Estimated reading time: 25 minutes

Domain 4 of the CISSP certification exam has had some changes you should be aware of. This domain focuses on communication, network security, and security information systems, which you must fully understand to be a cybersecurity professional. It comprises 13% of the exam material you need to learn.
In the following guide, we have compiled the essential aspects you need to know to pass Domain 4 of the CISSP exam and covered the 2021 update with new information.

4.1 Implement secure design principles in network architectures

Open System Interconnection (OSI) model

The CISSP exam contains technical elements, which especially apply to Domain 4, and is more technical than other domains. Networks allow organizations to identify and realize revenue opportunities and communicate and interact with clients. Therefore, networks are a valuable asset of any company and require protection.

What is a network?

A network is at least two devices that are connected to each other. Like people, in order to communicate, these devices must be able to speak a common language (which is what a protocol does), and common rules of communication must be followed.

What is a protocol?

The common rules of network communication are called protocols. A protocol is simply a standard set of rules that are understood, conformed to, and abided by so that two or more devices on a network can communicate.

OSI (Open System Interconnection) model

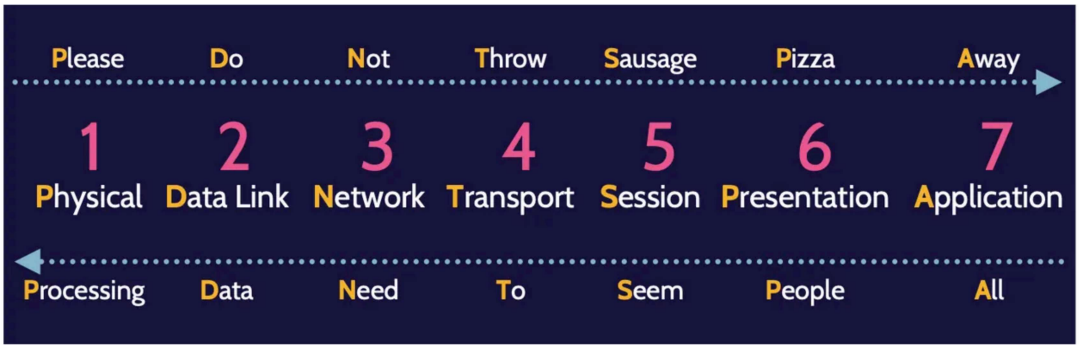
OSI stands for Open Systems Interconnection, which implies that the OSI model is about open systems that can interconnect and communicate with each other using protocols. The OSI model is a structured, layered

architecture comprising seven layers:

OSI	Description	Devices & Protocols	TCP/IP
7 Application	Identify capabilities of applications and resource availability	Application Firewall HTTP/S, DNS, SSH, SNMP, FTP	4 Application
6 Presentation	Formatting of data	XML, JPEG, ANSI	
5 Session	Interhost communication and session management	Circuit Proxy Firewall	
4 Transport	End-to-end connection with error correction and detection	TCP/UDP, iSCSI (SAN)	3 Transport
3 Network	Logical addressing, routing, and delivery of datagrams	Routers, Packet Filtering Firewalls, IP addresses, ICMP, NAT	2 Internet
2 Data Link	Physical addressing, and reliable point-to-point connection	Switches, bridges, MAC addresses, L2TP, PPTP	1 Link
1 Physical	Binary transmission of data across physical media (wire, fiber, etc.)	Hubs, NICs, Network media	

Table 4.2: OSI versus TCP/IP

The most commonly used mnemonics for OSI are: All People Seem To Need Data Processing and Please Do Not Throw Sausage Pizza Away.



The higher the layer, the more functional the security features become, and more comprehensive controls can be implemented; the lower the layer, the opposite is true.

The actual implementation is through TCP/IP. The internet protocol suite (TCP/IP) consists of many protocols—a family of protocols. TCP and IP, and the other members of the protocol family run at different layers of the OSI model to support the underlying tasks of a given layer.

For example, the Network layer is primarily responsible for taking information and routing that, breaking it—fragmentation—into manageable chunks called datagrams and providing addressing so those chunks can be communicated across a network using a logical addressing scheme called IP addresses.

On the other hand, as information moves down from the Application layer to the Physical layer, encapsulation is taking place. On the other side, when the fully encapsulated information arrives, a process called decapsulation takes place.

Layer 1: Physical

Layer 1, the Physical layer, focuses on how devices interconnect as well as encoding the bits, the 0s and 1s, that Layer 1 understands.

Devices can connect using wired or wireless technologies:

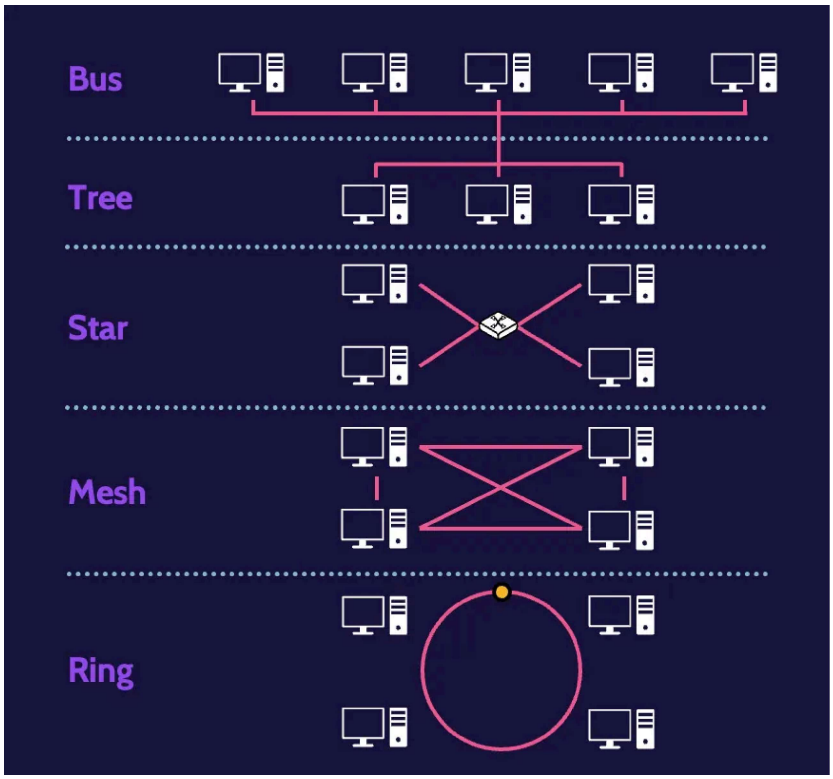
Wired	Wireless
• Twisted Pair • Coaxial • Fiber Optic	• Radio Frequency • Infrared/Optical • Microwave

Twisted pair cable refers to the fact that it is a pair of wires twisted together in a specific way that creates a magnetic field, which allows the signal traveling across the wire to remain within the magnetic field.

Coaxial cable is the cable often used by cable companies to bring television, telephone, and high-speed internet access to homes.

Unlike twisted pair and coaxial cable, which use voltage for communication, **fiber optic** utilizes light pulses to represent 0s and 1s. Both speed and security are great advantages of using fiber optic. Among other things, twisted pair and coaxial cable are both subject to what's known as **cross talk**—interference—because copper, by design, conducts electricity.

Cabling is one part of the equation; another part relates to **topologies**, or how the cables are laid out. The most common network topology is known as a **bus topology**, which simply means that all devices are connected to a central wire, called a bus.



From a security point of view, a bus topology has several weaknesses. For one, the bus represents a single point of failure. For another, devices are connected to a single wire, so by default, every device can intercept all the information being transmitted across the wire.

Another topology is known as a **tree topology**, which somewhat resembles a tree with different branches. By virtue of this structure, one of the immediate benefits is that transmissions can be isolated to certain branches of the tree, thereby limiting transmissions from being seen by the entire network.

A **star topology**, as the name suggests, resembles a star. All devices are connected to a central device, like a switch or a hub. One significant disadvantage of a star topology is that the central device represents a single point of failure.

A **mesh topology** interconnects every device with every other device. This is excellent for purposes of redundancy—if one device goes down, communication with other devices is not impacted.

A **ring topology** looks like a ring. Devices are connected to a closed loop, and in a sense, the loop is still essentially a bus, which can lead to issues like collisions.

Dealing with collisions

One of the major problems found in all the topologies except token ring is collisions. Three primary methods exist to handle them:

1. Token-based collision avoidance. A token is passed from device to device, and only the device holding the token can transmit information.
2. Polling. Interconnected devices poll each other to learn if any information needs to be transmitted. This method obviously implies a significant amount of network traffic, which explains why it is not popular or used often, if at all.
3. Carrier Sense Multiple Access (CSMA). Used by modern networks. Devices are connected to the same carrier, the same wire, and therefore each device can sense the wire to identify if another device is transmitting. Even with CSMA, collisions are still going to occur. This is why two flavors of CSMA exist—CSMA with Collision Avoidance (CSMA/CA) and CSMA with Collision Detection (CSMA/CD). CSMA/CA completely avoids collisions.

Transmission methods

How these devices communicate is through transmission methods. From a security perspective, unicast is the most secure method because communication is limited to a specific destination device.

Unicast	Multicast	Broadcast
One-to-One	One-to-Many	One-to-All

Layer 1 devices

Several important devices operate at Layer 1, among them:

- Hubs
- Repeaters

- Concentrators

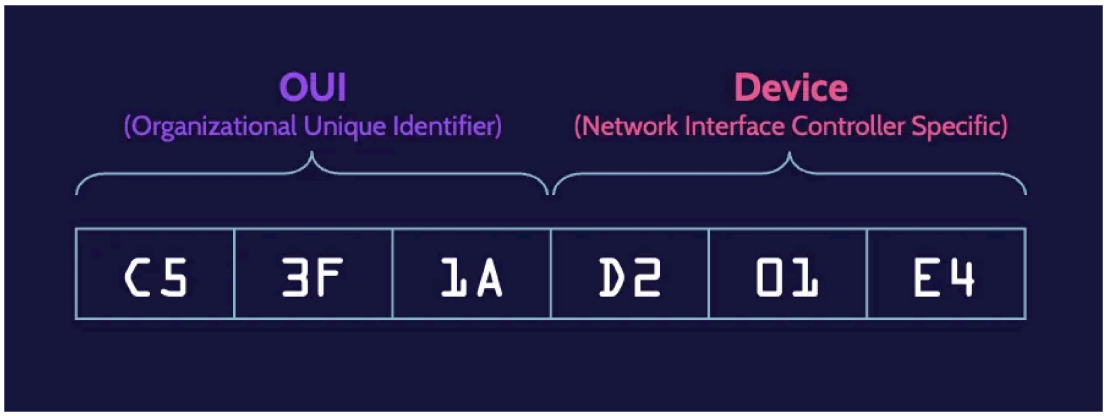
Layer 2: Data Link

Layer 2—the Data Link layer—acts as a conduit between Layer 1—the Physical layer—and Layer 3—the Network layer. The Physical layer only works with bits, and the Network layer works with datagrams. Between them, the Data Link layer takes datagrams from the Network layer and formats them in a manner that allows the Physical layer to work with them as bits.

