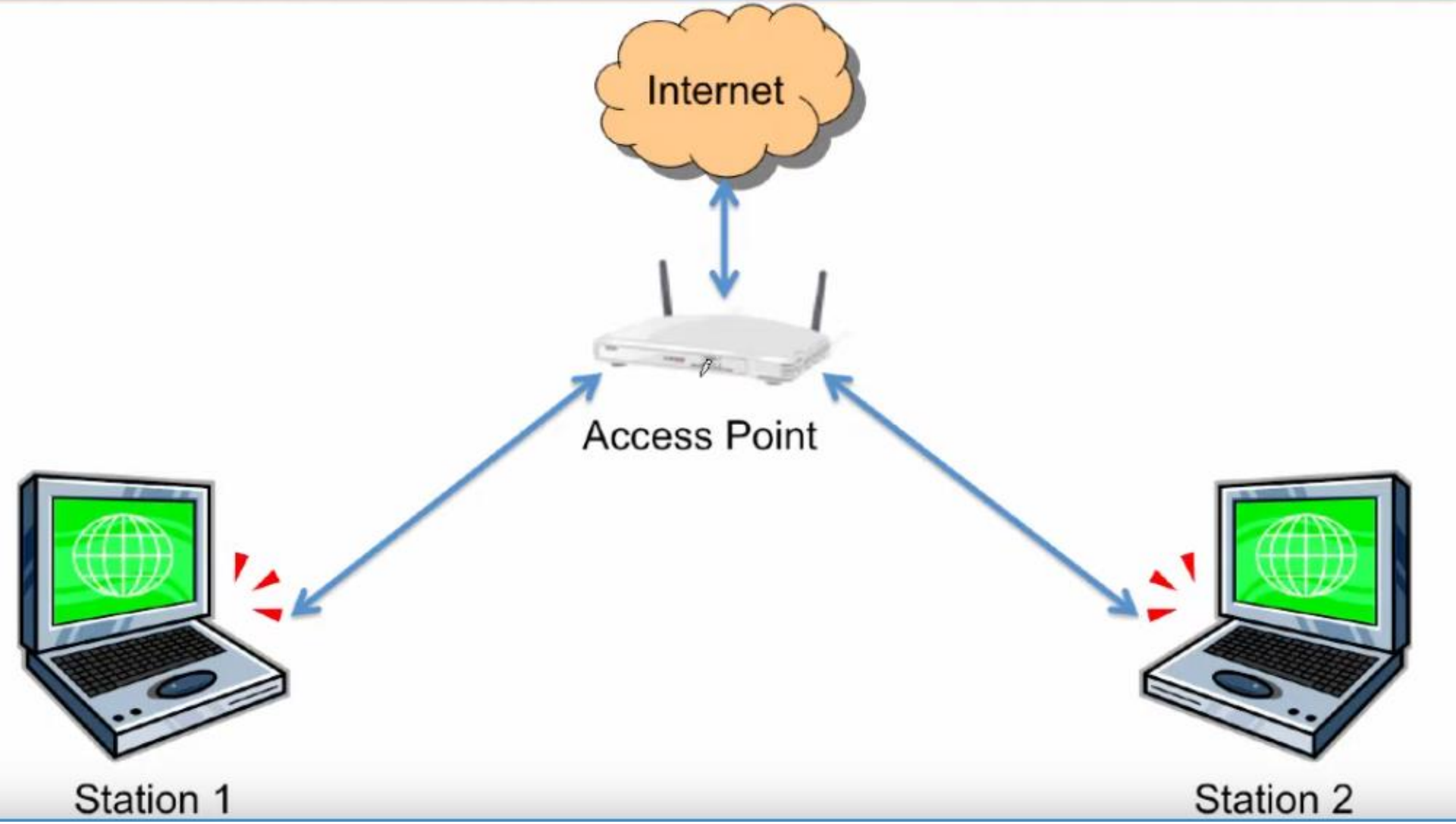
Wi-Fi Direct: Wi-Fi P2P Connection

Basic 802.11 Network



Beacon Frame

- Sent periodically by AP to identify itself to prospective stations
- Layout:

Time stamp	Capabilities	SSID	Data Rates	Other

- Typically sent once every second

What is TBTT?

TBTT (Target Beacon Transmission Time) is the scheduled time at which a beacon frame is transmitted by a device in a Wi-Fi network (like an access point or group owner).

