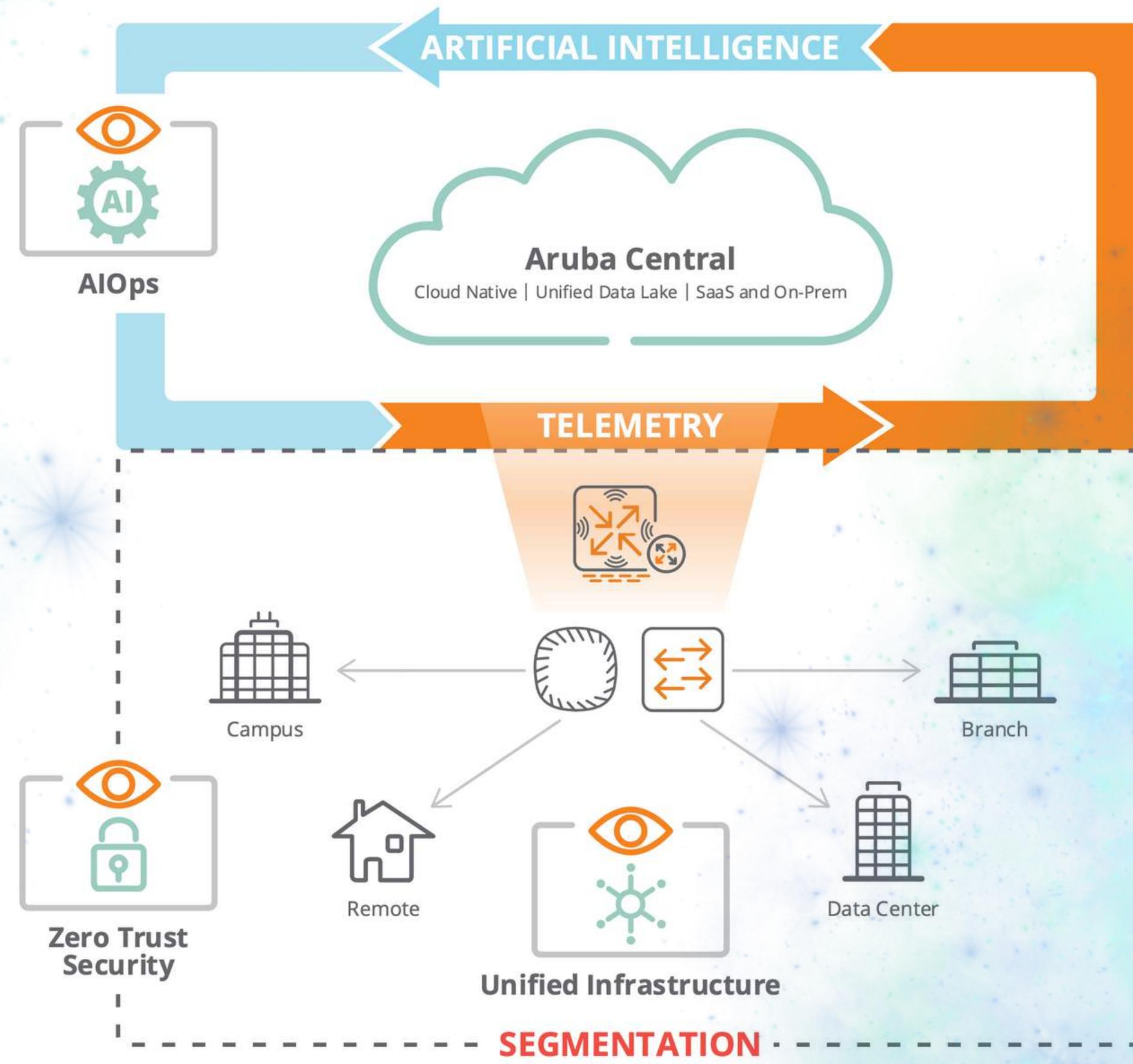


WIRELESS LAN DESIGN





RADIO FREQUENCY DESIGN

The primary design goal should be to determine the number and placement of APs required to support the projected number and density of clients while limiting co-channel interference and maximizing throughput.





RF SIGNAL COVERAGE

An important RF design consideration is the differing propagation patterns between higher and lower radio frequencies.

WLAN designs should target 5GHz signal coverage to ensure maximum network performance and capacity.

When properly implemented, a 5GHz network design can upgrade easily to 6GHz due to the similarity in propagation characteristics.

ACCESS POINT PLACEMENT

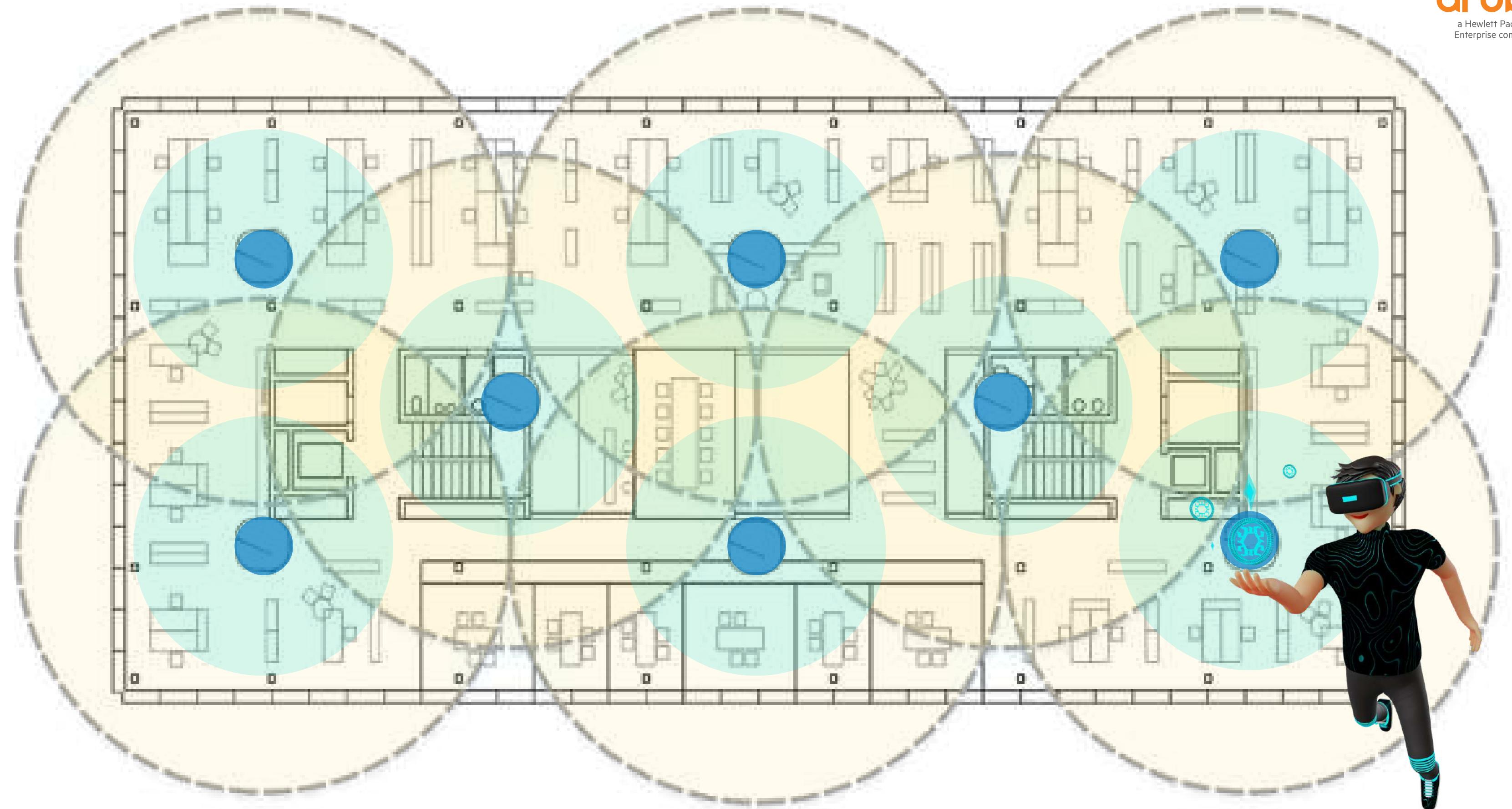
Space APs **10-15 meters** apart

Consider client performance, architecture, and interior design.

Design for the following capacity:

- > **30-40 clients per AP**
- > **2.5 Wi-Fi devices carried per user** (laptop, phone, tablet, smartwatch, etc.) with a 50% connection rate.
- > Add APs to areas with frequent or increased user **density**.
Conference rooms, atriums, or special event areas.
- > Identify peak-load periods when the WLANs have the highest usage or visibility.





CHANNEL PLANNING

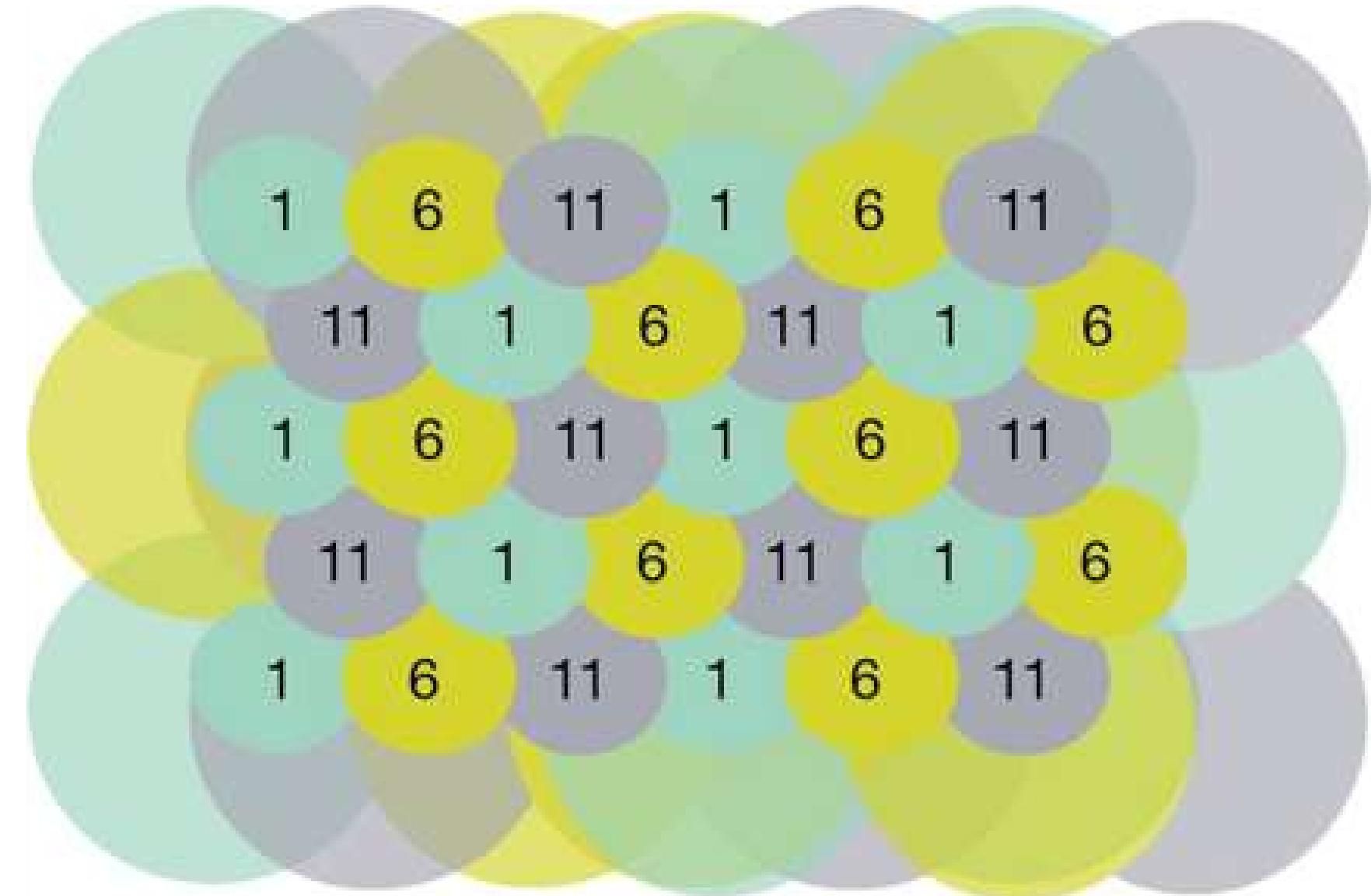
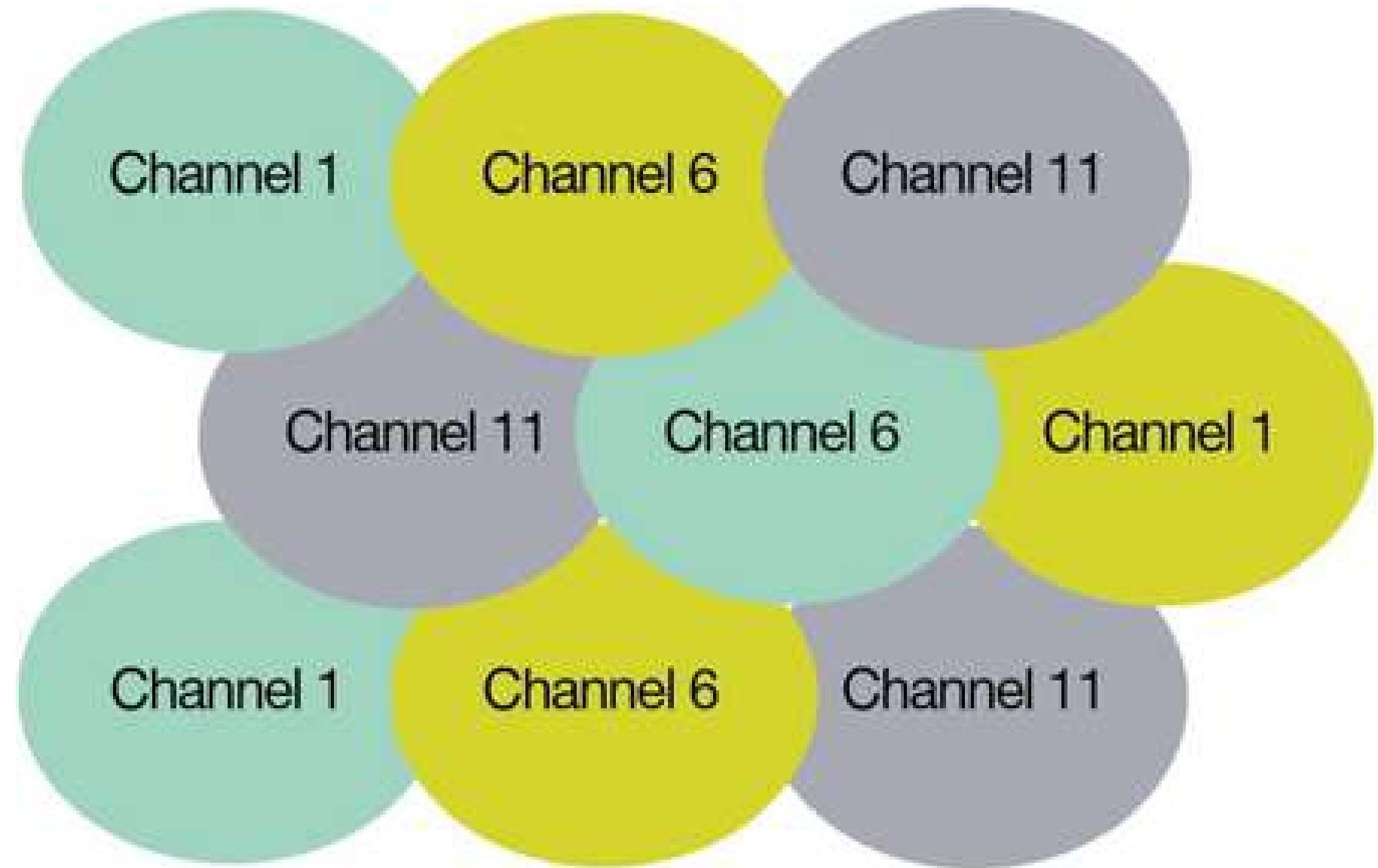
aruba
a Hewlett Packard
Enterprise company