Physical addressing

Layer 2 is also the layer where devices that operate across a network are physically and uniquely identified and separated from each other. For a network to work, the devices on it need to have unique physical addresses. This unique physical address exists and is known as a Media Access Control (MAC) address.

A MAC address is simply bits—0s and 1s—that uniquely identify and distinguish every device on a network, and this unique identifier is specified via a device's network card.



Networks work by virtue of logical address schemes that facilitate communication between devices. This is done at Layer 3 and is known as IP addressing, which can take IP addresses and convert them to MAC addresses and vice versa.

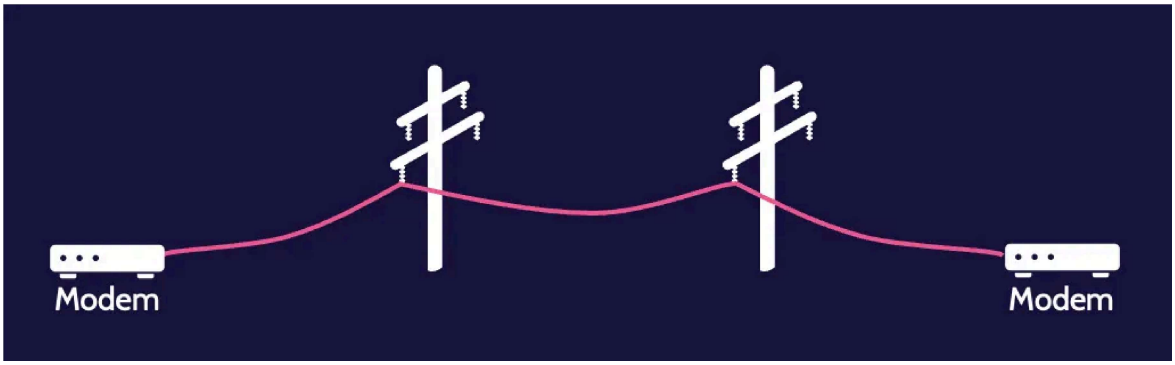
Specifically, two protocols handle these needs: Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP). ARP allows IP addresses to be mapped to physical addresses, while RARP allows physical addresses to be mapped to IP addresses.

Circuit-switched network

A great example of a circuit-switched network is the **Public Switched Telephone Network (PSTN)**, which has been in existence for many, many years. Connecting across the PSTN requires another person's telephone number, which can then be dialed, and a series of devices that comprise the PSTN will establish the circuit—the connection.

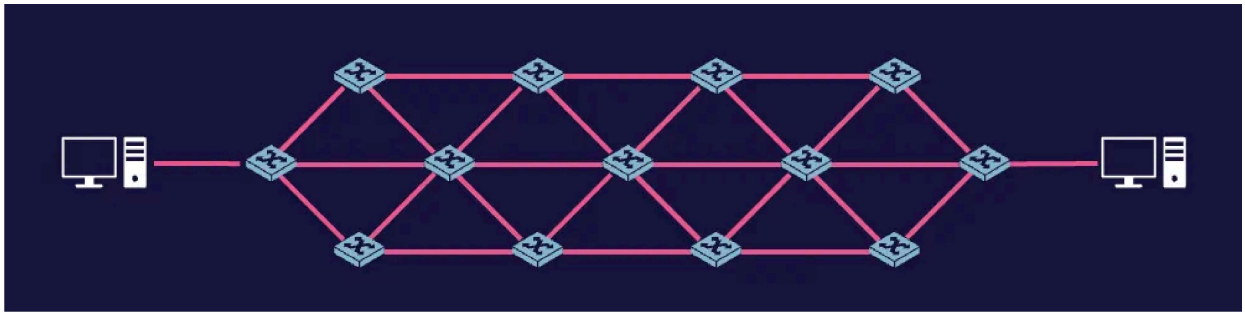
Transmission of digital data over analog connections

Data networks were built for speed and bandwidth, and it wasn't long before voice communications using data transmission were perfected. We know this as Voice over IP, or VoIP or IP telephony, which encapsulates the internet protocol to enable transmission of **digital data** over **analog connections**.



Packet-switched network

Packet-switched networks function by taking data that needs to be communicated from one device to another and breaking it into datagrams or **packets**. Each data packet contains information, such as addresses and sequence numbers.



Layer 2 protocols

Layer 2 protocols are:

- L2F
- PPTP
- L2TP

- SLIP
- ARP - IP to MAC
- RARP - MAC to IP

The first three are tunneling protocols, which are required to create virtual private networks (VPN).

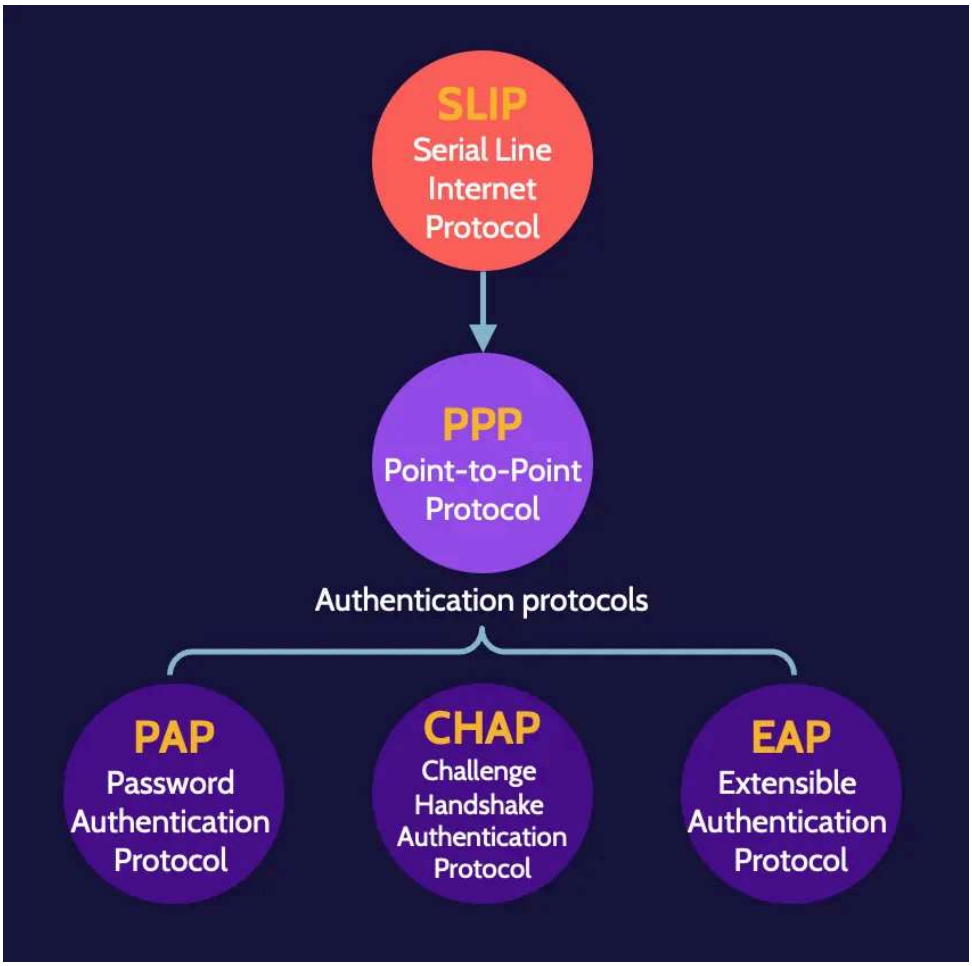
Layer 2 devices

Significant devices that operate at Layer 2 are bridges and switches.

Authentication protocols

As remote authentication needs have matured, authentication protocols have also matured to meet those needs. **Extensible Authentication Protocol (EAP)** is the best authentication protocol available, and its capabilities have been extended to Protected Extensible Authentication Protocol (PEAP).

Password Authentication Protocol (PAP) simply prompts for a user ID and password when establishing a connection, and **Challenge Handshake Authentication Protocol (CHAP)** is an improved version of PAP.



Layer 3: Network

Data at the Network layer exists as packets/datagrams, and logical addressing is used to map IP addresses to MAC addresses—ARP; Reverse ARP (RARP) maps MAC addresses to IP addresses.

Layer 3 protocols

Layer 3 is home to several significant TCP/IP protocols. In addition to the already discussed IP protocol, IGMP, IPsec, and routing protocols BGP, OSPF, and RIP operate at Layer 3.

ICMP	Internet Control Message Protocol is used for messaging and specifically provides feedback about problems in the network communication environment. Ping and traceroute are two important commands that utilize ICMP. Ping attempts to see if a host device is reachable; traceroute tries to map the path of traffic.
IGMP	Internet Group Management Protocol is used to establish and manage group memberships for hosts, routers, and similar devices
IPsec	IPsec is a tunneling protocol that supports authentication of other Layer 3 devices as well as encryption.
OSPF	Open Shortest Path First is a routing protocol used by routers to manage and direct network traffic properly and efficiently. OSPF includes security features that make it a more secure routing protocol than others.

Layer 3 devices

The most obvious are routers, but Layer 3 switches can also be found at the Network layer, along with packet-filtering firewalls.

Logical addressing

Internet protocol datagrams consist of data, also known as the payload.

IPv4 addresses are comprised of four numbers separated by dots, e.g., 192.168.1.254. The IP address is a 32-bit value, and each number represents an 8-bit octet, while **IPv6** addresses are comprised of 128 bits divided into eight groups of 16 bits.

LAN technologies

These are the three common IEEE standards from the 802 family:

Wired	Wireless	Virtual LAN (VLAN)
IEEE 802.3 defines a collection of communication standards for physical connections on a wired Ethernet network.	IEEE 802.11 is a collection of communication standards specific to the implementation of WLAN communication	IEEE 802.1Q defines the standard for virtual local area networks. VLANs are used to create isolated networks for purposes of security and to minimize broadcast traffic on a network.

Private IPv4 addresses

Private IP addresses are non-routable, which means their use within corporate or home networks provides a layer of security between public-facing internet devices and internal devices.

These are the private IPv4 IP address ranges that are not to be used on public networks (like the internet).

From	To
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Network classes

if networks were limited to only Class A, B, or C ranges, every network would have only 254, 65,534, or 16+ million IP addresses for host devices, and these limitations could create huge inefficiencies, potential security issues, significant administrative overhead, and potential network-related performance and congestion issues.

Through the use of subnetting, which reflects awareness of the current environment and planning for the future, the proper-size logical host environment can be architected and deployed and can mitigate many, if not all, of the issues noted.