Beacons are special management frames that announce the presence and capabilities of the device or group.

The TBTT is the reference point in time when such beacon transmissions are expected to occur.

While the actual beacon might be transmitted shortly before or after this time due to channel availability or power-saving mechanisms, the TBTT is the ideal scheduled time.

The client checks:

Is the SSID the one it wants?

Is the signal strength acceptable (RSSI)?

Is the security method compatible?

Is it allowed to connect (based on configured preferences or policies)?

Authentication Request

If the client chooses to join the network, it sends an authentication request to the AP.

The AP replies with an authentication response.

This is a null authentication in open networks, or

Uses shared key authentication in older WEP networks.

Association Request

Once authenticated, the client sends an association request frame.

This includes its capabilities (supported rates, QoS features, etc.)

The AP responds with an association response, which confirms the client is now associated.

INTRODUCTION

- **Wi-Fi direct** is new technology
  - enhancing **direct device to device communication without** requiring a wireless access point.

- Wi-Fi direct builds upon the successful IEEE 802.11 infrastructure mode
  - lets **devices negotiate** who will take over the **AP-like** functionalities.

TECHNICAL OVERVIEW

- In a **typical Wi-Fi network**, client scans and associate to wireless networks available, which are created and announced by Access Points (AP).

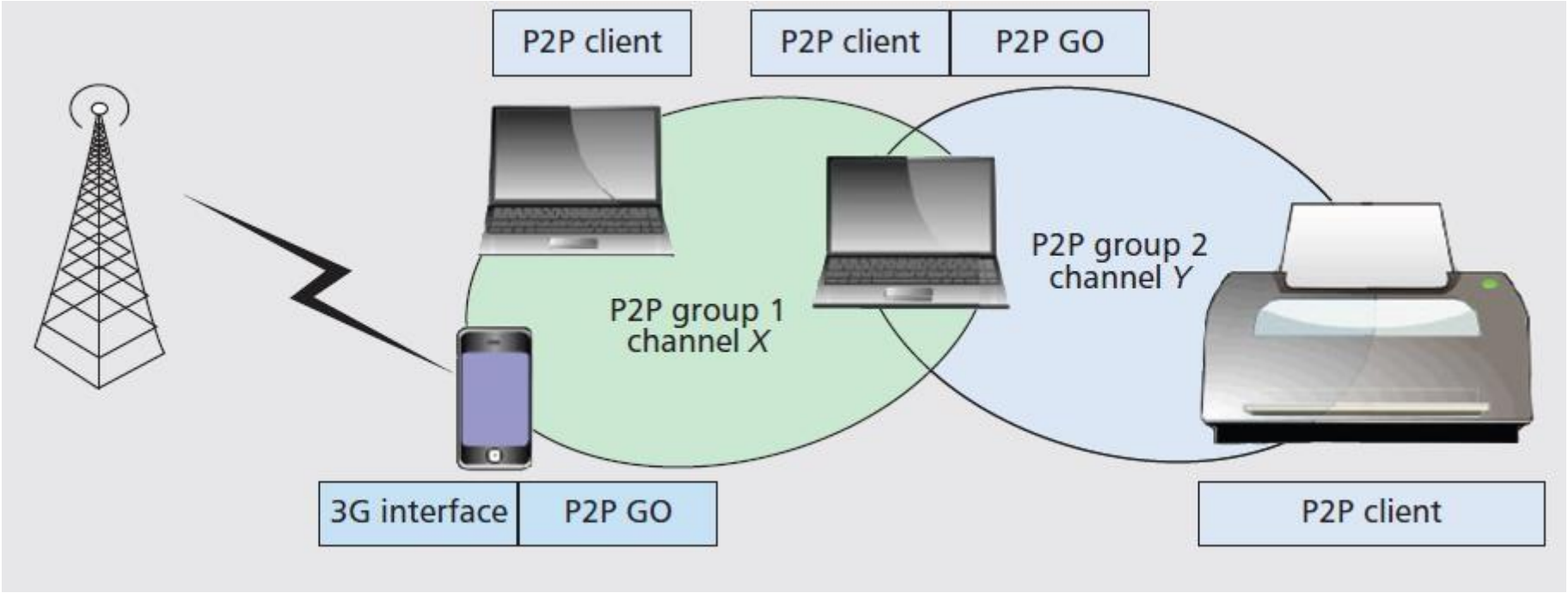
- Wi-Fi Direct is that **these roles are specified as dynamic**,
  - hence a Wi-Fi Direct device has to implement both the role of a client and the role of an AP.

