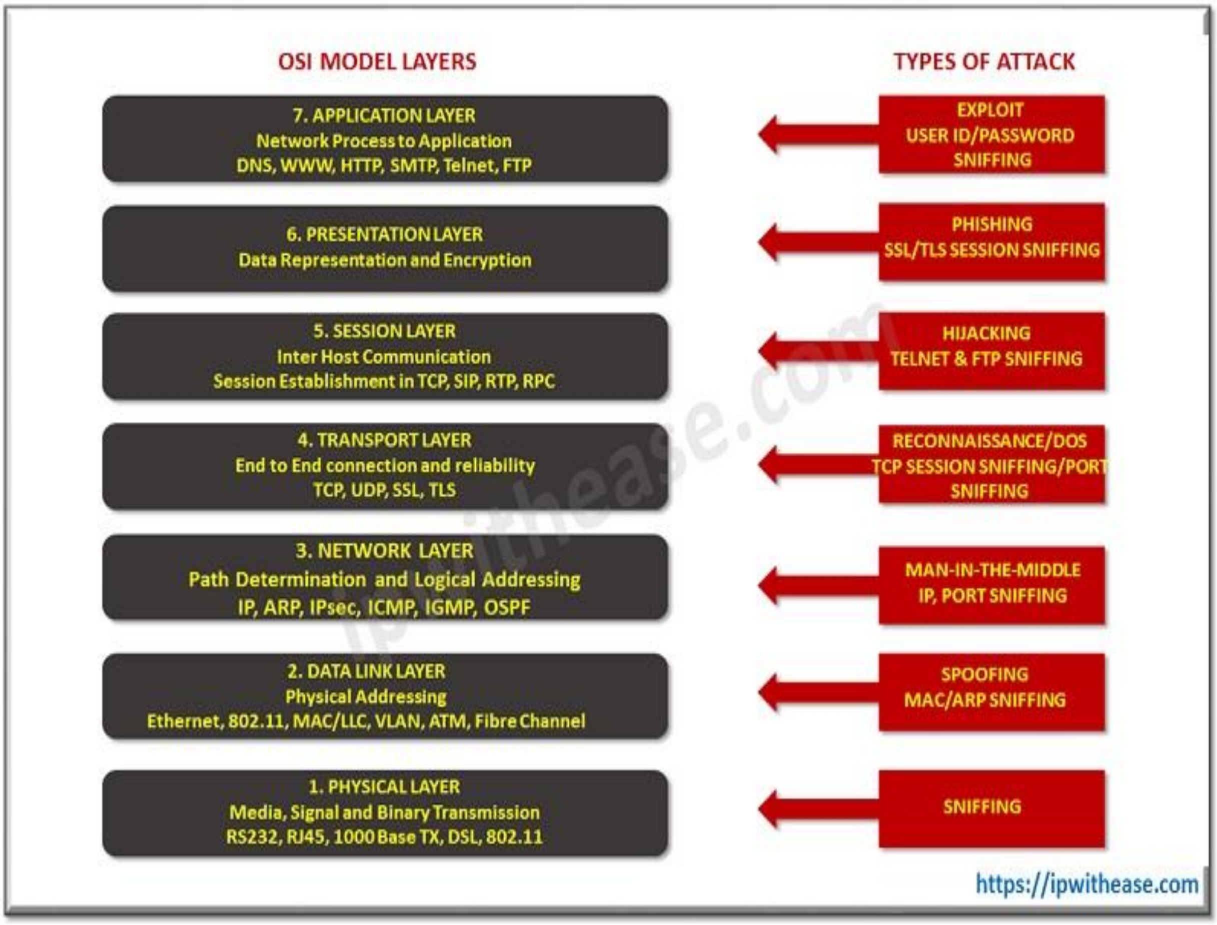
Week 3
Day 1 Session 2

OSI model is a reference model to understand how computer networks operate and communicate. Using this ISO standard, organizations can understand where network vulnerabilities may exist within their infrastructure and apply controls appropriately. OSI is hierarchical model which supports in understanding of how packets move throughout a network and how attacks and can disrupt can occur at any level.

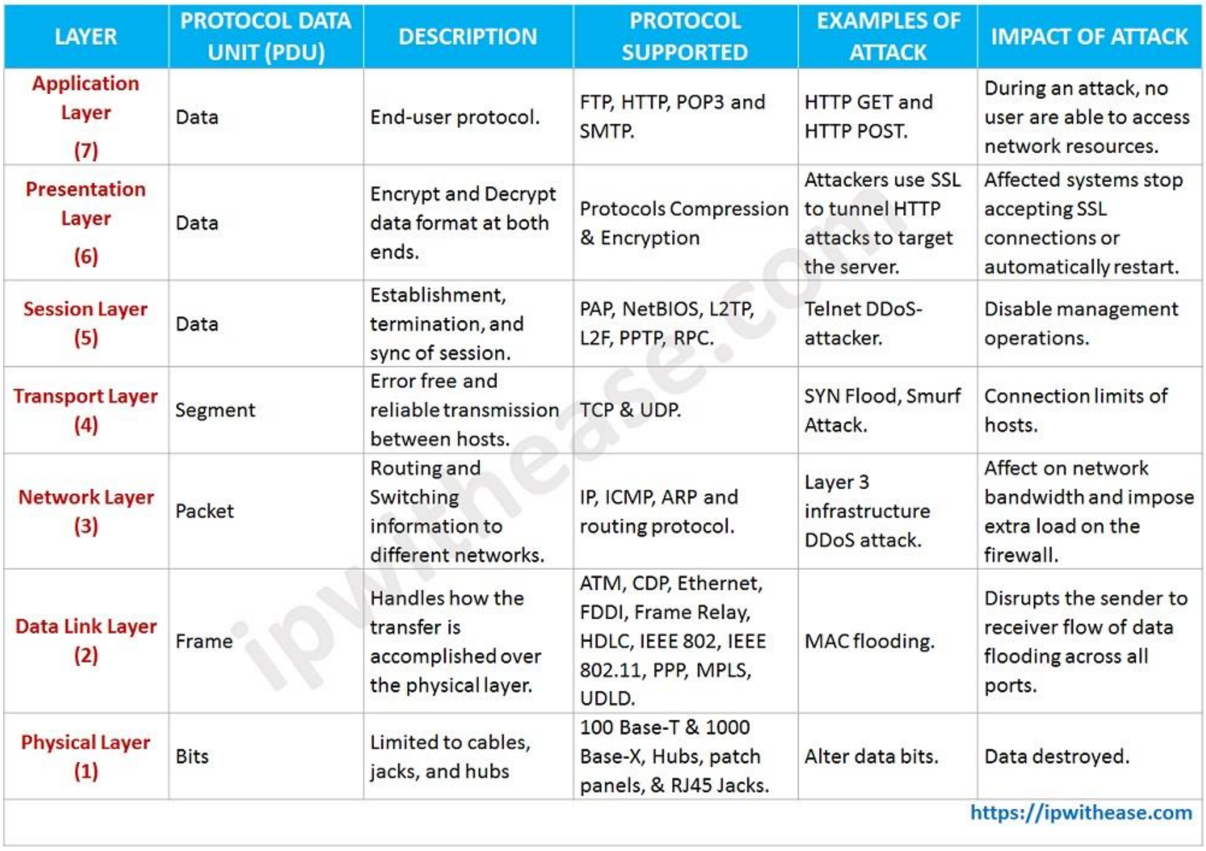
Network Vulnerabilities And the OSI Model Layers:



OSI MODEL LAYERS	TYPES OF ATTACK
7. APPLICATION LAYER Network Process to Application DNS, WWW, HTTP, SMTP, Telnet, FTP	EXPLOIT USER ID/PASSWORD SNIFFING
6. PRESENTATION LAYER Data Representation and Encryption	PHISHING SSL/TLS SESSION SNIFFING
5. SESSION LAYER Inter Host Communication Session Establishment in TCP, SIP, RTP, RPC	HIJACKING TELNET & FTP SNIFFING
4. TRANSPORT LAYER End to End connection and reliability TCP, UDP, SSL, TLS	RECONNAISSANCE/DOS TCP SESSION SNIFFING/PORT SNIFFING
3. NETWORK LAYER Path Determination and Logical Addressing IP, ARP, IPsec, ICMP, IGMP, OSPF	MAN-IN-THE-MIDDLE IP, PORT SNIFFING
2. DATA LINK LAYER Physical Addressing Ethernet, 802.11, MAC/LLC, VLAN, ATM, Fibre Channel	SPOOFING MAC/ARP SNIFFING
1. PHYSICAL LAYER Media, Signal and Binary Transmission RS232, RJ45, 1000 Base TX, DSL, 802.11	SNIFFING

https://ipwithease.com

Below table enlists the OSI layer, supported protocols and corresponding network vulnerabilities associated with the respective layer.



LAYER	PROTOCOL DATA UNIT (PDU)	DESCRIPTION	PROTOCOL SUPPORTED	EXAMPLES OF ATTACK	IMPACT OF ATTACK
Application Layer (7)	Data	End-user protocol.	FTP, HTTP, POP3 and SMTP.	HTTP GET and HTTP POST.	During an attack, no user are able to access network resources.
Presentation Layer (6)	Data	Encrypt and Decrypt data format at both ends.	Protocols Compression & Encryption	Attackers use SSL to tunnel HTTP attacks to target the server.	Affected systems stop accepting SSL connections or automatically restart.
Session Layer (5)	Data	Establishment, termination, and sync of session.	PAP, NetBIOS, L2TP, L2F, PPTP, RPC.	Telnet DDoS-attacker.	Disable management operations.
Transport Layer (4)	Segment	Error free and reliable transmission between hosts.	TCP & UDP.	SYN Flood, Smurf Attack.	Connection limits of hosts.
Network Layer (3)	Packet	Routing and Switching information to different networks.	IP, ICMP, ARP and routing protocol.	Layer 3 infrastructure DDoS attack.	Affect on network bandwidth and impose extra load on the firewall.
Data Link Layer (2)	Frame	Handles how the transfer is accomplished over the physical layer.	ATM, CDP, Ethernet, FDDI, Frame Relay, HDLC, IEEE 802, IEEE 802.11, PPP, MPLS, UDLD.	MAC flooding.	Disrupts the sender to receiver flow of data flooding across all ports.
Physical Layer (1)	Bits	Limited to cables, jacks, and hubs	100 Base-T & 1000 Base-X, Hubs, patch panels, & RJ45 Jacks.	Alter data bits.	Data destroyed.

https://ipwithease.com

Why We Need Security at Each Layer of OSI Model:

Network demands security against attackers and hackers.

Protecting confidentiality, integrity, availability of Data.

Network Security includes two basic securities i.e. Information Security and Computer Security.

Requires firewall for protecting systems or data from being attacked.

Top Network Vulnerabilities (Security Threats):

Privilege Escalation

Worm

Virus

Trojan

Spyware

Spam

Botnet

Logic Bomb

Layer 1: Physical Layer Security

Layer 1 refers to the physical aspect of networking disrupting this service, primarily resulting in Denial of Service (DoS) attacks**. Network vulnerabilities/threats** which occur at this level are the following:

1) Access Control

Permitting only authorized personnel to access.

Physical security keeps safe from unauthorized access.

Restricting access to critical servers and using strong passwords can prevent many attacks.

2) Damage data bits

3) Environmental issues

Environmental issues at the Physical layer include fire, smoke, water.

Less control over environmental factors such as temperature, humidity, dust, and ventilation can cause frequent failures.

4) Disconnection of Physical Links.

5) Backup

Layer 2 : Data Link security (Switch Security)

Layer 2 of the OSI model is the data link layer and focuses on the methods of delivering frame. Normally, this consists of switches utilizing protocols such as the Spanning Tree Protocol (STP) and the Dynamic Host Configuration Protocol (DHCP). Switches provide LAN connectivity and majority of threats come from internal LAN-

1) ARPs/ARP spoofing

ARP spoofing is targeted to rogue switch to forward packets to a different VLAN.

Security vulnerability occurs at the lower layer of OSI model but affects upper layer security.

To prevent this attack, configuration is performed to ignore gratuitous ARPs.

Edge VLAN (Private VLANs) segregation and ARP inspection is used to mitigate this threat.

(In cybersecurity, ‘spoofing’ is when fraudsters pretend to be someone or something else to win a person’s trust. The motivation is usually to gain access to systems, steal data, steal money, or spread malware.)

