IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

WIRELESS TRANSPORT LLC, Plaintiff, **v.** **FORTINET, INC.,** Defendant.	C.A. NO. **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

1. This is an action for patent infringement in which Wireless Transport LLC makes the following allegations against Fortinet, Inc.

PARTIES

2. Plaintiff Wireless Transport LLC ("Plaintiff" or "Wireless Transport") is a Delaware limited liability company with its principal place of business at 16192 Coastal Highway, Lewes, DE 19959.

3. On information and belief, Fortinet, Inc ("Defendant" or "Fortinet") is a corporation organized and existing under the laws of the State of Delaware, which can be served through its registered agent Corporation Service Company, 251 Little Falls Dr, Wilmington, DE 19808.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, Defendant is incorporated in the State of Delaware, and, thus, resides in the State of Delaware for the purposes of 28 U.S.C. § 1400(b).

6. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Delaware Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Delaware and in this Judicial District.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,563,813

7. Plaintiff is the owner of United States Patent No. 6,563,813 ("the '813 patent") entitled "Wireless Transport Protocol." The '813 Patent issued on May 13, 2003. A true and correct copy of the '813 Patent is attached as Exhibit A.

8. Defendant owns, uses, operates, advertises, controls, sells, and otherwise provides products and/or services that infringe the '813 patent. The '813 patent provides, among other things, " A communication system comprising: a wireless client; a wireless network; a land-line client; a land-line network; and a network backbone interfacing said land-line network and said wireless network to allow data packets to be exchanged between said wireless client and said land-line client, said communication system using a wireless transport layer protocol for data frame transmission over said land-line and wireless networks, each data frame including connection handling information specifying at least one data transport connection to be used to transmit data between said wireless client and said land-line client over said wireless and land-line networks; connection addressing information; a user data field including a data packet to be transmitted from one client to another client; and at least one sequencing field identifying the last packet received by the client that is transmitting a current data packet."

9. Defendant directly and/or through intermediaries, made, has made, used, imported, provided, supplied, distributed, sold, and/or offered for sale products and/or services that infringed one or more claims of the '813 patent, including at least Claim 6, in this district and elsewhere in the United States. For example, but without limitation, the FortiGate Integrated Wireless Management Solution forms a communication system within the meaning of the '813 Patent. By making, using, importing, offering for sale, and/or selling such products and services,

and all like products and services, Defendant has injured Plaintiff and is thus liable for infringement of the '813 patent pursuant to 35 U.S.C. § 271.

10. Fortinet makes, uses, sells and/or offers for sale a communication system. For example, Fortinet provides FortiGate Integrated Wireless Management Solution ("a communication system") which comprises network products including FortiAP Access Points and FortiGate with built-in Wireless LAN Controller (FortiWLC).

Overview | Models and specifications | Resources | Demo | FAQ

Overview of FortiGate Integrated Wireless Management

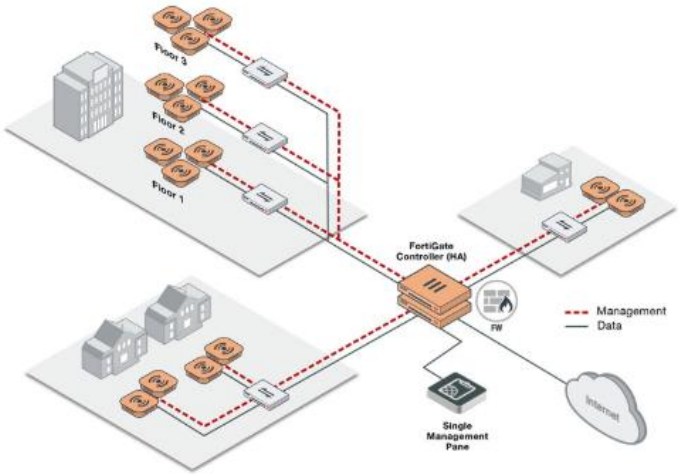
Customers demand more features provided by fewer components to reduce cost and complexity. FortiGate, Fortinet's security appliance, comes with Wireless LAN and integrated Switch controllers to provide secure Wi-Fi connectivity at no additional cost. The integrated solution is enabled for the Security Fabric and provides the broad visibility, automatic protection and integrated threat information needed to protect important assets and data from organizations around the world from a unified console. For assistance in selecting an AP, our AP product selector is located **here** .

Source: https://www.fortinet.com/it/products/secure-wifi/fortigate-integrated.html

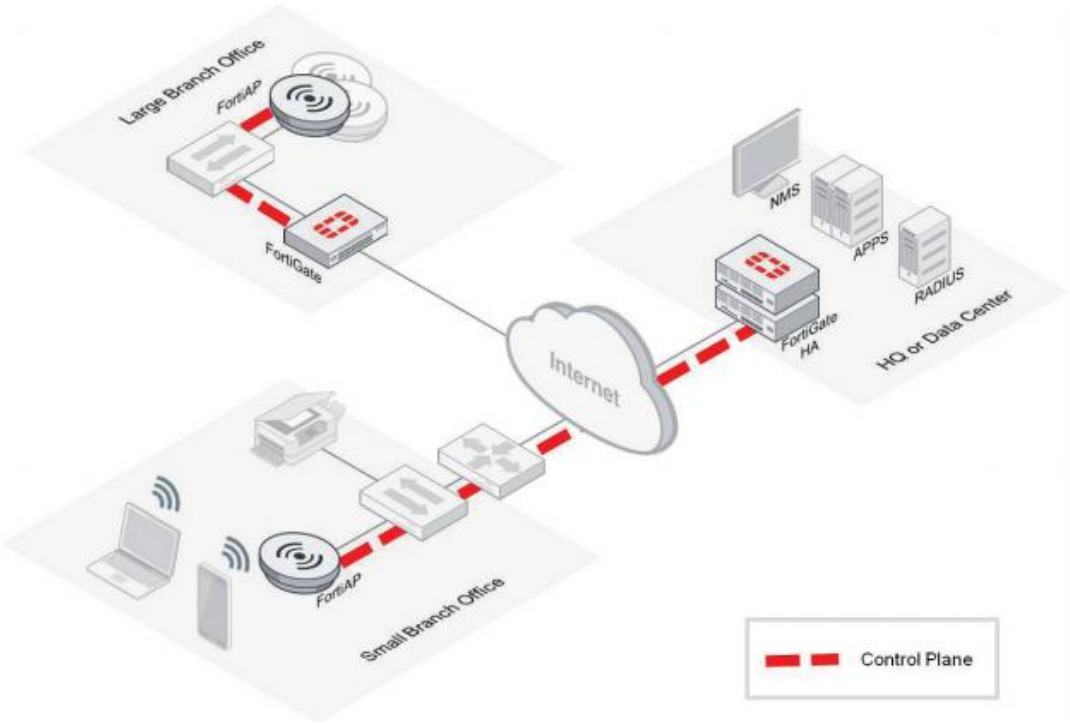
FortiGate Integrated Controller

- Single pane-of-glass for network security and wireless access
- Tight integration with Fortinet's Security Fabric
- No extra licenses necessary

Learn about deploying FortiAPs with a FortiGate »

