Week 12 : Implementing Secure Network Designs

## **LESSON INTRODUCTION**

Managing user authentication and authorization is only one part of building secure information technology services. The network infrastructure must also be designed to run services with the properties of confidentiality, integrity, and availability. While design might not be a direct responsibility for you at this stage in your career, you should understand the factors that underpin design decisions, and be able to implement a design by deploying routers, switches, access points, and load balancers in secure configurations.

## **LESSON OBJECTIVES**

In this lesson, you will:

* Implement secure network designs.
* Implement secure routing and switching.
* Implement secure wireless infrastructure.
* Implement load balancers.

While you may not be responsible for network design in your current role, it is important that you understand the vulnerabilities that can arise from weaknesses in network architecture, and some of the general principles for ensuring a well-designed network. This will help you to contribute to projects to improve resiliency and to make recommendations for improvements.

**SECURE NETWORK DESIGNS**

A secure network design provisions the assets and services underpinning business workflows with the properties of confidentiality, integrity, and availability. Weaknesses in the network architecture make it more susceptible to undetected intrusions or to catastrophic service failures. Typical weaknesses include:

* Single points of failure—a "pinch point" relying on a single hardware server or appliance or network channel.
* Complex dependencies—services that require many different systems to be available. Ideally, the failure of individual systems or services should not affect the overall performance of other network services.
* Availability over confidentiality and integrity—often it is tempting to take "shortcuts" to get a service up and running. Compromising security might represent a quick fix but creates long term risks.
* Lack of documentation and change control—network segments, appliances, and services might be added without proper change control procedures, leading to a lack of visibility into how the network is constituted. It is vital that network managers understand business workflows and the network services that underpin them.
* Overdependence on perimeter security—if the network architecture is "flat" (that is, if any host can contact any other host), penetrating the network edge gives the attacker freedom of movement.

**BUSINESS WORKFLOWS AND NETWORK ARCHITECTURE**

Network architecture is designed to support business workflows. You can illustrate the sorts of decisions that need to be made by analyzing a simple workflow, such as email:

* Access—the client device must access the network, obtaining a physical channel and logical address. The user must be authenticated and authorized to use the email application. The corollary is that unauthorized users and devices must be denied access.
* Email mailbox server—ensure that the mailbox is only accessed by authorized clients and that it is fully available and fault tolerant. Ensure that the email service runs with a minimum number of dependencies and that the service is designed to be resilient to faults.
* Mail transfer server—this must connect with untrusted Internet hosts, so communications between the untrusted network and trusted LAN must be carefully controlled. Any data or software leaving or entering the network must be subject to policy-based controls.

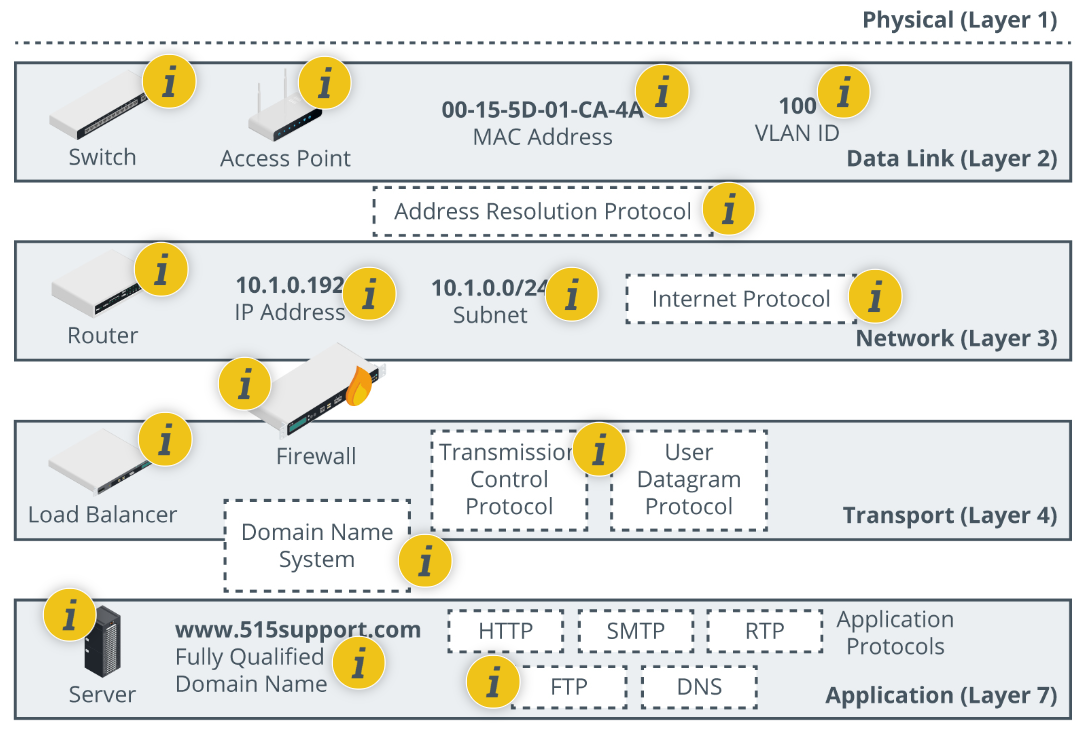
**NETWORK APPLIANCES**

A number of network appliances are involved in provisioning a network architecture:

* **Switches**—forward frames between nodes in a cabled network. Switches work at layer 2 of the OSI model*.*At layer 2 they make forwarding decisions based on the hardware or Media Access Control (MAC) address of attached nodes. Switches can establish network segments that either map directly to the underlying cabling or logical segments, created in the switch configuration as  **virtual LANs (VLANs)**.

*When designing and troubleshooting a network, it is helpful to compartmentalize functions to discrete layers. The Open Systems Interconnection (OSI) model is a widely quoted example of how to define layers of network functions.*

* Wireless access points—provide a bridge between a cabled network and wireless clients, or stations. Access points work at layer 2 of the OSI model.
* **Routers**—forward packets around an internetwork, making forwarding decisions based on IP addresses. Routers work at layer 3 of the OSI model. Routers can apply logical IP subnet addresses to segments within a network.
* Firewalls—apply an access control list (ACL) to filter traffic passing in or out of a network segment. Firewalls can work at layer 3 of the OSI model or higher.
* Load balancers—distribute traffic between network segments or servers to optimize performance. Load balancers can work at various layers of the OSI model.
* Domain Name System (DNS) servers—host name records and perform name resolution to allow applications and users to address hosts and services using fully qualified domain names (FQDNs) rather than IP addresses. DNS works at layer 7 of the OSI model. Name resolution is a critical service in network design. Abuse of name resolution is a common attack vector.



*Appliances, protocols, and addressing functions within the OSI network layer reference model.*

Week 12 Activity

Briefly describe all the appliances, protocols and addressing function within the OSI layer reference model.

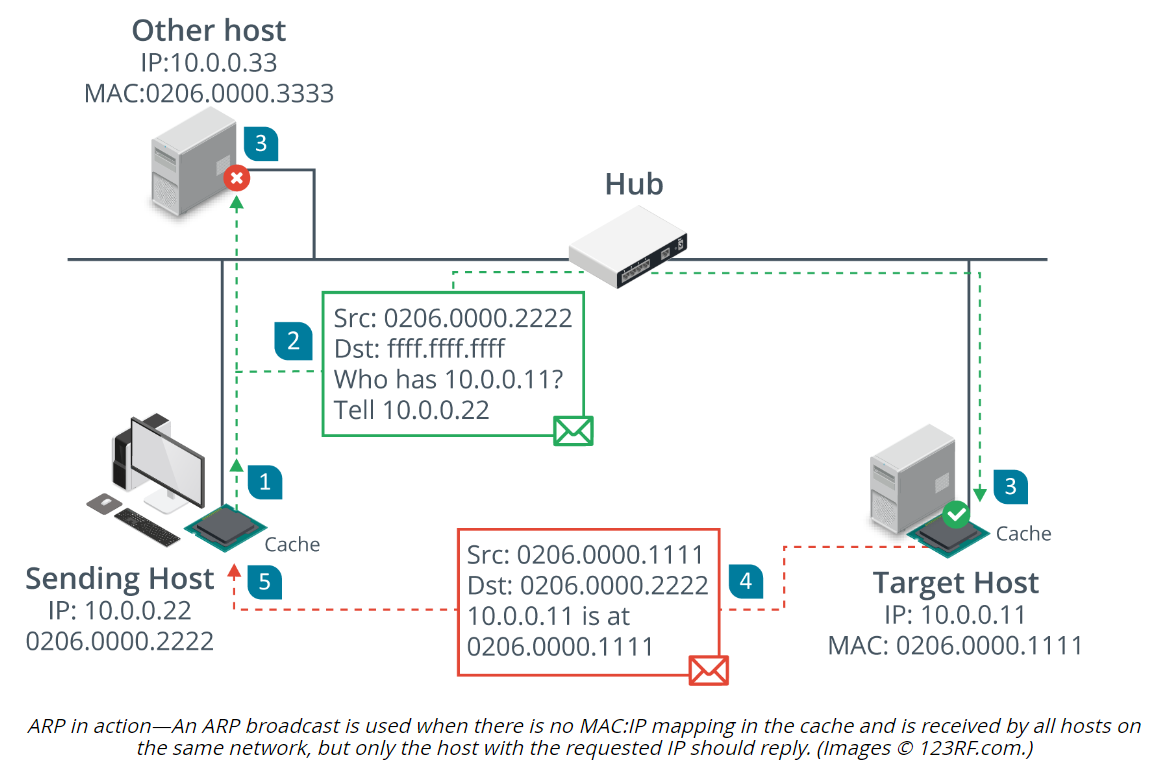
**ROUTING AND SWITCHING PROTOCOLS**

The basic function of a network is to forward traffic from one node to another. A number of routing and switching protocols are used to implement forwarding. The forwarding function takes place at two different layers:

* Layer 2 forwarding occurs between nodes on the same local network segment that are all in the same broadcast domain. At layer 2, a broadcast domain is either all the nodes connected to the same physical unmanaged switch, or all the nodes within a virtual LAN (VLAN) configured on one or more managed switches. At layer 2, each node is identified by the network interface's hardware or Media Access Control (MAC) address. A MAC address is a 48-bit value written in hexadecimal notation, such as 00-15-5D-F4-83-48.
* Layer 3 forwarding, or routing, occurs between both logically and physically defined networks. A single network divided into multiple logical broadcast domains is said to be subnetted. Multiple networks joined by routers form an internetwork. At layer 3, nodes are identified by an Internet Protocol (IP) address.

**Address Resolution Protocol (ARP)**

The Address Resolution Protocol (ARP) maps a network interface's hardware (MAC) address to an IP address. Normally a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an ARP Request packet, and the device with the matching IP responds with an ARP Reply.



**NETWORK SEGMENTATION**

A network **segment** is one where all the hosts attached to the segment can use local (layer 2) forwarding to communicate freely with one another. The hosts are said to be within the same broadcast domain. **Segregation** means that the hosts in one segment are restricted in the way they communicate with hosts in other segments. They might only be able to communicate over certain network ports, for instance.