- These roles are therefore **logical roles** that could even be **executed simultaneously** by the same device, this type of operation is called **Concurrent mode**.

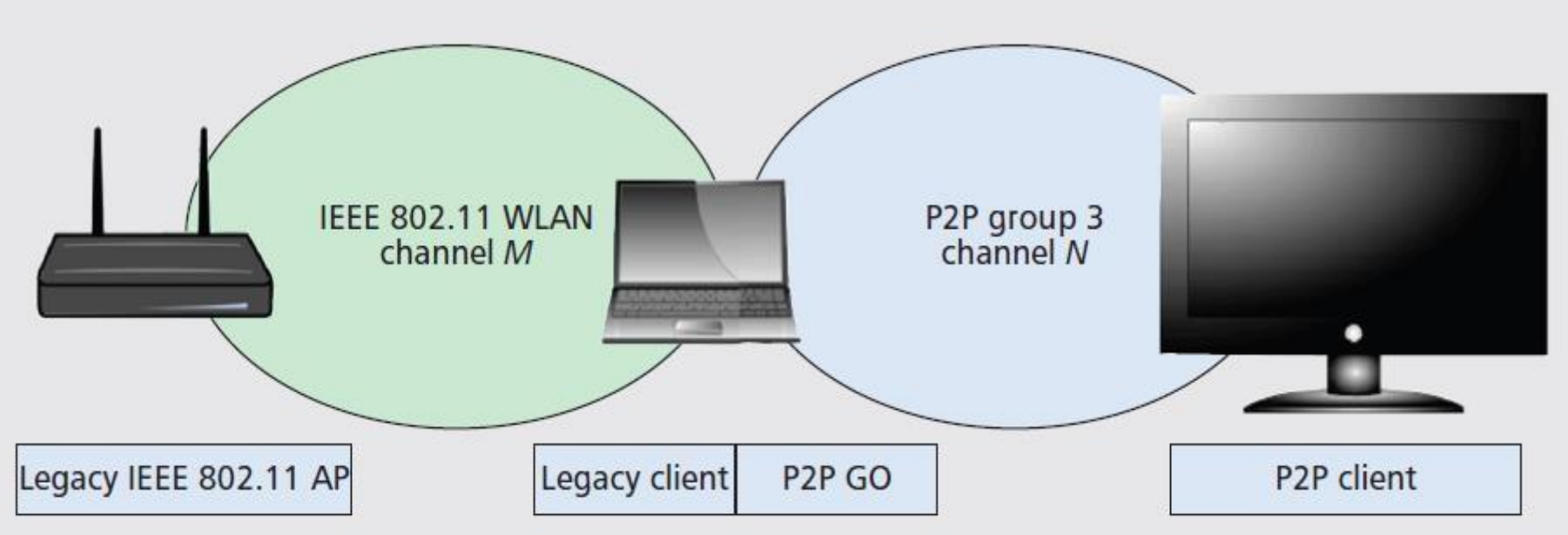
Wifi diect ARCHITECTURE

- Wi-Fi direct device communicate by **establishing P2P group**.
- The device implementing AP-like functionality in P2P group is referred to as the P2P Group Owner(P2P GO), and device acting as client are known as P2P clients.
- Once P2P group is established, other P2P clients can join the group as in a traditional Wi-Fi network.
- When the device act as both as P2P client and as P2P GO
  - the device will typically alternate between the two roles by time-sharing the Wi-Fi interface
- Like a traditional AP, a P2P GO announces itself through beacons, and has to support power saving for its associated clients.