5GHZ CHANNEL WIDTH

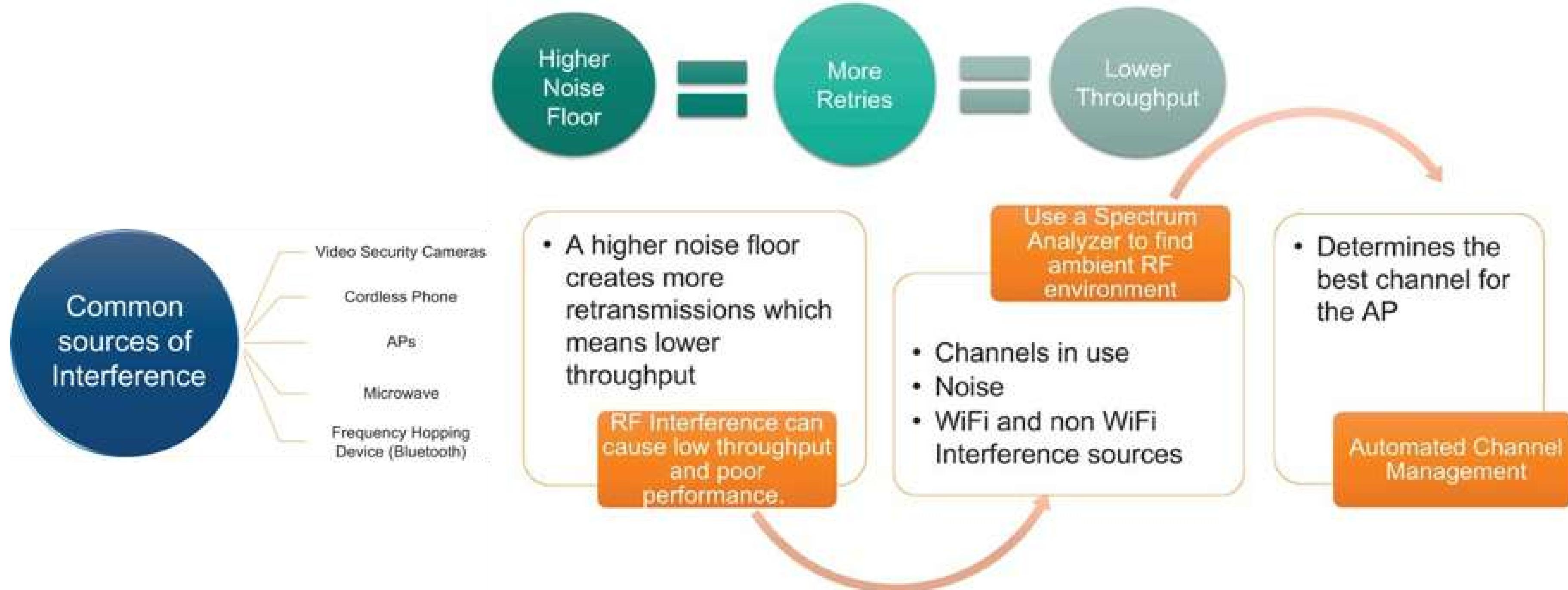
An important decision for 5 GHz deployments is the channel width to use.

Wider channels mean higher throughput for individual clients but fewer non-overlapping channels, while narrower channels result in lower data rates per client but more available channels, and thus less risk of co-channel interference.





RF coverage versus capacity



RF problems

2.4 GHz, minimum power threshold to 6 dBm and the maximum to 12 dBm.

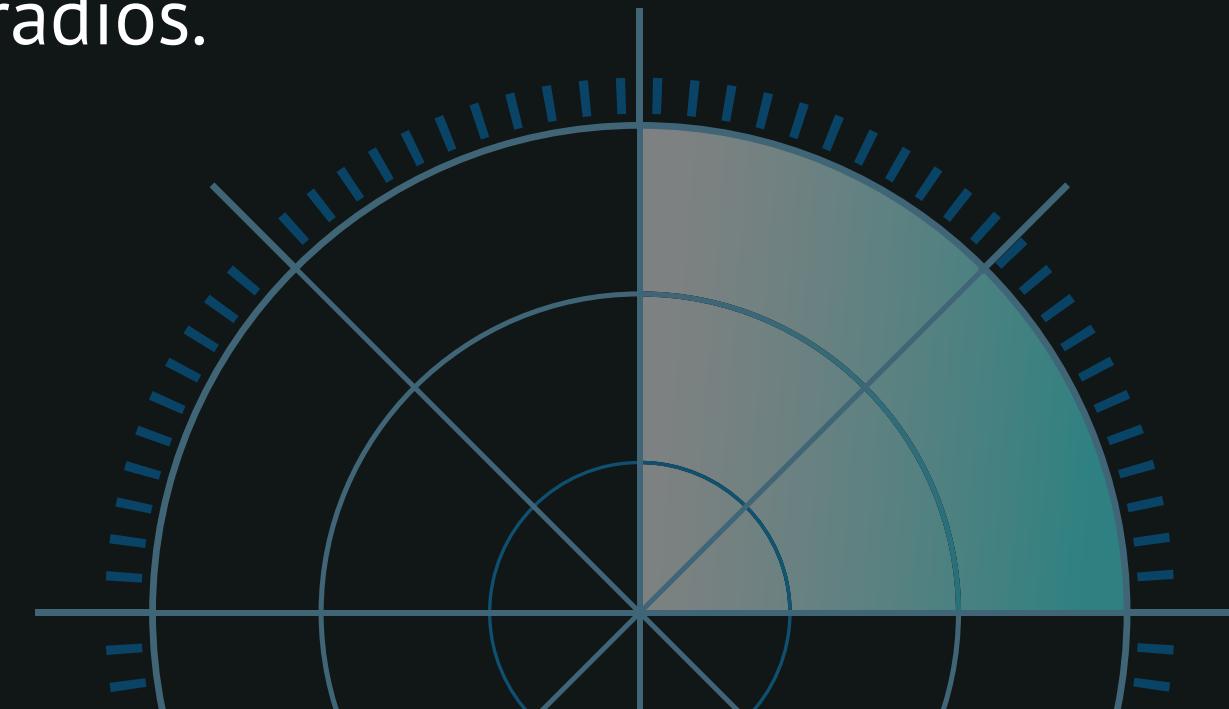
5 GHz, power threshold minimum to 18 dBm, maximum to 21 dBm.



POWER SETTINGS

Do not exceed a power level difference of 6 dBm between the minimum and maximum settings on all radio bands.

The transmit power for 5 GHz radios should be 6 dBm higher than for 2.4 GHz radios.



แนวทางการใช้ความถี่วิทยุย่าน 2.4 GHz และ 5 GHz
ในการให้บริการอินเทอร์เน็ต แบบ WiFi

1. ความถี่วิทยุท่อนูญาตให้ใช้งาน

1.1 ความถี่วิทยุย่าน 2.4 GHz และ 5 GHz ท่อนูญาตให้ใช้งานสำหรับการให้บริการอินเทอร์เน็ต

ช่วงความถี่วิทยุ (GHz)	กำลังส่งสูงสุดท่อนูญาตให้ใช้งาน E.I.R.P. (วัตต์)	เงื่อนไขการใช้งาน
2.400 – 2.500	0.1	ภายในอาคาร/ภายนอกอาคาร
5.150 – 5.350	0.2	ภายในอาคารท่า�ัน
5.470 – 5.725	1.0	ภายในอาคาร/ภายนอกอาคาร
5.725 – 5.850	1.0	ภายในอาคาร/ภายนอกอาคาร

1.2 วิธีการวัดกำลังส่ง

กำลังส่งสูงสุดท่อนูญาตให้ใช้งานกำหนดเป็นกำลังส่งของอากาศสมมูลแบบไอโซทรอปิก (Equivalent Isotropically Radiated Power : E.I.R.P.) ค่านิวนัณดังนี้

E.I.R.P. = กำลังส่งของเครื่องส่ง (Transmitter Power) ในหน่วยของ dBW
หรือ dBm + อัตราขยายสายอากาศ (Antenna Gain) ในหน่วยของ dBi

หมายเหตุ: โดยทั่วไป กรณีของเครื่องส่งที่มีการติดตั้งสายอากาศในตัว (integral antenna) หรือมีการติดตั้งสายอากาศเข้ากับตัวเครื่องส่งโดยตรง จะไม่นำค่าความสูญเสียกำลังของสัญญาณมาคำนวณด้วย

1.3 การอนุญาตให้ใช้งานในลักษณะ Point to Point หรือ Point to Multipoint

ผู้รับใบอนุญาตสามารถใช้งานความถี่วิทยุเฉพาะช่วง 5.725 – 5.850 GHz โดยมีกำลังส่ง (E.I.R.P.) ไม่เกิน 1 วัตต์ท่านนั้น ในลักษณะของข่ายเชื่อมโยง Point to Point หรือ Point to Multipoint เชื่อมต่อจากจุดหนึ่งไปยังอีกจุดหนึ่งเพื่อการกระจายสัญญาณการให้บริการอินเทอร์เน็ต ไม่อนุญาตให้ใช้ความถี่วิทยุในช่วงอื่นในข้อ 1.1 ในลักษณะข่ายเชื่อมโยง

ทั้งนี้ การอนุญาตให้ใช้งานความถี่วิทยุข้างต้นไม่วรวมถึงการใช้งานเป็นข่ายเชื่อมโยง (link) หรือนำไปใช้งานทดแทนบริการเดิมโดยระบบ Microwave link ซึ่งเป็นการให้บริการเชื่อมโยงโครงข่ายในกิจการวิทยุคมนาคมประจำที่ (Fixed Service) โดยการใช้งานในลักษณะดังกล่าว ผู้ใช้งานหรือผู้รับใบอนุญาตจะต้องได้รับการจัดสรรคุณภาพถ้วนตามแผนความถี่วิทยุกิจการประจำที่ ตามหลักเกณฑ์และวิธีการที่ กสทช. กำหนด

หมายเหตุ: ผู้รับใบอนุญาต หมายถึง ผู้รับใบอนุญาตการให้บริการอินเทอร์เน็ต หรือผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม

1.4 ข้อกฎหมายที่เกี่ยวข้อง

1.4.1 ความถี่วิทยุย่าน 2.4 GHz

1) ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง เครื่องวิทยุคมนาคมและสถานีวิทยุ-คมนาคมที่ได้รับยกเว้นไม่ต้องได้รับใบอนุญาต

2) ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ ว่าด้วยมาตรฐานทางเทคนิคของเครื่องโทรคมนาคมและอุปกรณ์ เรื่อง เครื่องวิทยุคมนาคมที่ใช้เทคโนโลยี Broadband Wireless Access ในลักษณะ Radio Local Area Network (RLAN)

1.4.2 ความถี่วิทยุย่าน 5 GHz

- 1) ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง การใช้ความถี่วิทยุสำหรับอุปกรณ์สื่อสารระยะสั้น (Short Range Devices) ย่านความถี่วิทยุ 5 GHz
- 2) ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ ว่าด้วยมาตรฐานทางเทคนิคของเครื่องโทรคมนาคมและอุปกรณ์ เรื่อง เครื่องวิทยุคมนาคมที่ใช้เทคโนโลยี Broadband Wireless Access ในลักษณะ Radio Local Area Network (RLAN)
- 3) มติคณะกรรมการกิจการโทรคมนาคม ครั้งที่ 10/2559 เมื่อวันที่ 17 พฤษภาคม 2559

2. เงื่อนไขในการอนุญาต

2.1 การใช้งานความถี่วิทยุย่าน 2.4 GHz และ 5 GHz สำหรับการให้บริการอินเทอร์เน็ต จะไม่ได้รับการคุ้มครองการบกวน และหากมีการบกวนข่ายการสื่อสารอื่นที่ได้รับอนุญาตให้ใช้คุณภาพถ้วน จึงต้องแก้ไขการบกวนหรือยุติการใช้งานทันที

2.2 การใช้งานความถี่วิทยุโดยย่าน 2.4 GHz และ 5 GHz โดยมีกำลังส่ง E.I.R.P. ตามที่กำหนด ได้รับยกเว้นใบอนุญาตวิทยุคมนาคมที่เกี่ยวข้อง

2.3 เครื่องโทรคมนาคมและอุปกรณ์ที่ผู้รับใบอนุญาตนามาใช้ในการให้บริการ จะต้องผ่านการดำเนินการตามแนวทางการตรวจสอบมาตรฐานของเครื่องโทรคมนาคมและอุปกรณ์มาตรฐานเครื่องวิทยุคมนาคมที่ใช้เทคโนโลยี Broadband Wireless Access ในลักษณะ Radio Local Area Network (RLAN) (กสทช. มท. 1012-2551) ดังนี้

- 1) การแสดงความสอดคล้องตามมาตรฐานตามหลักการรับรองตนเองของผู้ประกอบการ
- 2) การแสดงความสอดคล้องตามมาตรฐานความปลอดภัยให้การส่งออกสารประเมินประกอบการรับรองตนเองของผู้ประกอบการ

3. การบังคับทางปกติและทำหนดโทษ

3.1 ผู้รับใบอนุญาตจะต้องปฏิบัติตามกฎหมายและเงื่อนไขในการอนุญาตที่เกี่ยวข้อง โดยหากพบว่า ผู้รับใบอนุญาตฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายและเงื่อนไขในการอนุญาตที่เกี่ยวข้อง กสทช. อาจพักใช้หรือเพิกถอนใบอนุญาตได้

3.2 กรณีที่ผู้รับใบอนุญาตมีการใช้งานความถี่วิทยุโดยใช้กำลังส่งเกินกว่าที่กำหนด จะเข้าข่ายเป็นการใช้คุณภาพถ้วนในการประกอบกิจการโทรคมนาคมโดยไม่ได้รับอนุญาตตามมาตรา 67 แห่งพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 โดยต้องวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 10 ล้านบาท หรือทั้งจำทั้งปรับ

4. การดำเนินการของผู้รับใบอนุญาตที่ประสงค์จะให้บริการอินเทอร์เน็ตแบบ WiFi ย่านความถี่วิทยุ

2.4 GHz และ 5 GHz

ผู้รับใบอนุญาตที่มีความประสงค์จะให้บริการอินเทอร์เน็ตแบบ WiFi ย่านความถี่วิทยุ 2.4 GHz และ 5 GHz ให้ดำเนินการดังหนังสือแจ้งความประสงค์ขอให้บริการอินเทอร์เน็ตดังกล่าวให้แก่สำนักงาน กสทช. พร้อมจัดလงเอกสารข้อมูลรูปแบบการให้บริการและข้อมูลเพิ่มเติมอื่น ๆ ที่เกี่ยวข้อง และให้แจ้งรายละเอียดตำแหน่งสถานที่ติดตั้งอุปกรณ์ให้บริการอินเทอร์เน็ตแบบ WiFi ที่ใช้เชื่อมโยง Point to Point หรือ Point to Multipoint สำหรับการให้บริการด้วย



สอบถามข้อมูลเพิ่มเติม
สำนักการอนุญาตประกอบกิจการโทรคมนาคม 2 สำนักงาน กสทช.
โทร: 02 271 0151-60 ต่อ 710, 702 โทรดูพ่อเคลื่อนที่: 089 040 5063
email: tel_license2@nbtc.go.th



EQUIVALENT ISOTROPICALLY RADIATED POWER E.I.R.P.



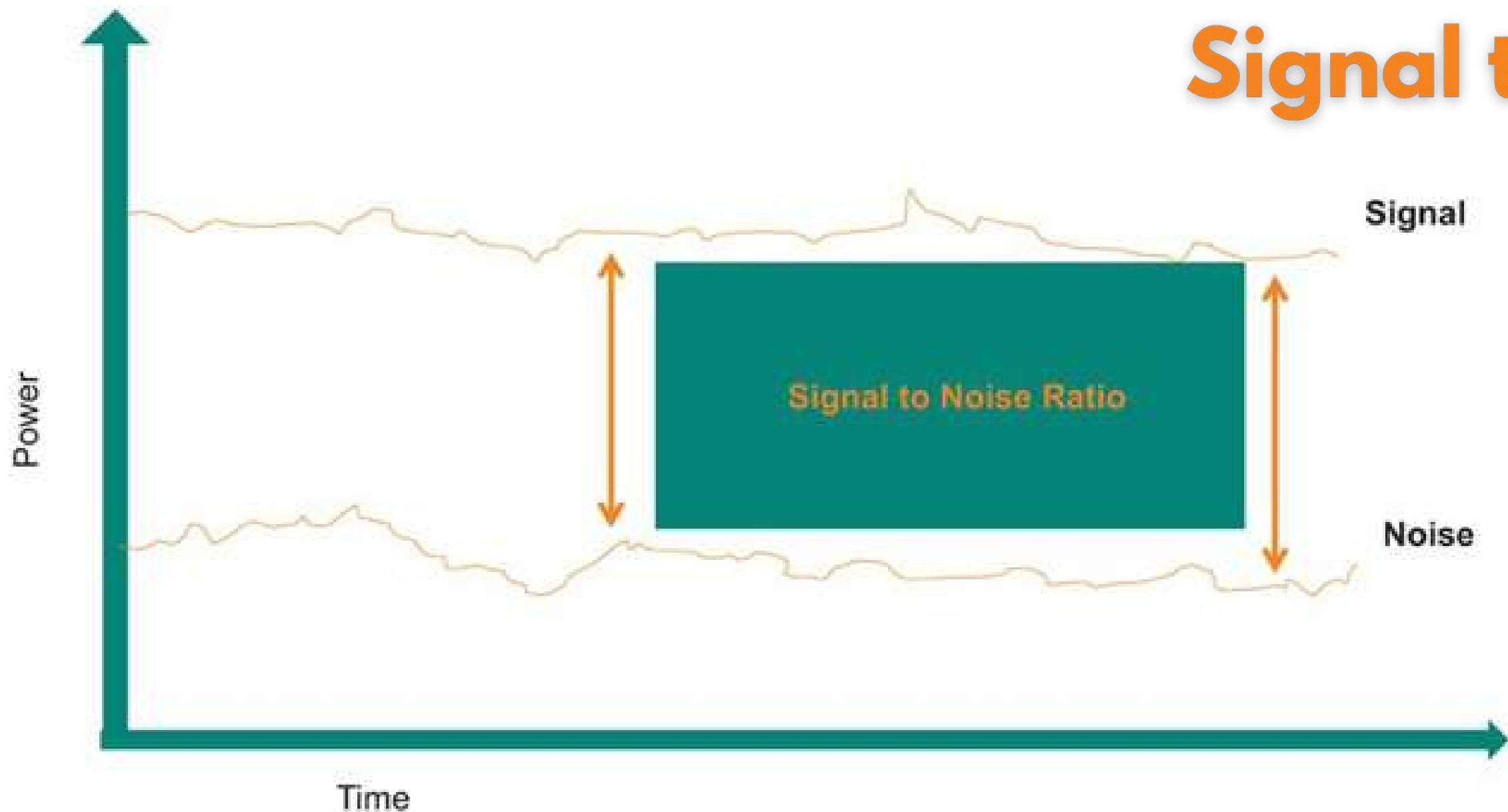


Top view—horizontal (H-plane) coverage



Side view—Vertical (E-plane) coverage

Signal to Noise ratio (SNR)

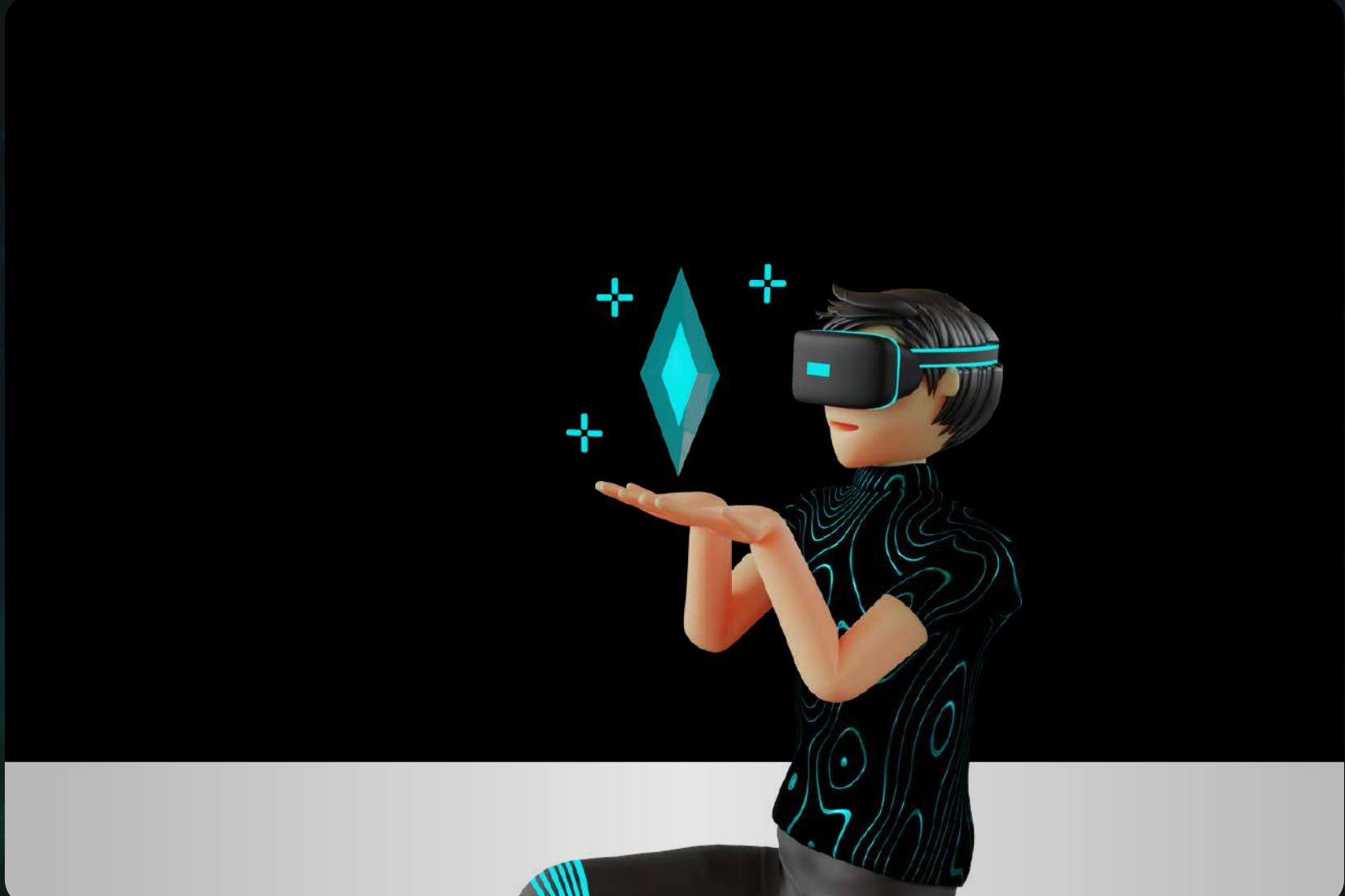


is a measurement of the power of the WLAN signal compared to the background noise of the RF environment.

SNR is a very important value and is used to evaluate the quality of the signal

RECEIVED SIGNAL STRENGTH INDICATOR (RSSI)

To maximize performance in Wi-Fi 6 deployments, the minimum **Received Signal Strength Indicator (RSSI) should be -55 dBm** at cell edge to deliver an MCS11 data rate on a 40MHz-wide channel with soft roaming support.



