IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SOVEREIGN PEAK VENTURES, LLC,	§	
	§	
Plaintiff,	§	
	§	**CASE NO. 2:24-cv-840**
v.	§	
	§	
ZYXEL COMMUNICATIONS CORPORATION and ZYXEL NETWORKS CORPORATION,	§	**JURY TRIAL**
	§	
	§	
	§	
	§	
Defendants.		

COMPLAINT AND JURY DEMAND

Plaintiff Sovereign Peak Ventures, LLC ("SPV") brings this action against Zyxel Communications Corporation and Zyxel Networks Corporation (collectively, "Zyxel") for infringement of U.S. Patent Nos. 7,796,512, 8,045,531, 8,270,384, 8,442,569, 8,467,723, and 8,792,453 and alleges the following:

THE PARTIES

1. Sovereign Peak Ventures, LLC, is a Texas Limited Liability Company with its principal place of business in Allen, Texas.

2. Upon information and belief, both Zyxel Communications and Zyxel Networks are corporations duly organized and existing under the laws of Taiwan, with a place of business located at No. 2, Industry East Rd. IX, Hsinchu Science

Park, Hsinchu, 30076, Taiwan. Zxyel Communications may also be served with process by serving the Texas Secretary of State, 1019 Brazos Street, Austin, Texas 78701, as its agent for service because it engages in business in Texas but has not designated or maintained a resident agent for service of process or a regular place of business in Texas as required by statute. This action arises out of that business.

3. Zyxel and each of their respective foreign and United States subsidiaries, affiliates, and related companies comprise the Zyxel brand under and through which they import, market, sell, and distribute an extensive portfolio of computer networking and communication products.

4. Zyxel and its affiliates, subsidiaries, and related companies are part of the same corporate structure and distribution chain for the making, importing, offering to sell, selling, and using of the accused devices in the United States including in the State of Texas and this judicial district.

5. Zyxel and its affiliates, subsidiaries, and related companies share the same management, common ownership, advertising platforms, facilities, distribution chains and platforms, and product lines, products, and related technologies that infringe SPV's patents.

6. Zyxel and its affiliates, subsidiaries, and related companies regularly contract with customers for provision of products or services by and on behalf of Zyxel and its affiliates, subsidiaries, and related companies.

7. Zyxel and its affiliates, subsidiaries, and related companies operate as a unitary business venture and are jointly and severally liable for the damages caused by infringing SPV's patents as alleged herein.

JURISDICTION AND VENUE

8. SPV brings this action for patent infringement under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

9. Zyxel is subject to this Court's personal jurisdiction pursuant to the Texas Long-Arm Statute and consistent with due process in view of its substantial and ongoing business in Texas and in this judicial district including (a) its infringing activities alleged in this complaint by which Zyxel purposefully avails itself of the privilege of conducting business activities in this state and district, and thus, submits to the jurisdiction of this Court; and (b) regularly doing or soliciting business, contracting with and engaging in other persistent conduct targeting residents of Texas and this district, and deriving substantial revenue from goods and services offered for sale, sold, and imported to and targeting residents of Texas and this district directly and through, or in concert with, intermediaries, agents, distributors, importers, customers, subsidiaries and/or consumers, retail and wholesale outlets, and via Internet sales.

10. Zyxel's presence and conduct directed to residents of Texas and into this district is intended to further and advance the development, design, manufacture, importation, distribution, sale, and use, including use by customers induced by Zyxel, of infringing Zyxel products in Texas and in this district.

11. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(c)(3) which provides that "a defendant not resident in the United States may be sued in any judicial district."

12. Zyxel transacts business in this judicial district and has committed acts of infringement in this judicial district.

13. Zyxel directly or through intermediaries, make, use, offer for sale, import, sell, advertise, or distribute products and services in the United States, the State of Texas, and in this district.

14. Zyxel advertises its products to residents in Texas and in this district via its website: www.zyxel.com.

15. Zyxel conducts its business of marketing, distributing, deploying, and selling products and services in Texas and in this district through its agents, representatives, affiliates, subsidiaries, related entities, partners, distributors, and retailers.

16. Zyxel continuously and systematically solicits business and contracts with residents of Texas and this district.

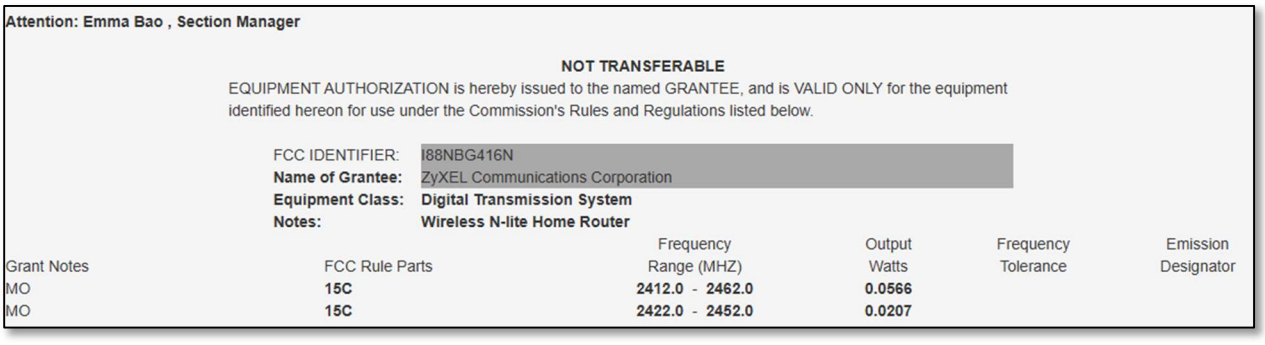
17. By way of example, and as a predicate for access and use, Zyxel requires end users, customers, and subscribers to enter a written contract containing certain terms and conditions governing their access and use of Zyxel's mobile applications including the Zyxel Nebula App, Nebula Control Center, Zyxel MPro Mesh App, and Zyxel Air App.

Zyxel Registers the Infringing Products with the FCC.

18. To sell the infringing products in the United States, Zyxel applied for and obtained registrations from the United States Federal Communications Commission (FCC). *See, e.g.,* https://fcc.report/FCC-ID/I88EE6601-00/.

19. In its application and disclosure to the FCC, Zyxel identified itself as the responsible manufacturing party of infringing products intended for the domestic market and for use by United States residents. *See, e.g.,* https://fcc.report/FCC-ID/I8803935/; https://fcc.report/FCC-ID/I88EE6601-00/.

20. Zyxel identified itself as "Grantee" for a non-transferrable "equipment authorization" from the FCC for the sale of certain Zyxel products in the United States. *See, e.g.,* https://fccid.io/I88NBG416N.



Attention: Emma Bao , Section Manager

NOT TRANSFERABLE

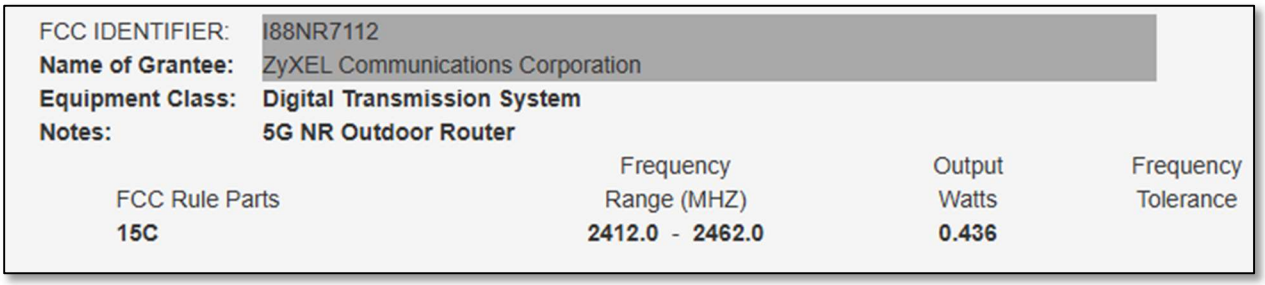
EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: I88NBG416N
Name of Grantee: ZyXEL Communications Corporation
Equipment Class: **Digital Transmission System**
Notes: **Wireless N-lite Home Router**

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
MO	**15C**	**2412.0 - 2462.0**	**0.0566**		
MO	**15C**	**2422.0 - 2452.0**	**0.0207**		

21. Zyxel sought and obtained from the FCC authorization for "equipment for operation at approved frequencies and sale within the USA." *See* FCC Grant of Equipment Authorization Certification for Zyxel, *available at* https://fccid.io/I88NBG416N.

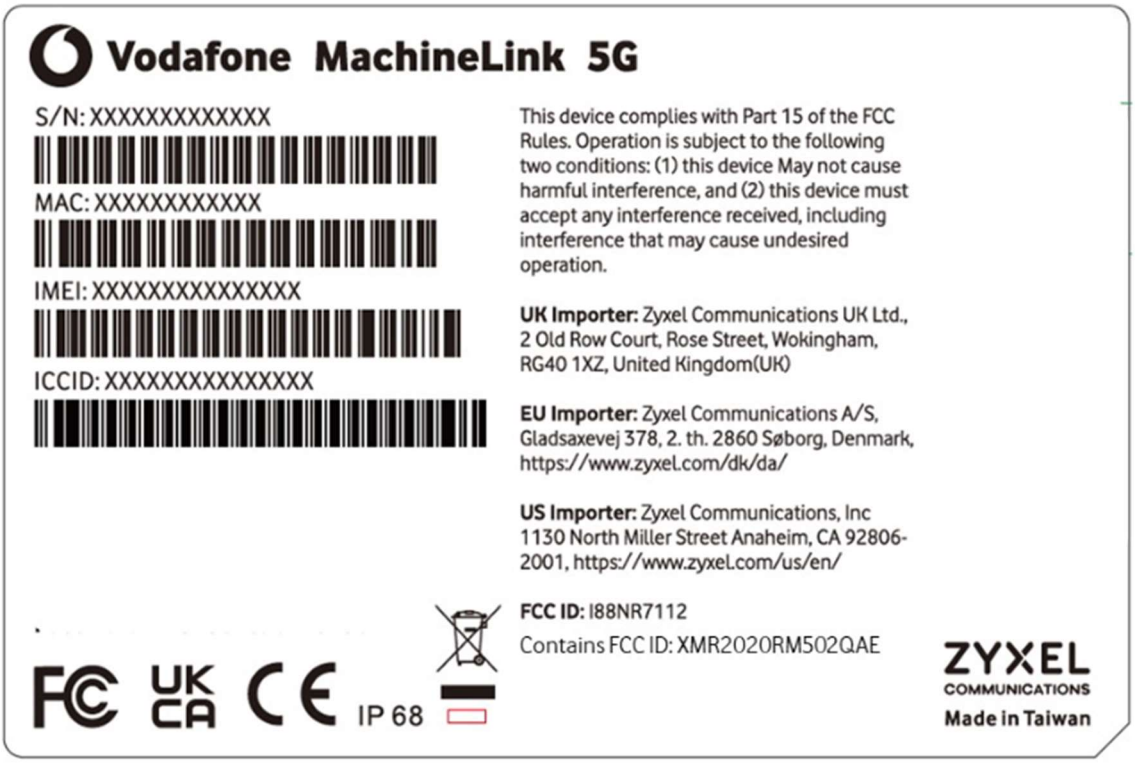
22. Zyxel's FCC product registrations include infringing Zyxel Access Point devices enabled for 802.11k/r: NWA/WAC series (https://fcc.report/FCC-ID/I88NWA5123-ACHD/); NWA/WAC/WAX Series (https://fcc.report/FCC-ID/I8811AXAP246E); NXC2500 (https://fccid.io/ANATEL/01545-15-08311/Manual-NXC-2500/82A9A4C7-8C95-4558-B158-9FC997E4F57B); and 5G NR Outdoor Router (https://fccid.io/I88NR7112).



FCC IDENTIFIER: I88NR7112
Name of Grantee: ZyXEL Communications Corporation
Equipment Class: **Digital Transmission System**
Notes: **5G NR Outdoor Router**

FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance
15C	**2412.0 - 2462.0**	**0.436**	

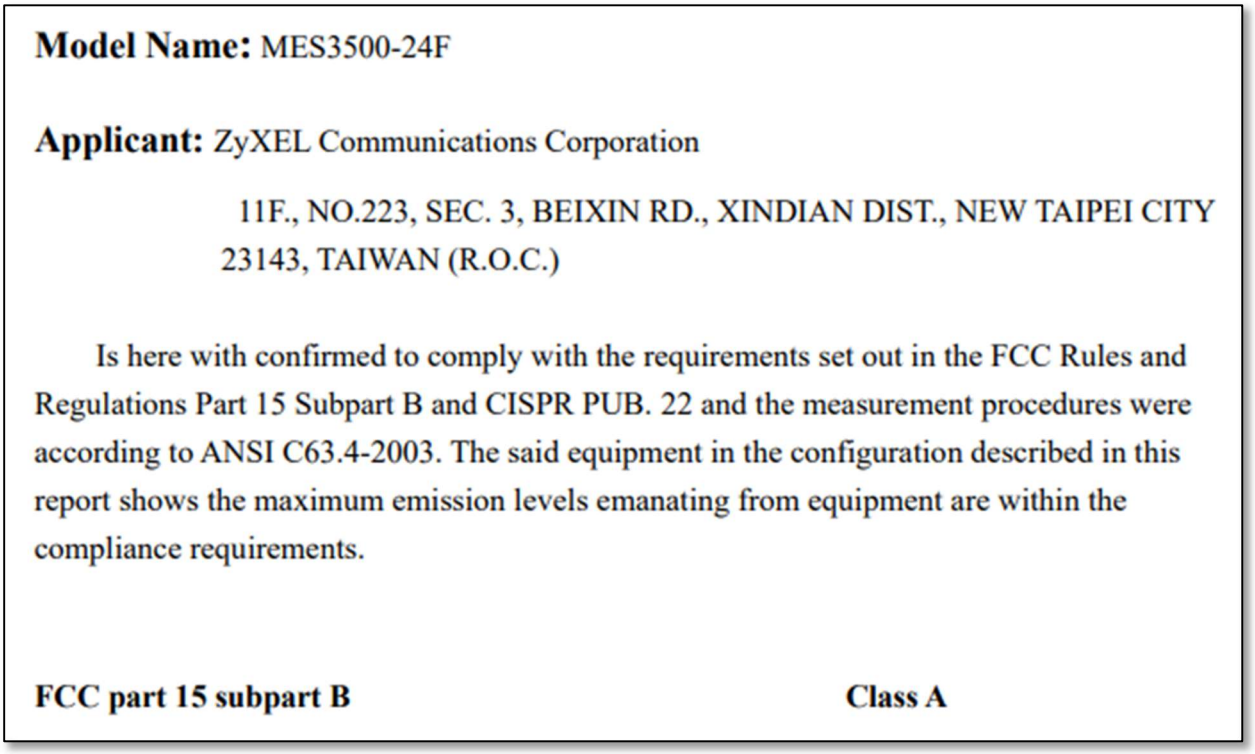
23. Zyxel identified itself on product labels as the importer.



https://fccid.io/I88NR7112/Label/ID-Label-Location-Info-5873511.

https://fcc.report/FCC-ID/I88NWA5123-ACHD/3560687.

24. Zyxel certifies that its products comply with all necessary FCC requirements governing usage in the U.S. *See e.g.*, https://spdl.zyxel.com/MES3500-24F/certification/MES3500-24F_001.351-01-00326.pdf; https://fcc.report/FCC-ID/I88NBG5615/1948302; https://biz.zyxel.com/webinar-08-15-2024.



Model Name: MES3500-24F

Applicant: ZyXEL Communications Corporation

11F., NO.223, SEC. 3, BEIXIN RD., XINDIAN DIST., NEW TAIPEI CITY 23143, TAIWAN (R.O.C.)

Is here with confirmed to comply with the requirements set out in the FCC Rules and Regulations Part 15 Subpart B and CISPR PUB. 22 and the measurement procedures were according to ANSI C63.4-2003. The said equipment in the configuration described in this report shows the maximum emission levels emanating from equipment are within the compliance requirements.

FCC part 15 subpart B **Class A**

https://spdl.zyxel.com/MES3500-24F/certification/MES3500-24F_001.351-01-00326.pdf.

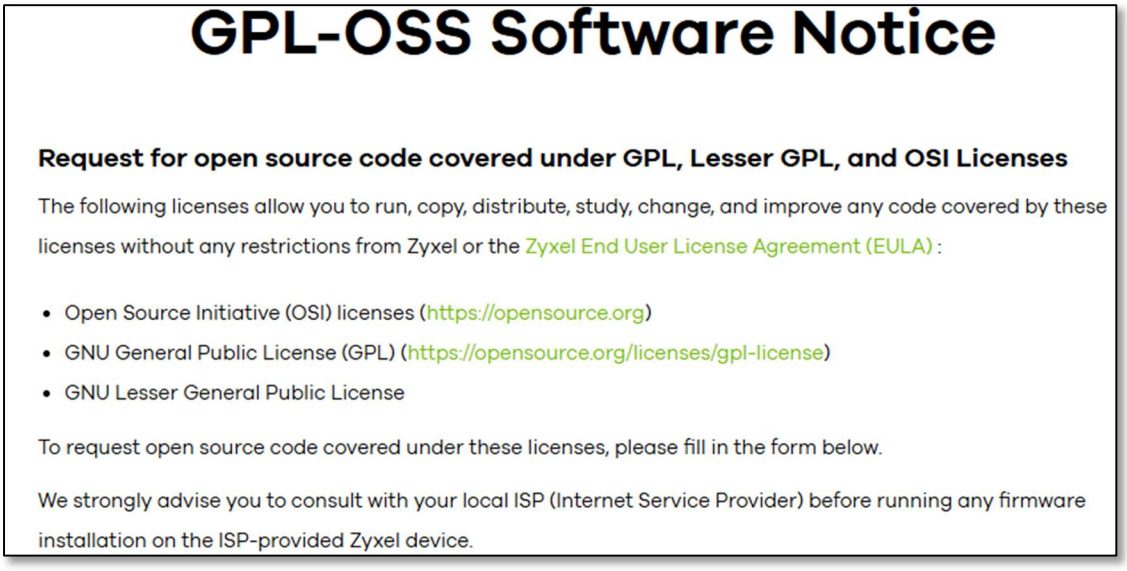
25. Zyxel certifies compliance with FCC requirements in order to sell Zyxel products in the United States.

Zyxel Designs and Packages Products for Sale in the United States.

26. Zyxel includes with the accused products sold in the United States power cords and electrical plugs compatible with United States power outlets. Zyxel knowingly and intentionally directs distribution of infringing products into the United States.

27. Zyxel identifies itself on packaging of infringing products imported and sold in the United States.

28. Zyxel includes written notices to U.S. customers that direct U.S. residents to ask Zyxel about its GNU General Public Licenses.



GPL-OSS Software Notice

Request for open source code covered under GPL, Lesser GPL, and OSI Licenses

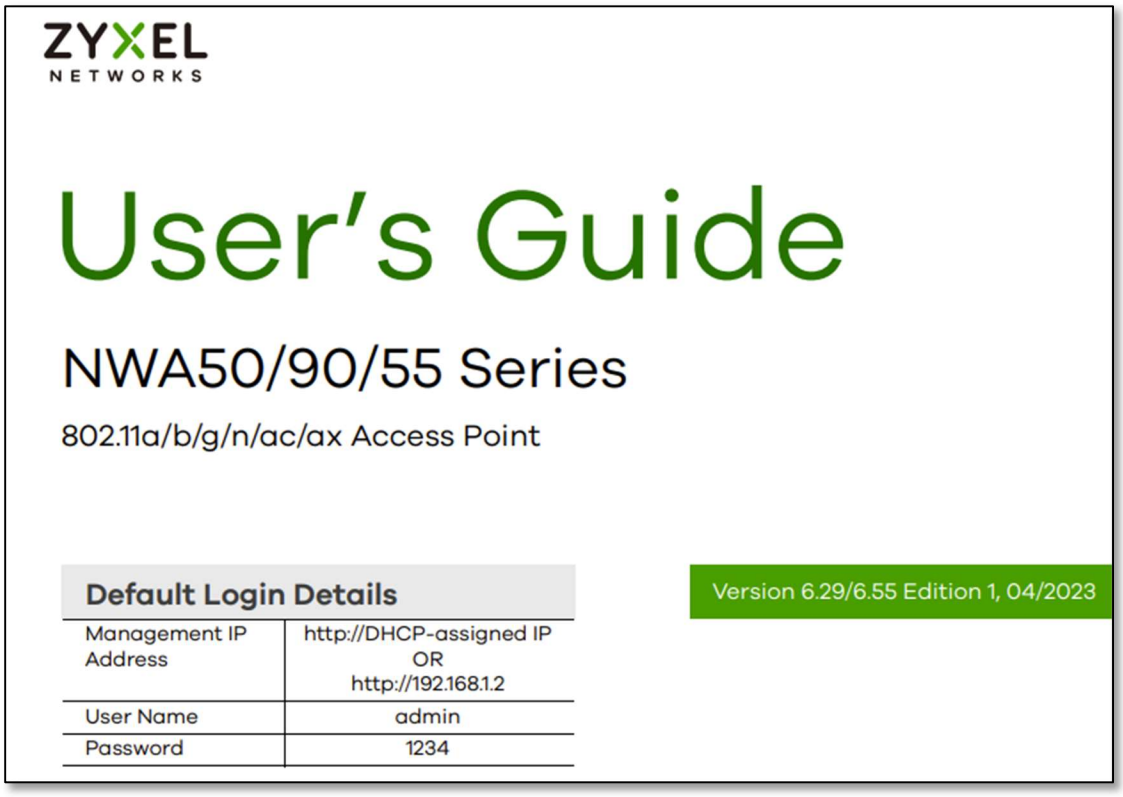
The following licenses allow you to run, copy, distribute, study, change, and improve any code covered by these licenses without any restrictions from Zyxel or the Zyxel End User License Agreement (EULA) :

- Open Source Initiative (OSI) licenses (https://opensource.org)
- GNU General Public License (GPL) (https://opensource.org/licenses/gpl-license)
- GNU Lesser General Public License

To request open source code covered under these licenses, please fill in the form below.

We strongly advise you to consult with your local ISP (Internet Service Provider) before running any firmware installation on the ISP-provided Zyxel device.

29. Zyxel includes English-language product manuals in its products along with the Zyxel logo.



ZYXEL NETWORKS

User's Guide

NWA50/90/55 Series

802.11a/b/g/n/ac/ax Access Point

Default Login Details	
Management IP Address	http://DHCP-assigned IP OR http://192.168.1.2
User Name	admin
Password	1234

Version 6.29/6.55 Edition 1, 04/2023

30. Zyxel purposefully places infringing Zyxel products into established

distribution channels in the stream of commerce destined for Texas via distribution partners, retailers (including national retailers), reseller partners, affiliates, related entities, solution partners, service providers, subsidiaris, consumers, and users.

Zyxel Purposefully Directs Sales Activities to Residents of Texas and this District Through Its Zyxel Website and Sales Channels.

31. Zyxel operates the www.Zyxel.com website, which provides United States customers with sales and product information, including referring links and directions on how to purchase Zyxel products in the United States, in Texas, and in this district.

32. Zyxel holds U.S. copyright registrations corresponding to Zyxel's websites. *See* https://www.zyxel.com/us/en-us/home; https://www.Zyxel.com/us/where-to-buy/; https://www.zyxel.com/us/en-us/where-to-buy/retail-stores and https://www.zyxel.com/us/en-us/products/wireless

33. Zyxel controls the content of its website, gathers consumer information through it, and controls how such information is utilized. For example, Zyxel and its affiliates are listed as the responsible parties on the Zyxel privacy policy. *See* https://www.zyxel.com/us/en-us/privacy-policy.

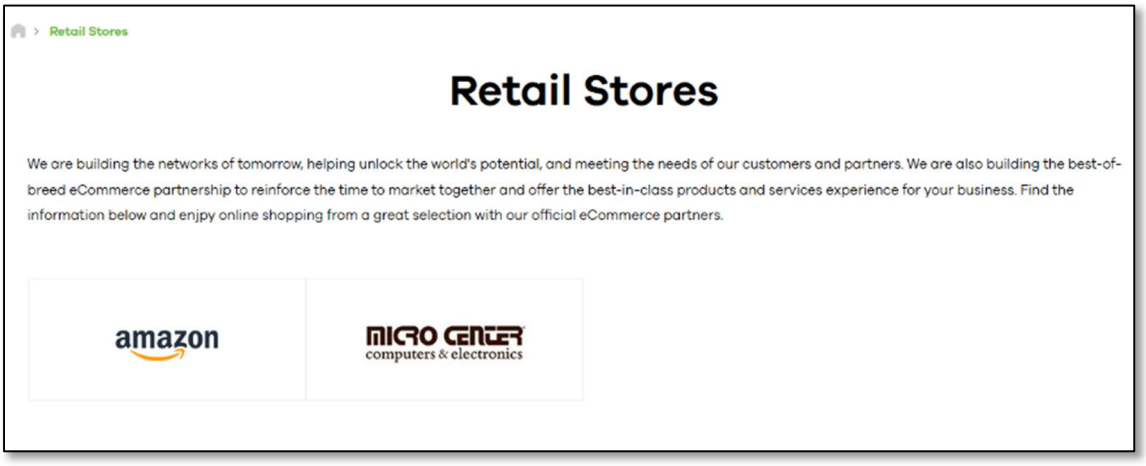
34. Zyxel represents on its website that its Data Protection Representative

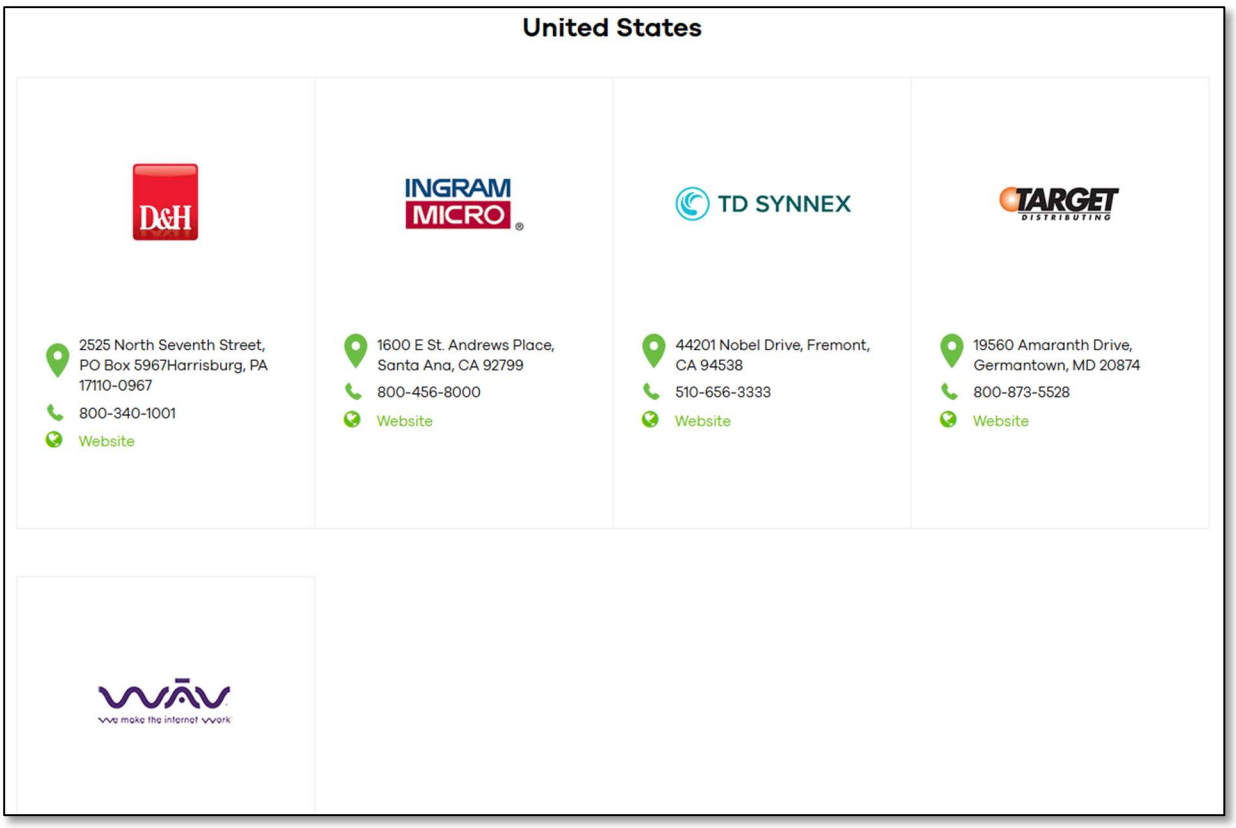
may be reached by U.S. customers by contacting "Zyxel Communications Corp. at No. 2, Industrial East 9th Road, Hsinchu Science Park, Hsinchu City 30076, Taiwan (R.O.C.) or privacy@zyxel.com.tw."

35. Zyxel provides specifications, user manuals, installation videos, and other technical support documents for certain referenced products on its website. *See* https://www.zyxel.com/us/en-us/support.

36. Zyxel ships products (including the accused products) to its affiliate Zyxel USA. Accused Zyxel products are currently sold at major retailers in Texas and in this district including Target and Home Depot stores.

37. Zyxel's website directs customers to purchase accused products from its website (i.e., "Where to Buy") and through its store, online stores, distribution partners, retailers, reseller partners and solution partners. For example, Zyxel lists and includes referring links to retailers that sell Zyxel products in this district including Amazon and Micro Center Computers & Electronics.





38. Zyxel sells its products in the United States and to residents in Texas and this district through the Online Stores, Distribution Partners, Retailers, and Reseller Partners.

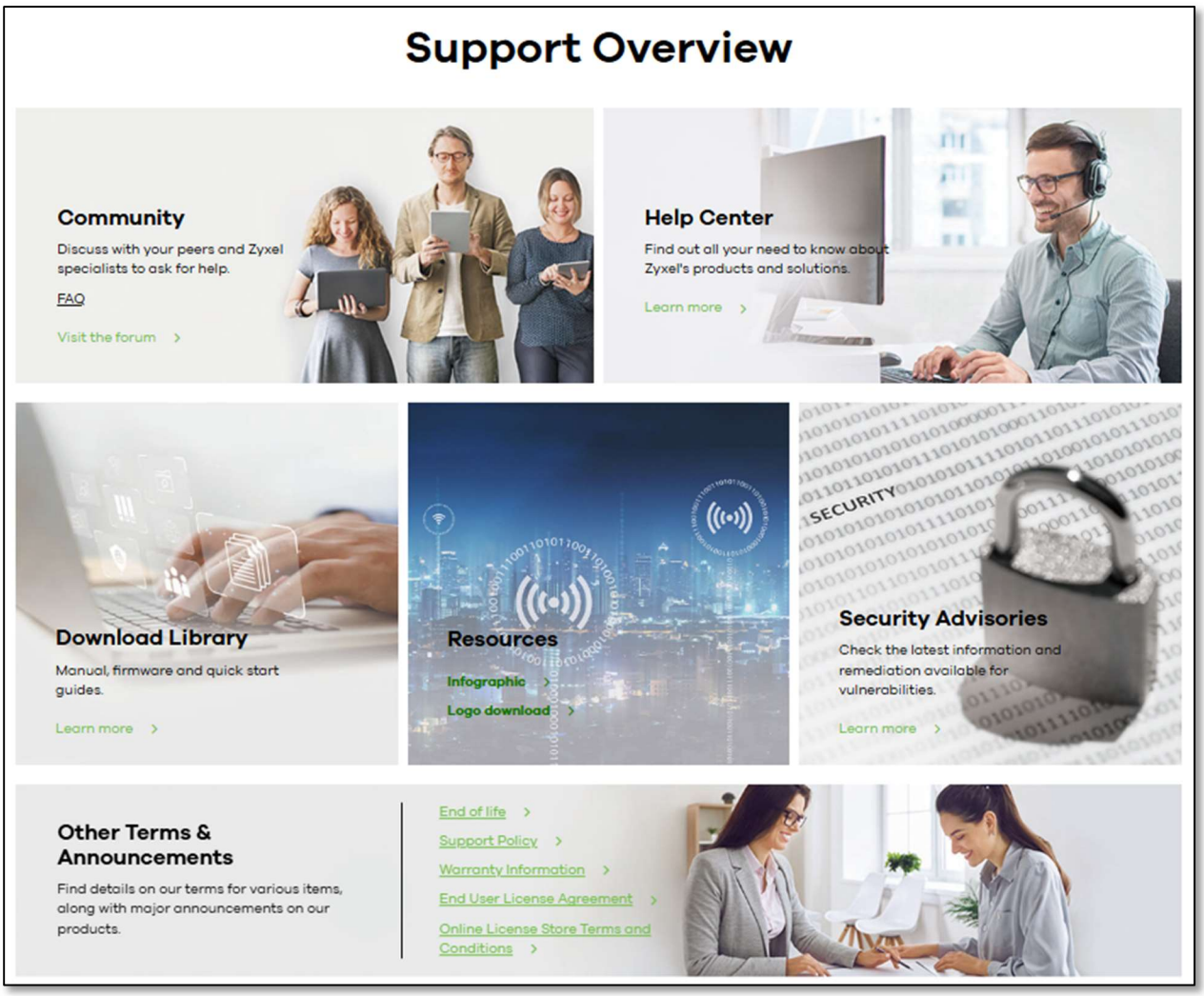
39. Through its website, Zyxel provides weblinks to distributors (i.e., referring links) and directs consumers where to purchase Zyxel products (including the Accused Products). *See* https://www.zyxel.com/us/en-us/where-to-buy/distributors.

40. Zyxel has sold and continues to sell infringing Zyxel products (e.g., NWA Series Access Points) to customers in Texas and in this district.

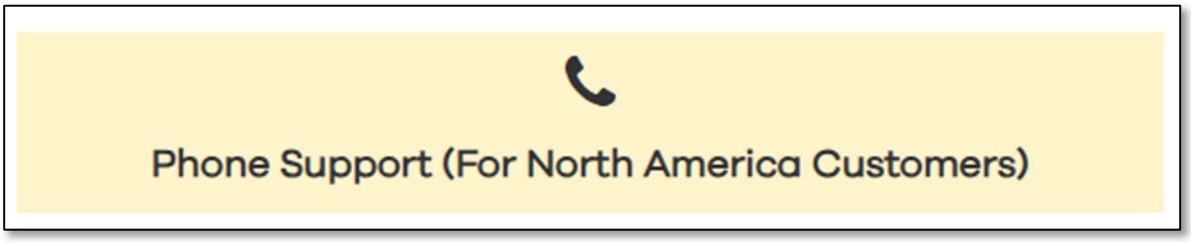
Zyxel Maintains Established Channels for Providing Pre- and Post-Sale Advice to Customers in Texas.

41. Zyxel provides technical support to users of its products (including applications) in Texas through its website, available at https://www.zyxel.com/us/en-us.

42. Zyxel provides technical support to its customers on its website through its download center, community, help center, resources, security advisories, and other terms & announcement tabs.



43. Zyxel provides contact information for users in Texas to access Technical Support for their home and business products.



https://mysupport.zyxel.com/hc/en-us/requests/new.

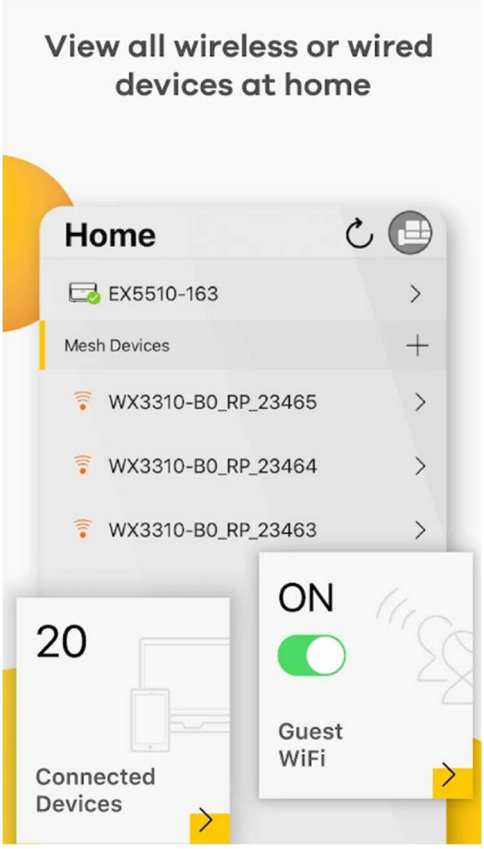
Zyxel Markets and Distributes Mobile Applications to Texas Residents.

44. Zyxel makes, distributes, develops, and operates application software, such as the Zyxel-branded MPro Mesh app and Zyxel Air, making them available to residents of Texas and this district for download and use in connection with Zyxel products including Wi-Fi routers and home network management devices.

45. The Zyxel applications are available via digital distribution platforms operated by Apple and Google.

46. Zyxel directs customers in the United States, in Texas, and in this district to download its applications for use with infringing Zyxel products.

47. Zyxel instructs customers in Texas and in this district to use the Zyxel applications with Zyxel products.



NR7301/NR7302/NR7303 SERIES

5G NR Outdoor Router

The Zyxel 5G NR Outdoor Router - NR7301/NR7302/NR7303 Series delivers exceptional performance for both subscribers and service providers. With ultra-high speeds, large capacity, low latency, and truly dependable coverage, the Series boasts unmatched performance and provides an outstanding user experience. Thanks to our in-house app and installation kit, you can also reduce deployment and service call costs with our purpose-built Series, which is easy to set up and manage.

- 5G NR, Sub-6 GHz
- NSA & SA modes
- 4x4 MIMO 4G/5G antennas
- Remote management
- 802.3af/at 2.5G PoE
- Self-installation
- IP67-certified
- Zyxel mobile app
- FOTA

48. Zyxel provides instructions to customers in the United States, in Texas, and in this district directing them to manage their Zyxel devices (e.g., the 5G NR Outdoor Router) via the Zyxel Air App.

1.3 How to Manage your Zyxel Device

You can use the following way to manage your Zyxel Device.

• Web Configurator. This is recommended for everyday management of Zyxel Device using a (supported) web browser.

• Zyxel Air app. The Zyxel Air app is available on App Store for Apple devices and Google Play for Android devices. Use the Zyxel Air app for setup and management of the Zyxel Device on your smartphone. You can also use the app for finding the optimal 5G NR signal strength. See the Zyxel Air app QSG for more information. To install the app, scan the QR code on the QSG.

https://spdl.zyxel.com/NR7302/user_guide/NR7302_NR%20Outdoor%20OPAL-Series_UG_V1.00_Ed5_2023-09-25.pdf.

49. Zyxel promotes the management of infringing devices using the Zyxel Air app products in the United States, in Texas, and in this district. *See* https://spdl.zyxel.com/NR7302/user_guide/NR7302_NR%20Outdoor%20OPAL-Series_UG_V1.00_Ed5_2023-09-25.pdf.

Zyxel Configures Products for Operation in the United States.

50. Zyxel configures its products for operation in the United States.

51. To sell infringing products in the United States, Zyxel certifies to the FCC that the accused products only operate on permitted channels one through eleven. https://fcc.report/FCC-ID/I88NBG7510/5823598.pdf.

Zyxel Communications Corporation

Attestation Letter

Federal Communications Commission

Authorization and Evaluation Division

We
Name: **Zyxel Communications Corporation**
Address: **No.2, Industry East Road IX, Science Park Hsinchu,Taiwan**

Declare that the device does not support channel 12 ~ 13 in 2.4GHz band and any non-US channels in all the operational mode(s) for the following product.

