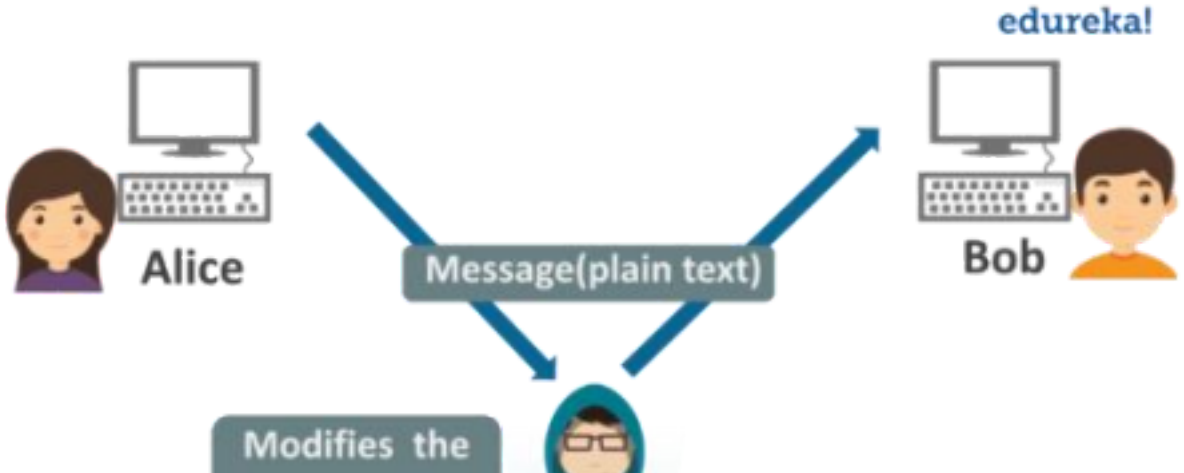
APPLY SECURE NETWORK ADMINISTRATION PRINCIPLES / SECURE WIRELESS TRAFFIC

Network Administration Security Methods

- ❑Flood guards
- ❑Loop protection
- ❑Port security
- ❑MAC limiting
- ❑MAC filtering



- ❑Network separation
- ❑VLAN management
- ❑Implicit deny
- ❑Log analysis

Network Administration Security Methods

Flood guards serves as preventive control against denial-of-service distributed denial-of-service (DDoS) attacks.

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network.

Port Security enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port.

Network Administration Security Methods

MAC LIMITING protects against flooding of the Ethernet switching table, and is enabled on Layer 2 interfaces (ports).

MAC FILTERING refers to a security access control method whereby the MAC address assigned to each network card is used to determine access to the network.

NETWORK SEPARATION is the tool used for dividing a network into smaller parts which are called subnetworks or network segments.

Network Administration Security Methods

VLAN MANAGEMENT is a network switch that contains a mapping of device information to VLAN.

IMPLICIT DENY is a security stance treats everything not given specific and selective permission as suspicious.

LOG ANALYSIS is the term used for analysis of computer-generated records for helping organizations, businesses or networks in proactively and reactively mitigating different risks.

Guidelines for Applying Network Security Administration Principles

✔ Manage network devices so that they are configured according to security policies.

✔ Maintain documentation for all current server configurations. ✔ Establish and document baselines.

✔ Implement strong ACLs and implement implicit deny.

✔ Update antivirus software regularly.

✔ Configure only required network services.

Guidelines for Applying Network Security Administration Principles

- ✔ Disable unused interfaces and unused application service ports.
- ✔ Create and implement a DRP.
- ✔ Apply security updates and patches.
- ✔ Encrypt sensitive data.
- ✔ Check event logs for unusual activity.
- ✔ Monitor network activity.

Wireless Networks

- ❑Portable
- ❑Inexpensive

- No obtrusive cabling
- Introduces new, significant security issues

A wireless LAN (WLAN) allows users to connect to a network while allowing them to remain mobile.

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

WIRELESS STANDARDS

Wireless standards are a set of services and protocols that dictate how your Wi

Fi network (and other data transmission networks)

acts.

WIRELESS STANDARDS

802.11: There were actually two variations on the initial 802.11 wireless standard.

Both offered 1 or 2Mbps transmission speeds and the same RF of

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

2.4GHz.

WIRELESS STANDARDS

802.11a - The first “letter” following the June 1997 approval of the 802.11 standard, this one provided for operation in the 5GHz frequency, with data rates up to 54Mbps.