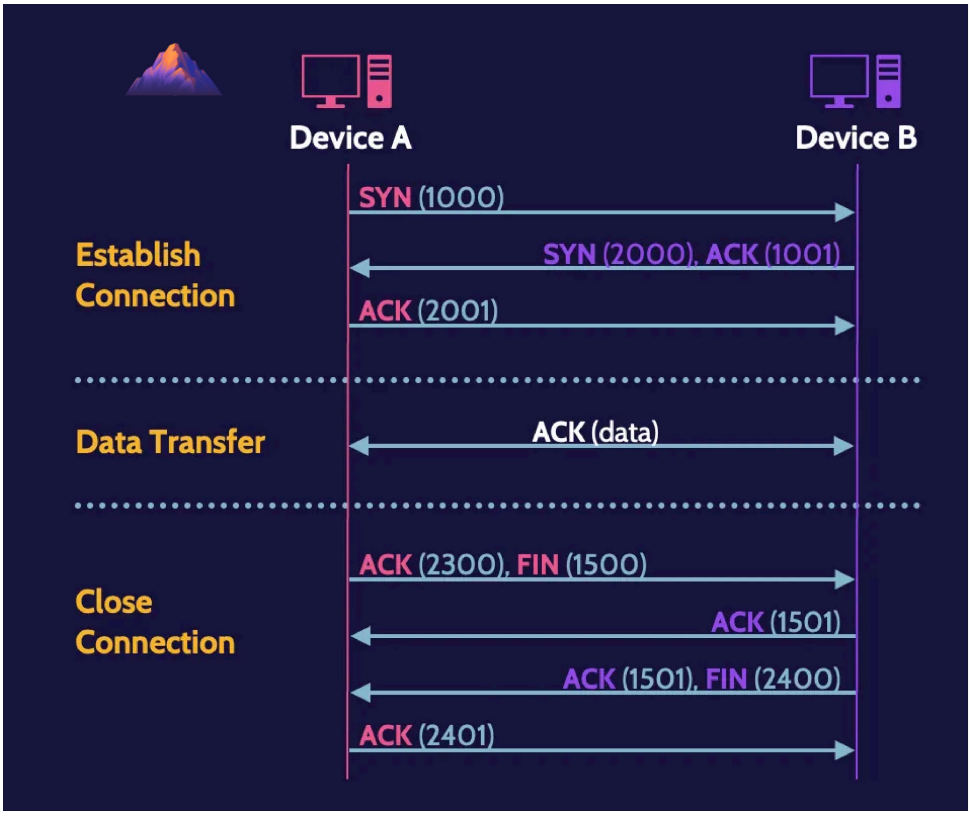
Layer 4: Transport

TCP and UDP are two transport protocols that reside at Layer 4.

both protocols are still heavily relied upon, and each serves a purpose. For reliable, perhaps a bit slower, transmissions, TCP is a clear choice. However, UDP is fast, and for things like video streaming, which requires speed, as well as handling DNS requests, UDP is very efficient.

TCP three-way handshake

What's known as the TCP three-way handshake is the building of the technological road to reliably connect hosts across a network. Let's examine this more closely through an example in the following figure:



Each transmission must be acknowledged by the receiving device, and in the three earlier steps, a full-duplex connection is established; thus, the term three-way handshake.

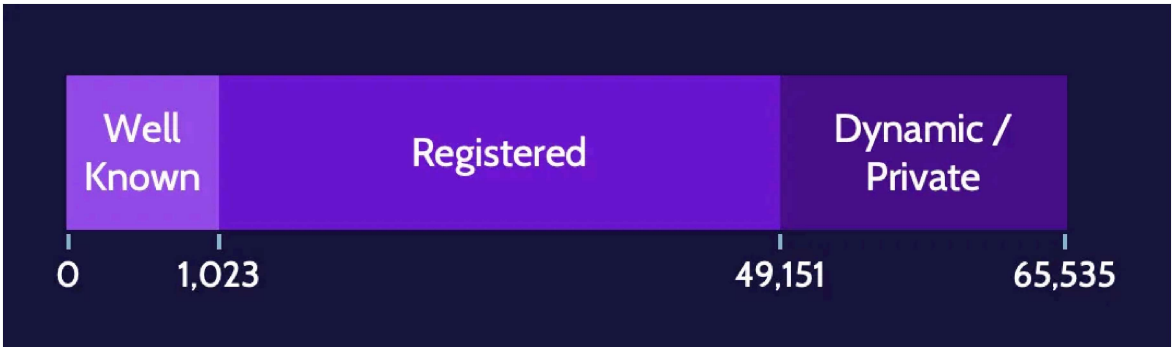
Ports

Ports equate to services, and services are small applications that provide specific functionality. For example, for the common web service, HTTP, port 80 is used by default.

If a service is not needed, especially ones that are dangerous, the associated port should be closed, and techniques like packet filtering can be used to block datagrams that reference the associated ports in the header.

There are three classes of available TCP and UDP ports:

- Well known: 0-1,023
- Registered: 1,024-49,151
- Dynamic/Private/Ephemeral: 49,152-65,535



These are common TCP ports:

21	File Transfer Protocol (FTP)
22	Secure Shell (SSH) (remote login protocol)
23	Telnet (remote command line protocol)
25	Simple Mail Transfer Protocol (SMTP)
80	Hypertext Transfer Protocol (HTTP)
443	Hypertext Transfer Protocol Secure (HTTPS)

In addition, the two main VoIP protocols are:

- **Secure Real-time Transport Protocol (SRTP).** This is the secure version of RTP, which supports encryption, authentication, integrity, and replay attack protection.
- **Session Initiation Protocol (SIP).** It is responsible for initiating, maintaining, and terminating voice and video sessions.

Vishing

Vishing is a form of phishing (**voice phishing**) that specifically takes place in the context of VoIP environments. Smishing, on the other hand, relates to the attacker sending SMS messages to the victim (**SMS phishing**).

Network security attacks

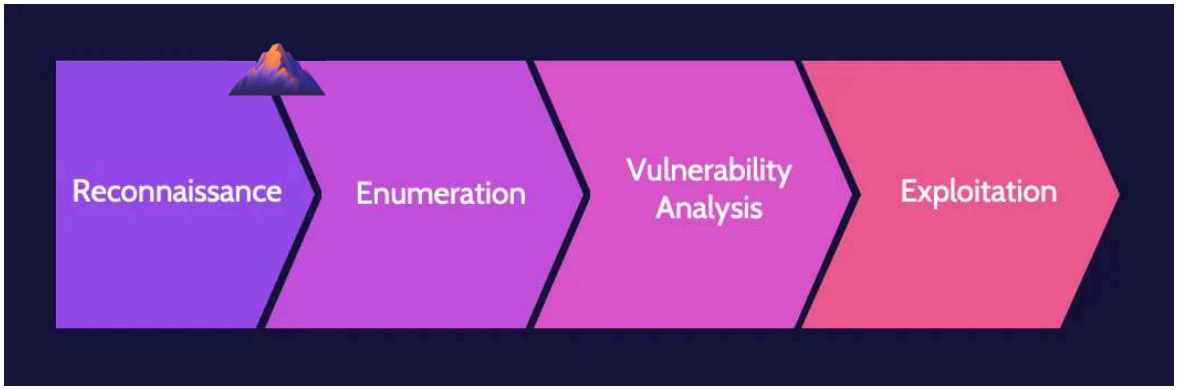
Network attacks resemble network assessments in terms of the steps/phases that each follows, with the exception of assessments including an exploitation phase. Passive attacks do not change the environment or information, while active attacks can change information.

Network attack phases

The main difference between network attacks and network assessments is that an attacker will not care if they inflict damage on the target network when they are launching an exploit, while the penetration tester will do that in a more controlled manner and while respecting the scope and rules of engagement.

In virtually all cases, any successful attack will sequentially go through the phases outlined here:

1. Reconnaissance
2. Enumeration
3. Vulnerability analysis
4. Exploitation



SYN scanning

Tools like Nmap can easily perform SYN scanning, which consists of:

1. A client sends an SYN packet to a target machine's specific port (e.g., TCP port 80) to try and identify if it's open or closed.
2. Possible responses are:
    1. If the port is open, the target replies with an SYN-ACK packet, and then the client responds with a final ACK packet, and the session is established.
    2. If the port is closed, the target responds with an RST packet, and the session is terminated.

SYN flooding

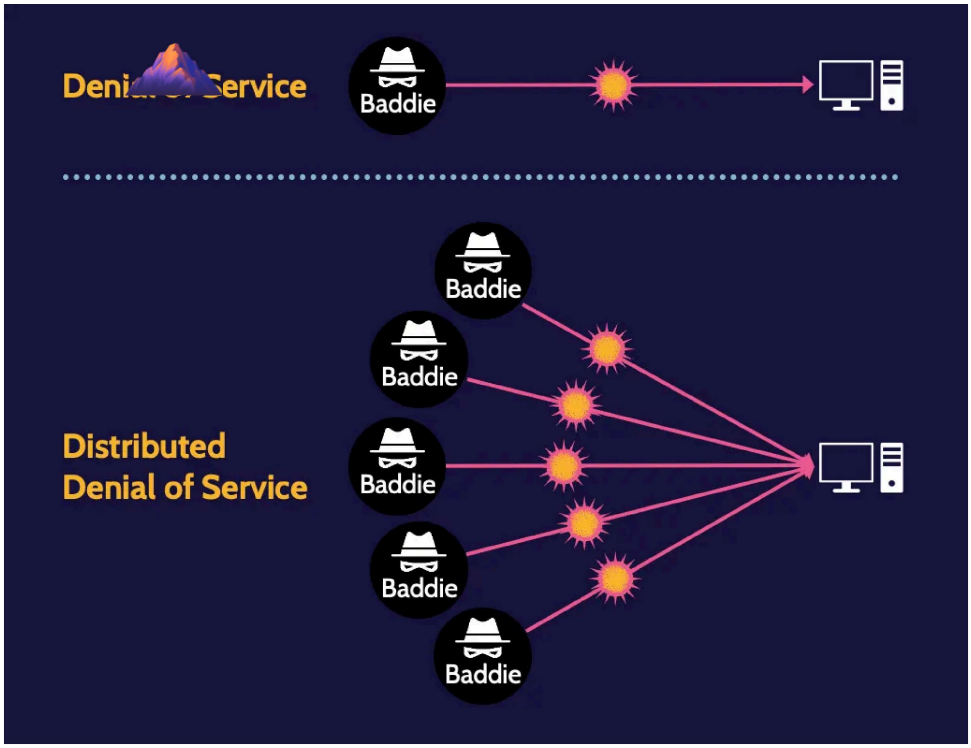
SYN flooding takes advantage of this fact when multiple SYN requests are sent in rapid succession to a target machine, which responds with an SYN-ACK packet, considering these valid connection requests. SYN floods are active attacks because they impact the host by degrading its performance or bringing it down altogether.

IP-based attacks

A number of IP-based attacks exist, like SYN flooding, eavesdropping, overlapping fragment, and teardrop attacks.