*﻿"Freely" means that no network appliances or policies are preventing communications. Each host may be configured with access rules or host firewalls or other security tools to prevent access, but the "view from the network" is that hosts in the same segment are all free to attempt to communicate.*

Assuming an Ethernet network, network segments can be established physically by connecting all the hosts in one segment to one switch and all the hosts in another segment to another switch. The two switches can be connected by a router and the router can enforce network policies or access control lists (ACL) to restrict communications between the two segments.

**NETWORK TOPOLOGY AND ZONES**

Given the ability to create segregated segments with the network, you can begin to define a topology of different network zones. A topology is a description of how a computer network is physically or logically organized. The logical and physical network topology should be analyzed to identify points of vulnerability and to ensure that the goals of confidentiality, integrity, and availability are met by the design.

The main building block of a security topology is the zone. A **zone** is an area of the network where the security configuration is the same for all hosts within it. Zones should be segregated from one another by physical and/or logical segmentation, using VLANs and subnets. Traffic between zones should be strictly controlled using a security device, typically a firewall.

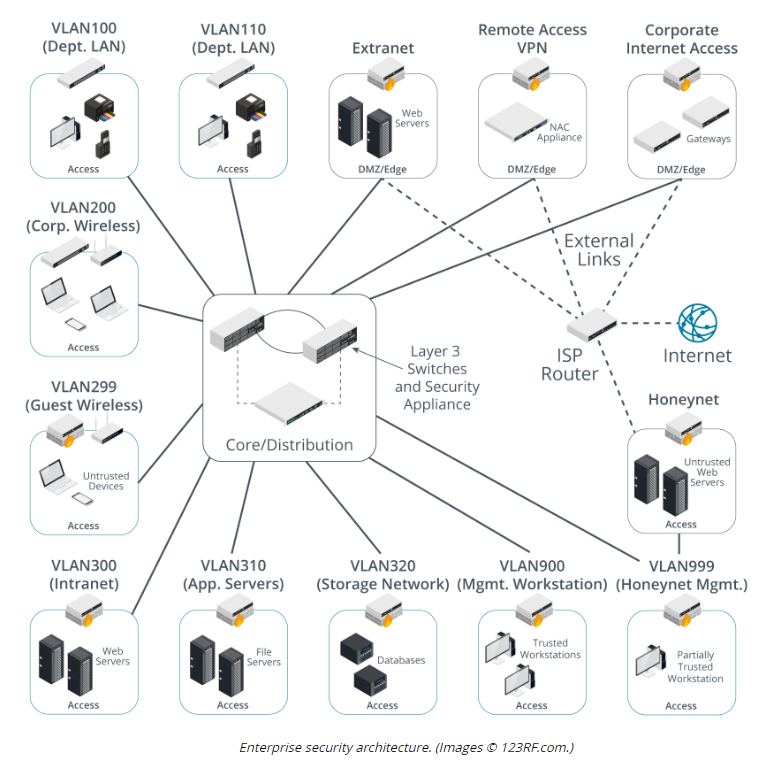
Dividing a campus network or data center into zones implies that each zone has a different security configuration. The main zones are as follows:

* **Intranet (private network)**—this is a network of trusted hosts owned and controlled by the organization. Within the intranet, there may be sub-zones for different host groups, such as servers, employee workstations, VoIP handsets, and management workstations.

*Hosts are trusted in the sense that they are under your administrative control and subject to the security mechanisms (antivirus software, user rights, software updating, and so on) that you have set up to defend the network.*

* Extranet—this is a network of semi-trusted hosts, typically representing business partners, suppliers, or customers. Hosts must authenticate to join the extranet.
* Internet/guest—this is a zone permitting anonymous access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the Internet.

A large network may need more zones to represent different host groups, such as separating wireless stations from desktop workstations, and putting servers in their own groups. Cisco's enterprise security architecture uses core and distribution layers to interconnect access blocks, with each access block representing a different zone and business function.



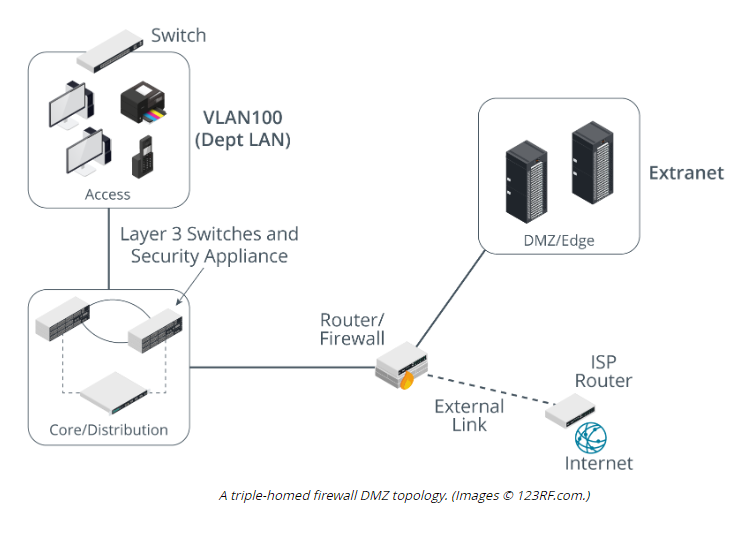
**DEMILITARIZED ZONES**

The most important distinction between different security zones is whether a host is Internet-facing. An Internet-facing host accepts inbound connections from and makes connections to hosts on the Internet. Internet-facing hosts are placed in one or more **demilitarized zones (DMZs)**. A DMZ is also referred to as a perimeter or edge network. The basic principle of a DMZ is that traffic cannot pass directly through it. A DMZ enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole. If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a proxy. For example, if an intranet host requests a connection with a web server on the Internet, a proxy in the DMZ takes the request and checks it. If the request is valid, it retransmits it to the destination. External hosts have no idea about what (if anything) is behind the DMZ.

Both **extranet** and Internet services are likely to be Internet-facing. The hosts that provide the extranet or public access services should be placed in one or more demilitarized zones. These would typically include web servers, mail and other communications servers, proxy servers, and remote access servers. The hosts in a DMZ are not fully trusted by the internal network because of the possibility that they could be compromised from the Internet. They are referred to as **bastion hosts** and run minimal services to reduce the attack surface as much as possible. A bastion host would not be configured with any data that could be a security risk to the internal network, such as user account credentials.

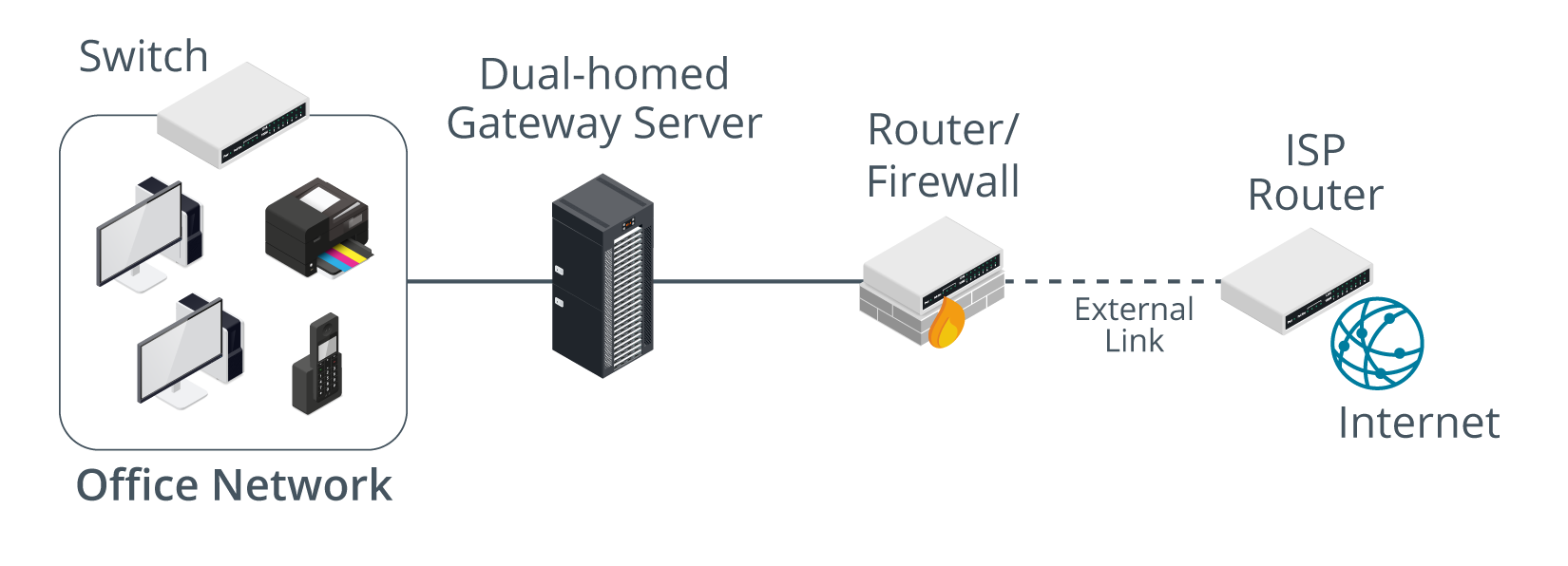
It is quite likely that more than one DMZ will be required as the services that run in them may have different security requirements :

* A DMZ hosting proxies or secure web gateways to allow employees access to web browsing and other Internet services.
* A DMZ hosting communication servers, such as email, VoIP, and conferencing.
* A DMZ for servers providing remote access to the local network via a Virtual Private Network (VPN).
* A DMZ hosting traffic for authorized cloud applications.
* A multi-tier DMZ to isolate front-end, middleware, and back-end servers.



**SCREENED HOSTS**

Smaller networks may not have the budget or technical expertise to implement a DMZ. In this case, Internet access can still be implemented using a dual-homed proxy/gateway server acting as a **screened host**.



*A screened host. (Images © 123RF.com.)*

Sometimes the term DMZ (or "DMZ host") is used by SOHO router vendors to mean a host on the local network that accepts connections from the Internet. This might be simpler to configure and solve some access problems, but it makes the whole network very vulnerable to intrusion and DoS. An enterprise DMZ is established by a separate network interface and subnet so that traffic between hosts in the DMZ and the LAN must be routed (and subject to firewall rules). Most SOHO routers do not have the necessary ports or routing functionality to create a true DMZ.

**IMPLICATIONS OF IPV6**

IPv6 has impacts for on-premises networks, for the way your company accesses cloud services, and for the way clients access web servers and other public servers that you publish.

IPv6 may be enabled by default on clients and servers, and even on network appliances (routers and firewalls), so there must be a management and security plan for it. If IPv6 is enabled but unmanaged, there is the potential for malicious use as a backdoor or covert channel. IPv6 also exposes novel attack vectors, such as spoofing and DoS attacks on neighbor discovery.

Hosts should be allocated IPv6 addresses that map to the same zones as the IPv4 topology. Firewalls should be configured with ACLs that either achieve the same security configuration as for IPv4 or block IPv6, if that is a better option. One issue here is that IPv6 is not intended to perform any type of address translation. Rather than obscure internal/external traffic flows with private to public address mapping, IPv6 routing and filtering policies should be configured to mirror the equivalent IPv4 architecture.

**OTHER SECURE NETWORK DESIGN CONSIDERATIONS**

Network design must also be considered for data centers and the cloud. A data center is a facility dedicated to hosting servers, rather than a mix of server and client workstation machines.