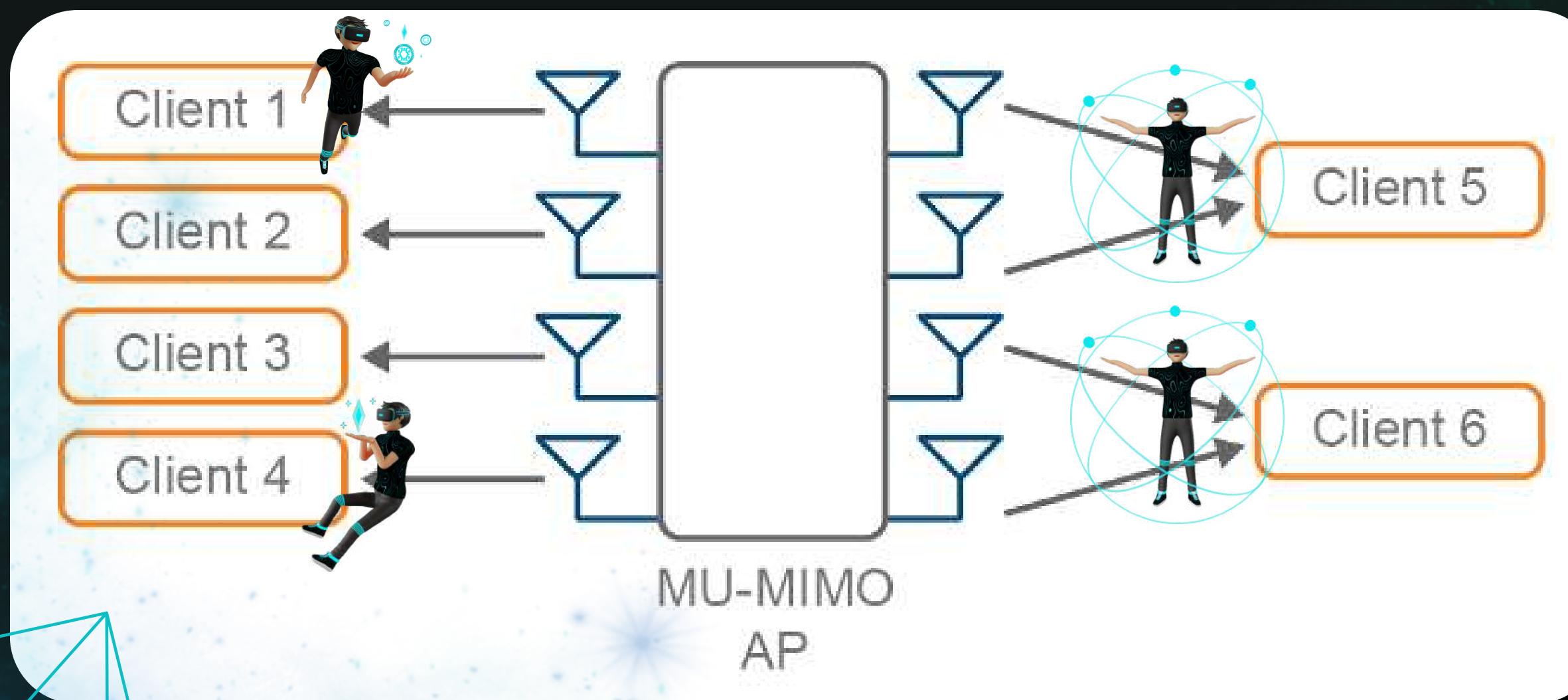
When deploying a Wi-Fi 6 network using dual-band APs, 2.4 GHz radios of some of the APs should be turned off to reduce co-channel interference.

TRANSMIT BEAMFORMING

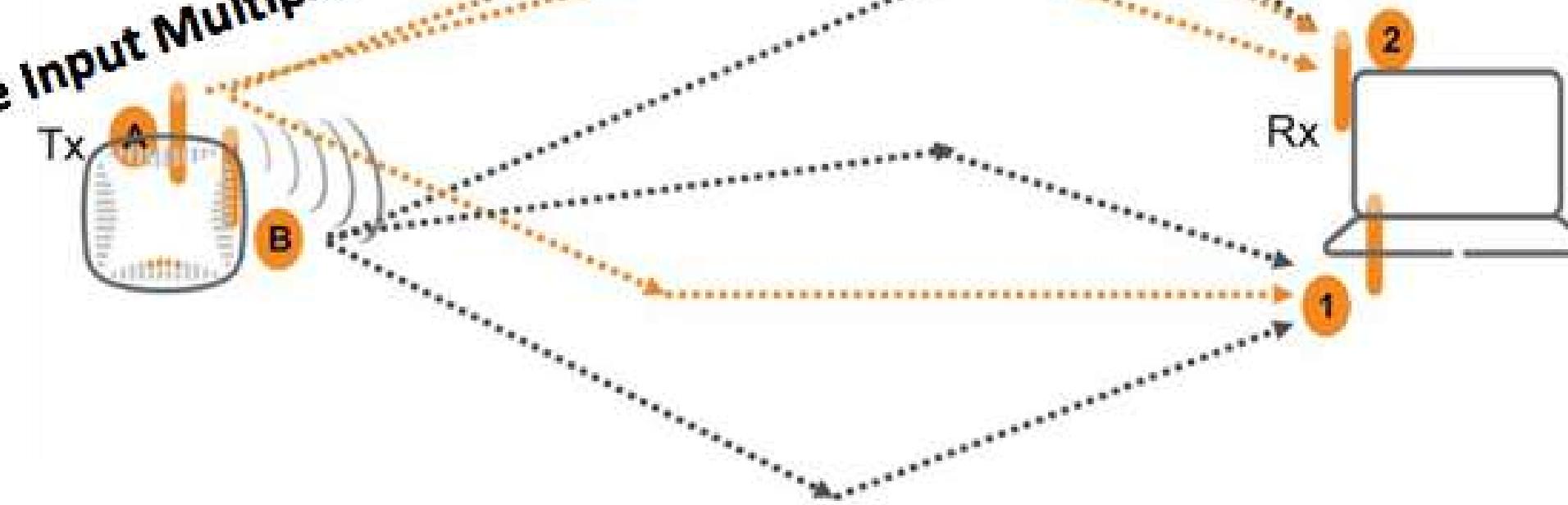
Wi-Fi 6 employs an explicit beamforming procedure using channel-sounding with a null data packet to compute the antenna weights and focus the RF energy for each user. Keep this feature enabled for optimal performance benefits.



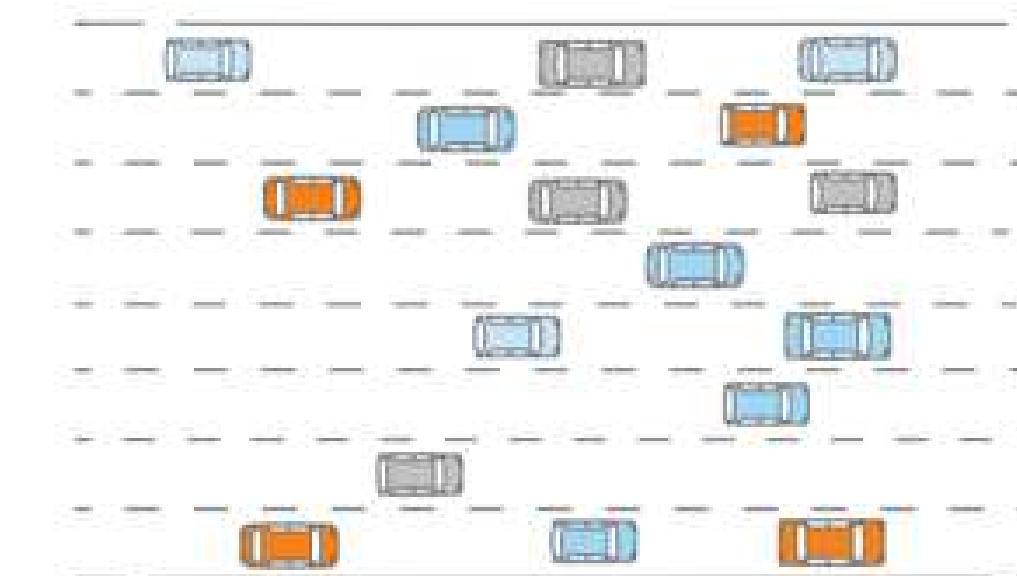
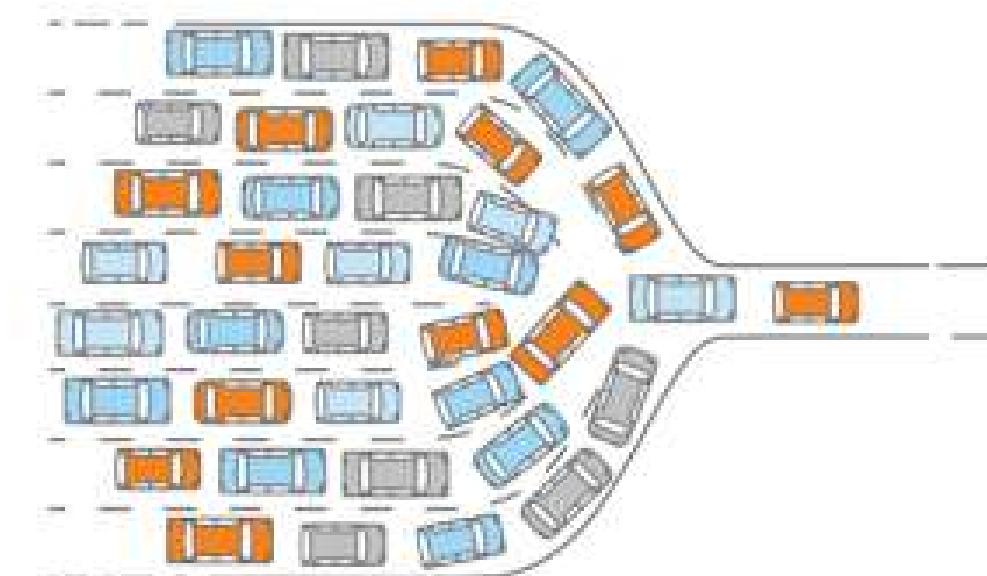
SINGLE AND DUAL STREAM CLIENTS



Multiple Input Multiple Output (MIMO)



Multi-user Multiple Input/Multiple Output (MU MIMO) is another way to handle traffic from multiple devices that was originally introduced in 802.11ac. Within 802.11ax, this feature has been enhanced by allowing up to 8 devices to transmit simultaneously using a dedicated channel per device. This allows for large packets such as streaming HD video to be handled more efficiently, while shorter packets from IoT devices and voice traffic would be better handled using OFDMA.





aruba

a Hewlett Packard
Enterprise company

ARUBA WIRELESS LAN CONTROLLER

Configuration the wireless LAN Wi-Fi 6
and setup the basic configure and the
personnel security



ARUBA WIRELESS LAN CONTROLLER

Specification Access Point

IAP - Wireless LAN Controller

SSID - Service Set Identifier

Channel management (Frequency: GHz)

RSSI - Received Signal Strength Indicator

Encryption Security (WPA-3 Personnel)



ARUBA AP-505



Aruba 500 Series Wi-Fi 6 (802.11ax) Indoor Access Points
HPE Aruba Networking 500 series Wi-Fi 6 Access Points. Perfect for mid-sized offices, schools, or retail spaces. View Series

[View Aruba Networking](#)

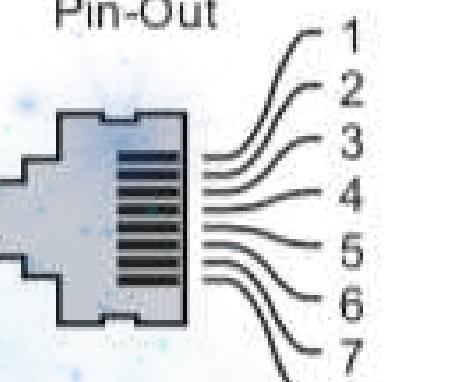
POWER OVER ETHERNET

PoE is a standard defining how to carry both power and data over an Ethernet cable.