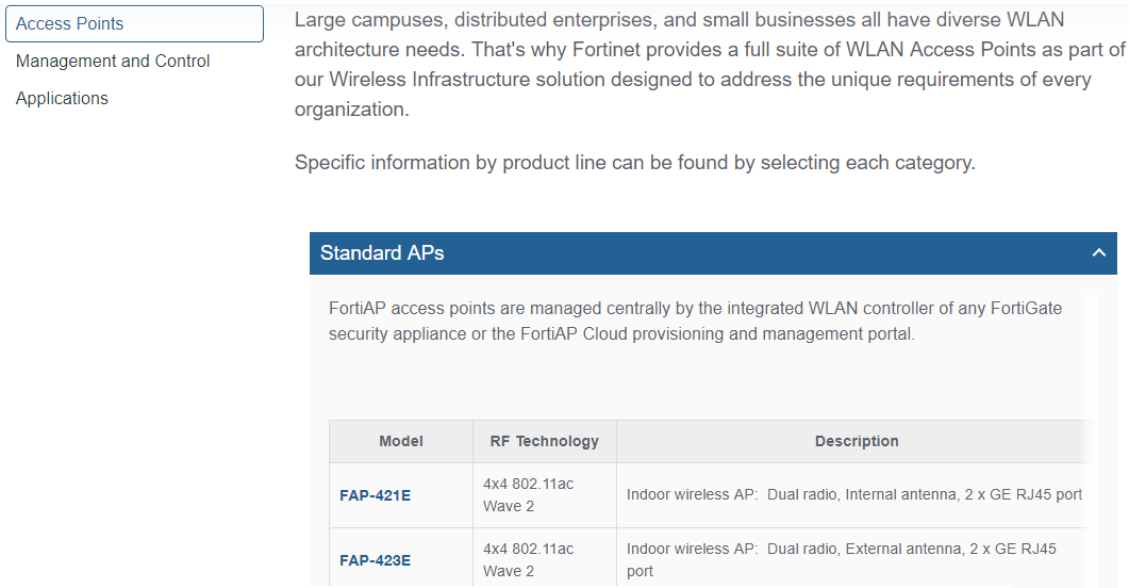


Source: https://www.fortinet.com/products/secure-wifi/wirelessmanagement.html



Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

11. Fortinet provides a communication system comprising a wireless client. For example, the FortiGate solution which when equipped with FortiAP Access Points (such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc.) provide connectivity for devices ("wireless clients") which support IEEE 802.11 a/b/g/n/ac standard.



Source: https://www.fortinet.com/products/secure-wifi/fortigate-integrated.html#models-specs

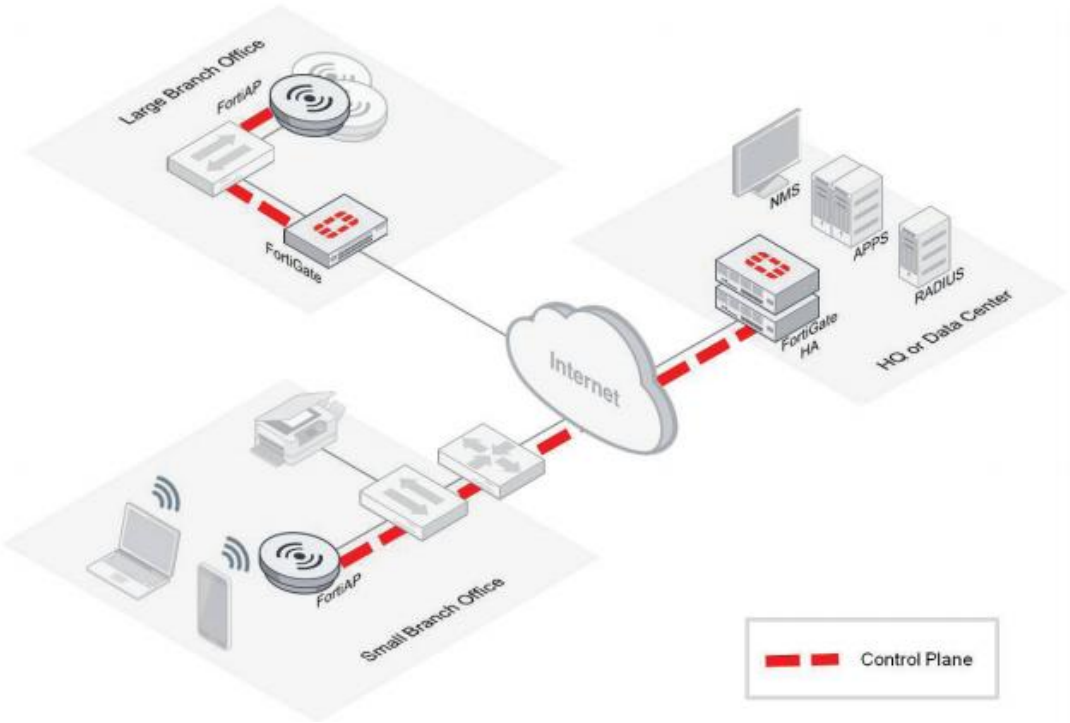
FortiAP-U Universally Manageable Indoor Access Points

	FAP-U221EV	FAP-U223EV	FAP-U321EV	FAP-U323EV	FAP-U421EV	FAP-U423EV
						
Suggested Use Case	Medium Density, 802.11ac indoor	Medium Density, 802.11ac indoor	High density, high performance 802.11ac W2 indoor	High density, high performance 802.11ac W2 indoor	High density, high performance 802.11ac W2 indoor	High density, high performance 802.11ac W2 indoor
Hardware						
Number of Radios	2 + 1 BT/BLE	2 + 1 BT/BLE	2 + 1 BT/BLE	2 + 1 BT/BLE	2 + 1 BT/BLE	2 + 1 BT/BLE
Number of Antennas	4 Internal + 1 BT/BLE Internal	4 External (RP-SMA) + 1 BT/BLE Internal	6 Internal + 1 BT/BLE Internal	6 External (RP-SMA) + 1 BT/BLE Internal	8 Internal + 1 BT/BLE Internal	8 External (RP-SMA) + 1 BT/BLE Internal
Antenna Type and Peak Gain	Patch: 3 dBi for 2.4 GHz, 4 dBi for 5 GHz	Dipole: 3 dBi for 2.4 GHz, 4 dBi for 5 GHz	Patch: 4.5 dBi for 2.4 GHz, 6.5 dBi for 5 GHz	Dipole: 3.5 dBi for 2.4 GHz, 5 dBi for 5 GHz	Patch: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz	Dipole: 3 dBi for 2.4 GHz, 3 dBi for 5 GHz
Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (3x3:3) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (3x3:3) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (4x4:4) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (4x4:4) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (3x3:3) 20/40/80 MHz (256/1024 QAM)	5 GHz a/n/ac (3x3:3) 20/40/80 MHz (256/1024 QAM)	5 GHz a/n/ac (4x4:4) 20/40/80/160 MHz (256/1024 QAM)	5 GHz a/n/ac (4x4:4) 20/40/80/160 MHz (256/1024 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 450 Mbps Radio 2: up to 2,600 Mbps	Radio 1: up to 450 Mbps Radio 2: up to 2,600 Mbps	Radio 1: up to 600 Mbps Radio 2: up to 3,466 Mbps	Radio 1: up to 600 Mbps Radio 2: up to 3,466 Mbps