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

WIRELESS STANDARDS

802.11b - Released in September 1999, it's most likely that your first home router was 802.11b, which operates in the 2.4GHz frequency and provides a data rate up to 11 Mbps.

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

WIRELESS STANDARDS

802.11g offers wireless transmission over distances of 150 feet and speeds

up to 54Mbps compared with the 11Mbps of the 802.11b

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

standard.

WIRELESS STANDARDS

802.11n (Wi-Fi 4)

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

WIRELESS STANDARDS

802.11ac(Wi-Fi 5) - Current home wireless routers are likely compliant, and operate in the 5 GHz frequency space.

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Wireless Security Protocols

Wireless security is the anticipation of unauthorized access or breaks to computers or data by means of wireless networks.

Wireless Security Protocols

WEP was included as part of the original IEEE 802.11

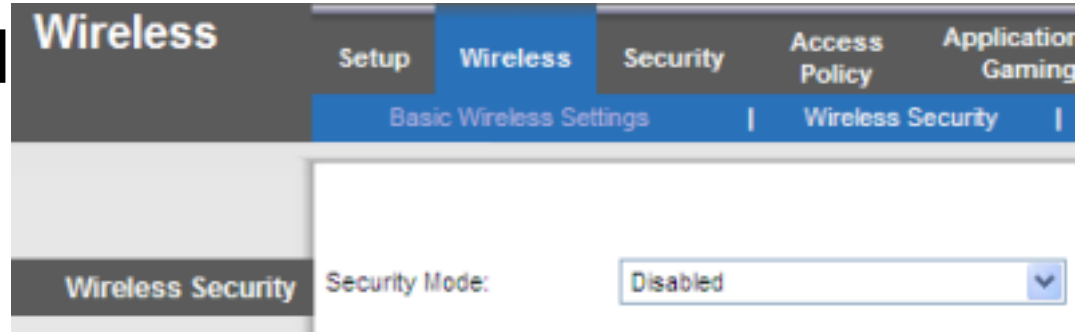
standard and was intended to provide privacy

WPA was designed as the interim successor to WEP.

WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control

WPA3, released in June 2018, is the successor to WPA2, which security experts describe as “broken.”

Wireless Security Method



- ❑Configure access point settings.
- ❑Adjust SSID settings.

❑Enable encryption.

❑Configure network security settings.

❑Adjust antenna and power source placement. ❑Adjust client settings.

Understanding Service Set IDentifier (SSID)

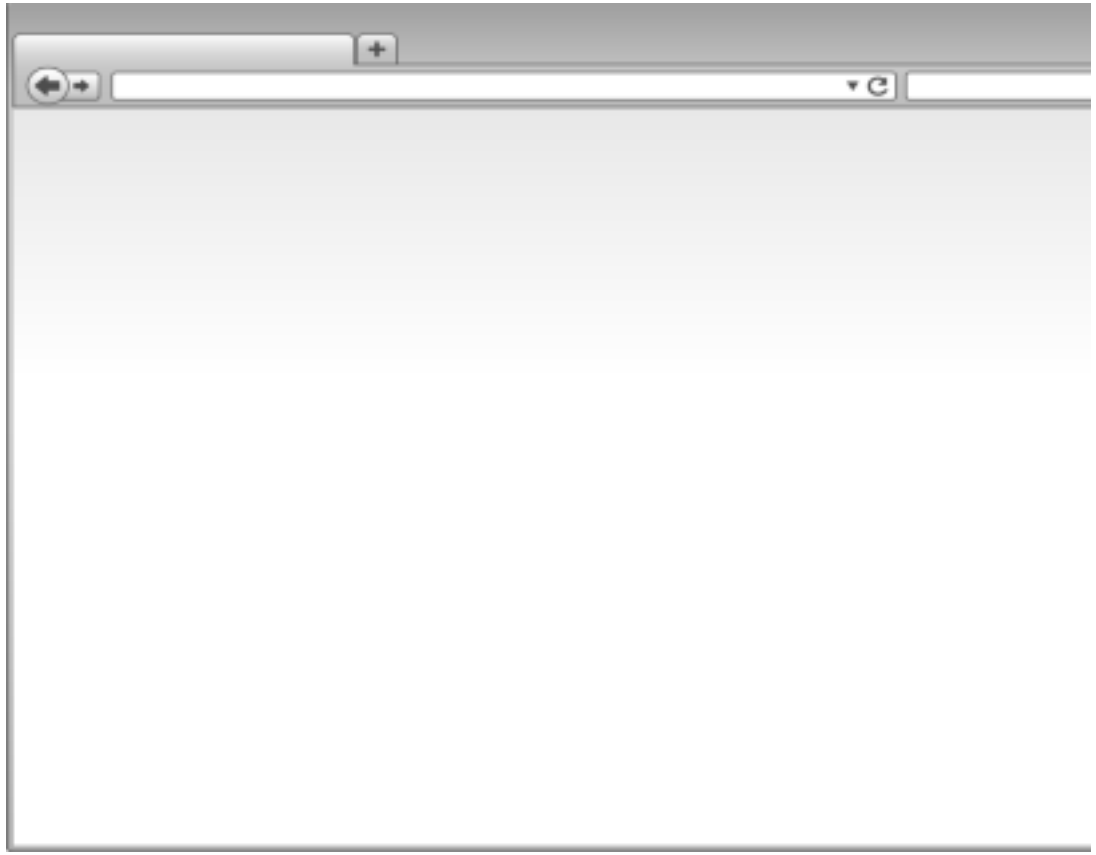
The most basic component of the wireless network is the SSID