IEEE 802.3af-2003 or PoE (capable of providing up to 15.4W)

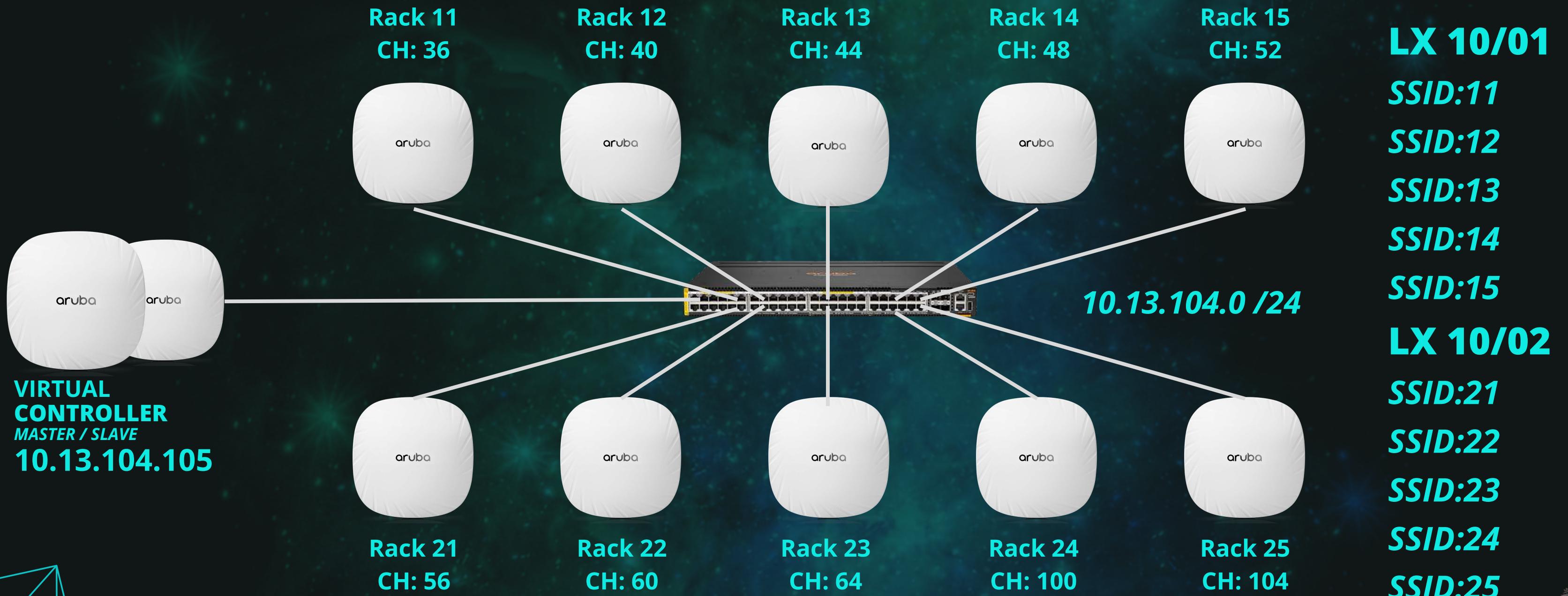
IEEE 802.3at-2009 or PoE+ (capable of providing up to 30W)

IEEE 802.3bt switches, Smart Rate switch ports provide up to 60W of PoE

1000Base-T Gigabit Ethernet Port	RJ-45 Female Pin-Out	Signal Name	Function
		1 2 3 4 5 6 7 8	BI_DA+ BI_DA- BI_DB+ BI_DC+ BI_DC- BI_DB- BI_DD+ BI_DD-
			Bi-directional pair +A, POE Negative
			Bi-directional pair -A, POE Negative
			Bi-directional pair +B, POE Positive
			Bi-directional pair +C, POE Positive
			Bi-directional pair -C, POE Positive
			Bi-directional pair -B, POE Positive
			Bi-directional pair +D, POE Negative
			Bi-directional pair -D, POE Negative



ARUBA WIRELESS LAN VIRTUAL CONTROLLER



SMART RATE MULTI-GIGABIT ETHERNET

HPE Smart Rate technology supports the industry standard IEEE 802.3bz and solves traffic bottlenecks without ripping and replacing existing twisted-pair cabling. The existing cabling infrastructure can be leveraged to protect existing investments and simplify upgrades to higher speed solutions.



ARUBA WIRELESS LAN CONTROLLER

Instant

Not secure | https://10.13.104.34:4343/monitoring/overview

aruba

Dashboard Overview Networks

Overview Networks 1 Active 1 Inactive 0

Country code: TH - Thailand

Management Local IPv6 Address: Uplink status: UP

Welcome to Instant

Please specify the Country Code

TH - Thailand

If the desired country code is not present, please try [Upgrading your AP](#) to the latest version and try again.

If your AP is already running the latest version, please contact technical support for more information.

OK

RF Dashboard

Clients Signal Speed Access Points Utilization Noise Errors

All Clients

19.40 19.41 19.42 19.43 19.44 19.40 19.41 19.42 19.43 19.44

Out In

aruba
a Hewlett Packard Enterprise company

ARUBA WIRELESS LAN CONTROLLER

Instant. Not secure | <https://10.13.104.34:4343/monitoring/overview>

aruba | VIRTUAL CONTROLLER | SetMeUp-C0:B2:80

Dashboard

Overview

Networks Access Points Clients

1 1 0

Active Inactive Up Down Wireless Wired

1 0 Up 1 Down 0 0 0

Dashboard IDS AirGroup 0 Alerts

Clients

Throughput (bps)

0 10

0 10

0 10

19:39 19:40 19:41 19:42 19:43 19:44 19:45

Out In

RF Dashboard

Clients Signal Speed

All Clients

Access Points Utilization Noise Errors

b8:3a:5a:c0:b2:80

The screenshot displays the Aruba Instant Virtual Controller monitoring interface. The top navigation bar shows the URL as https://10.13.104.34:4343/monitoring/overview. The main header includes the aruba logo, 'VIRTUAL CONTROLLER', and the device identifier 'SetMeUp-C0:B2:80'. On the left, a sidebar menu lists 'Dashboard' (selected), 'Overview', 'Networks', 'Access Points', 'Clients', 'Mesh Devices', 'Configuration', 'Maintenance', and 'Support'. The central 'Overview' section shows key metrics: 1 Network, 1 Access Point, and 0 Clients. Below these are detailed counts: Active (1), Inactive (0), Up (1), Down (0), Wireless (0), and Wired (0). A navigation bar at the bottom of this section includes 'Dashboard', 'IDS', 'AirGroup', and '0 Alerts'. To the right, the 'Info' section provides device details: Name (SetMeUp-C0:B2:80), Virtual Controller IP (0.0.0.0), Country code (TH), Management (Local), Conductor (10.13.104.34), IPv6 Address (--), Uplink type (Ethernet), and Uplink status (UP). Below this are two line graphs showing 'Throughput (bps)' over time (19:39 to 19:45) for Out (blue) and In (orange) traffic. The final section, 'RF Dashboard', includes tabs for 'Clients', 'Signal', and 'Speed', with a sub-section for 'All Clients'. At the bottom, a summary table shows 'Access Points', 'Utilization', 'Noise', and 'Errors' for the device b8:3a:5a:c0:b2:80.



ARUBA WIRELESS LAN CONTROLLER

The screenshot shows the Aruba Instant Virtual Controller web interface. The URL is <https://10.13.104.34:4343/configuration/networks>. The left sidebar includes links for Mesh Devices, Configuration (selected), Networks (highlighted in blue), Access Points, System, RF, Security, IDS, Routing, Tunneling, Services, DHCP Server, Maintenance, and Support. The main content area displays a table of networks:

Name	Type	Clients
SetMeUp (SetMeUp-C0:B2:80)	wireless	0
wired-SetMeUp	wired	0
default_wired_port_profile	wired	0

At the bottom right of the interface, there is a cartoon character of a person wearing a VR headset, sitting on a large green and black Aruba logo.

ARUBA WIRELESS LAN CONTROLLER

The screenshot shows the Aruba Instant Virtual Controller web interface. The left sidebar lists various configuration sections: Mesh Devices, Configuration (selected), Networks (highlighted in blue), Access Points, System, RF, Security, IDS, Routing, Tunneling, Services, DHCP Server, Maintenance, and Support. The main content area is titled "New Network" and is divided into four tabs: 1 Basic (selected), 2 VLAN, 3 Security, and 4 Access. The "Basic" tab contains fields for "Name" (empty), "Type" (Wireless selected), "Primary usage" (Employee selected), "Broadcast filtering" (set to ARP), "Multicast transmission optimization" (disabled), "Dynamic multicast optimization" (disabled), and a "DMO channel utilization threshold" input field (empty). The "Transmit Rates" section for 2.4 GHz shows "Min" set to 1 and "Max" set to 54. The top of the page shows the URL <https://10.13.104.34:4343/configuration/networks/network-add>.



Wi-Fi alliance certifications

Wi-Fi Alliance Security	Authentication Mechanism	Encryption	Hashing
WPA-Personal	Preshared Key	RC4-TKIP	Michael-MIC
WPA-Enterprise	802.1x/EAP RADIUS Server	RC4-TKIP	Michael-MIC
WPA2-Personal	Preshared Key	AES-CCMP TKIP (optional)	AES-CCMP Michael (optional)
WPA2-Enterprise	802.1X/EAP RADIUS Server	AES-CCMP TKIP (optional)	AES-CCMP Michael (optional)

ARUBA WIRELESS LAN CONTROLLER

Enterprise solution

Specification 2 Access Points

IAP - Wireless LAN Controller

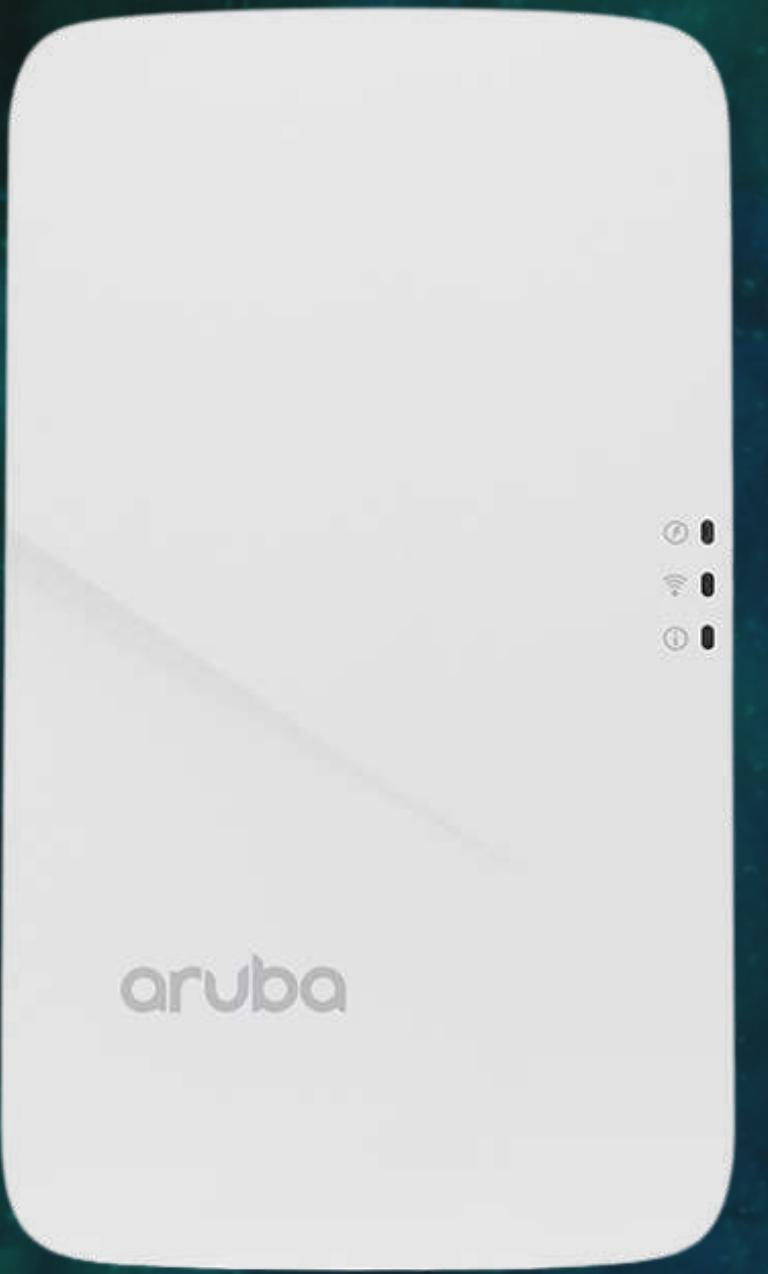
SSID - Service Set Identifier

Channel management (Frequency: GHz)

Encryption Security (WPA-3 Enterprise)



ARUBA AP-303H



Aruba 303H Series Hospitality Access Points

The cost-effective HPE Aruba Networking 303H series indoor AP Wi-Fi 5 is ideal for hospitality and branch offices.