Wi-Fi Direct Setup: Scenario 1



Wi-Fi Direct Setup: Scenario 2



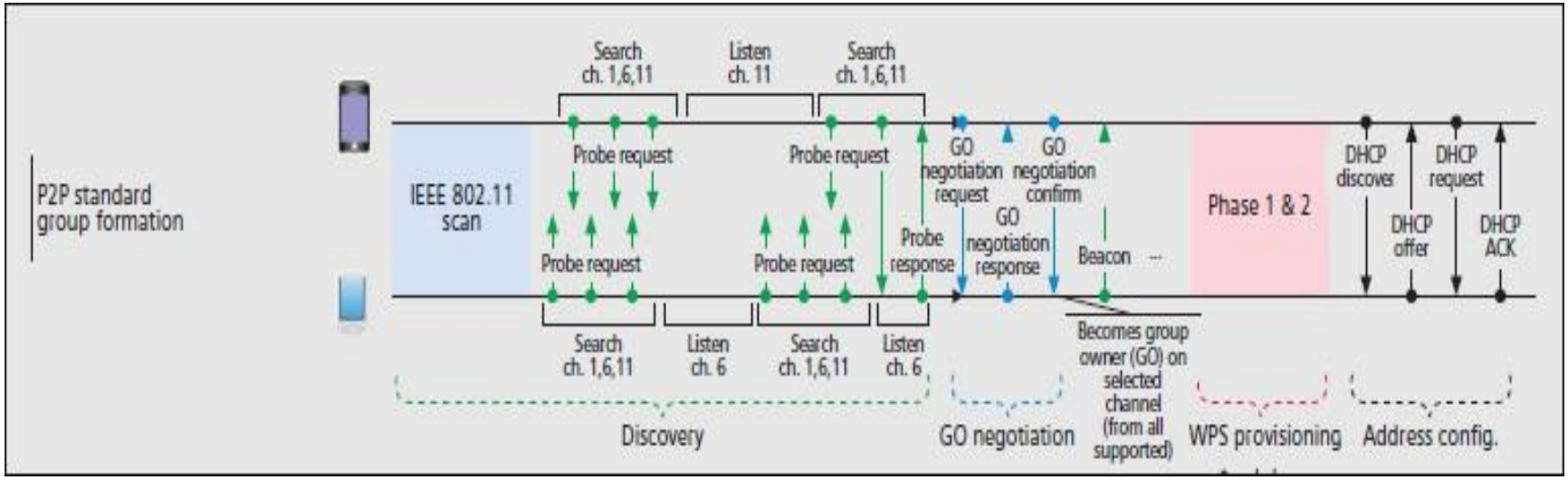
- Only the P2P GO is allowed to **cross-connect** the devices in its P2P group to an external network.
- Wi-Fi direct **does not allow transferring** the role of P2P GO within the group.
- If P2P **GO leaves** the P2P group then the group is **break down**, and has to re-established.

GROUP FORMATION

- Three types of group formation techniques
  - Standard
  - Autonomous
  - Persistent
- Group Formation procedure involves two phases-
  - Determination of P2P Group owner
    - Negotiated - Two P2P devices negotiate for P2P group owner based on desire/capabilities to be a P2P GO.
    - Selected - P2P group Owner role established at formation or at an application level
  - Provisioning of P2P Group
    - Establishment of P2P group session using appropriate credentials
    - Using Wi-Fi simple configuration to exchange credentials.

GROUP FORMATION: Standard

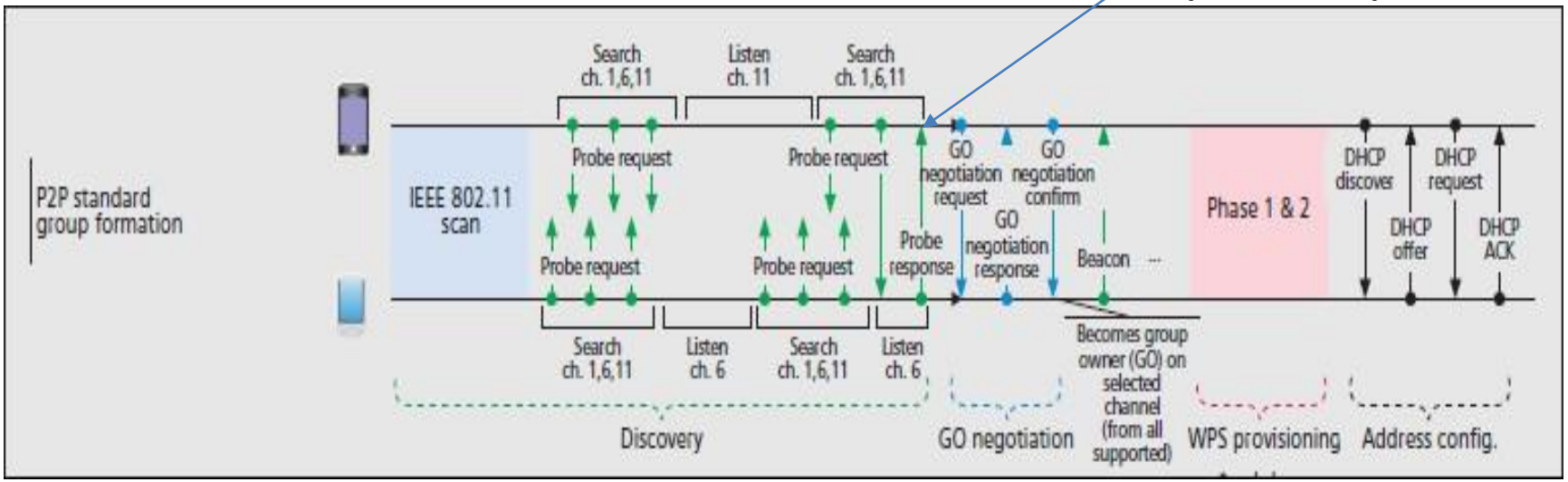
- In this case the P2P device have to discover each other, and then negotiate which device will act as P2P GO.
- Its start by performing a traditional Wi-Fi scan, by means of which they can discover existent groups and Wi-Fi network.