Product:	**AX1800 Dual-Band WiFi 6 Router**
FCC ID:	**I88NBG7510**
Model No.:	**NBG7510**

Sincerely,

Name: **Emma Bao**
Title: Manager
Email: Emma.bao@zyxel.com.tw
Date: **2022/04/12**

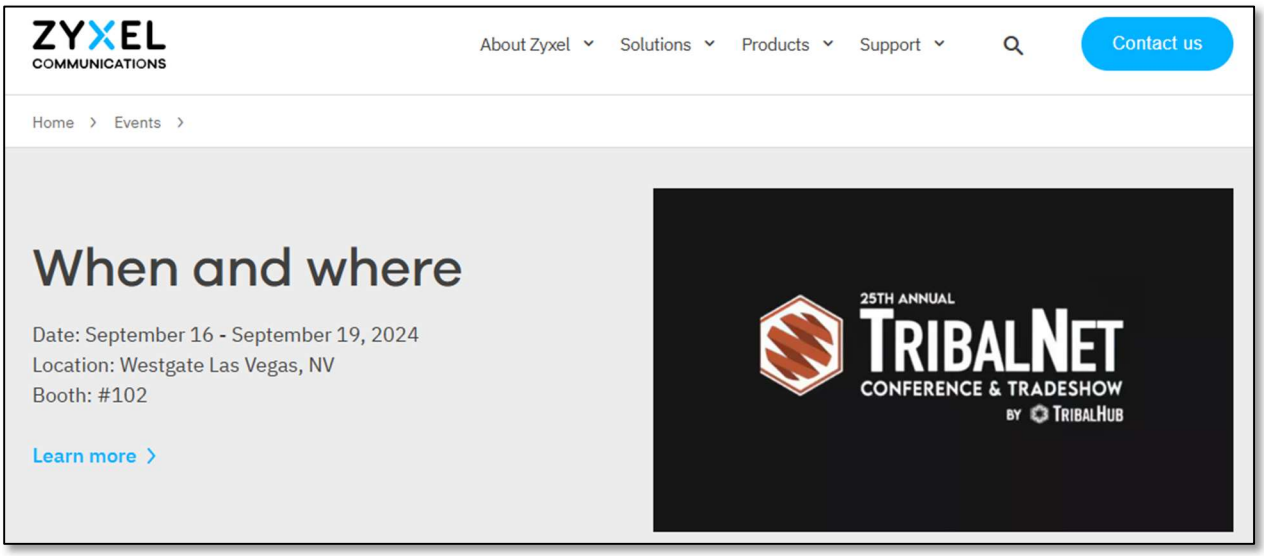
Zyxel Advertises and Offers to Sell Infringing Products to Residents of Texas.

52. Zyxel markets its products to U.S. consumers through its website. *See* https://www.zyxel.com/us/en-us/home.

53. Zyxel markets infringing products to consumers in the United States

through social media.

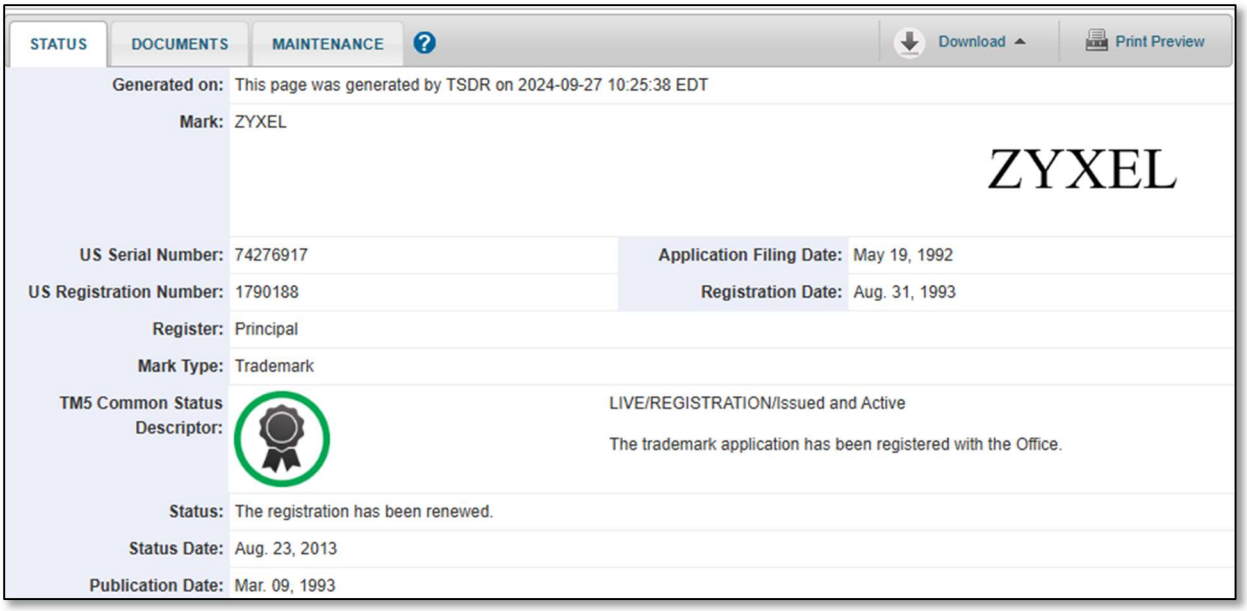
54. Zyxel markets its products to consumers in the United States at conferences and tradeshows. *See* https://www.zyxel.com/us/en-us/newsroom/events.



https://www.zyxel.com/service-provider/na/en/events/tribalnet-conference-tradeshow-2024.

Zyxel Registered U.S. Trademarks for Use in Selling Infringing Products.

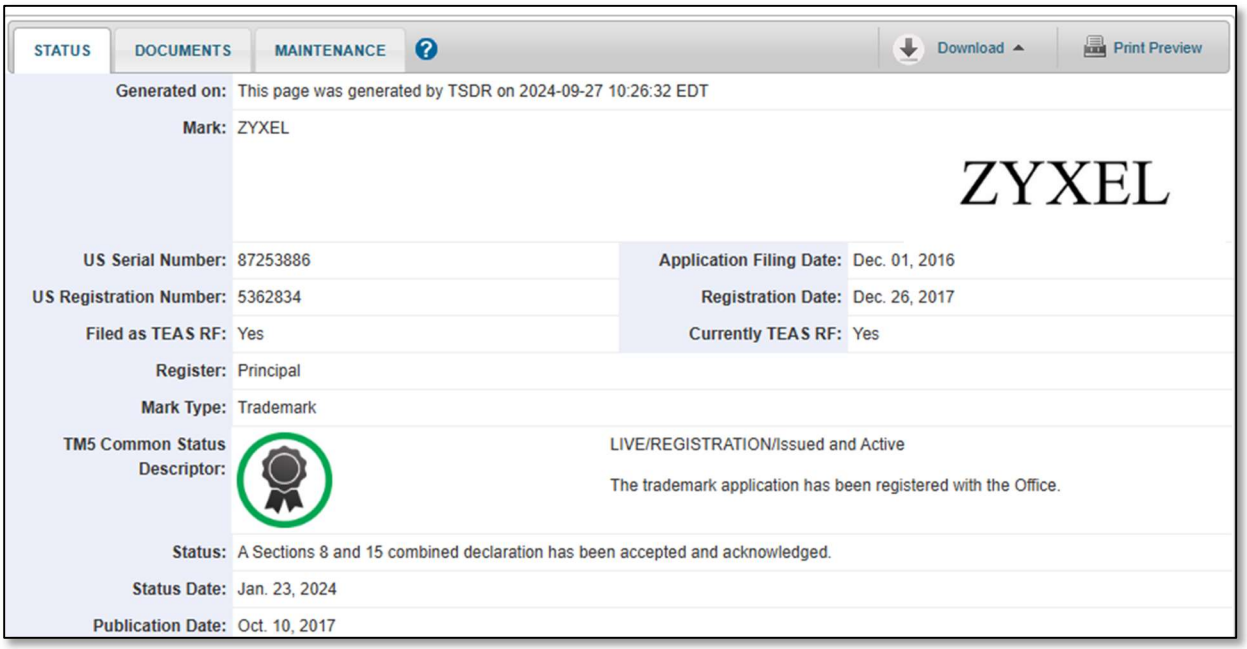
55. Zyxel has registered trademarks in the United States, including trademarks used with the accused products (e.g., Zyxel Nebula) and identifies itself as the owner of the marks.



STATUS | DOCUMENTS | MAINTENANCE | Download | Print Preview

Generated on:	This page was generated by TSDR on 2024-09-27 10:25:38 EDT
Mark:	ZYXEL
	ZYXEL
US Serial Number:	74276917
Application Filing Date:	May 19, 1992
US Registration Number:	1790188
Registration Date:	Aug. 31, 1993
Register:	Principal
Mark Type:	Trademark
TM5 Common Status Descriptor:	LIVE/REGISTRATION/Issued and Active The trademark application has been registered with the Office.
Status:	The registration has been renewed.
Status Date:	Aug. 23, 2013
Publication Date:	Mar. 09, 1993

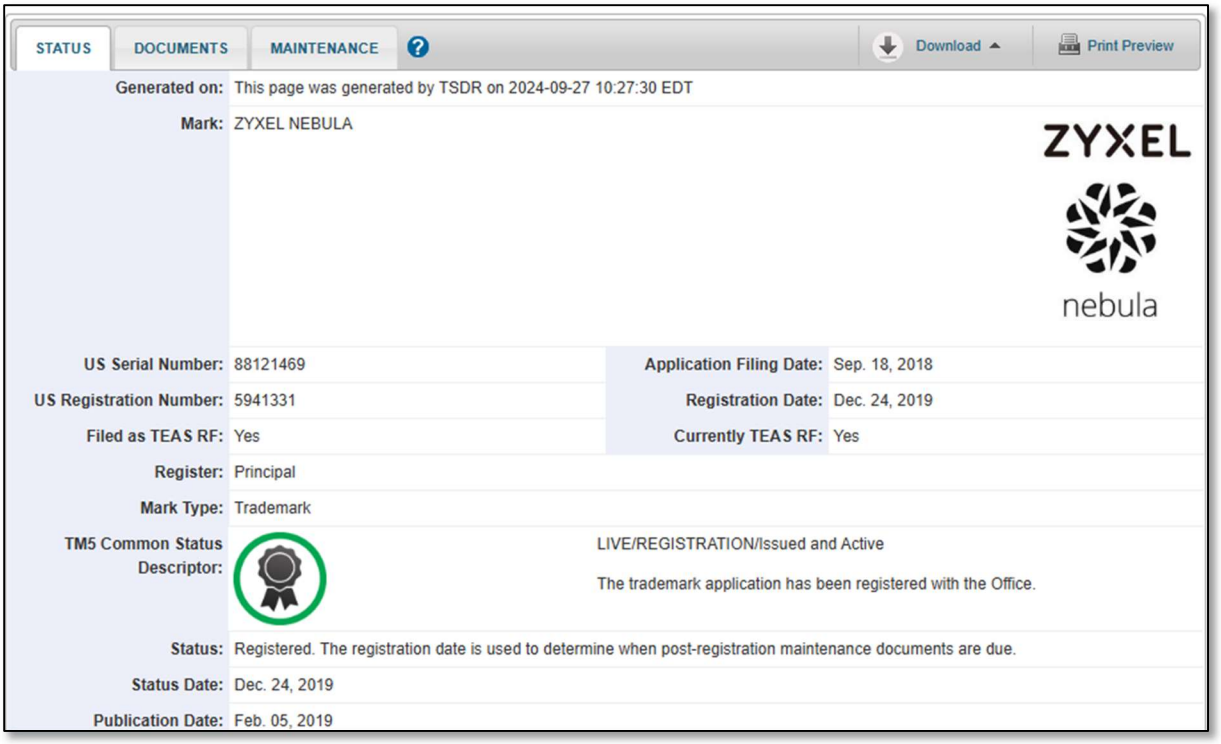
https://tsdr.uspto.gov/#caseNumber=74276917



STATUS | DOCUMENTS | MAINTENANCE | Download | Print Preview

Generated on:	This page was generated by TSDR on 2024-09-27 10:26:32 EDT
Mark:	ZYXEL
	ZYXEL
US Serial Number:	87253886
Application Filing Date:	Dec. 01, 2016
US Registration Number:	5362834
Registration Date:	Dec. 26, 2017
Filed as TEAS RF:	Yes
Currently TEAS RF:	Yes
Register:	Principal
Mark Type:	Trademark
TM5 Common Status Descriptor:	LIVE/REGISTRATION/Issued and Active The trademark application has been registered with the Office.
Status:	A Sections 8 and 15 combined declaration has been accepted and acknowledged.
Status Date:	Jan. 23, 2024
Publication Date:	Oct. 10, 2017

https://tsdr.uspto.gov/#caseNumber=87253886



STATUS | DOCUMENTS | MAINTENANCE | Download | Print Preview

Generated on:	This page was generated by TSDR on 2024-09-27 10:27:30 EDT
Mark:	ZYXEL NEBULA
US Serial Number:	88121469
Application Filing Date:	Sep. 18, 2018
US Registration Number:	5941331
Registration Date:	Dec. 24, 2019
Filed as TEAS RF:	Yes
Currently TEAS RF:	Yes
Register:	Principal
Mark Type:	Trademark
TM5 Common Status Descriptor:	LIVE/REGISTRATION/Issued and Active The trademark application has been registered with the Office.
Status:	Registered. The registration date is used to determine when post-registration maintenance documents are due.
Status Date:	Dec. 24, 2019
Publication Date:	Feb. 05, 2019

https://tsdr.uspto.gov/#caseNumber=88121469

56. Zyxel represented to the Patent and Trademark Office that it uses its marks in commerce in the United States.

Zyxel's Activities Directed into Texas and this District Give Rise to SPV's Claims.

57. SPV's claims for infringement arise out of and relate to Zyxel's activities in Texas and this district.

58. Zyxel's websites, mobile applications, affiliates, related entities, distributors, and retailers (including retailer physical stores) comprise Zyxel's intertwined omnichannel sales strategy for the sale of Zyxel products in the United States, in Texas, and in this district.

59. Through the Zyxel website, mobile applications, retailers, and distributors, Zyxel intends to serve Texas residents and sells to consumers in Texas and in this district.

60. Zyxel's marketing and sales strategy is intentional and designed to increase sales of Zyxel products (including products accused of infringement) in Texas and in this district.

61. Zyxel does not limit distribution of its products or services to exclude Texas residents. Nor has Zyxel changed or sought to change the functionality of its products and applications to operate in a non-infringing way in Texas or this district.

62. Zyxel has taken no action to limit its advertisement or sales in Texas. Zyxel has not refused to sell or ship its products to Texas customers or blocked access to Zyxel applications for Texas customers.

63. Zyxel, alone and in concert with its affiliates, distributors, retailers, and related entities, has purposefully directed its activities at Texas and reasonably anticipates being named as a defendant in this Court on this basis.

64. This Court has personal jurisdiction over Zyxel, directly and/or through the activities of Zyxel's intermediaries, affiliates, distributors, retailers, importers, and related entities. Through its own conduct and through direction and control of these entities, Zyxel has committed acts of direct and/or indirect patent

infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Zyxel would not offend traditional notions of fair play and substantial justice.

Zyxel is Subject to Personal Jurisdiction in this Court Under Rule 4(k)(2).

65. In the alternative, the Court has personal jurisdiction over Zyxel under Federal Rule of Civil Procedure 4(k)(2) because the claims for patent infringement in this action arise under federal law; Zyxel is not subject to the jurisdiction of the courts of general jurisdiction of any state; and exercising jurisdiction over Zyxel comports with due process under the U.S. Constitution.

66. Zyxel is subject to personal jurisdiction in this Court in view of its activities including through intermediaries, agents, related entities, affiliates, distributors, importers, customers, subsidiaries, and/or consumers. Alone and in concert with these entities, Zyxel has sufficient contacts do satisfy due process and has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action.

THE SOVEREIGN PEAK VENTURES PATENTS AND HOW ZYXEL INFRINGES THEM

67. SPV owns a portfolio of patents invented by employees of Panasonic Corporation. Since its founding in 1918, Panasonic has been at the forefront of the electronics industry for over a century. Since acquiring the Panasonic portfolio, SPV has promoted adoption of technologies claimed in the Panasonic portfolio and has entered into license agreements with numerous companies.

68. Over the years, Panasonic has innovated in the home appliance, battery, mobile phone, and television industries. Panasonic's invention of the "Paper Battery" in 1979 is widely credited as enabling the compact electronics of today. In 1991, Panasonic released the Mova P, the smallest and lightest mobile phone on the market, which revolutionized the industry by demonstrating the public's demand for a compact, lightweight device. Panasonic also produced the first wide-format plasma display and developed the first digital television for the U.S. market.

69. Panasonic's history of innovation is borne out by its intellectual property. Searching the Patent Office's database for Panasonic as patent assignee yields more than 27,000 matches.

70. Marking its centennial in 2018, Panasonic opened the Panasonic Museum to showcase its history of design philosophy and innovation.

ZYXEL INFRINGES U.S. PATENT NO. 7,796,512.

71. The Patent Office issued U.S. Patent No. 7,796,512, titled "Switching Source Device, Switching Destination Device, High Speed Device Switching System, and Signaling Method," on September 14, 2010, after a thorough examination and determination that the subject matter claimed is patentable.

72. Zyxel Accused Products with respect to the '512 patent include numerous models of Zyxel Business line APs enabled for 802.11k/r. By way of example, specific Zyxel Accused products include:

- 802.11ac Dual-Radio Ceiling Mount PoE Access Point
- 8012.11ac Wave 2 Dual-Radio Ceiling Mount PoE Access Point

- 802.11ac Dual-Radio Dual Mount PoE Access Point
- 802.11ac Wave 2 Dual-Radio Dual Mount PoE Access Point
- 802.ax (WiFi 6) Dual-Radio PoE Access Point
- 802.11ac Unified Wall Plate Access Point
- 802.11ac Unified Dual Radio Access Point
- 802.11ac Dual-Radio Unified Access Point
- 802.11ac Wave 2 Unified Wall Plate Access Point

Model	UniFi AP 5000 series		UniFi AP 6000 series		
	NWA5120 series		WAC6100 Series	WiFi 6	WAC6300 Series
	WAC5302D-S	WAC5302D-Sv2	WAC6103D-I	WAX610D	WAC6303D-S
Product Name	802.11ac Unified Wall Platel Access Point	802.11ac Unified Wall Platel Access Point	802.11 a/b/g/n/ac Dual-Radio Business Access Point	802.11ax (WiFi 6) Dual-Radio Unified Access Poin	802.11ac Wave 2 Dual-Radio Unified Pro Access Point
Fast Roaming (802.11r, k, v)	•	Yes	•	Yes	•

Model	UniFi AP 6000 series				
	WAC6500 sereis		WiFi 6	WAC6550 series	
	WAC6503D-S	WAC6502D-S	WAX650S	WAC6553D-E	WAC6552D-S
Product Name	802.11 a/b/g/n/ac Dual-Radio Business Access Point	802.11 a/b/g/n/ac Dual-Radio Business Access Point	802.11ax (WiFi 6) Dual-Radio Business Access Point	802.11 a/b/g/n/ac Dual-Radio Business Access Point	802.11 a/b/g/n/ac Dual-Radio Business Access Point
Fast Roaming (802.11r, k, v)	•	•	Yes	•	•

Model	Nebula Cloud Managed Access Points			
	NAP102	NAP203	NAP303	NAP353
Product description	802.11ac Dual-Radio Nebula Cloud Managed Access Point	802.11ac Dual-Radio, Dual-Optimized Antenna 3x3 Nebula Cloud Managed Access Point	802.11ac Dual-Radio Smart Antenna 3x3 Nebula Cloud Managed Access Point	802.11ac Dual-Radio External Antenna 3x3 Outdoor Nebula Cloud Managed Access Point
Fast roaming	Pre-authentication, PMK caching and 802.11r/k/v	Pre-authentication, PMK caching and 802.11r/k/v	Pre-authentication, PMK caching and 802.11r/k/v	Pre-authentication, PMK caching and 802.11r/k/v

73. The Accused Zyxel APs are switching source devices that assist connected clients with roaming to a switching destination device (a destination AP).

74. The Accused Zyxel APs support 802.11k/r (sometimes indicated as "fast roaming"):

75. Zyxel Accused APs supporting 802.11k/r operate as switching source devices for moving a session with connected clients to switching destination devices or APs.

4.3.11.10 Neighbor report

The neighbor report request is sent to an AP, which returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition. Neighbor reports contain information from dot11RMNeighborReportTable concerning neighbor APs. This request/report pair enables a STA to gain information about the neighbors of the associated AP to be used as potential roaming candidates.

76. Zyxel Accused APs include a service discovery section for obtaining information used to compile a neighbor report:

11.11.10 Usage of the neighbor report

11.11.10.1 General

A neighbor report is sent by an AP and it contains information on neighboring APs that are members of ESSs requested in the neighbor report request. A neighbor report might not be exhaustive either by choice, or due to the fact that there might be neighbor APs not known to the AP. The neighbor report contents are derived from the NeighborListSet parameter of the MLME-NEIGHBORREPRESP.request primitive. The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.

The BSSID Information field can be used to help determine neighbor service set transition candidates. It is 4 octets in length and contains the subfields as shown in Figure 9-296.

B0 B1	B2	B3	B4 B9	B10	B11	B12	B13	B14 B31
AP Reachability	Security	Key Scope	Capabilities	Mobility Domain	High Throughput	Very High Throughput	FTM	Reserved
Bits: 2	1	1	6	1	1	1	1	18

Figure 9-296—BSSID Information field

The AP Reachability field indicates whether the AP identified by this BSSID is reachable by the STA that requested the neighbor report. For example, the AP identified by this BSSID is reachable for the exchange of preauthentication frames as described in 12.6.10.2. The values are shown in Table 9-150.

B4	B5	B6	B7	B8	B9
Spectrum Management	QoS	APSD	Radio Measurement	Delayed Block Ack	Immediate Block Ack
Bits: 1	1	1	1	1	1

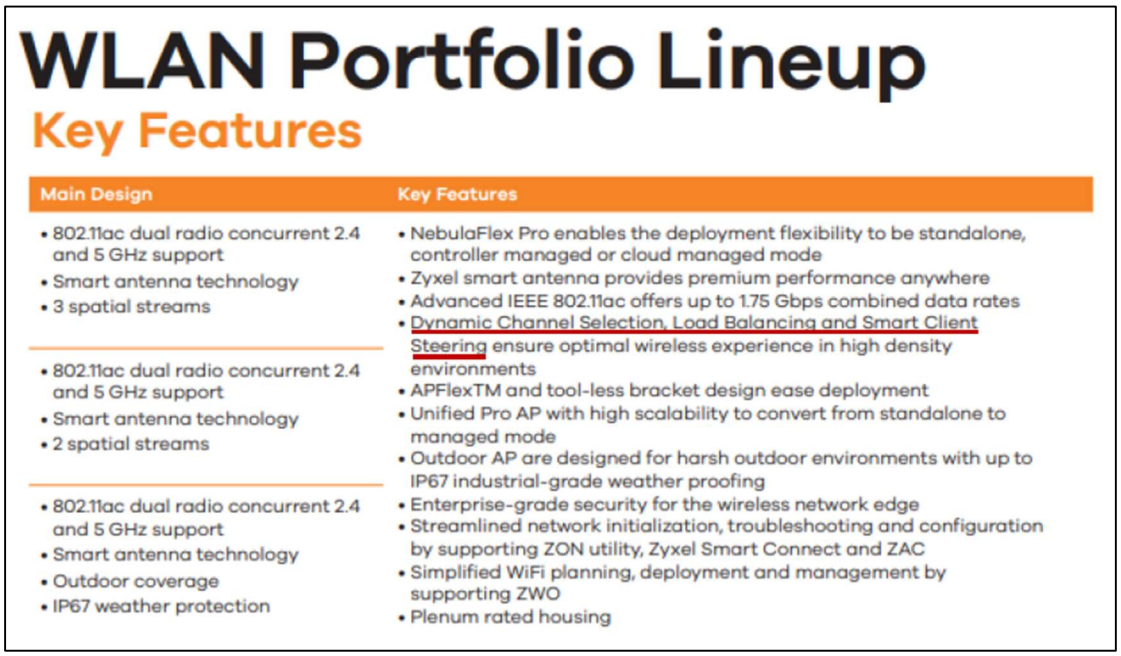
Figure 9-297—Capabilities subfield

The Mobility Domain bit is set to 1 to indicate that the AP represented by this BSSID is including an MDE in its Beacon frames and that the contents of that MDE are identical to the MDE advertised by the AP sending the report.

The High Throughput bit is set to 1 to indicate that the AP represented by this BSSID is an HT AP including the HT Capabilities element in its Beacons, and that the contents of that HT Capabilities element are identical to the HT Capabilities element advertised by the AP sending the report.

The Very High Throughput bit is set to 1 to indicate that the AP represented by this BSSID is a VHT AP and that the VHT Capabilities element, if included as a subelement in the report, is identical in content to the VHT Capabilities element included in the AP's Beacon.

77. Accused Zyxel APs include a service discovery section for obtaining information about neighboring communication devices from measurement reports or background scans. For example, Zyxel APs perform load balancing and band steering operations among clients and other APs:



WLAN Portfolio Lineup

Key Features

Main Design	Key Features
• 802.11ac dual radio concurrent 2.4 and 5 GHz support • Smart antenna technology • 3 spatial streams	• NebulaFlex Pro enables the deployment flexibility to be standalone, controller managed or cloud managed mode • Zyxel smart antenna provides premium performance anywhere • Advanced IEEE 802.11ac offers up to 1.75 Gbps combined data rates • Dynamic Channel Selection, Load Balancing and Smart Client Steering ensure optimal wireless experience in high density environments • APFlexTM and tool-less bracket design ease deployment • Unified Pro AP with high scalability to convert from standalone to managed mode • Outdoor AP are designed for harsh outdoor environments with up to IP67 industrial-grade weather proofing • Enterprise-grade security for the wireless network edge • Streamlined network initialization, troubleshooting and configuration by supporting ZON utility, Zyxel Smart Connect and ZAC • Simplified WiFi planning, deployment and management by supporting ZWO • Plenum rated housing
• 802.11ac dual radio concurrent 2.4 and 5 GHz support • Smart antenna technology • 2 spatial streams	
• 802.11ac dual radio concurrent 2.4 and 5 GHz support • Smart antenna technology • Outdoor coverage • IP67 weather protection	

https://www.zyxel.com/library/assets/tech library/Quick Sales Guide/SMB WLAN.pdf.

78. Zyxel Accused APs instruct their respective service discovery sections to inquire whether a service can be provided by requesting beacon reports from connected clients at arbitrary times:

11.11.9 Specific measurement usage

11.11.9.1 Beacon report

If a STA accepts a Beacon request it shall respond with a Radio Measurement Report frame containing Beacon reports for all observed BSSs matching the BSSID and SSID in the Beacon request, at the level of detail requested in the Reporting Detail. If the Reporting Detail is 1 and the optional Request subelement is

The BSSID is the BSSID of the BSS being reported. The subsequent fields in the Neighbor Report element pertain to this BSS.

The BSSID Information field can be used to help determine neighbor service set transition candidates. It is 4 octets in length and contains the subfields as shown in Figure 9-296.

B0 B1	B2	B3	B4 B9	B10	B11	B12	B13	B14 B31
AP Reachability	Security	Key Scope	Capabilities	Mobility Domain	High Throughput	Very High Throughput	FTM	Reserved
Bits: 2	1	1	6	1	1	1	1	18

Figure 9-296—BSSID Information field

79. Zyxel Accused APs determine switching destination candidate APs using information obtained by the service discovery sections. The determination may be made based upon the BSSID of a known AP or information relating to settings and capabilities of an AP.

80. The Accused Zyxel APs generate a switching destination candidate device list (e.g., a neighbor list) describing the switching destination candidate APs:

The following MLME primitives support the signaling of neighbor report responses.

6.3.33.2 MLME-NEIGHBORREPRESP.request

Name	Type	Valid range	Description
NeighborListSet	Set of Neighbor List elements each as defined in the Neighbor Report element format	As defined in 9.4.2.37	A set of Neighbor List elements, each representing a neighboring AP being reported as defined in the Neighbor Report element format.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

81. The Neighbor Report element for each neighbor contains the AP BSSID, which the Accused Zyxel APs use to establish a Fast Transition session with that AP:

Element ID	Length	BSSID	BSSID Information	Operating Class	Channel Number	PHY Type	Optional Subelements
1	1	6	4	1	1	1	variable

Figure 9-295—Neighbor Report element format

9.6.9.2 FT Request frame

The FT Request frame is sent by the STA to its associated AP to initiate an over-the-DS fast BSS transition.

Figure 9-688 shows the format of the FT Request frame Action field.

	Category	FT Action	STA Address	Target AP Address	FT Request frame body
Octets:	1	1	6	6	variable

Figure 9-688—FT Request frame Action field format

The Category field is defined in 9.4.1.11.

The FT Action field is defined in 9.6.9.1.

The STA Address field is set to the fast BSS transition originator's (FTO's) MAC address.

The Target AP Address field is set to the BSSID value of the target AP.

82. In normal operation of exemplary Zyxel Accused APs, the Source AP establishes a session, either over the air or over the distribution system, with a destination candidate device or target AP.

distribution system (DS): A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS).

13.10.2 Remote request broker (RRB)

The RRB resides in the SME on the APs and acts as a forwarding agent (at the current AP) and termination point (at the target AP) for protocol messages over the DS.

The RRB allows APs that are part of the same mobility domain to exchange information over the DS. APs that advertise the same MDID shall be reachable over the DS and support the over-the-DS communication.

As a termination point, when the RRB at the target AP receives a request frame from the current AP, it interacts with the MAC and other parts of the SME to process the request and respond with a Remote Response frame, through the RRB on the current AP, back to the requesting FTO.

As a forwarding agent, when the RRB at the current AP receives a request from an FTO directed to another AP in the same mobility domain, the current AP forwards the request to that target AP. The RRB on the

83. Zyxel Accused APs include an input section for receiving a switching destination candidate device list (e.g., the Neighbor Report) request from connected users' devices:

11.11.10.3 Responding to a neighbor report request

If dot11RMNeighborReportActivated is true, an AP receiving a neighbor report request shall respond with a Neighbor Report Response frame containing zero or more Neighbor Report elements. If an SSID element is

84. Zyxel Accused APs include an output section for presenting the Neighbor Report to a connected client in response to a neighbor report request:

4.3.11.10 Neighbor report

The neighbor report request is sent to an AP, which returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition. Neighbor reports contain information from dot11RMNeighborReportTable concerning neighbor APs. This request/report pair enables a STA to gain information about the neighbors of the associated AP to be used as potential roaming candidates.

11.11.10 Usage of the neighbor report

11.11.10.1 General

A neighbor report is sent by an AP and it contains information on neighboring APs that are members of ESSs requested in the neighbor report request. A neighbor report might not be exhaustive either by choice, or due to the fact that there might be neighbor APs not known to the AP. The neighbor report contents are derived from the NeighborListSet parameter of the MLME-NEIGHBORREPRESP.request primitive. The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.

85. In normal operation of the Accused Zyxel APs, when an AP receives a switching request (e.g., an FT Action Request) from a user device, the Zyxel AP sends a RemoteRequest to the Target AP:

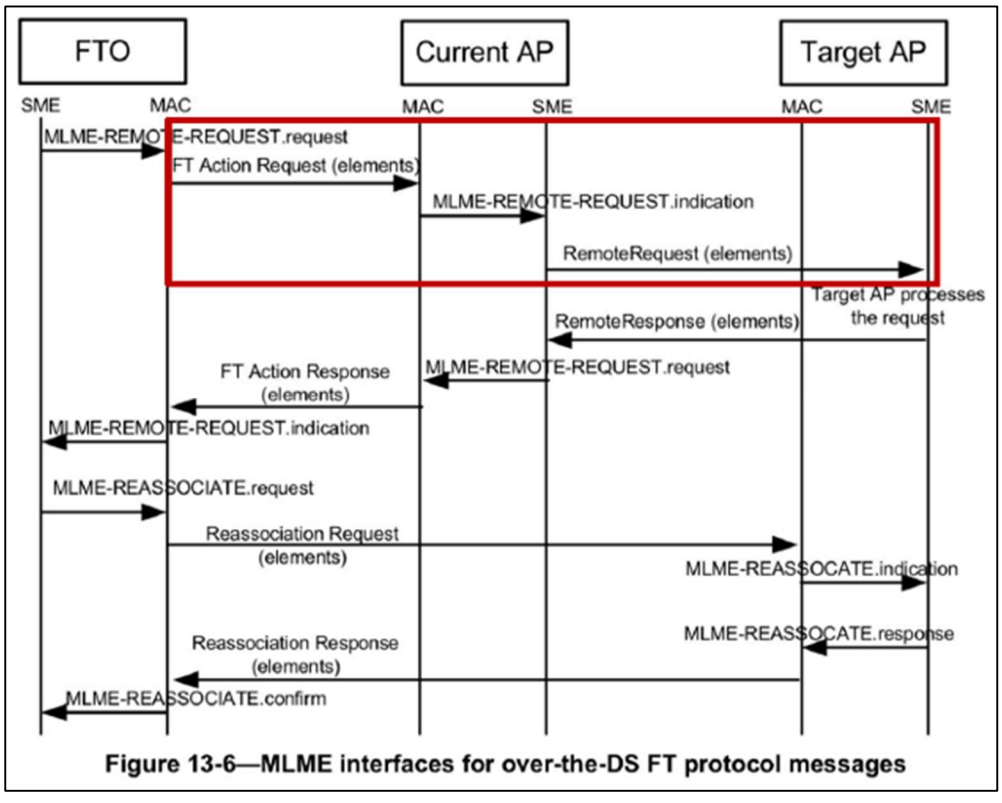


Figure 13-6—MLME interfaces for over-the-DS FT protocol messages

86. The RemoteRequest message contains a switching instruction including, for example, instructions for the robust security network (RSN) association:

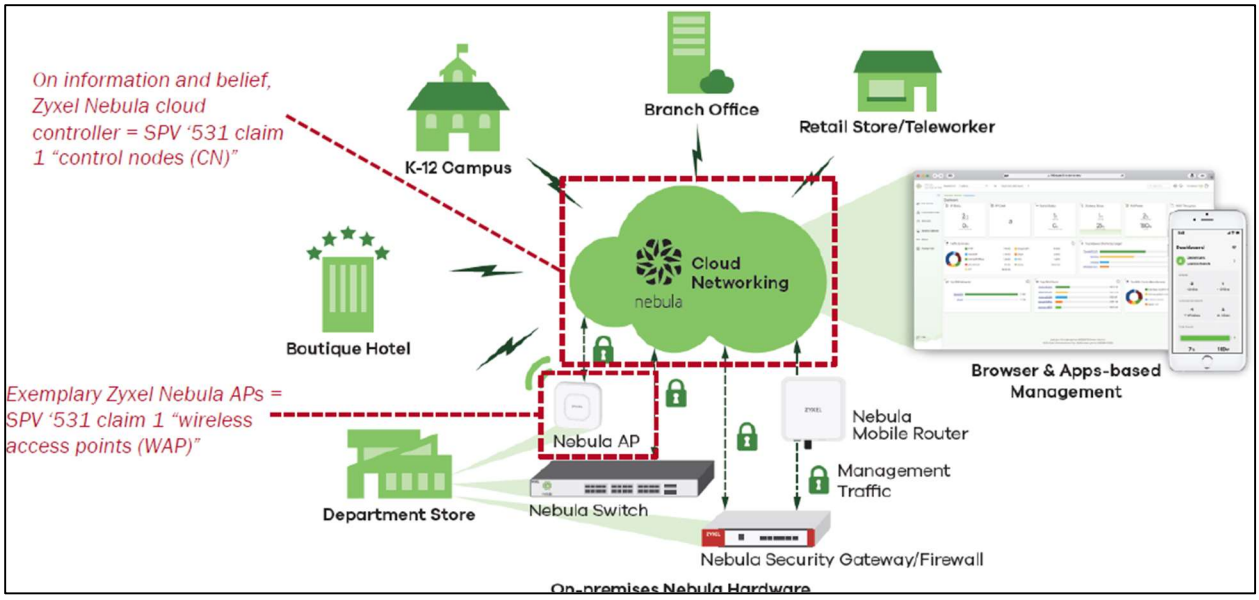
> **robust security network association (RSNA):** The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-way handshake or FT protocol. Note that existence of an RSNA between two STAs does not of itself provide robust security. Robust security is provided when all STAs in the network use RSNAs.

> **13.8 FT authentication sequence**
>
> **13.8.1 Overview**
>
> The FT authentication sequence comprises four sets of FT elements. Each set of FT elements is referred to in 13.8 as a *message*. These messages are included in the FT Protocol frames or FT Resource Request Protocol frames to initiate a fast BSS transition. The FT authentication sequence is always initiated by the FTO and responded to by the target AP.
>
> In an RSN, the first two messages in the sequence allow the FTO and target AP to provide association instance identifiers, SNonce and ANonce, respectively. SNonce and ANonce are chosen randomly or pseudorandomly and are used to generate a fresh PTK. The first two messages also enable the target AP to provision the PMK-R1 and the FTO and target AP to compute the PTK. The third and fourth messages demonstrate liveness of the peer, authenticate the elements, and enable an authenticated resource request.

ZYXEL INFRINGES U.S. PATENT NO. 8,045,531.

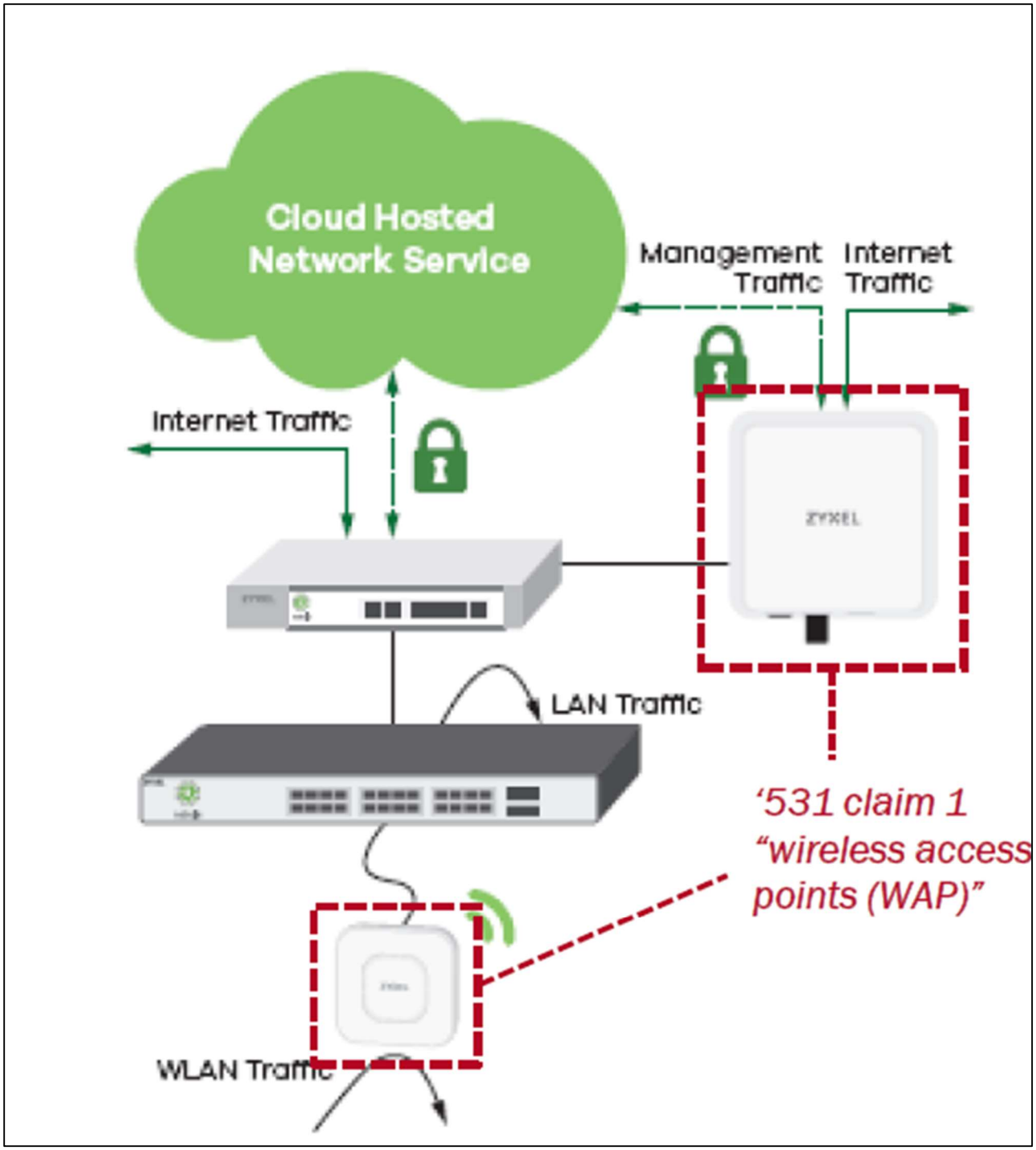
87. The Patent Office issued U.S. Patent No. 8,045,531, titled "System and method for negotiation of WLAN entity," on October 25, 2011, after a thorough examination and determination that the subject matter claimed is patentable.