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Wireless_Product_Matrix.pdf, page 5

Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4



Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

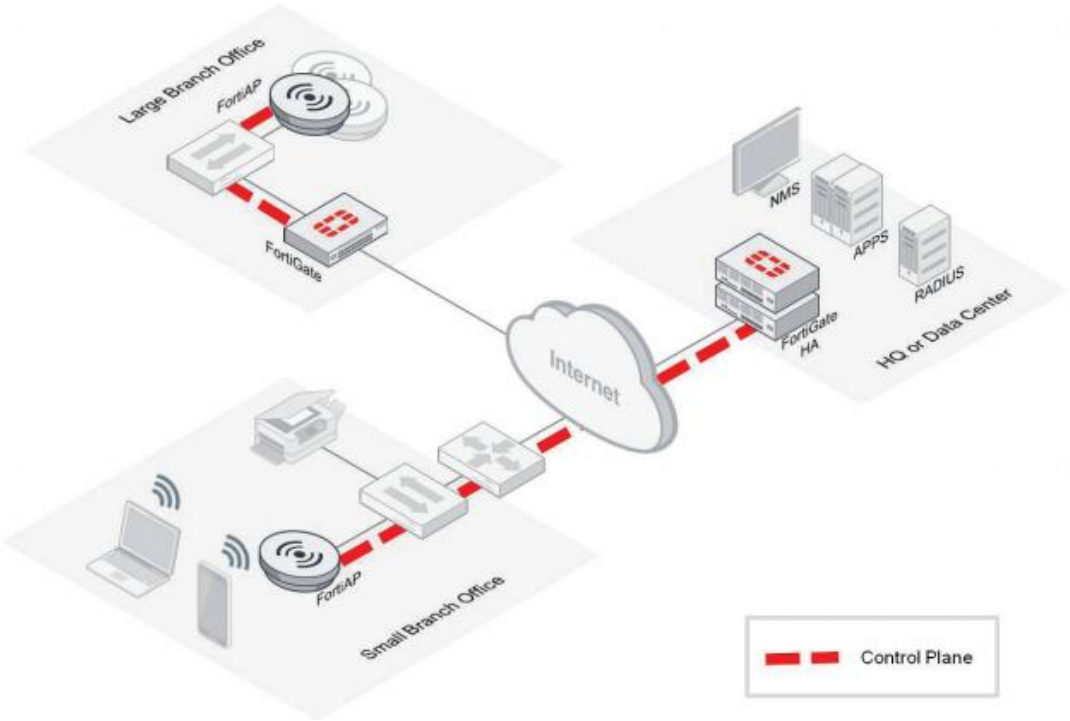
12. Fortinet provides a communication system comprising a wireless network. For example, the FortiAP Access Points (such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc.) and FortiWLC work on the wireless networking standards (such as IEEE 802.11 (WLAN) standard on 2.4 GHz and 5 GHz band frequencies).

Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4

Certifications	
Wi-Fi Alliance	Wi-Fi Alliance certified (802.11ac, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Save).
Firewall	ICSA firewall enterprise certification
	ICSA IPv6 certified firewall
	USGv6 certified firewall
IEEE Standard Compliance	802.11a, 802.11b, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (UAPSD), 802.11n with HT40 support, (4x4 MIMO)
	802.11e and WME/WMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues
	802.11h, 802.11j
	802.11i (TKIP/AES), 802.1x

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS_Wireless.pdf, page 5



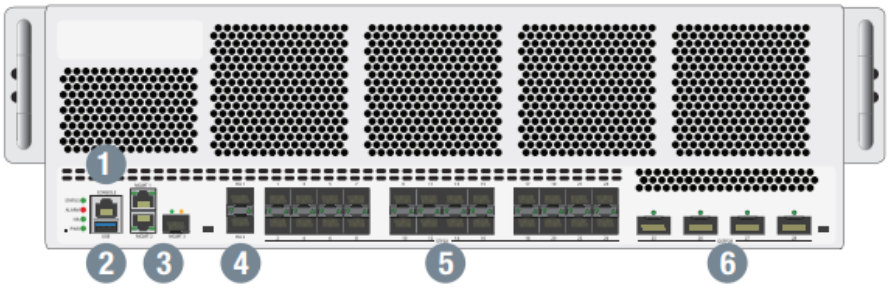
Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

13. Fortinet provides a communication system comprising a land-line client. For example, the FortiGate solution comprises FortiAP Access Points (such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc.) and FortiGate (such as 6000F Series) to support a land-line client.

Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4

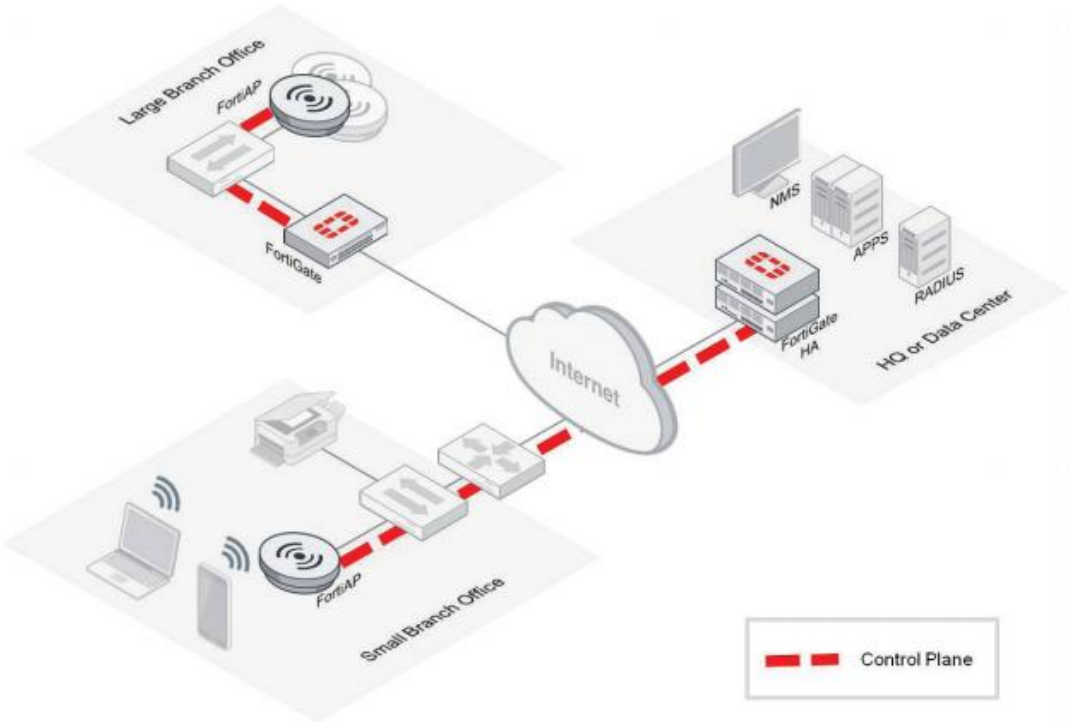
FortiGate 6300F/6301F/6500F/6501F



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45, 1x 1/10 GE SFP+ Management Ports