GROUP FORMATION: Standard

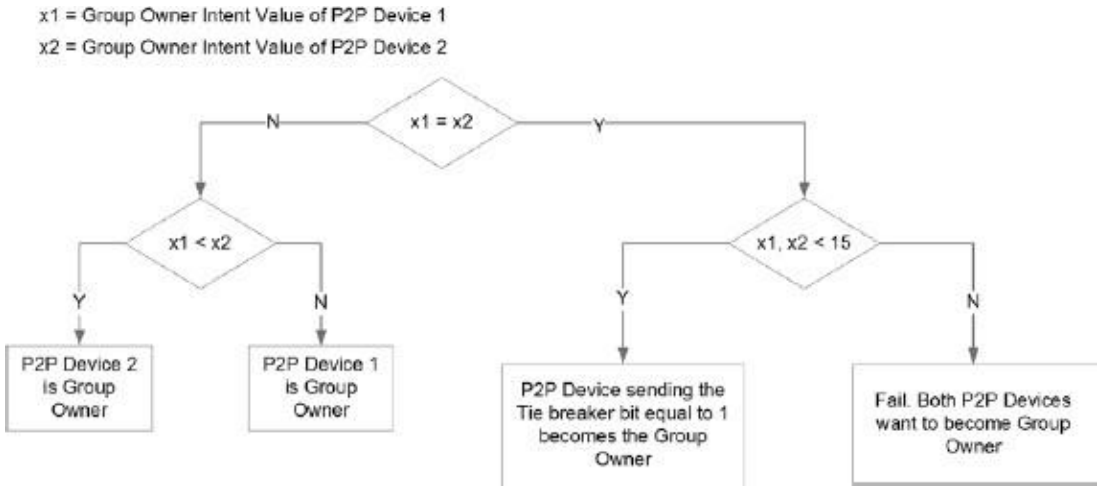
- Discovery algorithm: P2p device selects one of the social channels (2.4 GHz– ch-1, 6, 11)
- Two state – (a) search – sends Probe request (and listens for the probe response)
- (b) listen----listens for probe request ---- sends Probe response
- Each state ---------- 100 ms to 300 ms
  - Tradeoff (discovery time with throughput, energy)