### East-West Traffic

Traffic that goes to and from a data center is referred to as north-south. This traffic represents clients outside the data center making requests and receiving responses. In data centers that support cloud and other Internet services, most traffic is actually between servers within the data center. This is referred to as **east-west traffic**.

Consider a client uploading a photograph as part of a social media post. The image file might be checked by an analysis server for policy violations (indecent or copyright images, for instance), a search/indexing service would be updated with the image metadata, the image would be replicated to servers that provision content delivery networks (CDNs), the image would be copied to backup servers, and so on. A single request to the cloud tends to cascade to multiple requests and transfers within the cloud.

### Zero Trust

**Zero trust**architectures assume that nothing should be taken for granted and that all network access must be continuously verified and authorized. Any user, device, or application seeking access must be authenticated and verified. Zero Trust differs from traditional security models based on simply granting access to all users, devices, and applications contained within an organization's trusted network.

NIST SP 800-207 "Zero Trust Architecture" defines Zero Trust as "cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." A Zero Trust architecture can protect data, applications, networks, and systems from malicious attacks and unauthorized access more effectively than a traditional architecture by ensuring that only necessary services are allowed and only from appropriate sources. Zero Trust enables organizations to offer services based on varying levels of trust, such as providing more limited access to sensitive data and systems.

**MAN-IN-THE-MIDDLE AND LAYER 2 ATTACKS**

Attacks at the physical and data link layers, referred to in the OSI model as layer 1 and layer 2, are often focused on information gathering—**network mapping** and **eavesdropping** on network traffic.

### Man-in-the-Middle/On-Path Attacks

Attackers can also take advantage of the lack of security in low-level data link protocols to perform **man-in-the-middle (MitM) attacks**. A MitM or on-path attack is where the threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts. An on-path attack could also be used to covertly modify the traffic. For example, a MitM host could present a workstation with a spoofed website form, to try to capture the user credential. Another common on-path attack spoofs responses to DNS queries, redirecting users to spoofed websites. On-path attacks can be defeated using mutual authentication, where both hosts exchange secure credentials, but at layer 2 it is not always possible to put these controls in place.

### MAC Cloning

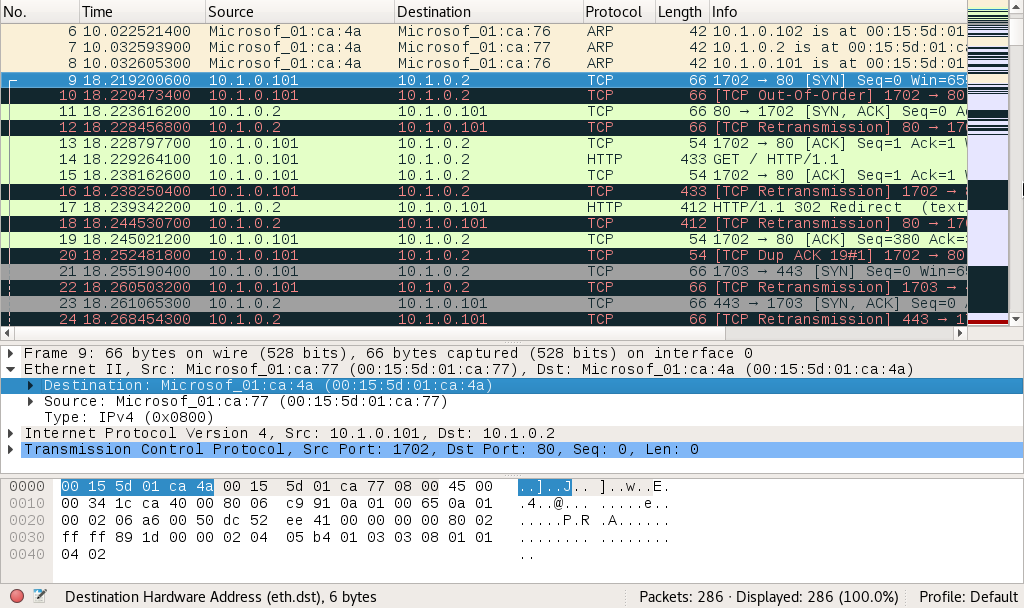
**MAC cloning**, or MAC address spoofing, changes the hardware address configured on an adapter interface or asserts the use of an arbitrary MAC address. While a unique MAC address is assigned to each network interface by the vendor at the factory, it is simple to override it in software via OS commands, alterations to the network driver configuration, or using **packet crafting** software. This can lead to a variety of issues when investigating security incidents or when depending on MAC addresses as part of a security control, as the presented address of the device may not be reliable.

**ARP POISONING AND MAC FLOODING ATTACKS**

A host uses the **Address Resolution Protocol (ARP)** to discover other hosts on the local segment that owns an IP address.

**ARP Poisoning Attacks**

An **ARP poisoning** attack uses a packet crafter, such as Ettercap, to broadcast unsolicited ARP reply packets. Because ARP has no security mechanism, the receiving devices trust this communication and update their MAC:IP address cache table with the spoofed address.



*Packet capture opened in Wireshark showing ARP poisoning. (Screenshot used with permission from*[*wireshark.org*](https://www.wireshark.org/)*.)*

This screenshot shows packets captured during a typical ARP poisoning attack:

* In frames 6-8, the attacking machine (with MAC address ending :4a) directs gratuitous ARP replies at other hosts (:76 and :77), claiming to have the IP addresses .2, .101, and .102.
* In frame 9, the .101/:77 host tries to send a packet to the .2 host, but it is received by the attacking host (with the destination MAC :4a).
* In frame 10, the attacking host retransmits frame 9 to the actual .2 host. Wireshark colors the frame black and red to highlight the retransmission.
* In frames 11 and 12, you can see the reply from .2, received by the attacking host in frame 11 and retransmitted to the legitimate host in frame 12.

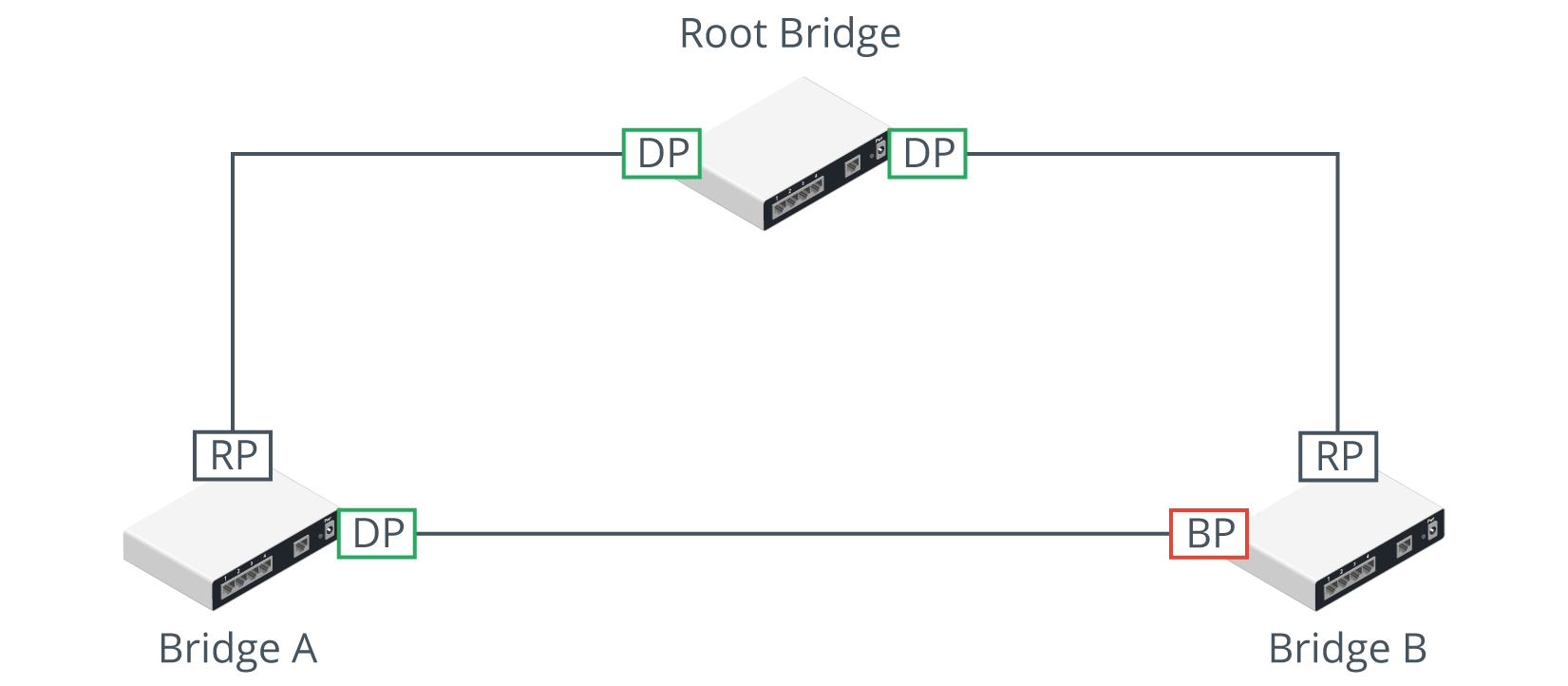
The usual target will be the subnet's default gateway (the router that accesses other networks). If the ARP poisoning attack is successful, all traffic destined for remote networks will be sent to the attacker. The attacker can perform a man-in-the-middle attack, either by monitoring the communications and then forwarding them to the router to avoid detection, or modifying the packets before forwarding them. The attacker could also perform a denial of service attack by not forwarding the packets.

**MAC Flooding Attacks**

Where ARP poisoning is directed at hosts, **MAC flooding** is used to attack a switch. The intention of the attacker is to exhaust the memory used to store the switch's MAC address table. The switch uses the **MAC address table** to determine which port to use to forward unicast traffic to its correct destination. Overwhelming the table can cause the switch to stop trying to apply MAC-based forwarding and flood unicast traffic out of all ports, working as a hub. This makes sniffing network traffic easier for the threat actor.

**LOOP PREVENTION**

An Ethernet switch's layer 2 forwarding function is similar to that of an older network appliance called a bridge. In a network with multiple bridges, implemented these days as switches, there may be more than one path for a frame to take to its intended destination. As a layer 2 protocol, Ethernet has no concept of Time To Live. Therefore, layer 2 broadcast traffic could continue to loop through a network with multiple paths indefinitely. Layer 2 loops are prevented by the **Spanning Tree Protocol (STP)**. Spanning tree is a means for the bridges to organize themselves into a hierarchy and prevent loops from forming.



*STP configuration. (Images © 123RF.com.)*

This diagram shows the minimum configuration necessary to prevent loops in a network with three bridges or switches. The root bridge has two designated ports (DP) connected to Bridge A and Bridge B. Bridges A and B both have root ports (RP) connected back to the interfaces on the root bridge. Bridges A and B also have a connection directly to one another. On Bridge A, this interface is active and traffic for Bridge B can be forwarded directly over it. On Bridge B, the interface is blocked (BP) to prevent a loop and traffic for Bridge A must be forwarded via the root bridge. Only Bridge Protocol Data Unit (BPDU) traffic will go across a blocked port.