2) MAC Flooding (Media Access Control)

MAC flooding is the attack on the network switch.

MAC Flooding occurs when the MAC table of a switch reaches its capacity and then floods.

A malicious user can sniff the flooded traffic to gather network sensitive information.

Cisco switches have a port option that prevents such flooding.

Configuration CLI is as below: –

```
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
Switchport port-security mac-address sticky.
```

Authentication with AAA server.

(sniffing is the act of intercepting and monitoring traffic on a network. This can be done using software that captures all data packets passing through a given network interface or by using hardware devices explicitly designed for this purpose.)

3) Spanning Tree Attacks

Occurs when an attacker inserts itself into a data stream and causes a DoS attack.

STP attack begins with a physical attack by a malicious user who inserts an unauthorized switch. Attacker assigns a lower root priority. Assigning the lower root priority causes the network connection between two switches to be dropped. The attacker’s switch thereby becomes the root switch, and the attacker get full control to data transmitted between all switches.

One-way of mitigating this problem is configuring a network’s root switch with Root Priority = 0.

Other Data Link attacks are –

4) Private VLAN attack

5) Multicast brute force attack

6) Random frame stress attack

Layer 3 : Network Security (Router Security)

Layer 3 is the Network layer, which utilizes multiple common protocols to perform routing on the network. Layer 3 protocol attacks consist of Internet Protocol (IP), packet sniffing and DoS attacks i.e. ICMP attacks or ping of death. These types of attacks can be performed remotely. To reduce the risk of these types of attacks, packet filtering controls should be used.

IP Address Spoofing

Routing attacks

Back Hole/Selective Forwarding

(Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.)

1) IP Address Spoofing

IP address spoofing is also known as IP address forgery or a host file hijack. This can be mitigated by deploying packet filtering to detect inconsistencies.

2) Back Hole

In this attack malicious node pretends like normal node and forward packets but selectively drops some packets.

Malicious node acts like a black hole, it discards all the packets passing through it.

Layer 4 : Transport Layer Security

Layer 4 is the transport layer and utilizes common transport protocols to enable network communication. This layer includes the Transport Control Protocol (TCP) and User Datagram Protocol (UDP). Port scanning is a method to identify vulnerable or open network port.

1) SYN Flood

Also known as Half open attack or TCP Sync Flood.

It includes DDoS attack on server.

Attack involves having a client repeatedly send SYN (synchronization) packets to every port on a server, using rogue IP addresses in order to make it over consumed and unresponsive.

Exploits TCP three-way handshake.

2) Smurf Attack

Smurf arrack is a DoS Attack in which a system is flooded with spoofed ping messages.

Attacker generates lots of ICMP Packets with the intended victims IP Address and Broadcasts those packets. As a result, most of devices in network respond.

Layer 5 : Session layer Security

Some of the most common attacks in this layer are –

1) Session Hijacking

Security attack on a user session. A session hijacking attack works when it compromises the token by guessing what an authentic token session will be, thus acquiring unauthorized access to the Web server.

2) MITM Attack

Common ways of Session Hijacking are Packet Sniffers and Cross Site Scripting (XSS Attack).

Layer 6 : Presentation Layer Security

SSL Hijacking

Superfish uses a process called SSL hijacking to get user's encrypted data. When Internet browser connects to the HTTP (insecure) site, HTTP server redirects to the HTTPS (secure) version. HTTPS server provides a certificate, this certificate provides an identification to user to get in and access to server. The connection is completed now.

Layer 7 : Application Layer Security

There are different attacks on application layer and some of them are: –

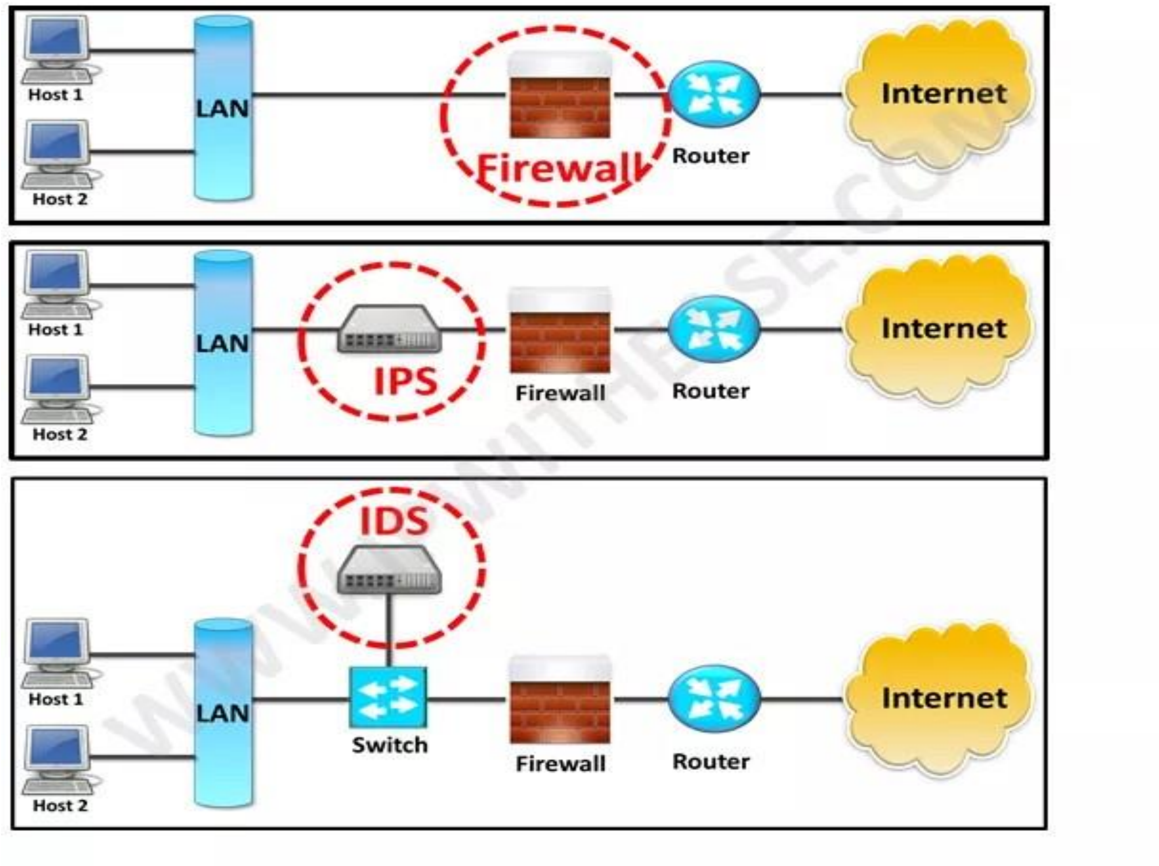
Virus
Worm
Phishing
Key Loggers
Backdoors
Program logic flaws
Bugs
Trojan Horses

Summary

OSI model is fundamental of understanding how networks communicate from the wire through to the application. This article has briefly looked at the OSI model, including the protocols and attacks that are utilized at each layer.