DoS and DDoS

A **Denial-of-Service (DoS)** attack is any attack that attempts to impede or completely deny functionality. A **Distributed-Denial-of-Service (DDoS)** attack involves multiple machines acting in unison.



Man-in-the-Middle

A man-in-the-middle attack manifests when the attacker inserts themselves in the communication path of two entities and thus has an opportunity to intercept and manipulate traffic between them.

Spoofing

Spoofing is pretending to be someone or something else, because that someone or something usually possesses more privileges or has access to a resource. It is not limited to one area of focus. Email, DNS entries, user IDs, IP and MAC addresses, and even biometrics can be spoofed.

Common tools and protocols

The next table summarizes some common tools and protocols that attackers use to take advantage of networks.

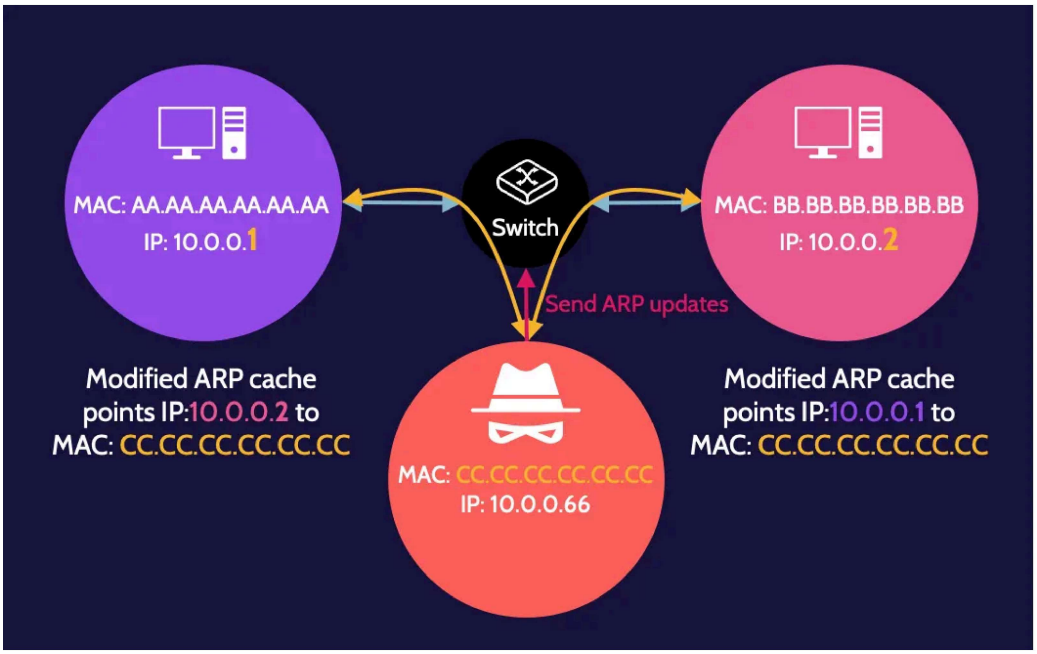
- Ping
- Traceroute
- ICMP

- DHCP
- Ipconfig
- WHOIS
- Dig
- Putty
- Nmap
- John the Ripper
- Netstat
- Nslookup

ARP poisoning

ARP poisoning involves a malicious user modifying their ARP table to direct network traffic meant for another device to their device.

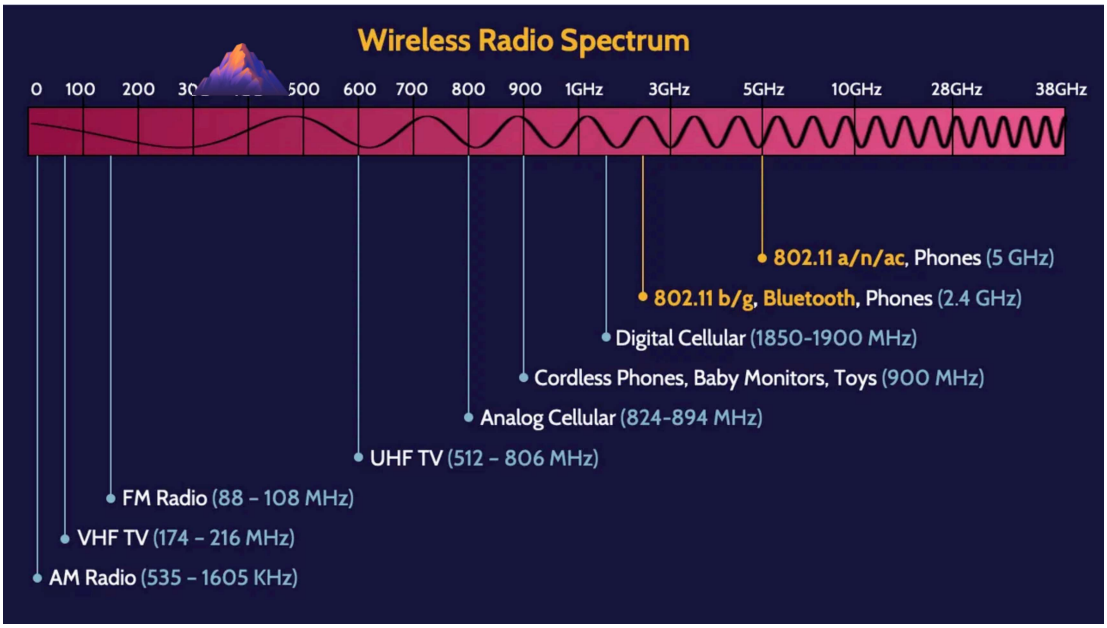
ARP uses tables to map IP addresses to physical addresses—the MAC addresses—of a device. Every device on a network has a physical address and an ARP table.



Wireless

Radio frequency management

Radio frequency management refers to the placement of devices that broadcast wireless traffic. Managing Wi-Fi signals is called radio frequency management, which can prove quite challenging at times as there is an abundance of different devices operating at different areas of the radio spectrum.



802.11 Wireless protocol family

These are the different IEEE 802.11 specifications, starting with 802.11:

Type	Frequency	Top Speed
802.11	2.4 GHz	2 Mbps
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz & 5 GHz	72–600 Mbps
802.11ac	5 GHz	422–1300 Mbps
802.11ax (Wi-Fi 6)	2.4 GHz & 5 GHz	10 Gbps
802.11ad (WiGig)	60 GHz	7 Gbps

802.11 Security Solutions

To secure wireless communication, four (4) security services are required:

- Access control
- Authentication
- Encryption
- Integrity protection

The following table illustrates how they are implemented:

	802.1x Dynamic WEP	Wi-Fi Protected Access (WPA)	Wi-Fi Protected Access (WPA2)	Wi-Fi Protected Access (WPA3)
Released	1997	2003	2004	2018
Access Control	802.1X	802.1X or Pre-Shared Key	802.1X or Pre-Shared Key	802.1X or Pre-Shared Key
Authentication	EAP methods	EAP methods or Pre-Shared Key	EAP methods or Pre-Shared Key	EAP methods or Pre-Shared Key
Encryption	WEP	TKIP (RC4)	CCMP (AES Counter Mode)	CCMP or GCMP (Galois Counter Mode Protocol)
Integrity	None	Michael MIC	CCMP	CCMP or GCMP

Wireless authentication

There are three main ways to authenticate to a wireless network:

- Open authentication
- Shared key
- EAP is used

Wireless encryption

The main encryption technologies are:

- **Temporal Key Integrity Protocol (TKIP)**
- **Counter-Mode-CBC-MAC Protocol (CCMP)**

Wireless integrity protection

Main methods for integrity protection are:

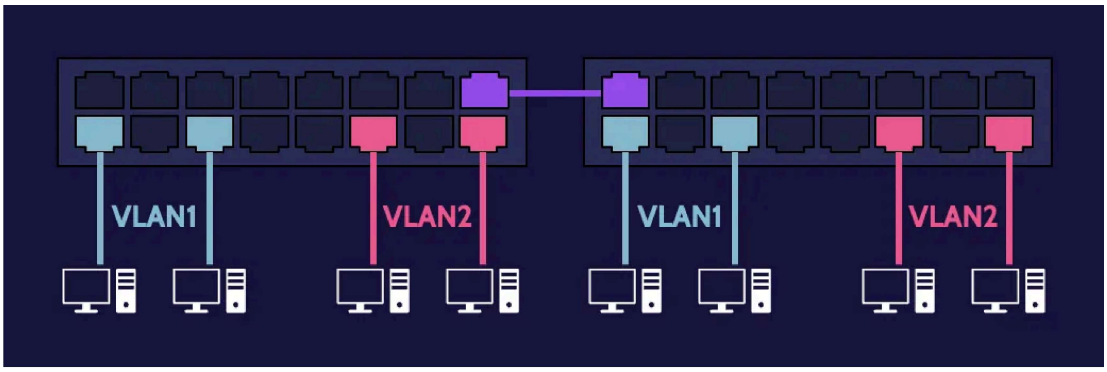
- **TKIP** uses a Message Integrity Code called “Michael.”
- **WPA2** uses **CCMP** (which uses AES in CBC-MAC mode).

VLAN and SDN

Virtual Local Area Network (VLAN)

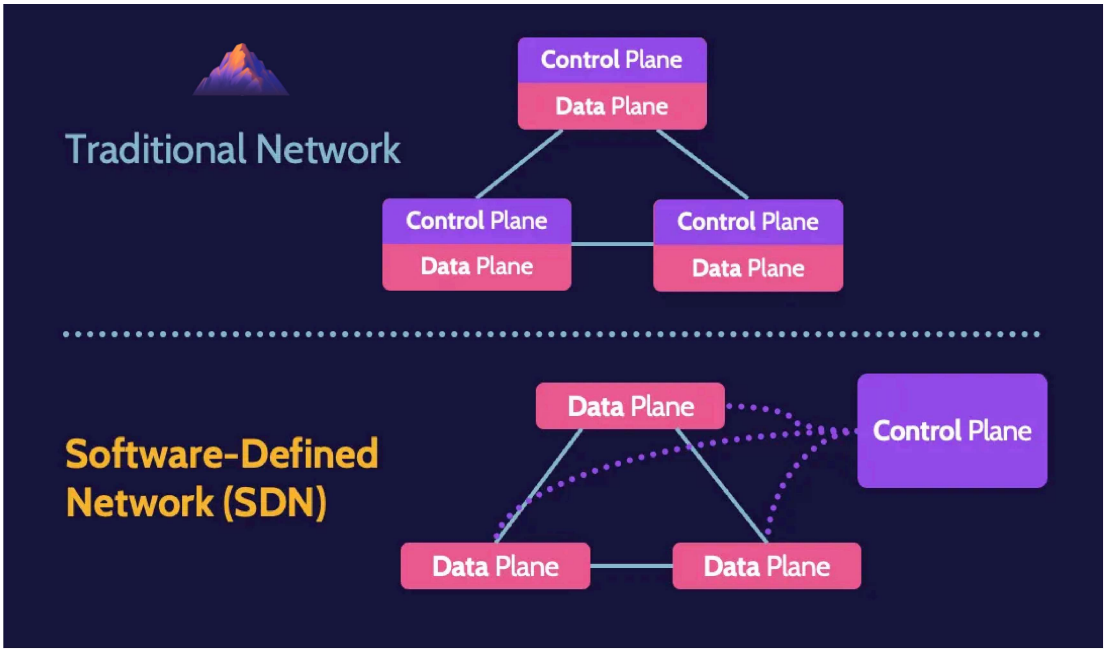
VLAN stands for virtual local area network, and a VLAN can be created using devices, technologies, and software. A VLAN **reduces the need for physical rewiring by creating virtual tunnels through physical networks to connect devices**.