**Broadcast Storm Prevention**

STP is principally designed to prevent **broadcast storms**. Switches forward broadcast, multicast, and unknown unicast traffic out of all ports. If a bridged network contains a loop, broadcast traffic will travel through the network, get amplified by the other switches, and arrive back at the original switch, which will re-broadcast each incoming broadcast frame, causing an exponential increase (the storm), which will rapidly overwhelm the switches and crash the network.

A loop can be created accidentally or maliciously by plugging a patch cable from one patch panel port to another or connecting two wall ports. Normally, STP should detect the loop and block a port to break or eliminate the loop, resulting in a few seconds of disruption. However, STP may be misconfigured, or a threat actor may have managed to disrupt it. A storm control setting on a switch is a backup mechanism to rate-limit broadcast traffic above a certain threshold.

**Bridge Protocol Data Unit (BPDU) Guard**

A threat actor might try to attack STP using a rogue switch or software designed to imitate a switch. When a switch does not know the correct port to use for a particular destination MAC address (if the cache has just been flushed, for instance), it floods the unknown unicast frame out to all ports. Topology changes in STP can cause a switch to flush the cache more frequently and to start flooding unicast traffic more frequently, which can have a serious impact on network performance and assists sniffing attacks.

**PHYSICAL PORT SECURITY AND MAC FILTERING**

Because of the risks from rogue devices and the potential to create loops by incorrect placement of patch cables, access to the physical switch ports and switch hardware should be restricted to authorized staff, using a secure server room and/or lockable hardware cabinets. To prevent the attachment of unauthorized client devices at unsecured wall ports, the switch port that the wall port cabling connects to can be disabled by using the management software, or the patch cable can be physically removed from the port. Completely disabling ports in this way can introduce a lot of administrative overhead and scope for error. Also, it doesn't provide complete protection, as an attacker could unplug a device from an enabled port and connect their own laptop. Consequently, more sophisticated methods of ensuring **port security** have been developed.

**MAC Filtering and MAC Limiting**

Configuring **MAC filtering** on a switch means defining which MAC addresses are allowed to connect to a particular port. This can be done by creating a list of valid MAC addresses or by specifying a limit to the number of permitted addresses. For example, if port security is enabled with a maximum of two MAC addresses, the switch will record the first two MACs to connect to that port, but then drop any traffic from machines with different MAC addresses that try to connect

**DHCP Snooping**

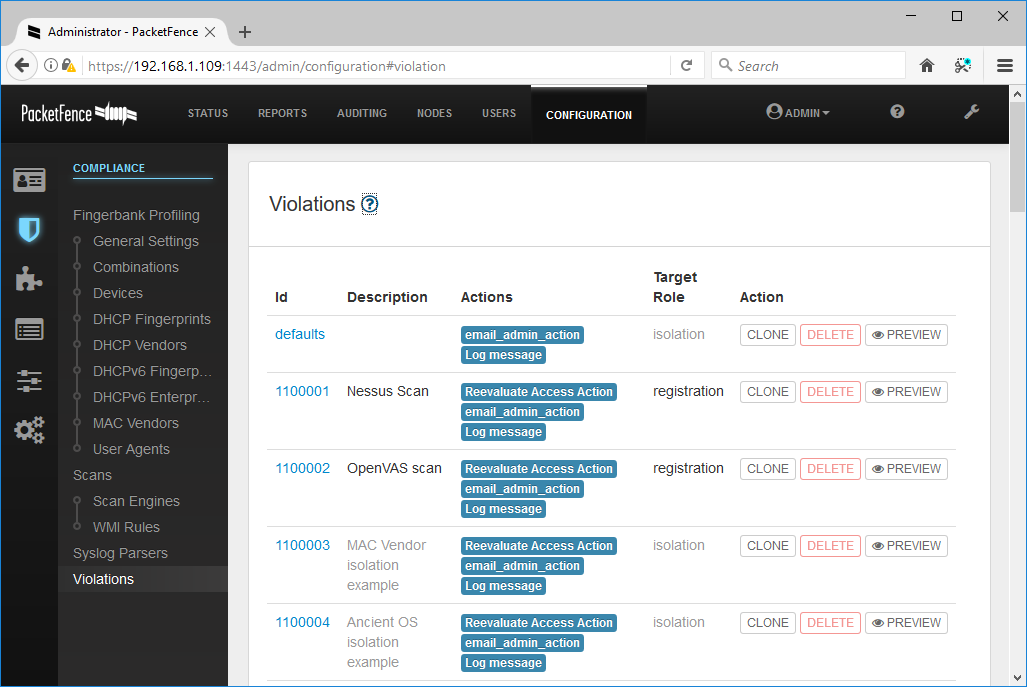
Another option is to configure **Dynamic Host Configuration Protocol (DHCP) snooping**. DHCP is the protocol that allows a server to assign IP address information to a client when it connects to the network. DHCP snooping inspects this traffic arriving on access ports to ensure that a host is not trying to spoof its MAC address. It can also be used to prevent rogue (or spurious) DHCP servers from operating on the network. With DHCP snooping, only DHCP messages from ports configured as trusted are allowed. Additionally dynamic ARP inspection (DAI), which can be configured alongside DHCP snooping, prevents a host attached to an untrusted port from flooding the segment with gratuitous ARP replies. DAI maintains a trusted database of IP:ARP mappings and ensures that ARP packets are validly constructed and use valid IP addresses

**NETWORK ACCESS CONTROL**

Endpoint security is a set of security procedures and technologies designed to restrict network access at a device level. Endpoint security contrasts with the focus on perimeter security established by topologies such as DMZ and technologies such as firewalls. Endpoint security does not replace these but adds defense in depth.

The IEEE 802.1X standard defines a **port-based network access control (PNAC)** mechanism. PNAC means that the switch uses an Authentication, Authorization, and Accounting (AAA) server to authenticate the attached device before activating the port. **Network access control (NAC)** products can extend the scope of authentication to allow administrators to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network access. This is called a health policy. Typical policies check things such as malware infection, firmware and OS patch level, personal firewall status, and the presence of up-to-date virus definitions. A solution may also be able to scan the registry or perform file signature verification. The health policy is defined on a NAC management server along with reporting and configuration tools.

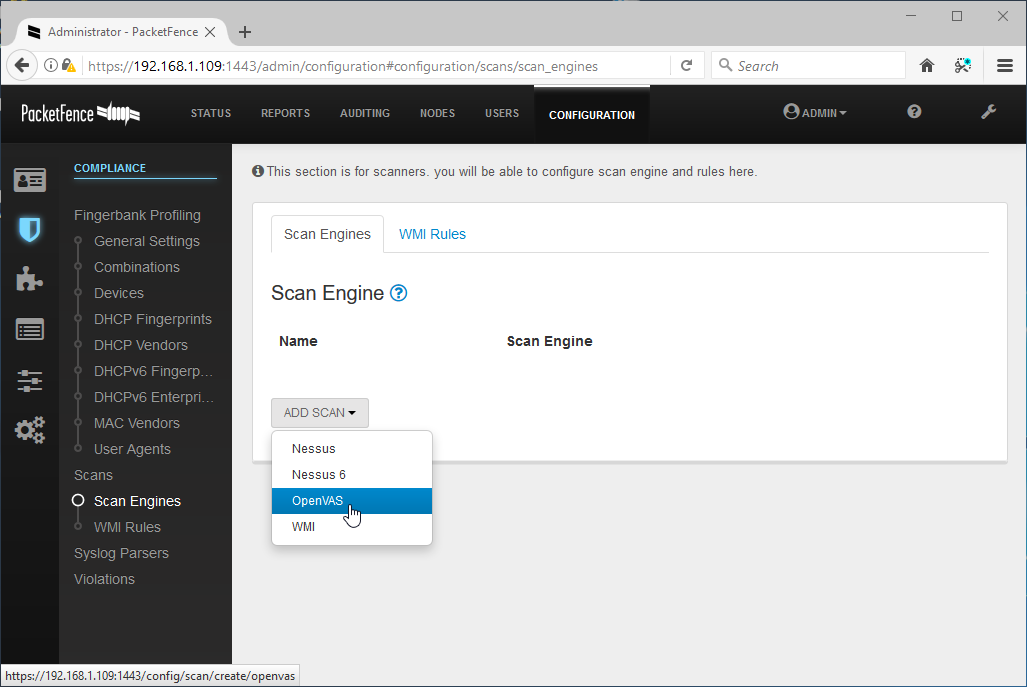
**Posture assessment** is the process by which host health checks are performed against a client device to verify compliance with the health policy. Most NAC solutions use client software called an agent to gather information about the device, such as its antivirus and patch status, presence of prohibited applications, or anything else defined by the health policy.



*Defining policy violations in Packet Fence Open Source NAC. (Screenshot used with permission from*[*packetfence.org*](https://packetfence.org/)*.)*

An agent can be persistent, in which case it is installed as a software application on the client, or nonpersistent. A nonpersistent (or dissolvable) agent is loaded into memory during posture assessment but is not installed on the device.

.



*Packet Fence supports the use of several scanning techniques, including vulnerability scanners, such as Nessus and OpenVAS, Windows Management Instrumentation (WMI) queries, and log parsers. (Screenshot used with permission from*[*packetfence.org*](https://packetfence.org/)*.)*

**ROUTE SECURITY**

A successful attack against route security enables the attacker to redirect traffic from its intended destination. On the Internet, this may allow the threat actor to herd users to spoofed websites. On an enterprise network, it may facilitate circumventing firewalls and security zones to allow lateral movement and data exfiltration.

Routes between networks and subnets can be configured manually, but most routers automatically discover routes by communicating with each other. Dynamic routers exchange information about routes using routing protocols. It is important that this traffic be separated from channels used for other types of data. Routing protocols do not always have effective integral security mechanisms, so they need to run in an environment where access is very tightly controlled.

Routing is subject to numerous vulnerabilities, including:

* Spoofed routing information (route injection)—Routing protocols that have no or weak authentication are vulnerable to route table poisoning. This can mean that traffic is misdirected to a monitoring port (sniffing), sent to a blackhole (nonexistent address), or continuously looped around the network, causing DoS. Most dynamic routing protocols support message authentication via a shared secret configured on each device. This can be difficult to administer, however. It is usually also possible to configure how a router identifies the peers from which it will accept route updates. This makes it harder to simply add a rogue router to the system. An attacker would have to compromise an existing router and change its configuration.
* Source routing—This uses an option in the IP header to pre-determine the route a packet will take through the network (strict) or "waypoints" that it must pass through (loose). This can be used maliciously to spoof IP addresses and bypass router/firewall filters. Routers can be configured to block source routed packets.
* Software exploits in the underlying operating system—Hardware routers (and switches) have an embedded operating system. For example, Cisco devices typically use the Internetwork Operating System (IOS). Something like IOS suffers from fewer exploitable vulnerabilities than full network operating systems. It has a reduced attack surface compared to a computer OS, such as Windows.

**WIRELESS NETWORK INSTALLATION CONSIDERATIONS**

Wireless network installation considerations refer to the factors that ensure good availability of authorized Wi-Fi access points. A network with patchy coverage is vulnerable to rogue access point and evil twin attacks.

*The 5 GHz band has more space to configure non-overlapping channels. Also note that a WAP can use bonded channels to improve bandwidth, but this increases risks from interference.*

**Wireless Access Point (WAP) Placement**

An infrastructure-based wireless network comprises one or more wireless access points, each connected to a wired network. The **access points** forward traffic to and from the wired switched network. Each WAP is identified by its MAC address, also referred to as its basic service set identifier (BSSID). Each wireless network is identified by its name, or **service set identifier (SSID)**.