Day 2 Session 1

IDS vs IPS vs Firewall – Know the Difference



IDS vs IPS vs Firewall

A very common query asked by network and security administrators is the difference between Firewall, IPS and IDS.

All the 3 terms related to providing security to network and are considered essential components of a Network especially Data Center Network.

The main difference being that firewall performs actions such as blocking and filtering of traffic while an IPS/IDS detects and alert a system administrator or prevent the attack as per configuration.

A firewall allows traffic based on a set of rules configured. It relies on the source, the destination addresses, and the ports. A firewall can deny any traffic that does not meet the specific criteria.

IDS is a passive device which watches packets of data traversing the network, comparing with signature patterns and setting off an alarm on detection on suspicious activity. On the contrary, IPS is an active device working in inline mode and prevent the attacks by blocking it.

Furthermore, below table enumerates the difference between Firewall vs IDS vs IPS in detail –

PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.

PARAMETER	FIREWALL	IPS	IDS
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	> Stateful packet filtering > permits and blocks traffic by port/protocol rules	> Anomaly based detection > Signature detection > Zero day attacks > Blocking the attack	> Anomaly based detection > Signature detection > Zero day attacks > Monitoring > Alarm

https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

What Is IPsec?

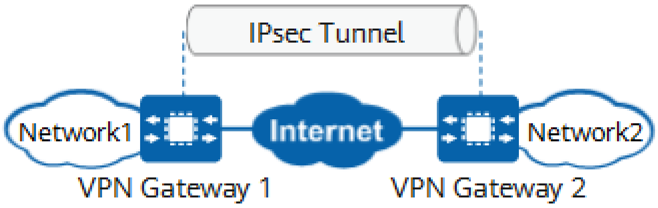
Internet Protocol Security (IPsec) is a suite of protocols and services that provide security for IP networks. It is a widely used virtual private network (VPN) technology. IP packets lack effective security mechanisms and may be forged, stolen, or tampered with when being transmitted on a public network, such as the Internet. To solve this problem, the communicating parties establish an IPsec tunnel for encrypted transmission of IP packets. This ensures secure transmission of IP packets on an insecure network, such as the Internet.

What Is an IPsec VPN?

Virtual private network (VPN) is a technology for establishing a private network on a public network. It is a logical network over a public network such as the Internet, allowing user data to be transmitted through a logical link. This is different from a traditional private network, where user data is transmitted through an end-to-end physical link.

Common VPN protocols include IPsec, Secure Sockets Layer (SSL), Generic Routing Encapsulation (GRE), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP). IPsec is a commonly used VPN technology and applies to multiple network access scenarios.

IPsec VPN is a VPN technology that uses IPsec for remote access. The technology allows establishing an IPsec tunnel between two or more private networks on a public network and using encryption and authentication algorithms to ensure the security of VPN connections.

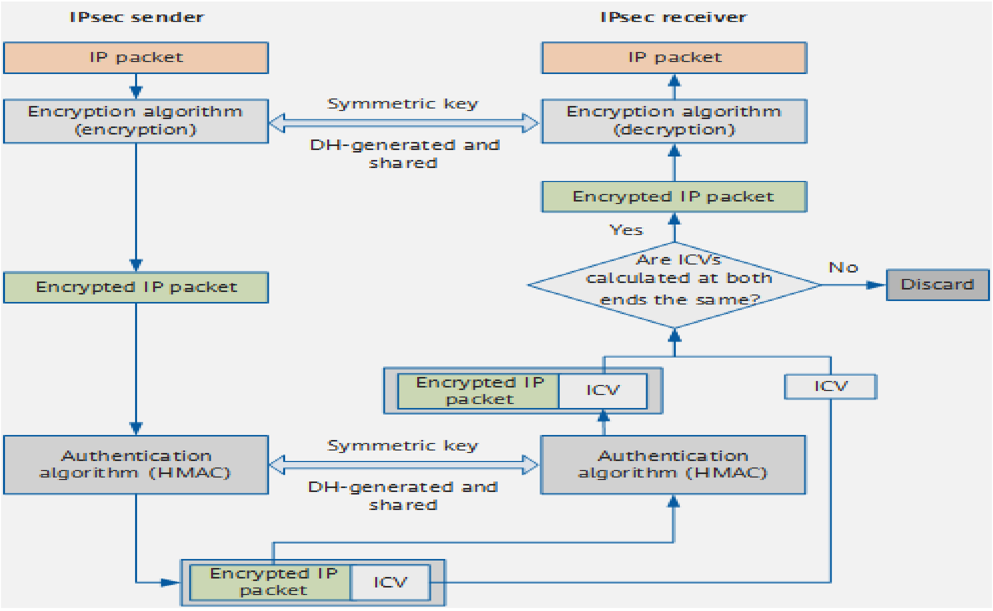


IPsec VPN protects point-to-point communication by establishing secure tunnels between hosts, between hosts and network security gateways, or between network security gateways (such as routers and firewalls). It operates at the IP layer to encrypt and authenticate data packets.

Compared with other VPN technologies, IPsec VPN is more secure because data is encrypted for transmission in IPsec tunnels. However, the configuration and networking deployment of IPsec VPN are more complex.

IPsec VPN

In the following figure, the IPsec sender uses the encryption algorithm and encryption key to encrypt an IP packet, that is, it encapsulates the original data. Then the sender and receiver use the same authentication algorithm and authentication key to process the encrypted packets to obtain the **integrity check value** (ICV). If the ICVs obtained at both ends are the same, the packet is not tampered with during transmission, and the receiver decrypts the packet. If the ICVs are different, the receiver discards the packet.