IEEE 802.1Q is the standard that supports VLANs on networks, and typically, a Layer 3 switch can be used to create VLANs based on needs and value.

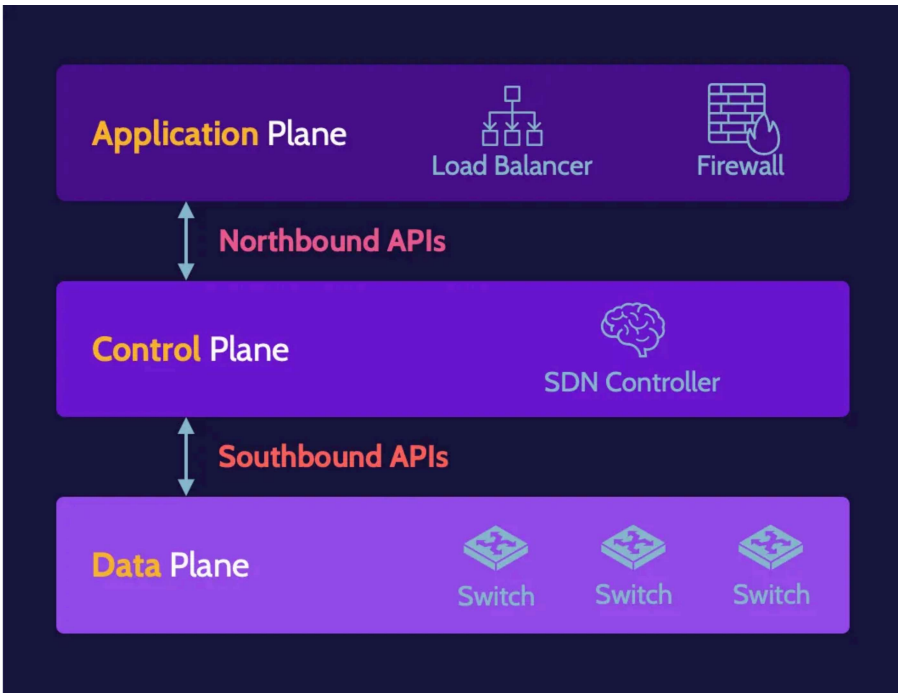


Software-defined networks (SDN)

Software-Defined Networks (SDN) refer to networks created and managed using software. SDN architecture includes application, control, and data planes. In an SDN, applications provide the functionality provided by hardware devices found in a traditional network.



Communication between application and control planes is facilitated by **northbound APIs**; communication between data and control planes is facilitated by **southbound APIs**.



Wide area networks (WAN)

WANs connect LANs through technologies such as dedicated leased lines, dial-up phone lines, satellite and other wireless links, and data packet carrier services.

WAN protocols include:

- X.25
- Frame Relay
- Asynchronous Transfer Mode (ATM)

- Multi-Protocol Label Switching (MPLS)

The Value of CISSP in Different Regions

4.2 Secure network components

Network architecture

Network architecture includes employing concepts such as defense in depth, partitioning, a well-protected network perimeter, network segmentation, and bastion hosts. Key elements of network architecture include the concepts defined below.

Defense in depth

The concept of defense in depth refers to combining multiple layers of security controls to protect a network.

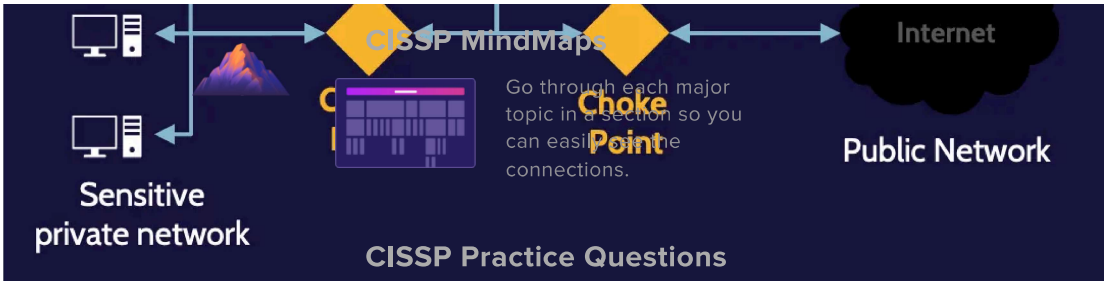
Partitioning

Partitioning is the practice of controlling the flow of traffic between segments. It can be used to prevent traffic from those areas from being seen across the entire network.

Network perimeter

The network perimeter is the last point that any organization can control. Like physical security, where controls should comprise preventive, detective, and corrective capabilities, the same should hold true for the network.

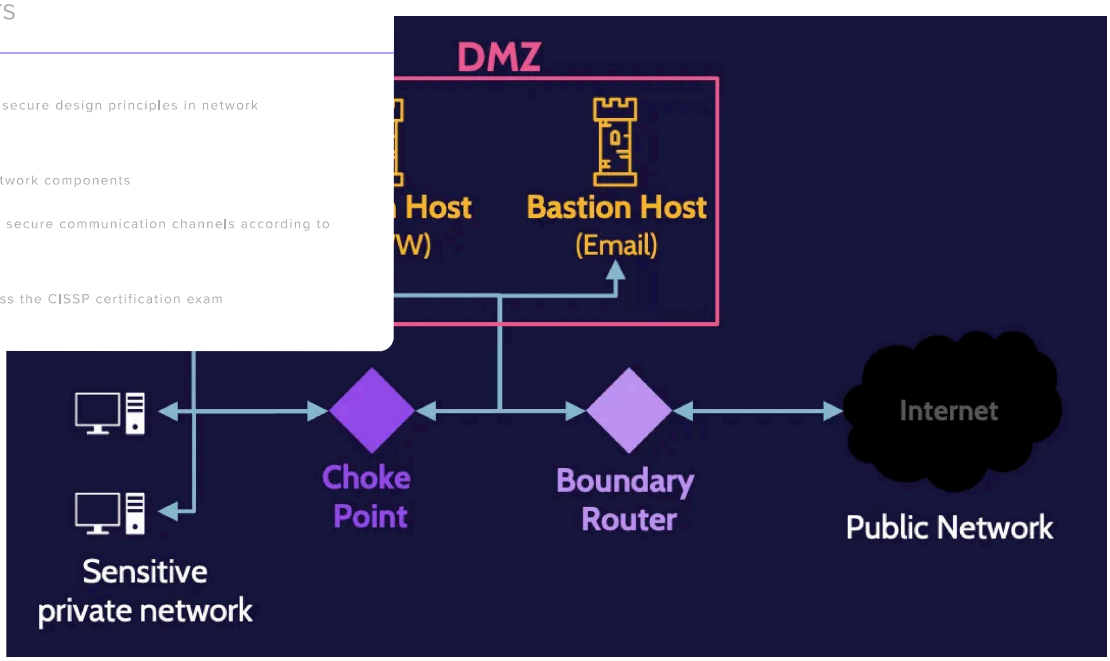
Limiting the ingress and egress point of a network to one creates a **choke point**—a point where devices and technologies that enforce rules can be placed to ensure all incoming and outgoing traffic is analyzed.



Bastion host

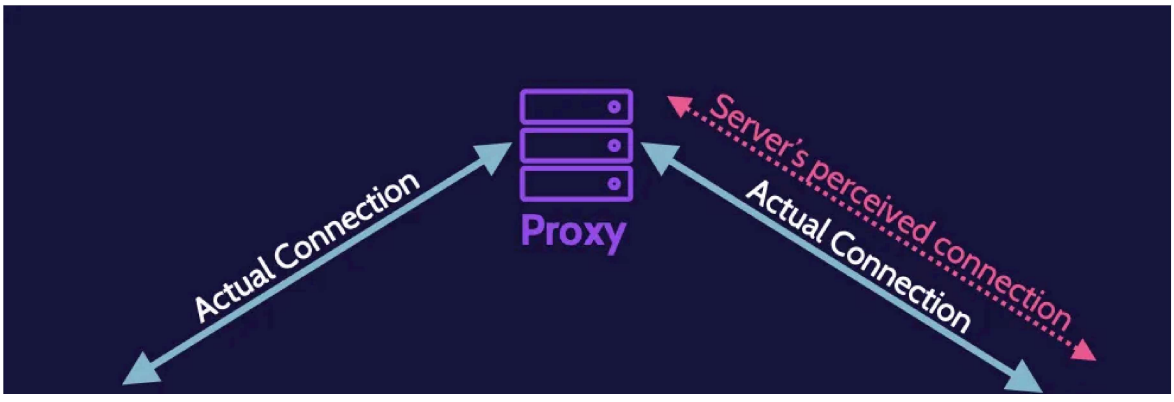
This risk can be mitigated through the creation of a subnetwork, usually referred to as a **Demilitarized Zone (DMZ)**, where services and applications that require public access can be segregated.

Because the organization controls the DMZ, it can also provide necessary protection for each application. In this context, devices and applications within a DMZ are often referred to as **bastion hosts** and bastion applications.