HPE Aruba Networking

ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE

RADIUS + LDAP
10.13.104.200



VIRTUAL
CONTROLLER
MASTER / SLAVE
10.13.104.105

Rack 11
CH: 36

Rack 12
CH: 40

Rack 13
CH: 44

Rack 14
CH: 48

Rack 15
CH: 52

Rack 21
CH: 56

Rack 22
CH: 60

Rack 23
CH: 64

Rack 24
CH: 100

Rack 25
CH: 104

10.13.104.0 /24

LX 10/01

SSID:11

SSID:12

SSID:13

SSID:14

SSID:15

LX 10/02

SSID:21

SSID:22

SSID:23

SSID:24

SSID:25



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE ACCOUNT

The screenshot shows the phpLDAPadmin interface with the following details:

- Header:** phpLDAPadmin
- Navigation:** Home | Purge caches
- Address Bar:** 10.13.104.200
- Toolbar:** schema, search, refresh, info, monitor, import, export, logout
- User Information:** Logged in as: uid=lab207,ou=People,ou=staff
- LDAP Tree Structure:**
 - dc=sit, dc=kmutt, dc=ac, dc=th (7)
 - ou=Computers
 - ou=Group (9)
 - ou=Idmap
 - ou=profile (4)
 - ou=st (1)
 - ou=People
 - ou=staff (1)
 - sambaDomainName=SMBLDAP
 - Create new entry here
- Buttons:** Create new entry here (multiple instances)



LDAP
10.13.104.200



RADIUS
10.13.104.200



**VIRTUAL
CONTROLLER
MASTER / SLAVE**
10.13.104.105

LDAP web admin:
<https://students.sit.kmutt.ac.th/ldap207admin/htdocs>

Username: uid=lab207,ou=People,ou=staff,dc=sit,dc=kmutt,dc=ac,dc=th
Password: Lab!!207



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE ACCOUNT



php LDAP admin

Home | Purge caches

10.13.104.200

schema search refresh info monitor import export logout

Logged in as: uid=lab207,ou=People,ou=staff

dc=sit,dc=kmutt,dc=ac,dc=th (7)

- ou=Computers
- ou=Group (9)
- ou=Idmap
- ou=profile (4)
- ou=st (1)
- ou=People
- Create new entry here**
- ou=staff (1)
- sambaDomainName=SMBLDAP
- Create new entry here**

Create Object

Server: 10.13.104.200 Container: ou=st,dc=sit,dc=kmutt,dc=ac,dc=th

Select a template for the creation process

Templates:

- Courier Mail: Alias
- Generic: Address Book Entry
- Generic: DNS Entry
- Generic: LDAP Alias
- Generic: Organisational Role
- Generic: Organisational Unit
- Generic: Posix Group
- Generic: Simple Security Object
- Generic: User Account**
- Kolab: User Entry
- Samba: Domain

- Samba: Group Mapping
- Samba: Machine
- Sendmail: Alias
- Sendmail: Cluster
- Sendmail: Domain
- Sendmail: Relays
- Sendmail: Virtual Domain
- Sendmail: Virtual Users
- Thunderbird: Address Book Entry
- Default

→



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE ACCOUNT



LDAP
10.13.104.200

Create Object

Server: 10.13.104.200 Container: ou=st,dc=sit,dc=kmutt,dc=ac,dc=th
Template: Generic: User Account (posixAccount)

New User Account (Step 1 of 1)

First name	alias
zabastien	
Last name	alias, required
bas	*
Common Name	alias, required
zabastien bas	*
User ID	alias, required, rdn
zabastien	*
Password	alias, hint
.....	md5
.....	(confirm)
Check password...	
UID Number	alias, required, hint, ro
1003	
GID Number	alias, required, hint
Domain Users	*
Home directory	alias, required
/home/users/zabastien	*
Login shell	alias
Create Object	

Create LDAP Entry

Server: 10.13.104.200 Container: ou=st,dc=sit,dc=kmutt,dc=ac,dc=th

Do you want to create this entry?

Attribute	New Value	Skip
uid=000bas,ou=st,dc=sit,dc=kmutt,dc=ac,dc=th		
First name	zabastien	<input type="checkbox"/>
Last name	Pua	<input type="checkbox"/>
Common Name	zabastien Pua	<input type="checkbox"/>
User ID	000bas	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1059	<input type="checkbox"/>
GID Number	513	<input type="checkbox"/>
Home directory	/home/users/000bas	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount radiusprofile	<input type="checkbox"/>

Commit Cancel



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE ACCOUNT



LDAP
10.13.104.200

Create Entry
Creation successful! DN: `uid=000bas,ou=st,dc=sit,dc=kmutt,dc=ac,dc=th` has been created.

`uid=000bas`

Server: `10.13.104.200` Distinguished Name: `uid=000bas,ou=st,dc=sit,dc=kmutt,dc=ac,dc=th`
Template: Default

[Refresh](#) [Show internal attributes](#)
[Switch Template](#) [Export](#)
[Copy or move this entry](#) [Delete this entry](#)
[Rename](#) [Compare with another entry](#)
[Create a child entry](#) [Add new attribute](#)

Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

cn required
zabastien Pua
(add value)

gidNumber required
513
Domain Users (Netbios Domain Users)

givenName
zabastien
(add value)

Add Attribute

radiusNTPassword
0x

radiusLoginIPHost
radiusLoginLATGroup
radiusLoginLATNode
radiusLoginLATPort
radiusLoginLATService
radiusLoginService
radiusLoginTCPPort
radiusLoginTime
radiusNASIpAddress
radiusNTPassword
radiusPasswordRetry
radiusPortLimit
radiusProfileDn
radiusPrompt
radiusProxyToRealm
radiusRealm
radiusReplicateToRealm
radiusReplyItem
radiusReplyMessage



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE ACCOUNT



Add Attribute

radiusNTPassword

0x = HEX

0x 78CAC99835888C5B3B074F9158D862D5

<https://www.browserling.com/tools/ntlm-hash>

NTLM Password Hasher
cross-browser testing tools

World's simplest online NTLM hash generator for web developers and programmers. Just paste your password in the form below, press the Calculate NTLM Hash button, and you'll get an NTLM hash. Press a button – get a hash. No ads, nonsense, or garbage.

Like 51K

Announcement: We just added three new tools categories – [Text tools](#), [Image tools](#), and [Math tools](#). Check them out!

78CAC99835888C5B3B074F9158D862D5

[Calculate NTLM Hash](#) [Copy to clipboard](#)

Generate an NTLM Hash - NTLM Password - Online - Browserling Web...

Useful, free online tool that computes NTLM password hashes. No ads, nonsense, or garbage....

browserling.com



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE TESTING THE ACCOUNT



LDAP
10.13.104.200

Create LDAP Entry

Server: 10.13.104.200 Container: ou=st,dc=sit,dc=kmutt,dc=ac,dc=th

Do you want to create this entry?

Attribute	New Value	Skip
uid=zabastien,ou=st,dc=sit,dc=kmutt,dc=ac,dc=th		<input type="checkbox"/>
First name	zabastien	<input type="checkbox"/>
Last name	bas	<input type="checkbox"/>
Common Name	zabastien bas	<input type="checkbox"/>
User ID	zabastien	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1003	<input type="checkbox"/>
GID Number	513	<input type="checkbox"/>
Home directory	/home/users/zabastien	<input type="checkbox"/>
ObjectClass	inetOrgPerson posixAccount radiusprofile	<input type="checkbox"/>

Commit Cancel

```
[labadmin@ldra4lab:~$ radtest zabastien 'zabastien' 10.13.104.200 11 LAB207
Sent Access-Request Id 227 from 0.0.0.0:46176 to 10.13.104.200:1812 length 79
User-Name = "zabastien"
User-Password = "zabastien"
NAS-IP-Address = 127.0.1.1
NAS-Port = 11
Message-Authenticator = 0x00
Cleartext-Password = "zabastien"

Received Access-Accept Id 227 from 10.13.104.200:1812 to 10.13.104.200:46176 length 20
```



```
[labadmin@ldra4lab:~$ radtest zabastien 'zabastien1' 10.13.104.200 11 LAB207
Sent Access-Request Id 0 from 0.0.0.0:35800 to 10.13.104.200:1812 length 79
User-Name = "zabastien"
User-Password = "zabastien1"
NAS-IP-Address = 127.0.1.1
NAS-Port = 11
Message-Authenticator = 0x00
Cleartext-Password = "zabastien1"

Received Access-Reject Id 0 from 10.13.104.200:1812 to 10.13.104.200:35800 length 20
(0) -: Expected Access-Accept got Access-Reject
```



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE CREATE LOCAL ACCOUNT



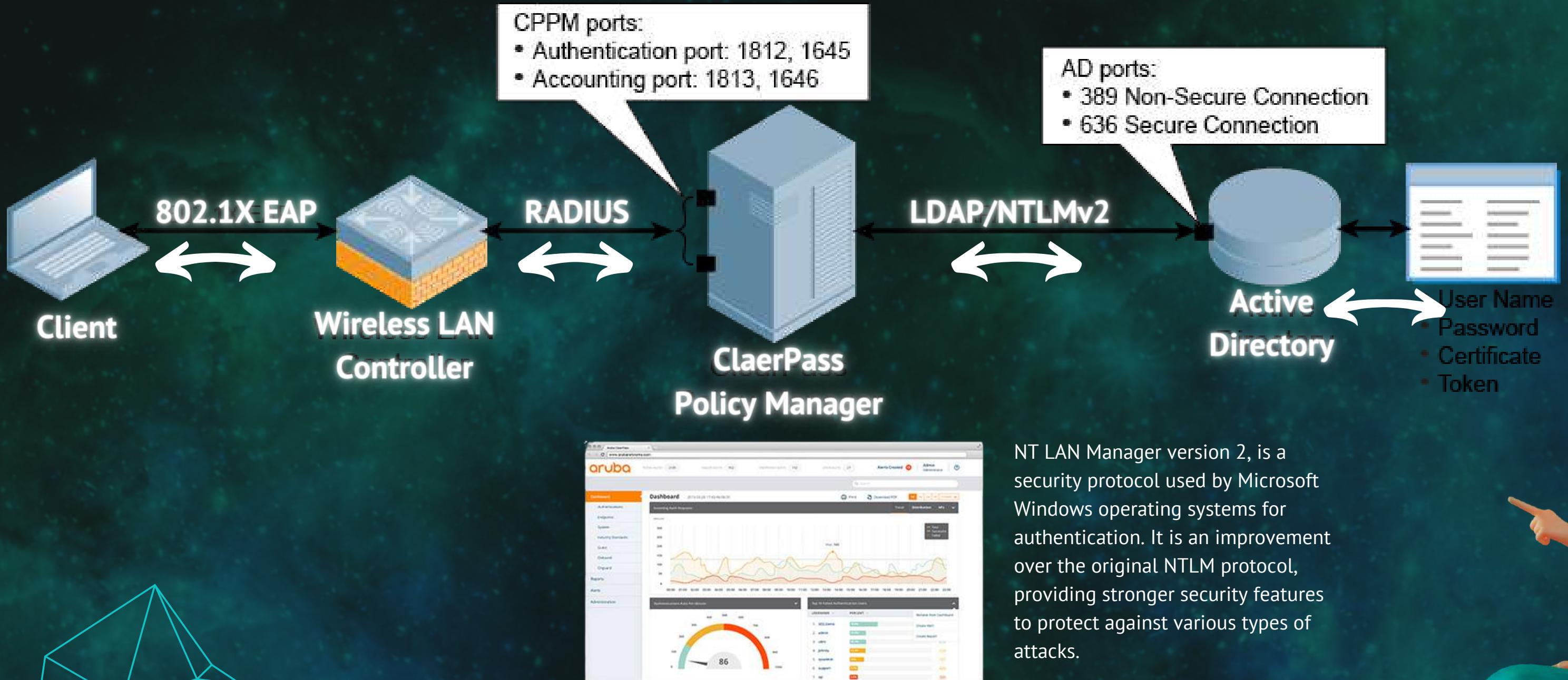
VIRTUAL
CONTROLLER
MASTER / SLAVE
10.13.104.105

The screenshot shows the Aruba Virtual Controller Enterprise web interface. The top navigation bar includes the Aruba logo, 'VIRTUAL CONTROLLER', and 'MASTER-Controller'. The left sidebar menu has sections: Dashboard, Overview, Networks, Access Points, Clients, Mesh Devices, Configuration (selected), Security (highlighted with a red arrow), IDS, Routing, and Tunneling. The main content area shows 'Authentication Servers' and 'Users' (selected). Under 'Users', there is a table with a single row for 'Name' (int208) and a 'Delete All' button. Below this is a 'Add new user' form with fields: Username (int208), Password (redacted), Retype (redacted), Type (Employee dropdown selected), and OK/Cancel buttons. At the bottom of the main content area is an 'Intra VLAN Traffic Allowlist' section.



AAA

AUTHENTICATION
AUTHORIZATION
ACCOUNTING



NT LAN Manager version 2, is a security protocol used by Microsoft Windows operating systems for authentication. It is an improvement over the original NTLM protocol, providing stronger security features to protect against various types of attacks.



aruba
a Hewlett Packard Enterprise company

AAA

AUTHENTICATION
AUTHORIZATION
ACCOUNTING

Remote Authentication **RADIUS** Dial-In User Service

Remote Authentication Dial-In User Service, is a protocol used for controlling access to a network. It provides a centralized way to authenticate users who want to connect to a network, such as through Wi-Fi or VPNs. RADIUS works by having a server that manages user authentication, authorization, and accounting information.

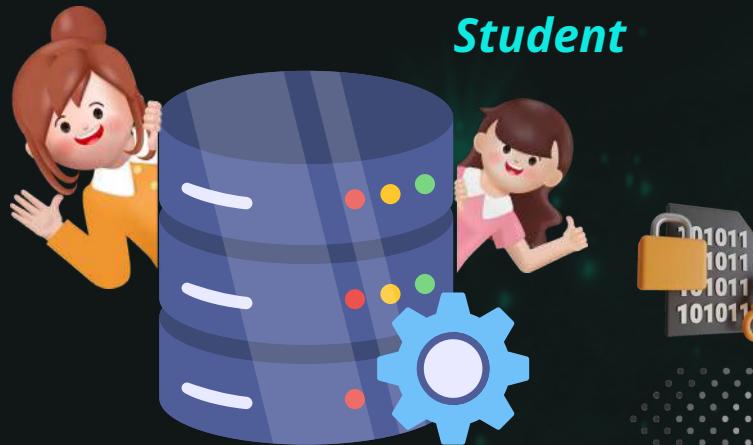
Lightweight Directory **LDAP** Access Protocol

LDAP is a standardized protocol commonly used for accessing and managing directory information services. It provides a way for clients to access and interact with directory servers, which store a variety of information such as user profiles, organizational data, and network resources.