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_6000F_Series.pdf, page 3

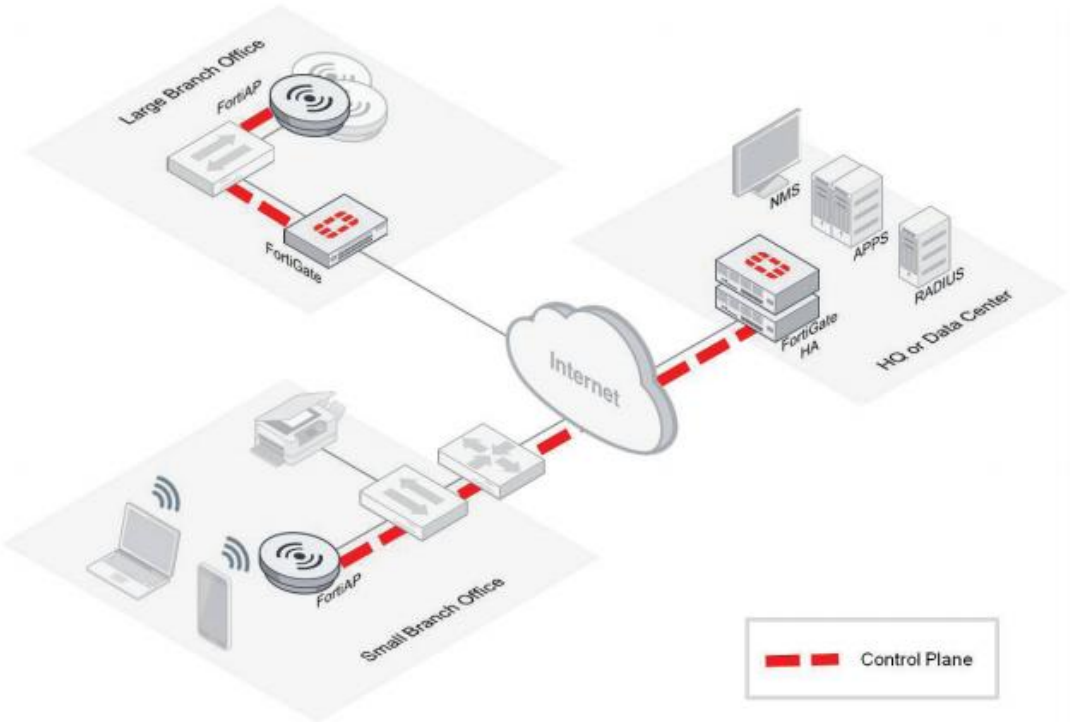


Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

14. Fortinet provides a communication system comprising a land-line network. For example, the FortiAP Access Points (such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc.) support IEEE 802.3 (Ethernet) wired network standard.

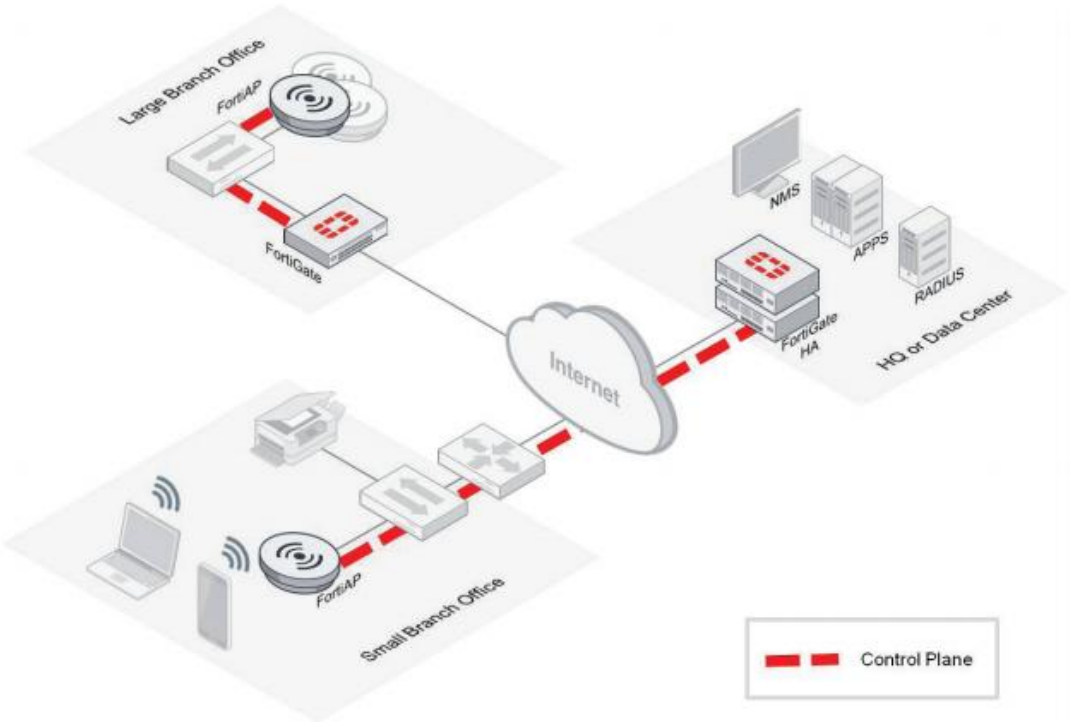
Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4



Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

15. Fortinet provides a communication system comprising a network backbone interfacing said land-line network and said wireless network to allow data packets to be exchanged between said wireless client and said land-line client. For example, Fortinet provide network products (including FortiAP Access Points such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc. and FortiGate such as 6000F series) for interfacing a land-line network and a wireless network. The network products support TCP/IP (Transmission Control Protocol/Internet Protocol) which allow exchange of packets between wireless network and land-line/wired network.



Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

Access Points
Management and Control
Applications

Large campuses, distributed enterprises, and small businesses all have diverse WLAN architecture needs. That's why Fortinet provides a full suite of WLAN Access Points as part of our Wireless Infrastructure solution designed to address the unique requirements of every organization.

Specific information by product line can be found by selecting each category.

Standard APs

FortiAP access points are managed centrally by the integrated WLAN controller of any FortiGate security appliance or the FortiAP Cloud provisioning and management portal.

Model	RF Technology	Description
FAP-421E	4x4 802.11ac Wave 2	Indoor wireless AP: Dual radio, Internal antenna, 2 x GE RJ45 port
FAP-423E	4x4 802.11ac Wave 2	Indoor wireless AP: Dual radio, External antenna, 2 x GE RJ45 port

Source: https://www.fortinet.com/products/secure-wifi/fortigate-integrated.html#models-specs

DATA SHEET

FortiGate® 6000F Series

FortiGate 6300F, 6301F, 6500F and 6501F

Next Generation Firewall
Segmentation
IPS
Mobile Security

The FortiGate 6000F series delivers high performance threat protection and SSL inspection for large enterprises and service providers, with the flexibility to be deployed at the enterprise/cloud edge, in the data center core or internal segments. The multiple high-speed interfaces, high port density, superior security efficacy and high throughput of the 6000F series keeps your network connected and secure.