88. Zyxel Accused Products with respect to the '531 patent include Zyxel Nebula (the Zebula WiFi System) comprising, by way of example, Zyxel Nebula cloud controller devices that interface with Zyxel APs to provide WLAN service:



https://www.zyxel.com/library/assets/tech library/Solution Guide/Nebula_CC_Solution_Guide.pdf.

89. Accused Zyxel WiFi Systems comprise one or more APs (WAPs) managed by a Nebula Controller including, without limitation, Zyxel APs identified at https://www.zyxel.com/us/en-us/products/wireless such as Zyxel Access Points Models NWA50AX, NWA90AX, NWA55AXE, NWA110AX, NWA210AX, NWA1122ACv2, NWA1123-AC PRO, WAX510D, WAX610D, WAX6305, WAX5505, NWA5123-AC HD, WAC6302D-5v2, WAC50D, WAC500H, WAC6103D-I, WAC6302D-5, WAC6503D-S, WAC6553D-5, and WAC6552D-E.



https://www.zyxel.com/library/assets/tech-library/SolutionGuide/Nebula_CC_Solution_Guide.pdf.

90. In the Accused Zyxel Systems, WLAN functionality is distributed

among the Nebula controller devices and the Zyxel APs. For example, Nebula APs are configured by a Nebula controller to implement (process) certain client-facing WLAN functions including, for example, load balancing, smart steering, and assisted (802.11k) + fast (802.11r) roaming functions that are a subset of functionality defined for the WLAN.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Access Point		Use these menus to monitor and configure the Access Points managed by the NCC. The settings are applied when a Nebula Access Point is registered and attached to the selected site.
	Monitor	
	Access points	Use this menu to view the list of Access Points added to the site.
	Clients	Use this menu to view WiFi clients which are connected to the Access Points in the site.
	Event log	Use this menu to view all events on the Access Point. An event is something that has happened to a Nebula managed device.
	Wireless health	Use this menu to view health of the WiFi networks for the supported Access Points and connected clients.
	Summary report	Use this menu to view network statistics specific to Access Points in the site.
	Configure	
	SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	SSID advanced settings	Use this menu to configure network access, traffic options and advanced settings for SSID profiles.
	Captive portal customization	Use this menu to configure captive portal settings for SSID profiles.
	SSID availability	Use this menu to configure SSID visibility settings and set whether the SSID is enabled or disabled on each day of the week.
	Radio settings	Use this menu to configure global radio settings, such as maximum output power or channel width, and enable smart client steering for all Access Points in the site.
	Traffic shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Security service	Use this menu to enable application visibility and optimization, and IP reputation filter on the managed Access Point.
	AP & port settings	Use this menu to configure load balancing settings and enable or disable a port on the managed Access Point and configure the port's VLAN settings.

Table 183 Access Point > Configure > Radio settings (continued)

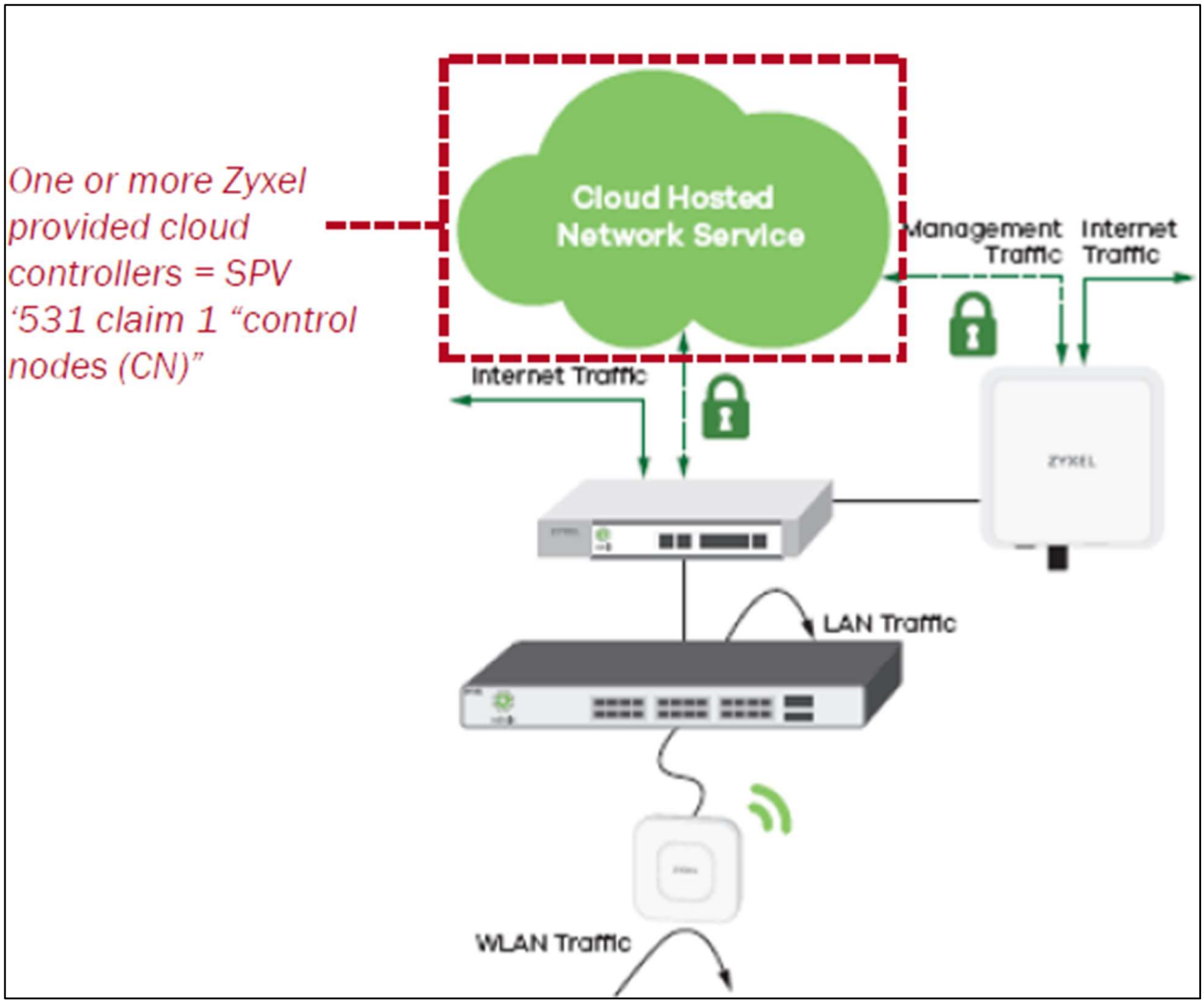
LABEL	DESCRIPTION
5 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation. Select **Auto** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between. Note: The method is automatically set to **Auto** when no channel is selected or any one of the previously selected channels is not supported.
Allow 802.11ax/ac/n stations only	Select **ON** to have the Nebula Device allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.
Smart Steering	Select **ON** to enable smart client steering on the Nebula Device. Client steering helps monitor wireless clients and drop their connections to optimize the bandwidth when the clients are idle or have a low signal. When a wireless client is dropped they have the opportunity to steer to an Nebula Device with a strong signal. Additionally, dual band wireless clients can also steer from one band to another. Select **OFF** to disable this feature on the Nebula Device.

Table 179 Access Point > Configure > SSID advanced settings (continued)

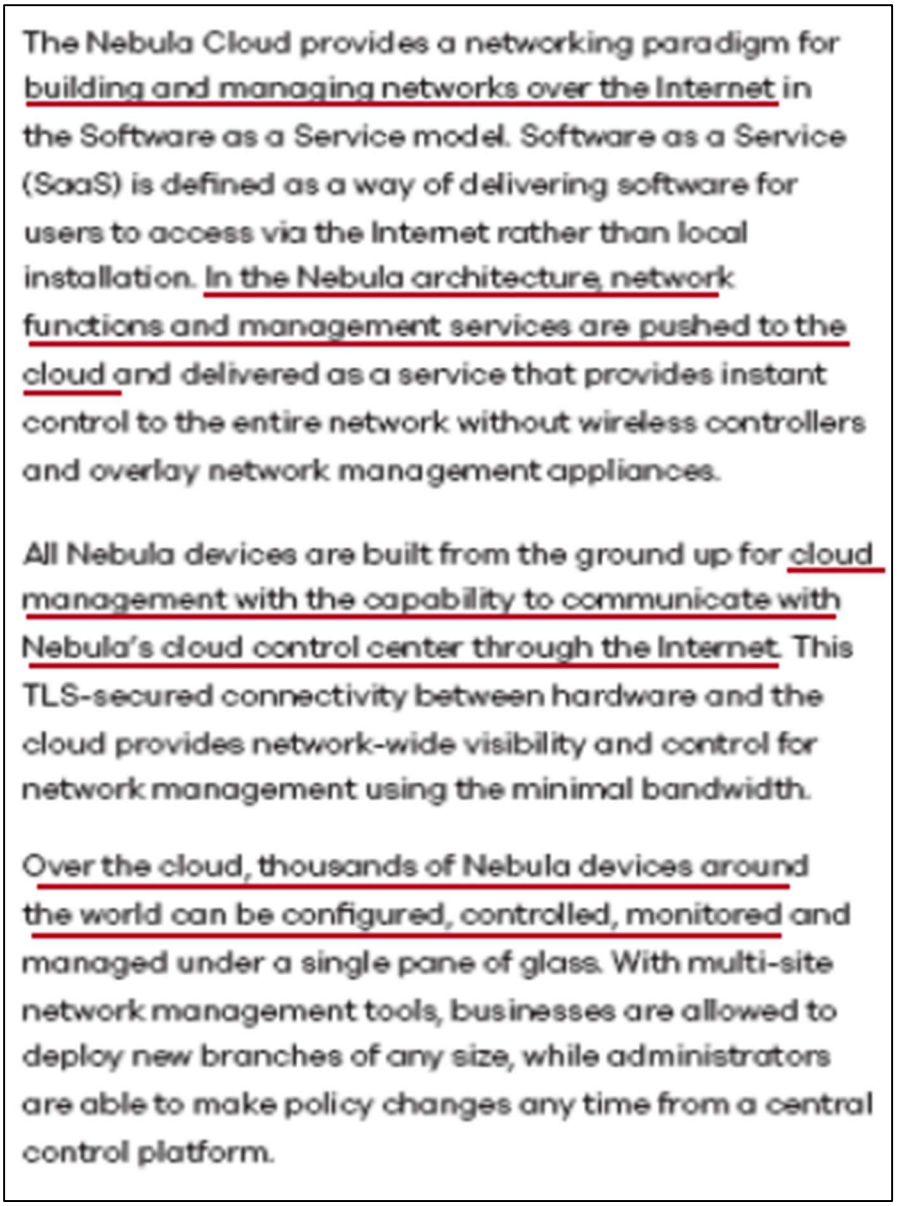
LABEL	DESCRIPTION
Assisted roaming	Select to turn on or off IEEE 802.11k/v assisted roaming on the Nebula Device. When the connected clients request 802.11k neighbor lists, the Nebula Device will response with a list of neighbor Nebula Devices that can be candidates for roaming. When the 802.11v capable clients are using the 2.4 GHz band, the Nebula Device can send 802.11v messages to steer clients to the 5 GHz band.
802.11r	Select to turn on or off IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another, by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process.

https://download.zyxel.com/Nebula_CC/user_guide/Nebula CC_V14.00_Ed1.pdf.

91. Zyxel Accused Systems comprise one or more control nodes (cloud controllers (on information and belief, cloud servers with WLAN controller application functionality).



Nebula secure cloud networking solution provides cloud-based, centralized control and visibility over all Nebula wired, wireless, security, and mobile router hardware — all without the cost and complexity of on-site control equipment or overlay management systems. With comprehensive product portfolio that can be centrally managed from the cloud, Nebula offers simple, intuitive and scalable management for all networks.



The Nebula Cloud provides a networking paradigm for building and managing networks over the Internet in the Software as a Service model. Software as a Service (SaaS) is defined as a way of delivering software for users to access via the Internet rather than local installation. In the Nebula architecture, network functions and management services are pushed to the cloud and delivered as a service that provides instant control to the entire network without wireless controllers and overlay network management appliances.

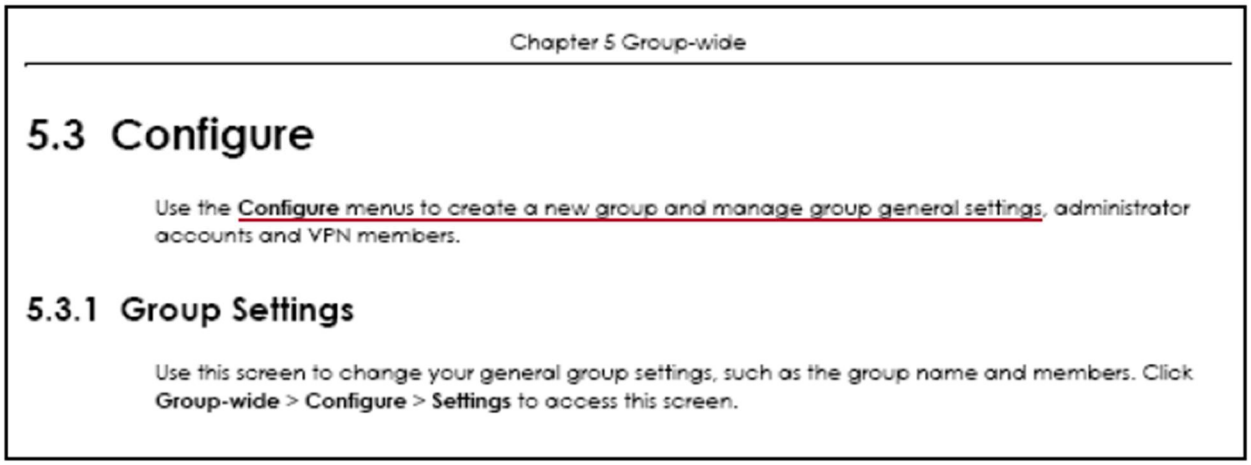
All Nebula devices are built from the ground up for cloud management with the capability to communicate with Nebula's cloud control center through the Internet. This TLS-secured connectivity between hardware and the cloud provides network-wide visibility and control for network management using the minimal bandwidth.

Over the cloud, thousands of Nebula devices around the world can be configured, controlled, monitored and managed under a single pane of glass. With multi-site network management tools, businesses are allowed to deploy new branches of any size, while administrators are able to make policy changes any time from a central control platform.

https://www.zyxel.com/library/assets/tech-library/Solution-Guide/Nebula_CC_Solution_Guide.pdf.

92. In the Zyxel Accused Systems, WLAN functionality is distributed among the Nebula controller devices ('531 CN) and the Zyxel APs. For example, Nebula controller devices provide certain network-facing WLAN functions that are a subset of functionalities defined for the WLAN. Functions include, without

limitation, Group-wide & Organization-wide configuration; configuring VLANs; and monitoring Groups, Organizations, and Sites.



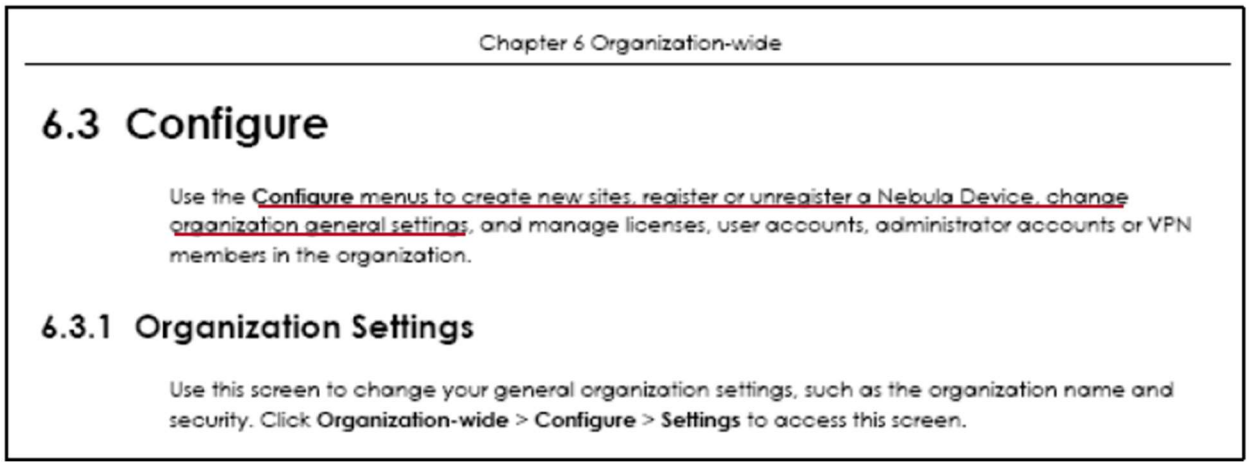
Chapter 5 Group-wide

5.3 Configure

Use the **Configure** menus to create a new group and manage group general settings, administrator accounts and VPN members.

5.3.1 Group Settings

Use this screen to change your general group settings, such as the group name and members. Click **Group-wide** > **Configure** > **Settings** to access this screen.



Chapter 6 Organization-wide

6.3 Configure

Use the **Configure** menus to create new sites, register or unregister a Nebula Device, change organization general settings, and manage licenses, user accounts, administrator accounts or VPN members in the organization.

6.3.1 Organization Settings

Use this screen to change your general organization settings, such as the organization name and security. Click **Organization-wide** > **Configure** > **Settings** to access this screen.

https://download.zyxel.com/Nebula_CC/user_guide/Nebula CC_V14.00_Ed1.pdf

93. The Accused Zyxel Systems provide for configuring and managing a management VLAN:

Table 9 NCC Menu Summary (continued)

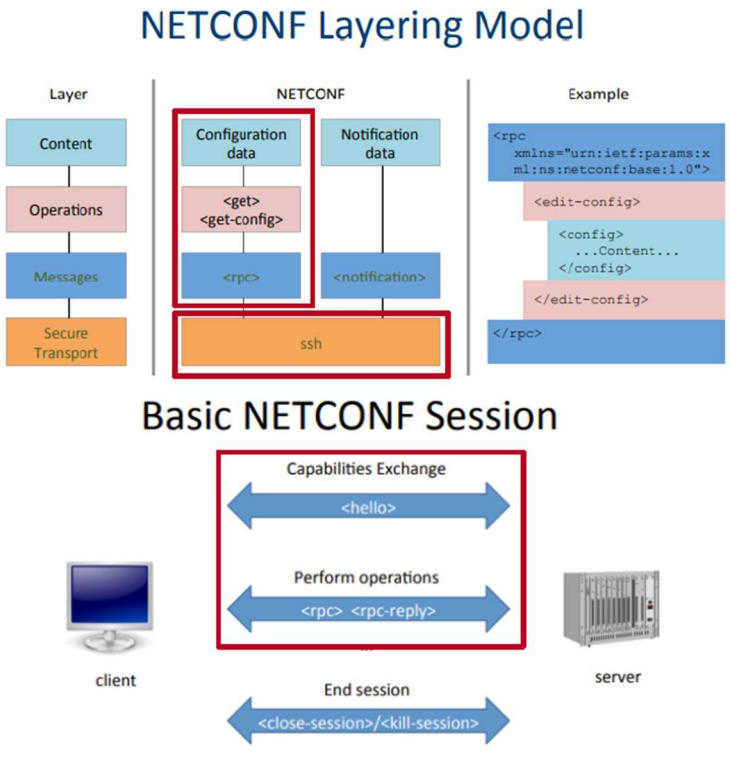
LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Access Point		Use these menus to monitor and configure the Access Points managed by the NCC. The settings are applied when a Nebula Access Point is registered and attached to the selected site.
	Monitor	
	Access points	Use this menu to view the list of Access Points added to the site.
	Clients	Use this menu to view WiFi clients which are connected to the Access Points in the site.
	Event log	Use this menu to view all events on the Access Point. An event is something that has happened to a Nebula managed device.
	Wireless health	Use this menu to view health of the WiFi networks for the supported Access Points and connected clients.
	Summary report	Use this menu to view network statistics specific to Access Points in the site.
	Configure	
	SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	SSID advanced settings	Use this menu to configure network access, traffic options and advanced settings for SSID profiles.
	Captive portal customization	Use this menu to configure captive portal settings for SSID profiles.
	SSID availability	Use this menu to configure SSID visibility settings and set whether the SSID is enabled or disabled on each day of the week.
	Radio settings	Use this menu to configure global radio settings, such as maximum output power or channel width, and enable smart client steering for all Access Points in the site.
	Traffic shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Security service	Use this menu to enable application visibility and optimization, and IP reputation filter on the managed Access Point.
	AP & port settings	Use this menu to configure load balancing settings and enable or disable a port on the managed Access Point and configure the port's VLAN settings.

https://download.zyxel.com/Nebula_CC/user_guide/Nebula%20CC_V14.00_Ed1.pdf

94. In normal operation of the Zyxel Accused Systems, Nebula APs convey their capabilities to a Nebula cloud controller (control node) that utilizes this information to configure the network and establish a secure session. This signaling exchange is handled via the NETCONF protocol via, at least in part, a

WAP negotiation unit.

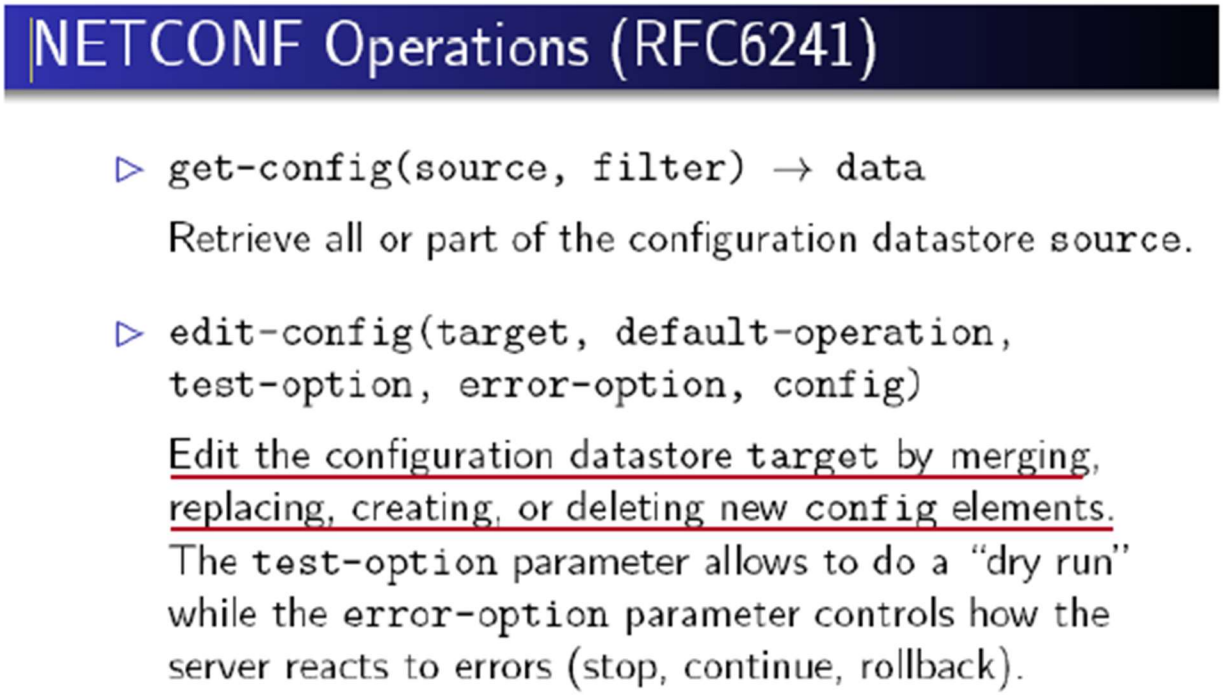
https://www.zyxel.com/library/assets/tech-library/Solution-Guide/Nebula_CC_Solution_Guide.pdf



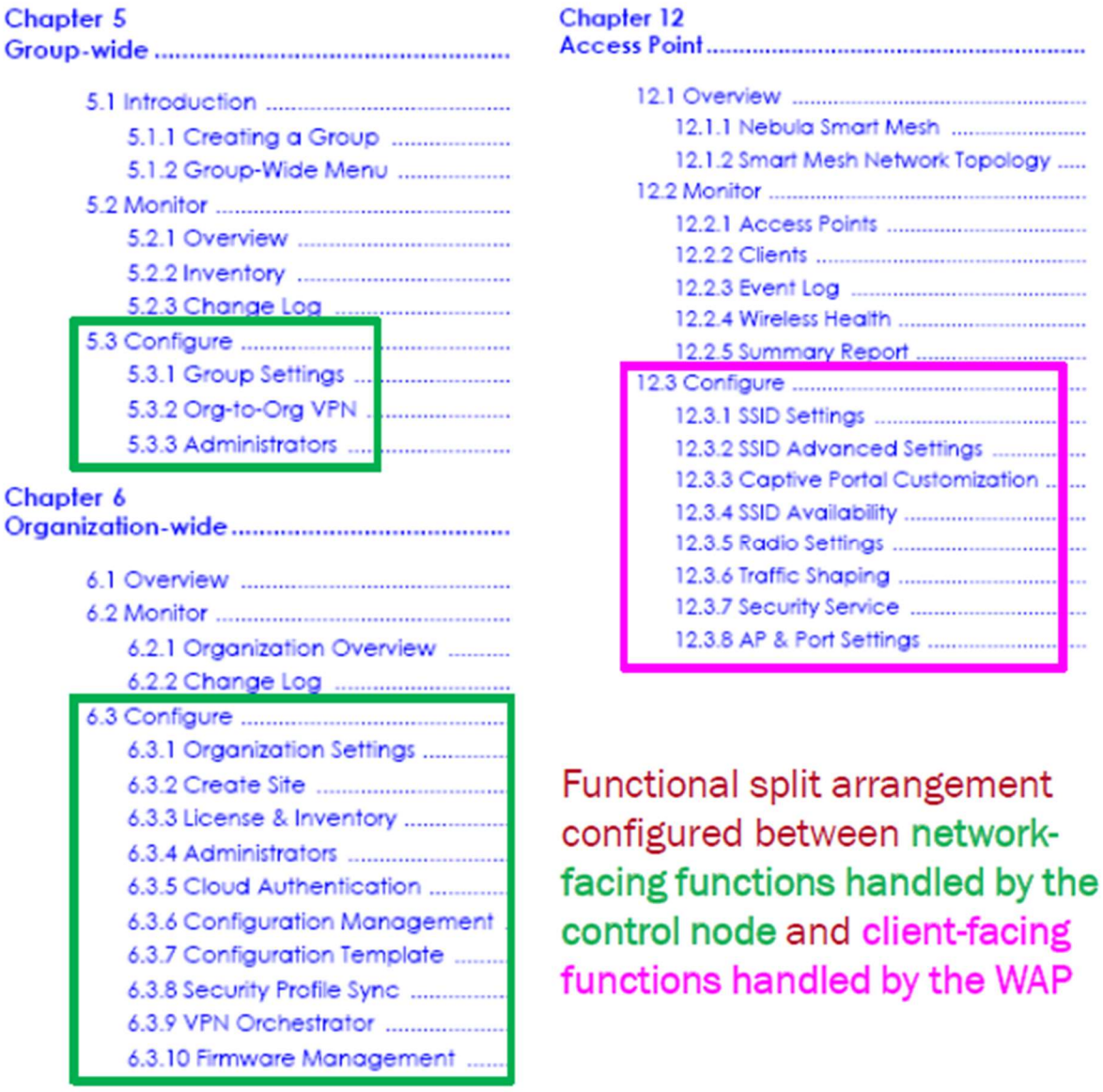
https://www.ietf.org/slides/slides-edu-network-configuration-with-netconf-00.pdf

95. The discovery and AP/network confirmation process involves the Nebula cloud controller and the Nebula AP negotiating a functional split arrangement.

The Network Configuration Protocol (NETCONF) defines a simple mechanism through which a network device can be managed, configuration data can be retrieved, and new configuration data can be uploaded and manipulated. NETCONF uses Extensible Markup Language (XML)-based data encoding for the configuration data and protocol messages.



https://www.ietf.org/slides/slides-edu-netconf-yang-00.pdf

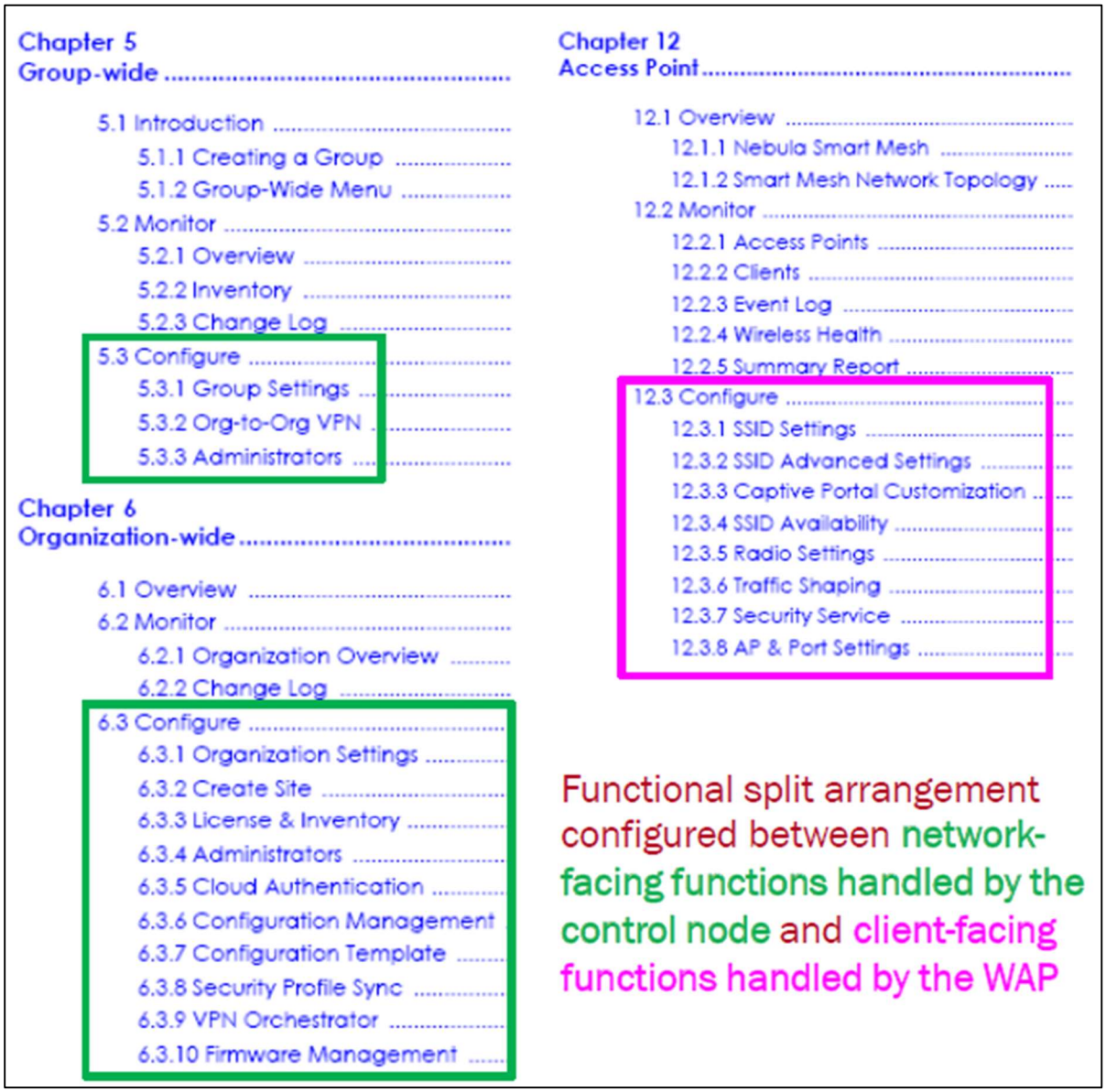


https://download.zyxel.com/Nebula_CC/user_guide/Nebula%20CC_V14.00_Ed1.pdf.

96. The Control Node responds to discovery and connection request messages from the APs and delivers configurations to the APs during adoption.

97. Zyxel Control Nodes provide complimentary functionality for the APs by, for example, providing the network facing functions used by the APs—this

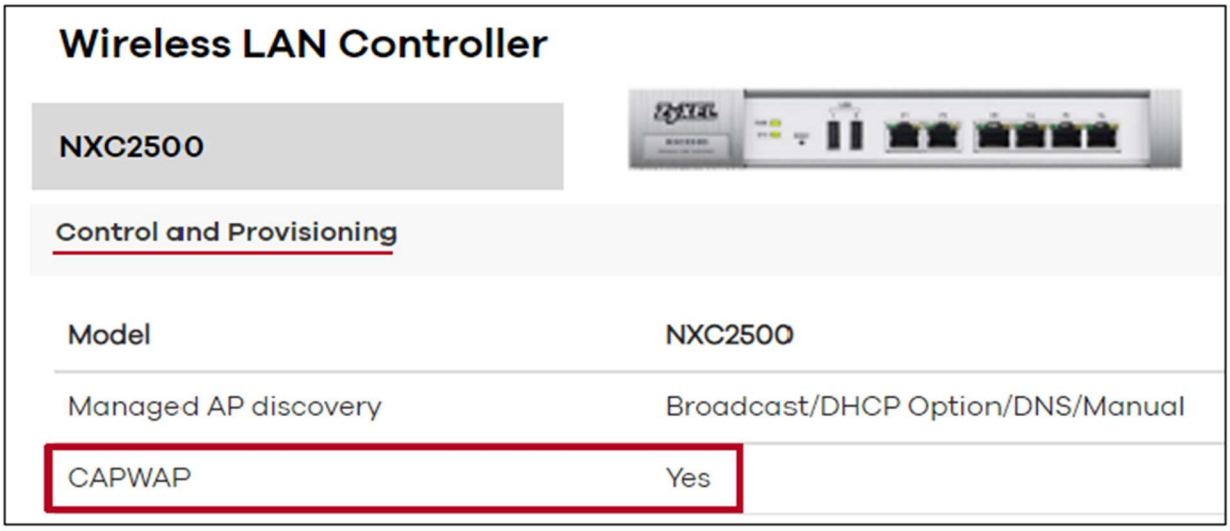
network facing functionality forming a complete WLAN functionality with the APs client-facing functionality.



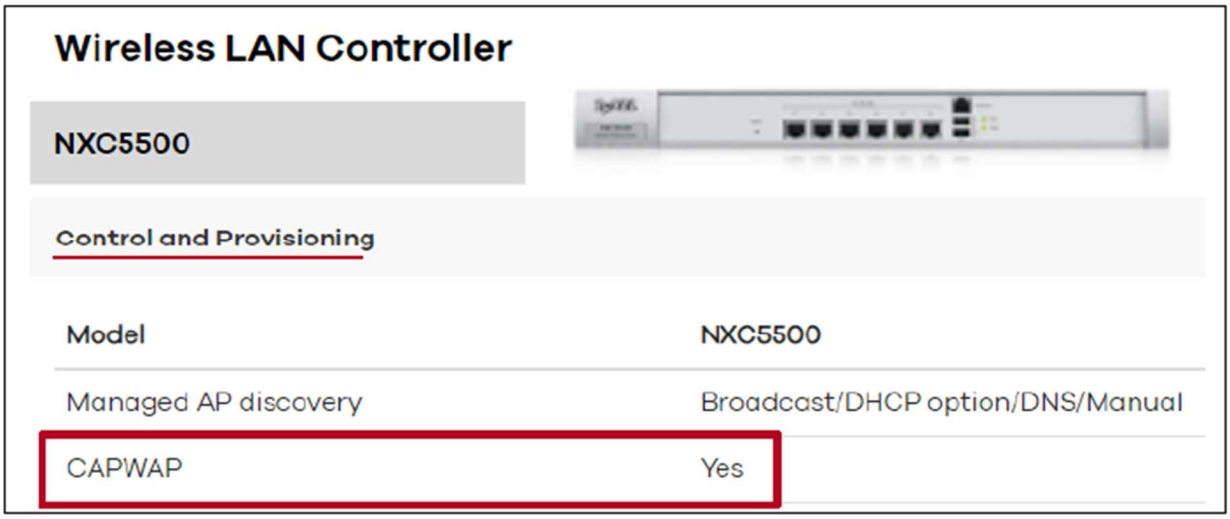
98. Zyxel Control Nodes provide complimentary functionality for APs by, for example, managing the APs provisioning, configuration, and operation—this network wide management functionality forming a complete WLAN functionality with the AP-specific operational functionality (e.g. running a specific

configuration, specific firmware, etc).

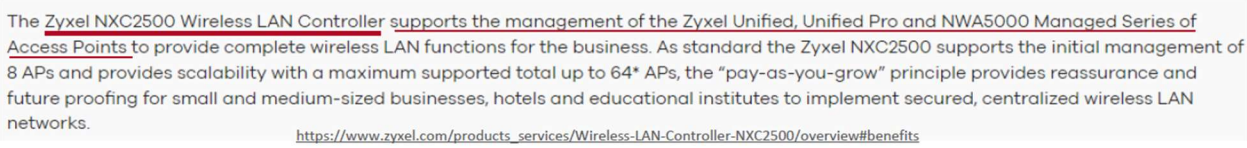
99. Additional Zyxel Accused Products with respect to the ’531 patent include the Zyxel Systems featuring Zyxel APs and Zyxel access controllers (ACs including, for example, Zyxel NXC2500 and NXC5500 wireless controllers) that support configuration using the CAPWAP protocol to provide service in a WLAN:



https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/specification

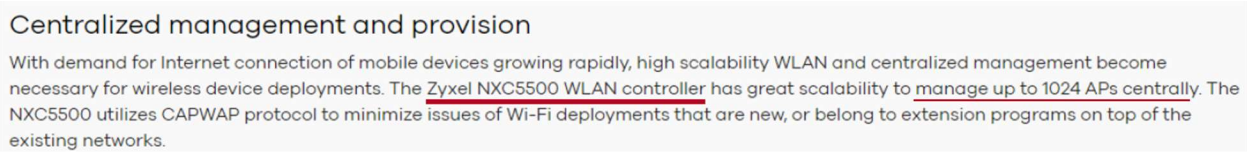


100. Zyxel APs support configuration using the CAPWAP protocol.


The Zyxel NXC2500 Wireless LAN Controller supports the management of the Zyxel Unified, Unified Pro and NWA5000 Managed Series of Access Points to provide complete wireless LAN functions for the business. As standard the Zyxel NXC2500 supports the initial management of 8 APs and provides scalability with a maximum supported total up to 64* APs, the "pay-as-you-grow" principle provides reassurance and future proofing for small and medium-sized businesses, hotels and educational institutes to implement secured, centralized wireless LAN networks.

