operation that requires supervisory control (prison, airport, etc.)

BOLLARDS

- Are strategically placed pylons meant to prohibit vehicles from entering certain areas:
  - They can be permanent and/or temporary pylon cones
  - They can be vertical or horizontal
- Are often placed in front of buildings, in parking lots, or along sidewalks to guide pedestrian traffic
- Are typically concrete or strong metal
- Can be mechanical and include cameras and sensors

SIGNAGE

- Signs are a deterrent control
- Signs and window stickers are designed to deter individuals from doing something unauthorized
- They may also be combined with harmful fences:
  - Danger: Electric Fence
  - No Unauthorized Access
  - No Trespassing – Do Not Enter
  - Armed Guard on Duty
  - This Area Under Video Surveillance
  - Beware of Dog

EXTERNAL SECURITY CAMERAS

- Monitor and record the property perimeter and other facility areas for intruders and potential attackers
- Are considered a detective control primarily:
  - Although their very presence can be a deterrent
- Often are recording devices sent to monitoring stations or security operations centers (SOCs):
  - Backup recorded media should be securely stored
- Should trigger alerts when a camera is disabled
- Should be combined with adequate lighting and all dead spots should be covered

EXTERNAL SECURITY LIGHTING

- Often works with external cameras and sensors:
  - Motion-activated lights:
    - Trip lighting is activated by some trigger or sensor
    - Standby lighting is activated at suspicious activity
    - Emergency lighting is used when power fails
  - Timed security lighting
  - Floodlights (all-night lighting)
  - Exterior soffit lights:
    - Decorative external lights that illuminate dark corners and pathways to deter potential intruders and stop accidents
  - High-intensity discharge (HID) security lights

HIGH-INTENSITY DISCHARGE LAMPS (HID)

- HID lights are a collection of gas-discharge arc lamps
- They generate light by producing an electric arc between two electrodes through ionized gas
- HID lamps are brighter than average headlights and have an HID light bulb
- This bulb holds two electrodes enclosed in a glass component filled with xenon gas and metal salts
- HID lamps are usually sealed in a special arc discharge tube formed from quartz

INDUSTRIAL CAMOUFLAGE

- These are cameras, surveillance devices, and sensors that are camouflaged in landscaping elements, statues, and tall trees:
  - For example, towers carrying cell phone or other equipment are covered by fake trees
- Certain high-security rooms can be underground and set at distance from main buildings

EXTERNAL SECURITY GUARDS

- External guards are typically at the property gate or perimeter and stationed 24x7:
  - They could be just on-site during business hours or off-hours
- They are a security control of multiple types: detective, preventative, and deterrent
- Guards provide credentials checks, authentication, communication, and rapid security response if an intrusion or incident occurs
- They should also interface with other law enforcement

GUARD CONSIDERATIONS

- Are they employees, contractors, or freelance?
- Are guards certified and/or licensed?
- Will they be armed or unarmed?
  - What are the insurance or liability ramifications?
- Is the organization involved with screening and background checks?
- Who provides initial and continuous training and awareness?

ROBOTIC SENTRIES

- Robot sentries can be used in home or commercial environments as security guards with cameras, sensors, guns, and more
- The Samsung SGR-A1 was an original type of sentry gun that was developed jointly with Korea University to support South Korean troops in the Korean Demilitarized Zone
- The Foster-Miller TALON is the fastest, remotely operated, tracked military robot designed for missions ranging from reconnaissance to combat:
  - It is made by QinetiQ-NA, a subsidiary of QinetiQ

LOCKS

- Locks are the most common facility and internal physical security mechanism
- They are considered a preventative control although they technically only delay entry – not prevent it in the long run (brute force)
- Locks keep honest people out but cannot deter resolute intruders, since most locks are easily bypassed, and most keys are readily duplicated
- They can be physical, electronic, cipher, and/or biometric

TYPES OF LOCKS

- Key lock:
  - A lock that requires a key to open
- Warded:
  - Obstructions to the keyhole that prevent all but the properly cut key from entering
- Wafer/tumbler:
  - Wafers under spring tension are in the core or plug of the lock and protrude outside the diameter of the plug into a shell formed by the lock body
- Deadbolt:
  - A bolt inserted into the frame of the door for additional security when combined with other locks

TYPES OF LOCKS

- Interchangeable core:
  - A core that can be removed and replaced using a special-change key
- Combination:
  - A sequence of numbers in proper order
- Electronic combination:
  - Digital readouts that obtain power from the energy created when the dials are turned
- Keyless:
  - Buttons that are pushed in sequence to open the door – sometimes called a cipher lock
- Smart lock:
  - An inexpensive plastic card that is pre-authenticated to open a door, used in most hotels

BREAKING INTO LOCKS

Picking

- Uses a tension wrench to rotate the key plug of the lock to find the lock tumblers
- At the same time, the pick is used to move the binding tumblers, one at a time, to the shear line
- When all the tumblers are aligned properly with the shear line, the lock opens

Raking

- Uses a pick that has a wider tip inserted all the way to the back of the plug
- The pick is then pulled out quickly so that all the pins are bounced up, and as the rake exits, a tension wrench turns the plug
- Upper pins will fall on the ledge created by the turning pins, so remaining pins can be picked

Brute

- Brute force techniques will always be successful given enough time and effort
- This involves using hammers, tire irons, firearms, explosives, and more
- This contributes to locks being a "delay" control, in practicality

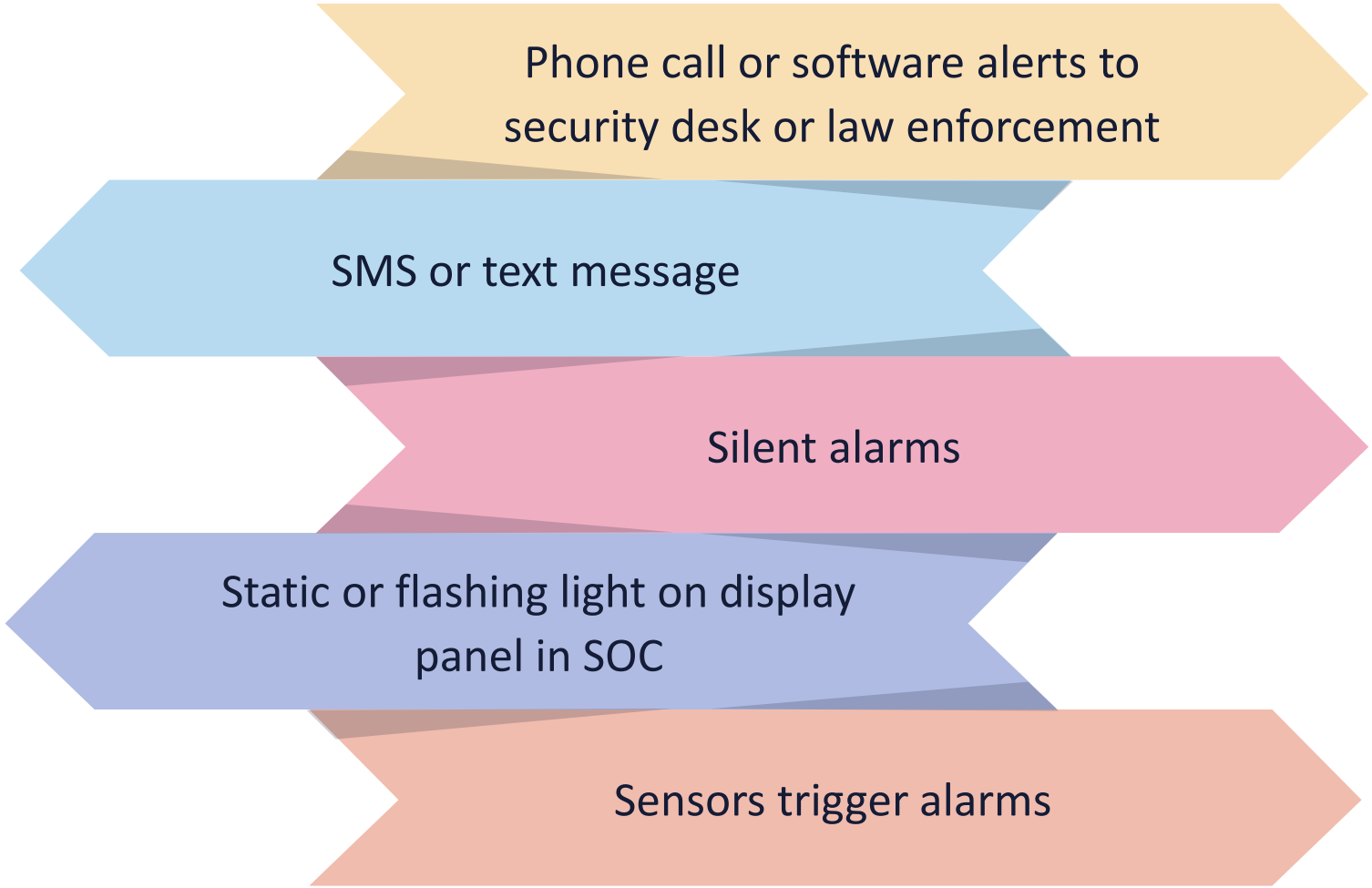
WINDOW SECURITY

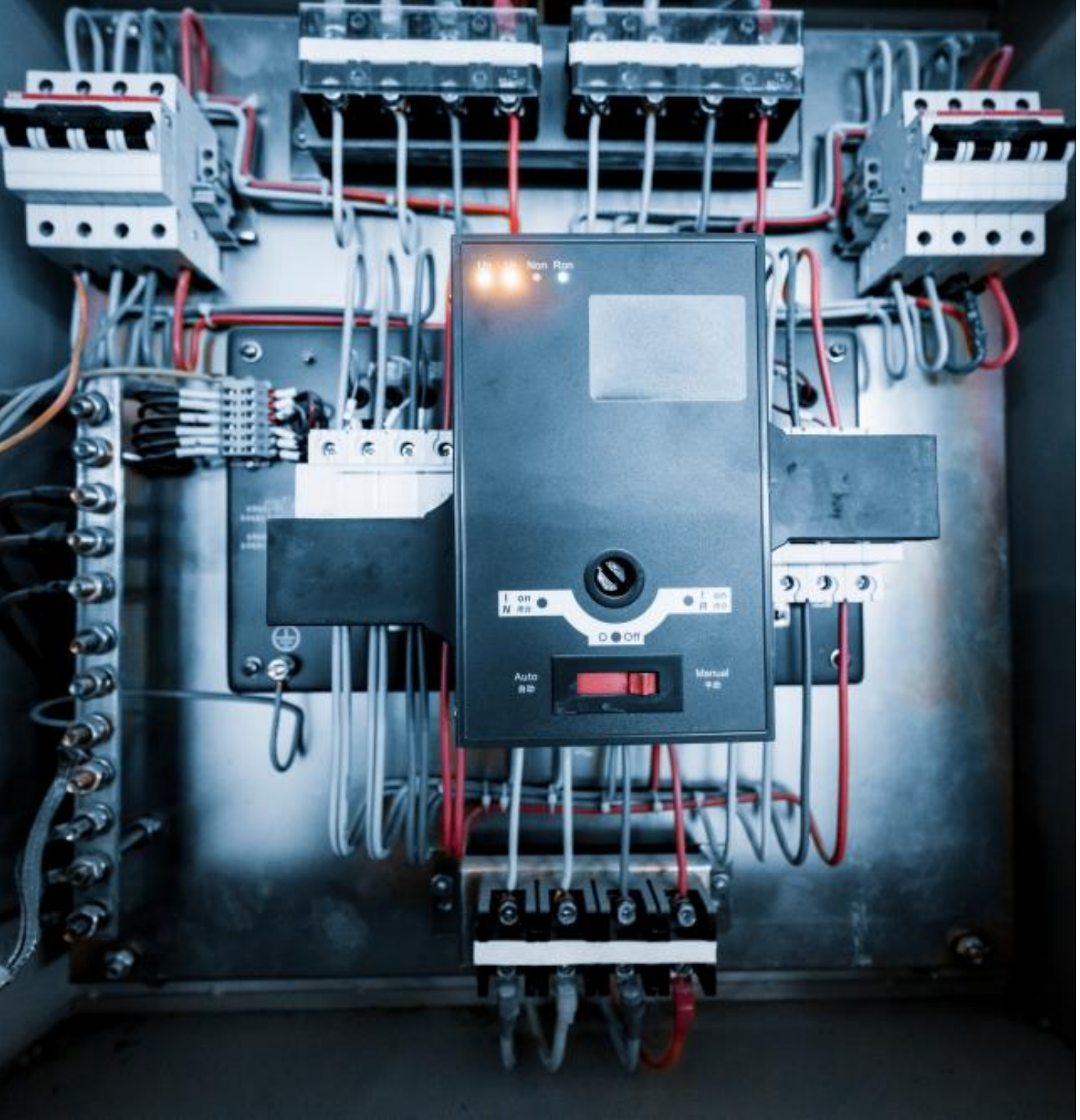
- It is true that most intruders gain entry through doors
- However, the second most common area susceptible to break-ins is first-floor windows
- Second-floor windows are harder to access and much less probable to be the source of attack entry
- Security techniques include
  - Window bars
  - Bullet-proof windows
  - Steel mesh and films in/on windows
  - Special window locks
  - Polycarbonate safety shields

INTERNAL MOTION DETECTION

- Photoelectric – break in a light beam
- Passive infrared – infrared light
- Vibration – change in the level of vibration
- Acoustic – change in sound waves
- Microwave – change in radio waves
- Electromechanical – break in an electrical circuit
- Electrostatic – change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental controls

SENSORS TRIGGER ALARMS

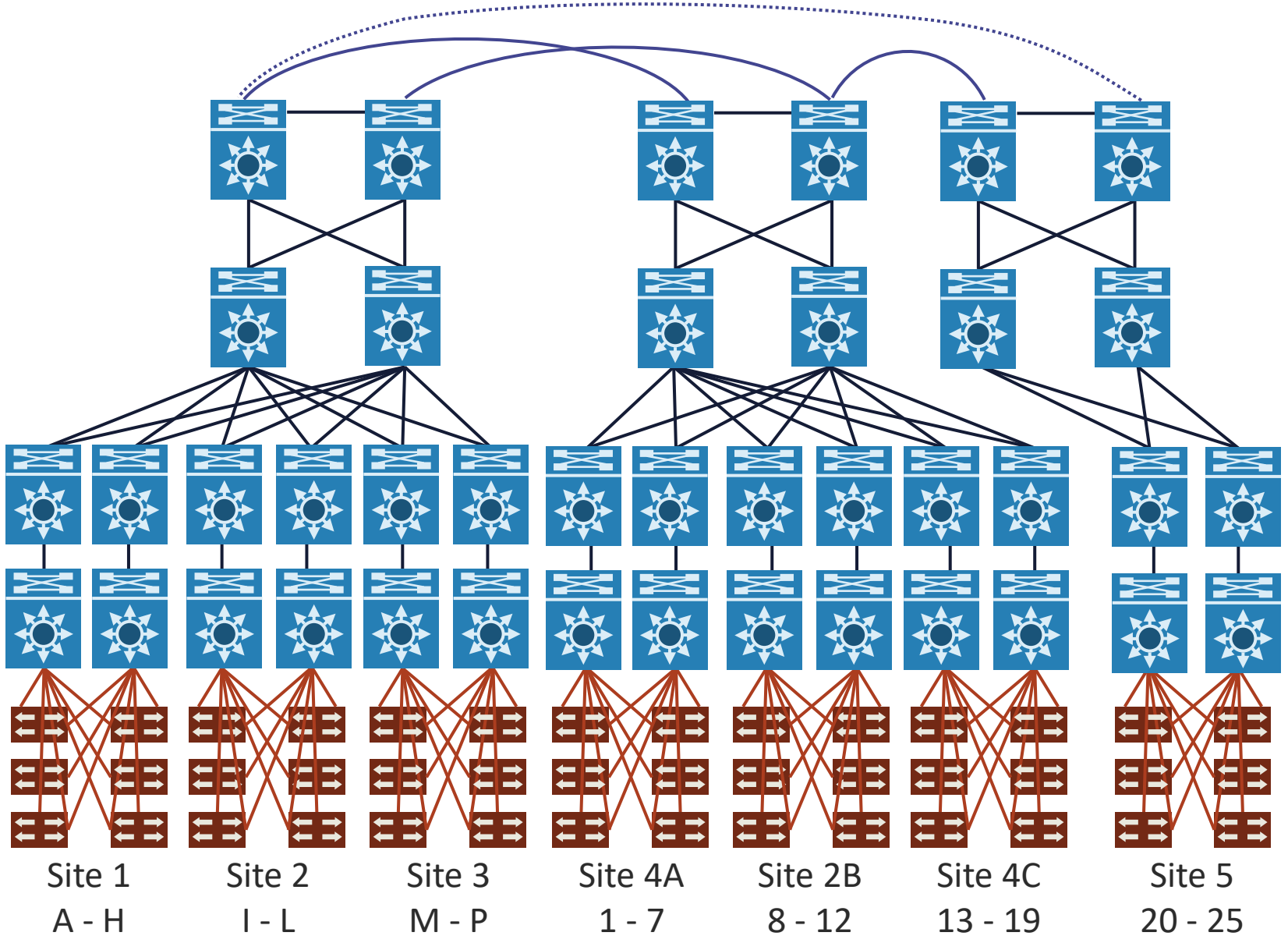




SECURE WIRING CLOSETS AND DISTRIBUTION FRAMES

- Security officers must have visibility into all EthFrame (MDF) rooms and closetsernet and fiber cable runs including the security of the main distribution:
  - Under the floor
  - Above ceiling panels
  - In the walls
- Use advanced locks with multiple factors for all doors to server/frame rooms if feasible
- Cameras, lights, and/or sensors can be used and should trigger alarms or alerts
- There should be little or no window access
- Consider CCTV monitoring from the SOC or security guard stations

CAMPUS/MAN DISTRIBUTION



Router MAN backbone
Connected by dark fiber
Site backbone
One per MAN region
Three on main campus

Core

Desktop cluster
One per site
Seven in main campus
BDF
Building distribution frame
One per building
41 in main campus

Distribution

IDF
Intermediate distribution frame
Two per floor

Access

SERVER ROOM AND DATA CENTER SECURITY

- Work with facilities management to integrate blueprints and topological diagrams into IT services
- Know all physical and logical ingress and egress points
- Implement full-body scanners to highly sensitive areas to look for removable media:
  - Log and audit all devices and objects entering and exiting the facility
- Have intrusion visibility (cameras) and sensors for all high-security compartmentalized areas
- Implement physical segregation of duties