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_6000F_Series.pdf, page

2. TCP/IP Overview

The generic term "TCP/IP" usually means anything and everything related to the specific protocols of TCP and IP. It can include other protocols, applications, and even the network medium. A sample of these protocols are: UDP, ARP, and ICMP. A sample of these applications are: TELNET, FTP, and rcp. A more accurate term is "internet technology". A network that uses internet technology is called an "internet".

2.1 Basic Structure

To understand this technology you must first understand the following logical structure:

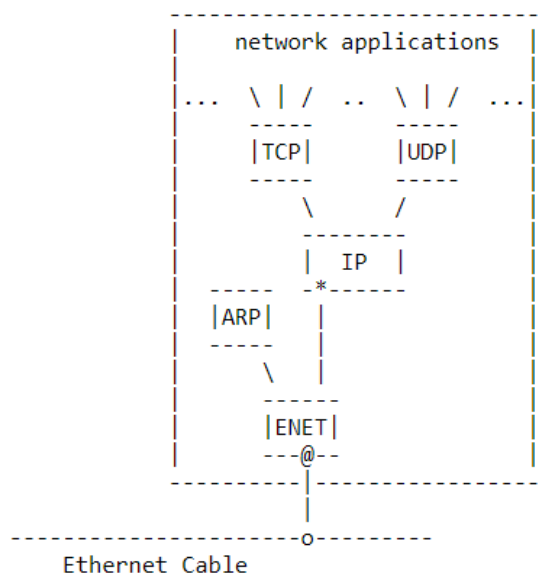


Figure 1. Basic TCP/IP Network Node

1

Source: https://tools.ietf.org/html/rfc1180, page 1

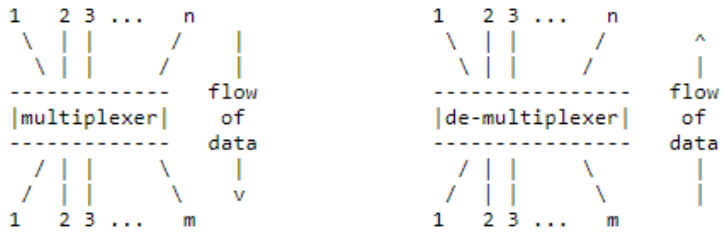


Figure 4. n-to-m multiplexer and m-to-n de-multiplexer

It performs this multiplexing in either direction to accommodate incoming and outgoing data. An IP module with more than 1 network interface is more complex than our original example in that it can forward data onto the next network. Data can arrive on any network interface and be sent out on any other.

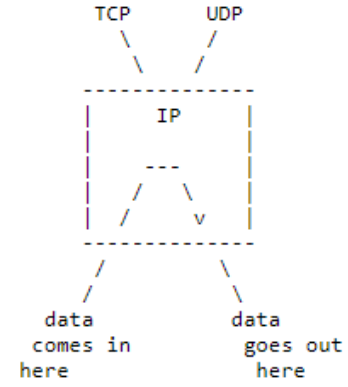


Figure 5. Example of IP Forwarding a IP Packet

The process of sending an IP packet out onto another network is called "forwarding" an IP packet. A computer that has been dedicated to the task of forwarding IP packets is called an "IP-router".

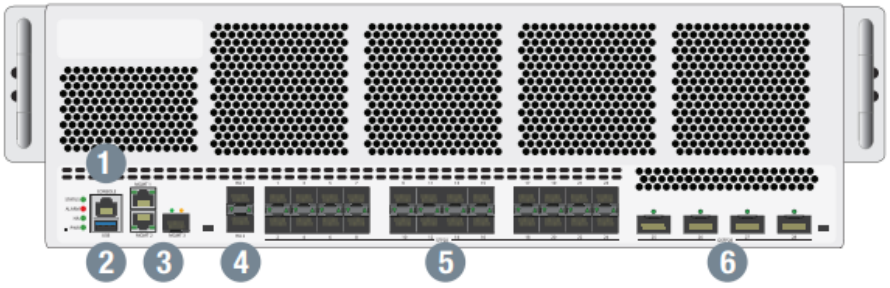
As you can see from the figure, the forwarded IP packet never touches the TCP and UDP modules on the IP-router. Some IP-router implementations do not have a TCP or UDP module.

Source: https://tools.ietf.org/html/rfc1180, page 5

Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4

FortiGate 6300F/6301F/6500F/6501F

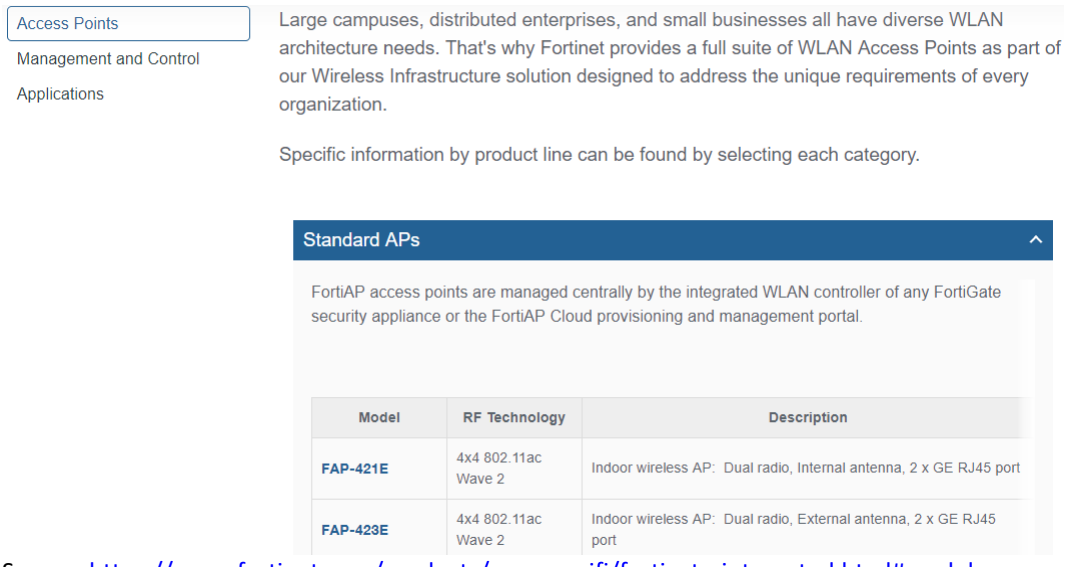


Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45, 1x 1/10 GE SFP+ Management Ports

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_6000F_Series.pdf, page 3

16. Fortinet provides a communication system which uses a wireless transport layer protocol for data frame transmission over said land-line and wireless networks, each data frame including connection handling information specifying at least one data transport connection to be used to transmit data between said wireless client and said land-line client over said wireless and land-line networks. For example, Fortinet provide network products (including FortiAP Access Points such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc. and FortiGate such as 6000F series) which support wireless protocols such as TCP/IP for transmission of data packets (such as Ethernet frame, IP packet, UDP datagram, and TCP segment and/or application message) over land-line and wireless networks. Further, TCP/IP data frames (such as Ethernet frame) contain connection handling information such as the destination address, source address ("connection addressing information"), type field and data.