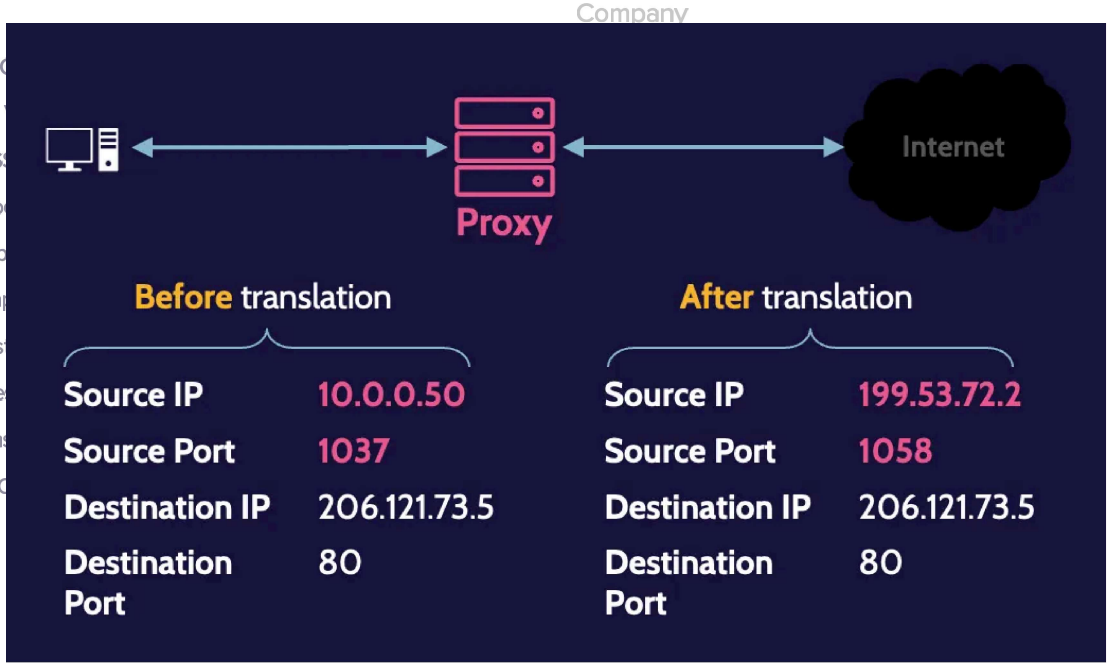
Proxy

A proxy or proxy server is an intelligent application or hardware that acts as an intermediary and is placed between clients and a server. They're usually found at Layer 7—the Application layer—of the OSI model.



NAT and PAT

NAT is the mechanism that allows us to translate private IP addresses to public ones and vice versa. PAT is another mechanism that can be used, which helps us perform port translation in the same notion as IP address translation is performed.



Firewall technologies

A firewall is a concept that enforces security rules between two or more networks by performing traffic filtering.

Different firewall technologies used nowadays are depicted in the following table:

Packet Filtering	• Examines packet headers to either block or pass packets • Uses access control lists (ACLs) that allow it to accept or deny access
Stateful Packet Filtering	• State and context data are stored and updated dynamically • Provides information for tracking connectionless protocols, e.g., Remote Procedure Call (RPC) and UDP-based applications, where source/destination ports and IP addresses are used to track state
Circuit-Level Proxy	• Create a circuit between client and server without requiring knowledge about the service • Have no application-specific controls • An example is a SOCKS server
	• Able to inspect packet payload

Application-Level Proxy

- A different proxy is needed for each service
- Can be a performance bottleneck

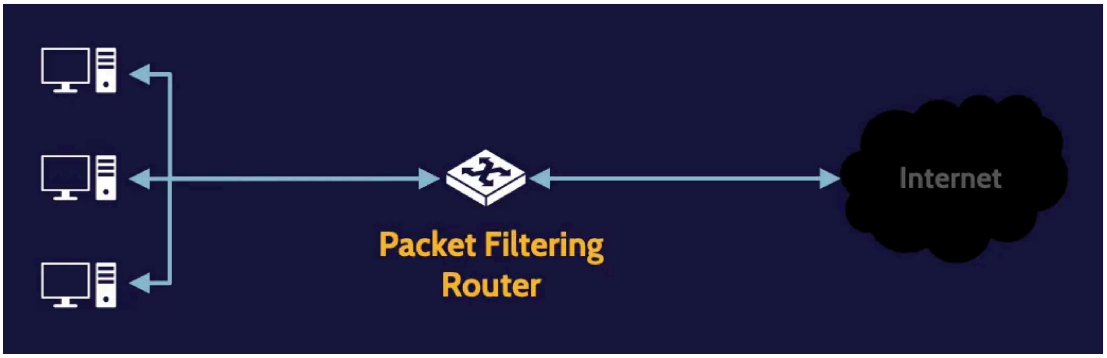
Context-Based Access Control (CBAC)

CBAC is a feature of firewall software that intelligently filters TCP and UDP packets based on application layer protocol session information. It allows for deep traffic inspection and filtering to take place.

Firewall architectures

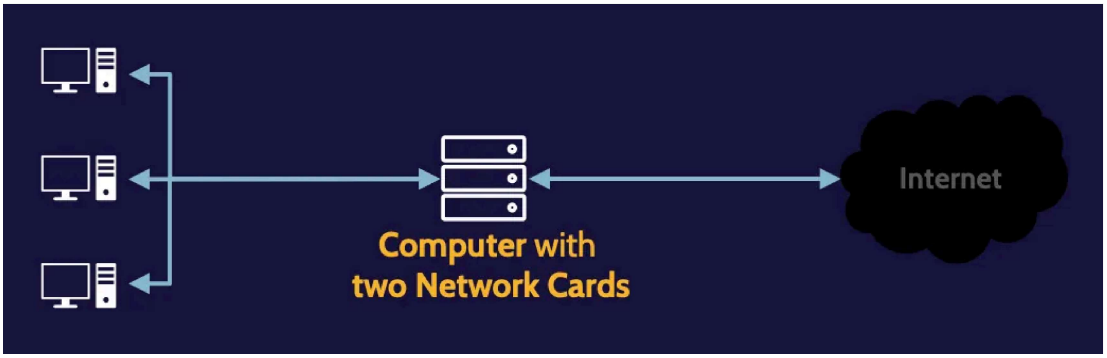
Packet filtering

A packet-filtering firewall architecture is the simplest one. The router, which operates at Layer 3, can only make decisions based upon information that exists at Layer 3—the header portion of the datagram, which contains information like source IP, destination IP, service being requested, and so on.



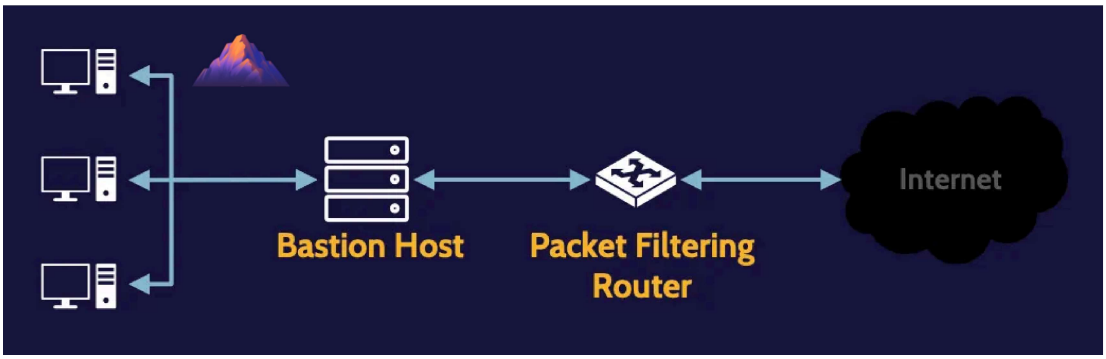
Dual-homed host

A dual-homed host improves upon a packet-filtering router by replacing it with a more intelligent computer or host that contains two network cards.



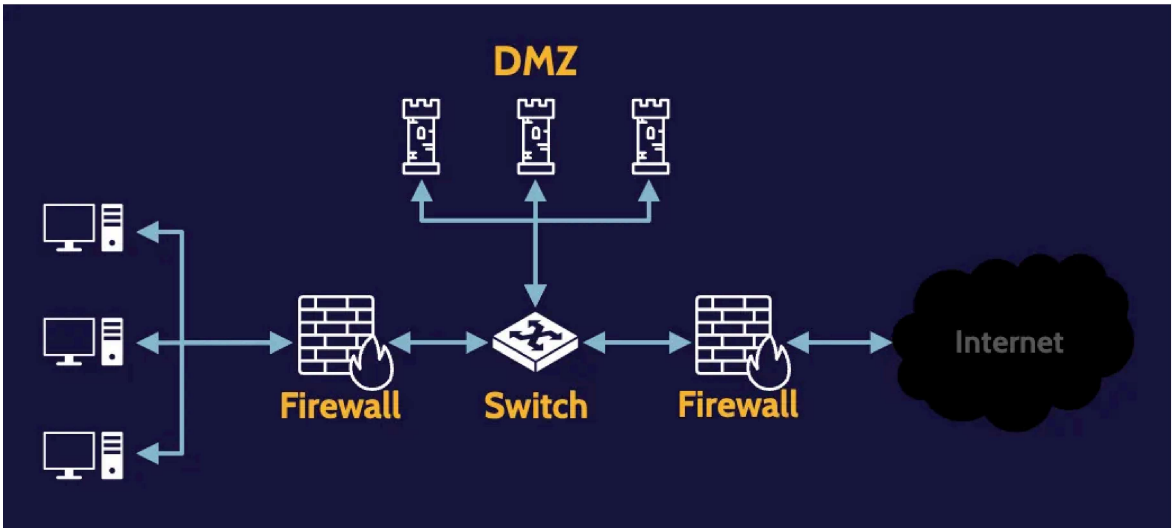
Screened host

By combining the architectural elements of a packet filtering and dual-homed host firewall, the router can handle the first level of decision-making related to incoming packets, and any packets that are allowed through can then be further examined by the bastion host, which can be any type of firewall technology.



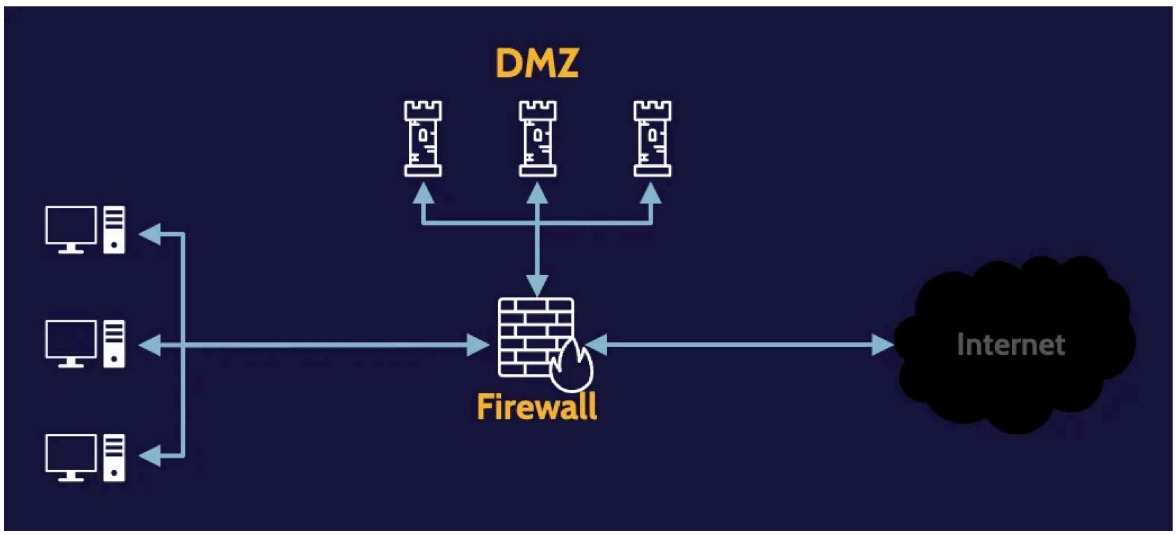
Screened subnet

Here, two firewalls are used, and between them, a subnet, such as a DMZ, can be created. Traffic from the outside can be specifically directed to the DMZ and thereby protect the internal network from potential attacks.