SERVER ROOM AND DATA CENTER SECURITY

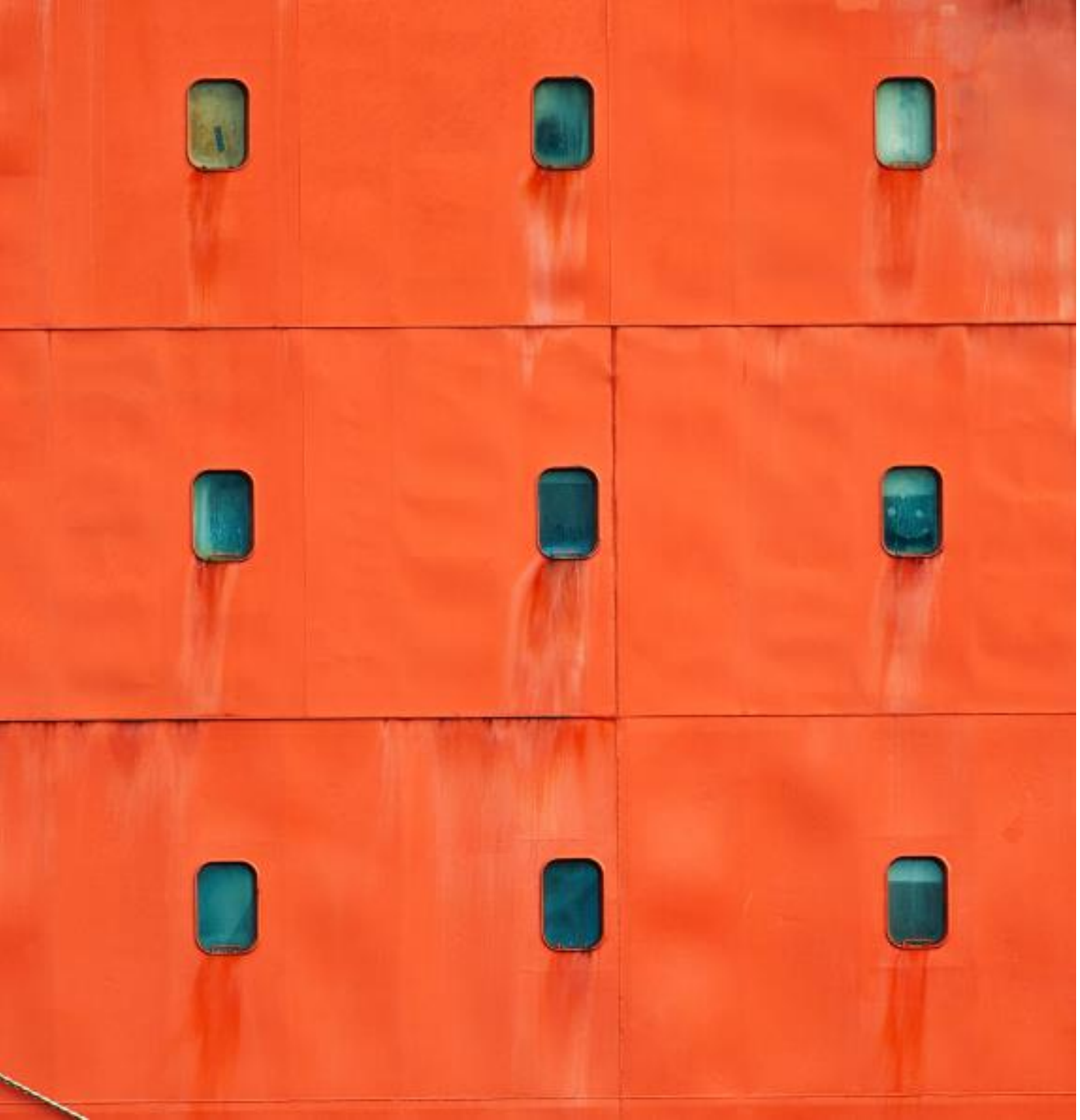
- Authorized staff should pass biometric multi-factor authentication (MFA) and authorization **a minimum of two times** to access data center floors and SOC
- Biometric MFA is highly recommended
- All visitors and contractors should show identification and be signed in and continually escorted by authorized staff:
  - When an employee no longer has a business need for data center privileges, access must be immediately revoked, even if they continue to be an employee

SERVER ROOM AND DATA CENTER SECURITY

- Automatic fire detection and suppression equipment must be employed
- The electrical power systems should be fully redundant and maintainable without impact to operations 24/7
- Uninterruptible power supply (UPS) units can provide back-up power for critical and essential loads in the facility in the event of an electrical failure
- Data centers should use generators to provide back-up power for the entire facility
- External chillers may be in place for temperature control

SERVER ROOM AND DATA CENTER SECURITY

- Get visibility into all power and HVAC conduits
- Airgap is the physical separation of the control network and other networks:
  - Separate the highly secure networks from the unsecured networks with physical or logical compartmentalization
- Use private clouds, sandboxes, and detonation chambers for secure activities when feasible



SECURE ENCLOSURES

- The organizational safe may store the highest value assets based on the contents:
  - These are bearer bonds, currency, deeds, securities, licenses, precious metals, cryptocurrency cold storage wallets, and failsafe passwords, among others
- Employees may also need a special area to store and protect valuables, such as lockers or locked cabinets
- A reinforced filing cabinet is a type of secured container designed to withstand burglary attempts
- The U.S. government provides container classifications for these reinforced containers, based on the time taken to break into them, either covertly or surreptitiously with no forced entry

SAFES

- The Underwriters Laboratory (UL) provides safe classifications that specify the degree to which safes can withstand attack
- For example, a safe that takes 30 minutes to break into using various tools and torches is classified as a Tool Resistant safe class - TL30
- Embedded "walk-in" safes with timers are more secure than removable standalone home safes – even if they are bolted down
- All adjacent walls must use tool and fire-resistant materials and awareness of neighboring businesses

SAFES

- Factors considered in classifying the safe:
  - Lock mechanism factors to open the safe
  - Material used to construct the safe
  - The weight and whether it's securely anchored or embedded in concrete
  - The tensile strength of the steel
  - Whether the safe has a relocking device

MEDIA STORAGE SECURITY

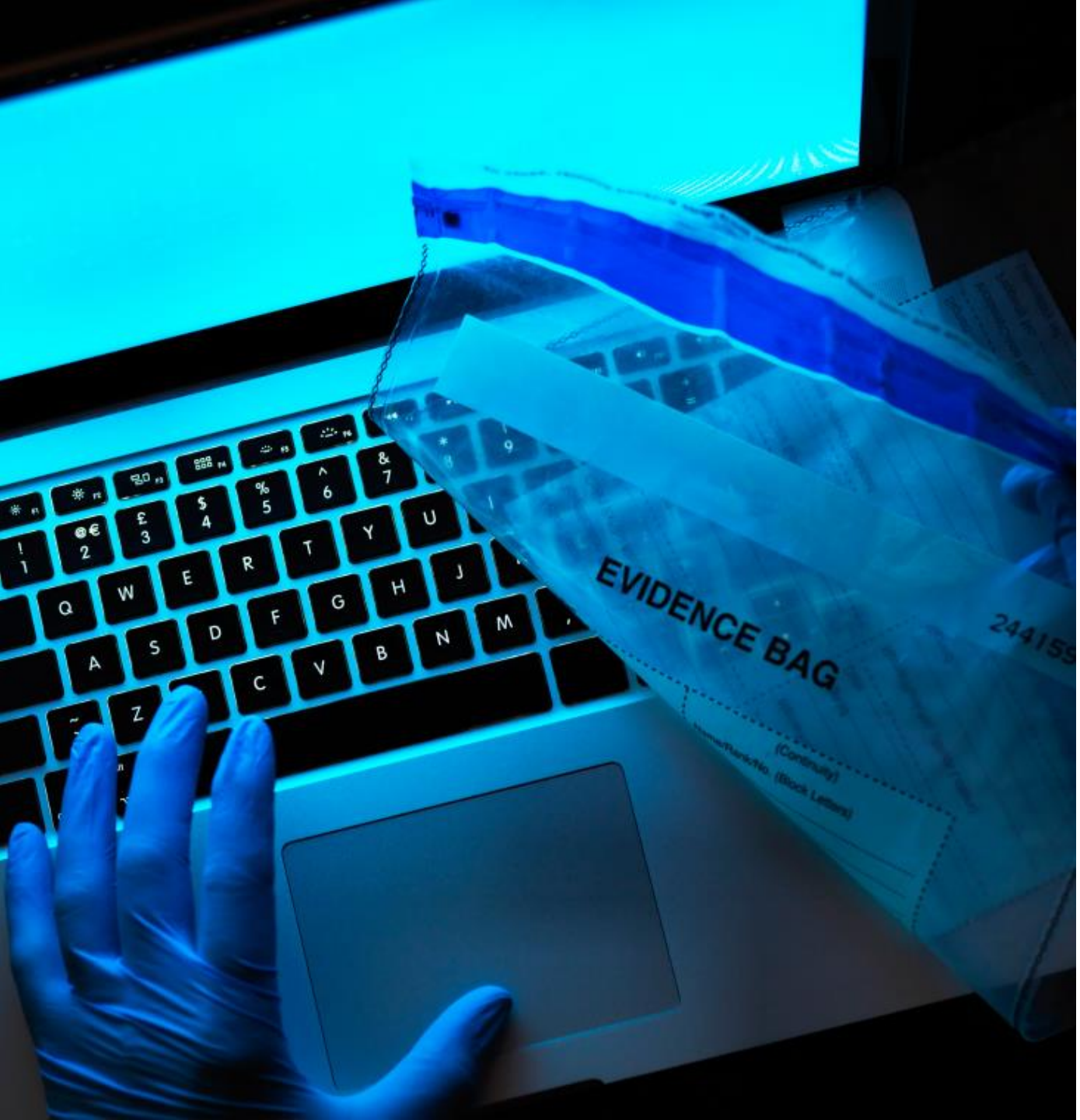
- This storage often holds data backups media, documents, and redundant spares:
  - For example: hard copies of documents and microfiches, etc.
- Facilities and media storage should be part of COO and business continuity planning
- The same access policies that apply to data center and server rooms should apply
- AWS, Google Cloud Platform (GCP), and Azure all offer long-term data/virtual tape archiving and hardware security modules (HSMs) with AEs-256 encryption

MEDIA STORAGE SECURITY

- Media storage should be covered with a disposition and destruction policy
- When a storage device has reached the end of its useful life, procedures should include a decommissioning process that prevents data from being exposed
- Consider a reference to NIST 800-88 ("Guidelines for Media Sanitization") as be part of the decommissioning policies

EVIDENCE STORAGE

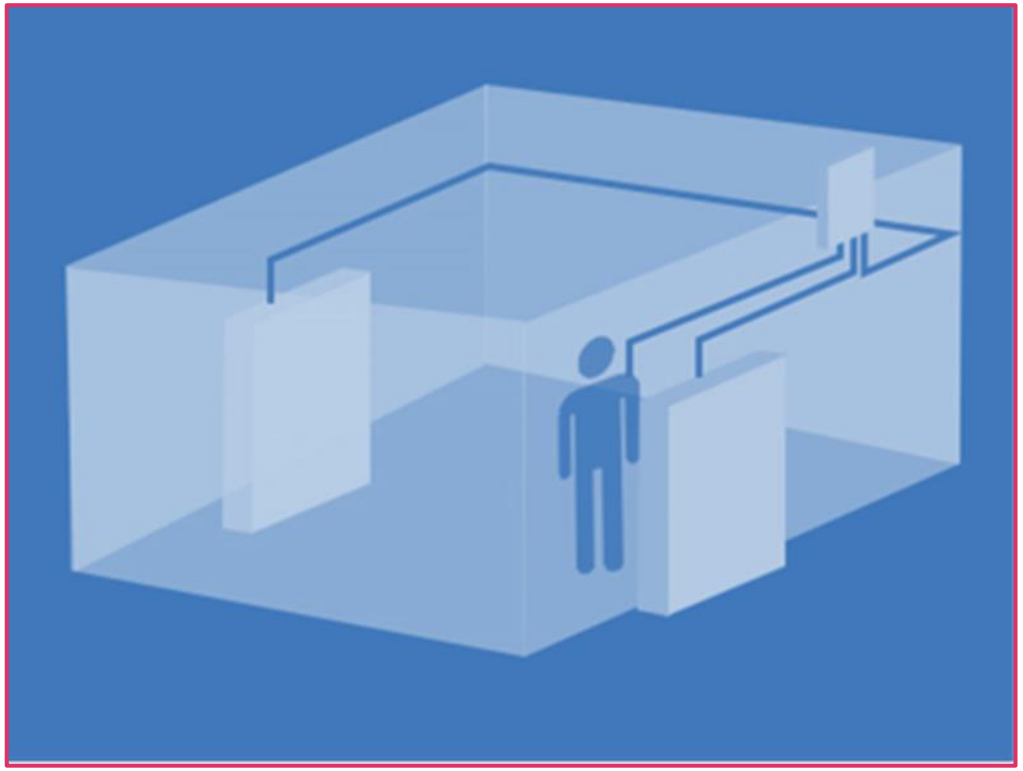
- Evidence room facilities are only as secure as the honesty of the staff:
  - Separation of duties and dual operator (two-person rules) are critical policies
- Chain of custody must be maintained for incident response, forensics, and law enforcement – contents of an evidence room may have a higher street value
- Modern digital evidence management software should be used



EVIDENCE STORAGE

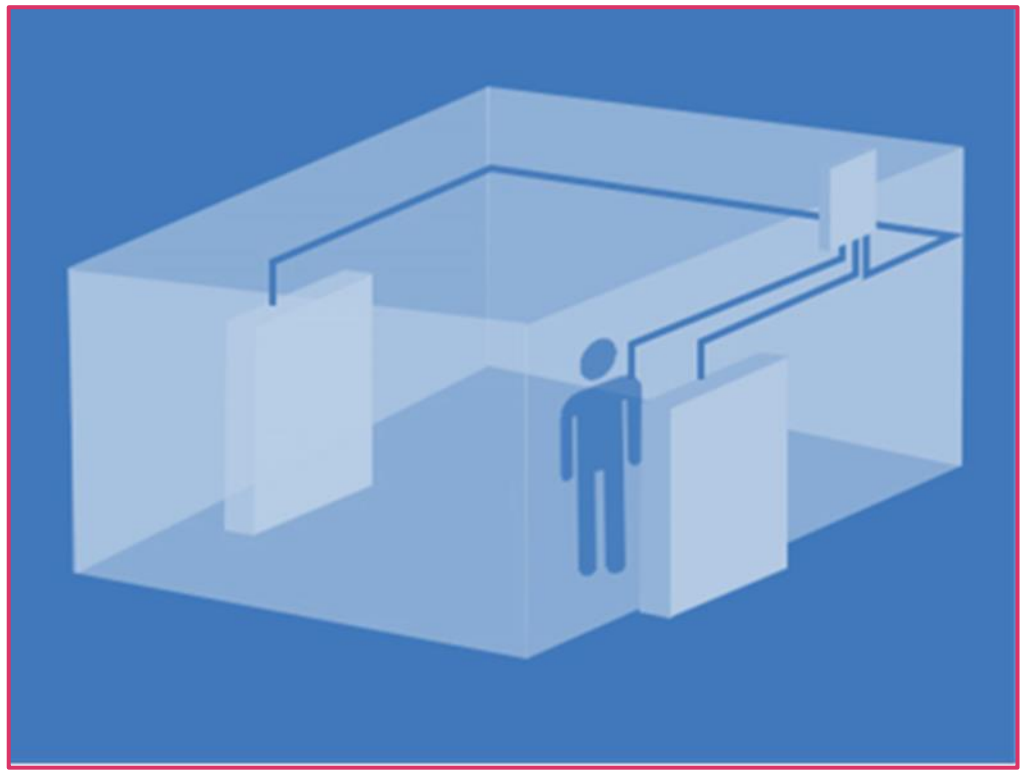
- Doors must be solid, preferably steel, with no glass – there should be no doors leading directly to the exterior of the building from the evidence room
- The rooms may be single-entry with no windows, concrete or cinder block walls
- **Access control vestibules** are common for entry and exit

ACCESS CONTROL VESTIBULES (MANTRAPS)



- With most access control vestibules, a person must produce some type of dual-factor identification proofing to enter an area
- Mantraps are more elaborate systems that direct people through **two** interlock-controlled doors into an area:
  - The design specifies that the inner door will not unlock if the outer door is open, or vice versa
- These will also prevent piggybacking and tailgating

ACCESS CONTROL VESTIBULES (MANTRAPS)



- Can identify and authenticate the person entering
- Provide credentials and license or passport
- Can include biometric readers
- Often use CCTV and intercom systems
- Keeps security guard behind bullet-proof glass
- Admits the person through a strong door with electronic locks

RESTRICTED AND WORK AREA SECURITY

- Some high-security restricted areas employ Faraday cages
- These are rooms, enclosures, or bags that block electromagnetic fields emanating from electromagnetic interference (EMI), Carrington Events, solar flares, and electromagnetic pulses (EMP)
- The shield may be fashioned from a continuous covering of conductive material, or in the case of a Faraday cage, a mesh of similar materials
- These can often be found in data centers or other enterprise safe rooms:
  - Military grade Faraday bags can also be used for removable drives, cold storage cybercurrency wallets, and other critical components

AIR GAP

- A strictly air gapped device or system is completely disconnected from any network and is only managed out-of-band:
  - Hardware security modules
  - Certificate servers
  - Specialty Supervisory Control and Data Acquisition (SCADA) components
- Loosely air-gapped systems have no public Internet access
- This can be physical or logical (PVLAN)
- The systems are still vulnerable to a rogue insider:
  - Stuxnet was introduced to air gapped area