Wireless networks can operate in either the 2.4 GHz or 5 GHz radio band. Each radio band is divided into a number of channels, and each WAP must be configured to use a specific channel. For performance reasons, the channels chosen should be as widely spaced as possible to reduce different types of interference:

* Co-channel interference (CCI)—when two WAPs in close proximity use the same channel, they compete for bandwidth within that channel, and signals have to be re-transmitted as they collide.
* Adjacent channel interference (ACI)—channels have only ~5 MHz spacing, but Wi-Fi requires 20 MHz of channel space. When the channels selected for WAPs are not cleanly spaced, the interference pattern creates significant numbers of errors and loss of bandwidth. For example, if two access points within range of one another are configured in the 2.4 GHz band with channels 1 and 6, they will not overlap. If a third access point is added using channel 3, it will use part of the spectrum used by both the other WAPs, and all three networks will suffer from interference.

**Site Surveys and Heat Maps**

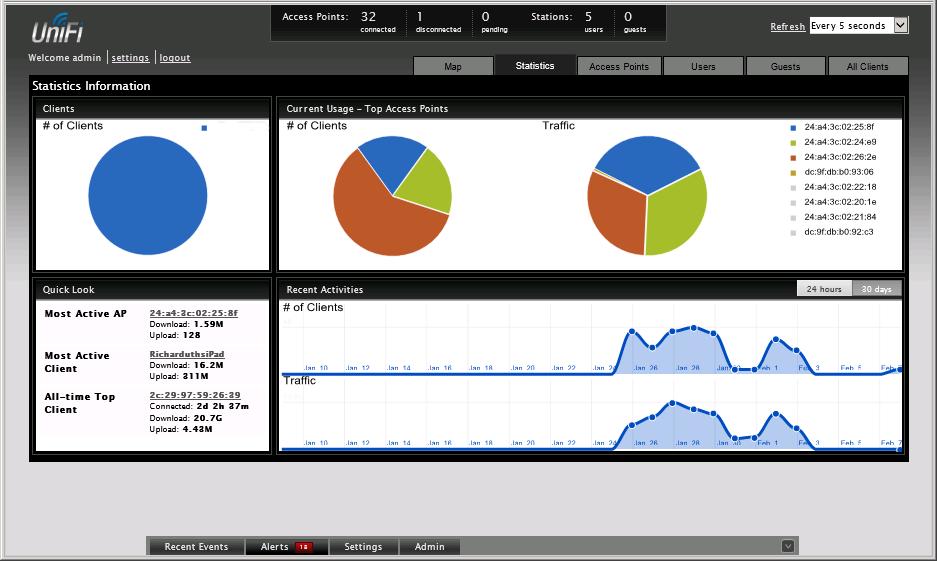
The coverage and interference factors mean that WAPs must be positioned and configured so that the whole area is covered, but that they overlap as little as possible. A **site survey** is used to measure signal strength and channel usage throughout the area to cover. A site survey starts with an architectural map of the site, with physical features that can cause background interference marked. These features include solid walls, reflective surfaces, motors, microwave ovens, and so on. The survey is performed with a Wi-Fi-enabled laptop or mobile device with Wi-Fi analyzer software installed. The Wi-Fi analyzer records information about the signal obtained at regularly spaced points as the surveyor moves around the area.

These readings are combined and analyzed to produce a **heat map**, showing where a signal is strong (red) or weak (green/blue), and which channel is being used and how they overlap. This data is then used to optimize the design, by adjusting transmit power to reduce a WAP's range, changing the channel on a WAP, adding a new WAP, or physically moving a WAP to a new location.

**CONTROLLER AND ACCESS POINT SECURITY**

Where a site survey ensures availability, the confidentiality and integrity properties of the network are ensured by configuring authentication and encryption. These settings could be configured manually on each WAP, but this would be onerous in an enterprise network with tens or hundreds of WAP. If access points are individually managed, this can lead to configuration errors and can make it difficult to gain an overall view of the wireless deployment, including which clients are connected to which access points and which clients or access points are handling the most traffic.

Rather than configure each device individually, enterprise wireless solutions implement **wireless controllers** for centralized management and monitoring. A controller can be a hardware appliance or a software application run on a server.



*UniFi Wireless Network management console. (Screenshot used with permission from Ubiquiti Networks.)*

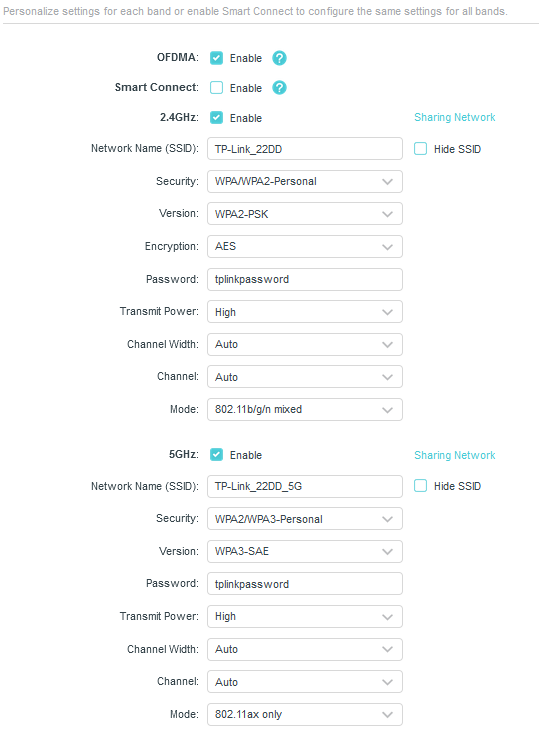
An access point whose firmware contains enough processing logic to be able to function autonomously and handle clients without the use of a wireless controller is known as a fat WAP, while one that requires a wireless controller in order to function is known as a thin WAP.

Controllers and access points must be made physically secure, as tampering could allow a threat actor to insert a rogue/evil twin WAP to try to intercept logons. These devices must be managed like switches and routers, using secure management interfaces and strong administrative credentials.

**WI-FI PROTECTED ACCESS**

As well as the site design, a wireless network must be configured with security settings. Without encryption, anyone within range can intercept and read packets passing over the wireless network. These choices are determined by device support for the various Wi-Fi security standards, by the type of authentication infrastructure, and by the purpose of the WLAN. The security standard determines the cryptographic protocols that are supported, the means of generating the encryption key, and available methods for authenticating wireless stations when they try to join (or associate with) the network.

The first version of **Wi-Fi Protected Access (WPA)** was designed to fix critical vulnerabilities in the earlier **wired equivalent privacy (WEP)** standard. Like WEP, version 1 of WPA uses the RC4 stream cipher but adds a mechanism called the **Temporal Key Integrity Protocol (TKIP)** to make it stronger.



*Configuring a TP-LINK SOHO access point with wireless encryption and authentication settings. In this example, the 2.4 GHz band allows legacy connections with WPA2-Personal security, while the 5 GHz network is for 802.11ax (Wi-Fi 6) capable devices using WPA3-SAE authentication. (Screenshot used with permission from TP-Link Technologies.)*

Neither WEP nor the original WPA version are considered secure enough for continued use. WPA2 uses the Advanced Encryption Standard (AES) cipher with 128-bit keys, deployed within the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES replaces RC4 and CCMP replaces TKIP. CCMP provides authenticated encryption, which is designed to make replay attacks harder.

Weaknesses have also been found in WPA2, however, which has led to its intended replacement by WPA3. The main features of WPA3 are as follows:

* **Simultaneous Authentication of Equals (SAE)**—replaces WPA's 4-way handshake authentication and association mechanism with a protocol based on Diffie-Hellman key agreement.
* Enhanced Open—enables encryption for the open authentication method.
* Updated cryptographic protocols—replaces AES CCMP with the **AES Galois Counter Mode Protocol (GCMP)** mode of operation. Enterprise authentication methods must use 192-bit AES, while personal authentication can use either 128-bit or 192-bit.
* Management protection frames—mandates use of these to protect against key recovery attacks.

*Wi-Fi performance also depends on support for the latest 802.11 standards. The most recent generation (802.11ax) is being marketed as Wi-Fi 6. The earlier standards are retroactively named Wi-Fi 5 (802.11ac) and Wi-Fi 4 (802.11n). The performance standards are developed in parallel with the WPA security specifications. Most Wi-Fi 6 devices and some Wi-Fi 5 and Wi-Fi 4 products should support WPA3, either natively or with a firmware/driver update.*

**WI-FI AUTHENTICATION METHODS**

In order to secure a network, you need to be able to confirm that only valid users are connecting to it. Wi-Fi authentication comes in three types: personal, open, and enterprise. Within the personal category, there are two methods: pre-shared key authentication (PSK) and simultaneous authentication of equals (SAE).

### WPA2 Pre-Shared Key Authentication

In WPA2, **pre-shared key (PSK)** authentication uses a passphrase to generate the key that is used to encrypt communications. It is also referred to as group authentication because a group of users share the same secret. When the access point is set to WPA2-PSK mode, the administrator configures a passphrase of between 8 and 63 ASCII characters. This is converted to a 256-bit HMAC (expressed as a 64-character hex value) using the PBKDF2 key stretching algorithm. This HMAC is referred to as the pairwise master key (PMK). The same secret must be configured on the access point and on each node that joins the network. The PMK is used as part of WPA2's 4-way handshake to derive various session keys.

*All types of Wi-Fi personal authentication have been shown to be vulnerable to attacks that allow dictionary or brute force attacks against the passphrase. At a minimum, the passphrase must be at least 14 characters long to try to mitigate risks from cracking.*

### WPA3 Personal Authentication

While WPA3 still uses a passphrase to authenticate stations in personal mode, it changes the method by which this secret is used to agree upon session keys. The scheme used is also referred to as Password Authenticated Key Exchange (PAKE). In WPA3, the Simultaneous Authentication of Equals (SAE) protocol replaces the 4-way handshake, which has been found to be vulnerable to various attacks. SAE uses the Dragonfly handshake, which is basically Diffie-Hellman over elliptic curves key agreement, combined with a hash value derived from the password and device MAC address to authenticate the nodes. With SAE, there should be no way for an attacker to sniff the handshake to obtain the hash value and try to use an offline brute-force or dictionary attack to recover the password. Dragonfly also implements ephemeral session keys, providing forward secrecy.

*The configuration interfaces for access points can use different labels for these methods. You might see WPA2-Personal and WPA3-SAE rather than WPA2-PSK and WPA3-Personal, for example. Additionally, an access point can be configured for WPA3 only or with support for legacy WPA2 (WPA3-Personal Transition mode). Researchers already found flaws in WPA3-Personal, one of which relies on a downgrade attack to use WPA2 (*[*wi-fi.org/security-update-april-2019*](https://www.wi-fi.org/security-update-april-2019)*).*

**WI-FI PROTECTED SETUP**

As setting up an access point securely is relatively complex for residential consumers, vendors have developed a system to automate the process called **Wi-Fi Protected Setup (WPS)**. To use WPS, both the access point and wireless station (client device) must be WPS-capable. Typically, the devices will have a pushbutton. Activating this on the access point and the adapter simultaneously will associate the devices using a PIN, then associate the adapter with the access point using WPA2. The system generates a random SSID and PSK. If the devices do not support the push button method, the PIN (printed on the WAP) can be entered manually.