Access Points
Management and Control
Applications

Large campuses, distributed enterprises, and small businesses all have diverse WLAN architecture needs. That's why Fortinet provides a full suite of WLAN Access Points as part of our Wireless Infrastructure solution designed to address the unique requirements of every organization.

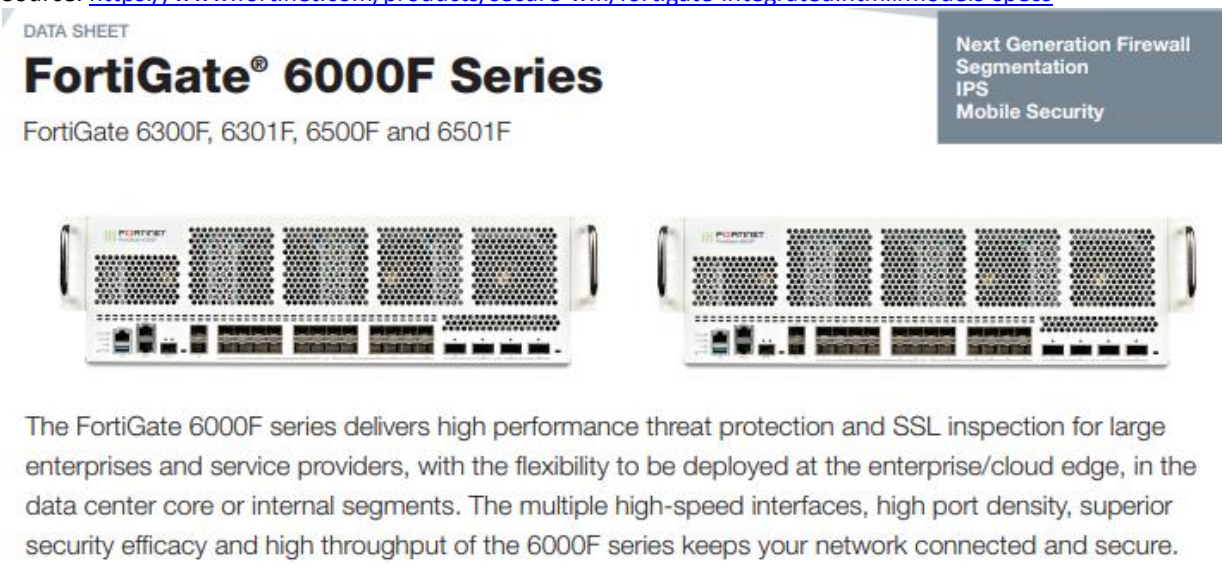
Specific information by product line can be found by selecting each category.

Standard APs

FortiAP access points are managed centrally by the integrated WLAN controller of any FortiGate security appliance or the FortiAP Cloud provisioning and management portal.

Model	RF Technology	Description
FAP-421E	4x4 802.11ac Wave 2	Indoor wireless AP: Dual radio, Internal antenna, 2 x GE RJ45 port
FAP-423E	4x4 802.11ac Wave 2	Indoor wireless AP: Dual radio, External antenna, 2 x GE RJ45 port

Source: https://www.fortinet.com/products/secure-wifi/fortigate-integrated.html#models-specs



DATA SHEET

FortiGate® 6000F Series

FortiGate 6300F, 6301F, 6500F and 6501F

Next Generation Firewall
Segmentation
IPS
Mobile Security

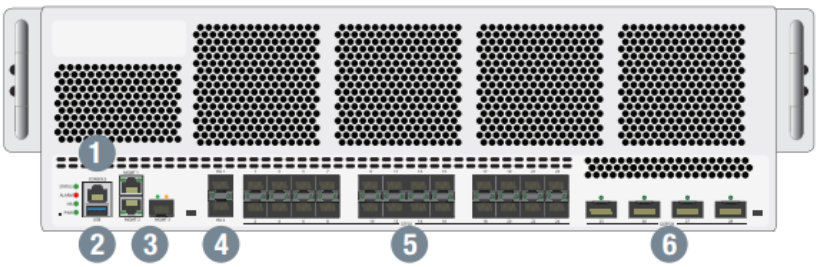
The FortiGate 6000F series delivers high performance threat protection and SSL inspection for large enterprises and service providers, with the flexibility to be deployed at the enterprise/cloud edge, in the data center core or internal segments. The multiple high-speed interfaces, high port density, superior security efficacy and high throughput of the 6000F series keeps your network connected and secure.

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_6000F_Series.pdf, page 1

Radio 1 Capabilities	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (64 QAM)
Radio 2 Capabilities	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maximum Data Rate	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps	Radio 1: up to 300 Mbps Radio 2: up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Interfaces	1x 10/100/1000 Base-T RJ45, 1x Type A USB	1x 10/100/1000 Base-T RJ45, 1x Type A USB
Power over Ethernet (PoE)	IEEE 802.3af or 802.3.at	IEEE 802.3af or 802.3.at
Simultaneous SSIDs	Up to 16 (14 if background scanning enabled)	Up to 16 (14 if background scanning enabled)
EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
User/Device Authentication	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Maximum Tx Power (Conducted)	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*	2.4 GHz: 25 dBm / 316 mW (2 chains combined)* 5 GHz: 23 dBm/ 200 mW (2 chains combined)*
Kensington Lock	Yes	Yes
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3at, 802.3az

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_U_Series.pdf, page 4

FortiGate 6300F/6301F/6500F/6501F



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45, 1x 1/10 GE SFP+ Management Ports

Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_6000F_Series.pdf, page 3

2.2 Terminology

The name of a unit of data that flows through an internet is dependent upon where it exists in the protocol stack. In summary: if it is on an Ethernet it is called an Ethernet frame; if it is between the Ethernet driver and the IP module it is called a IP packet; if it is between the IP module and the UDP module it is called a UDP datagram; if it is between the IP module and the TCP module it is called a TCP segment (more generally, a transport message); and if it is in a network application it is called a application message.

These definitions are imperfect. Actual definitions vary from one publication to the next. More specific definitions can be found in RFC 1122, section 1.3.3.

A driver is software that communicates directly with the network interface hardware. A module is software that communicates with a driver, with network applications, or with another module.

Source: https://tools.ietf.org/html/rfc1180, page 2

3. Ethernet

This section is a short review of Ethernet technology.

An Ethernet frame contains the destination address, source address, type field, and data.

An Ethernet address is 6 bytes. Every device has its own Ethernet address and listens for Ethernet frames with that destination address. All devices also listen for Ethernet frames with a wild-card destination address of "FF-FF-FF-FF-FF-FF" (in hexadecimal), called a "broadcast" address.

Ethernet uses CSMA/CD (Carrier Sense and Multiple Access with Collision Detection). CSMA/CD means that all devices communicate on a single medium, that only one can transmit at a time, and that they can all receive simultaneously. If 2 devices try to transmit at the same instant, the transmit collision is detected, and both devices wait a random (but short) period before trying to transmit again.