(** This hash, an **integrity check value** (ICV), can be either Message Authentication Code (MAC) or a digital signature.)

What is an SSL Certificate?

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).

It does this by making sure that any data transferred between users and sites, or between two systems **remain impossible to read**. It uses encryption algorithms to **scramble** data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL from DigiCert you are actually buying the most up-to-date TLS certificates with the option of ECC, RSA or DSA encryption.

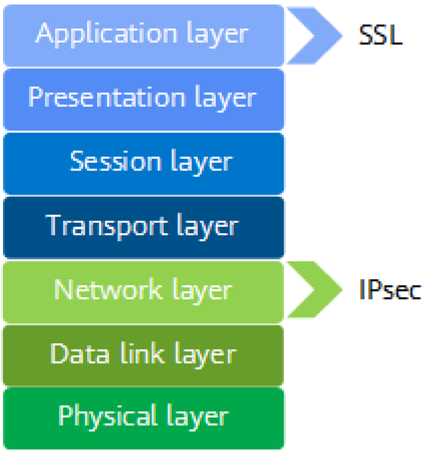
HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. The details of the certificate, including the issuing authority and the corporate name of the website owner, can be viewed by clicking on the lock symbol on the browser bar.

IPsec VPN vs SSL VPN

IPsec and SSL are the most commonly used VPN technologies. Both of them have encryption and authentication mechanisms to ensure remote access security. The following compares IPsec VPN and SSL VPN:

- Working layers of the OSI reference model

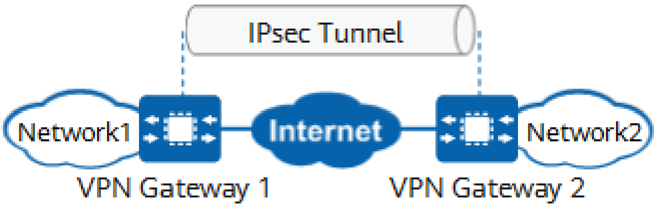
  OSI defines a seven-layer framework for network interconnection: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. IPsec works at the network layer and directly runs over the Internet Protocol (IP). SSL, working at the application layer, is an **application-layer protocol that encrypts HTTP traffic instead of IP packets.**



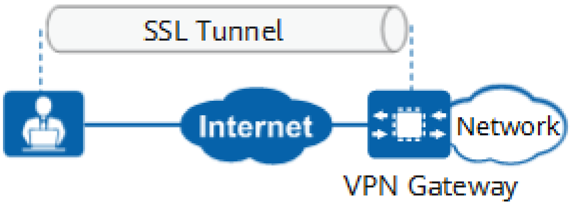
Working layers of IPsec and SSL

- Configuration and deployment

  IPsec VPN is applicable to site-to-site networking. In this networking, VPN gateways must be deployed at each site, or remote users need to install dedicated VPN clients. Therefore, the configuration and deployment are complex, and the maintenance cost is high. SSL VPN is applicable to client-to-site networking. In this networking, remote users only need to install the specified plug-in on the standard SSL-supporting browser. A VPN gateway is deployed in a data center for centralized management and maintenance. Therefore, the configuration and deployment are simple, and the maintenance cost is low.

  IPsec VPN

  SSL VPN

- Security

  IPsec works at the network layer to protect all data transmitted between sites. IPsec VPN requires remote users to install a dedicated VPN client or deploy a VPN gateway at the site. User access is checked by the client or gateway in terms of user authentication rules, security policy rules, or content security filtering. Therefore, IPsec VPN is more secure. SSL VPN does not require dedicated clients or gateways at access sites. Therefore, SSL VPN is more vulnerable to security threats.

- Access control

  IPsec works at the network layer and cannot implement fine-grained access control based on applications. SSL VPN is more flexible in fine-grained access control. Network administrators can classify network resources into different types based on application types. Each type of resources has different access permissions.

Week 3 Day 4 Session 1

Introduction to Wireless Security

Wireless networks are complex; there are many technologies and protocols required to offer a stable wireless network to end-users. It also sounds scary to transmit data through the air, where everyone can listen to it.

Wired networks *feel* secure; after all, you can’t easily listen to this traffic. You could connect to a switchport, but the only unicast traffic you’ll see is the traffic between your computer and the switch. You will see multicast and broadcast traffic from within the VLAN, though.

~~**Anyone can see the data that travels through the air**, which is why wireless security is so important. Someone can monitor wireless traffic, and you won’t even notice that it’s happening.~~

Wireless Topologies

The **802.11** standard identifies two main wireless topology modes: **infrastructure** mode and **Independent Basic Service Set (IBSS).** IBSS is also knows as **ad hoc** mode. With the ubiquity of wireless networks, mesh topologies are now common.

Infrastructure Mode

With infrastructure mode, **wireless clients interconnect via an AP**. Figure 22-4 illustrates infrastructure mode terminology. Notice that the configuration of the APs to share the same SSID allows wireless clients to roam between BSAs.