Unfortunately, WPS is vulnerable to a brute force attack. While the PIN is eight characters, one digit is a checksum and the rest are verified as two separate PINs of four and three characters. These separate PINs are many orders of magnitude simpler to brute force, typically requiring just hours to crack. On some models, disabling WPS through the admin interface does not actually disable the protocol, or there is no option to disable it. Some APs can lock out an intruder if a brute force attack is detected, but in some cases the attack can just be resumed when the lockout period expires. To counter this, the lockout period can be increased. However, this can leave APs vulnerable to a denial of service (DoS) attack. When provisioning a WAP, it is essential to verify what steps the vendor has taken to make their WPS implementation secure and the firmware level required to assure security.

**OPEN AUTHENTICATION AND CAPTIVE PORTALS**

Selecting open authentication means that the client is not required to authenticate. This mode would be used on a public WAP (or "hotspot"). In WPA2, this also means that data sent over the link is unencrypted. Open authentication may be combined with a secondary authentication mechanism managed via a browser. When the client associates with the open hotspot and launches the browser, the client is redirected to a **captive portal** or splash page. This will allow the client to authenticate to the hotspot provider's network (over HTTPS, so the login is secure). The portal may also be designed to enforce terms and conditions and/or take payment to access the Wi-Fi service.

When using open wireless, users must ensure they send confidential web data only over HTTPS connections and only use email, VoIP, IM, and file transfer services with SSL/TLS enabled. Another option is for the user to join a Virtual Private Network (VPN). The user would associate with the open hotspot then start the VPN connection. This creates an encrypted "tunnel" between the user's computer and the VPN server. This allows the user to browse the web or connect to email services without anyone eavesdropping on the open Wi-Fi network being able to intercept those communications. The VPN could be provided by the user's company or they could use a third-party VPN service provider. Of course, if using a third party, the user needs to be able to trust them implicitly. The VPN must use certificate-based tunneling to set up the "inner" authentication method.

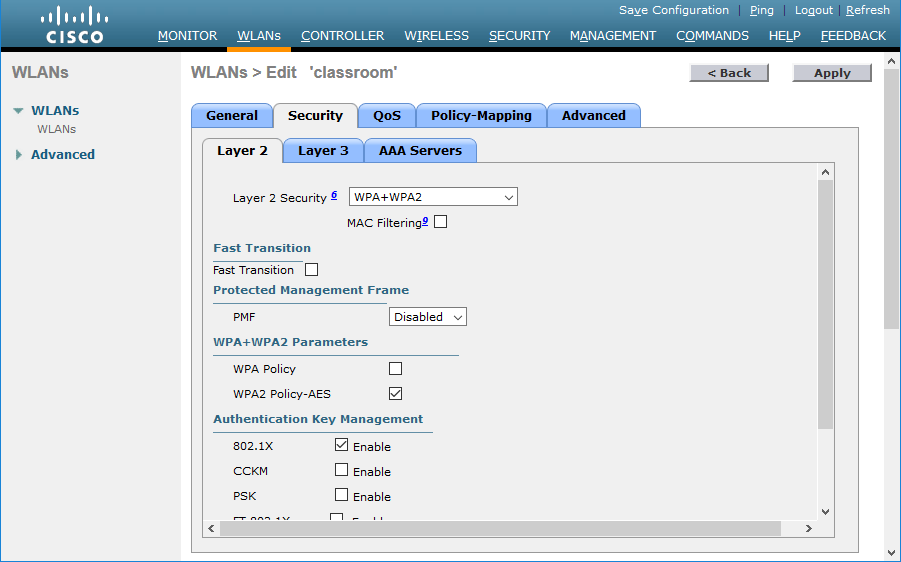
WPA3 can implement a mode called Wi-Fi Enhanced Open, which uses opportunistic wireless encryption (OWE). OWE uses the Dragonfly handshake to agree with ephemeral session keys on joining the network. This means that one station cannot sniff the traffic from another station, because they are using different session keys. There is still no authentication of the access point, however.

**ENTERPRISE/IEEE 802.1X AUTHENTICATION**

The main problems with personal modes of authentication are that distribution of the key or passphrase cannot be secured properly, and users may choose unsecure phrases. Personal authentication also fails to provide accounting, as all users share the same key.

As an alternative to personal authentication, the enterprise authentication method implements IEEE 802.1X to use an Extensible Authentication Protocol (EAP) mechanism. 802.1X defines the use of EAP over Wireless (EAPoW) to allow an access point to forward authentication data without allowing any other type of network access. It is configured by selecting WPA2-Enterprise or WPA3-Enterprise as the security method on the access point.

With enterprise authentication, when a wireless station requests an association, the WAP enables the channel for EAPoW traffic only. It passes the credentials of the user (supplicant) to an AAA (RADIUS or TACACS+) server on the wired network for validation. When the supplicant has been authenticated, the AAA server transmits a master key (MK) to the supplicant. The supplicant and authentication server then derive the same pairwise master key (PMK) from the MK. The AAA server transmits the PMK to the access point. The wireless station and access point use the PMK to derive session keys, using either the WPA2 4-way handshake or WPA3 SAE methods.

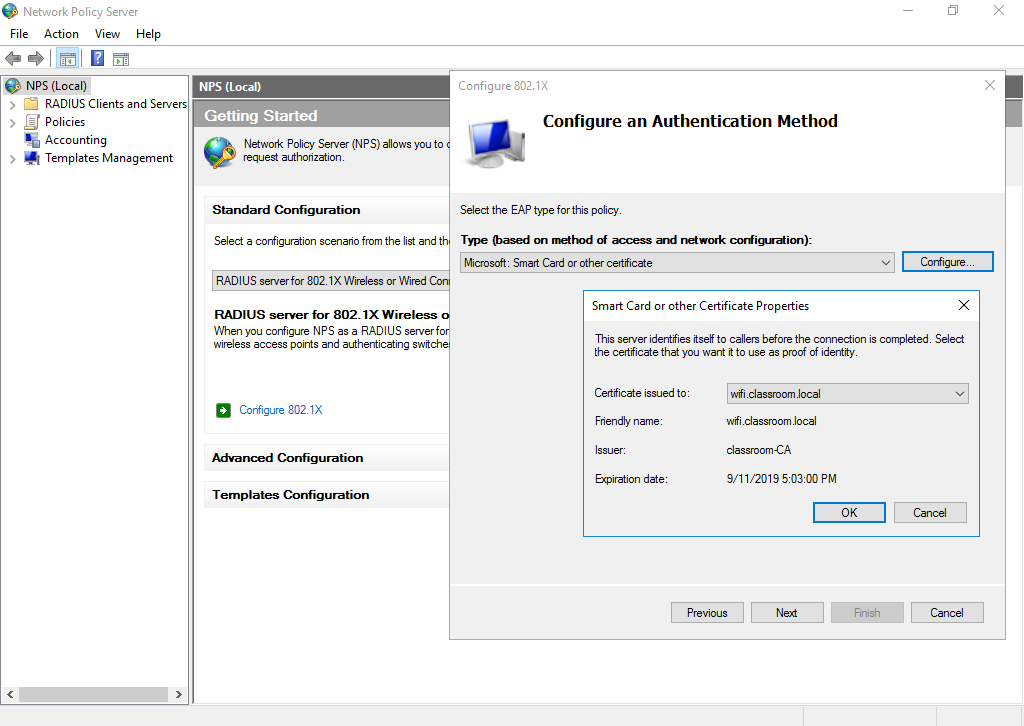


*Using Cisco's Virtual Wireless LAN Controller to set security policies for a WLAN—this policy enforces use of WPA2 and the use of 802.1X (Enterprise) authentication. (Screenshot used with permission from Cisco.)*

**EXTENSIBLE AUTHENTICATION PROTOCOL**

The Extensible Authentication Protocol (EAP) defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves. Vendors can write extensions to the protocol to support third-party security devices. EAP implementations can include smart cards, one-time passwords, biometric identifiers, or simpler username and password combinations.

**EAP-TLS** is one of the strongest types of authentication and is very widely supported. An encrypted Transport Layer Security (TLS) tunnel is established between the supplicant and authentication server using public key certificates on the authentication server and supplicant. As both supplicant and server are configured with certificates, this provides mutual authentication. The supplicant will typically provide a certificate using a smart card or a certificate could be installed on the client device, possibly in a Trusted Platform Module (TPM).



*Configuring Network Policy Server to authenticate wireless clients using 802.1X EAP-TLS. (Screenshot used with permission from Microsoft.)*

**PEAP, EAP-TTLS, AND EAP-FAST**

Provisioning certificates to each wireless device is a considerable management challenge. Other types of EAP are designed to provide secure tunneling with server-side certificates only.

### Protected Extensible Authentication Protocol (PEAP)

In **Protected Extensible Authentication Protocol (PEAP)**, as with EAP-TLS, an encrypted tunnel is established between the supplicant and authentication server, but PEAP only requires a server-side public key certificate. The supplicant does not require a certificate. With the server authenticated to the supplicant, user authentication can then take place through the secure tunnel with protection against sniffing, password-guessing/dictionary, and on-path attacks. The user authentication method (also referred to as the "inner" method) can use either EAP-MS-CHAPv2 or EAP-GTC. The Generic Token Card (GTC) method transfers a token for authentication against a network directory or using a one-time password mechanism.

### EAP with Tunneled TLS (EAP-TTLS)

**EAP-Tunneled TLS (EAP-TTLS)** is similar to PEAP. It uses a server-side certificate to establish a protected tunnel through which the user's authentication credentials can be transmitted to the authentication server. The main distinction from PEAP is that EAP-TTLS can use any inner authentication protocol (PAP or CHAP, for instance), while PEAP must use EAP-MS-CHAPv2 or EAP-GTC.

### EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)

**EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)** is similar to PEAP, but instead of using a certificate to set up the tunnel, it uses a Protected Access Credential (PAC), which is generated for each user from the authentication server's master key. The problem with EAP-FAST is in distributing (provisioning) the PAC securely to each user requiring access. The PAC can either be distributed via an out-of-band method or via a server with a digital certificate (but in the latter case, EAP-FAST does not offer much advantage over using PEAP). Alternatively, the PAC can be delivered via anonymous Diffie-Hellman key exchange. The problem here is that there is nothing to authenticate the access point to the user. A rogue access point could obtain enough of the user credential to perform an ASLEAP password cracking attack.