Three-legged firewall

A firewall by virtue of three connection points, although any number of connection points could really exist.



IDS and IPS

At a high level, data inspection involves monitoring and examining transmitted data and taking appropriate action if not allowed by security rules. It includes the following activities:

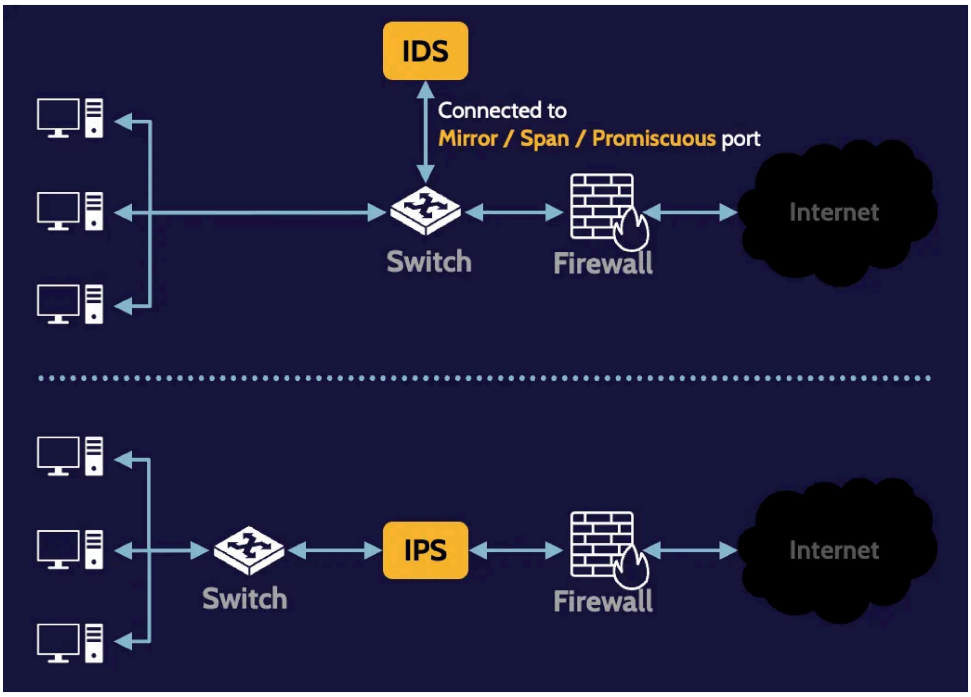
- Virus scanning
- Stateful inspection
- Content inspection

There are two types of IDS/IPS systems:

- **Network-based**. It requires strategically placed sensors across a network and monitoring network traffic to ensure that rules are applied.
- **Host-based**. Host-based IDS/IPS run as agents on specific devices, like servers and other mission-critical systems, and do the same thing

On the other hand, **Intrusion Detection System (IDS)** performs data inspection and detects, logs, and reports, and sometimes triggers other devices to take corrective action.

Intrusion Prevention System (IPS) performs data inspection and additionally prevents or takes corrective action.



Mirror/span/promiscuous port

When a port on a network device (e.g., switch) is described as **mirror**, **span**, or **promiscuous**, it's meant that traffic passing through that device is copied to that port, and any device connected to it, like an IDS, can obtain a copy of it for inspection.

IDS/IPS detection methods

There are two types of analyses engines used with IDS/IPS:

- **Pattern-based engines** focus on known types of attacks and use this information to build a database of patterns for detection purposes.
- **Anomaly-based engines** look for unusual, abnormal, and out-of-the-ordinary patterns, which implies they understand what is normal and predictable.

Ingress and egress monitoring

The terms ingress and egress refer to the direction of flow or, in this case, network traffic. **Ingress monitoring** refers to monitoring all traffic entering a network, while **egress monitoring** is monitoring all traffic exiting a network.

Ingress monitoring can help prevent malicious traffic from entering a network, and egress monitoring can help prevent data loss, denial-of-service, and other types of malicious activity from originating from the corporate environment.

Allow list and deny list (whitelisting and blacklisting)

A technique that IDS/IPS devices can use to detect and potentially block suspicious traffic is allow lists and deny lists.

Allow and deny lists are lists of IP addresses and specifically determine what action may or may not be performed with respect to the IP addresses in a given list.

Sandbox

A sandbox is a safe area where untrusted code can be isolated and run. Being able to run **potentially malicious software** in a sandbox environment is one of the corrective actions that an IDS/IPS can take.

Alert statuses

The next list illustrates the possible conditions of alerts that may be received by security tools:

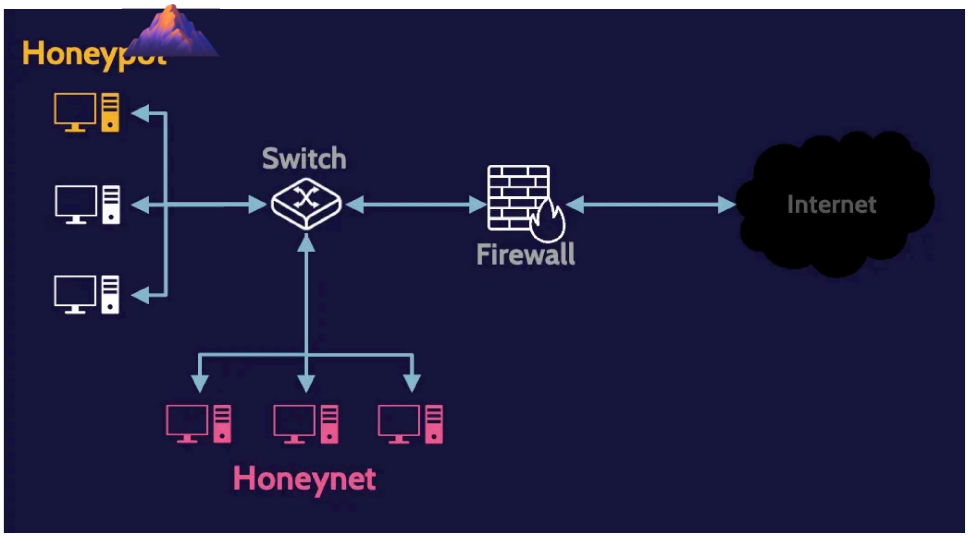
1. **True-Positive**: An attack is taking place, and the security tool raises an alert to denote that fact.
2. **True-Negative**: No attack is present, and no alert is generated by a security tool. This indicates the appropriate operation is in effect.
3. **False-Positive**: An alert is generated by the security tool; however, there's no actual attack taking place.
4. **False-Negative**: An attack is ongoing, but the security tool failed to raise an alert.

Honeypots and honeynets

Honeypots and honeynets are technical detective controls. They both contain vulnerabilities that entice intruders into exploring further.

Honeypots are individual computers (usually running a server OS posing as interesting targets for an attacker), but they contain no real data or value to the organization employing them.

Honeynets are two or more honeypots networked together, and a sophisticated honeynet will also employ the use of routers, switches, or gateways.



Enticement and entrapment

When working with honeypots and honeynets, an organization must be careful to avoid the entrapment of a potential attacker, which is illegal.

- The **enticement** is legal and pertains to situations where an intruder has already broken into a network.
- The **entrapment** is illegal and pertains to situations where somebody is persuaded to break into a network.

Endpoint security

Endpoint security focuses on the protection of devices found on corporate networks and seeks to minimize the attack surface and thereby prevent or minimize attacks.

Network access control (NAC) solutions seek to unify endpoint security technology, user authentication, and overall network security.

4.3 Implement secure communication channels according to design

Remote access

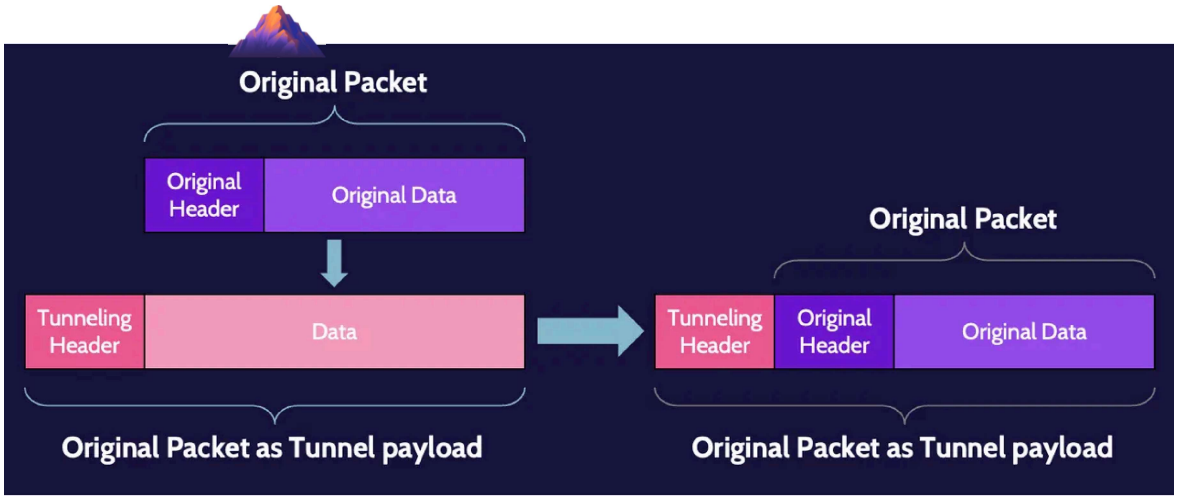
Implementing secure communication channels is an important component of network security. In other words, putting protections in place to support network connections—especially remote access—is critical.

Due to this fact, a method to protect traffic across that untrustworthy network must be utilized, and the best method is usually a VPN solution.