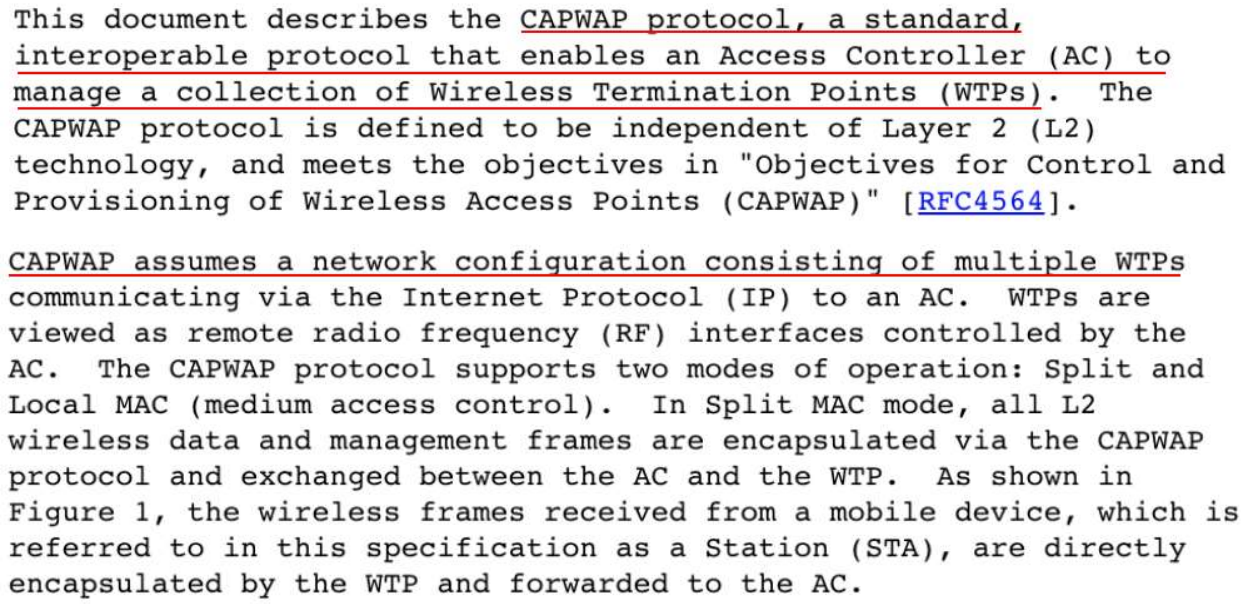
https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/overview#benefits

https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/overview#benefits.


Centralized management and provision

With demand for Internet connection of mobile devices growing rapidly, high scalability WLAN and centralized management become necessary for wireless device deployments. The Zyxel NXC5500 WLAN controller has great scalability to manage up to 1024 APs centrally. The NXC5500 utilizes CAPWAP protocol to minimize issues of Wi-Fi deployments that are new, or belong to extension programs on top of the existing networks.

101. Zyxel APs and ACs support configuration using the CAPWAP protocol to provide service in a WLAN. Zyxel ACs manage one or more Zyxel APs.


This document describes the CAPWAP protocol, a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs). The CAPWAP protocol is defined to be independent of Layer 2 (L2) technology, and meets the objectives in "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)" [RFC4564].

CAPWAP assumes a network configuration consisting of multiple WTPs communicating via the Internet Protocol (IP) to an AC. WTPs are viewed as remote radio frequency (RF) interfaces controlled by the AC. The CAPWAP protocol supports two modes of operation: Split and Local MAC (medium access control). In Split MAC mode, all L2 wireless data and management frames are encapsulated via the CAPWAP protocol and exchanged between the AC and the WTP. As shown in Figure 1, the wireless frames received from a mobile device, which is referred to in this specification as a Station (STA), are directly encapsulated by the WTP and forwarded to the AC.

https://tools.ietf.org/html/rfc5415.

102. In Accused Zyxel Systems, WLAN functionality is distributed among

the ACs and APs in the network. Zyxel ACs manage one or more Zyxel APs.

> Provisioning WTPs with security credentials and managing which WTPs are authorized to provide service are traditionally handled by proprietary solutions. Allowing these functions to be performed from a centralized AC in an interoperable fashion increases manageability and allows network operators to more tightly control their wireless network infrastructure.
>
> **1.1. Goals**
>
> The goals for the CAPWAP protocol are listed below:
>
> 1. To centralize the authentication and policy enforcement functions for a wireless network. The AC may also provide centralized bridging, forwarding, and encryption of user traffic. Centralization of these functions will enable reduced cost and higher efficiency by applying the capabilities of network processing silicon to the wireless network, as in wired LANs.
>
> 2. To enable shifting of the higher-level protocol processing from the WTP. This leaves the time-critical applications of wireless control and access in the WTP, making efficient use of the computing power available in WTPs, which are subject to severe cost pressure.

Id.

103. Through the discovery process, Zyxel APs convey their capabilities to an AC, which utilizes this information to configure the network and establish a secure DTLS session.

> The CAPWAP Protocol begins with a Discovery phase. The WTPs send a Discovery Request message, causing any Access Controller (AC) receiving the message to respond with a Discovery Response message. From the Discovery Response messages received, a WTP selects an AC with which to establish a secure DTLS session. In order to establish the secure DTLS connection, the WTP will need some amount of pre-provisioning, which is specified in Section 12.5. CAPWAP protocol messages will be fragmented to the maximum length discovered to be supported by the network.
>
> Once the WTP and the AC have completed DTLS session establishment, a configuration exchange occurs in which both devices agree on version information. During this exchange, the WTP may receive provisioning settings. The WTP is then enabled for operation.

8.1.1. Configuration Flexibility

The CAPWAP protocol provides the flexibility to configure and manage WTPs of varying design and functional characteristics. When a WTP first discovers an AC, it provides primary functional information

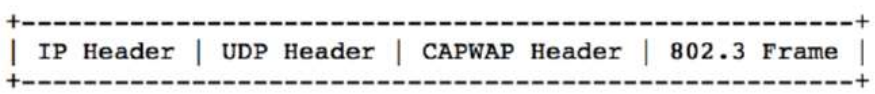
relating to its type of MAC and to the nature of frames to be exchanged. The AC configures the WTP appropriately. The AC also establishes corresponding internal state for the WTP.

Id.

104. For example, the Zyxel System network may be set up with one of two modes of encapsulation: 802.3 or native wireless.

4.4.2. Data Payload

A CAPWAP protocol Data Payload packet encapsulates a forwarded wireless frame. The CAPWAP protocol defines two different modes of encapsulation: IEEE 802.3 and native wireless. IEEE 802.3 encapsulation requires that for 802.11 frames, the 802.11 *Integration* function be performed in the WTP. An IEEE 802.3-encapsulated user payload frame has the following format:



The CAPWAP protocol also defines the native wireless encapsulation mode. The format of the encapsulated CAPWAP Data frame is subject to the rules defined by the specific wireless technology binding. Each wireless technology binding MUST contain a section entitled "Payload Encapsulation", which defines the format of the wireless payload that is encapsulated within CAPWAP Data packets.

For 802.3 payload frames, the 802.3 frame is encapsulated (excluding the IEEE 802.3 Preamble, Start Frame Delimiter (SFD), and Frame Check Sequence (FCS) fields). If the encapsulated frame would exceed the transport layer's MTU, the sender is responsible for the fragmentation of the frame, as specified in Section 3.4. The CAPWAP protocol can support IEEE 802.3 frames whose length is defined in the IEEE 802.3as specification [FRAME-EXT].

CAPWAP assumes a network configuration consisting of multiple WTPs communicating via the Internet Protocol (IP) to an AC. WTPs are viewed as remote radio frequency (RF) interfaces controlled by the AC. The CAPWAP protocol supports two modes of operation: Split and Local MAC (medium access control). In Split MAC mode, all L2 wireless data and management frames are encapsulated via the CAPWAP protocol and exchanged between the AC and the WTP. As shown in Figure 1, the wireless frames received from a mobile device, which is referred to in this specification as a Station (STA), are directly encapsulated by the WTP and forwarded to the AC.

The Local MAC mode of operation allows for the data frames to be either locally bridged or tunneled as 802.3 frames. The latter implies that the WTP performs the 802.11 Integration function. In either case, the L2 wireless management frames are processed locally

Id.

105. The Accused Zyxel ACs provide complimentary functionality for APs by, for example, performing the 802.11 integration function if split MAC mode is utilized.

8.3. Configuration Status Response

The Configuration Status Response message is sent by an AC and provides a mechanism for the AC to override a WTP's requested configuration.

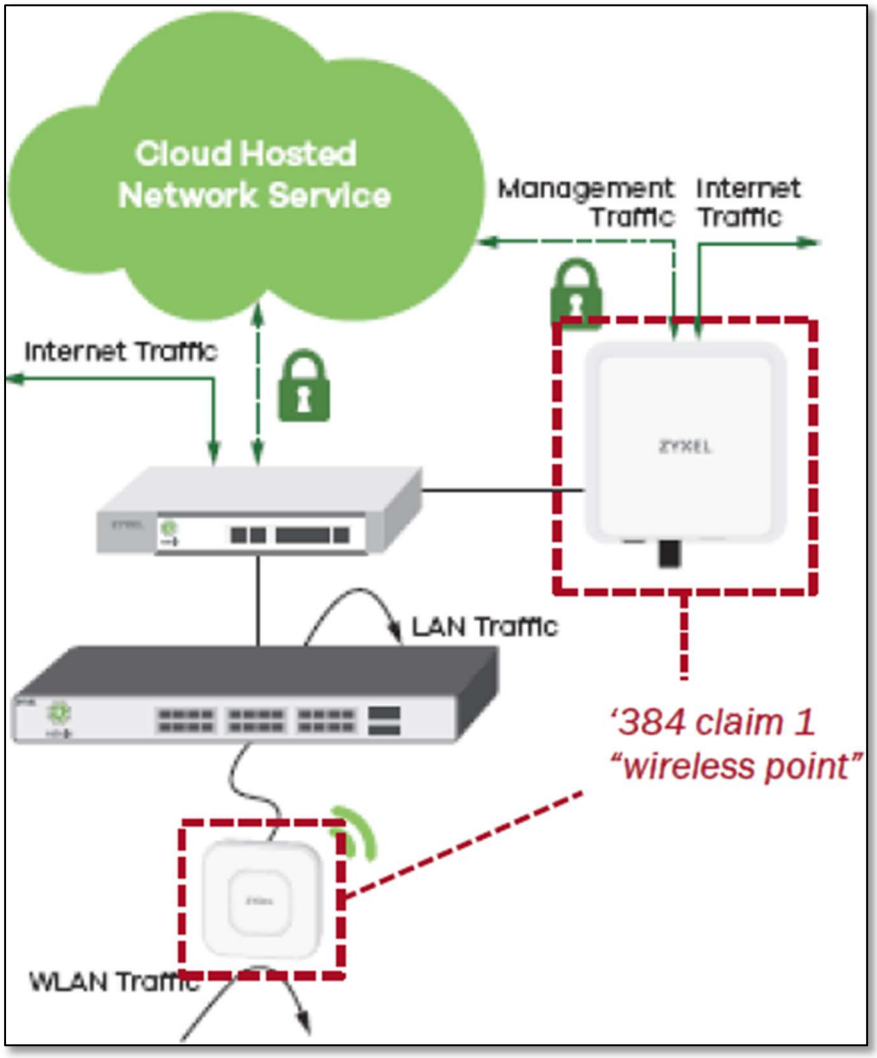
Id.

ZYXEL INFRINGES U.S. PATENT NO. 8,270,384.

106. The Patent Office issued U.S. Patent No. 8,270,384, titled "Wireless Point that Provides Functions for a Wireless Local Area Network to be Separated Between the Wireless Point and One or More Control Nodes, and Method for Providing Service in a Wireless Local Area Network Having Functions Separated Between a Wireless Point and One or More Control Nodes," on September 18,

2012, after a thorough examination and determination that the subject matter claimed is patentable.

107. Zyxel Accused Products with respect to the ’384 patent include the Zyxel Nebula WiFI system comprising Zyxel Nebula cloud controller devices that interface with Zyxel Nebula APs to provide WLAN service:



https://www.zyxel.com/library/assets/tech-library/Solution-Guide/Nebula_CC_Solution_Guide.pdf

108. Infringing Zyxel WiFi Systems comprise one or more Nebula APs (WAPs) managed by an Nebula Controller including, without limitation, Zyxel APs identified at https://www.zyxel.com/us/en-us/products/wireless such as Zyxel Access Points Models NWA50AX, NWA90AX, NWA55AXE, NWA110AX, NWA210AX, NWA1122ACv2, NWA1123-AC PRO, WAX510D, WAX610D, WAX6305, WAX5505, NWA5123-AC HD, WAC6302D-5v2, WAC50D, WAC500H, WAC6103D-I, WAC6302D-5, WAC6503D-S, WAC6553D-5, and WAC6552D-E.

Access Points with NebulaFlex Product Options

Model	NWA130BE	NWA220AX-6E	NWA210AX
Product name	BE11000 WiFi 7 Triple-Radio NebulaFlex Access Point	AXE5400 WiFi 6E Dual-Radio NebulaFlex Access Point	AX3000 WiFi 6 Dual-Radio NebulaFlex Access Point
			
Typical deployment	High density and interference-laden indoor envrionments	Medium to high density deployments	Medium to high density deployments
Radio specification	• 1 x 802.11 b/g/n/ax/be radio • 1 x 802.11 a/n/ac/ax/be radio • 11 Gbps max rate • Spatial Stream: 2+2+2	• 1 x 802.11 b/g/n/ax radio • 1 x 802.11 a/n/ac/ax radio • 5.375 Gbps max rate • Spatial Stream: 2+4	• 1 x 802.11 b/g/n/ax radio • 1 x 802.11 a/n/ac/ax radio • 2.975 Gbps max rate • Spatial Stream: 2+4
Power	DC input : 12 VDC 2 A PoE (802.3at): power draw 24 W	DC input: 12 VDC 2 A PoE (802.3at): power draw 21 W	DC input: 12 VDC 2 A PoE (802.3at): power draw 19 W
Antenna	Internal antenna	Internal antenna	Internal antenna

* Bundled licenses are not applicable to NebulaFlex AP.

Access Points with NebulaFlex/ NebulaFlex Pro

Model	NWA50AX	NWA90AX	NWA55AXE	NWA110AX
Product name	802.11ax (WiFi 6) Dual-Radio PoE Access Point	802.11ax (WiFi 6) Dual-Radio PoE Access Point	802.11ax (WiFi 6) Dual-Radio Outdoor PoE Access Point	802.11ax (WiFi 6) Dual-Radio PoE Access Point

Model	NWA210AX	NWA1123ACv3	NWA1123-AC PRO
Product name	802.11ax (WiFi 6) Dual-Radio PoE Access Point	802.11ac Wave 2 Dual-Radio Ceiling Mount PoE Access Point	802.11ac Dual-Radio Dual-Mount Access Point

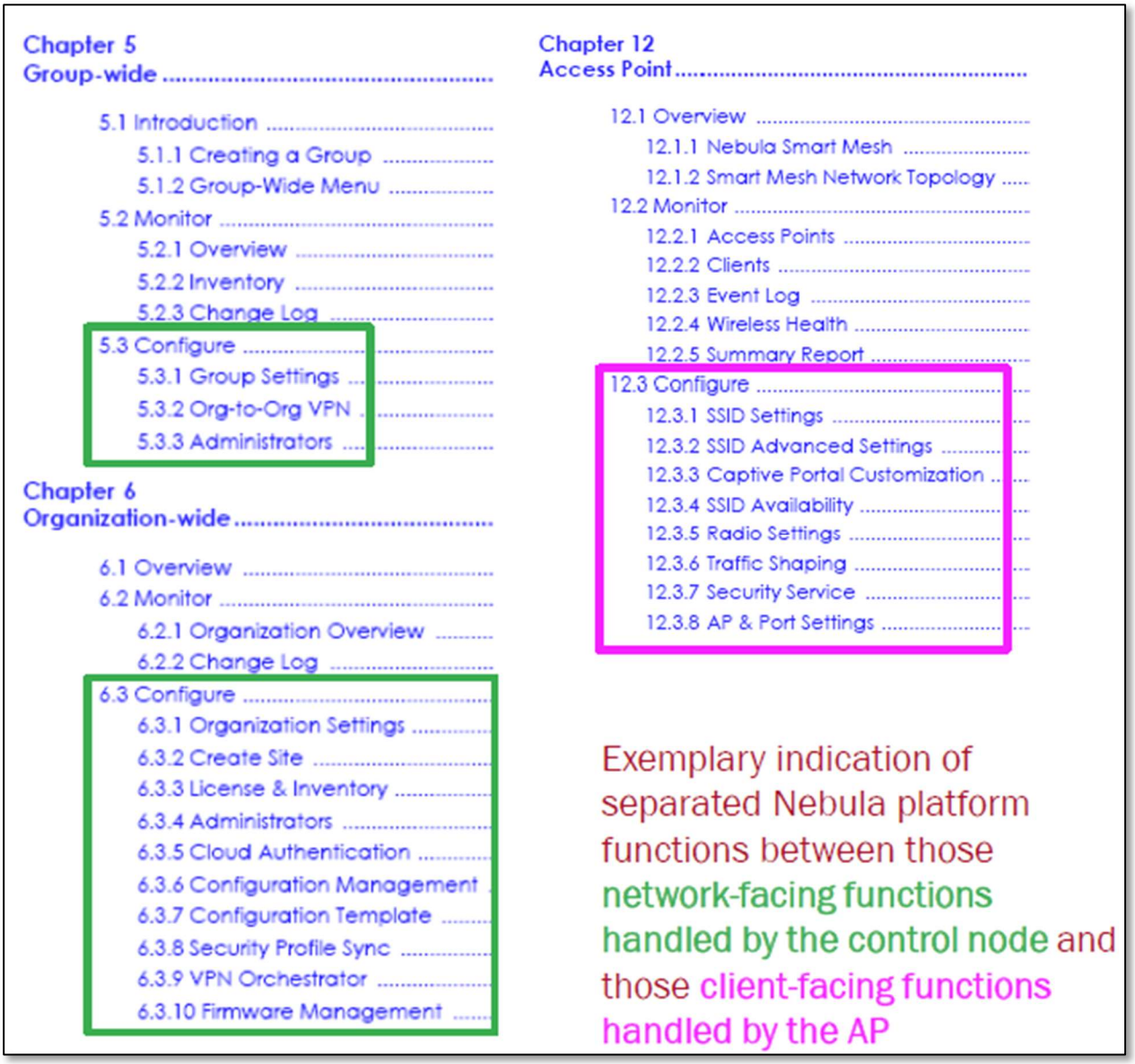
Model	WAX510D	WAX610D	WAX630S
Product name	802.11ax (WiFi 6) Dual-Radio Unified Access Point	802.11ax (WiFi 6) Dual-Radio Unified Pro Access Point	802.11ax (WiFi 6) Dual-Radio Unified Pro Access Point

Model	WAX650S	NWA5123-AC HD	WAC5302D-Sv2
Product name	802.11ax (WiFi 6) Dual-Radio Unified Pro Access Point	802.11ac Wave 2 Dual-Radio Unified Access Point	802.11ac Dual-Radio Unified Access Point

Model	WAC500	WAC500H	WAC6103D-I
Product name	802.11ac Wave 2 Dual-Radio Unified Access Point	802.11ac Wave 2 Wall-Plate Unified Access Point	802.11ac Dual-Radio Dual-optimized Antenna 3x3 Access Point

Model	WAC6303D-S	WAC6503D-S	WAC6552D-S	WAC6553D-E
Product name	802.11ac Wave 2 Dual-Radio Unified Pro Access Point	802.11ac Dual-Radio Smart Antenna 3x3 Access Point	802.11ac Dual-Radio Unified Pro Outdoor Access Point	802.11ac Dual-Radio External Antenna 3x3 Outdoor Access Point

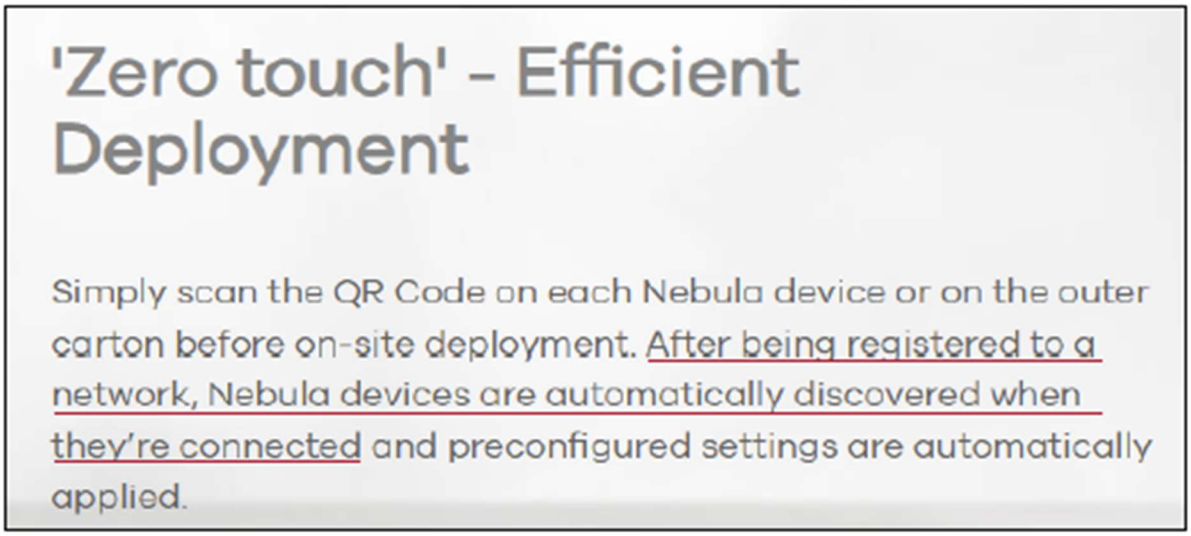
109. The Accused Zyxel Accused Systems include a separation between the AP functions and control node functions. For example, control nodes perform network-facing functions while APs perform client-facing functions. Additionally, control nodes perform network wide WLAN management functions while APs perform AP-specific operational functions.



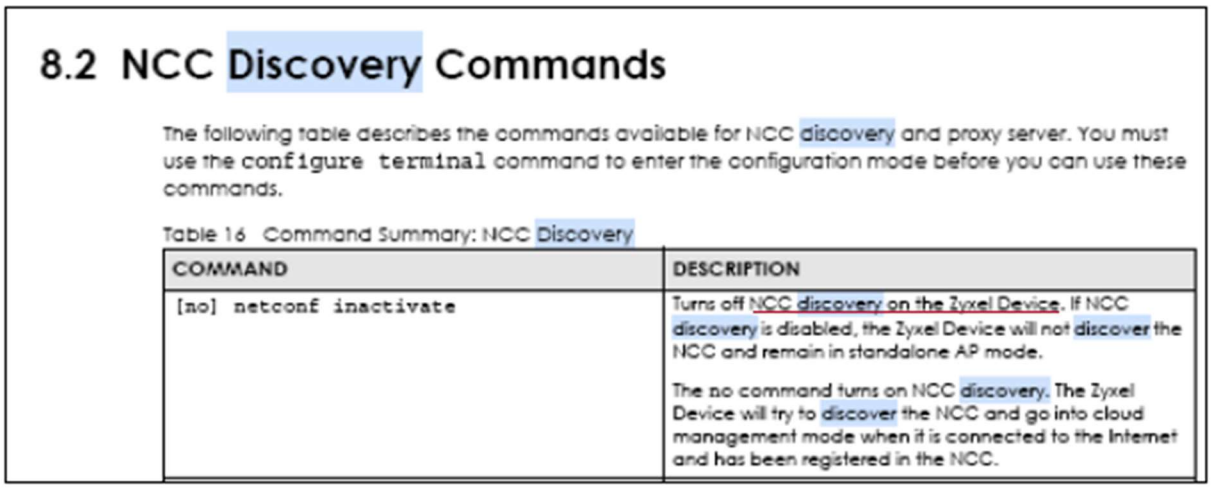
https://download.zyxel.com/Nebula_CC/user_guide/Nebula%20CC_V14.00_Ed1.

pdf

110. In the infringing Nebula WiFi system, the discovery unit of a Nebula AP sends (via broadcast) a discovery request message to Nebula controller devices (said one or more control nodes) on the AP's network. The discovery request messages are sent during the Nebula AP discovery and adoption signaling process.



https://www.zyxel.com/us/en/products_services/NCC-Nebula-Control-Center/



8.2 NCC Discovery Commands

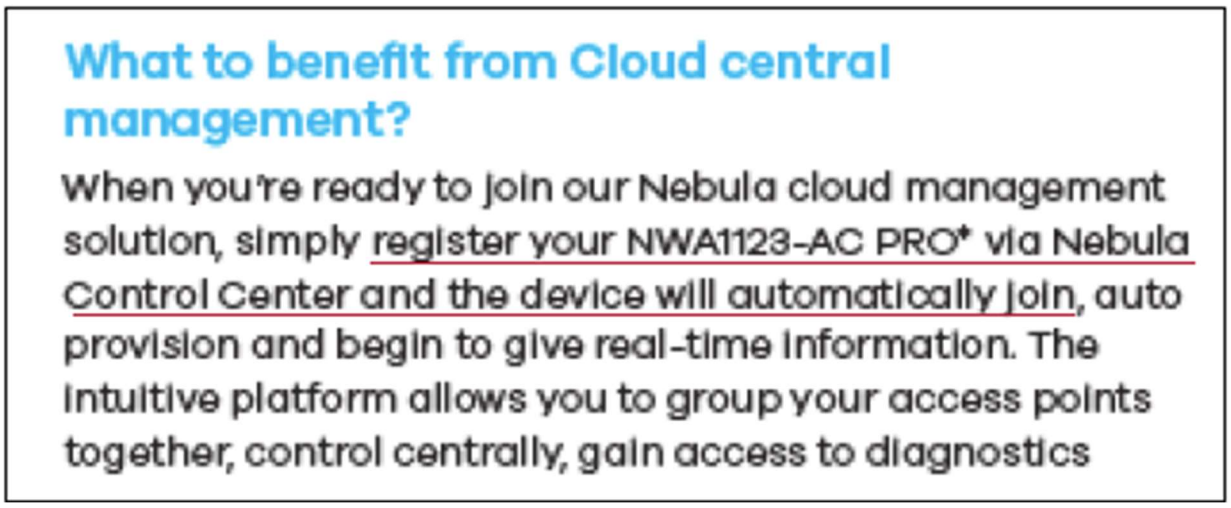
The following table describes the commands available for NCC discovery and proxy server. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 16 Command Summary: NCC Discovery

COMMAND	DESCRIPTION
`[no] netconf inactivate`	Turns off NCC discovery on the Zyxel Device. If NCC discovery is disabled, the Zyxel Device will not discover the NCC and remain in standalone AP mode. The no command turns on NCC discovery. The Zyxel Device will try to discover the NCC and go into cloud management mode when it is connected to the Internet and has been registered in the NCC.

https://download.zyxel.com/NWA1123-AC_PRO/cli_reference_guide/NWA1123-

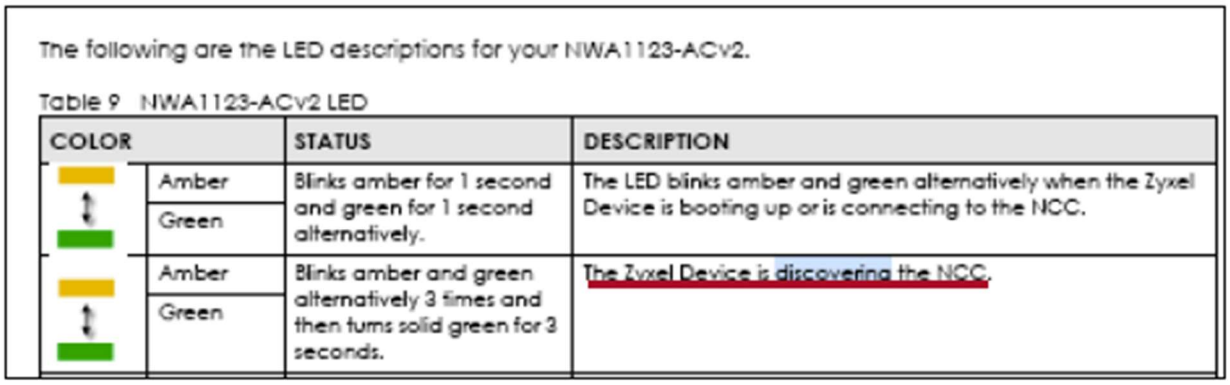
AC%20PRO_V6.25.pdf



What to benefit from Cloud central management?

When you're ready to join our Nebula cloud management solution, simply register your NWA1123-AC PRO* via Nebula Control Center and the device will automatically join, auto provision and begin to give real-time information. The intuitive platform allows you to group your access points together, control centrally, gain access to diagnostics

https://download.zyxel.com/NWA1123-AC_PRO/datasheet/NWA1123-AC%20PRO_10.pdf



The following are the LED descriptions for your NWA1123-ACv2.

Table 9 NWA1123-ACv2 LED

COLOR		STATUS	DESCRIPTION
	Amber / Green	Blinks amber for 1 second and green for 1 second alternatively.	The LED blinks amber and green alternatively when the Zyxel Device is booting up or is connecting to the NCC.
	Amber / Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC.

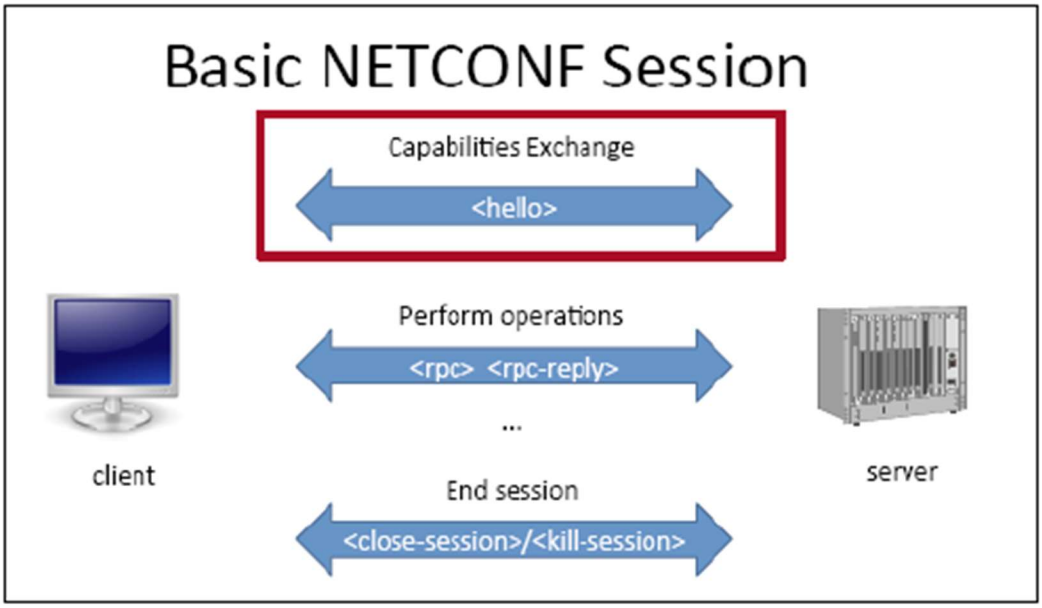
https://download.zyxel.com/NWA1123-AC_PRO/user_guide/NWA1123-AC%20PRO_V6.20.pdf

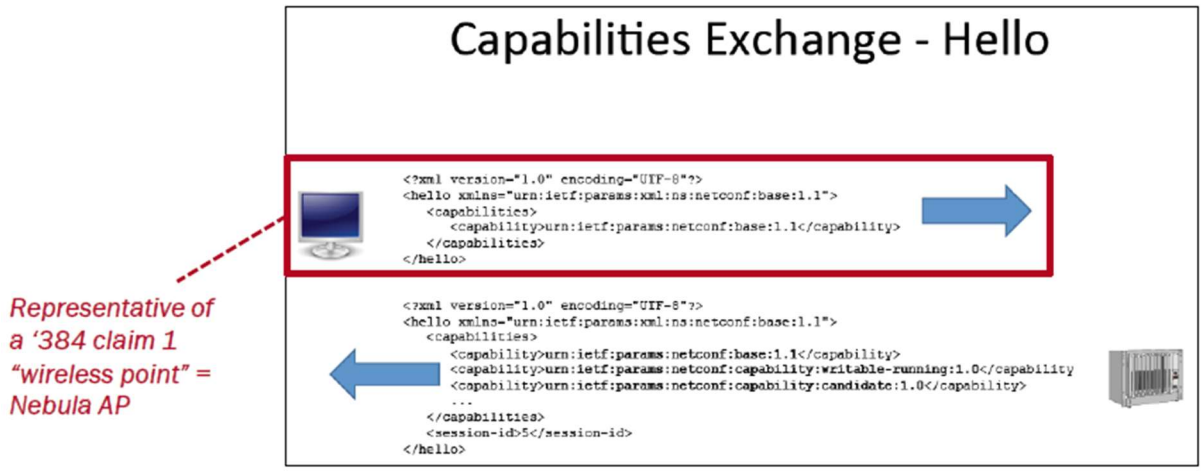
111. Discovery request messages are sent during the Nebula AP discovery and adoption process via the NETCONF protocol (via an AP/client initiated Hello call).

NETCONF Standard

Nebula is an industry-first solution that implements NETCONF protocol for safety of configuration changes in cloud management as all NETCONF messages are protected by TLS and exchanged using secure transports. Prior to NETCONF, CLI scripting and SNMP were two common approaches; but they have several limitations such as lacking of transaction management or useful standard security and commit mechanisms. The NETCONF protocol has been designed to address the shortcomings of the existing practices and protocols.

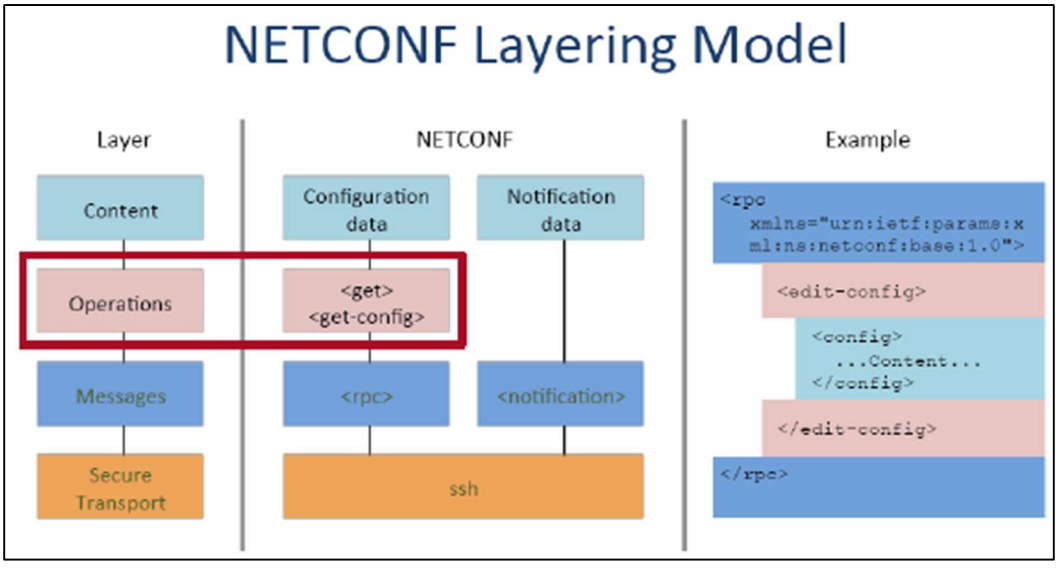
https://www.zyxel.com/library/assets/tech-library/Solution-Guide/Nebula_CC_Solution_Guide.pdf.

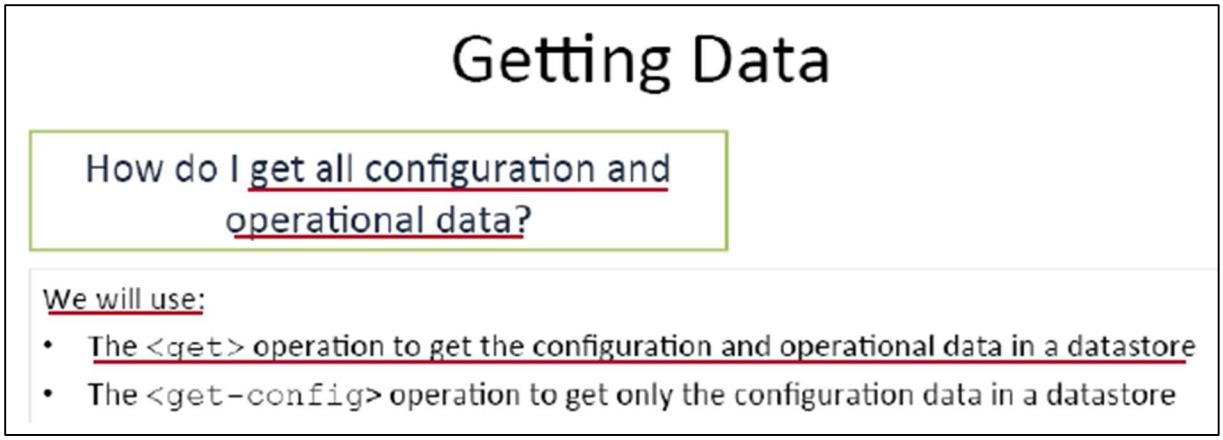


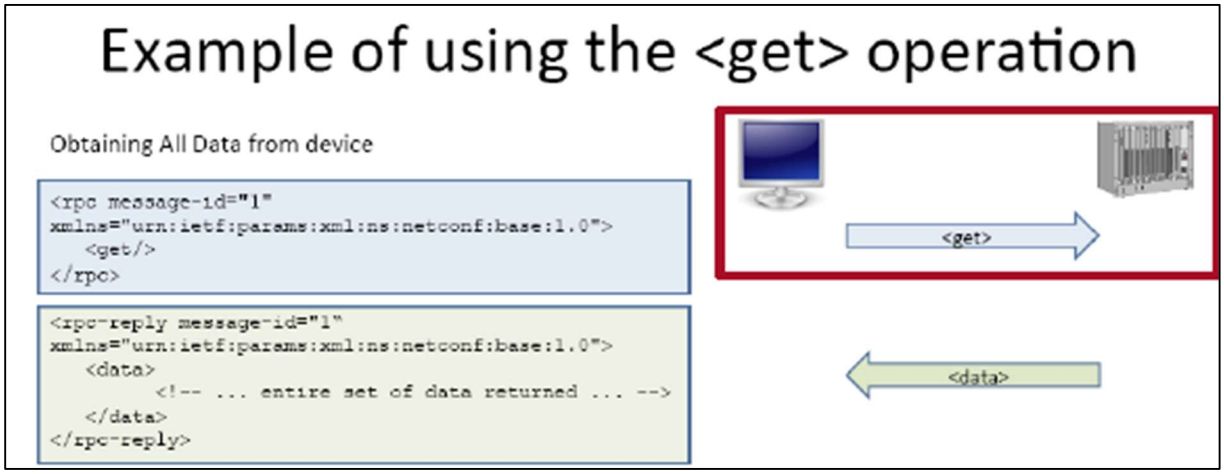


https://www.ietf.org/slides/slides-edu-network-configuration-with-netconf-00.pdf.