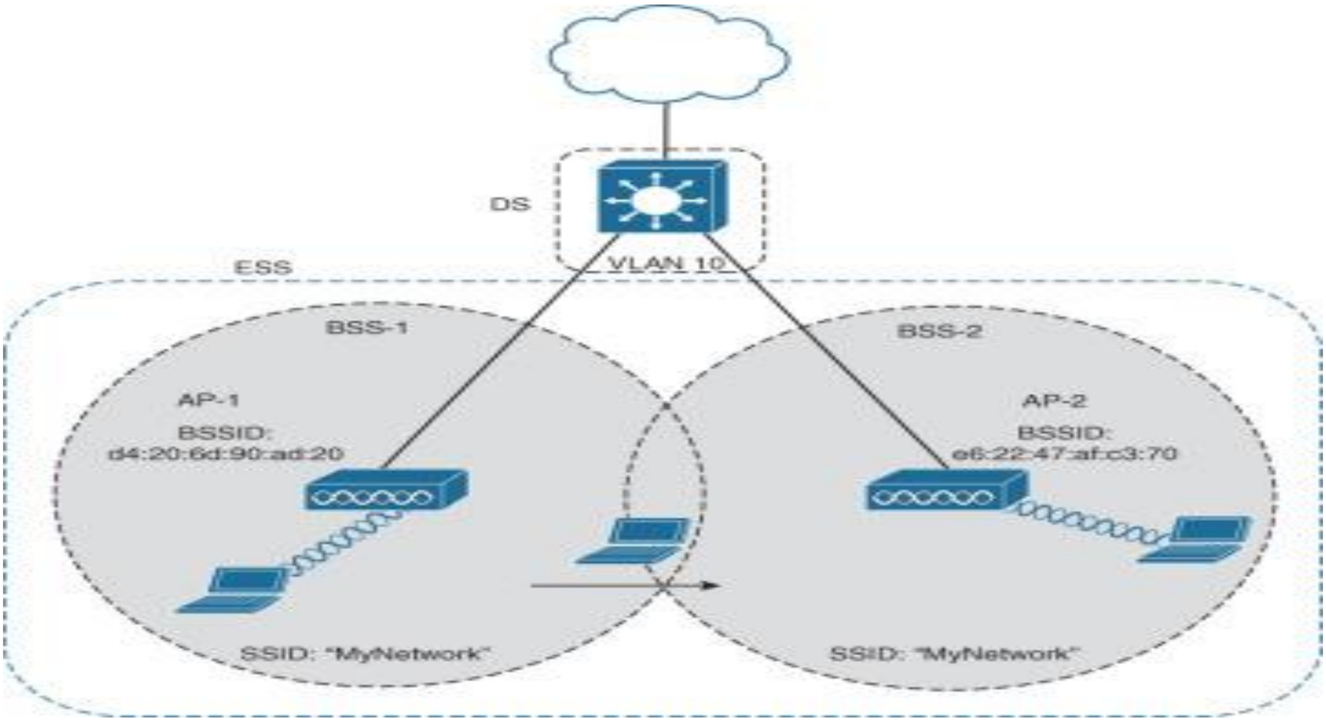


Figure 22-4 Example of ESS Infrastructure Mode

Infrastructure mode terminology includes the following:

- **Basic service set (BSS):** This consists of a single AP interconnecting all associated wireless clients.
- **Basic service area (BSA):** This is the area that is bound by the reach of the AP’s signal. The BSA is also called a *cell* (the gray area in Figure 22-4).
- **Basic service set identifier (BSSID):** This is the unique, machine-readable identifier for the AP that is in the format of a MAC address and is usually derived from the AP’s wireless MAC address.
- **Service set identifier (SSID):** This is a human-readable, non-unique identifier used by the AP to advertise its wireless service.
- **Distribution system (DS):** APs connect to the network infrastructure using the wired DS, such as Ethernet. An AP with a wired connection to the DS is responsible for translating frames between 802.3 Ethernet and 802.11 wireless protocols.
- **Extended service set (ESS):** When a single BSS provides insufficient coverage, two or more BSSs can be joined through a common DS into an ESS. An ESS is the union of two or more BSSs interconnected by a wired DS. Each ESS is identified by its SSID, and each BSS is identified by its BSSID.

P

IBSS, or Ad Hoc Mode

In the 802.11 standard, Independent Basic Service Set (IBSS) is defined as two devices connected wirelessly in a peer-to-peer (P2P) manner without the use of an AP. One device takes the role of advertising the wireless network to clients. The IBSS allows two devices to communicate directly without the need for any other wireless devices, as shown in Figure 22-5. IBSSs do not scale well beyond 8 to 10 devices.

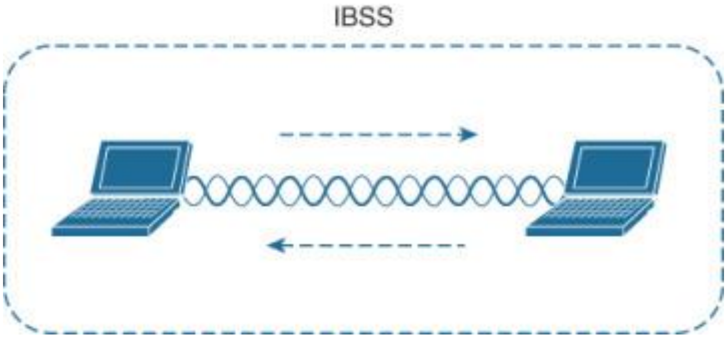


Figure 22-5 802.11 Independent Basic Service Set

Mesh

Having a wired DS connecting all APs is not always practical or necessary. Instead, APs can be configured to connect in mesh mode. In this mode, APs bridge client traffic between each other, as shown in Figure 22-6.

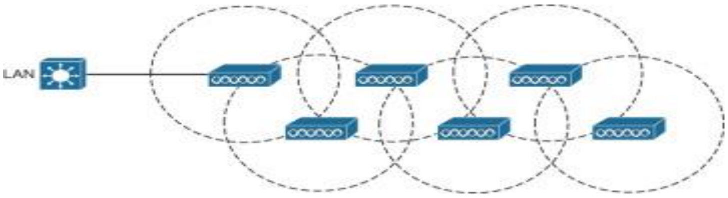
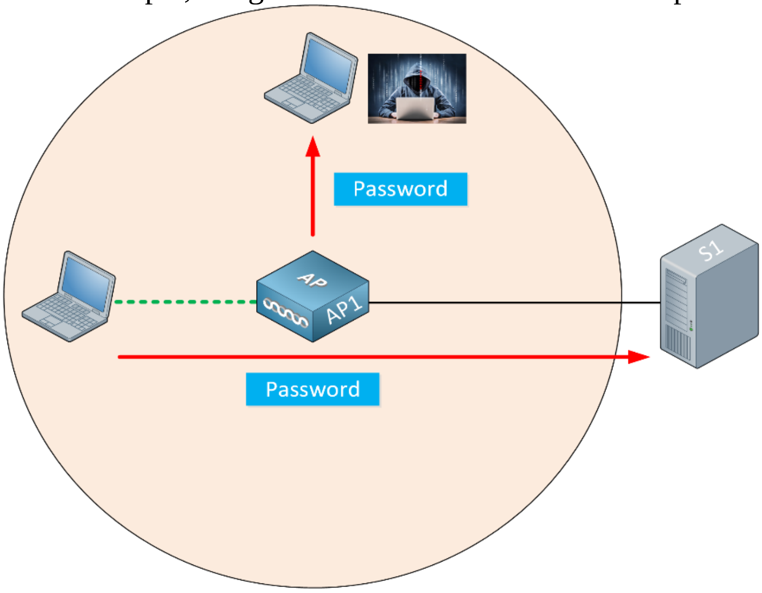


Figure 22-6 Example of a Wireless Mesh Network

Each AP in the mesh maintains a BSS on one channel used by wireless clients. Then the APs bridge between each other using other channels. The mesh network runs its own dynamic routing protocol to determine the best path to the wired network.