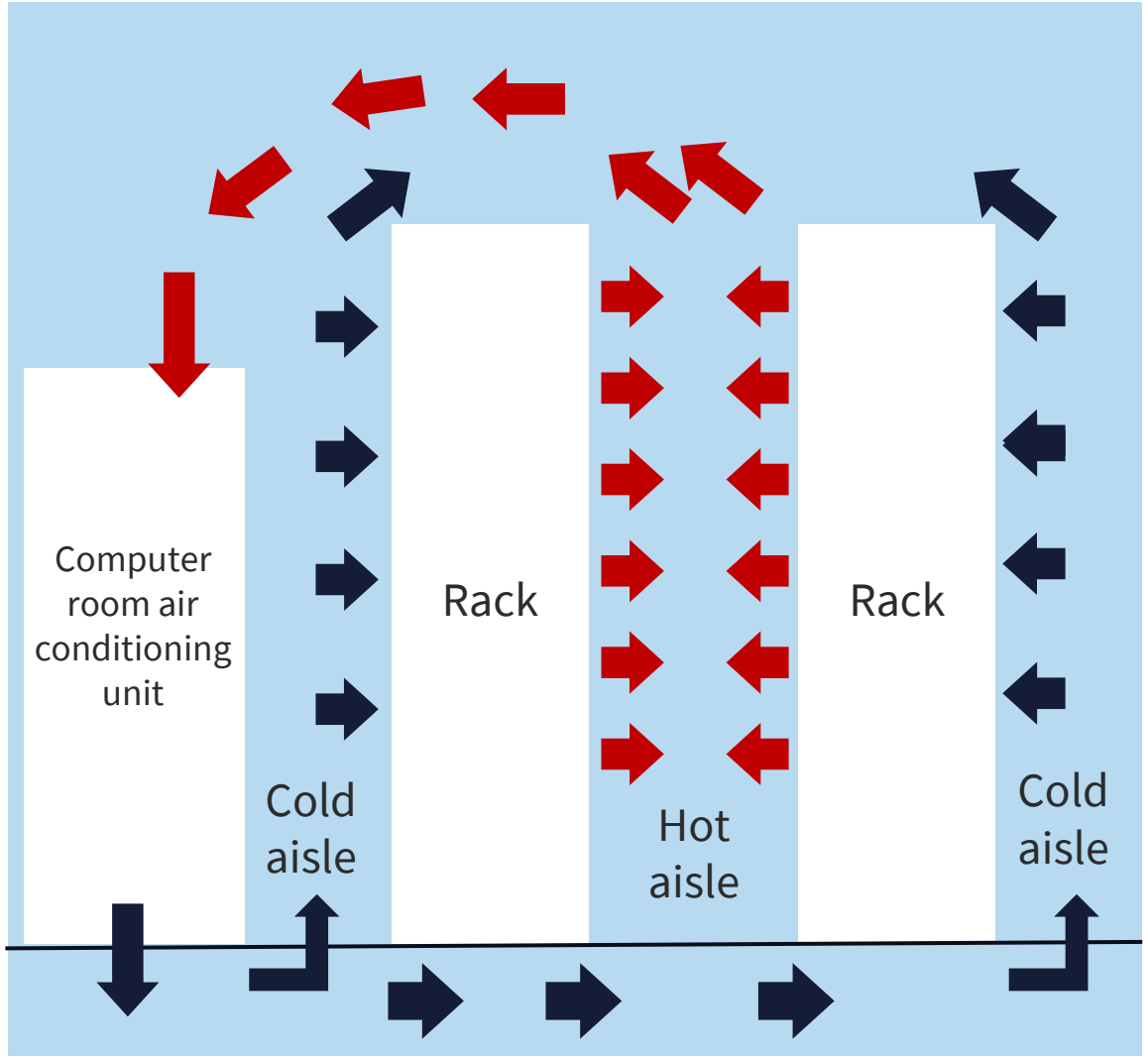
AIR GAP

- These are common with military and governmental agency networks and systems
- They are also found in use at:
  - Financial services such as stock and cryptocurrency exchanges
  - Industrial control systems, like SCADA, in water and nuclear processing facilities
  - Life-critical systems, power plants, computers used in aviation, and computerized medical equipment

UTILITIES AND HVAC

- Poor HVAC can lead to extreme heat, extreme cold, extreme humidity, and/or extreme dryness
- HVAC systems need proper monitoring and ongoing maintenance (e.g., pressurization and temperature)
- Physical security of all components and controllers is a concern
- Location options may be limited by the facility
- Environmental control can also include the possibility of chemical and biological leaks or attacks

HOT AND COLD AISLES



DATA CENTER AND SAN CHILLERS

- Data center chillers are very specific internal or external cooling systems that counter excess heat in server farms and data centers
- Chillers (i.e., adiabatic) must maintain 24/7 uptime to keep closely packed racks and cabinets of heat-generating equipment cool
- Chillers continuously cool the water used in the HVAC system so that temperatures stay at the proper levels
- Data center managers and engineers must guarantee that chillers have independent generators in case of a power grid failure

SECURITY MANAGERS MUST BE AWARE OF THE LIKELY ENVIRONMENTAL ISSUES

Hazard identification

Hazards

- Fire
- Explosion
- Natural hazards
- Hazardous materials spill or release
- Terrorism
- Workplace disease
- Utility outage
- Mechanical breakdown
- Supplier failure
- Cyber attack

Property & magnitude

Vulnerability assessment

Assets at risk

- People
- Property, including buildings and critical infrastructure
- Supply chain
- System/equipment
- Information technology
- Business operations
- Reputation of or confidence in entity
- Regulatory and contractual obligations
- Environment

Vulnerability

Impact analysis

Impacts

- Casualties
- Property damage
- Business interruption
- Loss of customers
- Financial loss
- Environmental contamination
- Loss of confidence in the organization
- Fines and penalties
- Lawsuits

https://www.ready.gov/risk-assessment

FIRE CONTROLS

Prevention

- It is a critical aspect of business continuity and disaster recovery planning
- Prevention involves using fire-rated construction materials and fire-resistant enclosures
- Organizations must conduct training, raise awareness, and focus on safety and preparation

Detection

- Organizations must deploy comprehensive smoke, gas, and fire detectors
- Different sensors will be used for different areas, vulnerabilities, and use cases
- Detect and control quickly to minimize damage
- Detection and suppression often work together in close phases

Suppression

- This action will quickly contain and extinguish the fire
- It creates barriers and firewalls to prevent the spread of fire
- Use portable fire extinguishers located strategically throughout the building
- Although water sprinklers are used in common areas, halon substitutes or carbon dioxide discharge systems are typical around computers and networking equipment

TYPES OF EXTINGUISHERS

- Type A – common combustibles, such as wood products, paper, and laminates:
  - Suppressed with dry chemical, clean agent, wet chemical, water, and foam
- Type B – combustible liquids, such as petroleum products and coolants:
  - Suppressed using halon substitutes, dry chemical, clean agent, foam, and carbon dioxide
- Type C – electrical equipment and wires:
  - Extinguished using dry chemical, clean agent, water mist, and carbon dioxide
- Type D – combustible metals:
  - Can be suppressed only with dry powder
- Type K – flammable liquids unique to cooking:
  - Extinguished using dry powder

PRIMARY AND SECONDARY LOSS

Primary

- Loss of life
- Interruption to operations
- Productivity loss
- Response
- Loss of revenue

Secondary

- Compromised confidentiality, integrity, and availability (CIA) of assets
- Replacement costs
- Damaged public image and reputation
- Loss of customers or competitive advantage
- Fines and judgments

POWER CONTROLS

- Power system security involves practices to keep the system operating when subcomponents fail
- Most power systems are operated so that any single initial failure event will not leave other components heavily overloaded
- Enterprises should deploy redundant providers (if possible), surge protectors, uninterruptible power supplies, and appropriate backup generators:
  - The Uptime Institute recommends 12 hours of fuel (diesel) or solar cell backup
- Junctions should be secured and have adequate lighting and cameras

UPTIME INSTITUTE (UI)

- UI is the standard bearer for digital Infrastructure performance whose Tier Standard has been used in thousands of sites in more than 100 countries
- **Tier 1 – The basic site infrastructure:**
  - This tier represents a modest and less expensive solution with little or no redundancy - only dedicated space for IT systems, UPS for backup, line conditioning, and cooling of mission-critical equipment
  - **Problematic personnel activity WILL cause downtime**
  - **All four tiers should have at least 12 hours of fuel for generators**

UPTIME INSTITUTE

- **Tier 2 – Redundant site infrastructure capacity component:**
  - It has everything from Tier 1 plus additional features and components
  - Critical operations do not have to be interrupted for scheduled maintenance or replacement (high availability)
  - There WILL be downtime for any disconnection from power distribution and sources
  - Problematic personnel activity MAY cause downtime
  - Unplanned component failure or systems MAY cause downtime

UPTIME INSTITUTE

- **Tier 3 – Concurrently maintainable site infrastructure:**
  - This tier has dual power supplies for all systems
  - Critical operations can continue to operate if a single component or power component is down for emergency replacement or a scheduled maintenance
  - An unplanned loss of a component MAY cause downtime
  - An unplanned loss of a single system WILL cause downtime

UPTIME INSTITUTE

- **Tier 4 – Fault-tolerant site infrastructure (the optimal data center):**
  - Tier 4 has features of all other tiers included with full redundancy of systems, power, cooling
  - The loss of a single element WILL NOT cause downtime
  - This tier deploys fully automated visibility and response systems with scheduled maintenance performed without downtime

PERSONNEL SAFETY AND SECURITY

- Many organizations will have all guests register at a reception area security desk:
  - Collect and input identification information in the visitor log and camera station for a temporary badge
  - Distribute temporary access cards or badges
  - Guests and contractors may go through rapid background checks and identity validation procedures
  - Guests may need to always be escorted by another employee or security officer
  - No piggybacking and tailgating

PERSONNEL SAFETY AND SECURITY

- Personal issues for joiners, movers, and leavers are often centralized and semi-automated activities between human resources, legal, security, inventory, and directory services
- As part of after-action activities, security managers may be involved in arranging post-trauma counseling, therapy, or a leave-of-absence from incidents and disasters, such as an active shooter

PERSONNEL SAFETY AND SECURITY

Security managers and HR may need to attend specialized training and workshops to prepare for:

- Ongoing security and awareness programs and initiatives
- Travel security practices and anti-theft awareness
- Reinforcement of acceptable use policies (AUPs) that relate to safety and preparedness
- Vulnerabilities of using social media sites
- **Attacks against MFA fatigue**
- Emergency management and duress:
  - Understanding if they need to take over a role or responsibility if someone is incapacitated

SECURE DESIGN PRINCIPLES IN NETWORK ARCHITECTURES (PART 1)

OBJECTIVES

- Provide an overview of OSI, TCP/IP Protocols, IPv4, and IPv6
- Describe secure protocols, multilayer protocols, and converged protocols
- Outline transport architectures
- Describe performance metrics and traffic flows

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	Presentation	Express and translate data formats
5	Session	Accommodate multiple session connections
4	Transport	Connect multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communicate across a single link, including media access control
1	**Physical**	**Specify connectors, data rates, and encoding bits**

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	Presentation	Express and translate data formats
5	Session	Accommodate multiple session connections
4	Transport	Connect multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	**Link**	**Communicate across a single link, including media access control**
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	Presentation	Express and translate data formats
5	Session	Accommodate multiple session connections
4	Transport	Connect multiple programs on same system
3	**Network (or internetwork)**	**Facilitate multihop communications across potentially different link networks**
2	Link	Communicate across a single link, including media access control
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	Presentation	Express and translate data formats
5	Session	Accommodate multiple session connections
4	**Transport**	**Connect multiple programs on same system**
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communicate across a single link, including media access control
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	Presentation	Express and translating data formats
5	**Session**	**Accommodate multiple session connections**
4	Transport	Connect multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communicate across a single link, including media access control
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	Accomplish a networked user task
6	**Presentation**	**Express and translating data formats**
5	Session	Accommodate multiple session connections
4	Transport	Connect multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communicate across a single link, including media access control
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	**Application**	**Accomplish a networked user task**
6	Presentation	Express and translating data formats
5	Session	Accommodate multiple session connections
4	Transport	Connect multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communicate across a single link, including media access control
1	Physical	Specify connectors, data rates, and encoding bits

THE OSI REFERENCE MODEL

Number	Name	Description
7	Application	HTTP, FTP, SMTP, DNS, TELNET, LDAP
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk, RTP
3	Network (or internetwork)	IP, IPX, ICMP, ARP, BGP, EIGRP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM, DOCSIS
1	Physical	Binary transmission, encoding, bit rates, voltages

THE OSI REFERENCE MODEL

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or internetwork)	**Internet** (internetwork)
2	Link	**Network access**
1	Physical	

THE OSI REFERENCE MODEL

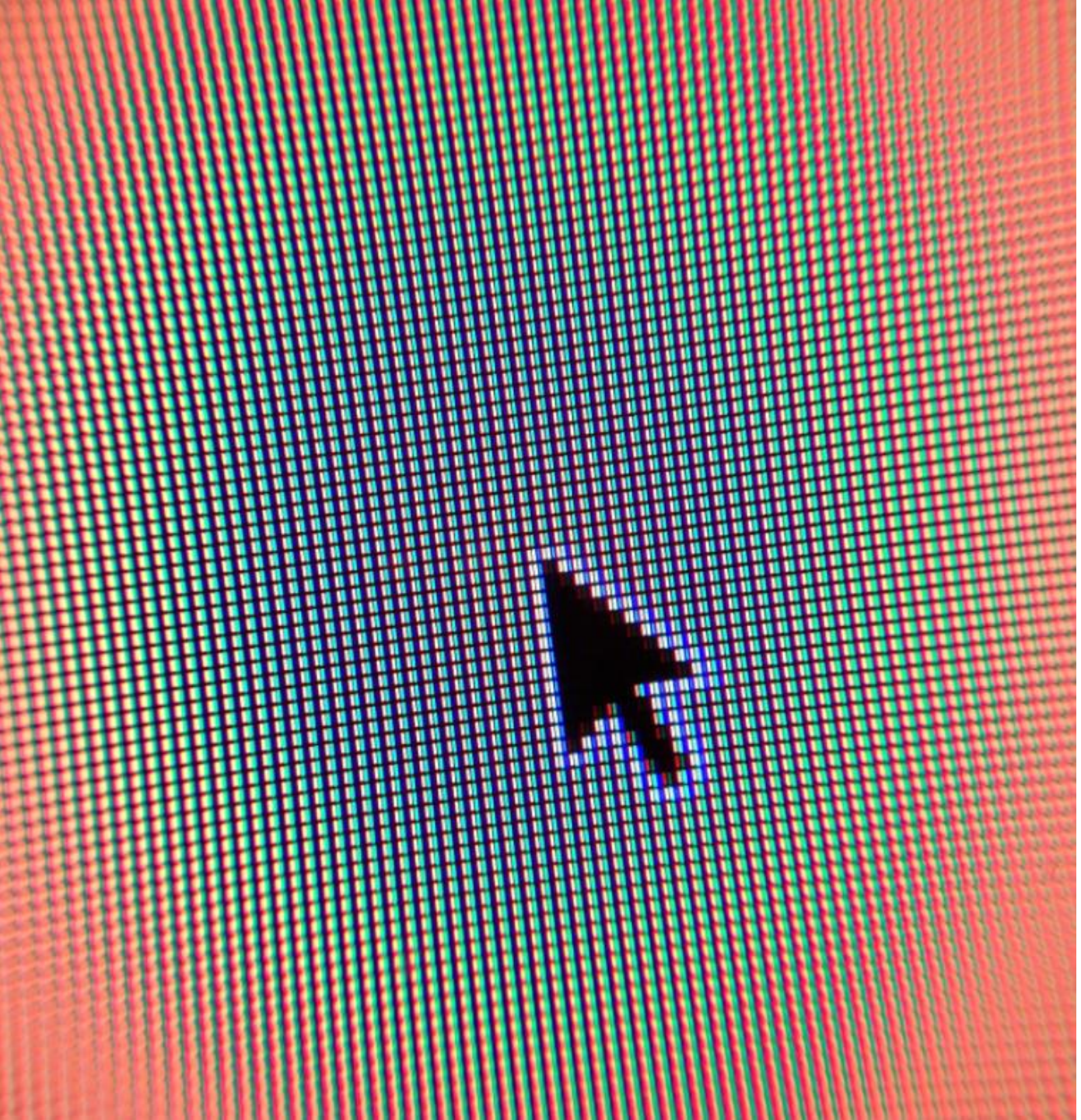
Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or internetwork)	**Internet** (internetwork)
2	Link	**Network access**
1	Physical	

THE OSI REFERENCE MODEL

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or internetwork)	**Internet** (internetwork)
2	Link	**Network access**
1	Physical	

THE OSI REFERENCE MODEL

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or internetwork)	**Internet** (internetwork)
2	Link	**Network access**
1	Physical	



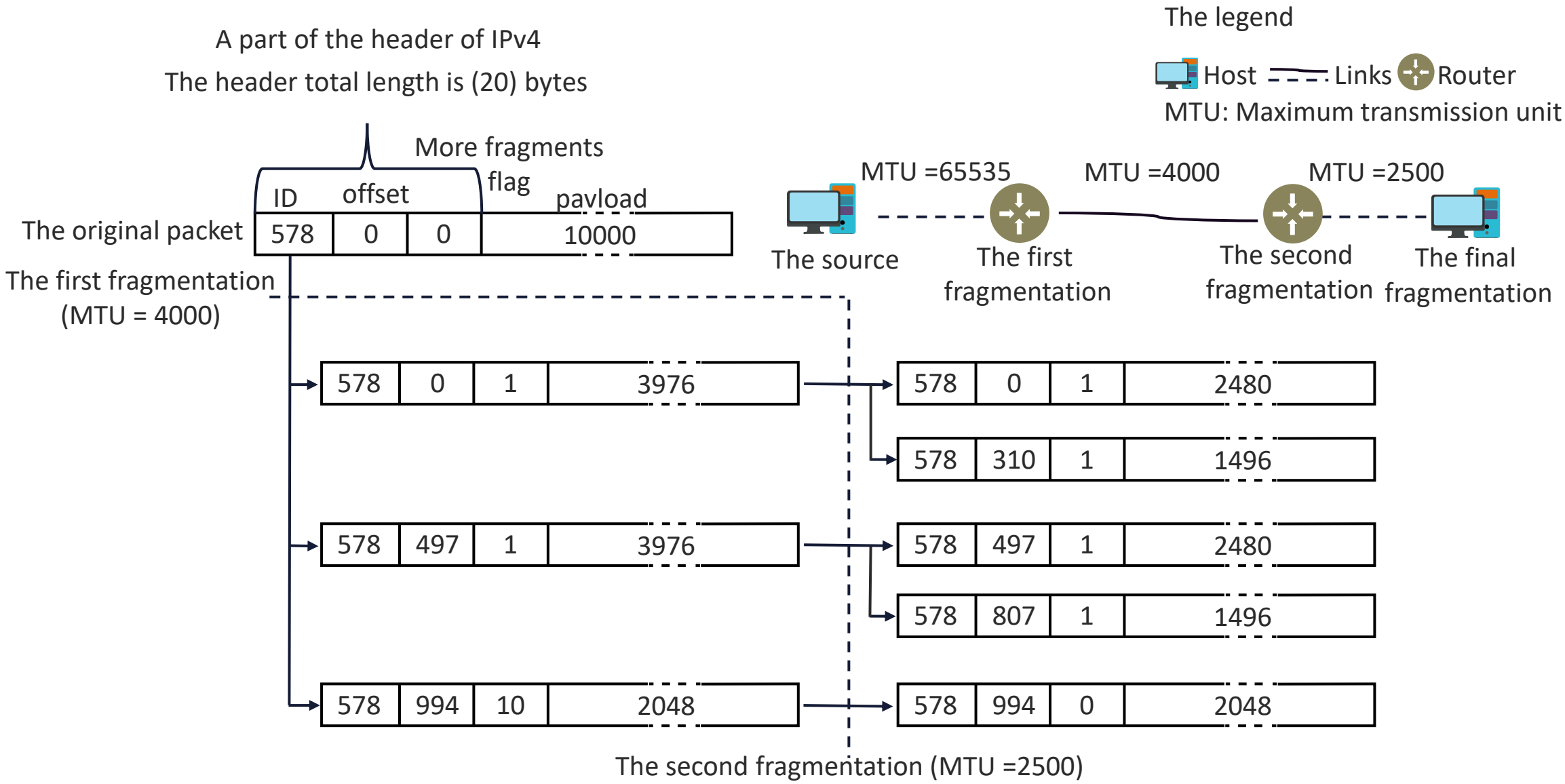
IPv4

- Internet Protocol (IP) is the core protocol of the TCP/IP suite and the main protocol of the network (internetwork) layer
- The main use is to offer internetwork datagram (packet) forwarding services to higher layer protocols and services
- Devices like routers, multilayer switches, load balancers, IPS sensors, and firewall appliances can all forward packets for IP