While there aren't any specific security capabilities associated with the SSID, there are some security considerations that should be taken into account:

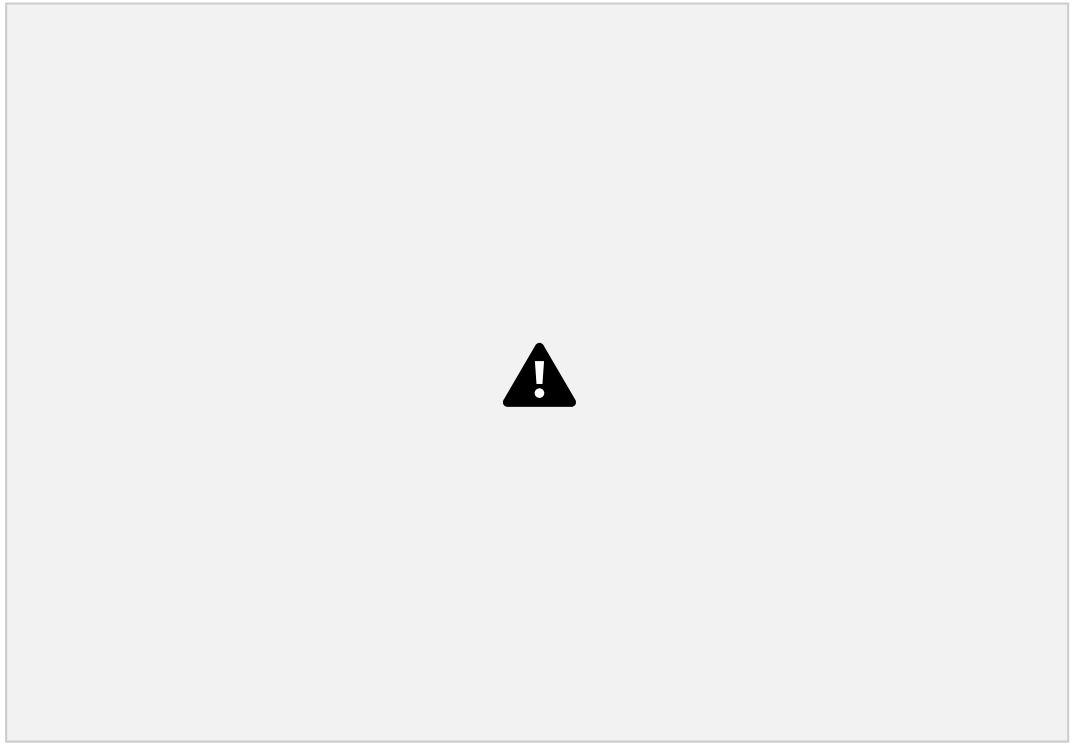
✔Choose your own SSID
✔Follow naming conventions
✔Turn off your SSID

Captive Portals

A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.



Site Surveys



Site surveys are inspections of an area where work is proposed, to gather information for a design or an estimate to complete the initial tasks required for an outdoor activity.

Guidelines for Securing Wireless Traffic

- ❑Keep sensitive data off of wireless devices.

❑Install antivirus software on wireless devices.

❑Harden wireless devices and routers. ❑Use a VPN with IPSec.

❑Conduct a site survey.

❑Implement security protocols.

Guidelines for Securing Wireless Traffic

❑Implement authentication and access control.

❑Implement an IDS.

❑Avoid relying on MAC filtering and disabling SSID broadcasts. ❑Implement captive portals that require login credentials. ❑Follow hardware and software vendors' security recommendations.

- ❑Document all changes.