~~In the 802.11 service sets lesson, you learned how wireless clients associate with APs~~. All wireless traffic has to go through the AP, instead of directly between the sender and receiver. **Anyone in range of the AP or other wireless clients can receive the signal**.

This can be a problem. For example, imagine we have a user who sends a password to a remote server:



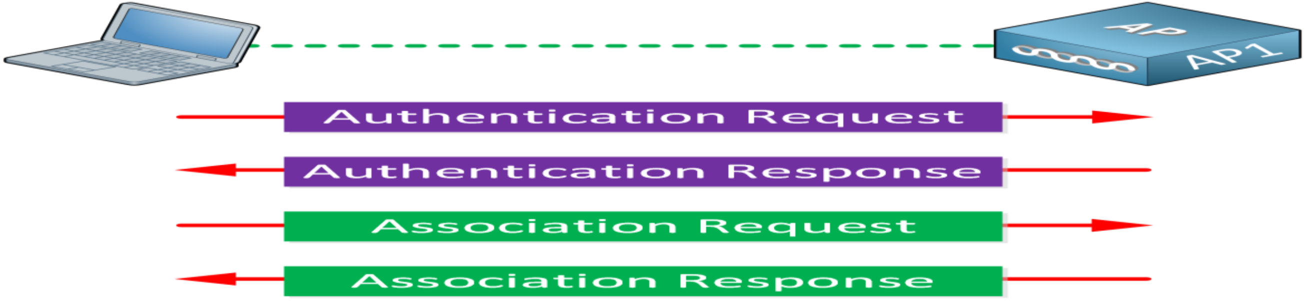
The wireless user transmits a password to the remote server. Because the attacker is in range of our wireless network, he can capture the password.

How can we securely transmit data through the air and ensure that it remains private and is not tampered with? The 802.11 standard offers security mechanisms that provide **authentication**, **encryption,** and **integrity**. ~~In this lesson, I'll give you an overview of these three items.~~

Authentication

To use a wireless network, the wireless client has to discover a BSS(**Basic service set (BSS):** This consists of a single AP interconnecting all associated wireless clients).

APs advertise beacons(Management Packets) with their SSID, and the wireless client selects the wireless network it wants to connect to and associates with the AP. By default, **authentication is open,** which means everyone is welcome.

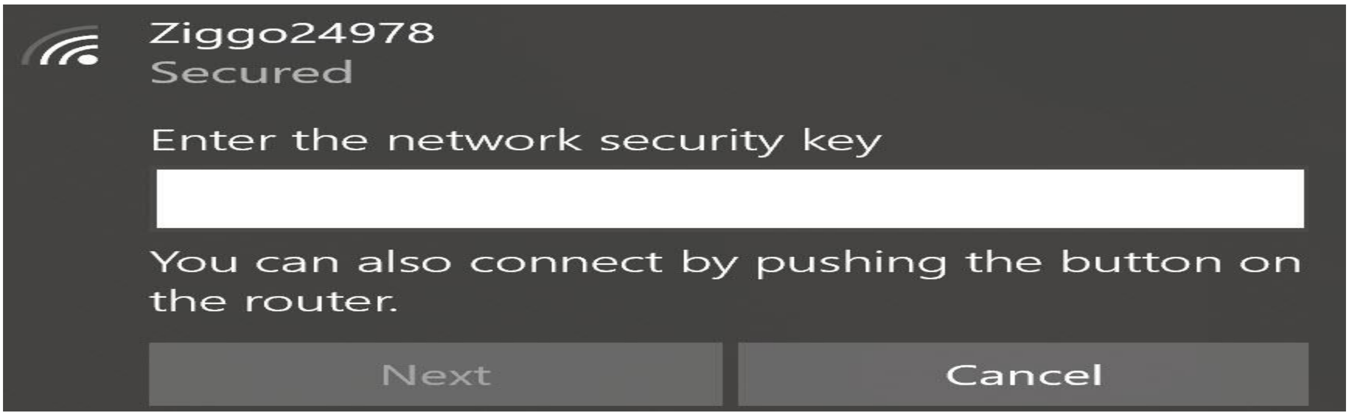


~~You probably want to authenticate your wireless clients, though. If you have a corporate network, you don't want just anyone to join the network. Only legitimate users should be able to use your wireless network. After all, the wireless network might be connected to the wired network where you can access all corporate resources.~~

What if you have guest users? If you want to offer a guest wireless network, you should configure a **second SSID, linked to a VLAN with restricted access**.

APs can authenticate wireless clients **before they associate with the AP**. This keeps **rogue clients** away from our wireless network.

There are many options for wireless authentication. You are probably familiar with the most common choice, a **pre-shared key**. We configure the pre-shared key on the AP. Any wireless client that wants to join the wireless network has to enter the pre-shared key.



Ziggo24978
Secured

Enter the network security key

You can also connect by pushing the button on the router.

What happens when someone steals one of the wireless clients? That's a problem because of two main reasons:

- The attacker has access to your pre-shared key:
  - And can now connect to the wireless network from any device.
  - And can decrypt traffic from other clients connected to the same wireless network.
- You need to configure a new pre-shared key on the AP and all wireless clients.

There are stronger authentication options where we ask users for a username and password instead. This helps. When a device is stolen, at least you can pinpoint which username was compromised and reset the password for that username. You don't have to reset the pre-shared key and configure it on all wireless clients.

Wireless Security Protocols

Wireless traffic is inherently different from traffic traveling over a wired infrastructure. Any wireless device operating in the same frequency can hear the frames and potentially read them. Therefore, WLANs need to be secured to allow only authorized users and devices and to prevent eavesdropping and tampering of wireless traffic.