112. Infringing Nebula APs select a Nebula controller (one control node) based on a received discovery response message from the controller. Selecting is accomplished via the Nebula AP using a NETCONF <get> operation to obtain its configuration from the Nebula cloud controller. Further, according to the NETCONF protocol these discovery response messages include information regarding the functions offered by the control node

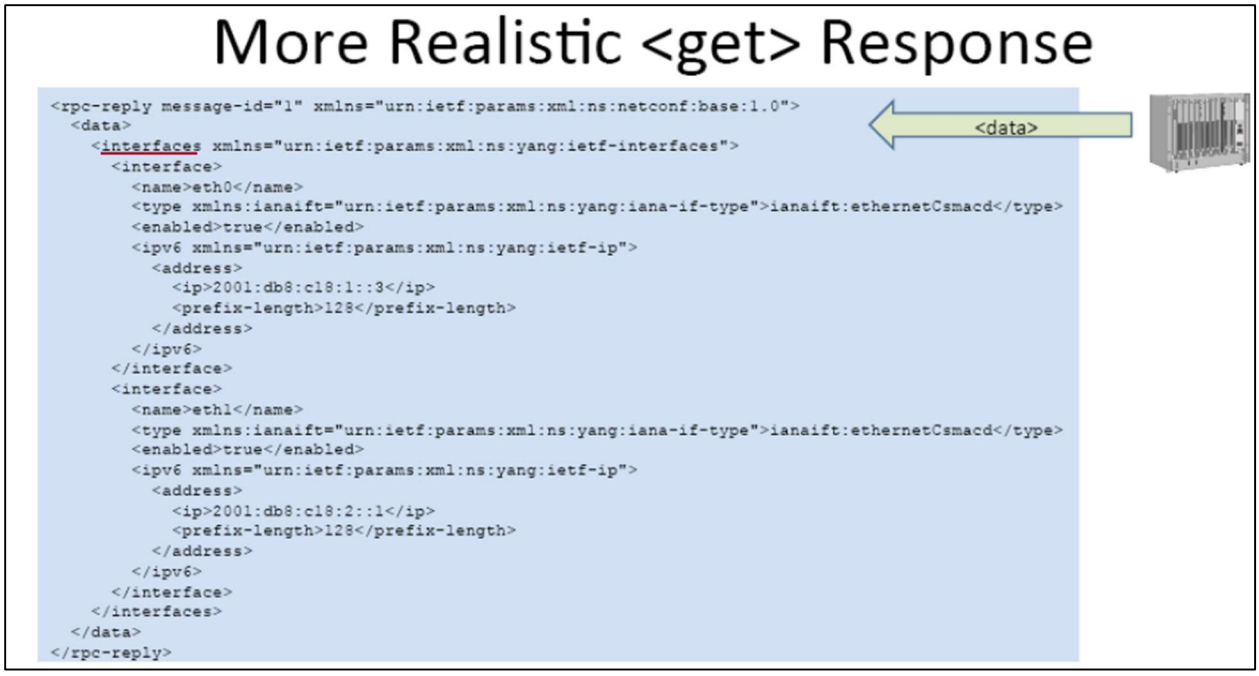






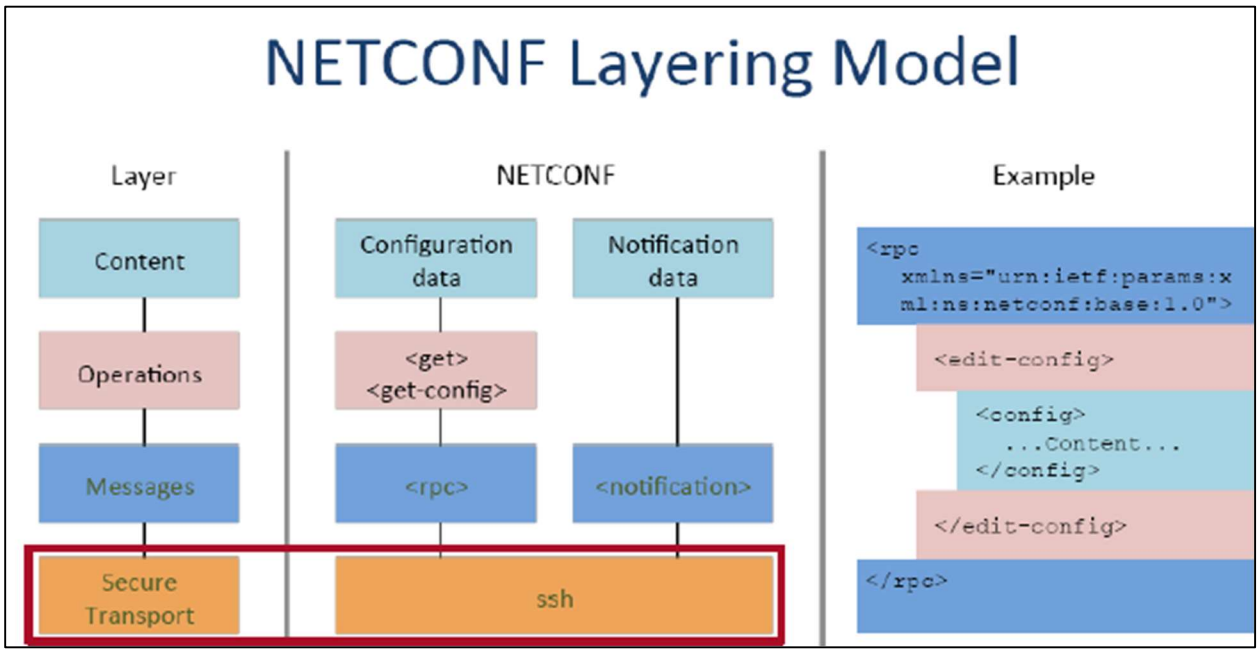
https://www.ietf.org/slides/slides-edu-network-configuration-with-netconf-00.pdf.

113. A discovery response message (The NETCONF server's a <get> response) to the client's <get> call includes information of functions offered by the control node, including without limitation, information regarding interfaces and addresses for the client to use.



https://www.ietf.org/slides/slides-edu-network-configuration-with-netconf-00.pdf.

114. During the adoption process the Nebula AP establishes a secure session with the chosen control node.



https://www.ietf.org/slides/slides-edu-network-configuration-with-netconf-00.pdf.

All Nebula devices are built from the ground up for cloud management with the capability to communicate with Nebula's cloud control center through the Internet. This TLS-secured connectivity between hardware and the cloud provides network-wide visibility and control for network management using the minimal bandwidth.

https://www.zyxel.com/library/assets/tech-library/Solution-Guide/Nebula_CC_Solution_Guide.pdf

115. Nebula APs use a negotiation unit (software on the AP including NETCONF implementation) to exchange information with the Nebula cloud controller about the functions to be separated between the controller and the AP.

Operations

NETCONF is an XML-formatted command and response protocol that runs primarily over Secure Shell (SSH) transport. The NETCONF protocol is analogous in some ways to traditional device console Command Line Interface (CLI), except that the XML-formatted commands and results are designed for management applications. Details of NETCONF communication between NNMi and therefore the managed device are transparent to the NNMi user. However, the subsequent overview could also be helpful for troubleshooting:

- A NETCONF client establishes an SSH connection with the NETCONF server on the managed device. Valid SSH user name and password credentials must be specified by the client and authenticated by the device.
- The client application and device exchange capabilities in the form of <hello> messages.
- The client initiates requests to the device in the form of Remote Procedure Call (RPC) messages; including standard <get> or <get-config> operations, plus any vendor-specific operations that are defined for the device.
- The device responds with results of the operations within the sort of RPC reply messages.
- When the client application has finished sending requests and processing the responses, it sends a <close-session> RPC message to the device.
- The device acknowledges with an <ok> RPC reply message.
- Finally, both sides terminate the SSH connection.

https://networkinterview.com/what-is-netconf-protocol/.

116. Additional Zyxel Accused Products with respect to the '384 patent

include the Zyxel Systems featuring Zyxel APs (including, for example, Zyxel NXC2500 and NXC5500 WLAN controllers) that support configuration using the CAPWAP protocol to provide service in a WLAN.

117. Zyxel APs support configuration using the CAPWAP protocol:

The Zyxel NXC2500 Wireless LAN Controller supports the management of the Zyxel Unified, Unified Pro and NWA5000 Managed Series of Access Points to provide complete wireless LAN functions for the business. As standard the Zyxel NXC2500 supports the initial management of 8 APs and provides scalability with a maximum supported total up to 64* APs, the "pay-as-you-grow" principle provides reassurance and future proofing for small and medium-sized businesses, hotels and educational institutes to implement secured, centralized wireless LAN networks.

https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/overview#benefits

Centralized management and provision

With demand for Internet connection of mobile devices growing rapidly, high scalability WLAN and centralized management become necessary for wireless device deployments. The Zyxel NXC5500 WLAN controller has great scalability to manage up to 1024 APs centrally. The NXC5500 utilizes CAPWAP protocol to minimize issues of Wi-Fi deployments that are new, or belong to extension programs on top of the existing networks.

https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC5500/overview#benefits

Wireless LAN Controller

NXC2500

Control and Provisioning

Model	NXC2500
Managed AP discovery	Broadcast/DHCP Option/DNS/Manual
CAPWAP	Yes

https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/specification

Wireless LAN Controller

NXC5500

Control and Provisioning

Model	NXC5500
Managed AP discovery	Broadcast/DHCP option/DNS/Manual
CAPWAP	Yes

https://www.zyxel.com/products_services/Wireless-LAN-Controller-

NXC5500/specification.

https://www.zyxel.com/products_services/Wireless-LAN-Controller-NXC2500/specification

118. Zyxel Access Points and Access Controllers support configuration using the CAPWAP protocol to separate WLAN functions between them.

This document describes the CAPWAP protocol, a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs). The CAPWAP protocol is defined to be independent of Layer 2 (L2) technology, and meets the objectives in "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)" [RFC4564].

1.1. Goals

The goals for the CAPWAP protocol are listed below:

1. To centralize the authentication and policy enforcement functions for a wireless network. The AC may also provide centralized bridging, forwarding, and encryption of user traffic. Centralization of these functions will enable reduced cost and higher efficiency by applying the capabilities of network processing silicon to the wireless network, as in wired LANs.

2. To enable shifting of the higher-level protocol processing from the WTP. This leaves the time-critical applications of wireless control and access in the WTP, making efficient use of the computing power available in WTPs, which are subject to severe cost pressure.

https://tools.ietf.org/html/rfc5415.

119. Zyxel APs send discovery requests to the one or more ACs in the network.

The CAPWAP Protocol begins with a Discovery phase. The WTPs send a Discovery Request message, causing any Access Controller (AC) receiving the message to respond with a Discovery Response message. From the Discovery Response messages received, a WTP selects an AC with which to establish a secure DTLS session. In order to establish the secure DTLS connection, the WTP will need some amount of pre-provisioning, which is specified in Section 12.5. CAPWAP protocol messages will be fragmented to the maximum length discovered to be supported by the network.

Discovery Thread: The AC's Discovery thread is responsible for receiving, and responding to, Discovery Request messages. The state machine transitions in Figure 4 are represented by numerals. Note that the Discovery thread does not maintain any per-WTP-specific context information, and a single state context exists. It is necessary for the AC to protect itself against various attacks that exist with non-authenticated frames. See Section 12 for more information.

Id.

120. Zyxel APs select an AC based on the discovery response message received, through which the AC advertises its services.

Upon receiving a Discovery Request message, the AC will respond with a Discovery Response message sent to the address in the source address of the received Discovery Request message. Once a Discovery Response has been received, if the WTP decides to establish a session with the responding AC, it SHOULD perform an MTU discovery, using the process described in Section 3.5.

5.2. Discovery Response Message

The Discovery Response message provides a mechanism for an AC to advertise its services to requesting WTPs.

When a WTP receives a Discovery Response message, it MUST wait for an interval not less than DiscoveryInterval for receipt of additional Discovery Response messages. After the DiscoveryInterval elapses, the WTP enters the DTLS-Init state and selects one of the ACs that sent a Discovery Response message and send a DTLS Handshake to that AC.

Id.

121. The AP establishes a secure DTLS session with the chosen AC.

The CAPWAP Protocol begins with a Discovery phase. The WTPs send a Discovery Request message, causing any Access Controller (AC) receiving the message to respond with a Discovery Response message. From the Discovery Response messages received, a WTP selects an AC with which to establish a secure DTLS session. In order to establish the secure DTLS connection, the WTP will need some amount of pre-provisioning, which is specified in Section 12.5. CAPWAP protocol messages will be fragmented to the maximum length discovered to be supported by the network.

Once the WTP and the AC have completed DTLS session establishment, a configuration exchange occurs in which both devices agree on version information. During this exchange, the WTP may receive provisioning settings. The WTP is then enabled for operation.

Id.

122. Zyxel APs contain a negotiation unit that sends functional information to the AC.

8.1.1. Configuration Flexibility

The CAPWAP protocol provides the flexibility to configure and manage WTPs of varying design and functional characteristics. When a WTP first discovers an AC, it provides primary functional information

relating to its type of MAC and to the nature of frames to be exchanged. The AC configures the WTP appropriately. The AC also establishes corresponding internal state for the WTP.

Id.

123. Zyxel APs contain a negotiation unit that sends functional information

to the AC. For example, functions may be split using two modes of operation: Split MAC and Local MAC.

> CAPWAP assumes a network configuration consisting of multiple WTPs communicating via the Internet Protocol (IP) to an AC. WTPs are viewed as remote radio frequency (RF) interfaces controlled by the AC. The CAPWAP protocol supports two modes of operation: Split and Local MAC (medium access control). In Split MAC mode, all L2 wireless data and management frames are encapsulated via the CAPWAP protocol and exchanged between the AC and the WTP. As shown in Figure 1, the wireless frames received from a mobile device, which is referred to in this specification as a Station (STA), are directly encapsulated by the WTP and forwarded to the AC.
>
> The Local MAC mode of operation allows for the data frames to be either locally bridged or tunneled as 802.3 frames. The latter implies that the WTP performs the 802.11 Integration function. In either case, the L2 wireless management frames are processed locally

Id.

124. As another example, functions may also be split using two modes of encapsulation, including 802.3 and native wireless.

> **4.4.2. Data Payload**
>
> A CAPWAP protocol Data Payload packet encapsulates a forwarded wireless frame. The CAPWAP protocol defines two different modes of encapsulation: IEEE 802.3 and native wireless. IEEE 802.3 encapsulation requires that for 802.11 frames, the 802.11 *Integration* function be performed in the WTP. An IEEE 802.3-encapsulated user payload frame has the following format:
>
> ```
> +-----------------------------------------------------+
> | IP Header | UDP Header | CAPWAP Header | 802.3 Frame |
> +-----------------------------------------------------+
> ```
>
> The CAPWAP protocol also defines the native wireless encapsulation mode. The format of the encapsulated CAPWAP Data frame is subject to the rules defined by the specific wireless technology binding. Each wireless technology binding MUST contain a section entitled "Payload Encapsulation", which defines the format of the wireless payload that is encapsulated within CAPWAP Data packets.
>
> For 802.3 payload frames, the 802.3 frame is encapsulated (excluding the IEEE 802.3 Preamble, Start Frame Delimiter (SFD), and Frame Check Sequence (FCS) fields). If the encapsulated frame would exceed the transport layer's MTU, the sender is responsible for the fragmentation of the frame, as specified in Section 3.4. The CAPWAP protocol can support IEEE 802.3 frames whose length is defined in the IEEE 802.3as specification [FRAME-EXT].

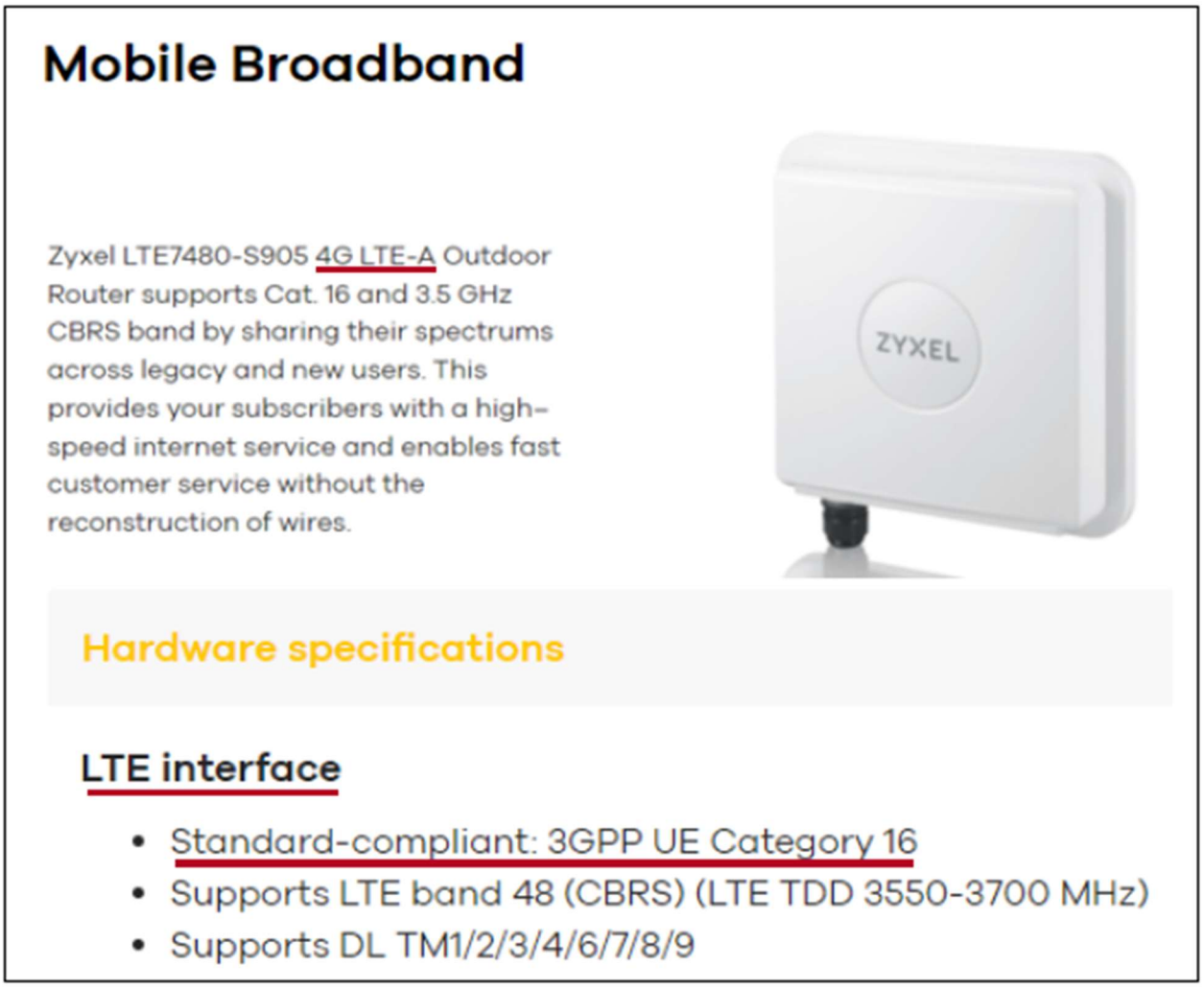
Id.

ZYXEL INFRINGES U.S. PATENT NO. 8,442,569.

125. The Patent Office issued U.S. Patent No. 8,442,569, titled "Radio Reception Apparatus, Radio Transmission Apparatus, and Radio Communication Method," on May 14, 2013, after a thorough examination and determination that the subject matter claimed is patentable.

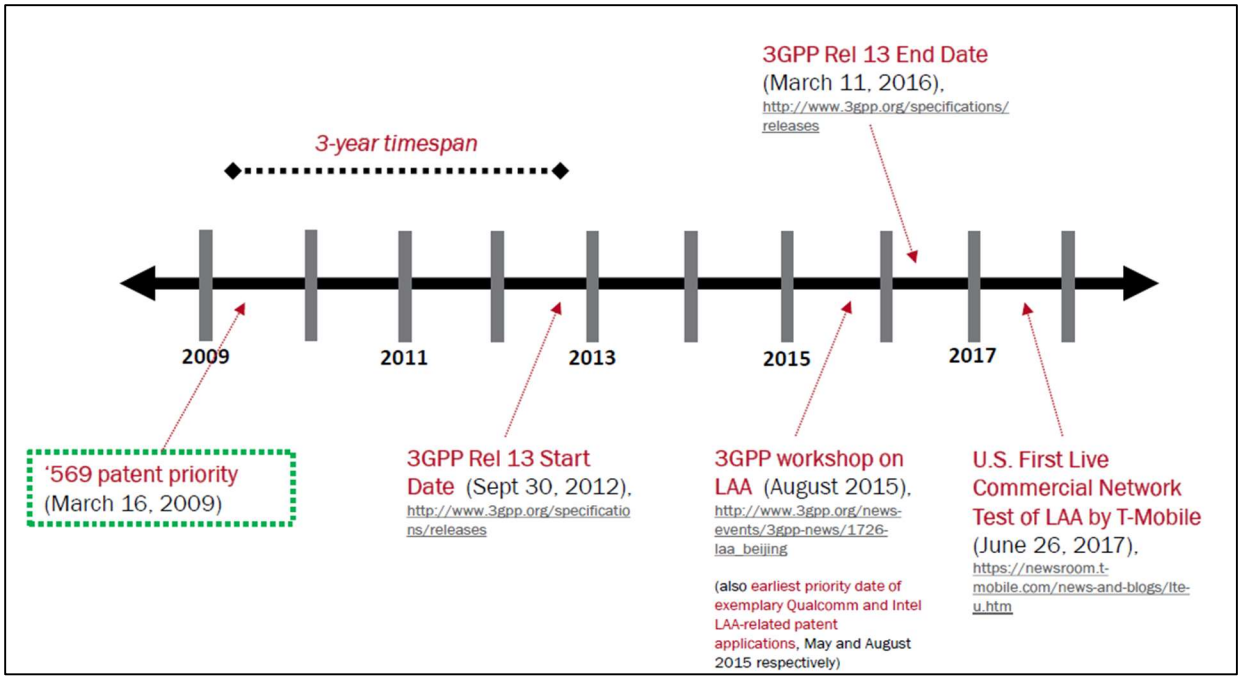
126. Zyxel Accused Products with respect to the '569 patent include the Zyxel devices that support License-Assisted Access (LAA), a plank of LTE-Advance. Zyxel's 5G NR/4G LTE CPE (under its Service Provider products) and its Mobile Broadband 4G LTE products (under its Business products) are exemplary infringing products enabled for LAA.

https://service-provider.zyxel.com/na/en/products/5g-nr4g-lte-cpe/4g-lte-cpe/idus/lte5388-s905#specifications/.



https://www.zyxel.com/us/en/products_services/4G-LTE-Advanced-Outdoor-Router-LTE7480-S905/specifications.

127. The '569 patent family predates standardization and implementation of LTE-Advanced Licensed Assisted Access (LAA).



128. LAA uses a discovery reference signal (DRS) for cell detection, synchronization, and radio resource management (RRM) measurement.

3.1.8.3 Physical Channels and Signals in an LAA SCell

LAA SCell supports:

- PDSCH, (E)PDCCH, CRS, CSI-RS and DRS

LAA SCell does not support:

- PHICH, PBCH and PMCH

Discovery reference signal (DRS)

DRS is 1ms (or 12 OFDM symbols) long and is transmitted at most once in any sub-frame during periodical occasions refereed as DRS measurement timing configuration (DMTC). The DMTC occasions have duration of 6 ms and a configurable period of 40 ms, 80 ms or 160 ms.

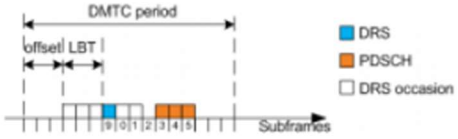


Figure 3-35: DRS allocation

DRS	= Discovery reference signal
LBT	= Listen-before-talk
DMTC	= DRS measurement timing configuration
DRS occasion	= Subframes during the DMTC period where DRS can occur
PDSCH	= Physical DL shared channel

129. LAA user equipment (UE) are radio reception apparatuses used in radio communication systems, such as cellular phone networks. LAA UE use certain cellular modems that are enabled to perform Licensed-Assisted Access using a primary cell (PCell) and one or more secondary cells (SCell).

5.7 Licensed-Assisted Access

Carrier aggregation with at least one SCell operating in the unlicensed spectrum is referred to as Licensed-Assisted Access (LAA). In LAA, the configured set of serving cells for a UE therefore always includes at least one SCell operating in the unlicensed spectrum according to Frame structure Type 3, also called LAA SCell. Unless otherwise specified, LAA SCells act as regular SCells and are limited to downlink transmissions in this release.

If the absence of IEEE802.11n/11ac devices sharing the carrier cannot be guaranteed on a long term basis (e.g., by level of regulation), and for this release if the maximum number of unlicensed channels that E-UTRAN can simultaneously transmit on is equal to or less than 4, the maximum frequency separation between any two carrier center frequencies on which LAA SCell transmissions are performed should be less than or equal to 62MHz. The UE is required to support frequency separation in accordance with TS 36.133 [21].

LAA eNB applies Listen-Before-Talk (LBT) before performing a transmission on LAA SCell. When LBT is applied, the transmitter listens to/senses the channel to determine whether the channel is free or busy. If the channel is determined to be free, the transmitter may perform the transmission; otherwise, it does not perform the transmission. If an LAA eNB uses channel access signals of other technologies for the purpose of LAA channel access, it shall continue to meet the LAA maximum energy detection threshold requirement.

The combined time of transmissions compliant with the channel access procedure described in section 15.1.2 of [6] by an eNB should not exceed 50 ms in any contiguous 1 second period on an LAA cell.

ETSI TS 136 300 V13.10.0 (2018-01)

http://www.etsi.org/deliver/etsi_ts/136300_136399/136300/13.10.00_60/ts_136300v131000p.pdf.

130. In both the LTE downlink and uplink, resources are defined by Resource Elements, which are mapped into Resource Blocks. *See, e.g.*, https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma245/1MA245_2e_LTE_Vulnerabilities.pdf,

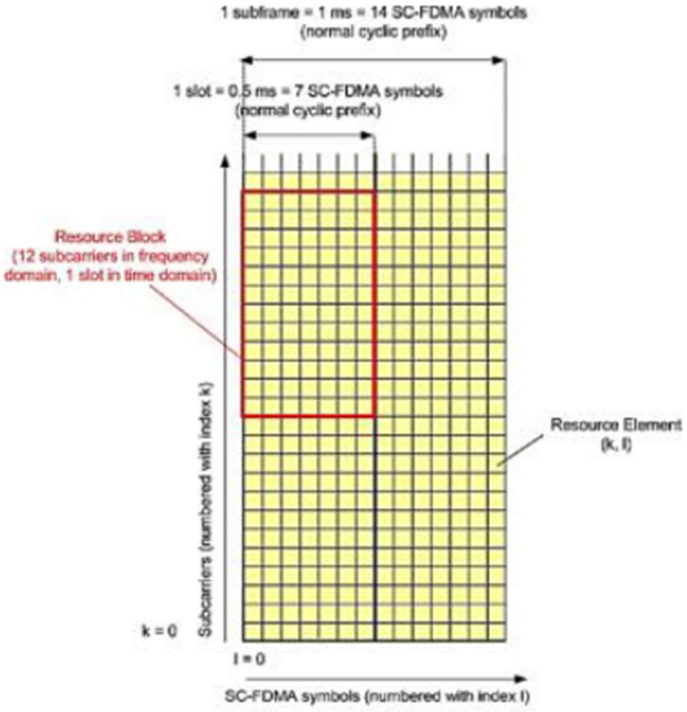


Fig. 2-2: Formation of a resource grid [1]

Fig. 2-2 shows the content of a resource grid. Each single element in the resource block is called a Resource Element (RE). A resource block consists of 12 consecutive subcarriers in the frequency domain and 7 OFDM symbols in the time domain [3]. This technique of mapping information into blocks with regard to time and frequency makes it possible for the interference or jamming to be selective with regards to information.

2.2.1.3 Downlink Data Transmission

Data is allocated to a device (User Equipment, UE) in terms of resource blocks, i.e. one UE can be allocated integer multiples of one resource block in the frequency domain. These resource blocks do not have to be adjacent to each other. In the time domain, the scheduling decision can be modified every transmission time interval of 1

2.2.2.3 Uplink Data Transmission

Scheduling of uplink resources is done by eNodeB. The eNodeB assigns certain time/frequency resources to the UEs and informs UEs about transmission formats to be used. The scheduling decisions may be based on QoS parameters, UE buffer status, uplink channel quality measurements, UE capabilities, UE measurement gaps, etc. In the uplink, data is allocated in multiples of one resource block. Uplink resource block size in the frequency domain are 12 subcarriers, i.e. the same as in downlink. However, not all integer multiples are allowed in order to simplify the DFT design in the uplink signal processing and so only factors 2, 3, and 5 are allowed.

131. LTE uses Orthogonal Frequency Division Multiple Access (OFDMA) for its downlink transmission scheme, in which each of the OFDMA subcarriers carries a separate stream of information mapped in both the frequency and time domains (i.e. defined in a frequency-time domain).

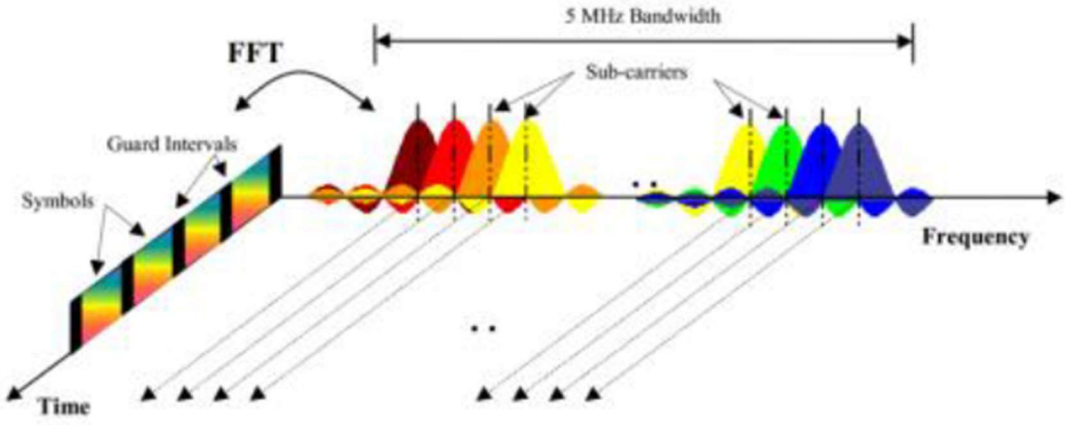
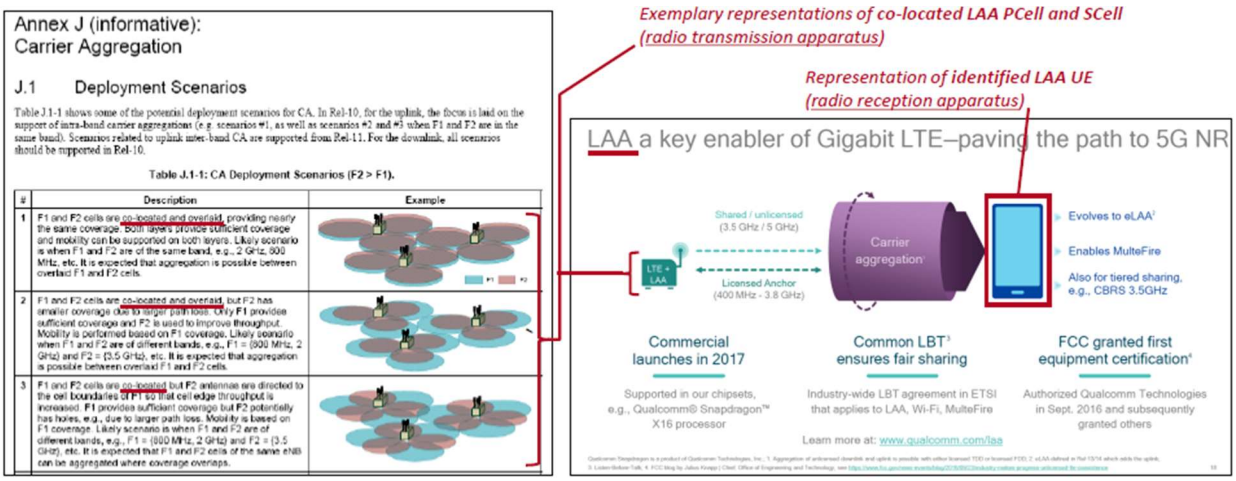


Fig. 2-1: Frequency- Time representation of an OFDM signal [2]

132. SC-FDMA (Single Carrier Frequency Division Multiple Access), which is used for the LTE UE's uplink transmission scheme, similarly allocates resources in a frequency-time domain.

133. In an applicable use case, an identified LAA UE (radio reception apparatus) is communicating via LAA with a base station comprising co-located PCell and SCell (radio transmission apparatus). The PCell represents a first communication system (i.e. LTE over licensed spectrum) and the SCell represents a second communication system (i.e. LTE over unlicensed spectrum).



http://www.etsi.org/deliver/etsi_ts/136300_136399/136300/13.10.00_60/ts_136300v131000p.pdf (pg. 305); https://www.mobiusconsulting.com/papers/the-essential-role-of-gigabit-lte-lte-advanced-pro-in-a-5g-world.pdf

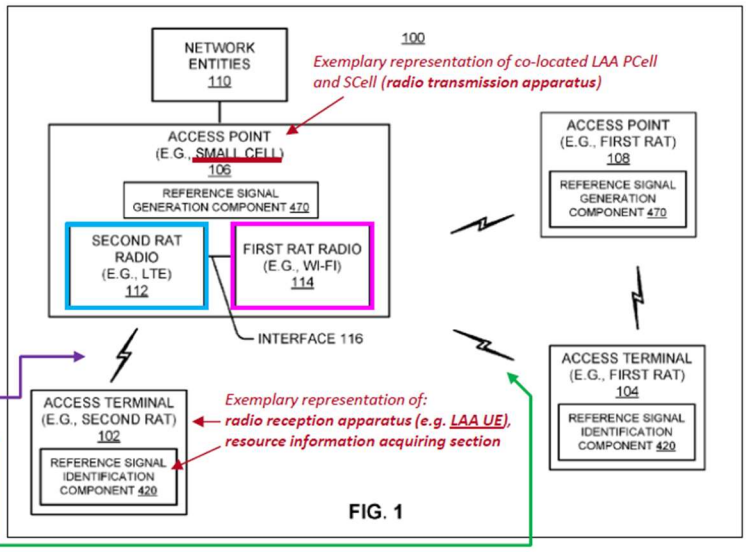
134. Each of the PCell and the SCell of the radio transmission apparatus transmit a reference signal—in the considered use case the PCell transmits a first reference signal and the SCell transmits a second reference signal. The radio transmission apparatus radios share physical-layer transmission information, such as the location of a DRS (distribution resource information), to allow the UE to properly detect and descramble DRS via the UE's resource information acquiring section, which US20170134148A1 (*see* below) labels the UE's "reference signal identification component".

- https://patents.google.com/patent/US20170134148A1 (emphasis added below)
- "The present aspects generally relate to transmitting and receiving transmissions including physical layer reference signals. For example, a discovery reference signal (DRS) may include physical-layer signals, such as a primary synchronization signal (PSS), a secondary synchronization signal (SSS), and a cell-specific reference signal (CRS). A user equipment (UE) may use a DRS to identify, select, and synchronize with a cell (e.g. of a base station such as an evolved Node B). Other physical-layer reference signals may include, but are not limited to, a channel state information reference signal (CSI-RS) and/or a channel-state information—interference measurement (CSI-IM) signal, such as for radio resource management (RRM) measurements and/or channel estimation (e.g., channel quality indicator (CQI)) measurements." [0031]
- "In an aspect, the UE may periodically or aperiodically measure physical-layer reference signals transmitted by neighbor cells to determine whether to select the neighbor as a new cell for service." [0032]
- "Moreover, in the LAA context, the DRS may be transmitted periodically or aperiodically, either by design or based on clear channel assessment (CCA) or listen before talk (LBT) restrictions on transmitting in unlicensed spectrum. As such, the UE may receive the DRS at a variable timing with respect to the discovery window. This variable timing, along with the fact that the UE may not know the timing of the transmitting neighboring cell, may cause problems for the UE in relation to cell detection, synchronization, and neighbor cell measurement." [0033]

135. Qualcomm U.S Patent Application Publication US20170134148A1 (earliest priority 11/6/2015, published 5/11/2017) titled "Discovery reference signal configuration and scrambling in license-assisted access," is illustrative of identified radio reception apparatuses using such a receiver.

- "The disclosure relates in some aspects to techniques referred to herein as carrier sense adaptive transmission (CSAT), which may be used to facilitate co-existence between different technologies operating on a commonly used resource (e.g., a particular unlicensed RF band or co-channel). The access point 106 includes co-located radios (e.g., transceivers) 112 and 114. The radio 112 uses a second RAT (e.g., LTE) to communicate. The radio 114 is capable of receiving signals using a first RAT (e.g., Wi-Fi). In addition, an interface 116 enables the radios 112 and 114 to communicate with one another. In another aspect, the **radio 114 may communicate using a second RAT (e.g., LTE in unlicensed spectrum) that is related to the first RAT (e.g., LTE in licensed spectrum)**. Radios 112, 114 may share physical-layer transmission information, such as the location of a DRS. **Accordingly, the second radio 112 may transmit a DRS in a secondary component carrier while the first radio 114 sends an indication of the placement of the DRS on a primary component carrier**." [0045] (emphasis added)

Exemplary representations of :
- ***distribution resource information for a second reference signal***
- ***second reference signal***
- ***second communication system***
- ***first reference signal***
- ***first communication system***



136. This patent publication describes techniques for detecting and descrambling discovery reference signals (DRS) by user equipment (UE) using licensed-assisted access (LAA) in an unlicensed spectrum. UE uses the detected DRS for neighbor cell measurements related to processes like cell selection in the

unlicensed spectrum. UE receives a DRS in a subframe, with a transceiver, processor, and memory component supporting communication. DRS includes physical layer signals such as primary/secondary synchronization signals (PSS/SSS) and cell-specific reference signals (CRS) used for cell identification and synchronization. The UE's receivers process RF signals and forward information to the RX processor for Layer 1 (L1) signal processing.

137. In a downlink (DL) frame structure in LTE, a frame (10 ms) is divided into 10 subframes, each containing two time slots and represented by a resource grid. Resource grid contains resource elements (REs), some designated for downlink reference signals (DL-RS) like cell-specific RS (CRS) and UE-specific RS (UE-RS). Subframes with a discovery reference signal (DRS) also contain resource elements for PSS, SSS, and CSI-RS, with UE rate-matching around DRS elements to transmit a transport block. Reference signals include PSS, SSS, CRS, CSI-RS, and other signals to facilitate UE connection with a network entity.

138. Fig. 3B of Qualcomm US20170134148A1 is shown below. The distributed type resources (identified above) are resources "in which a resource unit defined in the frequency-time domain is divided in a time direction and distributed at predetermined frequency intervals."