Listens for the probe response



GROUP FORMATION: Standard

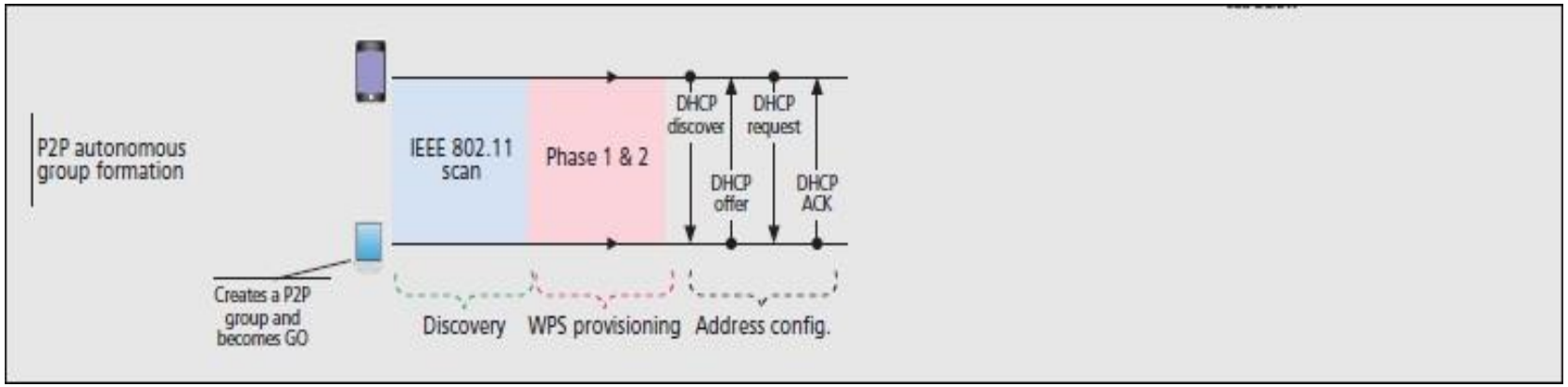
- Select GO----GO negotiation phase
- Three way handshake (request/response/confirmation)
- Selects GO and channel (2.4Ghz, 5Ghz)
- P2p device sends a numerical value --- GO Intent
  - Highest value



- To prevent conflicts when two devices declare the same GO Intent, a tie-breaker bit is included in the GO Negotiation Request,
- Randomly set every time a GO Negotiation Request is sent.

GROUP FORMATION: Autonomous

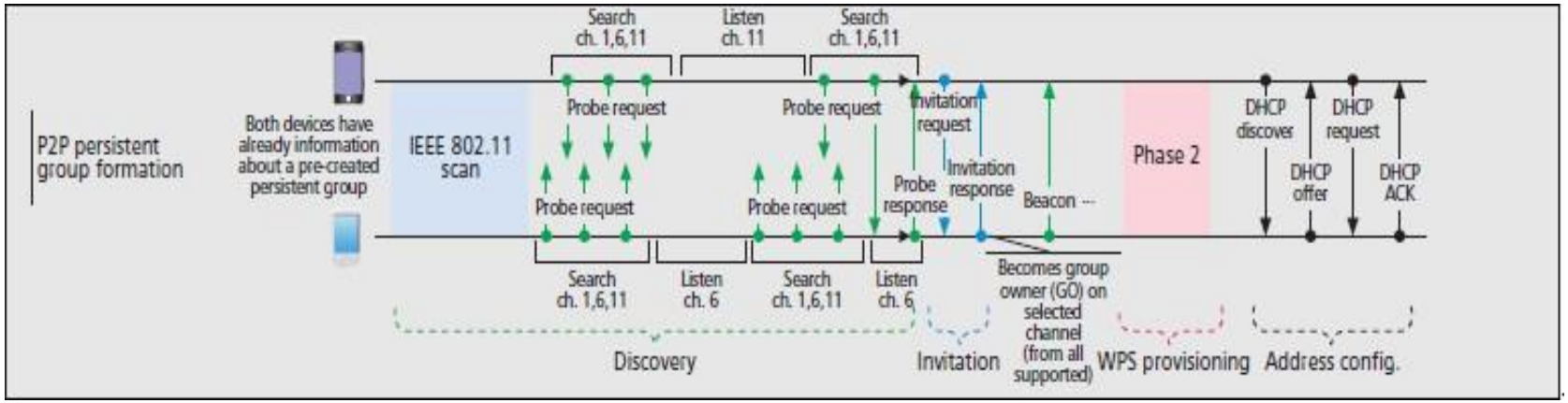
- A P2P device may autonomously create a P2P group,
  - it immediately becomes the P2P GO, by sitting on a channel and starting a beacon.