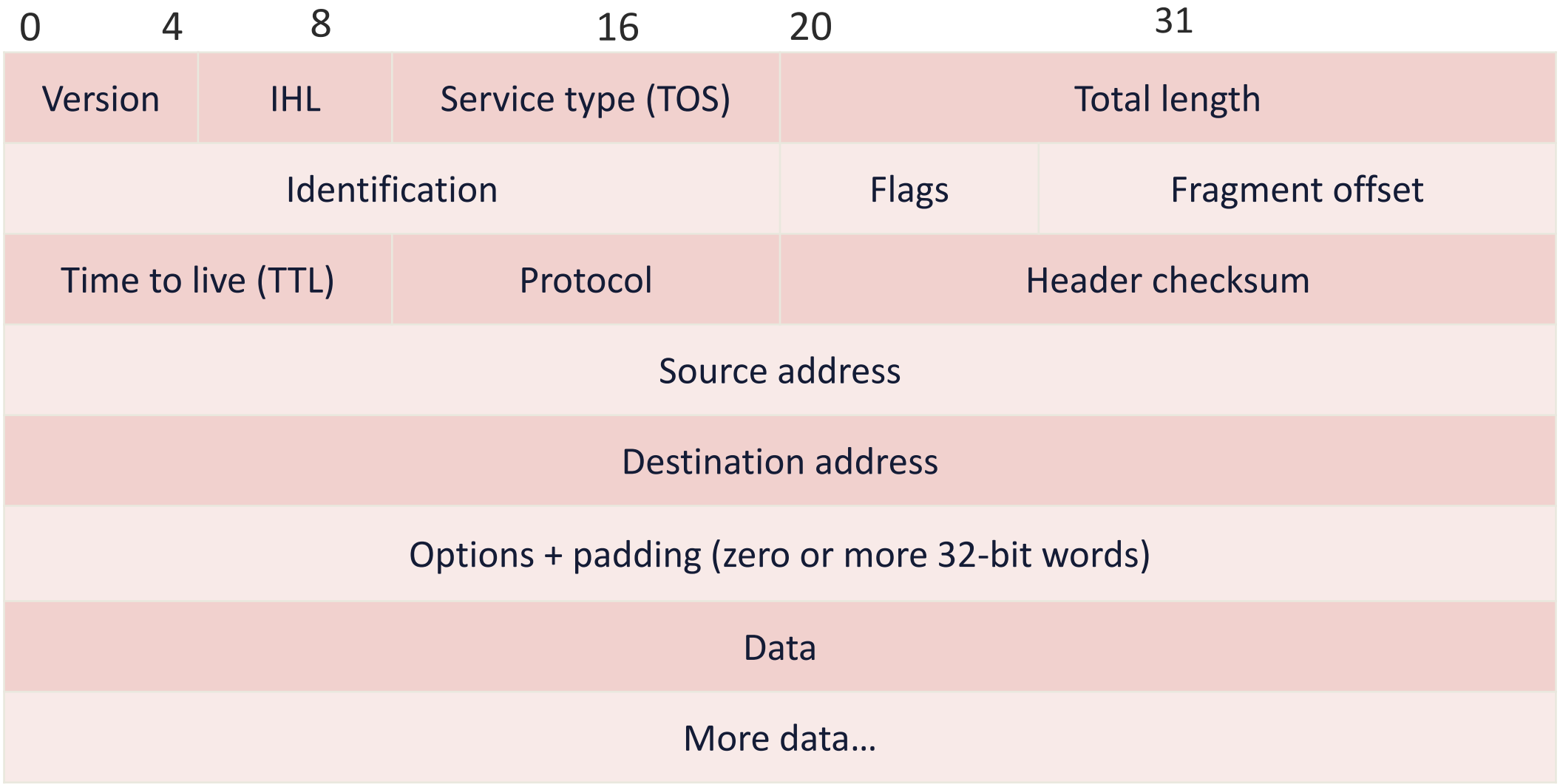
CHARACTERISTICS OF INTERNET PROTOCOL

- Universal addressing:
  - Defines addressing mechanism with IP version 4 and 6 addressing schemes
- Protocol independent:
  - Works with both the Ethernet, 802.11 wireless, frame relay, ATM, Fiber, cellular, satellite, and more
- Connectionless delivery:
  - Requires no handshake setup before transmission to remote host or persistent connection
- Unreliable and unacknowledged delivery:
  - Does not provide tracking of packets

IP PACKET FRAGMENTATION



IPv4 HEADER


0
4
8
16
20
31
Version
IHL
Service type (TOS)
Total length
Identification
Flags
Fragment offset
Time to live (TTL)
Protocol
Header checksum
Source address
Destination address
Options + padding (zero or more 32-bit words)
Data
More data…

CLASSLESS INTER-DOMAIN ROUTING (CIDR)

- Also called slash notation, it is a compact way to express an IPv4 address
- CIDR removes the predefined partitioning of network and host numbers in the IP address
- The number of network (N) bits can be arbitrarily placed without regard to the legacy classes (A-E)
- For instance: the traditional Class C address 192.168.3.15 can now be expressed as 192.168.3.15/24 or 192.168.3.15/16 or 192.168.3.15/23

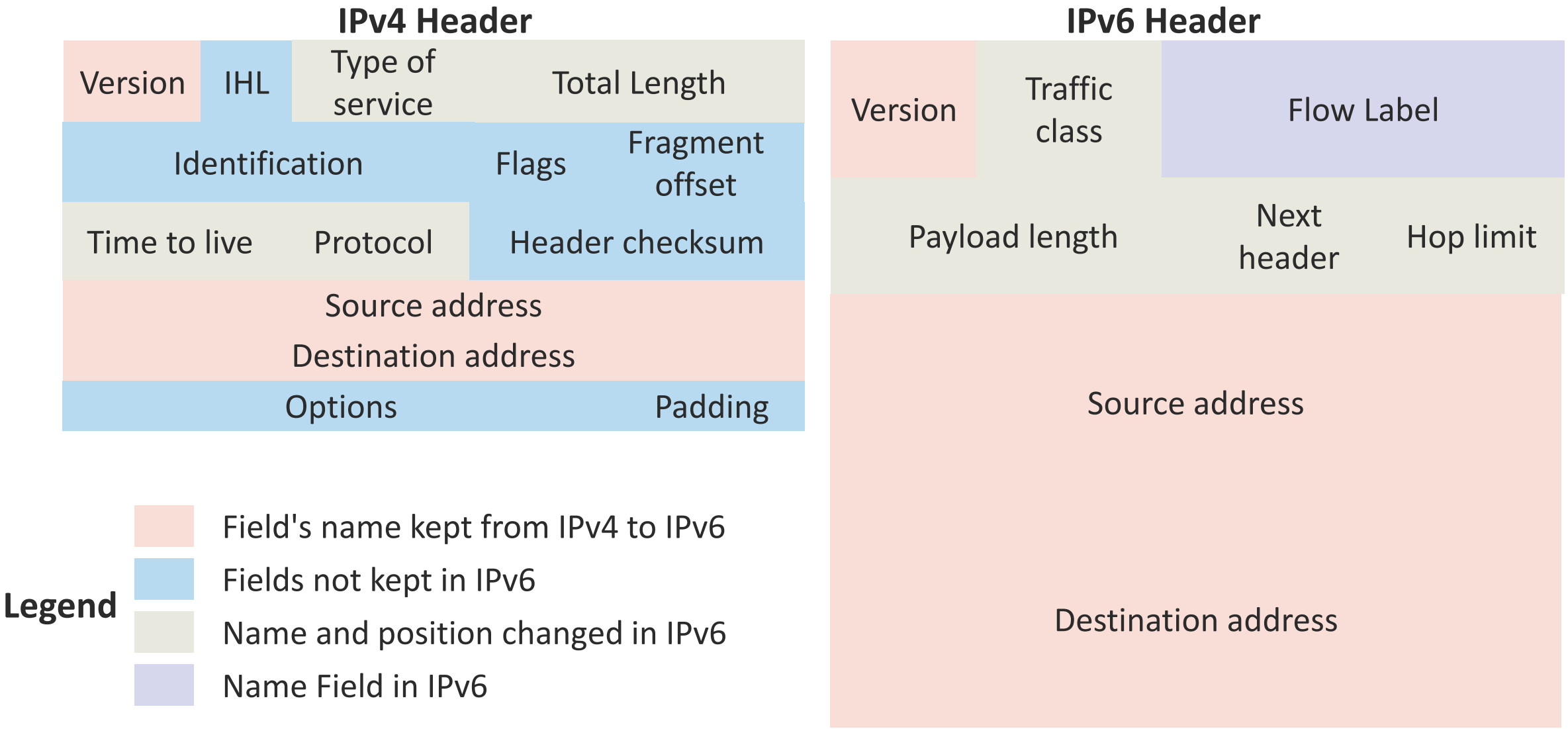
IPv6

- IPv6 was intended to supersede the widely used IPv4 which is still the backbone of modern networking
- IPv6 is often referred to as the next generation Internet due to its extended functionality and its growth in recent large-scale deployments
- It uses a 128-bit hexadecimal address instead of a 24-bit dotted decimal:
  - For example, FF02:0:0:0:0:0:0:0002 can be expressed as FF02::2

ASSIGNING AN IPv6 ADDRESS

- There are three methods for assigning IPv6 addresses:
  - Manual
  - Stateless address autoconfiguration (SLAAC):
    - Neighbor discovery locates routers and dynamically generates IPv6 addresses
    - The connected IPv6 nodes can self-configure with an IPv6 address and routing parameters without further human intervention (RFC 2462)
  - Stateful autoconfiguration (using a DHCPv6 server)

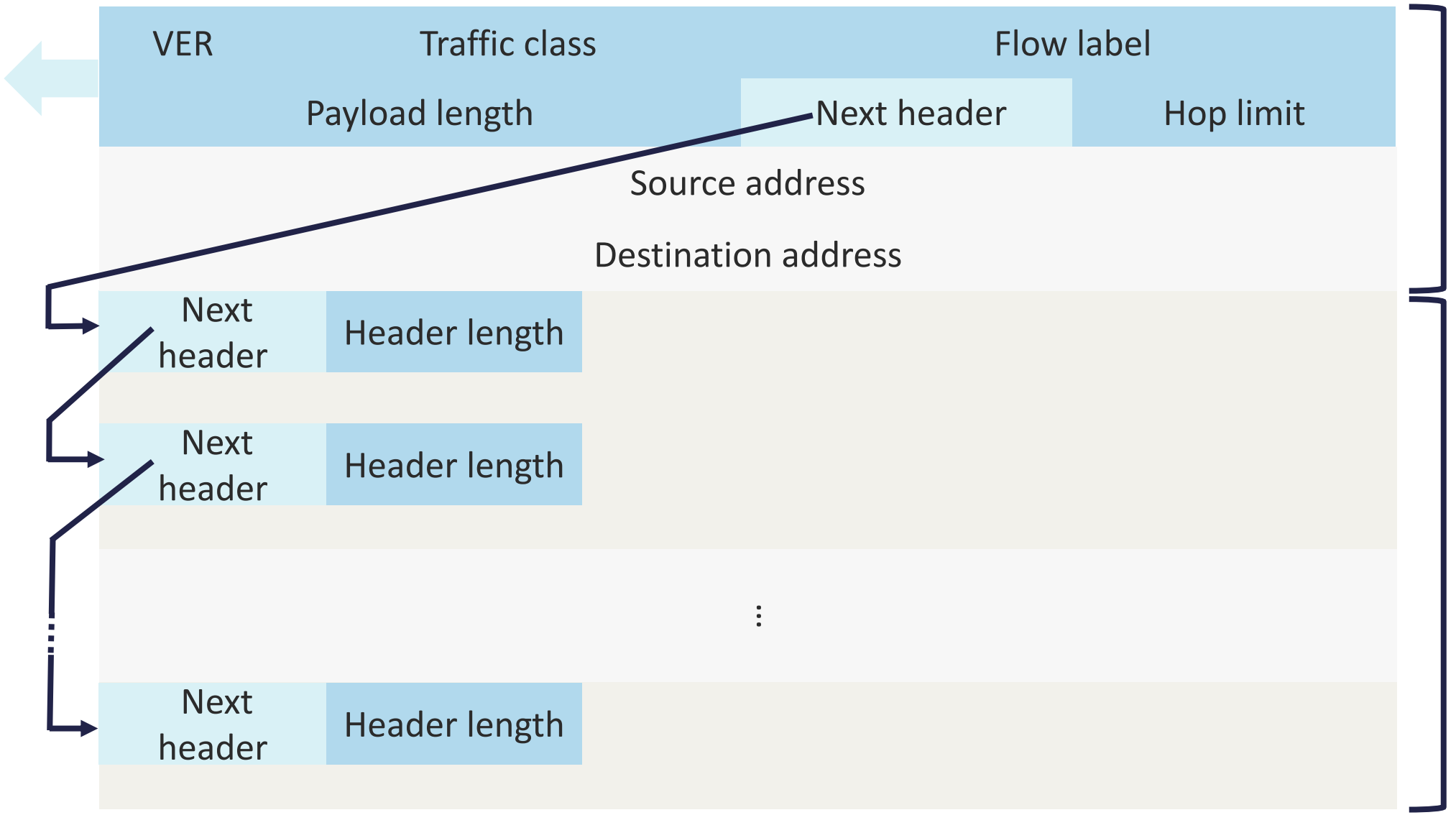
THE IPv6 HEADER



IPv6 EXTENSION HEADERS

- IPv6 uses two distinct types of headers:
  - The fixed IPv6 header
  - The IPv6 extension headers (EH)
- The extension headers, if there are any, follow the original eight fields
- The number of extension headers is not fixed, so the total length of the extension header chain is variable
- These are used to add additional functionality and extensibility to the protocol

IPV6 EXTENSION HEADERS



IPv6 EXTENSION HEADERS

- Authentication EH and Encapsulating Security Payload (ESP) are for native IPsec
- The fragmentation EH is critical
- Hop-by-hop EH is used for the support of jumbo-grams
- Destination EH is used in IPv6 mobility
- Routing EH is used in IPv6 mobility and in source routing
- Mobility EH is used in support of mobile IPv6 services

Version 4	Version 6
2^{32} address space	2^{128} address space
Dotted decimal format	Hexadecimal notation
DHCP dynamic addressing	SLAAC and DHCPv6
Header has 20 bytes and 13 fields	Header has 40 bytes and 8 fields
Variable header length	Fixed header length
Header options (obsolete)	Header extensions
Header checksum	No header checksum

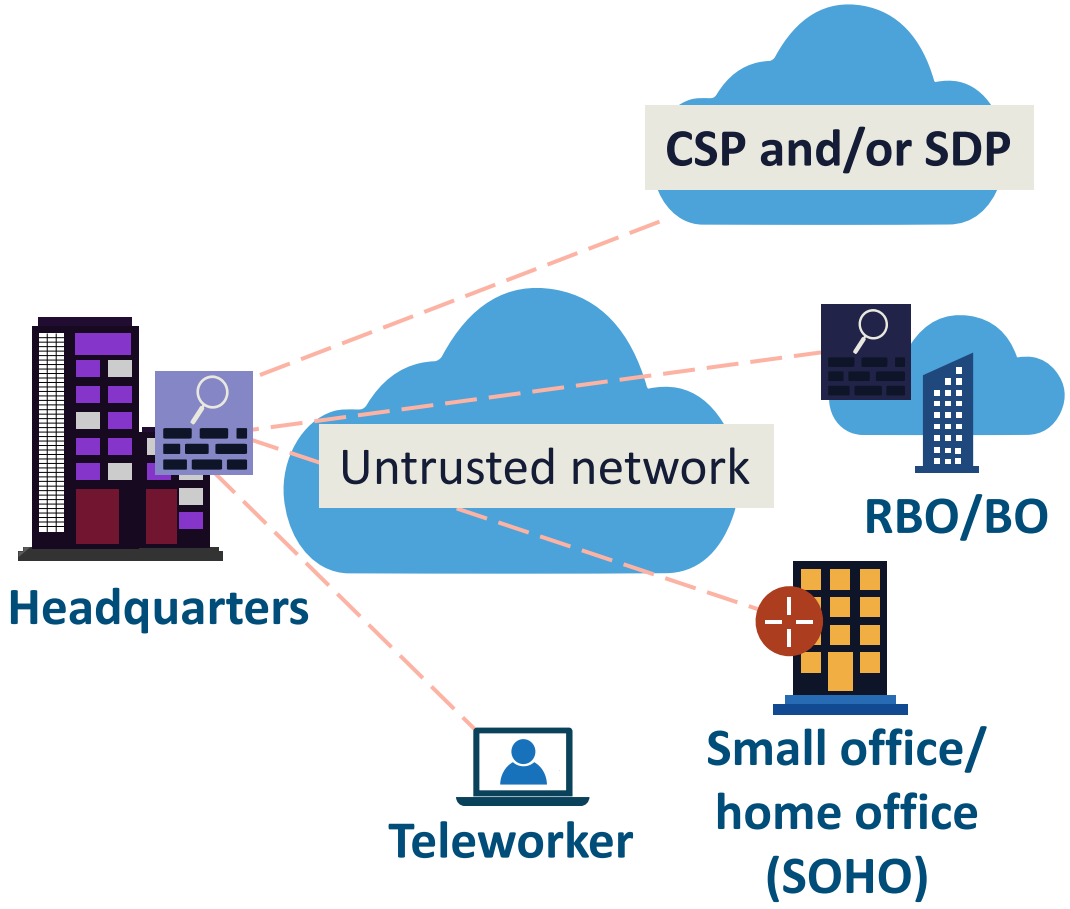
Version 4	Version 6
Packet size: 576 bytes are required, fragmentation optional	Packet size: 1280 bytes required without fragmentation
Packet fragmentation: Routers and sending hosts	Packet fragmentation: Sending hosts only
IPv4 was never designed to be secure	Has native encryption and authentication
IPsec optional	IPsec mandatory
Non-equal geographical distribution (>50% USA)	No geographic limitations