Tunneling

VPN is tunneling plus encryption; without encryption, it can only be called a tunnel. Tunneling is simply the process of taking a datagram and placing it inside the data portion of another datagram. Some people also

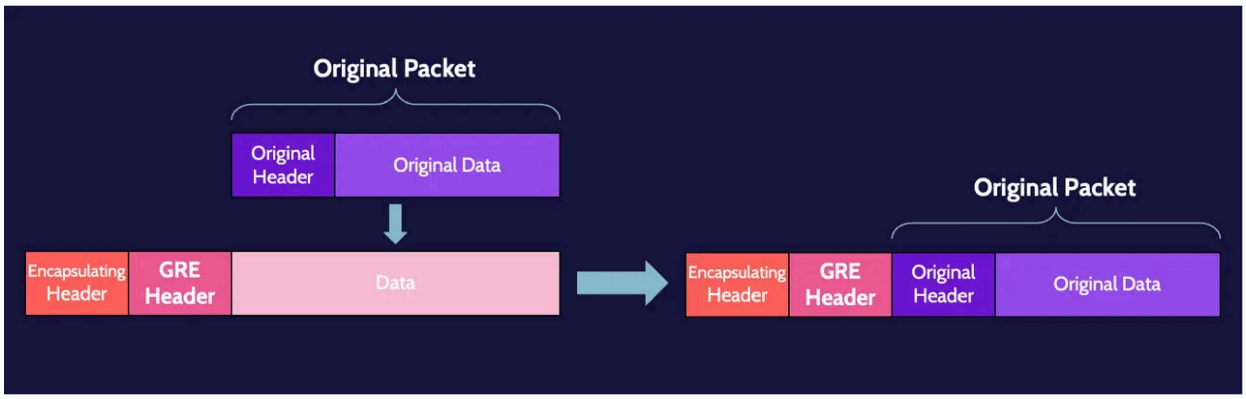
refer to this as **encapsulation**.



This **encapsulation** process does not hide anything. It's simply placing the original datagram inside the data portion of another one.

Generic Routing Encapsulation (GRE)

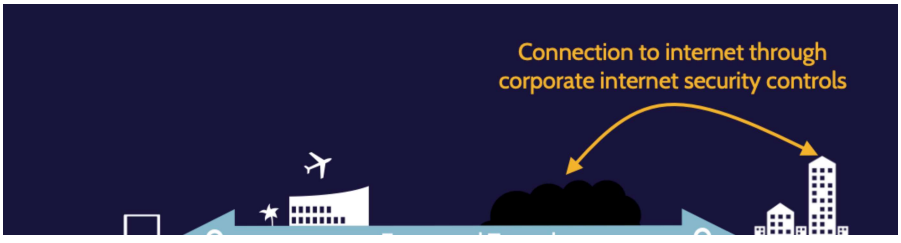
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of protocols and route them over IP networks. GRE can transport traditional IPv4 traffic as well as multicast and IPv6 traffic, and it provides a means by which traffic can be exchanged between two networks using a network like the internet.

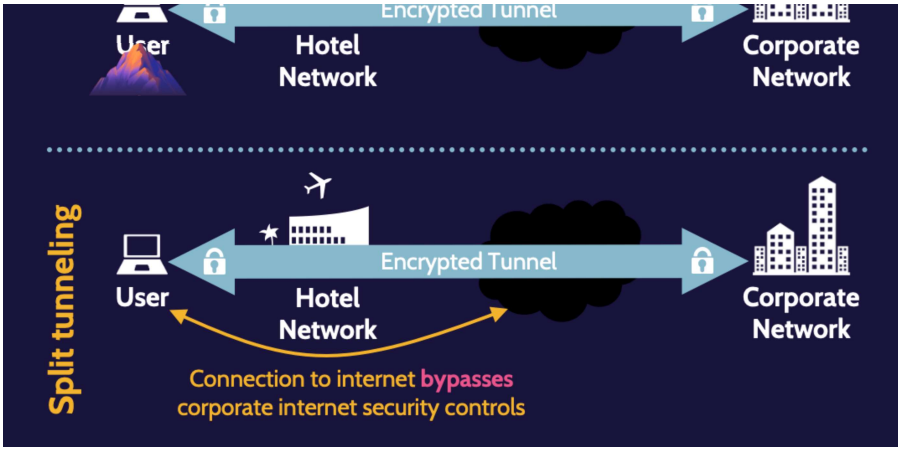


Split tunneling

Split tunneling allows a user to access disparate resources—the internet and a LAN, for example—at the same time, without all the traffic passing through the VPN.

Running internet traffic directly from the user's computer through the hotel network can bypass organizational security controls, which can create significant risk for the organization.

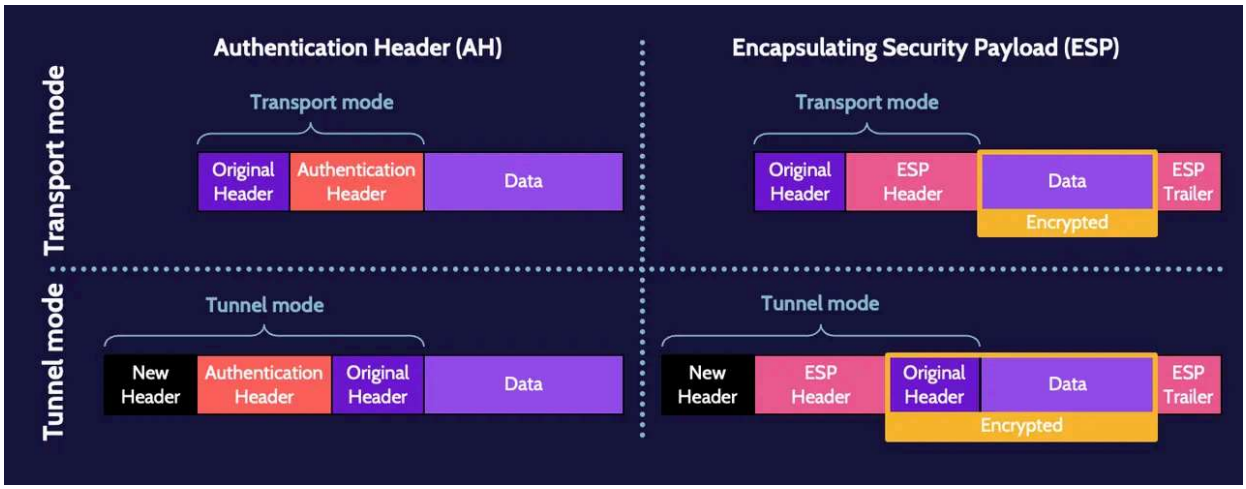




IPsec

IPsec is preferred for establishing a VPN and is embedded in IPv6 as a default feature. It offers authentication via Authentication Header (AH) and encryption via Encapsulating Security Payload (ESP).

IPsec works in one of two modes. **Transport** mode uses the header of the original datagram, whereas, in **tunnel** mode, the header of the new datagram encapsulates and encrypts the AH or ESP header and original IP header in the data, or payload, portion of the new datagram.



Internet Key Exchange (IKE)

To create a VPN, two things are required: tunneling plus encryption. The only type of encryption that can be used for a VPN is symmetric, meaning the same key is utilized at each end of the VPN connection.

In the context of IPsec, the key management protocol used is known as **Internet Key Exchange** or IKE. IKE is essentially a version of Diffie–Hellman and is used by IPsec to generate the same session key at each end of a VPN.

Security Association (SA)

IPsec tunnels are established through a Security Association (SA). *SA is a **one-way** establishment of attributes at the start of communication between two entities.*

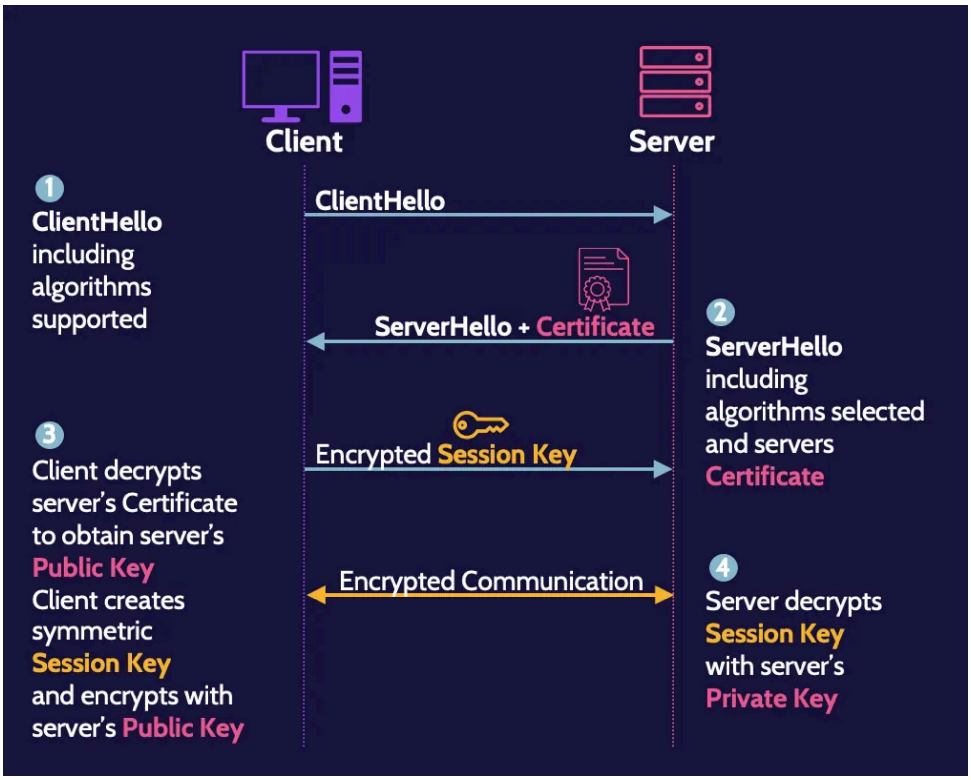
SSL/TLS

Secure Sockets Layer/Transport Layer Security (SSL/TLS) provides secure client-to-server connections; the two names refer to the same thing, but TLS is now the proper standard and most current version, as SSL is obsolete.

SSL/TLS is used extensively. It could result in what is known as the **DROWN attack** exploiting a specific vulnerability in SSLv2. If successful, a DROWN attack could result in a session being compromised, and sensitive information—passwords, credit card numbers, proprietary, and other valuable data—could be read or stolen.

These are the SSL/TLS connection steps:

1. Client hello
2. Server hello
3. Creation and sharing of session key
4. Establishment of secure session



Asymmetric cryptography is used to encrypt the symmetric session key created by the client. In addition, unencrypted SSL sessions can exist, where a browser and server authenticate to one another, but the communications channel is not encrypted.

Remote authentication

Remote authentication protocols include RADIUS, TACACS+, and Diameter.

- **RADIUS** was originally developed to support dial-in networking and provides authentication, authorization, and accounting.

- **TACACS+** uses TCP and encrypts all packets.
- **Diameter** is the successor to RADIUS and includes much-improved security, including EAP.

4.4 How to pass the CISSP certification exam

We have seen how technical Domain 4 is and all the concepts you must learn for the CISSP certification exam. Becoming a cybersecurity or IT professional is no easy path, and the exam can be challenging. That's why we offer one of the best learning tools available for it: our CISSP MasterClass.

We have decades of experience and involvement with ISC2 to help you learn everything you need to know to pass all domains of the CISSP exam, with a personalized learning path and targeted recommendations for an optimal learning style.

Enroll now in our CISSP MasterClass on Destination Certification. Your cybersecurity career starts here.