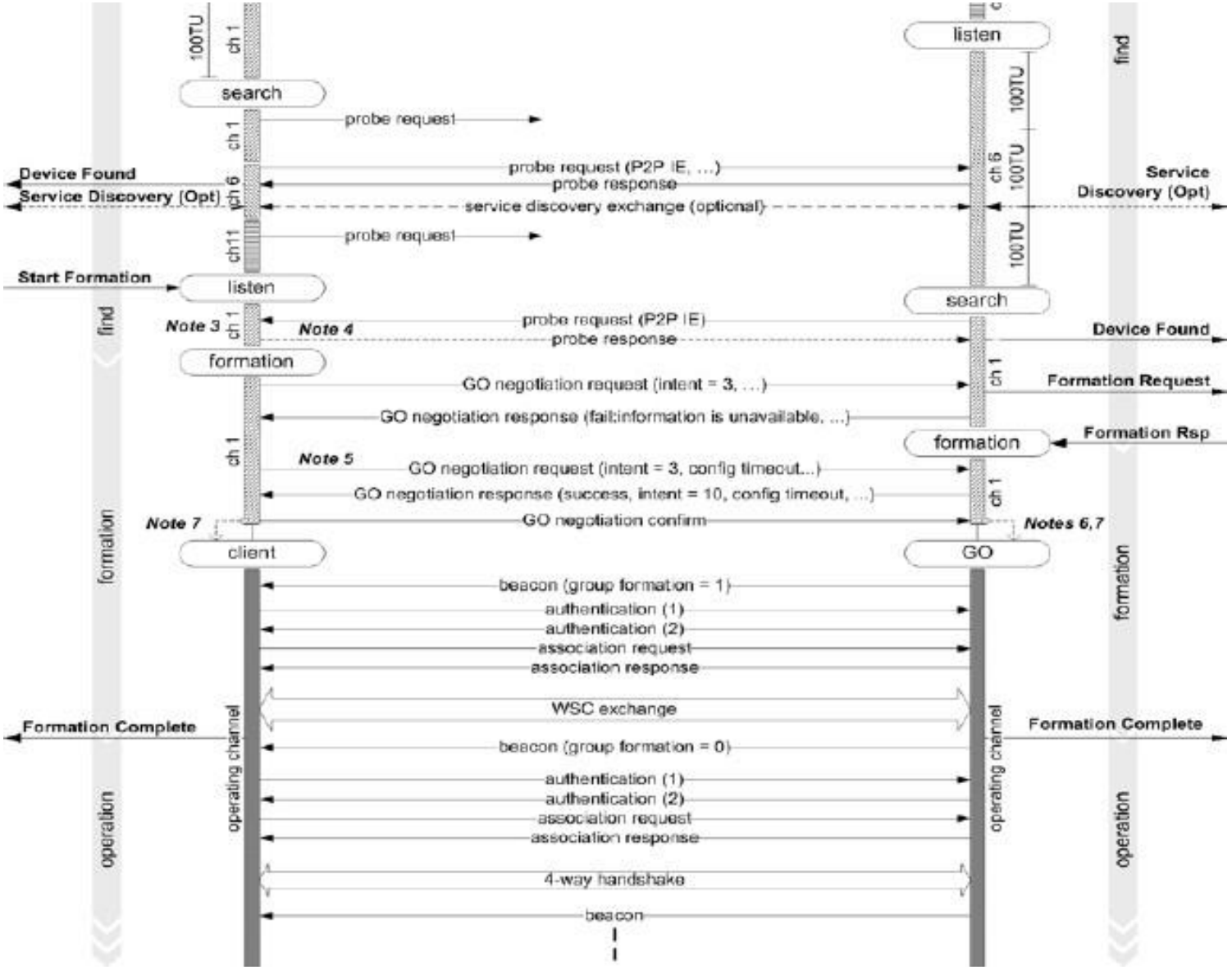
- Other devices can discover the established group using traditional scanning mechanisms.
- As compared to previous case, the discovery phase is simplified
  - the device establishing the group does not alternate between states, and indeed no GO negotiation phase is required.

GROUP FORMATION: Persistent

- In this process, P2P device can declare a group as persistent, by using flag in the P2P capabilities attribute present in beacon frames.



- After the discovery phase, if a P2P device recognizes to have formed a persistent group with the corresponding peer in the past, any of the two P2P devices can use the Invitation Procedure to quickly re-instantiate the group.