IP SECURITY (IPsec)

- IPsec offers security services to traffic transiting untrusted networks, like the Internet, between two or more trusted devices or networks
- IPsec VPNs can also be used to protect management traffic as it crosses an organization's intranet and between front-end and back-end services
- IPsec is also popular for linking to cloud service providers (CSPs) using managed site-to-site and peer-to-site VPN solutions
- IPsec is also native to the IPv6 stack through the Authentication Header (AH) and ESP extension headers

IPsec

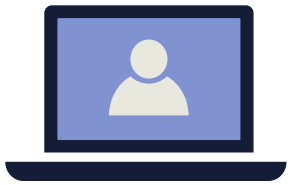
- IPsec (and TLS) VPNs are cryptographic-based
- There are two basic deployment types, site-to-site VPNs and remote-access VPNs:
  - Remote access can be full-tunnel or clientless
  - Can operate in tunnel or transport modes
- The two main protocols are AH and ESP
- IPsec offers five essential security functions:
  - Confidentiality (3DES, AES-128/256)
  - Data integrity (SHA1, SHA2, SHA384)
  - Origin authentication using pre-shared keys or RSA/DSA/ECDSA signatures
  - Key management (IKEv1/2, and DHKE, ECDHE)
  - Anti-replay protection



TRANSPORT LAYER SECURITY (TLS)

- SSL/TLS is the most universal certificate-based peer authentication in use on the Internet (HTTPS)
- Transport Layer Security is the next-generation standardized by the Internet Engineering Task Force (IETF)
- TLS 1.3 is the most recent published version
- It is also used with, FTP, SMTP, LDAP, and POP3 among others
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures

TLS HANDSHAKE



TLS VPN tunnel

1 User makes a connection to TCP port 443

2 The server response contains server's public key

3 User software verifies signature on identity certificate, validating authenticity of public key

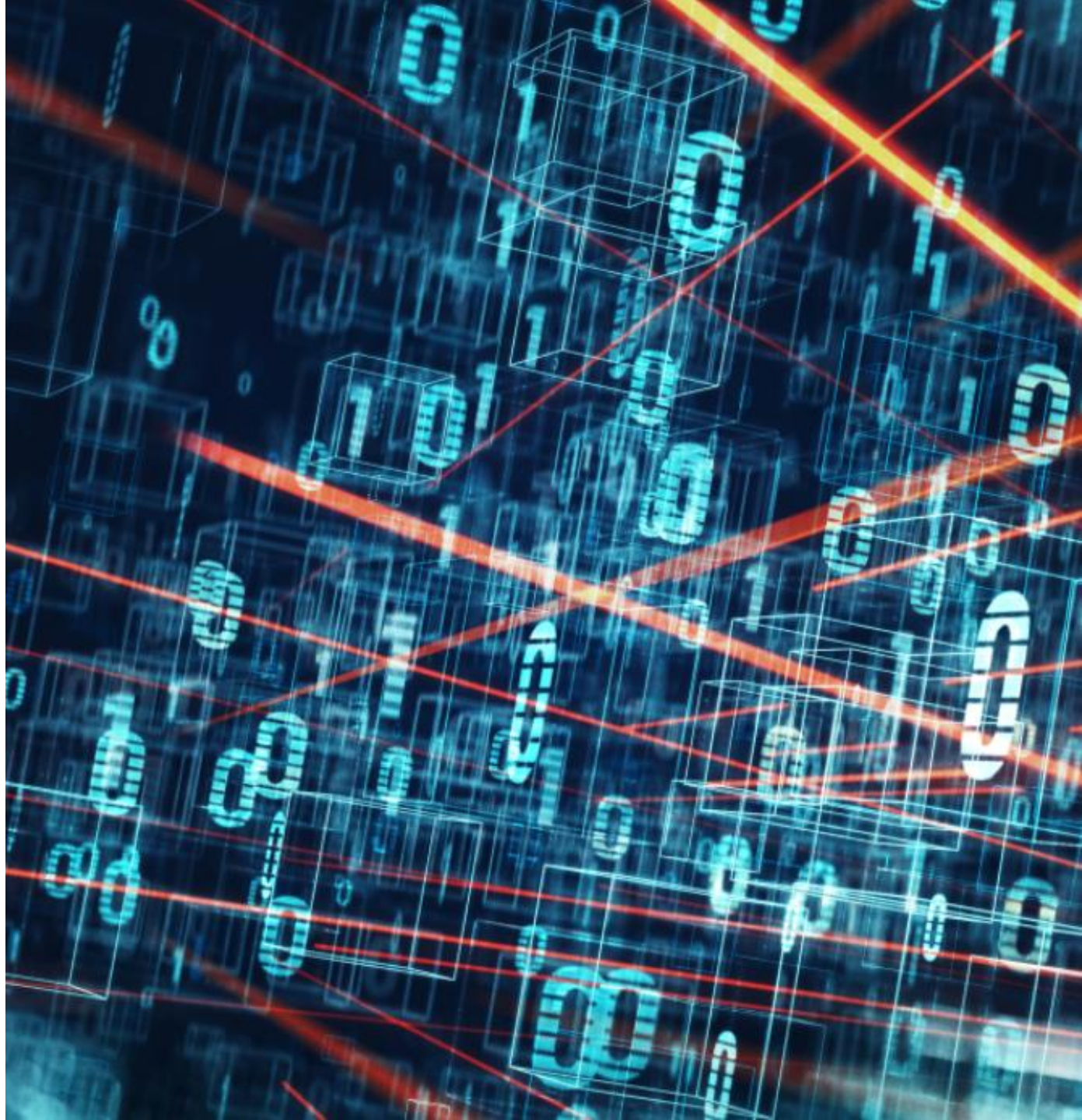
4 User software creates a shared-secret key

5 Shared-secret key, encrypted with public key of the server, is sent to the server

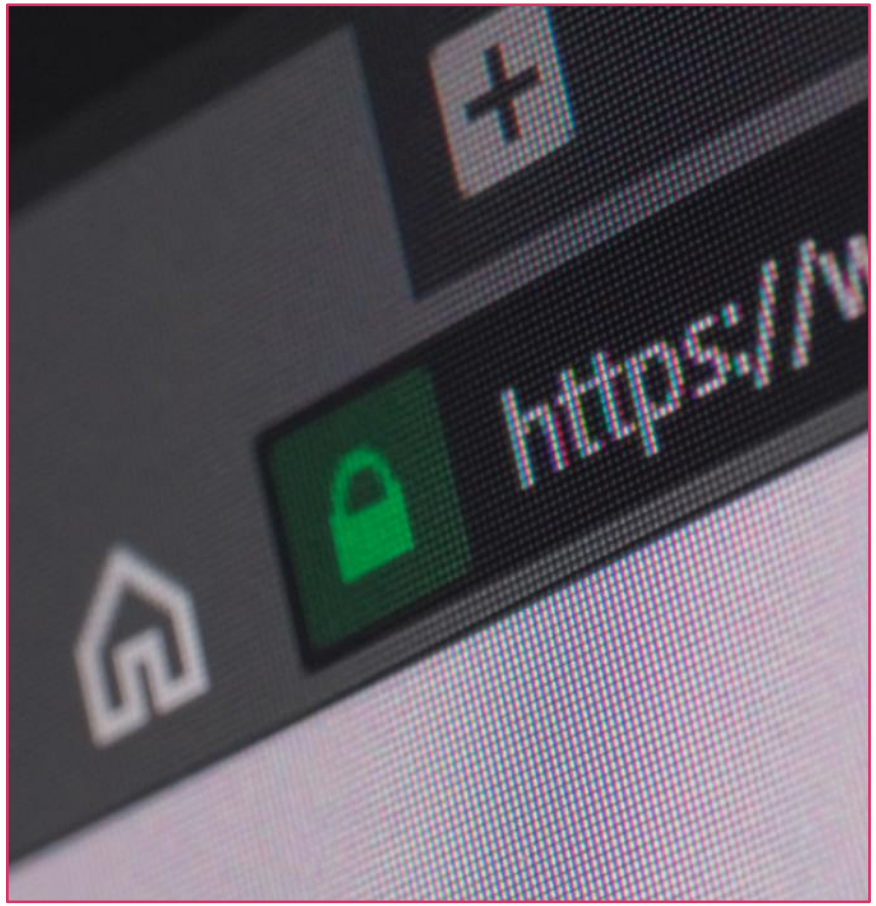
6 Bulk encryption occurs using the shared-secret key with a symmetric encryption algorithm

SINGLE PACKET AUTHORIZATION (SPA)

- SPA (aka port knocking), is a technique for securely establishing authentication and authorization over closed firewall ports
- It usually accomplishes opening specific ports to allow temporary access through Internet or cloud controllers
- With SPA, the endpoint sends a single packet of encrypted data to the authentication server (TLS)
- The TLS server then uses a unique algorithm to decode the packet containing the user's identity and request for access



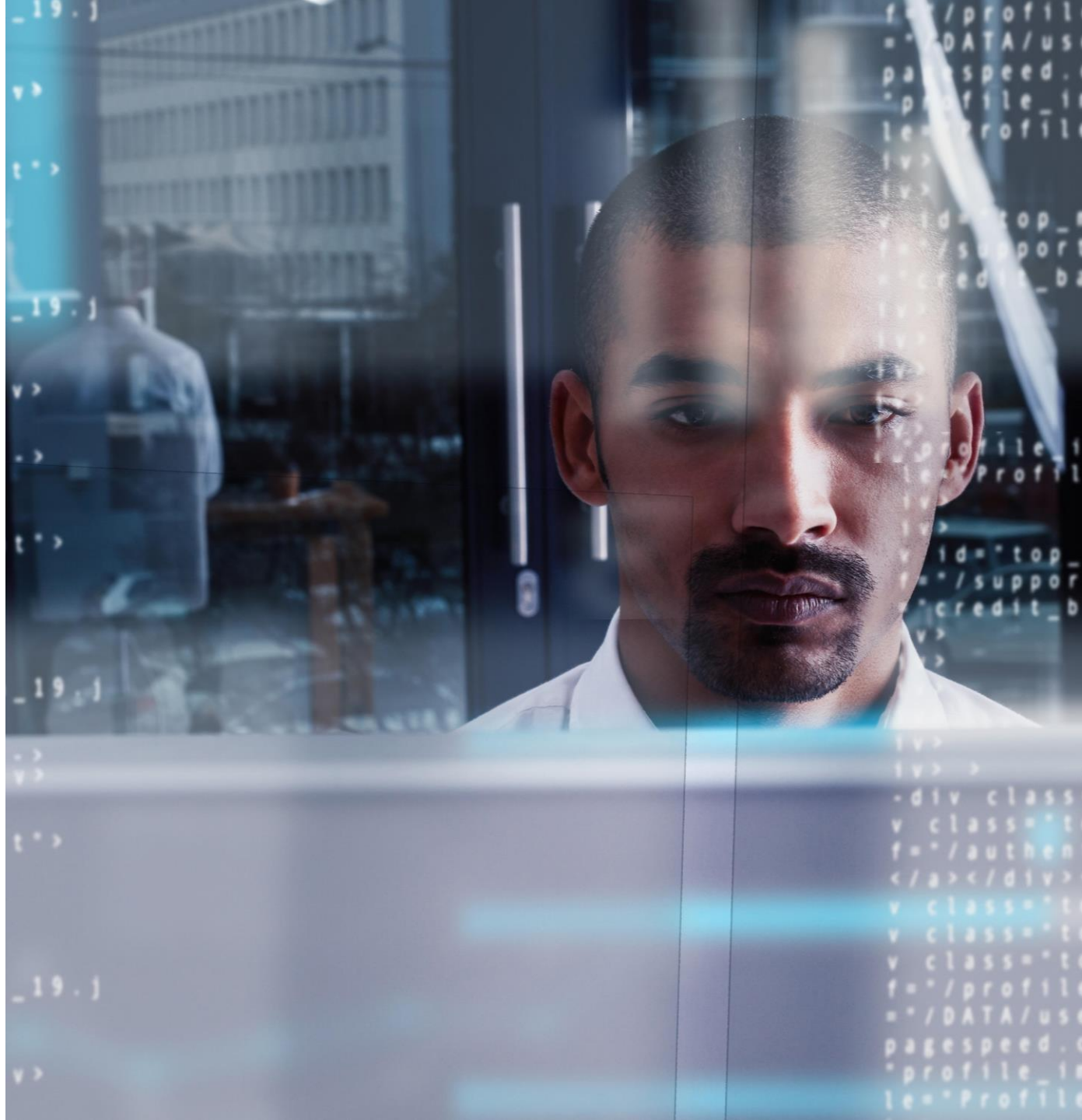
SINGLE PACKET AUTHORIZATION (SPA)



- Mutual Transport Layer Security (mTLS) is a form of authentication in which the two parties in a communication channel authenticate one other with TLS
- mTLS affirms that the parties on each end (a browser and software-defined perimeter [SDP] controller, for example) are who they claim to be by verifying that they both have the proper private key
- The data within their respective TLS certificates provides additional verification
- It is often used with SDPs in a Zero Trust security framework to verify application programming interfaces (APIs), users, devices, and servers within an organization without the overhead and hazards of an initial TCP handshake

TLS BEST PRACTICES

- Prevent downgrade attacks from web clients
- Use HTTP Strict Transport Security (HSTS)
- Use the most recent security suites (no RC4 or DES/3DES)
- Do not let vendor-installed code intercept traffic
- Verify encryption and use SPA with mTLS whenever possible
- Perform Online Certificate Status Protocol (OCSP) stapling from browsers to enforce certificate expirations
- Implement certificate pinning to trusted CAs



SECURE SHELL (SSH)

- Management access should be limited to secure protocol alternatives, as in SSH instead of Telnet
- SSH2 is preferable to SSH1 whenever possible
- SSH2 uses symmetric encryption for the bulk data encryption and asymmetric algorithms in their key management processes
- SSH2 uses Diffie-Hellman (DH) for key exchange

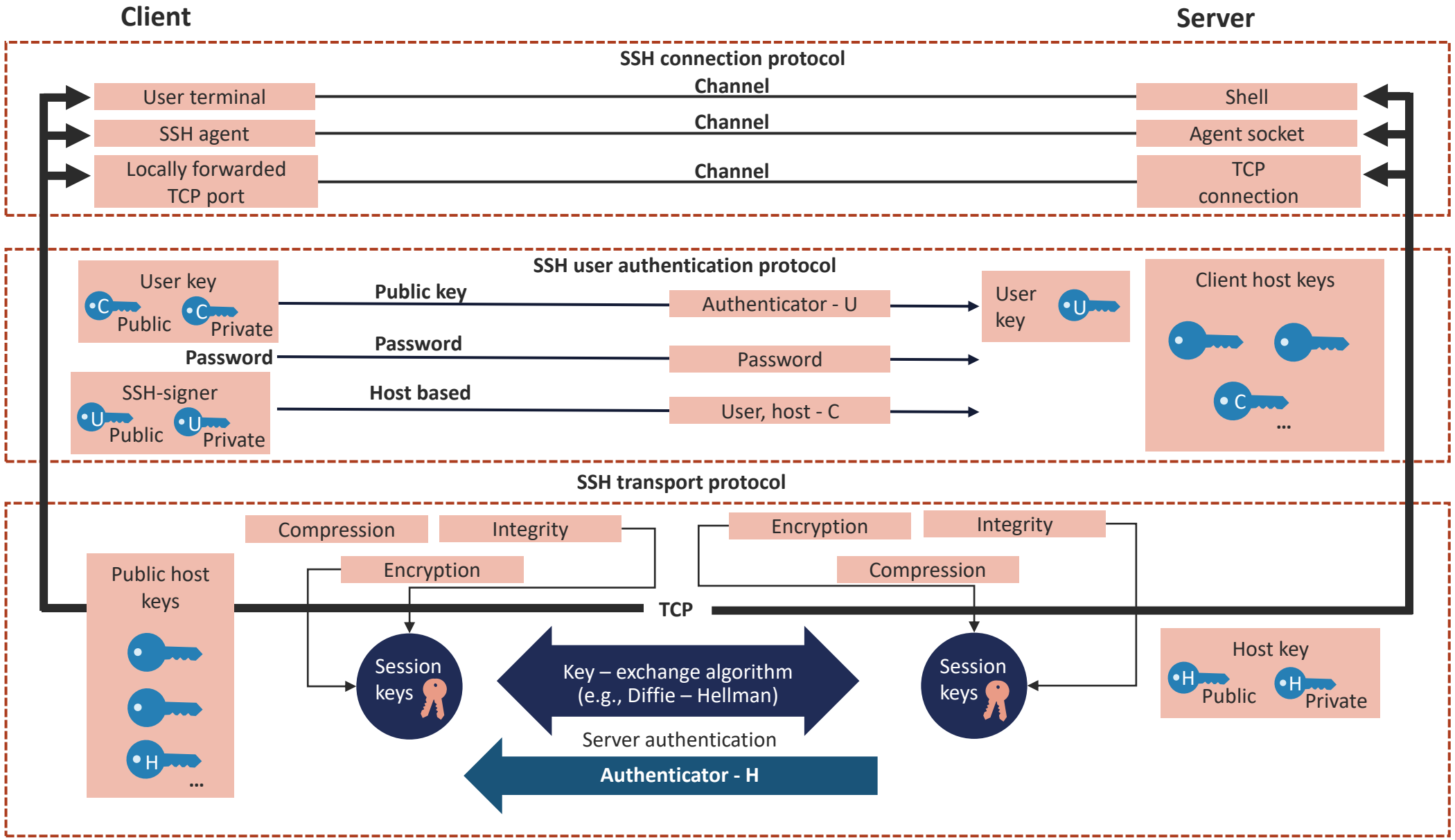
SSH2 CONFIGURATION

```
Router(config)#hostname CISSP-R1

CISSP-R1(config)#ip domain-name
example.com

CISSP-R1(config)#crypto key generate ecdsa
general-keys modulus 2048

The name for the keys will be: CISSP-
R1.example.com

% The key modulus size is 2048 bits

% Generating 2048 bit RSA keys, keys will
be non-exportable…

  [OK](elapsed time was 0 seconds)

*Apr 9 24:01:50.517: %SSH-5-ENABLED: SSH
1.99 has been enabled
```