**RADIUS FEDERATION**

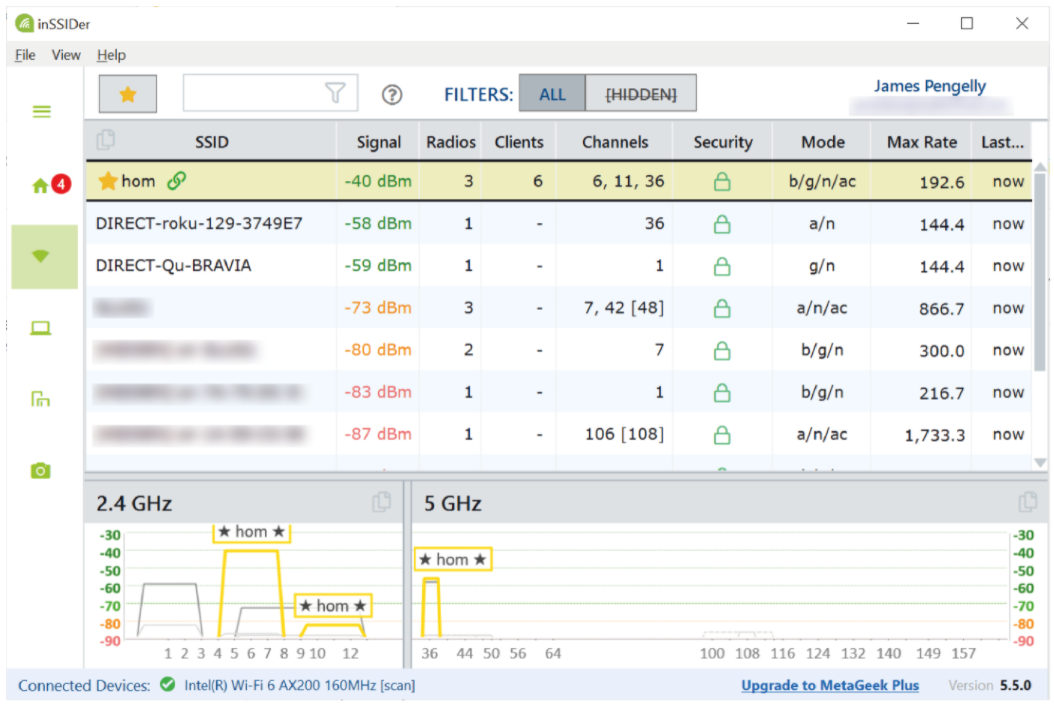
Most implementations of EAP use a RADIUS server to validate the authentication credentials for each user (supplicant). RADIUS federation means that multiple organizations allow access to one another's users by joining their RADIUS servers into a RADIUS hierarchy or mesh. For example, when Bob from widget.foo needs to log on to grommet.foo's network, the RADIUS server at grommet.foo recognizes that Bob is not a local user but has been granted access rights and routes the request to widget.foo's RADIUS server.

One example of RADIUS federation is the eduroam network ([eduroam.org](https://www.eduroam.org/)), which allows students of universities from several different countries to log on to the networks of any of the participating institutions using the credentials stored by their "home" university.

**ROGUE ACCESS POINTS AND EVIL TWINS**

A rogue access point is one that has been installed on the network without authorization, whether with malicious intent or not. It is vital to periodically survey the site to detect rogue WAPs. A malicious user can set up such an access point with something as basic as a smartphone with tethering capabilities, and a non-malicious user could enable such an access point by accident. If connected to a LAN without security, an unauthorized WAP creates a backdoor through which to attack the network. A rogue WAP could also be used to capture user logon attempts, allow man-in-the-middle attacks, and allow access to private information.

A rogue WAP masquerading as a legitimate one is called an evil twin. An **evil twin** might just have a similar name (SSID) to the legitimate one, or the attacker might use some DoS technique to overcome the legitimate WAP. The evil twin might be able to harvest authentication information from users entering their credentials by mistake.



*Surveying Wi-Fi networks using MetaGeek inSSIDer—Note the presence of smart TV appliances with Wi-Fi Direct enabled. (MetaGeek, LLC. © Copyright 2005-2021)*

A rogue hardware WAP can be identified through physical inspections. There are also various Wi-Fi analyzers and monitoring systems that can detect rogue WAPs, including inSSIDer ([metageek.com/products/inssider](https://www.metageek.com/products/inssider/)) and Kismet ([kismetwireless.net](https://www.kismetwireless.net/)).

**DISASSOCIATION AND REPLAY ATTACKS**

In the normal course of operations, an access point and client, exchange management frames to control connections. The access point normally broadcasts a beacon frame to advertise service capabilities. Clients can choose to first authenticate and then associate to an access point when they move into range of the beacon. The client or access point can use **disassociation** and/or **deauthentication** frames to notify the other party that it has ended a connection. A legitimate client might disassociate but not deauthenticate because it is roaming between wireless access points in a distribution system. A disassociation attack exploits the lack of encryption in management frame traffic to send spoofed frames. One type of disassociation attack injects management frames that spoof the MAC address of a single victim station in a disassociation notification, causing it to be disconnected from the network. Another variant of the attack broadcasts spoofed frames to disconnect all stations. Frames can be spoofed to send either disassociation or deauthentication notifications.

Disassociation/deauthentication attacks may be used to perform a denial of service attack against the wireless infrastructure or to exploit disconnected stations to try to force reconnection to a rogue WAP. Disassociation/deauthentication attacks might also be used in conjunction with a replay attack aimed at recovering the network key. The attacks can be mitigated if the wireless infrastructure supports Management Frame Protection (MFP/802.11w). Both the WAP and clients must be configured to support MFP.

WPA and WPA2 are not vulnerable to **IV attacks**, but a serious vulnerability was discovered in 2017 ([krackattacks.com](https://www.krackattacks.com/)). A KRACK attack uses a replay mechanism that targets the 4-way handshake. KRACK is effective regardless of whether the authentication mechanism is personal or enterprise. It is important to ensure both clients and access points are fully patched against such attacks.

**JAMMING ATTACKS**

A wireless network can be disrupted by interference from other radio sources. These are often unintentional, but it is also possible for an attacker to purposefully jam an access point. This might be done simply to disrupt services or to position an evil twin on the network with the hope of stealing data. A Wi-Fi **jamming** attack can be performed by setting up a WAP with a stronger signal. Wi-Fi jamming devices are also widely available, though they are often illegal to use and sometimes to sell. Such devices can be very small, but the attacker still needs to gain fairly close physical proximity to the wireless network.

The only ways to defeat a jamming attack are either to locate the offending radio source and disable it, or to boost the signal from the legitimate equipment. WAPs for home and small business use are not often configurable, but the more advanced wireless access points, such as Cisco's Aironet series, support configurable power level controls. The source of interference can be detected using a **spectrum analyzer**. Unlike a Wi-Fi analyzer, a spectrum analyzer must use a special radio receiver (Wi-Fi adapters filter out anything that isn't a Wi-Fi signal). They are usually supplied as handheld units with a directional antenna, so that the exact location of the interference can be pinpointed

**DISTRIBUTED DENIAL OF SERVICE ATTACKS**

Most **denial of service (DoS)** attacks against websites and gateways are **distributed DoS (DDoS)**. This means that the attack is launched from multiple hosts simultaneously. Typically, a threat actor will compromise machines to use as handlers in a command and control network. The handlers are used to compromise hundreds or thousands or millions of hosts with DoS tools (bots) forming a botnet.

Some types of DDoS attacks simply aim to consume network bandwidth, denying it to legitimate hosts, by using overwhelming numbers of bots. Others cause resource exhaustion on the hosts' processing requests, consuming CPU cycles and memory. This delays processing of legitimate traffic and could potentially crash the host system completely. For example, a **SYN flood attack** works by withholding the client's ACK packet during TCP's three-way handshake. Typically the client's IP address is spoofed, meaning that an invalid or random IP is entered so the server's SYN/ACK packet is misdirected. A server, router, or firewall can maintain a queue of pending connections, recorded in its state table. When it does not receive an ACK packet from the client, it resends the SYN/ACK packet a set number of times before timing out the connection. The problem is that a server may only be able to manage a limited number of pending connections, which the DoS attack quickly fills up. This means that the server is unable to respond to genuine traffic

**AMPLIFICATION, APPLICATION, AND OT ATTACKS**

In a distributed reflection DoS (DRDoS) or amplification SYN flood attack, the threat actor spoofs the victim's IP address and attempts to open connections with multiple servers. Those servers direct their SYN/ACK responses to the victim server. This rapidly consumes the victim's available bandwidth.

### Application Attacks

Where a network attack uses low-level techniques, such as SYN or SYN/ACK flooding, an application attack targets vulnerabilities in the headers and payloads of specific application protocols. For example, one type of **amplification attack** targets DNS services with bogus queries. One of the advantages of this technique is that while the request is small, the response to a DNS query can be made to include a lot of information, so this is a very effective way of overwhelming the bandwidth of the victim network with much more limited resources on the attacker's botnet.

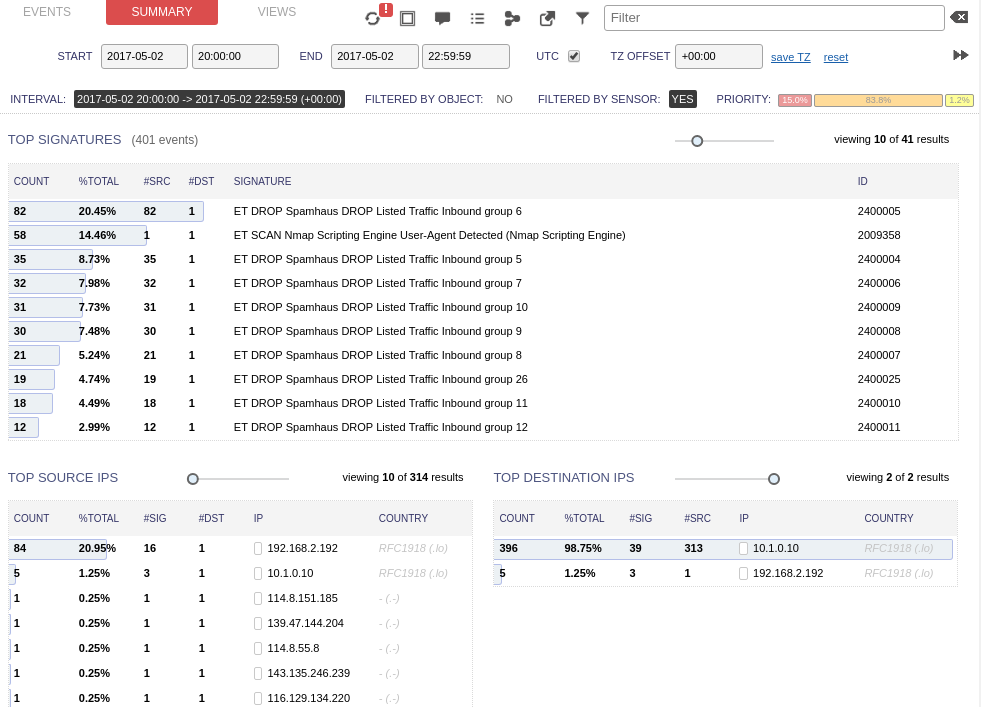
The **Network Time Protocol (NTP)** can be abused in a similar way. NTP helps servers on a network and on the Internet to keep the correct time. It is vital for many protocols and security mechanisms that servers and clients be synchronized. One NTP query (monlist) can be used to generate a response containing a list of the last 600 machines that the NTP server has contacted. As with the DNS amplification attack, this allows a short request to direct a long response at the victim network.

### Operational Technology (OT) Attacks

An **operational technology (OT)** network is established between embedded systems devices and their controllers. The term "operational" is used because these systems monitor and control physical electromechanical components, such as valves, motors, electrical switches, gauges, and sensors. DDoS attacks against the controllers in such networks can use the same techniques as against computer networks.