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE

Lecturer



LDAP
10.13.104.200

Accounting

Student



Authentication + Authorization
RADIUS
10.13.104.200



**VIRTUAL
CONTROLLER
MASTER / SLAVE**
10.13.104.105



tunnel



**PoE+
802.3af**

**WPA3-Enterprise
encryption**



**802.1x
user-authentication**



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE SECURITY PROFILE

VIRTUAL
CONTROLLER
MASTER / SLAVE
10.13.104.105



aruba | VIRTUAL CONTROLLER | MASTER-Controller

New Network → 1 Basic 2 VLAN 3 Security 4 Access

Security Level

Security Level: Enterprise (selected)

Key management: WPA3-Enterprise (CCM 128)

Authentication server 1: -- Select Server -- +

EAP offload: Off

Reauth interval: 0 min.

MAC authentication: Perform MAC authentication before 802.1X MAC authentication fail-thru

Accounting: Disabled

Denylisting: Off

Enforce DHCP: Off

Fast Roaming

Opportunistic Key Caching(OKC): On

802.11r: On

802.11k: On

802.11v: On

Dashboard Overview Networks Access Points Clients Mesh Devices

Configuration

Networks

Access Points System RF Security IDS Routing Tunneling Services DHCP Server

The screenshot shows the Aruba Virtual Controller interface for creating a new network. The 'Security' tab is selected. The 'Security Level' dropdown is set to 'Enterprise', which is highlighted with an orange border. The 'Key management' dropdown is set to 'WPA3-Enterprise (CCM 128)'. The 'Authentication server 1' field has a placeholder 'Select Server' and a '+' button. Other security settings like 'EAP offload', 'Reauth interval', and 'MAC authentication' options are visible. The 'Fast Roaming' section includes 'OKC', '802.11r', '802.11k', and '802.11v' options, all of which are currently enabled (indicated by the 'On' status).



ARUBA WIRELESS LAN VIRTUAL CONTROLLER ENTERPRISE RADIUS PROFILE

New Authentication Server

Type: RADIUS

Name: LabRADIUS

RadSec: Off

IP Address: 10.13.104.200

Auth port: 1812

Accounting port: 1813

Shared key:

Retype key:

Timeout: 5 sec.

Retry count: 3

Dynamic Authorization: Off

Status-Server: Authentication (checked), Accounting (unchecked)

NAS-IP-Address: (optional)

NAS-Identifier: (optional)

Dead time: 5 min.

DRP IP:

DRP Mask:

DRP VLAN:

DRP Gateway:

Service-Type Framed-User: 802.1X (checked), Captive Portal (unchecked), MAC (unchecked)

CPPM username:

CPPM password:

Cancel OK



LDAP

10.13.104.200



RADIUS

10.13.104.200



**VIRTUAL
CONTROLLER
MASTER / SLAVE
10.13.104.105**

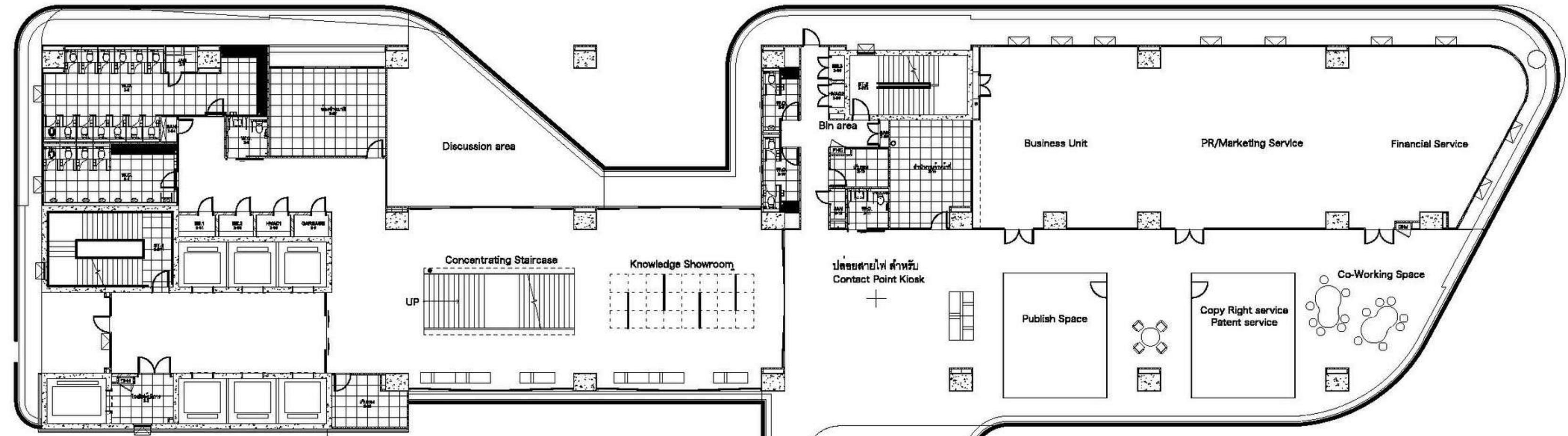
**RADIUS for LAB:
IP: 10.13.104.200
Authentication Port : 1812
Accounting Port : 1813
Shared Key : LAB207**



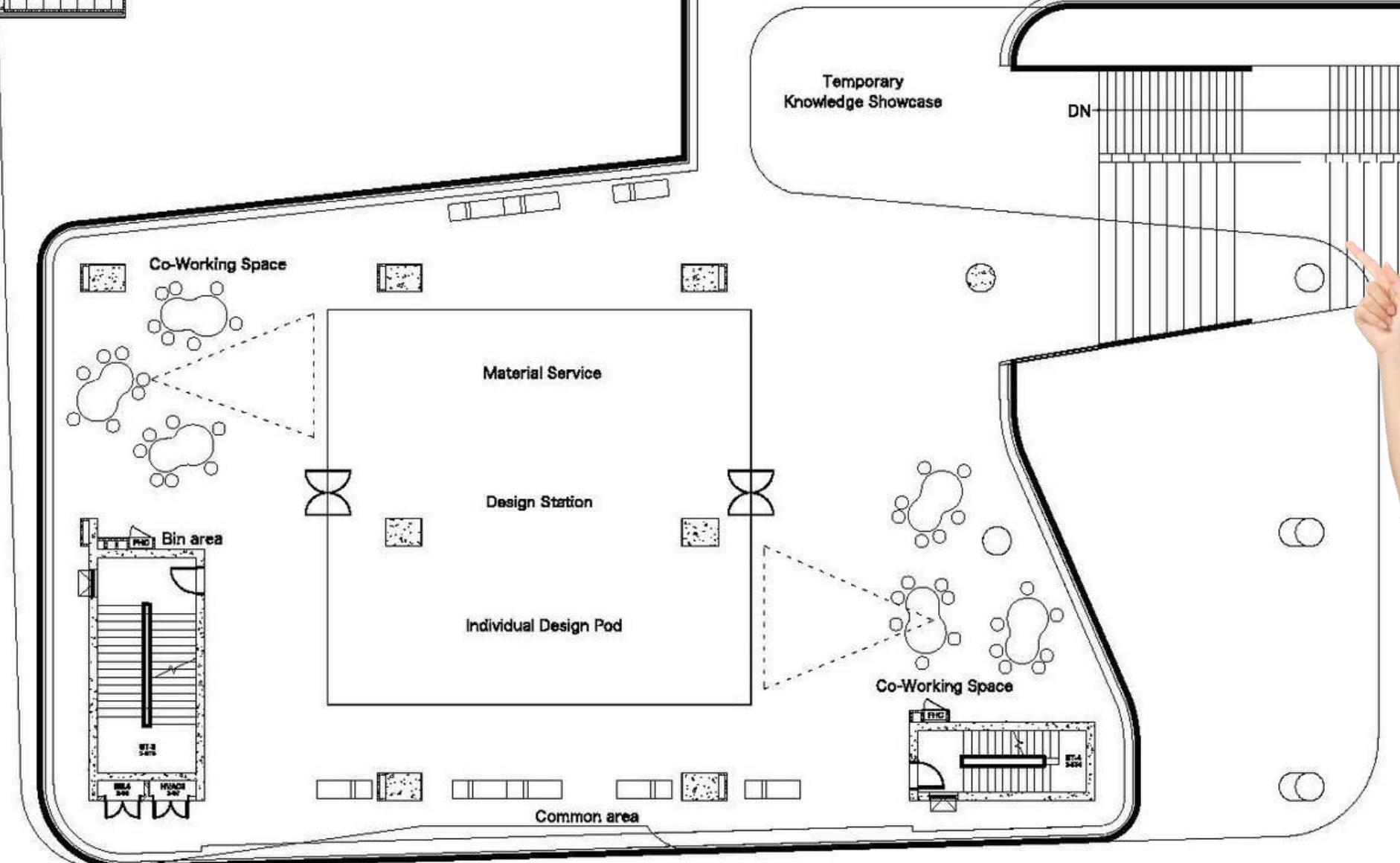
ASSIGMENT

Design the wireless LAN Wi-Fi 6/6E and
Wi-Fi 7 (optional) and simulation the design