SSH2 CONFIGURATION

```
CISSP-R1(config)#username admin secret
C!55PS3cur!Ty
CISSP-R1(config)#line vty 0 15
CISSP-R1(config-line)#login local
CISSP-R1(config-line)#transport input ssh2
```

SSH2 PROCESS



MULTILAYER PROTOCOLS

- Multilayer protocols structure network communications into separate logical layers, each with a designated function
- This facilitates flexibility and security in network operations
- The most common multilayer protocol that security professionals encounter is the TCP/IP suite of network protocols

MULTILAYER PROTOCOLS

- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) was a popular multilayer routed protocol created by Novell
- Intermediate System to Intermediate System (IS-IS) is a multilayer routing protocol still used in modern datacenter VXLAN environments (Cisco ACI)
- The Distributed Network Protocol or DNP3 is a set of networking protocols created explicitly for Supervisory Control And Data Acquisition (SCADA) systems
- The Extensible Authentication Protocol (EAP) is a protocol for wireless (and wired) networks that expands the authentication methods used by the Point-to-Point Protocol (PPP)

CONVERGED PROTOCOLS

- Converged protocols merge specialty or proprietary protocols with standard protocols
- Common examples of converged protocols include Fiber Channel over Ethernet (FCoE), Multiprotocol Label Switching (MPLS), Internet Small Computer System Interface (iSCSI), and Voice over Internet Protocol (VoIP)
- The main advantage of converged protocols is the ability to use existing TCP/IP supporting network infrastructure to host special or proprietary services without the need for additional networking hardware

INTERNET SMALL COMPUTER SYSTEMS INTERFACE iSCSI

- iSCSI is a storage transport protocol that gives client devices access to block-level (HDD and SDD volumes) storage components using Ethernet
- Along with Fiber Channel, iSCSI is often utilized for storage area networks (SANs) and other shared networks or dedicated storage
- It does not file access solutions like network attached storage (NAS) or object storage solutions, which use different transport protocols

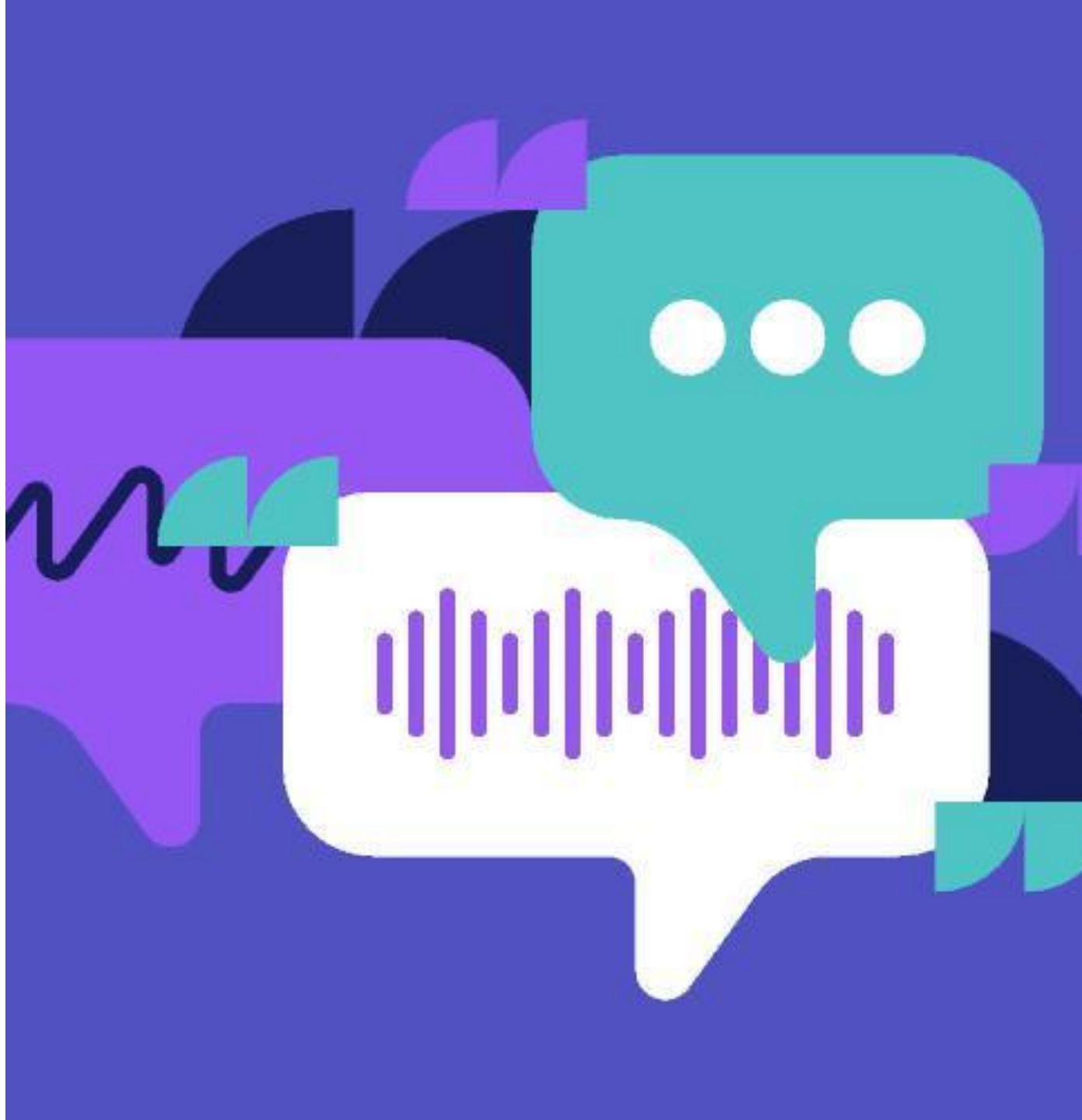
SECURING iSCSI

iSCSI is secured using the same mechanisms to protect other TCP/IP-based networks:

- Run it on a dedicated switch fabric and private VLAN (PVLAN)
- Detect packet sniffers and scanning tools
- Use IPsec Authentication Header
- Use 802.1AE MACsec with AES-256/GMAC
- Move to an SDN and software-defined security (Zero Trust) environment:
  - Require the host, or initiator, to authenticate to the iSCSI device, or target, with a digitally signed certificate whenever it tries to access data on the target logical unit number (LUN), a numbered disk drive

VOICE OVER INTERNET PROTOCOL (VoIP)

- A VoIP system uses a computer, smartphone, VoIP phone, or WebRTC-enabled browser to make telephone calls and transfer data
- Instead of a traditional landline, VoIP typically uses a broadband Internet connection to transmit data that is transformed from the original analog data into digitized packets
- Solutions offer many features such as automated attendant with interactive voice response (IVR), caller ID, holding with music on hold, queuing, custom ring back, hot desking, call flipping, conferencing, recording, and transcription among others



SECURING VoIP

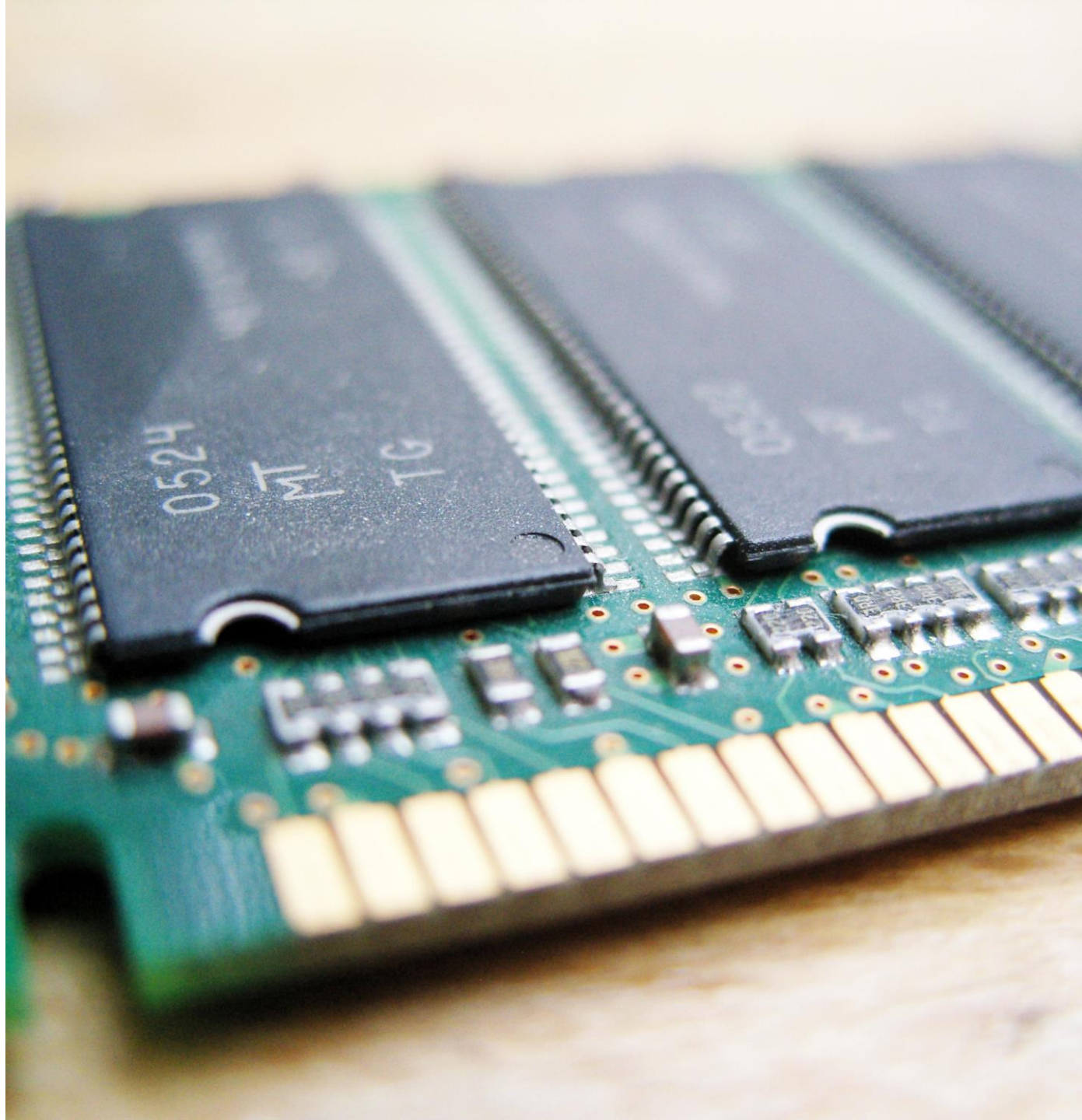
- Unified threat management (UTM) – deploying security infrastructure that protects all traffic and not just common data transport
- Call encryption utilizing WebRTC technology and Secure Real-time Transport Protocol (SRTP) for encryption and authentication
- Reliance on TLS protocols to hide information like usernames and phone numbers
- Two-factor authentication (2FA) to mitigate brute-force attacks
- Employee acceptable use training

INFINIBAND OVER ETHERNET (IBoE)

- IBoE or RDMA over Converged Ethernet (RoCE) is a network protocol that enables remote direct memory access (RDMA) over an Ethernet network:
  - RDMA involves the access of memory of one system by another in a network without involving either one's operating system, processor, or cache
- IBoE encapsulates an InfiniBand (IB) transport packet over Ethernet:
  - There are two RoCE versions, RoCE v1 and RoCE v21
- Media Access Control Security (MACsec) frame protection is popular with supporting switch infrastructure

COMPUTE EXPRESS LINK (CXL)

- CXL is a cache-coherent open interconnect standard for high-speed CPU connection to memory and other devices
- It leverages the standard Peripheral Component Interconnect Express (PCIe) physical layer but uses a supported alternate protocol
- By creating a common memory space for connected devices, the CXL standard brings performance advantages for hyper-scaling and other advanced applications
- CXL utilizes a flexible processor port that can operate in either PCIe or CXL modes
- Homomorphic encryption works well here

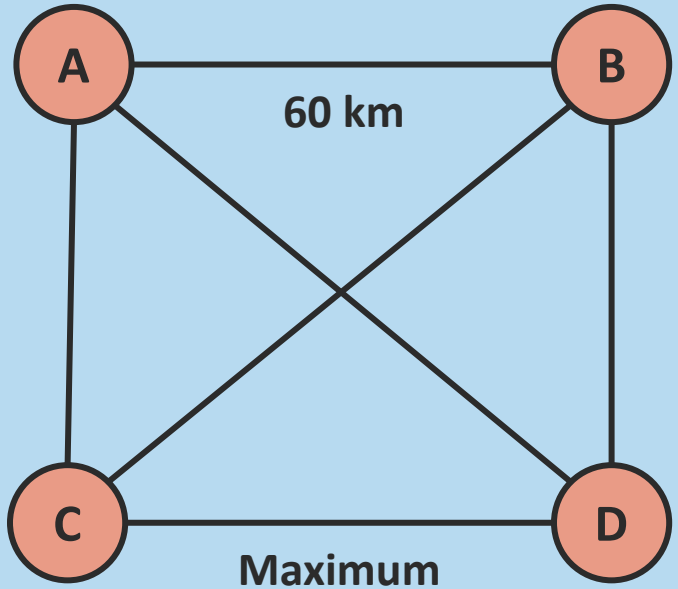


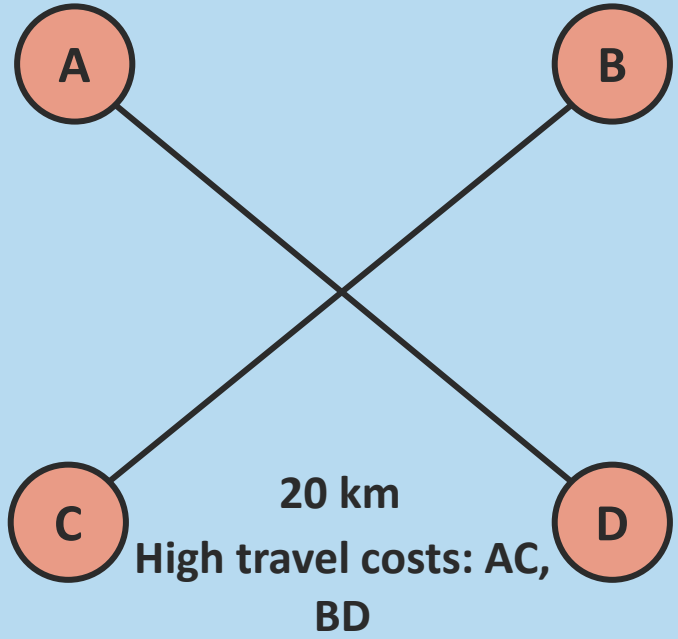
HOMOMORPHIC ENCRYPTION

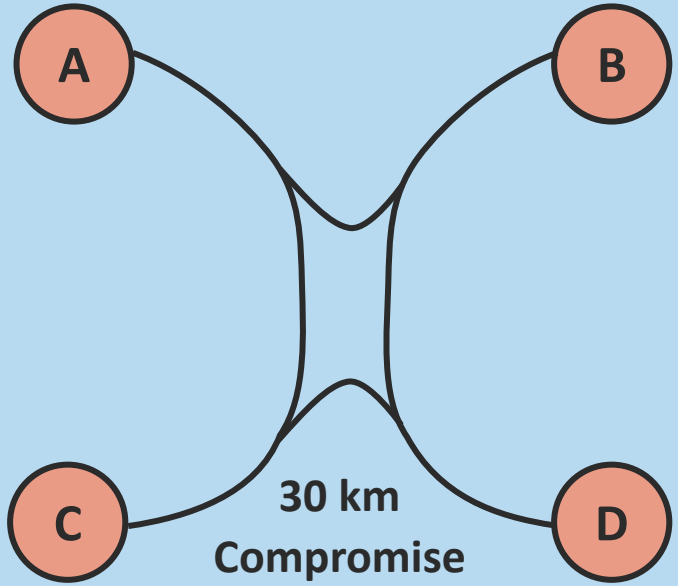
- Fully homomorphic encryption (FHE) is an innovative technique for achieving Zero Trust on untrusted or shared domains without needing to decrypt it
- It leverages algebraic functions and a symmetric key cryptosystem to securely access data while keeping it encrypted
- It is valuable in environments where data is being shared by analysts in hybrid cloud deployments or shared enclaves (AWS Nitro) in the cloud