**DISTRIBUTED DENIAL OF SERVICE ATTACK MITIGATION**

DDoS attacks can be diagnosed by traffic spikes that have no legitimate explanation, but can usually only be counteracted by providing high availability services, such as load balancing and cluster services. In some cases, a stateful firewall can detect a DDoS attack and automatically block the source. However, for many of the techniques used in DDoS attacks, the source addresses will be randomly spoofed or launched by bots, making it difficult to detect the source of the attack.



*Dropping traffic from block-listed IP ranges using Security Onion IDS. (Screenshot used with permission from Security Onion.)*

When a network is faced with a DDoS or similar flooding attack, an ISP can use either an access control list (ACL) or a blackhole to drop packets for the affected IP address(es). A blackhole is an area of the network that cannot reach any other part of the network. The blackhole option is preferred, as evaluating each packet in a multi-gigabit stream against ACLs overwhelms the processing resources available. The blackhole also makes the attack less damaging to the ISP's other customers. With both approaches, legitimate traffic is discarded along with the DDoS packets.

Another option is to use **sinkhole** routing so that the traffic flooding a particular IP address is routed to a different network where it can be analyzed. Potentially some legitimate traffic could be allowed through, but the real advantage is to identify the source of the attack and devise rules to filter it. The target can then use low TTL DNS records to change the IP address advertised for the service and try to allow legitimate traffic past the flood.

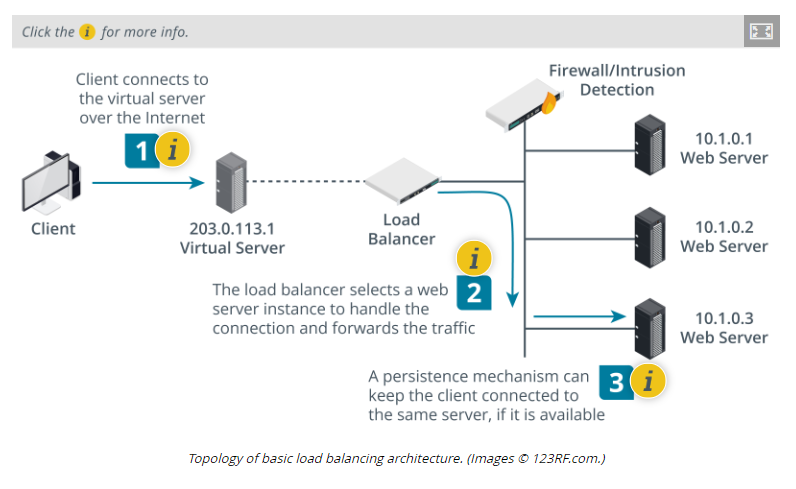
*There are cloud DDoS mitigation services that can act as sinkhole network providers and try to "scrub" flooded traffic.*

**LOAD BALANCING**

A **load balancer** distributes client requests across available server nodes in a farm or pool. This is used to provision services that can scale from light to heavy loads, and to provide mitigation against DDoS attacks. A load balancer also provides fault tolerance. If there are multiple servers available in a farm, all addressed by a single name/IP address via a load balancer, then if a single server fails, client requests can be routed to another server in the farm. You can use a load balancer in any situation where you have multiple servers providing the same function. Examples include web servers, front-end email servers, and web conferencing, A/V conferencing, or streaming media servers.

There are two main types of load balancers:

* Layer 4 load balancer—basic load balancers make forwarding decisions on IP address and TCP/UDP port values, working at the transport layer of the OSI model.
* Layer 7 load balancer (content switch)—as web applications have become more complex, modern load balancers need to be able to make forwarding decisions based on application-level data, such as a request for a particular URL or data types like video or audio streaming. This requires more complex logic, but the processing power of modern appliances is sufficient to deal with this.



**1. Virtual Server/Load Balancer**

The website (or other service) is published to DNS using its public IP address. This is referred to as a virtual server.

The machine operating as the virtual server is not a web server but a load balancing router. It accepts connections from Internet clients on the public address. The load balancer may use a firewall to drop any traffic that does not match its policy.

**2. Scheduling**

The load balancer uses some type of scheduling algorithm to select a web server instance to handle the client connection. It forwards the traffic to the instance, translating between the public IP address and the internal IP scheme.

This traffic can be subject to further filtering by a firewall or other security appliance.

**3. Source IP Affinity and Persistence**

An affinity or persistence mechanism can try to keep all the connection requests from a client session directed to the same server, if it is available.

Affinity uses IP and port data (layer 4), while persistence uses application data, such as a cookie (layer 7). Persistence is more reliable than affinity.

### Scheduling

The scheduling algorithm is the code and metrics that determine which node is selected for processing each incoming request. The simplest type of scheduling is called round robin; this just means picking the next node. Other methods include picking the node with the fewest connections or the best response time. Each method can also be weighted, using administrator set preferences or dynamic load information or both.

The load balancer must also use some type of heartbeat or health check probe to verify whether each node is available and under load or not. Layer 4 load balancers can only make basic connectivity tests while layer 7 appliances can test the application's state, as opposed to only verifying host availability.

### Source IP Affinity and Session Persistence

When a client device has established a session with a particular node in the server farm, it may be necessary to continue to use that connection for the duration of the session. Source IP or **session affinity** is a layer 4 approach to handling user sessions. It means that when a client establishes a session, it becomes stuck to the node that first accepted the request.

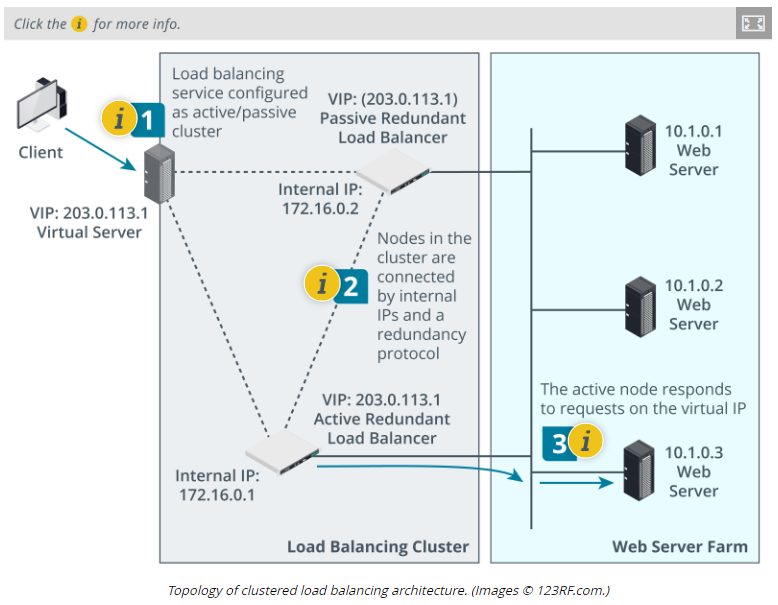
An application-layer load balancer can use **persistence** to keep a client connected to a session. Persistence typically works by setting a cookie, either on the node or injected by the load balancer. This can be more reliable than source IP affinity, but requires the browser to accept the cookie.

**CLUSTERING**

Where load balancing distributes traffic between independent processing nodes, **clustering** allows multiple redundant processing nodes that share data with one another to accept connections. This provides redundancy. If one of the nodes in the cluster stops working, connections can **failover** to a working node. To clients, the cluster appears to be a single server.

### Virtual IP

For example, you might want to provision two load balancer appliances so that if one fails, the other can still handle client connections. Unlike load balancing with a single appliance, the public IP used to access the service is shared between the two instances in the cluster. This is referred to as a virtual IP or shared or floating address. The instances are configured with a private connection, on which each is identified by its "real" IP address. This connection runs some type of redundancy protocol, such as Common Address Redundancy Protocol (CARP), that enables the active node to "own" the virtual IP and respond to connections. The redundancy protocol also implements a heartbeat mechanism to allow failover to the passive node if the active one should suffer a fault.



**1. Active/Passive Cluster**

This load balancing service has been configured as an active/passive cluster, so that if one load balancer fails, the other can take over.

In an active/active cluster, both load balancers would be used to handle traffic.

**2. Redundancy Protocol and Heartbeat**

The two load balancer nodes have a private connection. Each node is identified by a private IP address. In this example, they are 172.16.0.1 for the active node and 172.16.0.2 for the passive node.

The nodes exchange heartbeat information to allow failover when one node stops responding.

**3. Virtual IP**

The node configured as active "owns" the virtual IP (203.0.113.1). It uses its scheduling algorithm to select a web server node to handle the client connection request.

### Active/Passive (A/P) and Active/Active (A/A) Clustering

In the previous example, if one node is active, the other is passive. This is referred to as active/passive clustering. The major advantage of active/passive configurations is that performance is not adversely affected during failover. However, the hardware and operating system costs are higher because of the unused capacity.

An active/active cluster means that both nodes are processing connections concurrently. This allows the administrator to use the maximum capacity from the available hardware while all nodes are functional. In the event of a failover the workload of the failed node is immediately and transparently shifted onto the remaining node. At this time, the workload on the remaining nodes is higher and performance is degraded.

### Application Clustering

Clustering is also very commonly used to provision fault tolerant application services. If an application server suffers a fault in the middle of a session, the session state data will be lost. Application clustering allows servers in the cluster to communicate session information to one another. For example, if a user logs in on one instance, the next session can start on another instance, and the new server can access the cookies or other information used to establish the login.

**QUALITY OF SERVICE (QOS)**

Most network appliances process packets on a best effort and first in, first out (FIFO) basis. **Quality of Service (QoS)** is a framework for prioritizing traffic based on its characteristics. It is primarily used to support voice and video applications that require a minimum level of bandwidth and are sensitive to latency and jitter. **Latency** is the time it takes for a transmission to reach the recipient, measured in milliseconds (ms). **Jitter** is defined as being a variation in the delay, or an inconsistent rate of packet delivery. FIFO-based delivery makes it more likely that other applications sharing the same network will cause loss of bandwidth and increase latency and jitter for a real-time service.

Implementing QoS is a complex project, as there are many different ways to do it, and many different protocols and appliances involved. In overview, a QoS implementation could work as follows:

1. The organization performs application discovery to identify bandwidth, latency, and jitter thresholds of the protocols in use and determine their relative priority. The applications are then mapped to standard class of service (CoS) codes at layer 2 and layer 3. These codes are configured across the range of hosts and intermediate systems that handle QoS traffic.
2. A QoS-compatible endpoint device or application uses the **DiffServ** field in the IP header (layer 3) and adds an 802.1p field to the Ethernet header (layer 2) to indicate that the packet should be treated as priority (traffic marking). It transmits the frame to the switch.
3. If the switch supports QoS, it uses the 802.1p header to prioritize the frame. Note that it can only do this by holding a queue of outgoing traffic and delaying non-priority frames. If the queue is full, a traffic policing policy must state whether non-priority frames should be dropped, or whether the queue should be cleared at the expense of reducing QoS.
4. A similar process occurs at routers and load balancers on the network edge, though they can inspect the DiffServ IP packet header, rather than having to rely on the more limited 802.1p header. Note that prioritization always takes place on the outbound interface, with low priority traffic being held in a queue.

QoS marking introduces the potential for DoS attacks. If a threat actor can craft packets that are treated as high priority and send them at a high rate, the network can be overwhelmed. Part of QoS involves identifying trust boundaries to establish a legitimate authority for marking traffic. You should also ensure that there is always sufficient bandwidth for security-critical monitoring data and network management/configuration traffic.