Wireless Authentication Methods

For wireless devices to communicate over a network, they must first associate with the AP. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. During this process, transmitted frames can reach any device within range. If the wireless connection is not secured, then others can read the traffic, as shown in Figure 22-11.

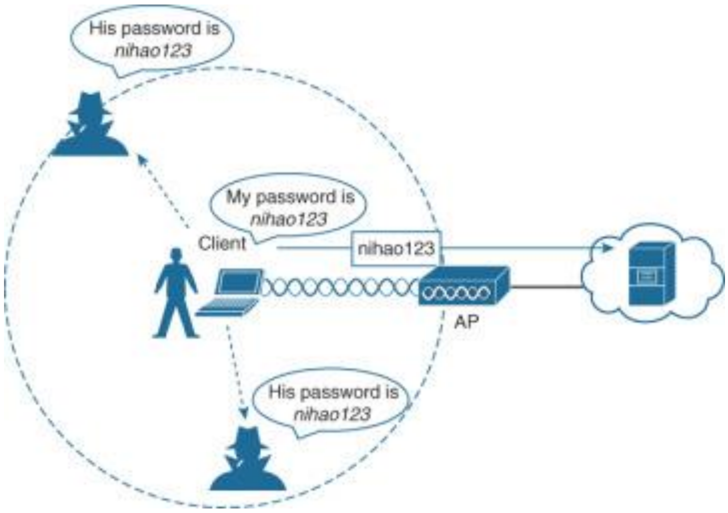


Figure 22-11 **Open Wireless Network**

The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

- **Open system authentication:** Should only be used in situations where security is of no concern. The wireless client is responsible for providing security such as by using a virtual private network (VPN) to connect securely.
- **Shared key authentication:** Provides mechanisms shown in Table 22-3 to authenticate and encrypt data between a wireless client and an AP. However, the password must be pre-shared between the parties to allow connection.

Table 22-3 Shared Key Authentication Methods

Authentication Method	**Description**
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a **static** key. However, the key never changes when exchanging packets. This makes WEP easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger **Temporal Key Integrity Protocol (TKIP)** encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	The current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

WPA and WPA2

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. WPA2 authentication methods included the following:

- **Personal:** Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise:** Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server, and then users must authenticate using the 802.1X standard, which uses Extensible Authentication Protocol (EAP) for authentication.

802.1X/EAP

With open and WEP authentication, wireless clients are authenticated locally at the AP without further intervention. The scenario changes with 802.1X: The client uses open authentication to associate with the AP, and then the client authentication process occurs at a dedicated authentication server. Figure 22-11 shows the three-party 802.1X arrangement, which consists of the following entities:

- **Supplicant:** The client device that is requesting access.
- **Authenticator:** The network device that provides access to the network. In Figure 22-11, the AP forwards the supplicant's message to the WLC.
- **Authentication server (AS):** The device that permits or denies network access based on a user database and policies (usually a RADIUS server).

WPA3

WPA3 includes four features:

- **WPA3-Personal:** In WPA2-Personal, threat actors can listen in on the "handshake" between a wireless client and the AP and use brute-force attacks to try to guess the PSK. WPA3-Personal thwarts such attacks by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.
- **WPA3-Enterprise:** WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) suite, which is commonly used in high-security Wi-Fi networks.
- **Open networks:** Open networks in WPA2 send user traffic in unauthenticated plaintext. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.
- **IoT onboarding:** Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices that were not previously configured, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration and need any easy way to get connected to the wireless network. Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hard-coded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although DPP is not strictly part of the WPA3 standard, it will replace WPS over time.

Wireless Encryption Methods

Encryption is used to protect data. An intruder may be able to captured encrypted data, but he or she would not be able to decipher it in any reasonable amount of time. The following encryption protocols are used with wireless authentication:

- **Temporal Key Integrity Protocol (TKIP):** TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment and addresses the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP but encrypts the Layer 2 payload using TKIP and carries out a message integrity check (MIC) in the encrypted packet to ensure that the message has not been altered.
- **Advanced Encryption Standard (AES):** AES is the encryption method used by WPA2. It is the preferred method because it is a very strong method of encryption. It uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), which allows destination hosts to recognize if the encrypted and nonencrypted bits have been altered.
- **The Galois/Counter Mode Protocol (GCMP):** This is a robust authenticated encryption suite that is more secure and more efficient than CCMP. GCMP is used in WPA3.

Table 22-4 summarizes the basic differences between WPA, WPA2, and WPA3. Each successive version is meant to replace prior versions and offer better security features. You should avoid using WPA and use WPA2 instead—at least until WPA3 becomes widely available on wireless client devices, APs, and WLCs.

Table 22-4 Wireless Authentication and Encryption Comparison

Feature	**WPA**	**WPA2**	**WPA3**
Authentication with pre-shared keys?	Yes	Yes	Yes
Authentication with 802.1X?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

[Content collected from https://www.ciscopress.com/articles/article.asp?p=2999384

https://networklessons.com/cisco/ccna-200-301/wireless-authentication-methods

https://networklessons.com/cisco/ccna-200-301/introduction-to-wireless-security

https://wiki.apnictraining.net/netsec-20220627-bdnog14/agenda

https://academy.apnic.net/wp-content/uploads/2020/12/Webinar-Wifi-Security-FIN.pdf

Suggested Read

https://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/5.1.0/administration/guide/C1_Network_Security.html#wp1050709

https://www.ibm.com/in-en/products/maas360/mobile-security?utm_content=SRCWW&p1=Search&p4=43700068113644641&p5=p&gclid=Cj0KCQiAyM

KbBhD1ARIsANs7rEFW1yV_nYVVadP2EqkgkLGeA9jpTpuZoWWHKrTs6DxAcFpn1_bIFk8aAkd3EALw_wcB&gclsrc=aw.ds

]

OWASP Juice Shop
https://pwning.owasp-juice.shop/part1/running.html

From sources

1. Install Node.js on your computer.
2. On the command line run `git clone https://github.com/juice-shop/juice-shop.git --depth 1`.
3. Go into the cloned folder with `cd juice-shop`
4. Run `npm install`. This only has to be done before the first start or after you changed the source code.
5. Run `npm start` to launch the application.
6. Browse to http://localhost:3000