DATA FLOW MODELS: IN THE CLOUD

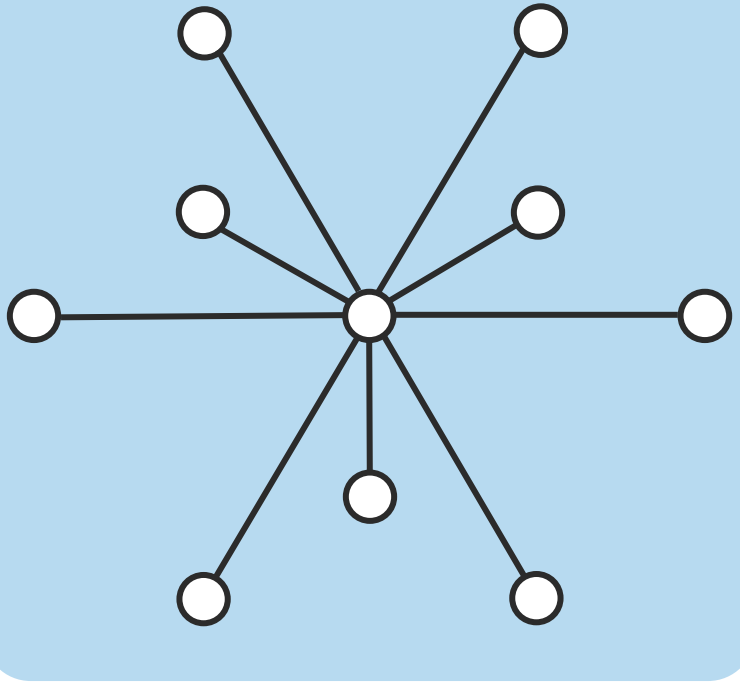
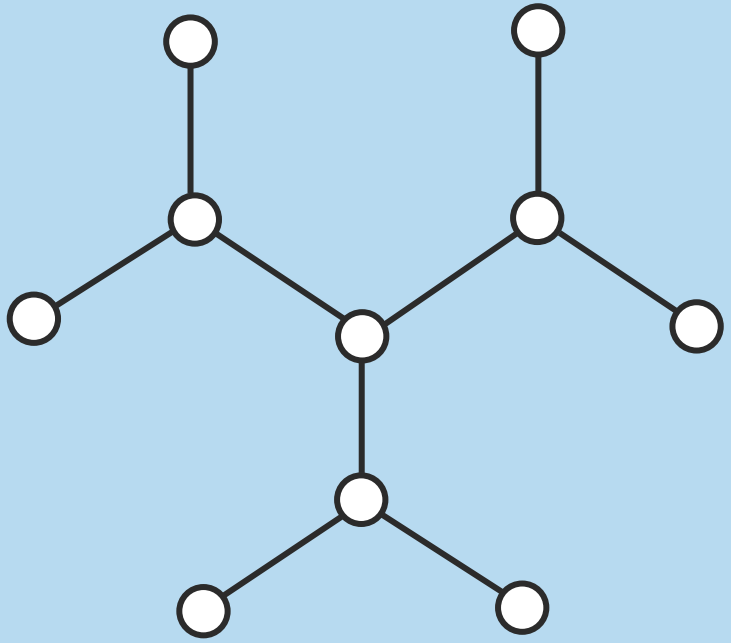
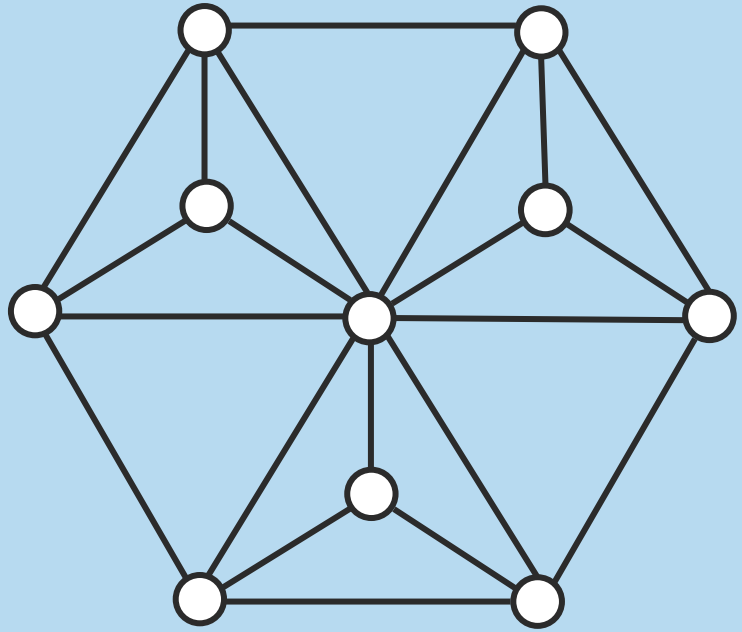
Least cost to use	Least cost to build	Hybrid





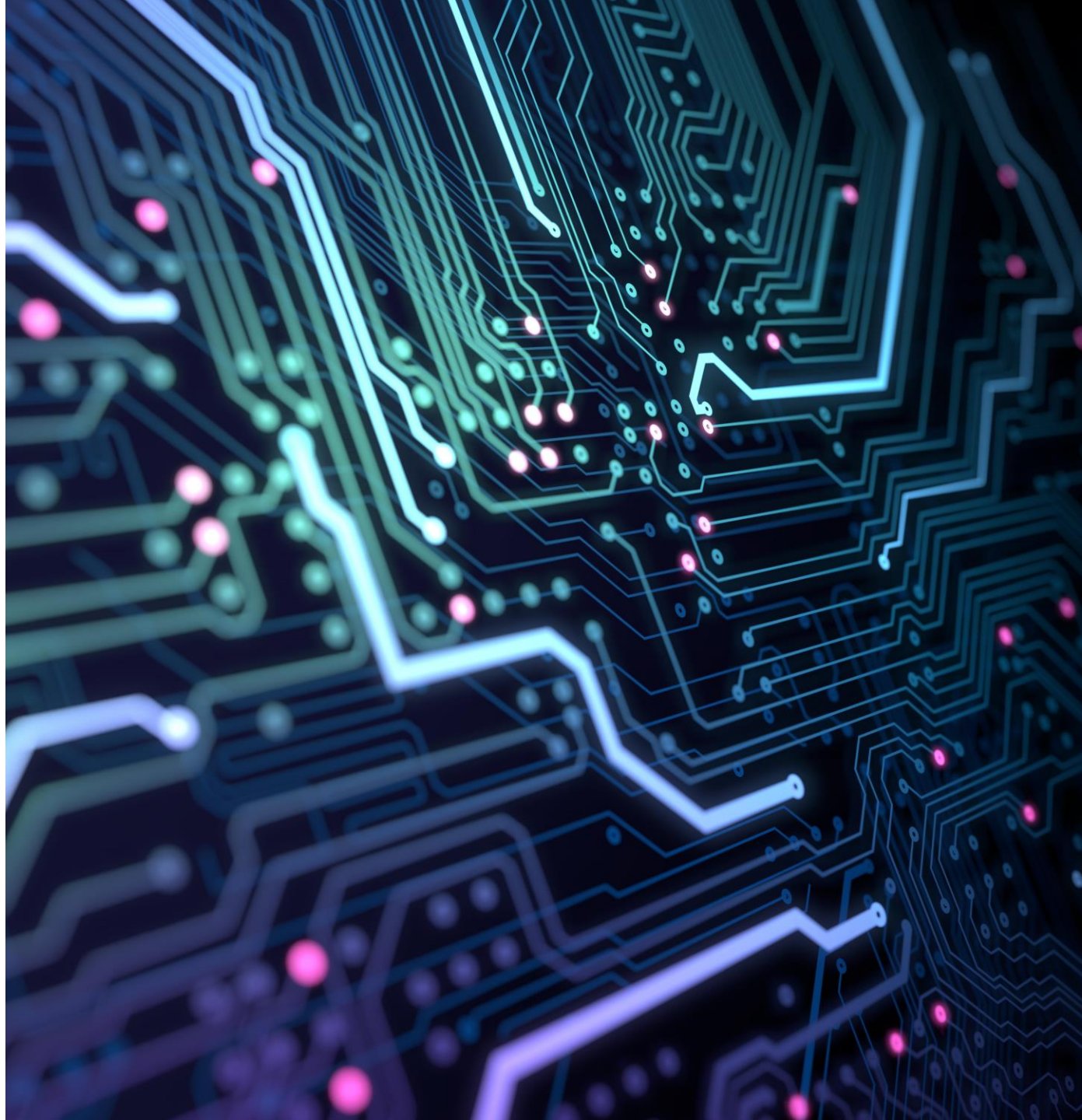


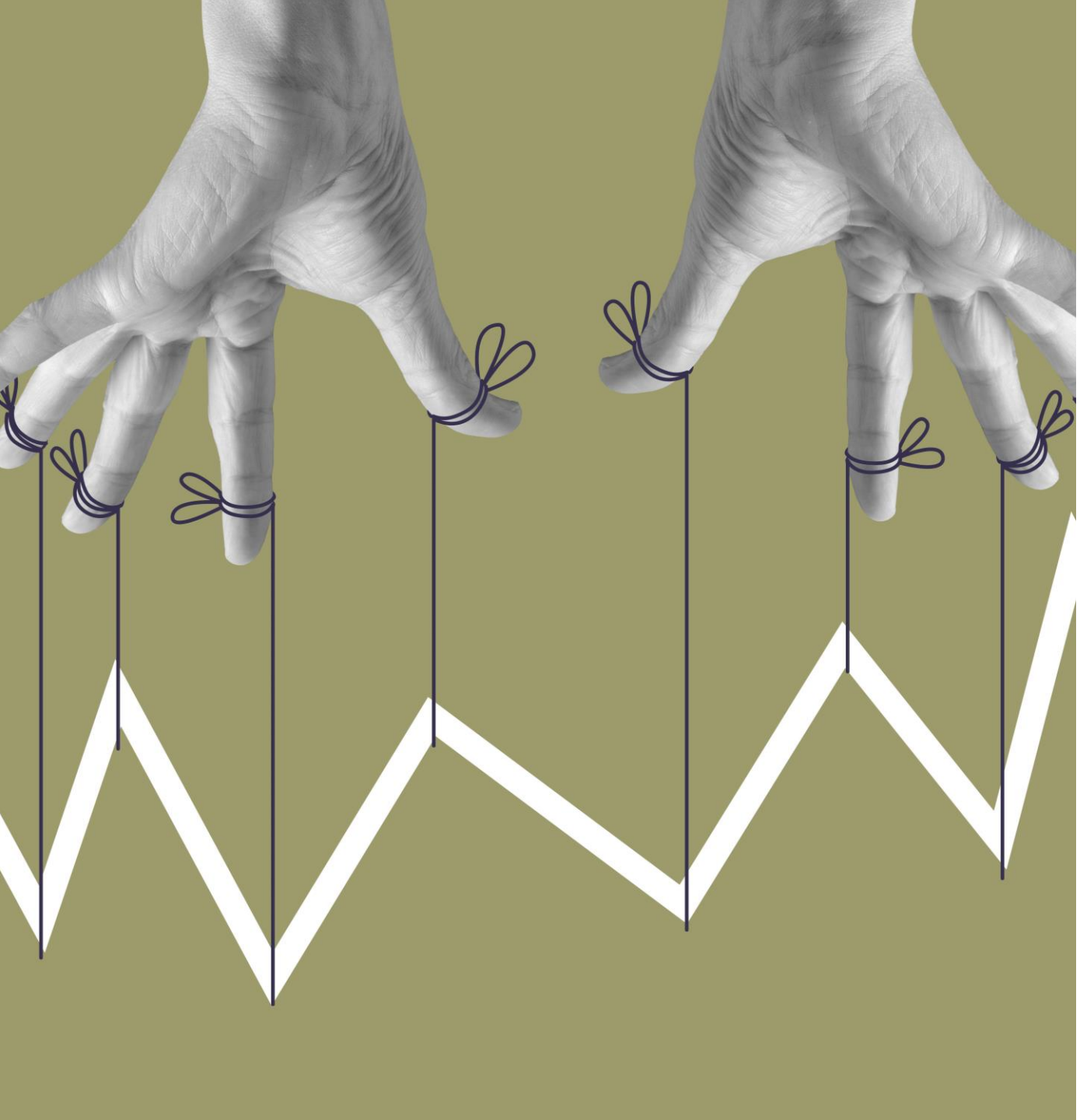
TRANSPORT ARCHITECTURES

Centralized	Decentralized	Distributed
		

DATA PLANE

- In networking, a plane is an abstract term that simply describes where processes take place, as in a plane of existence
- The data plane is the process mechanism that forwards the packetized frames therefore it is also called the forwarding plane
- It is also referred to as the user plane, carrier plane, or bearer plane since it is the component of a network that conveys user traffic
- This plane must have protections for data-in-transit and data-in-use



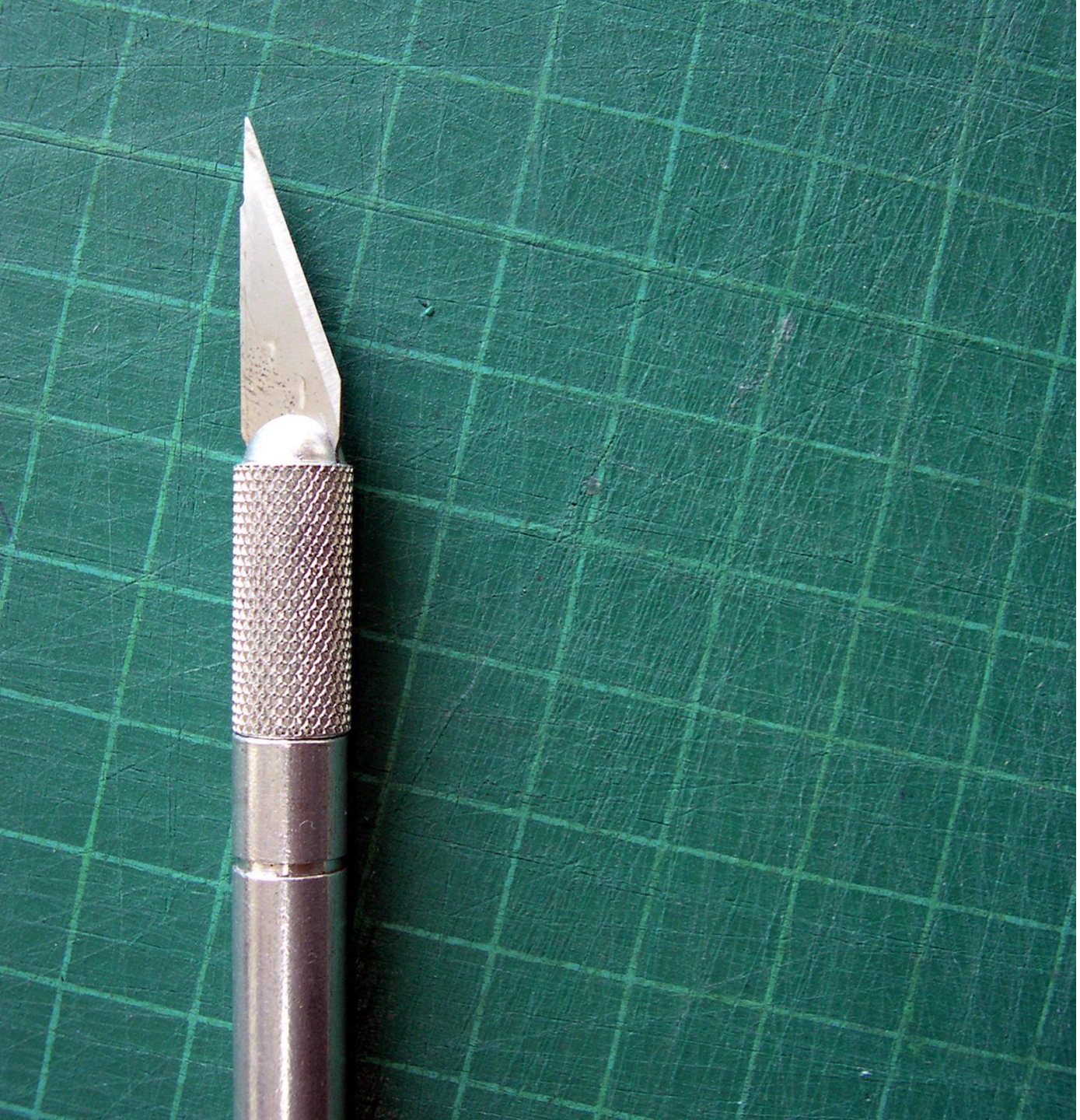


CONTROL PLANE

- The control plane is the aspect of a network that manages HOW data packets are forwarded
- This is typically accomplished using a static routing table or dynamic routing protocol like Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF)
- This plane is protected with
  - Control Plane Protection on individual infrastructure devices like switches, multilayer switches, routers, gateways, wireless controllers, firewalls, and IPS sensors
  - Hashed Message Authentication Codes (Sha-2/3
  - MACsec with GMACs

MANAGEMENT PLANE

- The management plane is responsible for the supervision and monitoring of all wired and wireless network operations
- This is where all connected devices are securely configured and operated using optimal due diligence and due care
- This plane is also responsible for software and firmware updates, security, and visibility
- Common solutions on this plane are SNMPv3, NTPv3, IaC, NetFlow v9, SDN, and security information and event management (SIEM)/ security orchestration, automation, and response (SOAR) systems to name a few

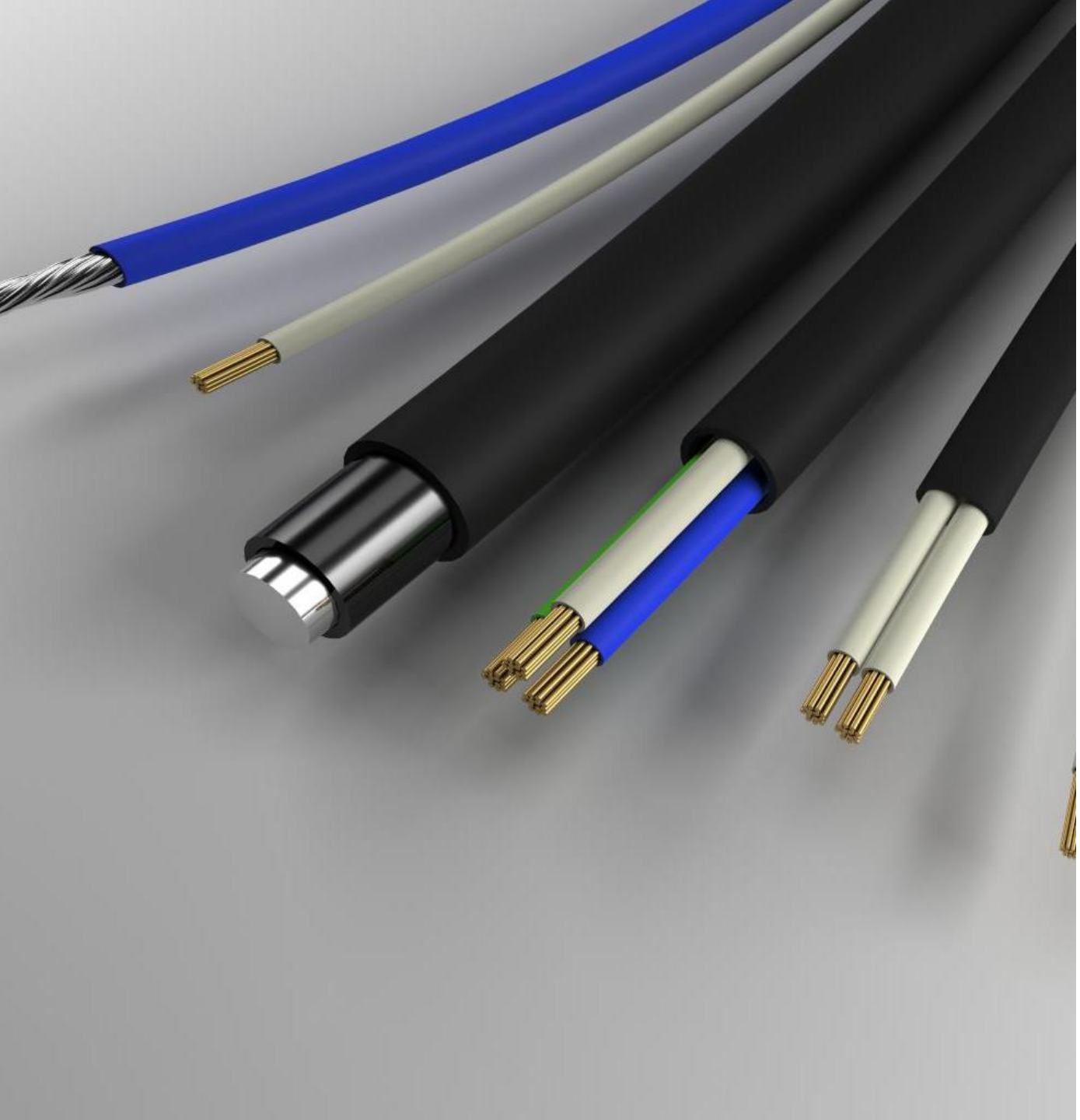


CUT-THROUGH SWITCHING AND ROUTING

- Cut-through is a packet-switching method, where the switch, router, or gateway forwards the packet as soon as the destination address is processed
- The device does not wait for the entire datagram to be received, but rather only a fraction of the frame or packet
- The next packet is sent as soon as the previous one has been confirmed as reaching the target without waiting for the complete transmission of the previous packet