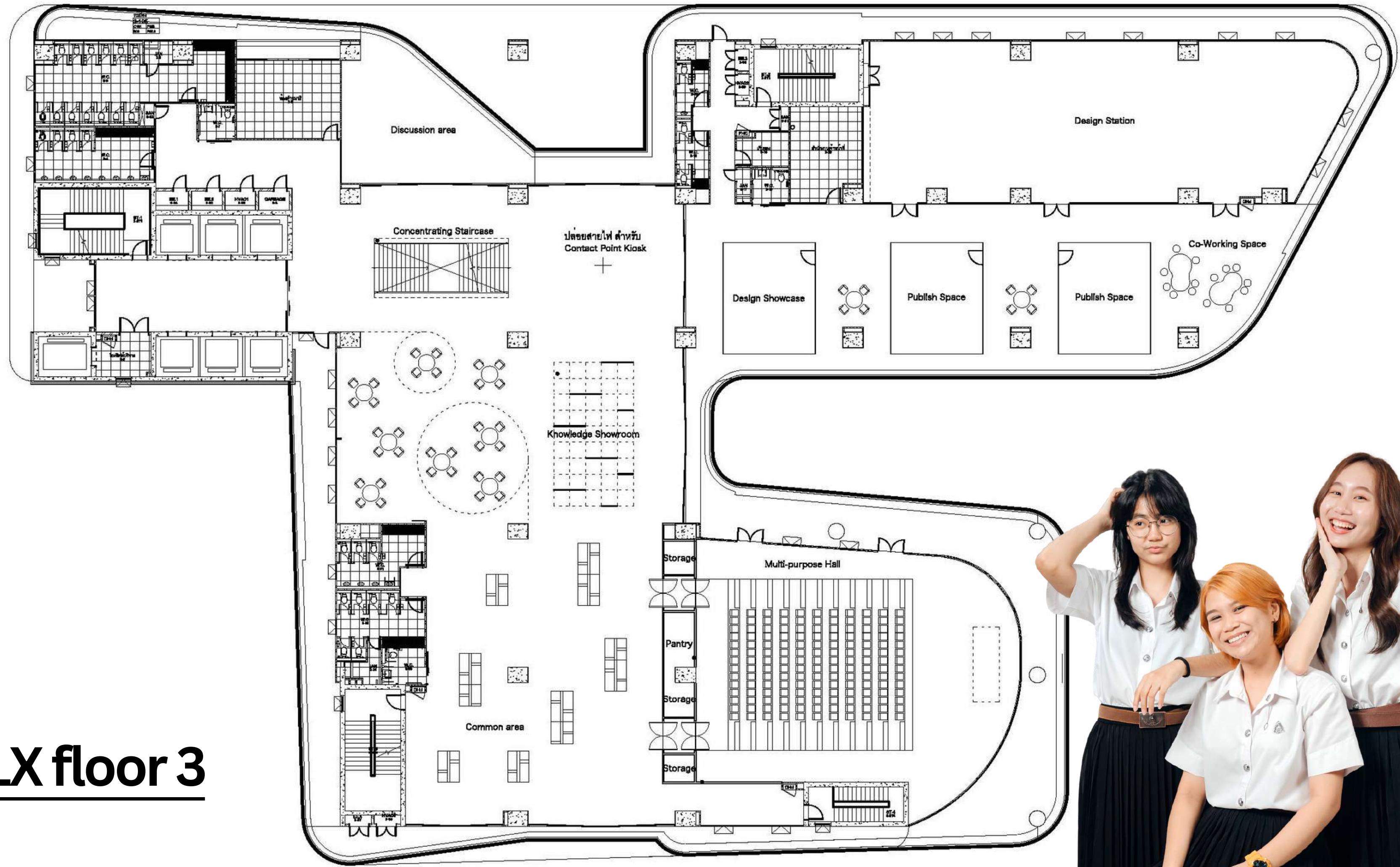


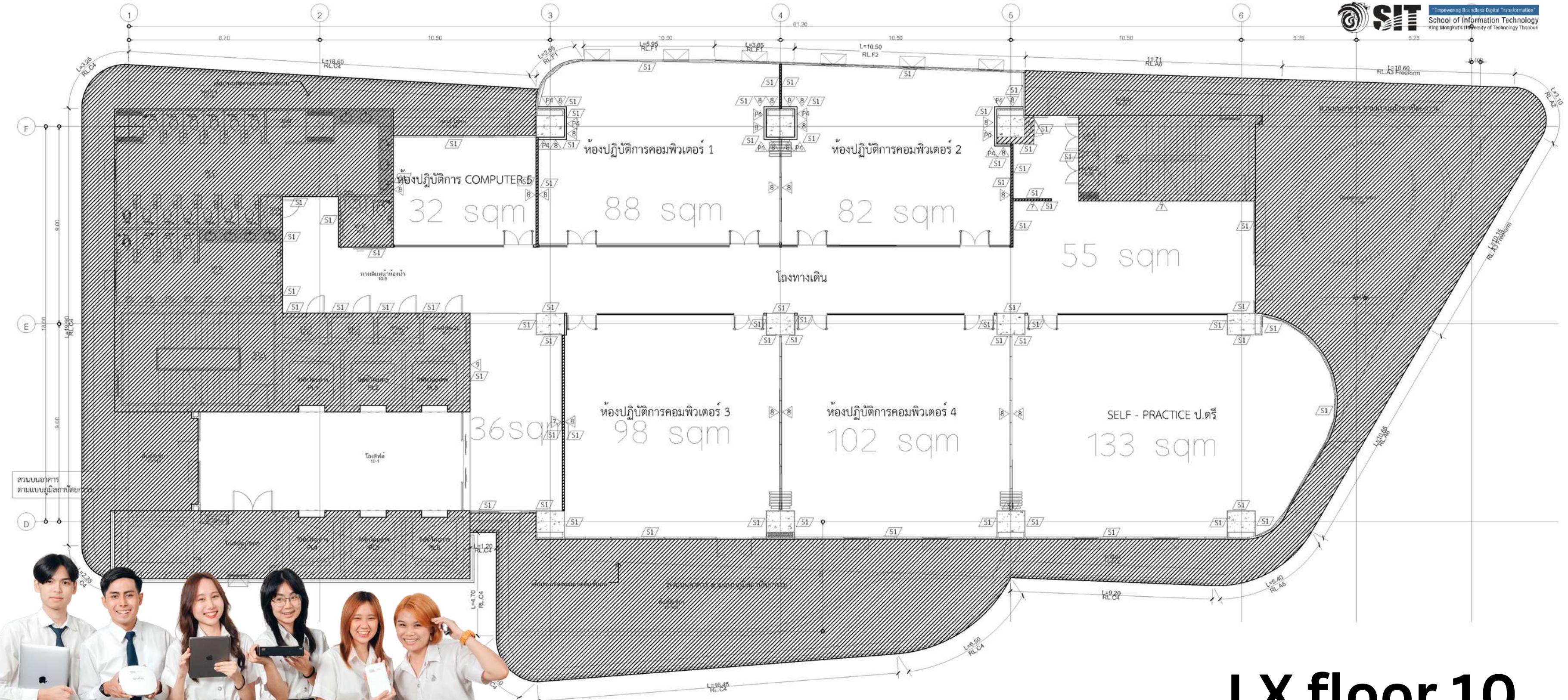


LX floor 2

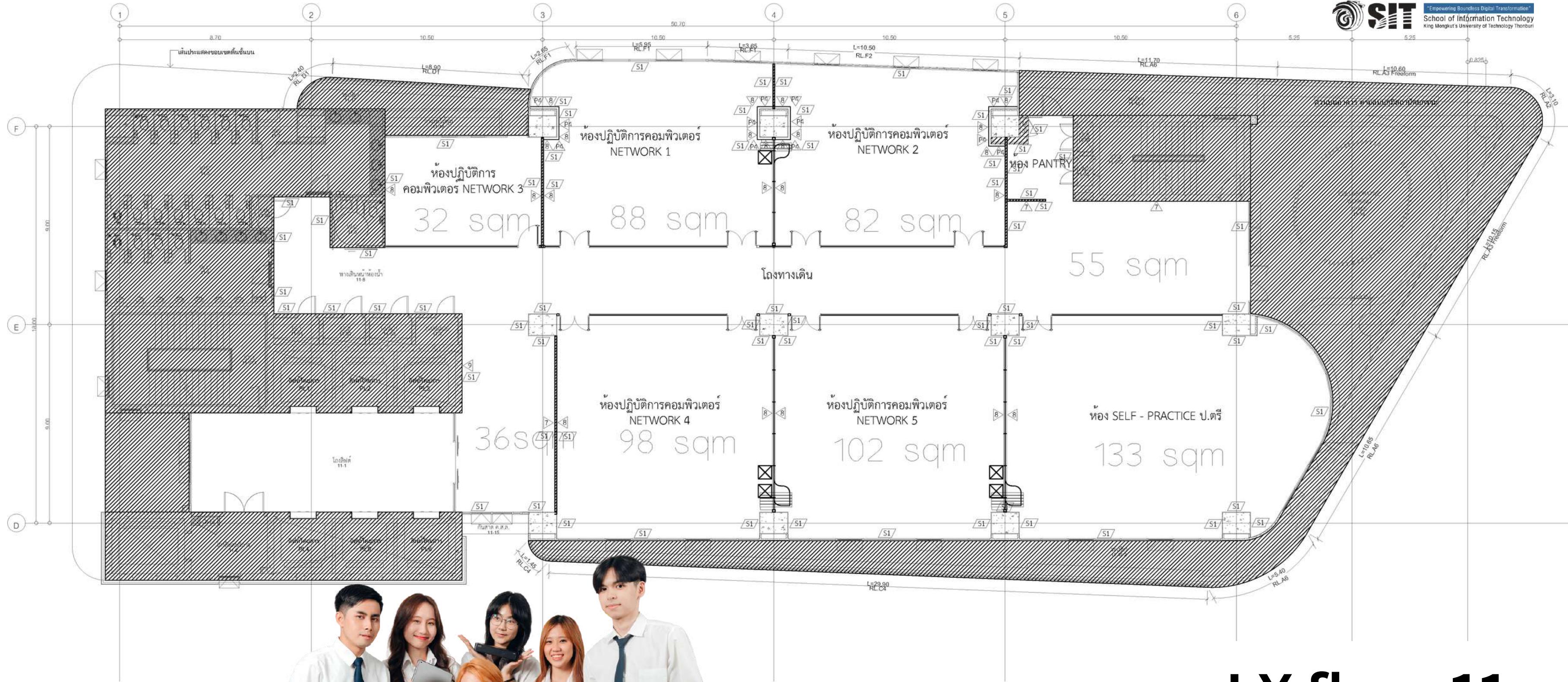


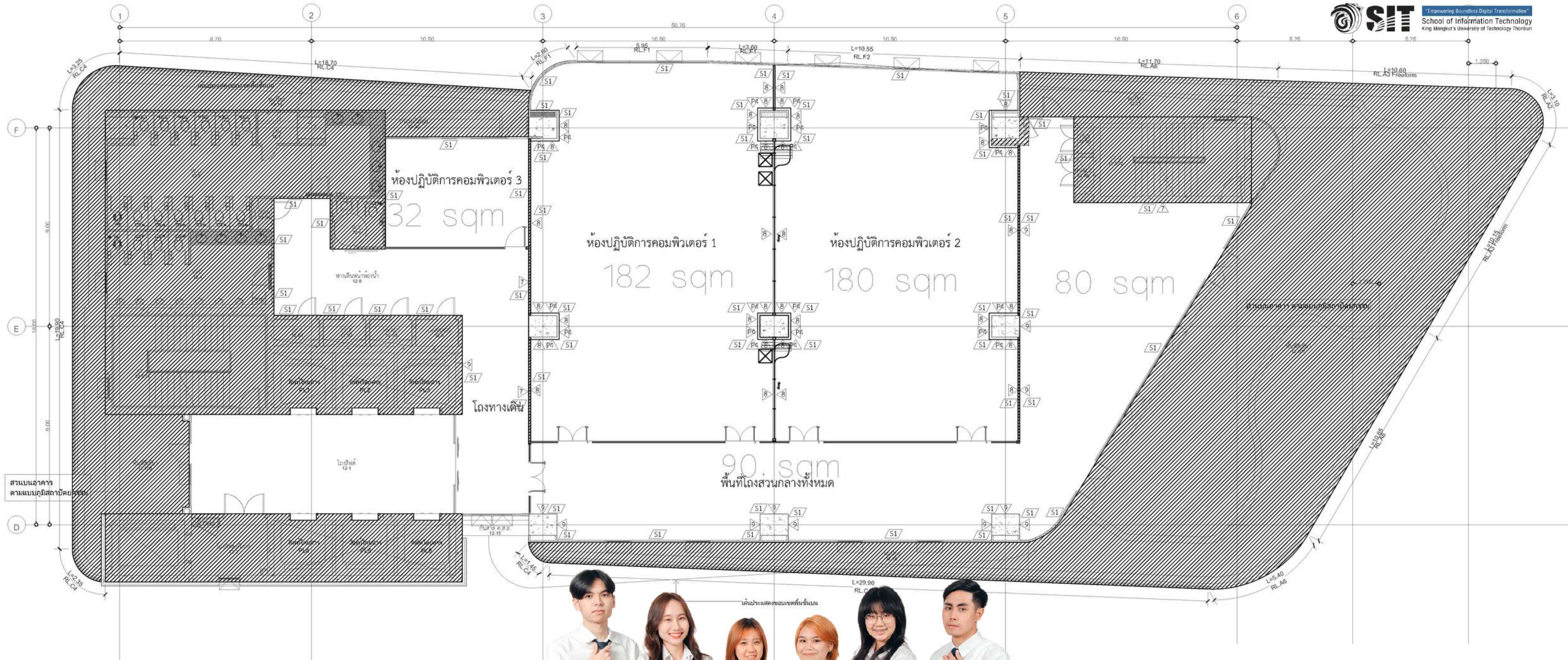
LX floor 3



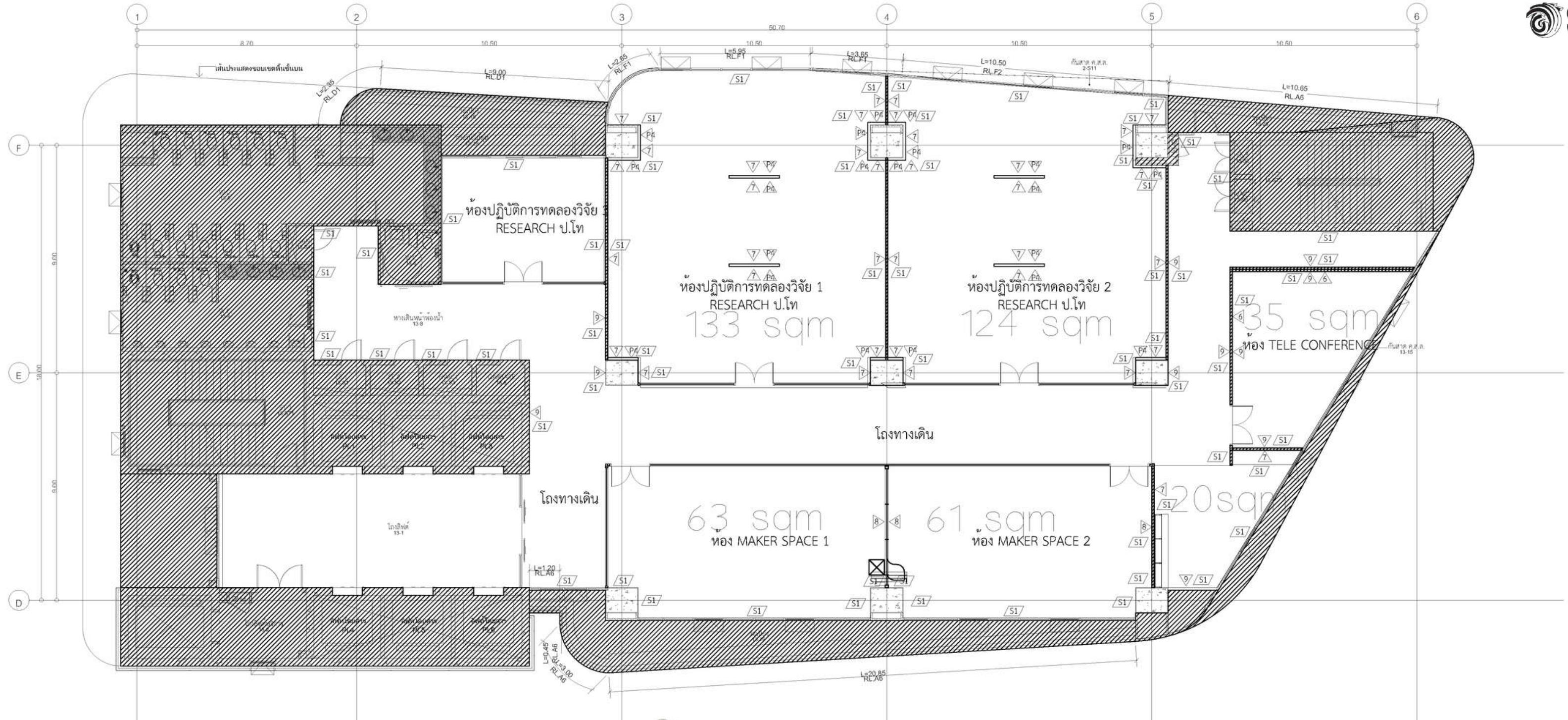


LX floor 10





LX floor 12



LX floor 13