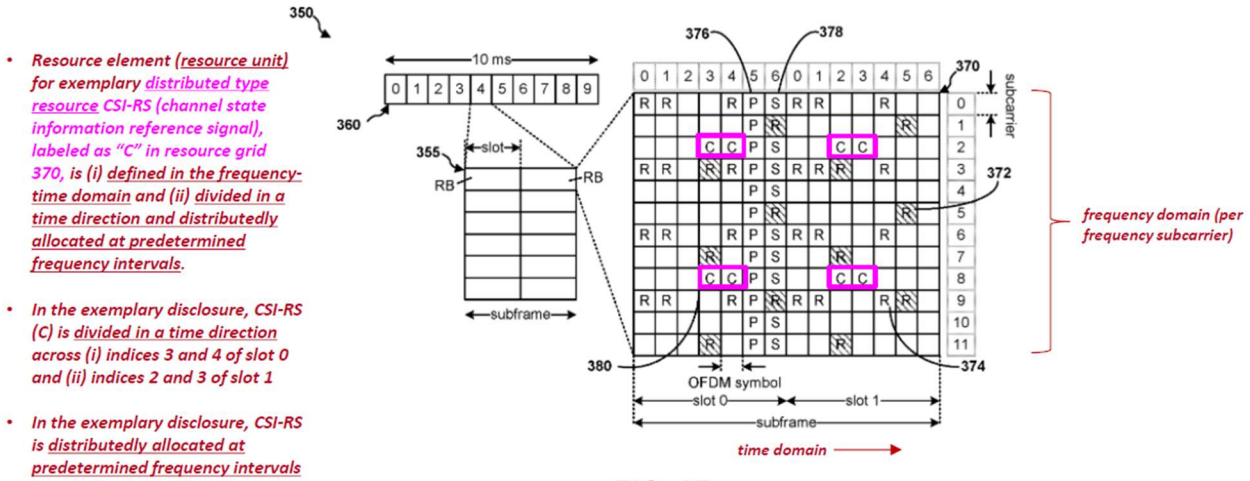


FIG. 3B

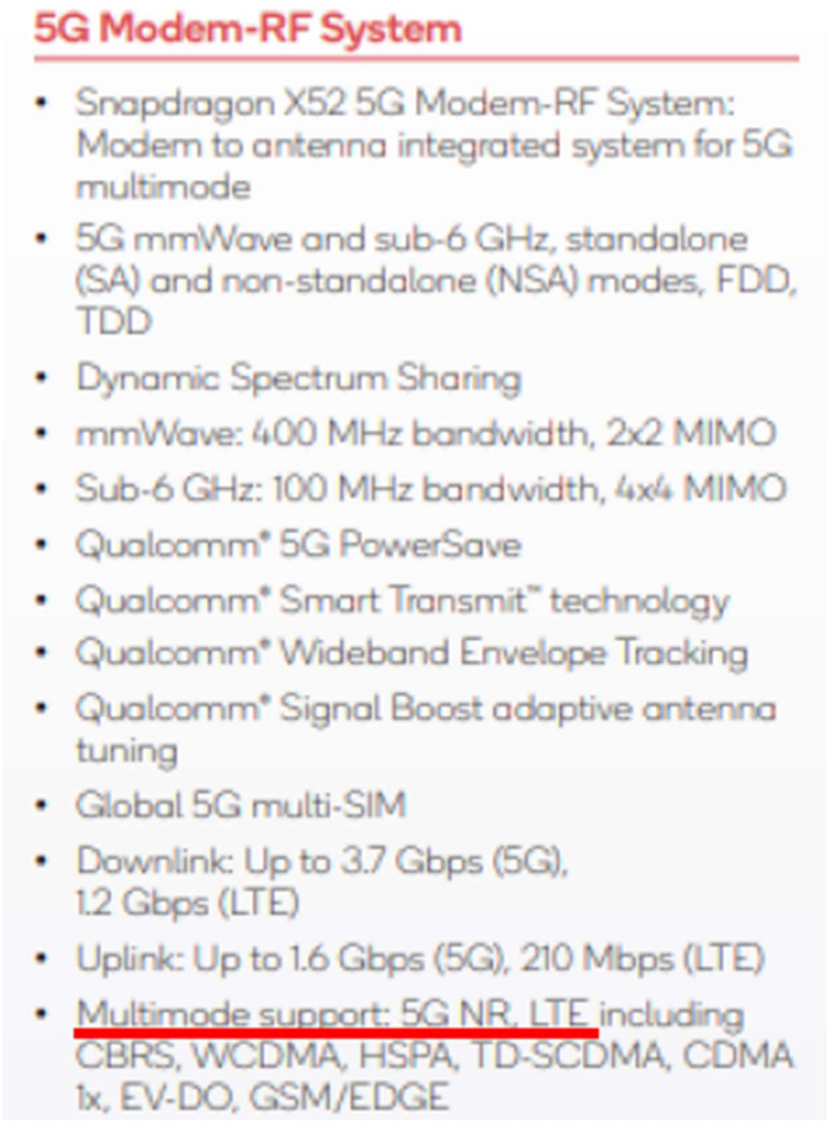
139. Each of the identified LAA UE (each a radio reception apparatus) includes a receiver that is configured to receive a DRS from a LAA SCell (i.e. to receive a signal containing the second reference signal transmitted from the transmission apparatus). For example, the Snapdragon mobile platform used by exemplary LAA UE includes an LTE modem that contains an RF transceiver, which comprises and transmitter and a receiver.

140. Zyxel 5G products feature Qualcomm's Snapdragon x55 chipset.

5G technology partners

Zyxel's 5G products are built on Qualcomm's leading Snapdragon x55 chipset in conjunction with Quectel module technology. We start releasing our 5G product portfolio with weather hardened outdoor units, ready to be easily mounted on the outside of buildings or poles, yielding the best possible conditions for 5G FWA connectivity.

https://www.zyxel.com/service-provider/global/en/news/solutions-products/zyxel-ready-5g-samples-august-2019.



5G Modem-RF System

- Snapdragon X52 5G Modem-RF System: Modem to antenna integrated system for 5G multimode
- 5G mmWave and sub-6 GHz, standalone (SA) and non-standalone (NSA) modes, FDD, TDD
- Dynamic Spectrum Sharing
- mmWave: 400 MHz bandwidth, 2x2 MIMO
- Sub-6 GHz: 100 MHz bandwidth, 4x4 MIMO
- Qualcomm® 5G PowerSave
- Qualcomm® Smart Transmit™ technology
- Qualcomm® Wideband Envelope Tracking
- Qualcomm® Signal Boost adaptive antenna tuning
- Global 5G multi-SIM
- Downlink: Up to 3.7 Gbps (5G), 1.2 Gbps (LTE)
- Uplink: Up to 1.6 Gbps (5G), 210 Mbps (LTE)
- Multimode support: 5G NR, LTE including CBRS, WCDMA, HSPA, TD-SCDMA, CDMA 1x, EV-DO, GSM/EDGE

https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/snapdragon_750g_5g_mobile_platform_product_brief_0.pdf

141. Each of the identified LAA UE includes a channel quality measuring section that is configured to measure a channel quality of a transmission channel by using the received DRS from a LAA SCell (SCell's DRS being a second reference signal). For example, the Snapdragon mobile platform of exemplary LAA UE includes contain components evidencing the presence of a channel

quality measuring section.

https://www.qualcomm.com/news/onq/2018/01/why-qualcomm-uniquely-positioned-become-leader-rffe.

https://www.qualcomm.com/media/documents/files/making-5g-nr-a-commercial-reality.pdf (slide 31)

142. Each of the identified LAA UE includes a channel quality measuring section that is configured to measure a channel quality of a transmission channel by using the received DRS from a LAA SCell (SCell's DRS being a second reference signal). Qualcomm's US20170134148A1 is illustrative of the identified radio reception apparatuses including a channel quality measuring section.

- "A user equipment (UE) may use a DRS to identify, select, and synchronize with a cell (e.g. of a base station such as an evolved Node B). Other physical-layer reference signals may include, but are not limited to, a channel state information reference signal (CSI-RS) and/or a channel-state information–interference measurement (CSI-IM) signal, such as for radio resource management (RRM) measurements and/or channel estimation (e.g., **channel quality indicator (CQI)**) measurements." [0031]
- "In another aspect, reference signal identification component 420 may include **channel state determination component** 444, which may be configured to determine channel state information (CSI) resources based on a received reference signal. In an aspect, for example, UE 402 may receive a DRS in the form of a cell-specific resource signal (CRS). UE 402 may use relative position determination component 440 to determine the relative position of the CRS in relation to the discovery window. UE 402 may, in an aspect, use **channel state determination component** 444 to determine whether **CSI resources** are present. In an aspect, the determination may be based on the relative position of the subframe including the CRS in relation to the discovery window." [0072]
- "For example, **UE 402 may use CSI-RS resources for different processes, such as for periodic CSI-RS transmission configuration, for radio resource management (RRM) measurements, and/or, for channel estimates**. In an aspect, the CSI-RS resources may be configured for each of these processes independently. In order to avoid collisions, UE 402 and/or network entity 404 may restrict the processes that by access and/or use the CSI-RS resources. For example, UE 402 may be restricted to use CSI-RS for only one of RRM measurements or channel determinations (e.g., channel measurements for determining a **channel quality indicator (CQI)**, channel estimates, and/or determining reference signal received power (RSRP)). In an aspect, UE 402 may also use the CSI-RS for channel state information when processing a DRS (e.g., a CRS). In such instances, the CSI-RS resources used for the DRS and for other processes (e.g., RRM measurement, etc.) may be identical. In an aspect, this may prevent UE 402 from configuring CSI-RS resources using the last two symbols in a subframe." [0073]

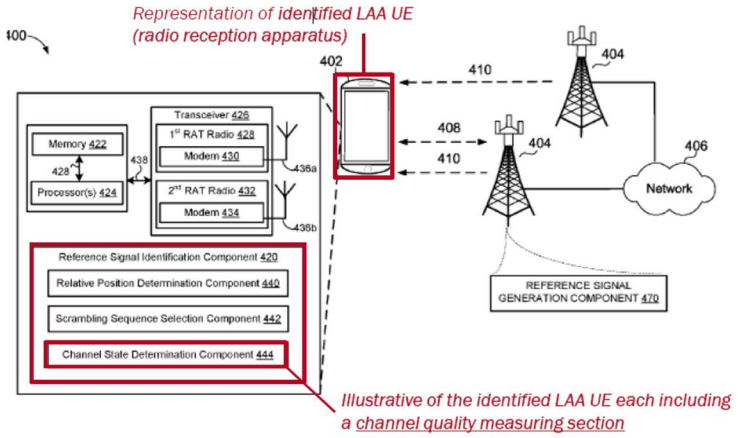


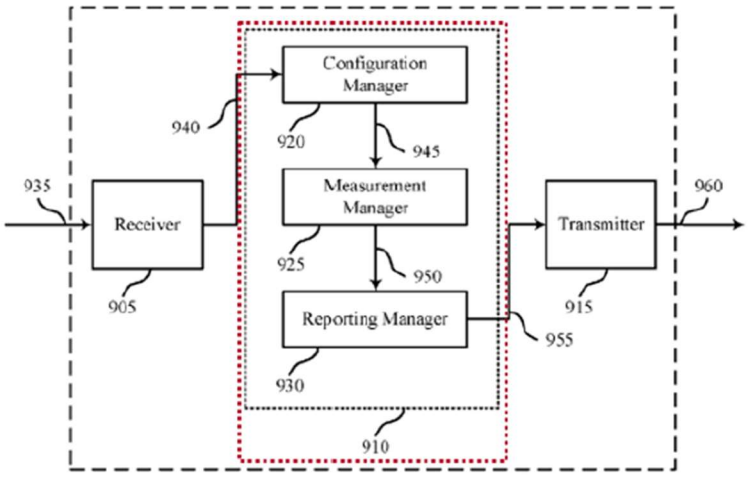
FIG. 4

https://patents.google.com/patent/US20170134148A1/en?oq=US20170134148A1

143. The identified LAA UE each contain a RF transceiver, which includes a transmitter—the transmitter is configured to transmit feedback information containing channel quality information to a transmission apparatus such as an LAA small cell operating co-located LAA PCell and SCell.

144. The transmitter (a feedback information transmitter) is the identified LAA UE being configured to send RRM measurement reports to the transmission apparatus, with the RRM measurement reports containing channel quality feedback information such as the channel quality indicator (CQI)) measurements discussed in Qualcomm US20170134148A1.

145. Additionally, Qualcomm US20160338118A1 (Nov. 17, 2016), titled "RRM measurement and reporting for license assisted access," discloses a "RRM measurement and reporting manager" that interfaces with a LAA UE's transmitter, as shown in Fig. 9 (depicted below).

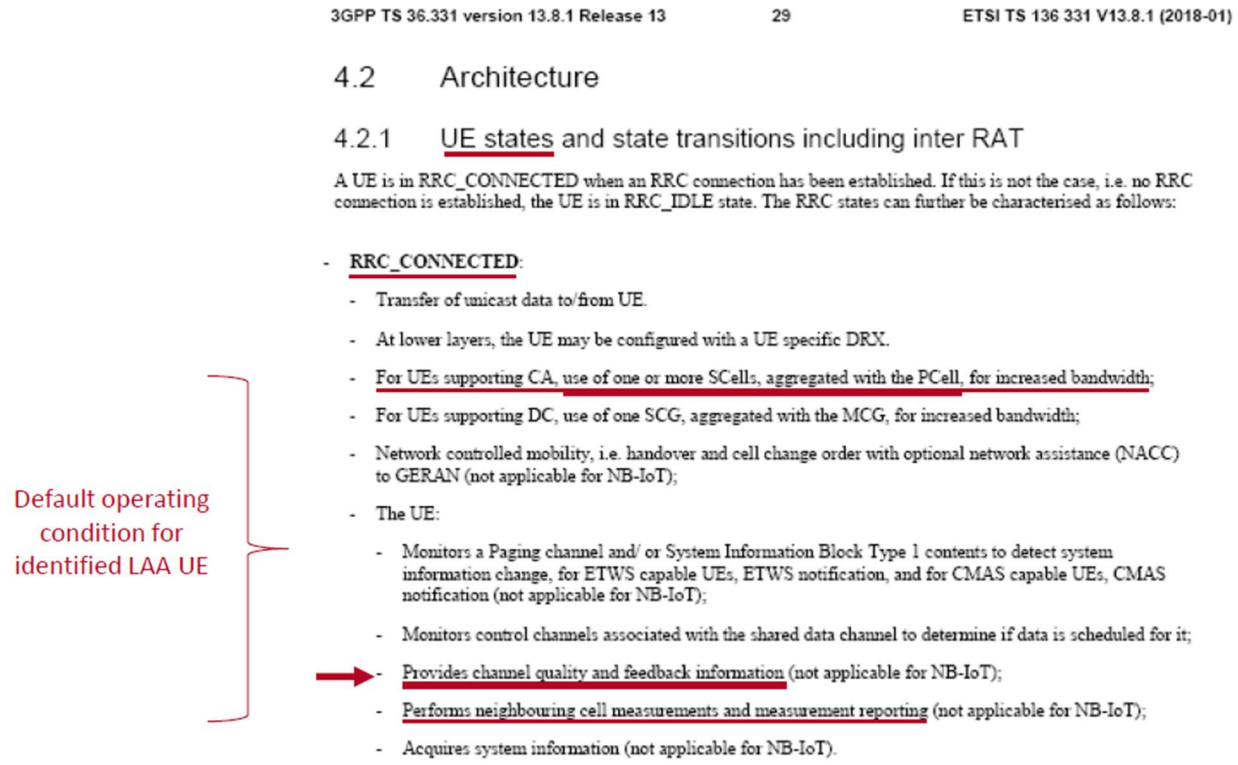


*"Wireless device **900** may include a receiver **905**, a **RRM measurement and reporting manager 910**, or a **transmitter 915**."* [0098] (emphasis added)

https://patents.google.com/patent/US20160338118A1/en

146. A LAA UE's transmitter transmits channel quality feedback

information to LAA small cells.



http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_136331v130801p.pdf.

147. CSI-RS is used by the identified LAA UE (radio reception apparatus) to estimate the channel being measured and report its channel quality information (CQI) to the radio transmission apparatus (e.g. LAA small cell). The identified LAA UE are configured to measure CSI-RS based discovery reference signals.

– *MeasResults*

The IE *MeasResults* covers measured results for intra-frequency, inter-frequency and inter- RAT mobility.

measResultCSI-RS-List   Measured results of the CSI-RS resources in discovery signals measurement.

UE-EUTRA-Capability field descriptions	*FDD/ TDD diff*
crs-DiscoverySignalsMeas Indicates whether the UE supports CRS based discovery signals measurement, and PDSCH/EPDCCH RE mapping with zero power CSI-RS configured for discovery signals.	FFS
csi-RS-DiscoverySignalsMeas Indicates whether the UE supports CSI-RS based discovery signals measurement. If this field is included, the UE shall also include *crs-DiscoverySignalsMeas*.	FFS
discoverySignalsInDeactSCell Indicates whether the UE supports the behaviour on DL signals and physical channels when SCell is deactivated and discovery signals measurement is configured as specified in TS 36.211 [21, 6.11A]. This field is included only if UE supports carrier aggregation and includes *crs-DiscoverySignalsMeas*.	FFS

Including **LAA**

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_136331v130801p.pdf.

148. CSI measurements involve measuring RSRP and RSRQ.

5.5.3 Performing measurements

5.5.3.1 General

For all measurements, except for UE Rx–Tx time difference measurements, RSSI, UL PDCP Packet Delay per QCI measurement, channel occupancy measurements, and except for WLAN measurements of Band, Carrier Info, Available Admission Capacity, Backhaul Bandwidth, Channel Utilization, and Station Count, the UE applies the layer 3 filtering as specified in 5.5.3.2, before using the measured results for evaluation of reporting criteria or for measurement reporting.

The UE shall:

1> whenever the UE has a *measConfig*, perform RSRP and RSRQ measurements for each serving cell as follows:

2> for the PCell, apply the time domain measurement resource restriction in accordance with *measSubframePatternPCell*, if configured;

5> if the UE supports CSI-RS based discovery signals measurement; and

5> if the *eventId* in the associated *reportConfig* is set to *eventC1* or *eventC2*, or if *reportStrongestCSI-RSs* is included in the associated *reportConfig*:

CSI-RS = Channel State Information Reference Signal

6> perform the corresponding measurements of CSI-RS resources on the frequency indicated in the concerned *measObject*, applying the discovery signals measurement timing configuration in accordance with *measDS-Config* in the concerned *measObject*;

6> if *reportCRS-Meas* is included in the associated *reportConfig*, perform the corresponding measurements of neighbouring cells on the frequencies indicated in the concerned *measObject* as follows:

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_136331v130801p.pdf.

149. CSI-RS measurements are based on RSRP, RSRQ, and RSSI, as measured by the LAA UE via RRM measurements.

6.3.6 Other information elements

– *UE-EUTRA-Capability*

The IE *UE-EUTRA-Capability* is used to convey the E-UTRA UE Radio Access Capability Parameters, see TS 36.306 [5], and the Feature Group Indicators for mandatory features (defined in Annexes B.1 and C.1) to the network. The IE *UE-EUTRA-Capability* is transferred in E-UTRA or in another RAT.

crossCarrierSchedulingLAA-DL
Indicates whether the UE supports cross-carrier scheduling from a licensed carrier for LAA cell(s) for downlink. This field can be included only if *downlinkLAA* is included.

csi-RS-DRS-RRM-MeasurementsLAA
Indicates whether the UE supports performing RRM measurements on LAA cell(s) based on CSI-RS-based DRS. This field can be included only if *downlinkLAA* is included.

downlinkLAA
Presence of the field indicates that the UE supports downlink LAA operation including identification of downlink transmissions on LAA cell(s) for full downlink subframes, decoding of common downlink control signalling on LAA cell(s), CSI feedback for LAA cell(s), RRM measurements on LAA cell(s) based on CRS-based DRS.

rssi-AndChannelOccupancyReporting
Indicates whether the UE supports performing measurements and reporting of RSSI and channel occupancy. This field can be included only if *downlinkLAA* is included.

ETSI TS 136 331 V13.8.1 (2018-01)

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_136331v130801p.pdf.

5.1.1 Reference Signal Received Power (RSRP)

Definition	Reference signal received power (RSRP), is defined as the linear average over the power contributions (in [W]) of the resource elements that carry cell-specific reference signals within the considered measurement frequency bandwidth. For RSRP determination the cell-specific reference signals R_0 according to TS 36.211 [3] shall be used. If the UE can reliably detect that R_1 is available it may use R_1 in addition to R_0 to determine RSRP.
	If higher layers indicate measurements based on discovery signals, the UE shall measure RSRP in the subframes in the configured discovery signal occasions. For frame structure 1 and 2, if the UE can reliably detect that cell-specific reference signals are present in other subframes, the UE may use those subframes in addition to determine RSRP.
	The reference point for the RSRP shall be the antenna connector of the UE. If receiver diversity is in use by the UE, the reported value shall not be lower than the corresponding RSRP of any of the individual diversity branches.
Applicable for	RRC_IDLE intra-frequency, RRC_IDLE inter-frequency, RRC_CONNECTED intra-frequency, RRC_CONNECTED inter-frequency

NOTE 1: The number of resource elements within the considered measurement frequency bandwidth and within the measurement period that are used by the UE to determine RSRP is left up to the UE implementation with the limitation that corresponding measurement accuracy requirements have to be fulfilled.

NOTE 2: The power per resource element is determined from the energy received during the useful part of the symbol, excluding the CP.

5.1.3 Reference Signal Received Quality (RSRQ)

Definition	Reference Signal Received Quality (RSRQ) is defined as the ratio $N \times RSRP/(E\text{-}UTRA\ carrier\ RSSI)$, where N is the number of RB's of the E-UTRA carrier RSSI measurement bandwidth. The measurements in the numerator and denominator shall be made over the same set of resource blocks.
	E-UTRA Carrier Received Signal Strength Indicator (RSSI), comprises the linear average of the total received power (in [W]) observed only in certain OFDM symbols of measurement subframes, in the measurement bandwidth, over N number of resource blocks by the UE from all sources, including co-channel serving and non-serving cells, adjacent channel interference, thermal noise etc. Unless indicated otherwise by higher layers, RSSI is measured only from OFDM symbols containing reference symbols for antenna port 0 of measurement subframes. If higher layers indicate all OFDM symbols for performing RSRQ measurements, then RSSI is measured from all OFDM symbols of the DL part of measurement subframes. If higher-layers indicate certain subframes for performing RSRQ measurements, then RSSI is measured from all OFDM symbols of the DL part of the indicated subframes. If higher layers indicate measurements based on discovery signals, RSSI is measured from all OFDM symbols of the DL part of the subframes in the configured discovery signal occasions.
	The reference point for the RSRQ shall be the antenna connector of the UE. If receiver diversity is in use by the UE, the reported value shall not be lower than the corresponding RSRQ of any of the individual diversity branches.
Applicable for	RRC_IDLE intra-frequency, RRC_IDLE inter-frequency, RRC_CONNECTED intra-frequency, RRC_CONNECTED inter-frequency

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_13633

1v130801p.pdf.

150. Identified LAA UEs are configured to measure discovery reference signals, including CSI-RS.

– *MeasDS-Config*

The IE *MeasDS-Config* specifies information applicable for discovery signals measurement.

MeasDS-Config field descriptions
csi-RS-IndividualOffset CSI-RS individual offset applicable to a specific CSI-RS resource. Value dB-24 corresponds to -24 dB, dB-22 corresponds to -22 dB and so on.
dmtc-PeriodOffset Indicates the discovery signals measurement timing configuration (DMTC) periodicity (*dmtc-Periodicity*) and offset (*dmtc-Offset*) for this frequency. For DMTC periodicity, value ms40 corresponds to 40ms, ms80 corresponds to 80ms and so on. The value of DMTC offset is in number of subframe(s). The duration of a DMTC occasion is 6ms.
ds-OccasionDuration Indicates the duration of discovery signal occasion for this frequency. Discovery signal occasion duration is common for all cells transmitting discovery signals on one frequency. If the *carrierFreq* in the measurement object is on an unlicensed band as specified in [42], the UE shall ignore the field *ds-OccasionDuration* for the carrier frequency and apply a value 1 instead.
measCSI-RS-ToAddModList List of CSI-RS resources to add/ modify in the CSI-RS resource list for discovery signals measurement.
measCSI-RS-ToRemoveList List of CSI-RS resources to remove from the CSI-RS resource list for discovery signals measurement.
physCellId Indicates the physical cell identity where UE may assume that the CSI-RS and the PSS/SSS/CRS corresponding to the indicated physical cell identity are quasi co-located with respect to average delay and doppler shift.
resourceConfig Parameter: CSI reference signal configuration, see TS 36.211 [21, table 6.10.5.2-1 and 6.10.5.2-2]. If the *carrierFreq* in the measurement object is on an unlicensed band as specified in [42], E-UTRAN does not configure the values {0, 4, 5, 9, 10, 11, 18, 19}.
scramblingIdentity Parameter: Pseudo-random sequence generator parameter, n_{ID}, see TS 36.213 [23, 7.2.5].
subframeOffset Indicates the subframe offset between SSS of the cell indicated by physCellId and the CSI-RS resource in a discovery signal occasion. The field *subframeOffset* is set to values 0 if the *carrierFreq* in the measurement object is on an unlicensed band as specified in [42].

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_13633

1v130801p.pdf.

– *CSI-Process*

The IE *CSI-Process* is the CSI process configuration that E-UTRAN may configure on a serving frequency.

***CSI-Process* information elements**

CSI-Process field descriptions
alternativeCodebookEnabledFor4TXProc Indicates whether code book in TS 36.213 [23] Table 7.2.4-0A to Table 7.2.4-0D is being used for deriving CSI feedback and reporting for a CSI process. EUTRAN may configure the field only if the number of CSI-RS ports for non-zero power transmission CSI-RS configuration is 4.
cqi-ReportAperiodicProc If *csi-MeasSubframeSets-r12* is configured for the same frequency as the CSI process, *cqi-ReportAperiodicProc* applies for CSI subframe set 1. If *csi-MeasSubframeSet1-r10* or *csi-MeasSubframeSet2-r10* are configured for the same frequency as the CSI process, *cqi-ReportAperiodicProc* applies for CSI subframe set 1 or CSI subframe set 2. Otherwise, *cqi-ReportAperiodicProc* applies for all subframes. E-UTRAN configures *cqi-ReportAperiodicProc-v1310* only if *cqi-ReportAperiodicProc-r11* is configured
cqi-ReportAperiodicProc2 *cqi-ReportAperiodicProc2* is configured only if *csi-MeasSubframeSets-r12* is configured for the same frequency as the CSI process. *cqi-ReportAperiodicProc2* is for CSI subframe set 2. E-UTRAN shall set *cqi-ReportModeAperiodic-r11* in *cqi-ReportAperiodicProc2* the same as in *cqi-ReportAperiodicProc*. E-UTRAN configures *cqi-ReportAperiodicProc2-v1310* only if *cqi-ReportAperiodicProc2-r12* is configured.
cqi-ReportBothProc Includes CQI configuration parameters applicable for both aperiodic and periodic CSI reporting, for which CSI process specific values may be configured. E-UTRAN configures the field if and only if *cqi-ReportPeriodicProcId* is included and/ or if *cqi-ReportAperiodicProc* is included.
cqi-ReportPeriodicProcId Refers to a periodic CQI reporting configuration that is configured for the same frequency as the CSI process. Value 0 refers to the set of parameters defined by the REL-10 CQI reporting configuration fields, while the other values refer to the additional configurations E-UTRAN assigns by *CQI-ReportPeriodicProcExt-r11* (and as covered by *CQI-ReportPeriodicProcExtId*).
csi-IM-ConfigId Refers to a CSI-IM configuration that is configured for the same frequency as the CSI process. If *csi-IM-ConfigId-v1250* or *csi-IM-ConfigId-v1310* is configured, the UE only considers this extension (and ignores *csi-IM-ConfigId-r11* or *csi-IM-ConfigId-r12*).
csi-IM-ConfigIdList Refers to one or two CSI-IM configurations that are configured for the same frequency as the CSI process. *csi-IM-ConfigIdList* can include 2 entries only if *csi-MeasSubframeSets-r12* is configured for the same frequency as the CSI process.
csi-RS-ConfigNZPId Refers to a CSI RS configuration using non-zero power transmission that is configured for the same frequency as the CSI process.
eMIMO-Type Parameter: *eMIMO-Type*, see TS 36.213 [23], TS 36.211 [21]. If *eMIMO-Type* is set to *nonPrecoded*, the codebooks used for deriving CSI feedback are in TS 36.213 [23, Table 7.2.4-10 to Table 7.2.4-17]. Choice values *nonPrecoded* and *beamformed* correspond to '*CLASS A*' and '*CLASS B*' respectively, see TS 36.212 [22] and TS 36.213 [23].
p-C-AndCBSRList The UE shall ignore *p-C-AndCBSRList-r11* if configured with *eMIMO-Type* unless it is set to *beamformed*, *alternativeCodebookEnabledBeamformed* is set to *FALSE* and *csi-RS-ConfigNZPIdListExt* is not configured.

– *CSI-RS-Config*

The IE *CSI-RS-Config* is used to specify the CSI (Channel-State Information) reference signal configuration.

***CSI-RS-Config* information elements**

***CSI-RS-Config* field descriptions**
ace-For4Tx-PerResourceConfigList The field indicates the *alternativeCodeBookEnabledFor4TX-r12* per CSI-RS resource. E-UTRAN configures the field only if *csi-RS-ConfigNZPIdListExt* is configured.
antennaPortsCount Parameter represents the number of antenna ports used for transmission of CSI reference signals where value an1 corresponds to 1 antenna port, an2 to 2 antenna ports and so on, see TS 36.211 [21, 6.10.5].
ds-ZeroTxPowerCSI-RS Parameter for additional *zeroTxPowerCSI-RS* for a serving cell, concerning the CSI-RS included in discovery signals.
p-C Parameter: P_C, see TS 36.213 [23, 7.2.5]. The UE shall ignore *p-C-r10* if configured with *eMIMO-Type* unless it is set to *beamformed*, *alternativeCodebookEnabledBeamformed* is set to *FALSE* and *csi-RS-ConfigNZPIdListExt* is not configured.
resourceConfig Parameter: CSI reference signal configuration, see TS 36.211 [21, table 6.10.5.2-1 and 6.10.5.2-2].
subframeConfig Parameter: I_{CSI-RS}, see TS 36.211 [21, table 6.10.5.3-1].
zeroTxPowerCSI-RS2 Parameter for additional *zeroTxPowerCSI-RS* for a serving cell. E-UTRAN configures the field only if *csi-MeasSubframeSets-r12* and *TM 1 – 9* are configured for the serving cell.
zeroTxPowerResourceConfigList Parameter: *ZeroPowerCSI-RS*, see TS 36.213 [23, 7.2.7].
zeroTxPowerSubframeConfig Parameter: I_{CSI-RS}, see TS 36.211 [21, table 6.10.5.3-1].

CSI is determined based on CSI measurements, per *CSI-RS-Config*, as part of discovery reference signal (DRS) measurements by LAA UE

CSI-Process configures Channel Quality Information (CQI) reporting for a LAA UE (this config is received by LAA UE from the LAA small cell)

The LAA UE's feedback information transmitter reports CQI (information containing channel quality information indicative of the channel quality) to the transmission apparatus as part of the *CSI-Process*

http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.08.01_60/ts_136331v130801p.pdf.

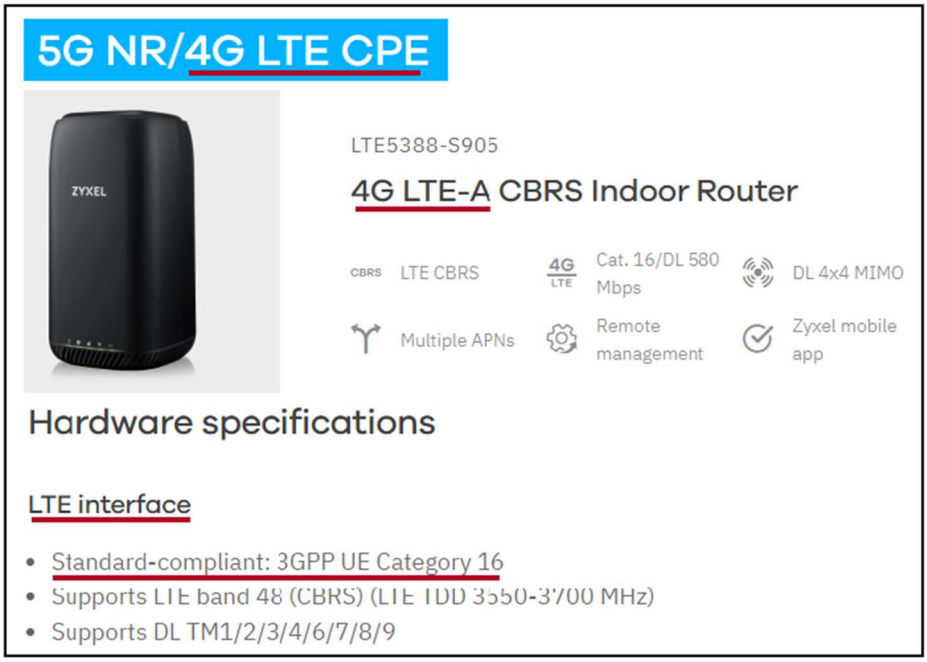
ZYXEL INFRINGES U.S. PATENT NO. 8,467,723.

151. The Patent Office issued U.S. Patent No. 8,467,723, titled "Base Station Apparatus, Mobile Apparatus, and Communication Method," on June 18, 2013, after a thorough examination and determination that the subject matter claimed is patentable.

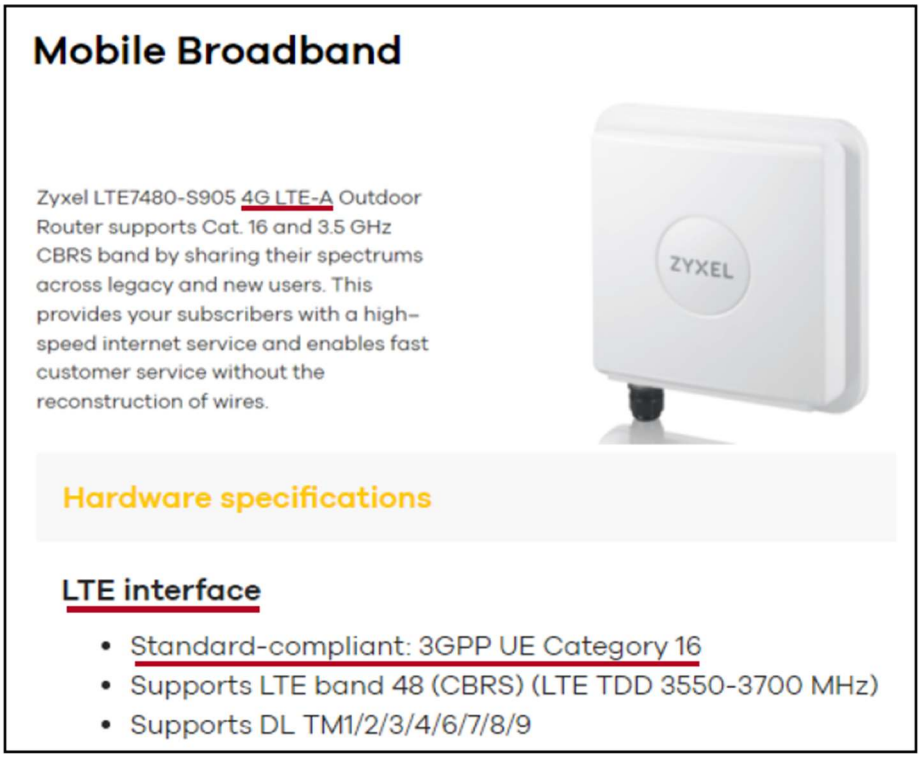
152. Zyxel Accused Products with respect to the '723 patent include the Zyxel devices that are enabled to perform inter-RAT handover, which commonly occurs when e.g. a 3GPP user equipment's (UE's) LTE signal becomes weak enough to result in a handover to 3G. On information and belief, Zyxel's 5G NR/4G LTE CPE (under its Service Provider products) and its Mobile Broadband 4G LTE products (under its Business products) are enabled to perform inter-RAT handover including, at least, the following:

- 4G LTE
  - LTE7461-M602 / 4G LTE-A Outdoor Router
  - LTE7480-S905 / 4G LTE-A CBRS Outdoor Router
  - LTE7485-S905 / 4G LTE-A CBSD Category B Outdoor Router
  - LTE5388-S905 / 4G LTE-A CBRS Indoor Router

- 5G
  - NR5201 / 5G NR Indoor Router
  - NR5203 / 5G NR Indoor Router
  - R7201 / 5G NR Outdoor Router
  - NR7203 / 5G NR Outdoor Router
  - NR7223 / 5G NR Outdoor Router



https://service-provider.zyxel.com/na/en/products/5g-nr4g-lte-cpe/4g-lte-cpe/idus/lte5388-s905#specifications.



https://www.zyxel.com/us/en/products_services/4G-LTE-Advanced-Outdoor-

Router-LTE7480-S905/specifications.

153. The Evolved Packet Core (EPC), the core network of the LTE system, supports multiple access technologies and allows for handover between these accesses. It focuses on accommodation of LTE and 3G as shown in Figure 1 below. In EPC, the Serving Gateway (SGW) (i) transports IP data traffic between the User Equipment (UE) and the external networks, and (ii) is the point of interconnect between the radio side and the EPC. Importantly, the SGW is the anchor point for the inter RAT mobility (i.e. in case of handover between LTE and other 3GPP).

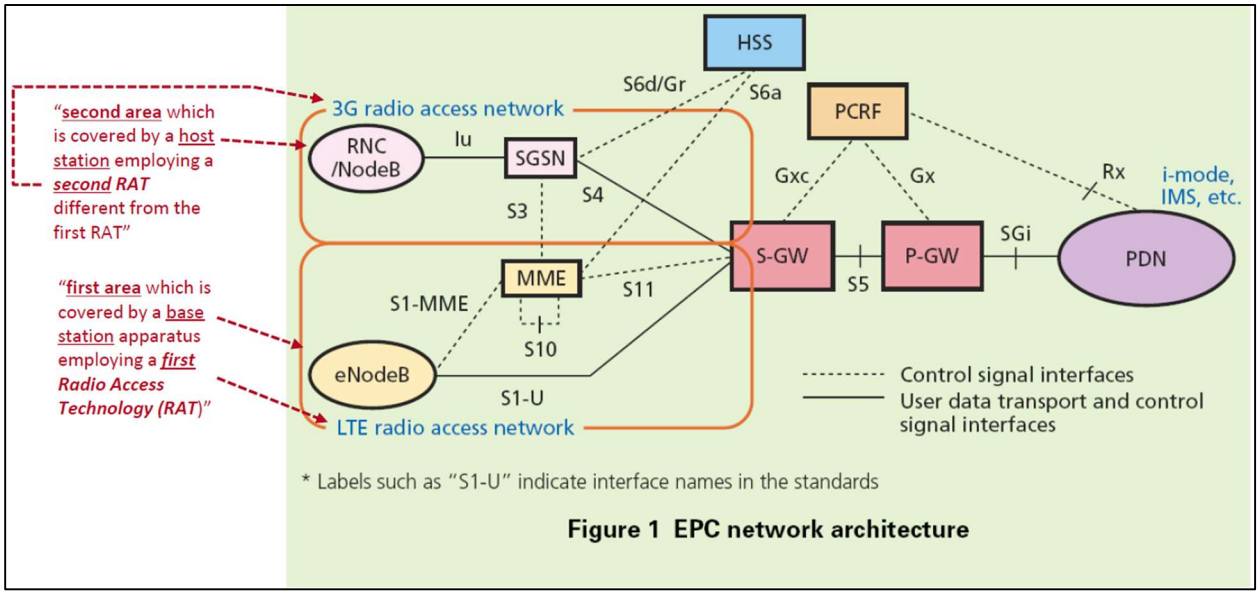


Figure 1 EPC network architecture

https://www.cultofmac.com/421369/https:/www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_004en.pdf.