STORE AND FORWARD PACKET SWITCHING

- The first widely used forwarding method at the Ethernet layer was referred to as store-and-forward switching
- Here, the frame is received entirely before a forwarding decision is made based on destination MAC address
- Once received (and buffered), the frame check sequence (FCS) frame is calculated to ensure the integrity of the frame
- This method has higher latency than cut-through and usually rejects frames smaller than 64 bytes (runts) and larger than 1518 bytes (giants) by default



PERFORMANCE METRICS: THROUGHPUT

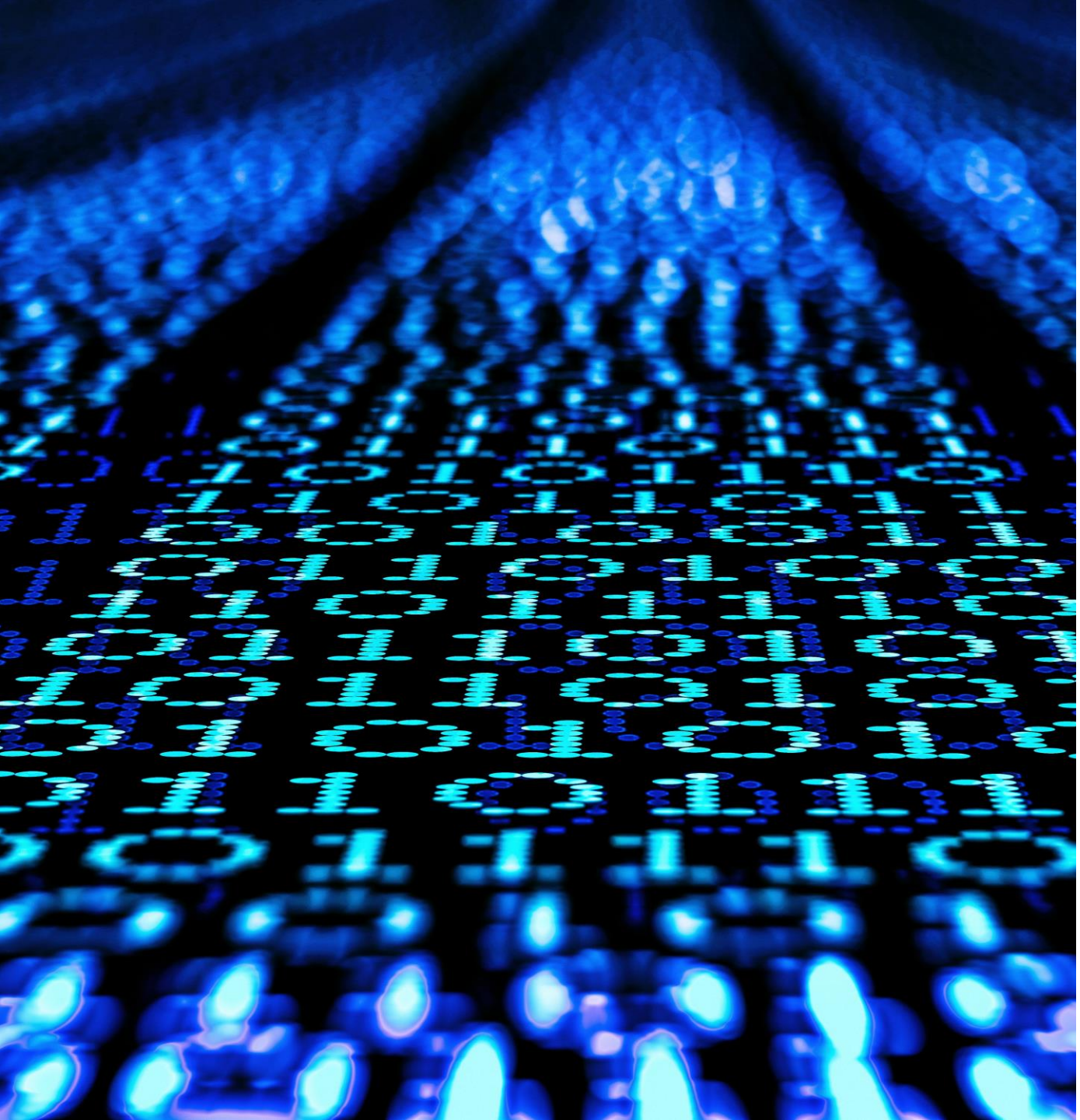
- Network **throughput** is the amount of data transmitted successfully from one node to another in a time frame
- Network throughput refers to the degree of message delivery over a communication channel, such as Ethernet or Fiber
- Network throughput is typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps)
- **Bandwidth** is often synonymous when relating to the amount of data that a network connection can handle at a given point in time

PERFORMANCE METRICS: BANDWIDTH

- **Bandwidth** has several technical meanings, but it usually refers to the volume of information per unit of time that a transmission medium (like an Ethernet or Fiber) link channel can tolerate
- Bandwidth and throughput are typically expressed in bits per second, like 100 Mbps or 100 Mb/s, which is a data transfer rate of 100 million bits (megabits) every second
- A common connection of "1 Gig" would be 1000 megabits per second
- Bandwidth can also refer to the actual width of a band in the radio frequency (RF) spectrum in bits or bytes

PERFORMANCE METRICS: LATENCY

- Latency is the time it takes for data to move from one host to another on a wired or wireless network
- If a server sends a packet at 03:38:00.000 GMT and a client receives it at 03:38:00.145 GMT, then the amount of latency is the difference between these two times: 0.145 seconds or 145 milliseconds
- This performance metric helps developers know how quickly a webpage or app will load for end users as well as measuring the presentation of real-time services



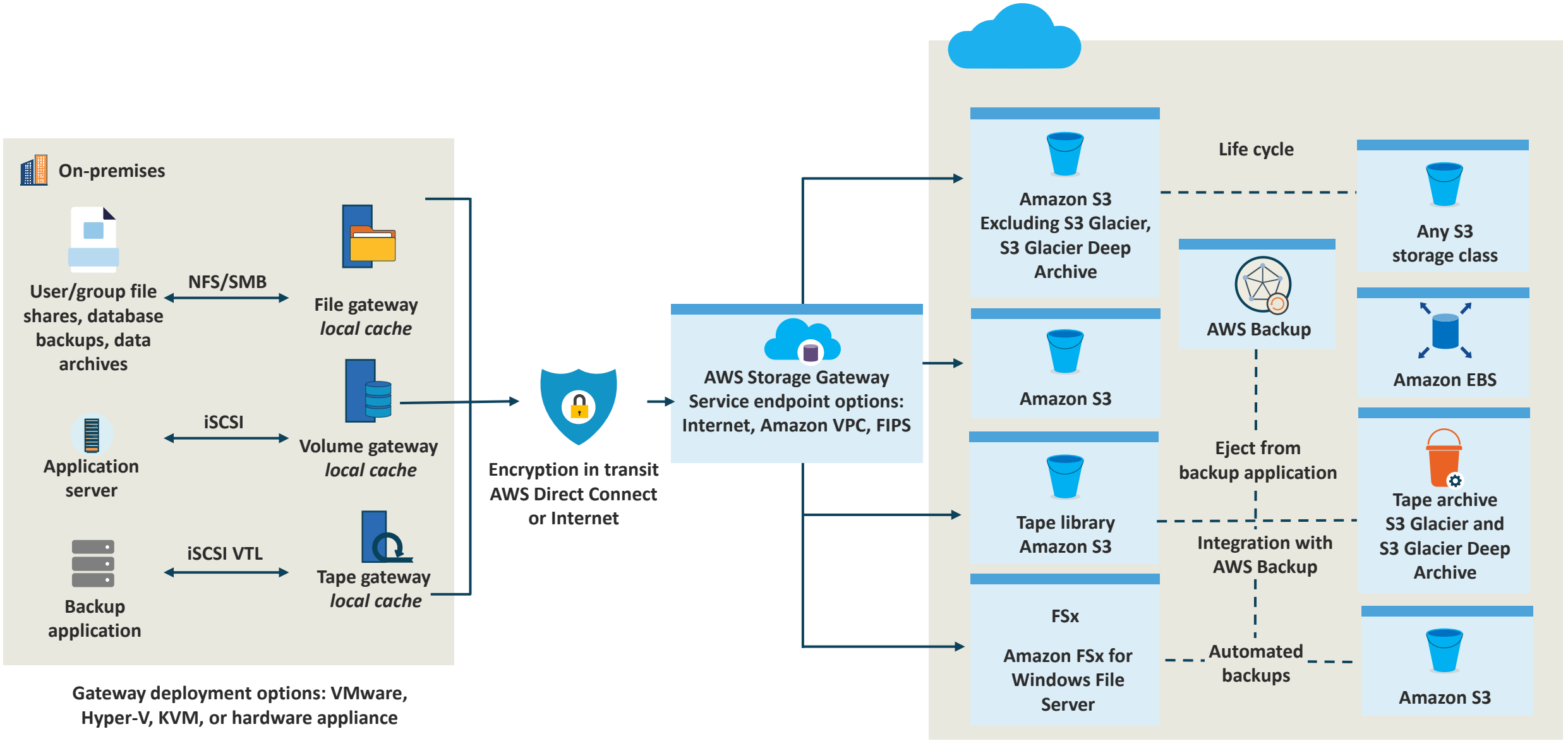
PERFORMANCE METRICS: JITTER

- Jitter is the negative impact of a time delay in the sending of data packets over a network connection
- Fundamentally, the longer data packets take to arrive, the more jitter can negatively affect video and/or audio streaming
- It is often the result of network congestion, route hop changes, or denial-of-service (DoS) attacks
- This is a common nuisance when attempting to use conferencing software such as Zoom or ON24 in a live setting

PERFORMANCE: SIGNAL-TO-NOISE RATIO

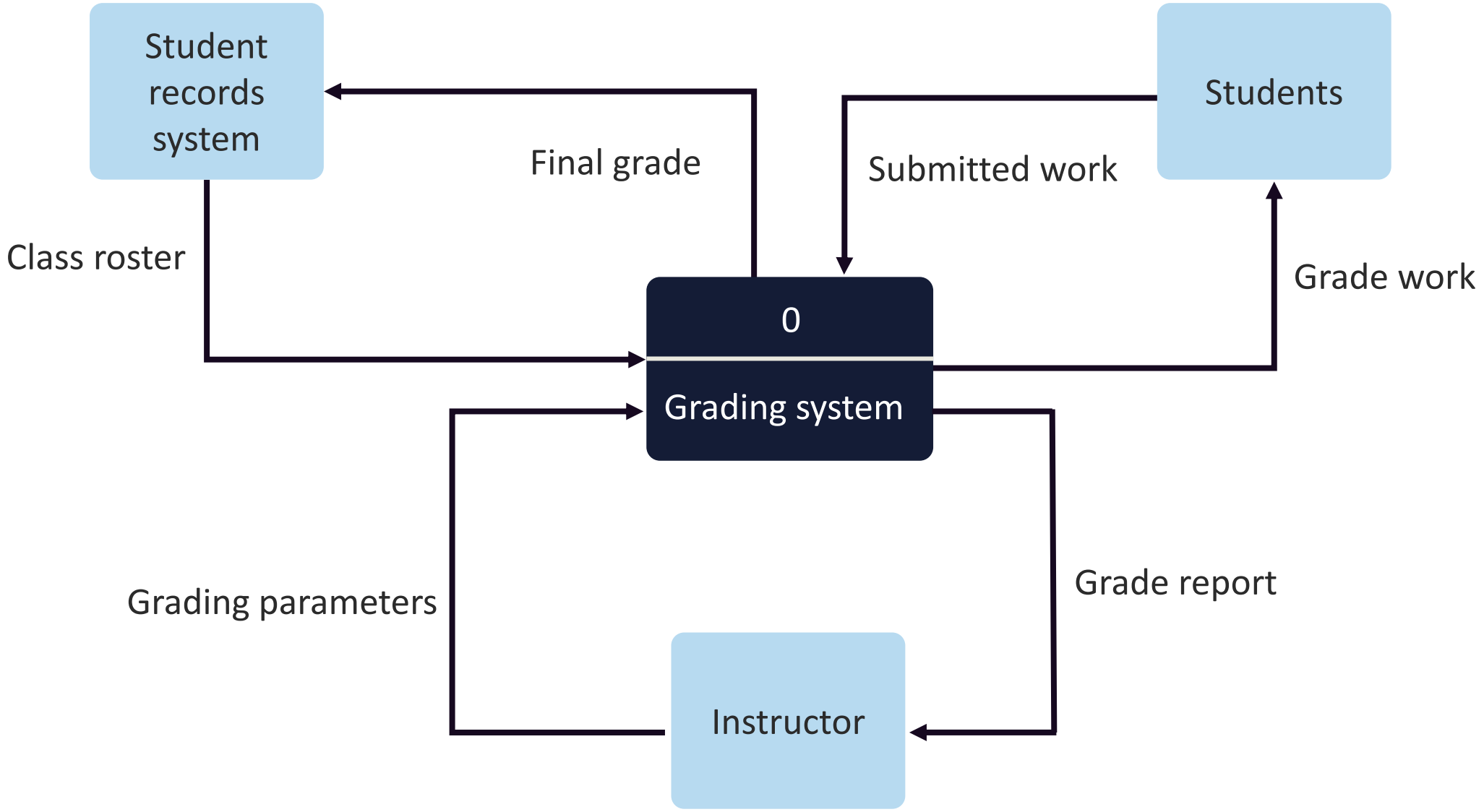
- Signal-to-noise ratio is usually abbreviated as SNR or S/N
- This performance metric is a mathematical technical measurement that relates to a system or services overall sound quality
- SNR compares a level of signal power to a level of noise power and is often expressed as a measurement of decibels (dB)
- Higher numbers typically mean a better specification since there's more beneficial information (signal) than unwelcome data (noise)
- It is also a common wireless analysis metric

DATA FLOW MODELS: IN THE CLOUD

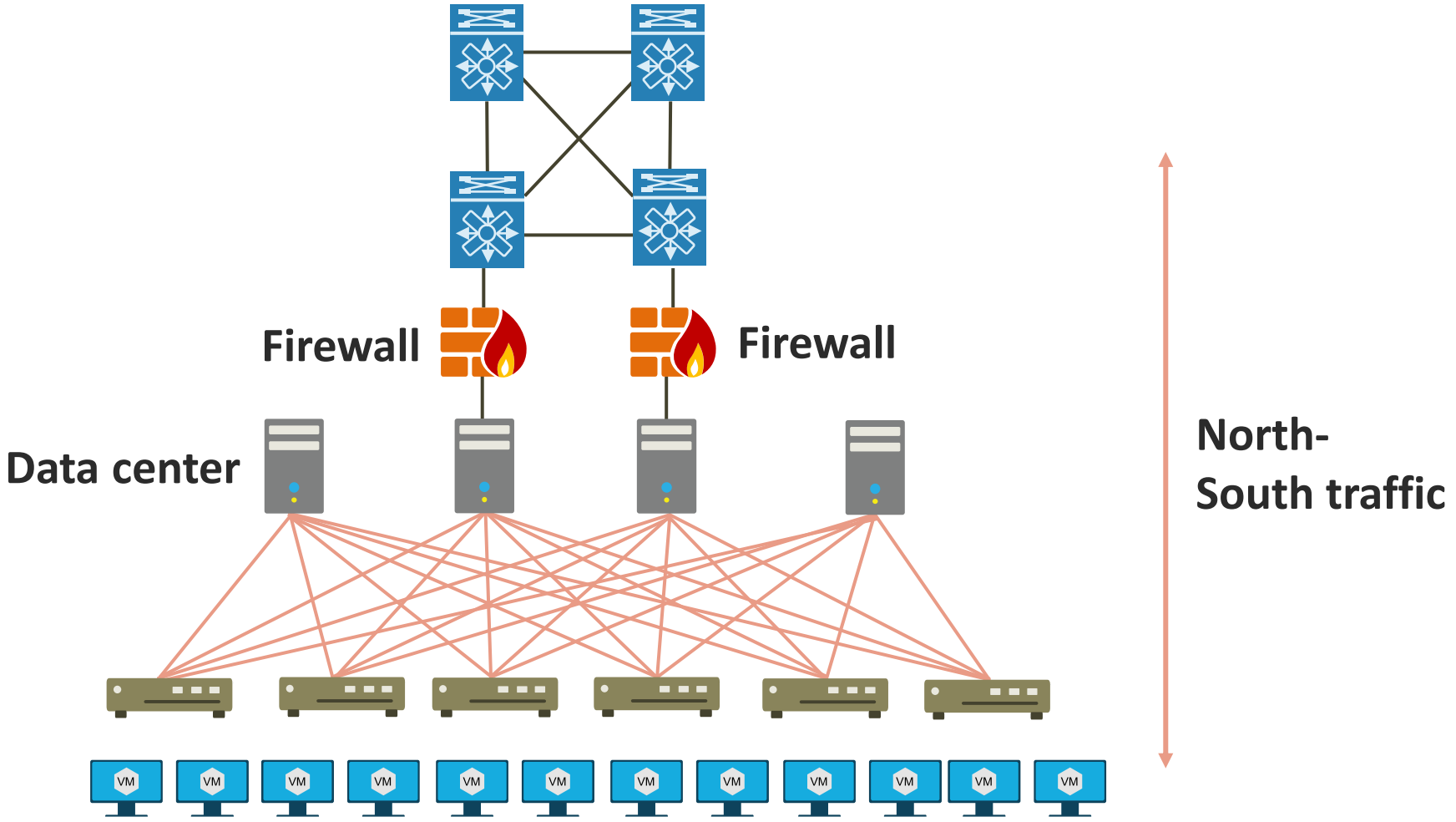


Gateway deployment options: VMware, Hyper-V, KVM, or hardware appliance

DATA FLOW MODELS: IN THE APPLICATION



TRAFFIC FLOW: NORTH-SOUTH



TRAFFIC FLOW: EAST-WEST