Source: https://tools.ietf.org/html/rfc1180, page 7

4. ARP

When sending out an IP packet, how is the destination Ethernet address determined?

ARP (Address Resolution Protocol) is used to translate IP addresses to Ethernet addresses. The translation is done only for outgoing IP packets, because this is when the IP header and the Ethernet header are created.

4.1 ARP Table for Address Translation

The translation is performed with a table look-up. The table, called the ARP table, is stored in memory and contains a row for each computer. There is a column for IP address and a column for Ethernet address. When translating an IP address to an Ethernet address, the table is searched for a matching IP address. The following is a simplified ARP table:

IP address	Ethernet address
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

TABLE 1. Example ARP Table

The human convention when writing out the 4-byte IP address is each byte in decimal and separating bytes with a period. When writing out the 6-byte Ethernet address, the conventions are each byte in hexadecimal and separating bytes with either a minus sign or a colon.

The ARP table is necessary because the IP address and Ethernet address are selected independently; you can not use an algorithm to translate IP address to Ethernet address. The IP address is selected by the network manager based on the location of the computer on the internet. When the computer is moved to a different part of an internet, its IP address must be changed. The Ethernet address is selected by the manufacturer based on the Ethernet address space licensed by the manufacturer. When the Ethernet hardware interface board changes, the Ethernet address changes.

Source: https://tools.ietf.org/html/rfc1180#page-2, page 8

application, the TCP module, and the IP module. At this point the IP packet has been constructed and is ready to be given to the Ethernet driver, but first the destination Ethernet address must be determined.

The ARP table is used to look-up the destination Ethernet address.

4.3 ARP Request/Response Pair

But how does the ARP table get filled in the first place? The answer is that it is filled automatically by ARP on an "as-needed" basis.

Two things happen when the ARP table can not be used to translate an address:

1. An ARP request packet with a broadcast Ethernet address is sent out on the network to every computer.

2. The outgoing IP packet is queued.

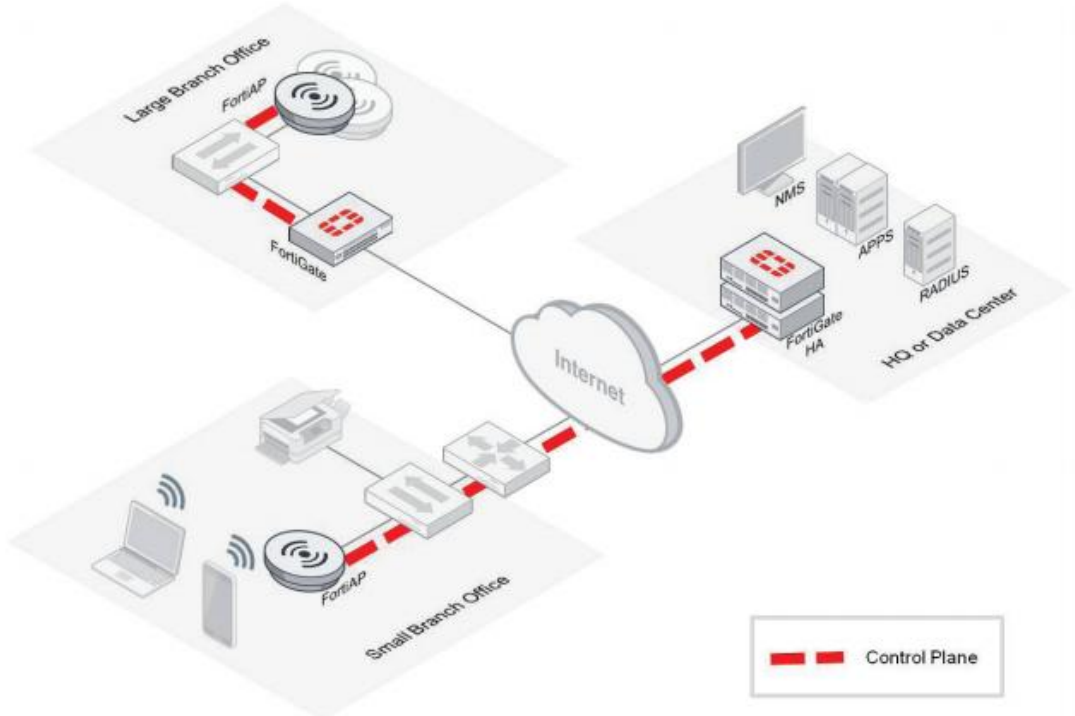
Every computer's Ethernet interface receives the broadcast Ethernet frame. Each Ethernet driver examines the Type field in the Ethernet frame and passes the ARP packet to the ARP module. The ARP request packet says "If your IP address matches this target IP address, then please tell me your Ethernet address". An ARP request packet looks something like this:

Sender IP Address	223.1.2.1
Sender Enet Address	08-00-39-00-2F-C3
Target IP Address	223.1.2.2
Target Enet Address	<blank>

TABLE 2. Example ARP Request

Each ARP module examines the IP address and if the Target IP address matches its own IP address, it sends a response directly to the source Ethernet address. The ARP response packet says "Yes, that target IP address is mine, let me give you my Ethernet address". An ARP response packet has the sender/target field contents swapped as compared to the request. It looks something like this:

Source: https://tools.ietf.org/html/rfc1180#page-2, page 9

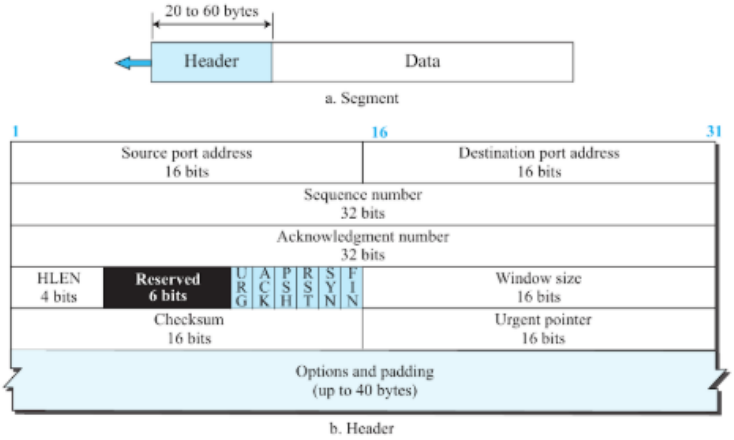


Source: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11n_Series.pdf, page 2

17. Fortinet provides a user data field including a data packet to be transmitted from one client to another client. For example, the network products (including FortiAP Access Points such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc. and FortiGate such as 6000F series) support wireless transport protocol such as TCP/IP. The protocol allows transmission of user data between wired and wireless devices ("client") in the form of TCP segments/data packets.

there are no options and up to 60 bytes if it contains options. We will discuss some of the header fields in this section. The meaning and purpose of these will become clearer as we proceed through the section.