154. The 3GPP specification addresses inter RAT handover of a UE between LTE radio access networks (E-UTRAN) and radio access networks using

older generation radio access technologies such as UTRAN (3G), UMTS (3G GSM), GPRS (GSM 2G, 3G packet mobile data), and GERAN (3G GSM EDGE RAN). The information below depicts features of the different RAN and how they coexist and are arranged.

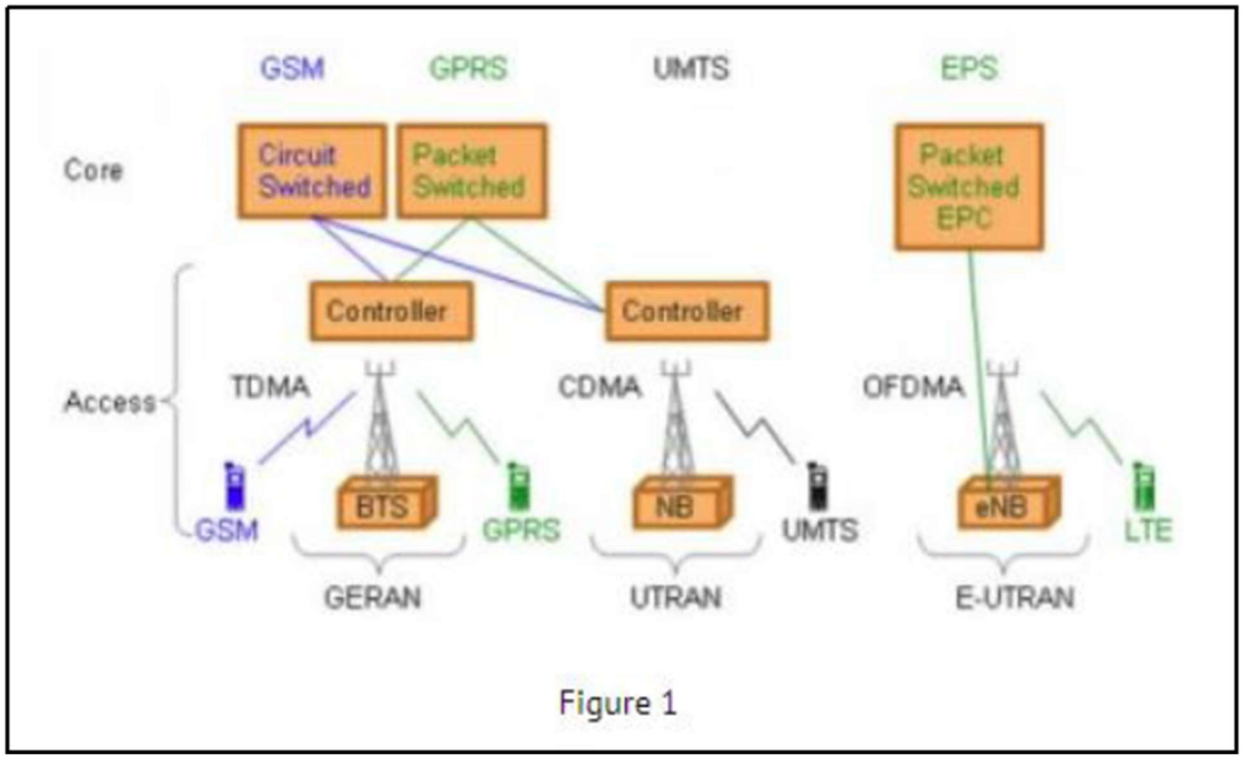
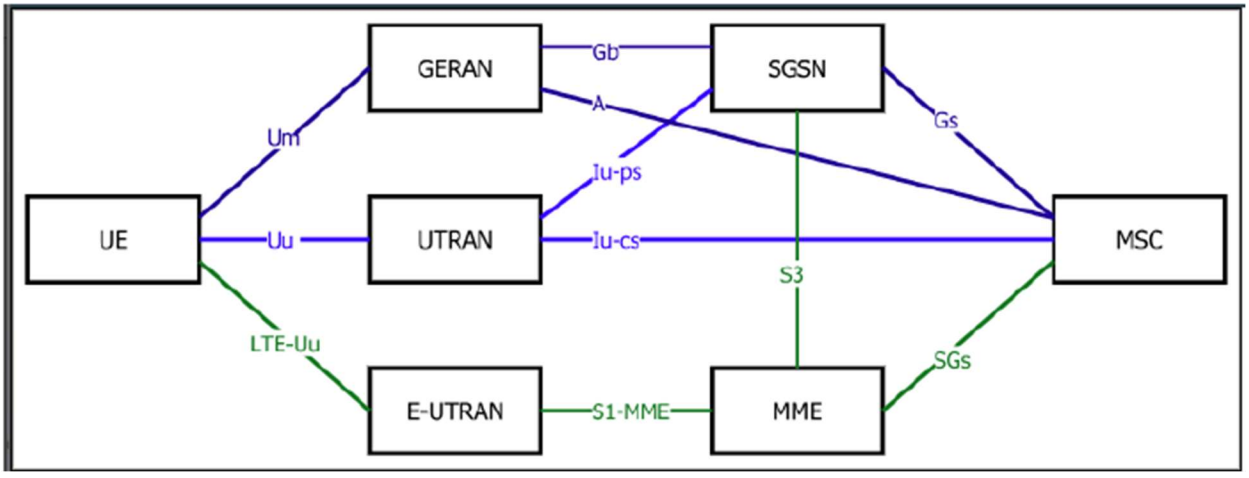


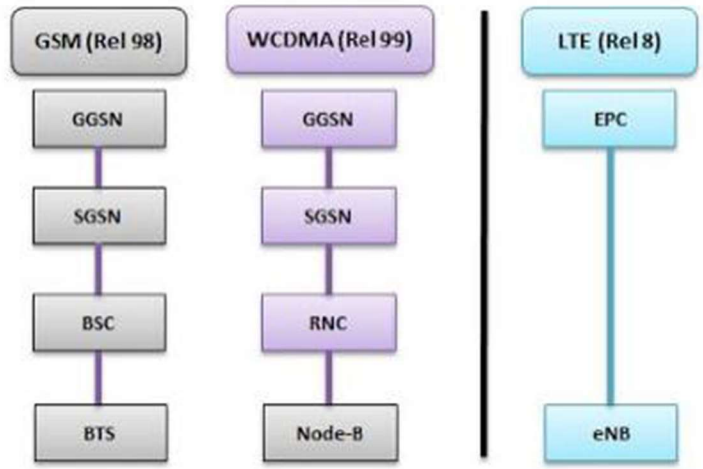
Figure 1

http://www.techplayon.com/lte-overview/



https://upload.wikimedia.org/wikipedia/en/a/af/LTE-CSFB-E-UTRAN-UTRAN-GERAN-Interfaces.svg

Below figure shows the architecture comparison of GERAN vs UTRAN vs E-UTRAN



GERAN vs UTRAN vs E-UTRAN

Design Comparison

Refer the below mentioned table for design comparison GERAN vs UTRAN vs E-UTRAN

Comparision	GERAN	UTRAN	LTE
Radio Access	FDMA/TDMA	WCDMA	OFDMA/SC-FDMA
Bandwidth	200KHz	5MHz	1.4,3,5,10,15,20 MHz
Data Rate	14.4Kbps ~ 1.89Mbps	384Kbps~42Mbps	300Mbps
Mobility (KM/Hr)	100	120	350
Latency	700 ~ 180ms	220~110ms	< 100ms for Control Plane < 5ms for Data Plane
Services	Both circuit & packet switched	Both circuit & packet switched	Packet Switched only
Architecture	4 NW nodes (not flat)	4 NW nodes (not flat)	2 NW nodes (flat)

Design Comparison

https://know-lte.blogspot.com/2016/09/geran-utran-comparison-with-lte.html

155. The Zyxel Accused Products are "mobile station apparatuses" and 3GPP user equipment (UE). These UEs perform Inter RAT handover, where the mobile station's radio connection is switched from the first base station (e.g. LTE

eNB) employing a first RAT (LTE) to a second base station (e.g. RNC/ NodeB) employing a second (different) RAT (GERAN/UTRAN).

RAT handover scenarios include: (i) between E-UTRAN (LTE) and UTRAN or GERAN (both 3G), (ii) between UMTS (3G UTRAN) and GERAN (3G).

Inter-RAT handover: indicates the transfer of the connection, under the control of the network, between the MS and two different radio access technologies (e.g. UMTS to GERAN Iu mode).

3GPP TS 44.118 version 15.0.0 Release 15

"MS" = "mobile station"

5.5.2.1 E-UTRAN to UTRAN Iu mode Inter RAT handover

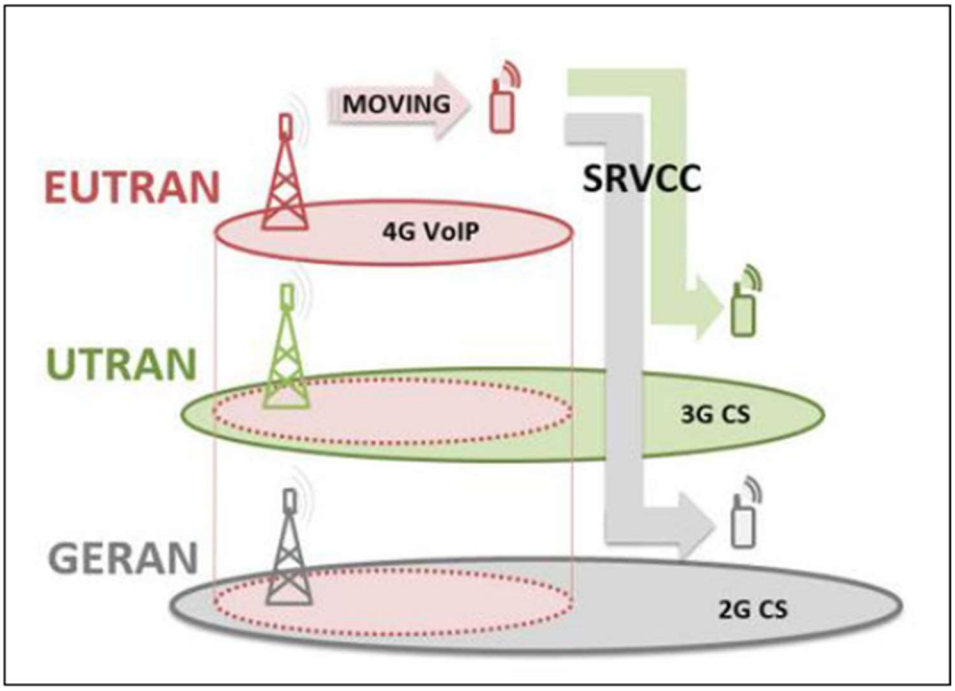
5.5.2.1.1 General

1. The source eNodeB decides to initiate an Inter-RAT handover to the target access network, UTRAN Iu mode. At this point both uplink and downlink user data is transmitted via the following: Bearer(s) between UE and source eNodeB, GTP tunnel(s) between source eNodeB, Serving GW and PDN GW.

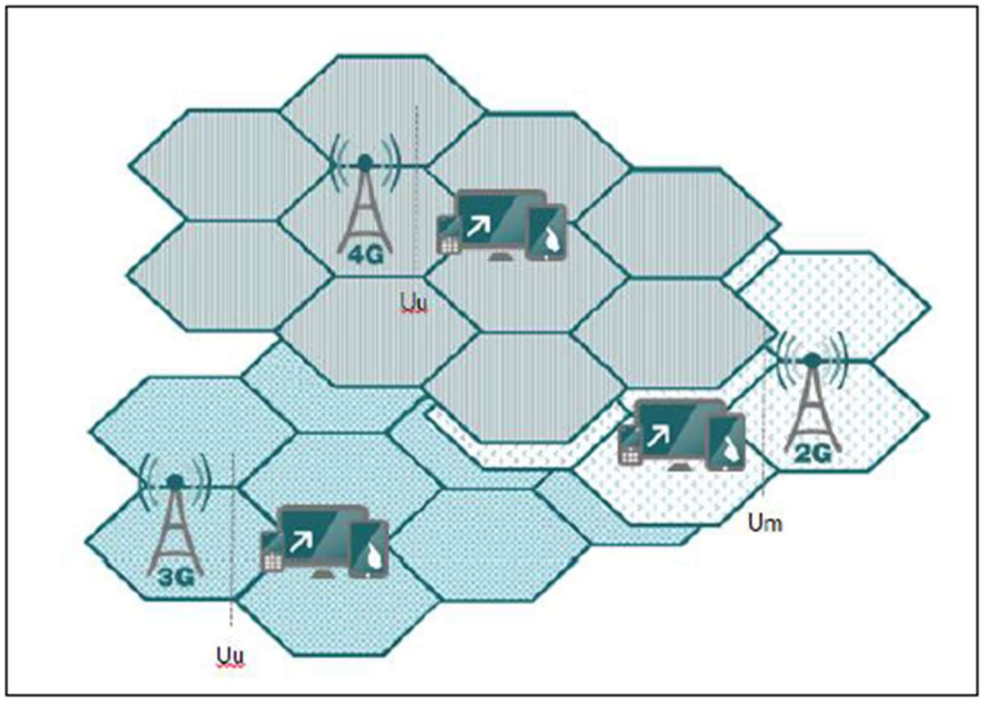
   If the UE has an ongoing emergency bearer service the source eNodeB shall not initiate PS handover to a UTRAN cell that is not IMS voice capable.

3GPP TS 23.401 version 15.6.0 Release 15

156. For each carrier operating in a given area, the areas covered by different RAT overlap with one another according to where carriers' eNB/NodeB/RNC are. For economies of scale and cost savings, many carriers deploy their eNB/ NodeB /RNC from the same physical location (e.g. cell tower), thus resulting in a direct overlapping RAT area in the vicinity of the deployment (as shown in below diagram).



https://www.netmanias.com/en/?m=view&id=blog&no=10908



https://www.prismatelecomtesting.com/solutions/network-equipment-manufacturers/ran-testing/inter-rat-ho-testing/

157. By way of example, Qualcomm's U.S. Patent No. 8,792,365, issued July 29, 2014, and titled "Service-based inter-radio access technology (inter-RAT) handover," exemplifies a given geographic area being covered by multiple overlapping radio access technologies.

FIG. 4 illustrates a geographical area with coverage from three radio access technologies according to one aspect.

Deployment of a TD-SCDMA network may not provide complete geographic coverage in certain areas during the migration from 2G to 3G Radio Access Technologies (RATs). In areas where TD-SCDMA networks are deployed, other networks (such as WCDMA and Global System for Mobile Communications (GSM)) may also have a geographical presence. FIG. 4 illustrates a geographical area with coverage from three radio access technologies according to one aspect.

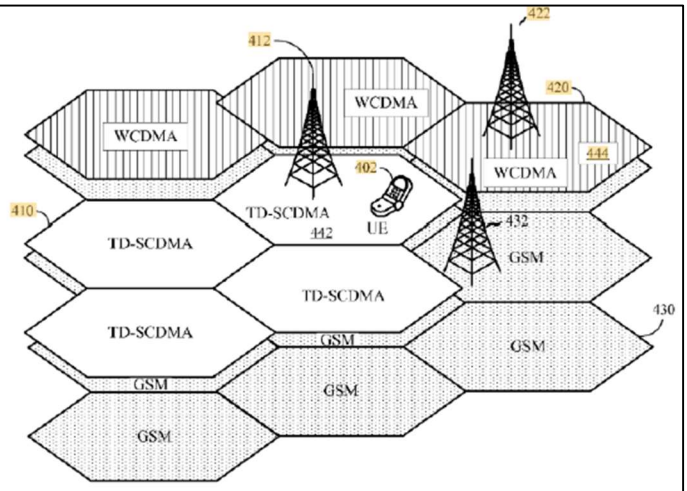
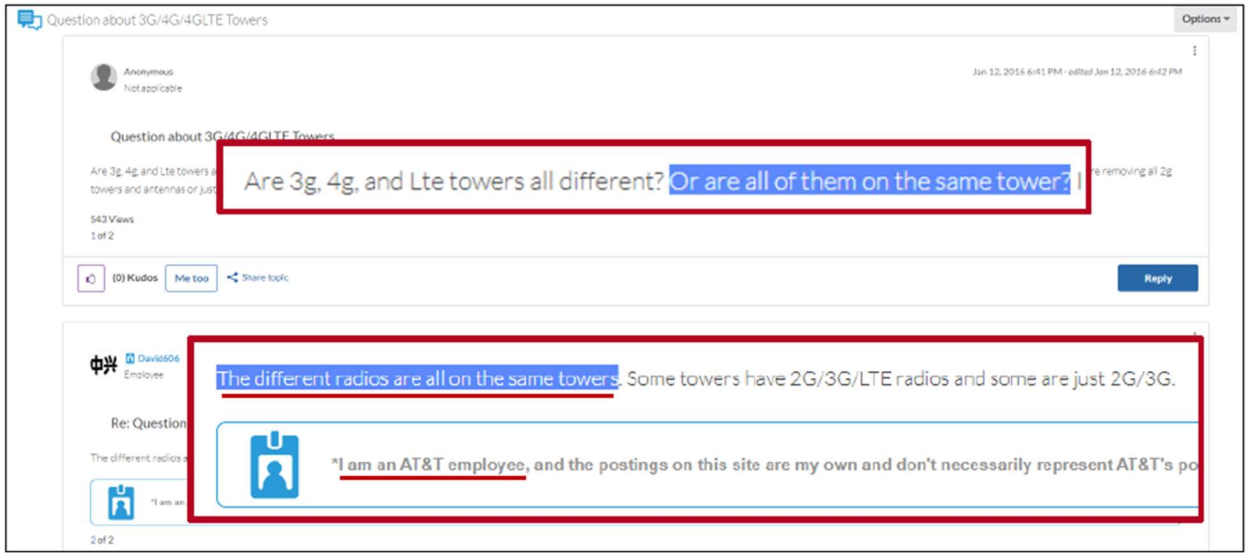


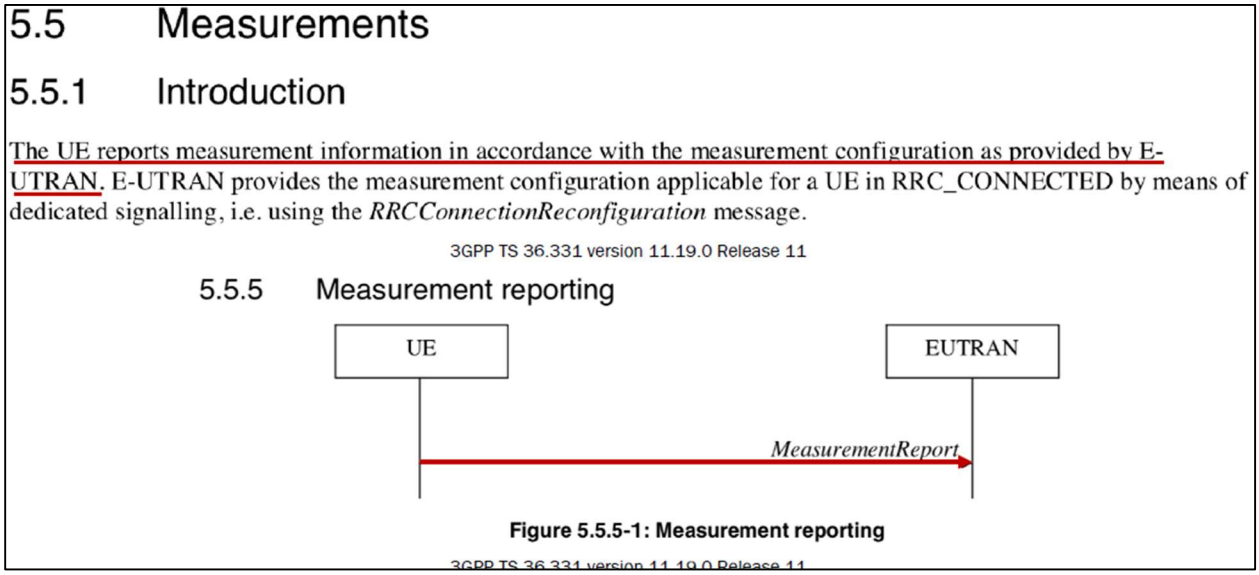
FIG. 4

158. For each carrier operating in a given area, the areas covered by different RAT overlap with one another according to wherecarriers' eNB/NodeB/RNC are. For economies of scale and cost savings, many carriers deploy their eNB/ NodeB /RNC from the same physical location (e.g. cell tower), thus resulting in a direct overlapping RAT area in the vicinity of the deployment.



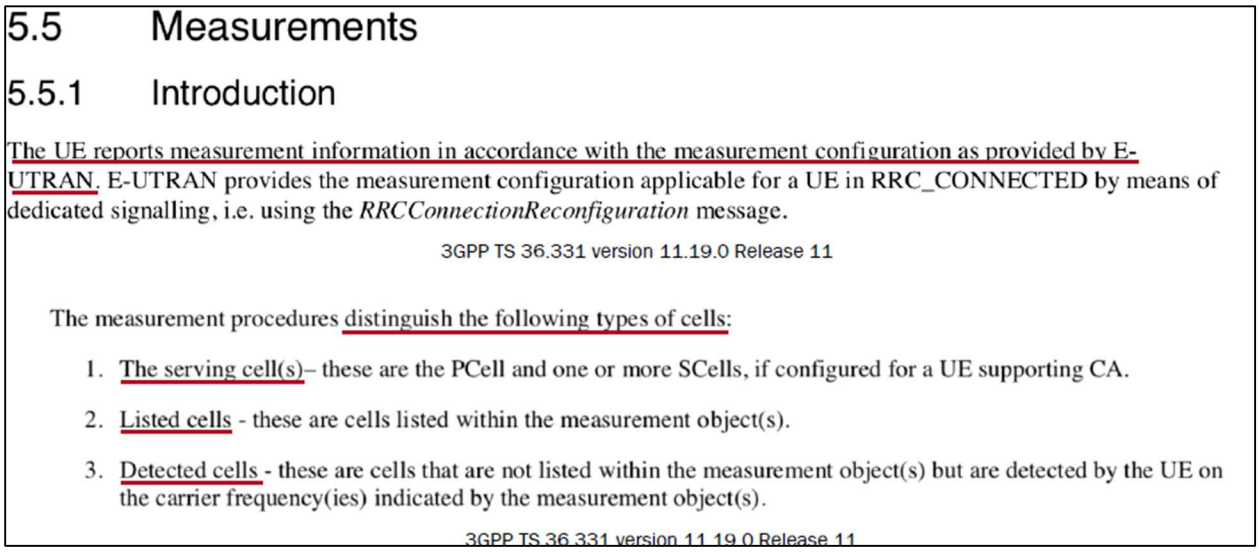
https://forums.att.com/t5/Network-Coverage/Question-about-3G-4G-4GLTE-Towers/td-p/4734190.

159. E-UTRAN UE includes a transmitter to transmit notification information, e.g., measurement information, to the E-UTRAN eNB ("base station") while using the first RAT (LTE).



160. In the 4G to 3G use case, E UTRAN UEs report measurement

information for multiple types of RAT cells according to UE's measurement configuration. For example, when a E-UTRAN UE "detects that [it] is located in the second area while using the first RAT" (within a 3G radio cell while still connected to its LTE eNB) the UE will procure measurement data for the cells of the second area.



5.5 Measurements

5.5.1 Introduction

The UE reports measurement information in accordance with the measurement configuration as provided by E-UTRAN. E-UTRAN provides the measurement configuration applicable for a UE in RRC_CONNECTED by means of dedicated signalling, i.e. using the *RRCConnectionReconfiguration* message.

3GPP TS 36.331 version 11.19.0 Release 11

The measurement procedures distinguish the following types of cells:

1. The serving cell(s)– these are the PCell and one or more SCells, if configured for a UE supporting CA.
2. Listed cells - these are cells listed within the measurement object(s).
3. Detected cells - these are cells that are not listed within the measurement object(s) but are detected by the UE on the carrier frequency(ies) indicated by the measurement object(s).

3GPP TS 36.331 version 11.19.0 Release 11

161. In the 4G to 3G use case, the UE belongs to an LTE macro cell covered by an LTE eNB ("a first area which is covered by a base station apparatus employing a first Radio Access Technology (RAT)"). As E-UTRAN UEs measure and report on multiple cells of base/host stations employing various RATs, overlap exists in base/host station cell coverage as explained, and the first area that the E-UTRAN UE belongs to (covered by 4G LTE eNB, "base station") includes part or the entirety of a second area covered by a host station (3G NodeB or RNC). This cell coverage overlap is present during a UE inter-RAT handover. The 3GPP TS

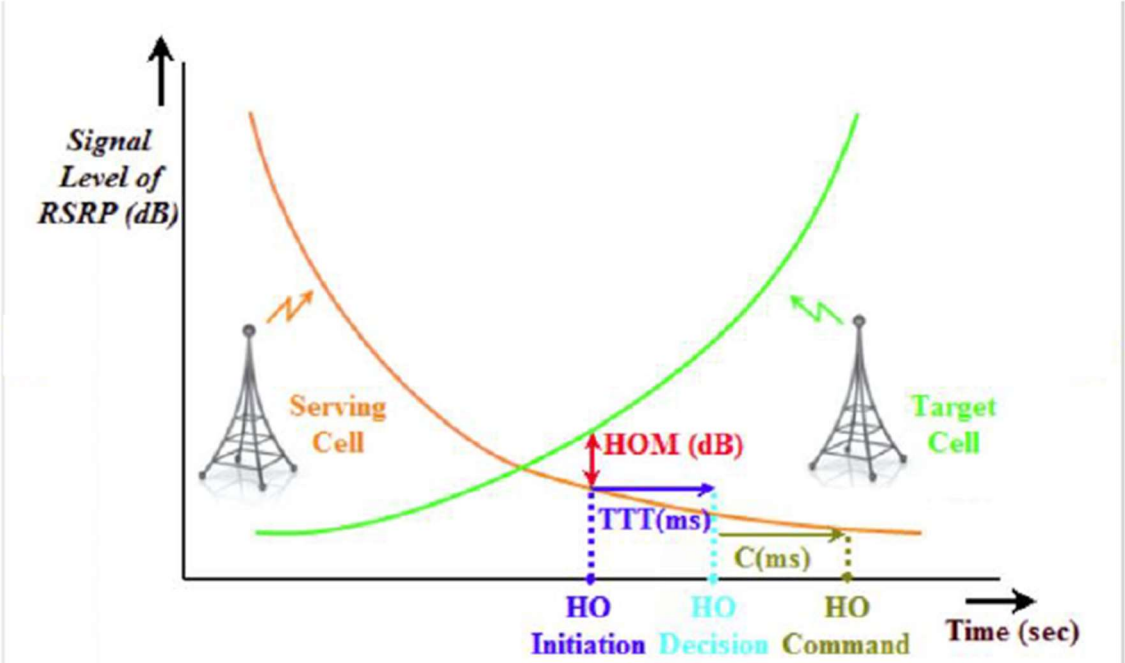
excerpt below explains the types of cells (e.g. serving, listed, detected, and within range) measured and reported on under the various inter-RAT scenarios.

For E-UTRA, the UE measures and reports on the serving cell(s), listed cells and detected cells. For inter-RAT UTRA, the UE measures and reports on listed cells and optionally on cells that are within a range for which reporting is allowed by E-UTRAN. For inter-RAT GERAN, the UE measures and reports on detected cells. For inter-RAT CDMA2000, the UE measures and reports on listed cells.

NOTE 2: For inter-RAT UTRA and CDMA2000, the UE measures and reports also on detected cells for the purpose of SON.

3GPP TS 36.331 version 11.19.0 Release 11

162. The diagram below illustrates how a UE moving from the area of a serving cell ("first area" with eNB "base station apparatus") into a separate area covered by a target cell ("second area" with a NodeB or RNC "host station") will experience changing RF signal conditions from each cell (illustrated by the orange and green plotted curves in the diagram). As the diagram indicates, these changing signal conditions (i.e. the serving cell's signal becoming weaker as the target cell 's signal becomes stronger) will trigger the UE handing over from the serving cell ("first area") to the target cell ("second area"). The UE is aware of the changing RF signal conditions based on its measuring of the cells' RF signals as explained.



Principle of the LTE hard handover process.

Is it possible to get 3G signals from a 2G tower?

5 Answers

Balakrishnan Vasudevan, 3 years as a Telecommunications Engineer for Ericsson
Answered Jun 20, 2016 · Author has 611 answers and 2.1m answer views

As Mukesh Bhakar rightly mentions, the tower has nothing to do with the class of signals you receive. Towers hold equipment designed to operate at a particular frequency in the spectrum and provide services for whatever technology the equipment can handle.

A mobile phone keeps track of at least 5 towers in its vicinity, these towers have a signal strength that exceeds a particular threshold. This list keeps getting updated dynamically as the user keeps moving around and even when the user is stationary. If the phone is using a 3G compatible SIM, then the phone would try and latch on to a 3G base station. If the strength of the signals from the 3G base stations is below the threshold, the mobile phone would try and latch on to the 2G tower that provides the highest signal strength. So even though there are two 2G towers in your vicinity, your phone gets a 3G signal from another tower with enough strength to latch on to. You can use an app to find the ID of the tower that you are currently connected to and then use Airtel's network status page to find where the tower is.

2.8k Views · View 4 Upvoters

163. In the 4G-to-3G use case, the trigger for the E-UTRAN UE to send notification information (measurement results) to its connected eNB is based on the UE's measurement configuration, which configures the types of inter-RAT neighbor cells to measure and other variables such as thresholds and timing for measurement events. Measurement Event B1, which relates to Inter-RAT handover, is shown below (Event B2 is also applicable). When a UE is within range (in the second area) of the inter RAT neighbor cell, the UE will take measurements, the results of which, if meeting a configured measurement process, will trigger a handover to the inter-RAT neighbor or cell. As such, the notification information is transmitted when a UE detects that it is located in the second area while using the first RAT.

5.5.4 Measurement report triggering

5.5.4.7 Event B1 (Inter RAT neighbour becomes better than threshold)

The UE shall:

1> for UTRA and CDMA2000, only trigger the event for cells included in the corresponding measurement object;

1> consider the entering condition for this event to be satisfied when condition B1-1, as specified below, is fulfilled;

1> consider the leaving condition for this event to be satisfied when condition B1-2, as specified below, is fulfilled;

Inequality B1-1 (Entering condition)

$Mn + Ofn - Hys > Thresh$

Inequality B1-2 (Leaving condition)

$Mn + Ofn + Hys < Thresh$

The variables in the formula are defined as follows:

Mn is the measurement result of the inter-RAT neighbour cell, not taking into account any offsets. For CDMA 2000 measurement result, *pilotStrength* is divided by -2.

Ofn is the frequency specific offset of the frequency of the inter-RAT neighbour cell (i.e. *offsetFreq* as defined within the *measObject* corresponding to the frequency of the neighbour inter-RAT cell).

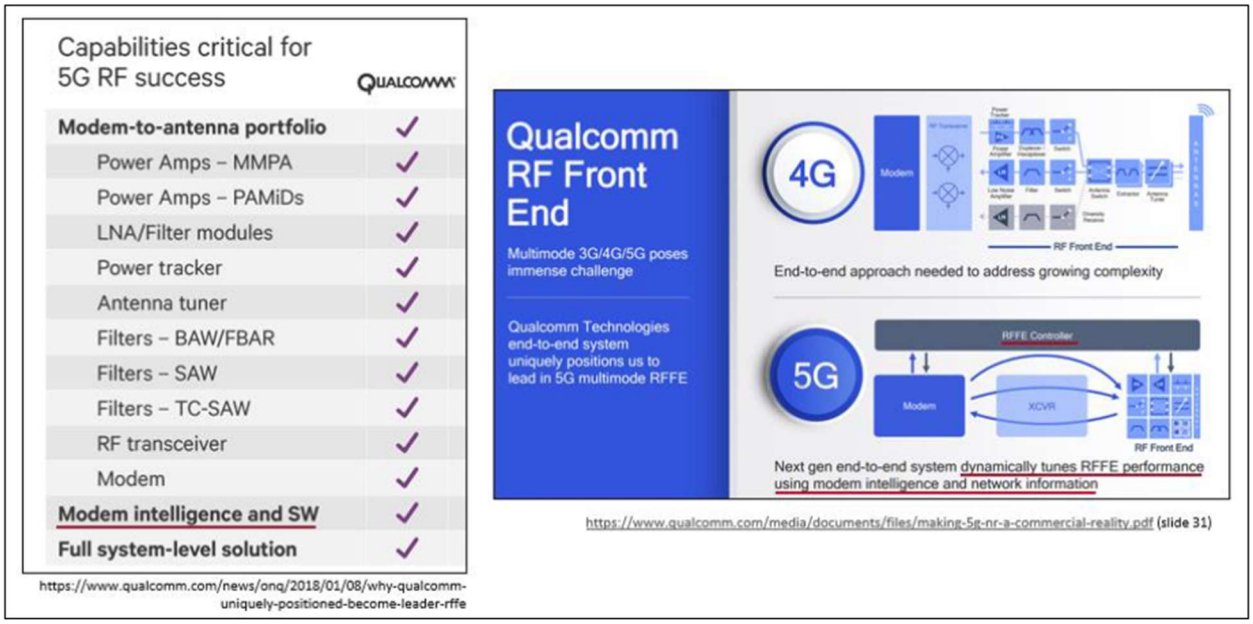
Hys is the hysteresis parameter for this event (i.e. *hysteresis* as defined within *reportConfigInterRAT* for this event).

Thresh is the threshold parameter for this event (i.e. *b1-Threshold* as defined within *reportConfigInterRAT* for this event). For CDMA2000, *b1-Threshold* is divided by -2.

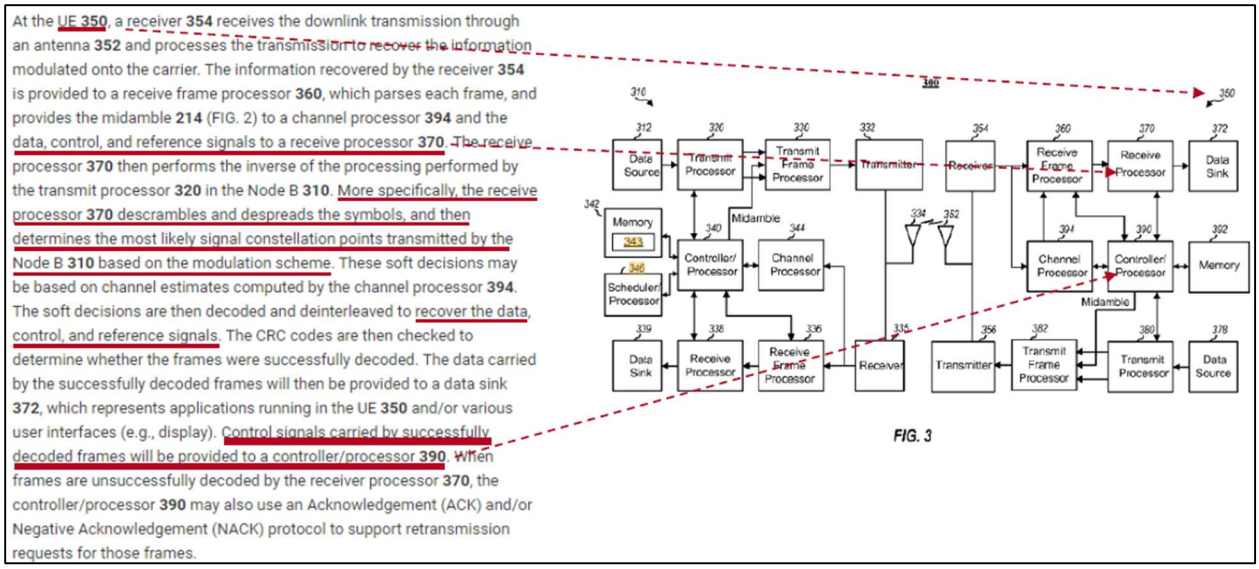
3GPP TS 36.331 version 11.19.0 Release 11

164. The UE's controller is implemented via a combination of hardware and software within the UE's mobile platform. High level, functional information

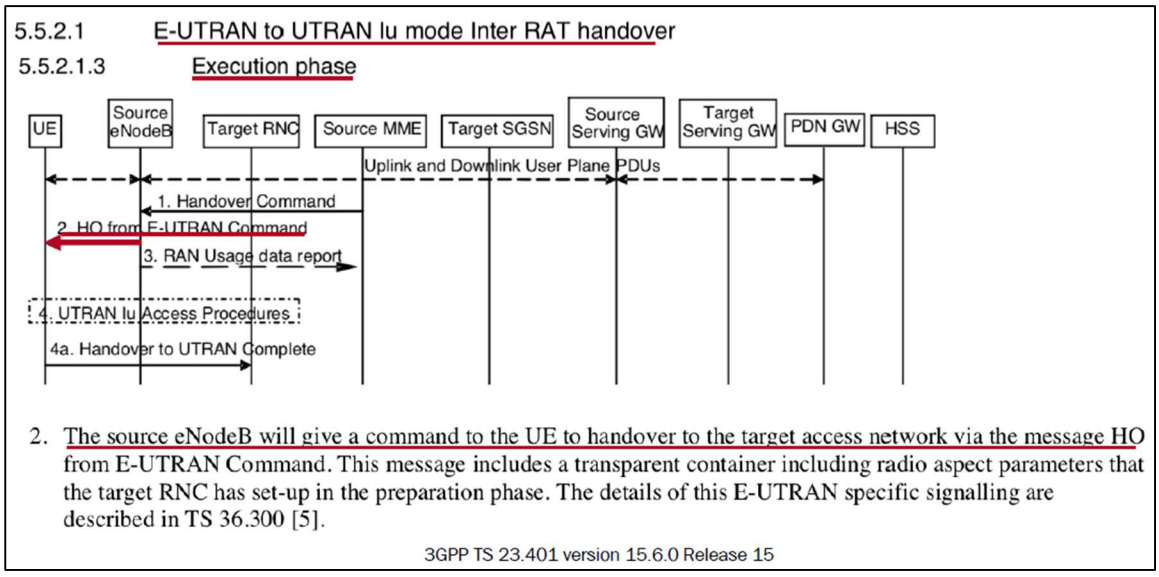
regarding exemplary UE with controllers (as part of mobile platforms, for example, supplied by Qualcomm) is shown below.



165. The UE's controller is implemented via a combination of hardware and software within the UE's mobile platform. As an example, Qualcomm's U.S. Patent No. 8,792,365, issued July 29, 2013, titled "Service based inter radio access technology (inter-RAT) handover," is exemplary of a UE having a controller configured to perform handover; '365 discloses that UE architecture includes a "Receive Processor" and a "Controller/Processor" (370 & 390 in FIG. 3) that enables handover according to a HO command from its serving eNB.