Figure 3.44 *TCP segment format*



Source: https://books.google.co.in/books?id=o8CjAgAAQBAJ&printsec=frontcover&dq=forouzan+computer+networks&hl=en&sa=X&ved=0ahUKEwjV95WPruPhAhVFQo8KHWsUBtsQ6AEIKDAA#v=onepage&q=forouzan%20computer%20networks&f=false, page 186

18. Fortinet provides at least one sequencing field identifying the last packet received by the client that is transmitting a current data packet. For example, the WLAN network products (including FortiAP Access Points such as FAP-U421EV, FAP-U423EV, FAP-S421E, FAP-223E, etc. and FortiGate such as 6000F series) support wireless protocols such as TCP/IP for transmission. Further, TCP/IP uses sequence numbers and acknowledgement numbers for maintaining the sequence of the packets. Initial Sequence Number (ISN) is given to the first byte of the data to reassemble the bytes at the receiver end (wired and/or wireless devices).

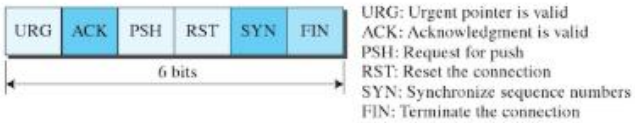
Acknowledgement number ("sequencing field") is the next byte number that the receiver expects to receive which also provides acknowledgement for receiving the previous bytes/packets.

- ***Source port address.*** This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.
- ***Destination port address.*** This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.
- ***Sequence number.*** This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence is the first byte in the segment. During connection establishment (discussed later) each party uses a random number generator to create an **initial sequence number** (ISN), which is usually different in each direction.
- ***Acknowledgment number.*** This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it returns $x + 1$ as the acknowledgment number. Acknowledgment and data can be piggybacked together.
- ***Header length.*** This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field is always between 5 ($5 \times 4 = 20$) and 15 ($15 \times 4 = 60$).

Source:
https://books.google.co.in/books?id=o8CjAgAAQBAJ&printsec=frontcover&dq=forouzan+computer+networks&hl=en&sa=X&ved=0ahUKEwjV95WPruPhAhVFQo8KHWsUBtsQ6AEIKDAA#v=onepage&q=forouzan%20computer%20networks&f=false, page 186

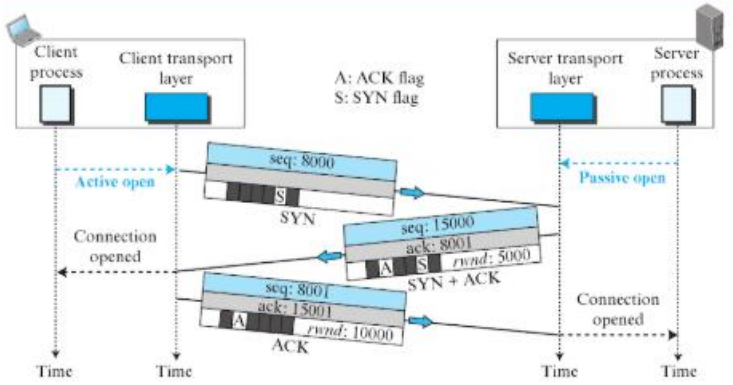
- ***Control.*** This field defines 6 different control bits or flags, as shown in Figure 3.45. One or more of these bits can be set at a time. These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP. A brief description of each bit is shown in the figure. We will discuss them further when we study the detailed operation of TCP later in the chapter.

Figure 3.45 *Control field*



Source:
https://books.google.co.in/books?id=o8CjAgAAQBAJ&printsec=frontcover&dq=forouzan+computer+networks&hl=en&sa=X&ved=0ahUKEwjV95WPruPhAhVFQo8KHWsUBtsQ6AEIKDAA#v=onepage&q=forouzan%20computer%20networks&f=false, page 187

Figure 3.47 *Connection establishment using three-way handshaking*



number, the control flags (only those that are set), and window size if relevant. The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. The client in our example chooses a random number as the first sequence number and sends this number to the server. This sequence number is called the initial sequence number (ISN). Note that this segment does not contain an acknowledgment number. It does not define the window size either; a window size definition makes sense only when a segment includes an acknowledgment. The segment can also include some options that we discuss later in the chapter. Note that the SYN segment is a control segment and carries no data. However, it consumes one sequence number because it needs to be acknowledged. We can say that the SYN segment carries one imaginary byte.

A SYN segment cannot carry data, but it consumes one sequence number.

Source:
https://books.google.co.in/books?id=o8CjAgAAQBAJ&printsec=frontcover&dq=forouzan+computer+networks&hl=en&sa=X&ved=0ahUKEwjV95WPruPhAhVFQo8KHWsUBtsQ6AEIKDAA#v=onepage&q=forouzan%20computer%20networks&f=false, page 189

2. The server sends the second segment, a SYN + ACK segment with two flag bits set as: SYN and ACK. This segment has a dual purpose. First, it is a SYN segment for communication in the other direction. The server uses this segment to initialize a sequence number for numbering the bytes sent from the server to the client. The server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client. Because it contains an acknowledgment, it also needs to define the receive window size, *rwnd* (to be used by the client), as we will see in the flow control section. Since this segment is playing the role of a SYN segment, it needs to be acknowledged. It, therefore, consumes one sequence number.

A SYN + ACK segment cannot carry data, but it does consume one sequence number.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the ACK segment does not consume any sequence numbers if it does not carry data, but some implementations allow this third segment in the connection phase to carry the first chunk of data from the client. In this case, the segment consumes as many sequence numbers as the number of data bytes.

An ACK segment, if carrying no data, consumes no sequence number.

Source: https://books.google.co.in/books?id=o8CjAgAAQBAJ&printsec=frontcover&dq=forouzan+computer+networks&hl=en&sa=X&ved=0ahUKEwjV95WPruPhAhVFQo8KHWsUBtsQ6AEIKDAA#v=onepage&q=forouzan%20computer%20networks&f=false, page 190

19. In the alternative, because the manner of use by Defendant differs in no substantial way from language of the claims, if Defendant is not found to literally infringe, Defendant infringes under the doctrine of equivalents.

20. Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

21. In addition to what is required for pleadings in patent cases, and to the extent any marking was required by 35 U.S.C. § 287, Plaintiff and all predecessors in interest to the '095 Patent complied with all marking requirements under 35 U.S.C. § 287.

22. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of the Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendant has infringed the '813 Patent;

2. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendant's infringement of the '813 Patent as provided under 35 U.S.C. § 284;

3. An award to Plaintiff for enhanced damages resulting from the knowing, deliberate, and willful nature of Defendant's prohibited conduct with notice being made at least as early as the date of the filing of this Complaint, as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully Submitted,

WIRELESS TRANSPORT LLC

/s/ Jimmy Chong

Dated: July 29, 2019 By: _____

Jimmy Chong, Esq
Chong Law Firm, PA
2961 Centerville Rd., Ste 350
Wilmington, DE 19808
Tel. 302-999-9480/Fax 888-796-4627
chong@chonglawfirm.com

Of counsel:
PAPOOL S. CHAUDHARI
Sul Lee Law Firm PLLC
3030 LBJ Fwy, Suite 1130
Dallas, Texas 75234
pchaudhari@sulleelaw.com
Tel. (214) 206-4064/Fax. (214) 206-4068
ATTORNEYS FOR PLAINTIFF
WIRELESS TRANSPORT LLC