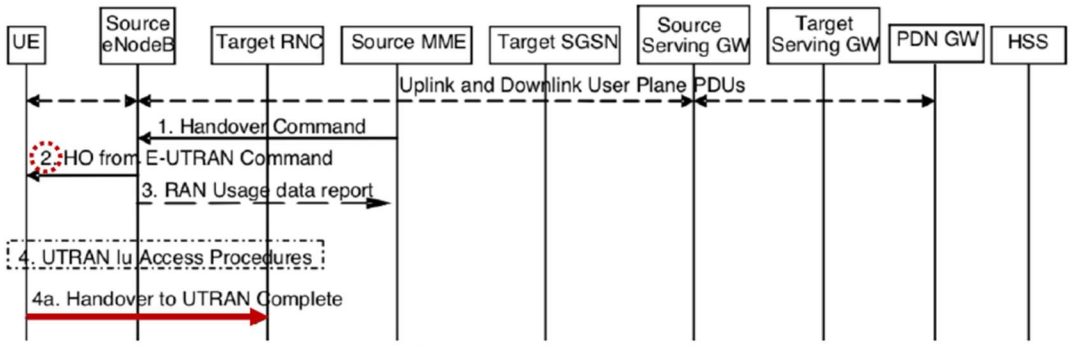
166. The UE's controller is implemented via a combination of hardware and software within the UE's mobile platform. In the 4G-to-3G use case, the UE's controller is responsive to ("configured to") a HO (handover) message received from its LTE eNB ("perform handover based on traffic control by the base station apparatus using the notification information"), based on the UE's measurement configuration and its reported measurement results.



167. In the 4G-to-3G use case, the base station performs traffic control for the UE by sending the UE a HO message, which triggers a handover by causing the UE to detach from 4G E-UTRAN and attach to 3G (UTRAN in the diagram below) according to the parameters provided in the HO message.

5.5.2.1 E-UTRAN to UTRAN Iu mode Inter RAT handover

5.5.2.1.3 Execution phase



3GPP TS 23.401 version 15.6.0 Release 15

4. The UE moves to the target UTRAN Iu (3G) system and executes the handover according to the parameters provided in the message delivered in step 2. The procedure is the same as in step 6 and 8 in clause 5.2.2.2 in TS 43.129 [8] with the additional function of association of the received RABs and existing Bearer Id related to the particular NSAPI.

3GPP TS 23.401 version 15.6.0 Release 15

ZYXEL INFRINGES U.S. PATENT NUMBER 8,792,453.

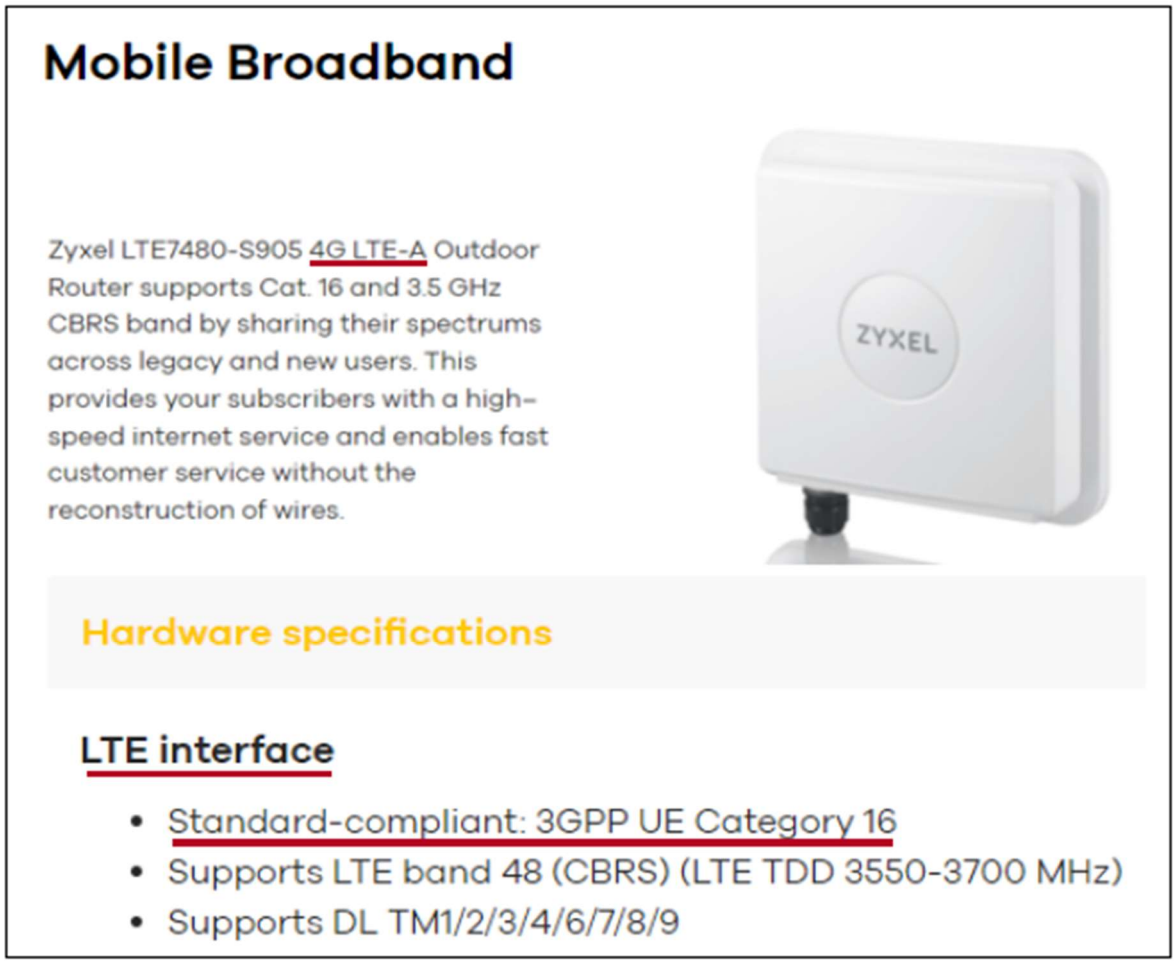
168. The Patent Office issued U.S. Patent No. 8,792,453, titled "Secure Tunnel Establishment Upon Attachment or Handover to an Access Network," on July 29, 2014, after a thorough examination and determination that the subject matter claimed is patentable.

169. Zyxel Accused Products with respect to the '569 patent include Zyxel "mobile nodes" (4G/5G devices, a/k/a user equipment (UE)) that establish a secure

tunnel to a trusted packet data gateway upon initially attaching to or performing a handover to a target access network. This occurs when the UE establishes an IPsec tunnel with an evolved packet data gateway (ePDG) in a target access network..

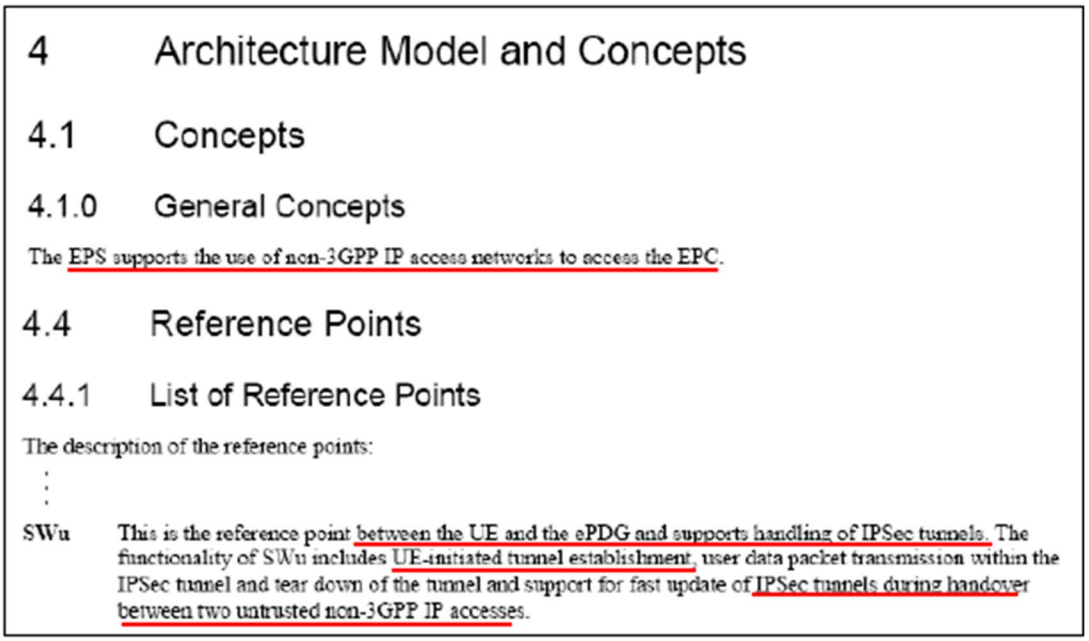
On information and belief, Zyxel's 5G NR/4G LTE CPE (under its Service Provider products) and its Mobile Broadband 4G LTE products (under its Business products) are enabled to perform this method by connecting to a 4G or 5G network. Exemplary Accused Products shown below.

https://service-provider.zyxel.com/na/en/products/5g-nr4g-lte-cpe/4g-lte-cpe/idus/lte5388-s905#specifications.



https://www.zyxel.com/us/en/products_services/4G-LTE-Advanced-Outdoor-Router-LTE7480-S905/specifications

170. 3GPP UE's ("a mobile node," e.g. the implicated Datalogic devices) establish a secure tunnel to a trusted packet data gateway upon the UE initially attaching to or performing a handover to a target access network. This occurs when a UE establishes an IPsec tunnel with an evolved packet data gateway (ePDG) in a target access network.



4 Architecture Model and Concepts

4.1 Concepts

4.1.0 General Concepts

The EPS supports the use of non-3GPP IP access networks to access the EPC.

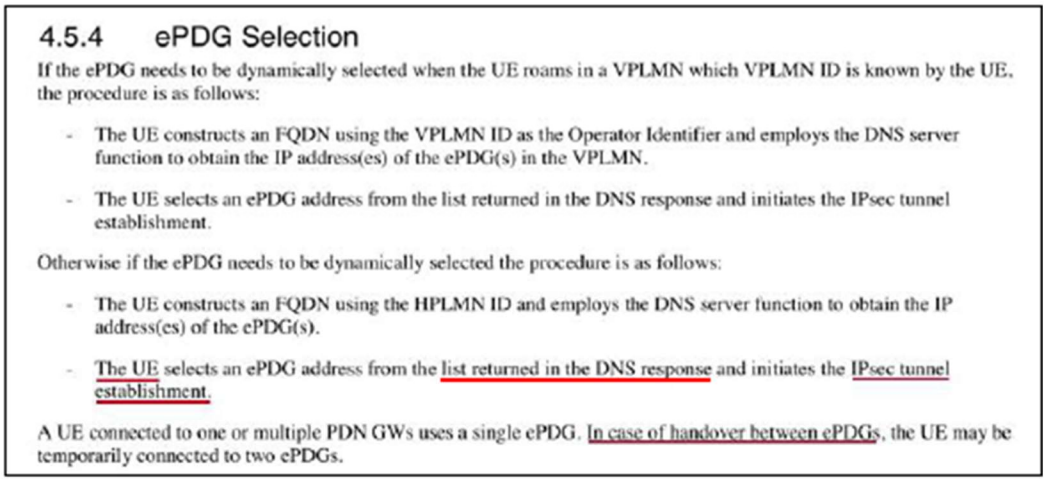
4.4 Reference Points

4.4.1 List of Reference Points

The description of the reference points:

⋮

SWu This is the reference point between the UE and the ePDG and supports handling of IPSec tunnels. The functionality of SWu includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel and tear down of the tunnel and support for fast update of IPSec tunnels during handover between two untrusted non-3GPP IP accesses.



4.5.4 ePDG Selection

If the ePDG needs to be dynamically selected when the UE roams in a VPLMN which VPLMN ID is known by the UE, the procedure is as follows:

- The UE constructs an FQDN using the VPLMN ID as the Operator Identifier and employs the DNS server function to obtain the IP address(es) of the ePDG(s) in the VPLMN.
- The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.

Otherwise if the ePDG needs to be dynamically selected the procedure is as follows:

- The UE constructs an FQDN using the HPLMN ID and employs the DNS server function to obtain the IP address(es) of the ePDG(s).
- The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.

A UE connected to one or multiple PDN GWs uses a single ePDG. In case of handover between ePDGs, the UE may be temporarily connected to two ePDGs.

3GPP TS 23.402 version 12.10.0 Release 12

171. 3GPP UE has a pre-configured list (reachability list) of non-3GPP access technologies, access networks, or serving network operators that allow for trusted non-3GPP IP Access. The UE also receives an indication of whether the non-3GPP IP access is trusted (the received indication takes precedence if there is conflict with the pre-configured information). The UE may obtain a reachability

list from a DNS server prior to establishment of the IPsec tunnel.

> 6 Authentication and key agreement procedures
>
> 6.1 General
>
> The non-3GPP access networks, which are trusted, can be pre-configured in the UE. The UE can e.g. have a list with non-3GPP access technologies, or access networks, or serving network operators that allow procedures for trusted non-3GPP IP access. Additionally, during 3GPP-based access authentication the UE may receive an indication whether the non-3GPP IP access is trusted or not. If such an indication is sent it shall be sent by the 3GPP AAA server as part of an EAP-AKA or EAP-AKA' request. If no such indication is received by the UE, and there is no pre-configured information in the UE, the UE shall consider the non-3GPP IP access as untrusted. In case of pre-configured information and indication received as part of an EAP-AKA or EAP-AKA' request are in conflict, the received indication shall take precedence.
>
> 3GPP TS 33.402 version 14.2.0 Release 14

172. If a reachability list is not pre-configured, the UE dynamically selects an ePDG using a DNS server function to obtain IP addresses of reachable ePDGs, the UE then selects an ePDG from the returned list. The '453 specification supports data path indication by various indications including e.g. access point name (e.g., IP address) as well as receiving the reachability list from another network node as a replacement for the UE's maintained reachability list.

> 4.5.4 ePDG Selection
>
> Otherwise if the ePDG needs to be dynamically selected the procedure is as follows:
>
> - The UE constructs an FQDN using the HPLMN ID and employs the DNS server function to obtain the IP address(es) of the ePDG(s).
> - The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.
>
> A UE connected to one or multiple PDN GWs uses a single ePDG. In case of handover between ePDGs, the UE may be temporarily connected to two ePDGs.
>
> 3GPP TS 23.402 version 12.10.0 Release 12

In some of the exemplary embodiments discussed above, the mobile node has been updating and building up its reachability list based on the successful and failed connection attempts to trusted packet data gateways. In another embodiment, the reachability list of the mobile node may be received from another mobile node or network node in the access network or core network connected thereto. The received reachability list could be used to update the already existing "local" reachability list of the mobile node or as a replacement thereof.

8,792,453 Specification, Col 5 65-70, Col 6 1-7

In another embodiment of the invention, the reachability list is listing data sets. The data sets indicate data paths and the reachability status of respective known trusted packet data gateways for each respective data path. The way a respective data path is indicated in the reachability list is implementation specific. For example the data paths could be indicated by combinations of access network identifiers, core network identifiers and access point names, combinations of core network identifiers and access point names or simply by access point names.

8,792,453 Specification, Col 5 20-29

173. The 3GPP UE establishes a secure IPsec tunnel to the trusted data packet gateway (ePDG) determined from the reachability list maintained in the UE (mobile node) prior to attaching to the target access network.

4.5.4 ePDG Selection

Otherwise if the ePDG needs to be dynamically selected the procedure is as follows:

- The UE constructs an FQDN using the HPLMN ID and employs the DNS server function to obtain the IP address(es) of the ePDG(s).
- The UE selects an ePDG address from the list returned in the DNS response and initiates the IPsec tunnel establishment.

A UE connected to one or multiple PDN GWs uses a single ePDG. In case of handover between ePDGs, the UE may be temporarily connected to two ePDGs.

3GPP TS 23.402 version 12.10.0 Release 12

ZYXEL INFRINGES SPV's PATENTS

174. Zyxel infringes, directly and indirectly, certain claims of U.S. Patent Nos. 7,796,512, 8,045,531, 8,270,384, 8,442,569, 8,467,723, and 8,792,453.

COUNT 1

INFRINGEMENT OF U.S. PATENT NO. 7,796,512

175. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

176. SPV is the owner, by assignment, of U.S. Patent No. 7,796,512. The

'512 Patent was issued by the United States Patent and Trademark Office on September 14, 2010.

177. As the owner of the '512 Patent, SPV holds all substantial rights in and under the '512 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

178. The '512 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

179. Zyxel has infringed, and continues to infringe, at least claim 1 of the '512 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services, which include Zyxel Access Points enabled for compliance with 802.11k/r and related software and mobile applications.

180. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the '512 Patent and feature functionality that meets each and every limitation of at least claim 1.

181. Zyxel has used and tested the Zyxel Accused Products in the United States.

182. Zyxel's users, customers, agents and/or other third parties (collectively, "third-party infringers") have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused

Products in accordance with instructions and direction from Zyxel.

183. Zyxel has, since at least as early as May 13, 2022, known or been willfully blind to the fact that the third-party infringers' use of the Zyxel Accused Products directly infringes the '512 Patent.

184. Zyxel's knowledge of the '512 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the '512 Patent demonstrates Zyxel's intent for the third-party infringers to use them to infringe.

185. With knowledge of or willful blindness to the fact that the third-party infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '512 Patent are met directly infringes the '512 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '512 Patent by making, using, testing, selling, offering for sale, importing and/or licensing the accused products by, for example: marketing Zyxel's Access Point 802.11 k/r switching capabilities to the third-party infringers; supporting and managing the third-party infringers' use of the Zyxel 801.11 k/r functionalities; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the

802.11 k/r switching features of the Zyxel Accused Products.

186. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the'512 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;
- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

187. Zyxel has induced and continues to induce infringement of the asserted claims of the '512 Patent under 35 U.S.C. § 271(b).

188. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '512 Patent. For example, these include the Zyxel Accused Products include 802.11 k/r switching features identified above which the third-party infringers used in a manner such

that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

189. The 802.11 k/r switching features are not a staple article or commodity of commerce, and, because the functionality is designed to work solely in a manner that is covered by the '512 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and adapted for—and was in fact used in—the accused products in a manner that is claimed in the '512 Patent.

190. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '512 Patent under 35 U.S.C. § 271(c).

191. Zyxels' acts of infringement of the '512 Patent are ongoing and have continued since notice and have been, therefore, carried out with knowledge of the'512 Patent and how the Zyxel Accused Products infringe them. Rather than take a license to the '512 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

192. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages

sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

COUNT 2
INFRINGEMENT OF U.S. PATENT NO. 8,045,531

193. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

194. SPV is the owner, by assignment, of U.S. Patent No. 8,045,531. The '531 Patent was issued by the United States Patent and Trademark Office on October 25, 2011.

195. As the owner of the '531 Patent, SPV holds all substantial rights in and under the '531 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

196. The '531 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

197. Zyxel has infringed, and continues to infringe, at least claim 1 of the '531 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services, which include Zyxel Nebula products and the Nebula platform, NebulaFlex/NebulaFlex Pro functionality, cloud controllers, Nebula Access Points, including those enabled for compliance with

802.11k/r, Zyxel wireless LAN controllers (including, for example, the Zyxel NXC2500 and NXC 550) and Access Points utilizing the CAPWAP protocol, Zyxel products featuring TR-069 remote management protocol including, for example Zyxel Band Pilot Remote Management System and MPro Mesh Solutions, and related software and mobile applications. These products include, without limitation, the Zyxel Nebula WiFi system comprising, by way of example, Zyxel Nebula cloud controller devices that interface with Zyxel APs to provide WLAN service. Infringing Zyxel WiFi Systems also comprise one or more Nebula APs (WAPs) managed by a Nebula Controller including, without limitation, Zyxel Access Points Models NWA50AX, NWA90AX, NWA55AXE, NWA110AX, NWA210AX, NWA1122ACv2, NWA1123-AC PRO, WAX510D, WAX610D, WAX6305, WAX5505, NWA5123-AC HD, WAC6302D-5v2, WAC50D, WAC500H, WAC6103D-I, WAC6302D-5, WAC6503D-S, WAC6553D-5, and WAC6552D-E. Additional Zyxel Accused Products with respect to the ’531 patent include the Zyxel Systems featuring Zyxel APs and Zyxel access controllers (ACs including, for example, Zyxel NXC2500 and NXC5500 wireless controllers) that support configuration using the CAPWAP protocol to provide service in a WLAN

198. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the ’531 Patent and feature

functionality that meets each and every limitation of at least claim 1.

199. Zyxel has used and tested the Zyxel Accused Products in the United States.

200. Zyxel's users, customers, agents and/or other third parties (collectively, "third-party infringers") have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused Products in accordance with instructions and direction from Zyxel.

201. Zyxel has, since at least as early as May 13, 2022, known or been willfully blind to the fact that the third-party infringers' use of the Zyxel Accused Products directly infringes the '531 Patent.

202. Zyxel's knowledge of the '531 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the '531 Patent demonstrates Zyxel's intent for the third-party infringers to use them to infringe.

203. With knowledge of or willful blindness to the fact that the third-party infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '531 Patent are met directly infringes the '531 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '531 Patent by making, using, testing, selling, offering for sale, importing and/or licensing the accused products by, for example: marketing Zyxel's product capabilities to the third-party infringers; supporting and managing

the third-party infringers' use of the infringing Zyxel functionality; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the Zyxel Accused Products to practice the '531 Patent.

204. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the'531 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;
- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

205. Zyxel has induced and continues to induce infringement of the asserted claims of the '531 Patent under 35 U.S.C. § 271(b).

206. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '531 Patent. For example, these include the Zyxel Accused Products hardware and software for performing communication and switching functionality identified herein that the third-party infringers used in a manner such that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

207. These features are not a staple article or commodity of commerce, and, because the functionality is designed to work solely in a manner that is covered by the '531 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and adapted for—and was in fact used in—the accused products in a manner that is claimed in the '531 Patent.

208. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '531 Patent under 35 U.S.C. § 271(c).

209. Zyxels' acts of infringement are ongoing and have continued since notice and have been, therefore, carried out with knowledge of the'531 Patent and

how the Zyxel Accused Products infringe them. Rather than take a license to the '531 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

210. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

COUNT 3
INFRINGEMENT OF U.S. PATENT NO. 8,270,384

211. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

212. SPV is the owner, by assignment, of U.S. Patent No. 8,270,384. The '384 Patent was issued by the United States Patent and Trademark Office on September 18, 2012.

213. As the owner of the '384 Patent, SPV holds all substantial rights in and under the '384 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

214. The '384 Patent is valid, enforceable and was duly issued in full

compliance with Title 35 of the United States Code.

215. Zyxel has infringed, and continues to infringe, at least claim 1 of the '384 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services, which include Zyxel Nebula products and the Nebula platform, NebulaFlex/NebulaFlex Pro functionality, cloud controllers, Nebula Access Points, including those enabled for compliance with 802.11k/r, Zyxel wireless LAN controllers (including, for example, the Zyxel NXC2500 and NXC 550) and Access Points utilizing the CAPWAP protocol, Zyxel products featuring TR-069 remote management protocol including, for example Zyxel Band Pilot Remote Management System and MPro Mesh Solutions, and related software and mobile applications. These products include, without limitation, the Zyxel Nebula WiFI system comprising, by way of example Zyxel Nebula cloud controller devices that interface with Zyxel APs to provide WLAN service. Accused Zyxel WiFi Systems also comprise one or more Nebula APs (WAPs) managed by a Nebula Controller including, without limitation, Zyxel Access Points Models NWA50AX, NWA90AX, NWA55AXE, NWA110AX, NWA210AX, NWA1122ACv2, NWA1123-AC PRO, WAX510D, WAX610D, WAX6305, WAX5505, NWA5123-AC HD, WAC6302D-5v2, WAC50D, WAC500H, WAC6103D-I, WAC6302D-5, WAC6503D-S, WAC6553D-5, and WAC6552D-E. Additional Zyxel Accused Products with respect to the '531

patent include the Zyxel Systems featuring Zyxel APs and Zyxel access controllers (ACs including, for example, Zyxel NXC2500 and NXC5500 wireless controllers) that support configuration using the CAPWAP protocol to provide service in a WLAN.

216. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the ’384 Patent and feature functionality that meets each and every limitation of at least claim 1.

217. Zyxel has used and tested the Zyxel Accused Products in the United States.

218. Zyxel’s users, customers, agents and/or other third parties (collectively, “third-party infringers”) have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused Products in accordance with instructions and direction from Zyxel.

219. Zyxel has, since at least as early as May 13, 2022, known or been willfully blind to the fact that the third-party infringers’ use of the Zyxel Accused Products directly infringes the ’384 Patent.

220. Zyxel’s knowledge of the ’384 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the ’384 Patent demonstrates Zyxel’s intent for the third-party infringers to use them to infringe.

221. With knowledge of or willful blindness to the fact that the third-party

infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '384 Patent are met directly infringes the '384 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '384 Patent by making, using, testing, selling, offering for sale, importing and/or licensing the accused products by, for example: marketing Zyxel's product capabilities to the third-party infringers; supporting and managing the third-party infringers' use of the infringing Zyxel functionality; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the Zyxel Accused Products to practice the '384 Patent.

222. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the '384 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;

- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

223. Zyxel has induced and continues to induce infringement of the asserted claims of the '384 Patent under 35 U.S.C. § 271(b).

224. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '384 Patent. For example, these include the Zyxel Accused Products hardware and software for performing communication and switching functionality identified herein that the third-party infringers used in a manner such that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

225. These features are not a staple article or commodity of commerce, and, because the functionality is designed to work solely in a manner that is covered by the '384 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and

adapted for—and was in fact used in—the accused products in a manner that is claimed in the '384 Patent.

226. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '384 Patent under 35 U.S.C. § 271(c).

227. Zyxels' acts of infringement are ongoing and have continued since notice and have been, therefore, carried out with knowledge of the'531 Patent and how the Zyxel Accused Products infringe them. Rather than take a license to the '384 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

228. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

COUNT 4
INFRINGEMENT OF U.S. PATENT NO. 8,442,569

229. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

230. SPV is the owner, by assignment, of U.S. Patent No. 8,442,569. The

’569 Patent was issued by the United States Patent and Trademark Office on May 14, 2013.

231. As the owner of the ’569 Patent, SPV holds all substantial rights in and under the ’569 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

232. The ’569 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

233. Zyxel has infringed, and continues to infringe, at least claim 1 of the ’384 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services, which include Zyxel Datalogic devices that support License-Assisted Access (LAA), Zyxel’s 5G NR/4G LTE CPE products (under its Service Provider products), its Mobile Broadband 4G LTE products (under its Business products) are enabled for LAA, and related software and mobile applications.

234. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the ’569 Patent and feature functionality that meets each and every limitation of at least claim 1.

235. Zyxel has used and tested the Zyxel Accused Products in the United States.

236. Zyxel’s users, customers, agents and/or other third parties

(collectively, "third-party infringers") have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused Products in accordance with instructions and direction from Zyxel.

237. Zyxel has, since at least as early as September 20, 2024, known or been willfully blind to the fact that the third-party infringers' use of the Zyxel Accused Products directly infringes the '569 Patent.

238. Zyxel's knowledge of the '569 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the '569 Patent demonstrates Zyxel's intent for the third-party infringers to use them to infringe.

239. With knowledge of or willful blindness to the fact that the third-party infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '569 Patent are met directly infringes the '569 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '569 Patent by making, using, testing, selling, offering for sale, importing and/or licensing the accused products by, for example: marketing Zyxel's product capabilities to the third-party infringers; supporting and managing the third-party infringers' use of the infringing Zyxel functionality; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge

center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the Zyxel Accused Products to practice the '569 Patent.

240. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the '569 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;
- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

241. Zyxel has induced and continues to induce infringement of the asserted claims of the '569 Patent under 35 U.S.C. § 271(b).

242. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '569 Patent. For

example, these include the Zyxel Accused Products hardware and software enabling LAA functionality and compliance identified herein that the third-party infringers used in a manner such that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

243. These features are not a staple article or commodity of commerce, and, because the functionality is designed to work solely in a manner that is covered by the '569 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and adapted for—and was in fact used in—the accused products in a manner that is claimed in the '569 Patent.

244. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '569 Patent under 35 U.S.C. § 271(c).

245. Zyxels' acts of infringement are ongoing and have continued since notice and have been, therefore, carried out with knowledge of the '569 Patent and how the Zyxel Accused Products infringe them. Rather than take a license to the '569 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

246. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

COUNT 5
INFRINGEMENT OF U.S. PATENT NO. 8,467,723

247. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

248. SPV is the owner, by assignment, of U.S. Patent No. 8,467,723. The '723 Patent was issued by the United States Patent and Trademark Office on June 18, 2013.

249. As the owner of the '723 Patent, SPV holds all substantial rights in and under the '723 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

250. The '723 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

251. Zyxel has infringed, and continues to infringe, at least claim 5 of the '723 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services enabled to perform Inter-RAT handover. These products include, without limitation, Zyxel's 5G NR/4G LTE

CPE (under its Service Provider products) and its Mobile Broadband 4G LTE products (under its Business products) that are enabled to perform Inter-RAT handover such as the LTE7461-M602 / 4G LTE-A Outdoor Router, LTE7480-S905 / 4G LTE-A CBRS Outdoor Router, LTE7485-S905 / 4G LTE-A CBSD Category B Outdoor Router, LTE5388-S905 / 4G LTE-A CBRS Indoor Router, NR5201 / 5G NR Indoor Router, NR5203 / 5G NR Indoor Router, R7201 / 5G NR Outdoor Router, NR7203 / 5G NR Outdoor Router, the NR7223 / 5G NR Outdoor Router, and related software and mobile applications.

252. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the '723 Patent and feature functionality that meets each and every limitation of at least claim 5.

253. Zyxel has used and tested the Zyxel Accused Products in the United States.

254. Zyxel's users, customers, agents and/or other third parties (collectively, "third-party infringers") have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused Products in accordance with instructions and direction from Zyxel.

255. Zyxel has, since at least as early as May 13, 2022, known or been willfully blind to the fact that the third-party infringers' use of the Zyxel Accused Products directly infringes the '723 Patent.

256. Zyxel's knowledge of the '723 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the '723 Patent demonstrates Zyxel's intent for the third-party infringers to use them to infringe.

257. With knowledge of or willful blindness to the fact that the third-party infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '723 Patent are met directly infringes the '723 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '723 Patent by making, using, testing, selling, offering for sale, importing and/or licensing the accused products by, for example: marketing Zyxel's product capabilities to the third-party infringers; supporting and managing the third-party infringers' use of the infringing Zyxel functionality; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the Zyxel Accused Products to practice the '723 Patent.

258. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the '723 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to

encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;
- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

259. Zyxel has induced and continues to induce infringement of the asserted claims of the '723 Patent under 35 U.S.C. § 271(b).

260. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '723 Patent. For example, these include the Zyxel Accused Products featuring hardware and software enabling Inter-RAT handover herein that the third-party infringers used in a manner such that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

261. These features are not a staple article or commodity of commerce,

and, because the functionality is designed to work solely in a manner that is covered by the '723 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and adapted for—and was in fact used in—the accused products in a manner that is claimed in the '723 Patent.

262. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '723 Patent under 35 U.S.C. § 271(c).

263. Zyxels' acts of infringement are ongoing and have continued since notice and have been, therefore, carried out with knowledge of the '723 Patent and how the Zyxel Accused Products infringe them. Rather than take a license to the '723 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

264. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

COUNT 6
INFRINGEMENT OF U.S. PATENT NO. 8,792,453

265. SPV realleges and incorporates by reference the allegations set forth above as if restated verbatim here.

266. SPV is the owner, by assignment, of U.S. Patent No. 8,792,453. The '453 Patent was issued by the United States Patent and Trademark Office on July 29, 2014.

267. As the owner of the '453 Patent, SPV holds all substantial rights in and under the '453 Patent, including the right to grant licenses, exclude others, and to enforce, sue, and recover damages for past and future infringement.

268. The '453 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

269. Zyxel has infringed, and continues to infringe, at least claim 1 of the '453 Patent by making, using, selling, offering to sell, and/or importing into the United States the accused products and services enabled to establish a secure tunnel to a trusted packet data gateway and include, without limitation, Zyxel 5G NR/4G LTE CPE (under its Service Provider products) and its Mobile Broadband 4G LTE products (under its Business products), for example the Zyxel LTE7480-S905 4G LTE-A Outdoor Router and Zyxel LTE5388-S905 4G LTE-A CBRS Indoor Router, and related software and mobile applications that are enabled to perform this method by connecting to a 4G or 5G network.

270. The Zyxel Accused Products are designed, manufactured, and intended to be used in normal operation to practice the '453 Patent and feature functionality that meets each and every limitation of at least claim 5.

271. Zyxel has used and tested the Zyxel Accused Products in the United States.

272. Zyxel's users, customers, agents and/or other third parties (collectively, "third-party infringers") have infringed and continue to infringe the asserted claims including under 35 U.S.C. § 271(a) by using the Zyxel Accused Products in accordance with instructions and direction from Zyxel.

273. Zyxel has, since at least as early as September 20, 2024, known or been willfully blind to the fact that the third-party infringers' use of the Zyxel Accused Products directly infringes the '453 Patent.

274. Zyxel's knowledge of the '453 Patent and how the function, structure, and operation of the Zyxel Accused Products practice the '453 Patent demonstrates Zyxel's intent for the third-party infringers to use them to infringe.

275. With knowledge of or willful blindness to the fact that the third-party infringers' use of the Zyxel Accused Products in their intended manner such that all limitations of the asserted claims of the '453 Patent are met directly infringes the '453 Patent, Zyxel has actively encouraged the third-party infringers to directly infringe the '453 Patent by making, using, testing, selling, offering for sale,

importing and/or licensing the accused products by, for example: marketing Zyxel's product capabilities to the third-party infringers; supporting and managing the third-party infringers' use of the infringing Zyxel functionality; and providing technical assistance to the third-party infringers during their continued use of the Zyxel Accused Products such as by, for example, publishing instructional information on the Zyxel websites (including, without limitation, the knowledge center, instructional videos and on the Zyxel branded websites) directing and encouraging third-party infringers how to make and use the Zyxel Accused Products to practice the '453 Patent.

276. Zyxel specifically intends to induce, and did induce, the third-party infringers to infringe the '453 Patent by, for example, providing instructions, encouragement, and direction through publications and materials intended to encourage, aid, and abet infringing use. Exemplary publications include:

- https://www.zyxel.com/us/en-us/support;
- https://community.zyxel.com/en;
- https://mysupport.zyxel.com/hc/en-us;
- https://www.zyxel.com/us/en-us/support/download;
- https://info.zyxel.com/infographic;
- https://www.zyxel.com/global/en/support/security-advisories; and
- www.zyxel.com (including help documentation).

277. Zyxel has induced and continues to induce infringement of the asserted claims of the '453 Patent under 35 U.S.C. § 271(b).

278. Zyxel has sold, provided and/or licensed to the third-party infringers and continues to sell, provide and/or license the Zyxel Accused Products that are especially made and adapted—and specifically intended by Zyxel—to be used as components and material parts of the inventions claimed in the '453 Patent. For example, these include the Zyxel Accused Products featuring hardware and software enabling Inter-RAT handover herein that the third-party infringers used in a manner such that all limitations of the asserted claims are met, and without which the third-party infringers would have been unable to use and avail themselves of the intended functionality of the accused products.

279. These features are not a staple article or commodity of commerce, and, because the functionality is designed to work solely in a manner that is covered by the '453 Patent, it has no substantial non-infringing use. Zyxel knew of or was willfully blind to the fact that such functionality was especially made and adapted for—and was in fact used in—the accused products in a manner that is claimed in the '453 Patent.

280. Zyxel has contributorily infringed and continues to contributorily infringe the asserted claims of the '453 Patent under 35 U.S.C. § 271(c).

281. Zyxels' acts of infringement are ongoing and have continued since

notice and have been, therefore, carried out with knowledge of the '453 Patent and how the Zyxel Accused Products infringe them. Rather than take a license to the '453 Patent, Zyxel's ongoing infringing conduct reflects a business decision to "efficiently infringe" the asserted claims and in doing so constitutes willful infringement under the standard of *Halo Elecs., Inc. v. Pulse Elecs., Inc*., 136 S. Ct. 1923 (2016).

282. Zyxel's acts of direct and indirect infringement have caused and continue to cause damage to SPV for which SPV is entitled to recover damages sustained as a result of Zyxel's infringing 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, pursuant to 35 U.S.C. § 284.

NOTICE OF REQUIREMENT OF LITIGATION HOLD

283. Zyxel is hereby notified it is legally obligated to locate, preserve, and maintain all records, notes, drawings, documents, data, communications, materials, electronic recordings, audio/video/photographic recordings, and digital files, including edited and unedited or "raw" source material, and other information and tangible things that Zyxel knows, or reasonably should know, may be relevant to actual or potential claims, counterclaims, defenses, and/or damages by any party or potential party in this lawsuit, whether created or residing in hard copy form or in the form of electronically stored information (hereafter collectively referred to as

"Potential Evidence").

284. As used above, the phrase "electronically stored information" includes without limitation: computer files (and file fragments), e-mail (both sent and received, whether internally or externally), information concerning e-mail (including but not limited to logs of e-mail history and usage, header information, and deleted but recoverable e-mails), text files (including drafts, revisions, and active or deleted word processing documents), instant messages, audio recordings and files, video footage and files, audio files, photographic footage and files, spreadsheets, databases, calendars, telephone logs, contact manager information, internet usage files, and all other information created, received, or maintained on any and all electronic and/or digital forms, sources and media, including, without limitation, any and all hard disks, removable media, peripheral computer or electronic storage devices, laptop computers, mobile phones, personal data assistant devices, Blackberry devices, iPhones, video cameras and still cameras, and any and all other locations where electronic data is stored. These sources may also include any personal electronic, digital, and storage devices of any and all of Zyxel's agents, resellers, distributors or employees if Zyxel's electronically stored information resides there.

285. Zyxel is hereby further notified and forewarned that any alteration, destruction, negligent loss, or unavailability, by act or omission, of any Potential

Evidence may result in damages or a legal presumption by the Court and/or jury that the Potential Evidence is not favorable to Zyxel's claims and/or defenses. To avoid such a result, Zyxel's preservation duties include, but are not limited to, the requirement that Zyxel immediately notify its agents, distributors, and employees to halt and/or supervise the auto-delete functions of Zyxel's electronic systems and refrain from deleting Potential Evidence, either manually or through a policy of periodic deletion.

NOTICE

286. SPV does not currently distribute, sell, offer for sale, or make products embodying the Asserted Patents.

287. SPV provided actual notice of infringement of the '512, '531, '384, and '723 Patents to Zyxel on or about May 13, 2022, and SPV provided actual notice of infringement of the '569 and '453 Patents to Zyxel on or about September 20, 2024.

288. SPV has complied with all notice requirements of 35 U.S.C. § 287.

JURY DEMAND

SPV hereby demands a trial by jury on all claims, issues, and damages so triable.

PRAYER FOR RELIEF

SPV prays for the following relief:

a. That Zyxel be summoned to appear and answer;

b. That the Court enter judgment that Zyxel has infringed the '512, '531, '384, '569, '723 and '453 Patents.

c. That the Court grant SPV judgment against Zyxel for all actual, consequential, special, punitive, increased, and/or statutory damages, including, if necessary, an accounting of all damages; pre- and post-judgment interest as allowed by law; and reasonable attorney's fees, costs, and expenses incurred in this action;

d. That Zyxel's infringement be found to have been willful;

e. That this case be found to be exceptional under 35 U.S.C. § 285; and

f. That SPV be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 18, 2024

Respectfully submitted,

CONNOR LEE & SHUMAKER PLLC

By: 

Cabrach J. Connor
Cab@CLandS.com
Texas Bar No. 24036390
Jennifer Tatum Lee
Jennifer@CLandS.com
Texas Bar No. 24046950
John M. Shumaker
John@CLandS.com
Texas Bar No. 24033069

609 Castle Ridge Road, Suite 450

Austin, Texas 78746
512.646.2060 Telephone
888.387.1134 Facsimile