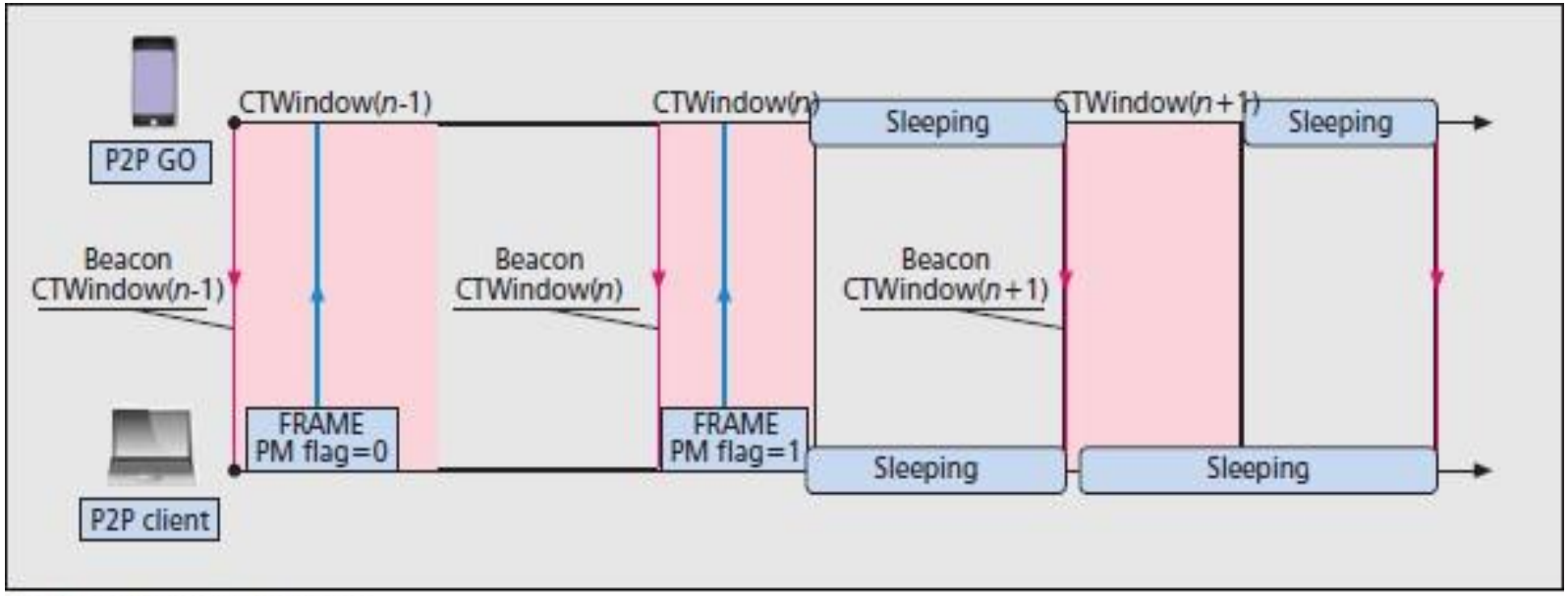

100TU
ch 1
search
probe request
ch 1
Device Found
Service Discovery (Opt)
ch 6
probe request (P2P IE, ...)
probe response
service discovery exchange (optional)
ch11
probe request
Start Formation
listen
find
Note 3
ch 1
Note 4
probe request (P2P IE)
probe response
formation
GO negotiation request (intent = 3, ...)
GO negotiation response (fail:information is unavailable, ...)
ch 1
Note 5
GO negotiation request (intent = 3, config timeout...)
GO negotiation response (success, intent = 10, config timeout, ...)
Note 7
GO negotiation confirm
client
formation
beacon (group formation = 1)
authentication (1)
authentication (2)
association request
association response
WSC exchange
Formation Complete
operating channel
beacon (group formation = 0)
authentication (1)
authentication (2)
association request
association response
4-way handshake
beacon
operation
listen
100TU
ch 6
100TU
100TU
search
find
Service Discovery (Opt)
Device Found
ch 1
Formation Request
formation
Formation Rsp
ch 1
Notes 6,7
GO
formation
Formation Complete
operating channel
operation

POWER SAVING

- Wifi provides power saving of p2p clients
  - Power management bit
    - Client goes to sleep
  - No option for power saving for AP
- Wi-Fi Direct defines two new power saving mechanisms:
  - Opportunistic Power Save
  - Notice of Absence

POWER SAVING: Opportunistic Power Save

- P2p clients can move to sleep state
- Allows a P2P GO to save power when all its associated clients are sleeping.
- The P2P Group Owner can only save power when all its clients are sleeping.



Opportunistic power save

POWER SAVING: Opportunistic Power Save

Target Beacon Transmission Time

Traffic indicator map

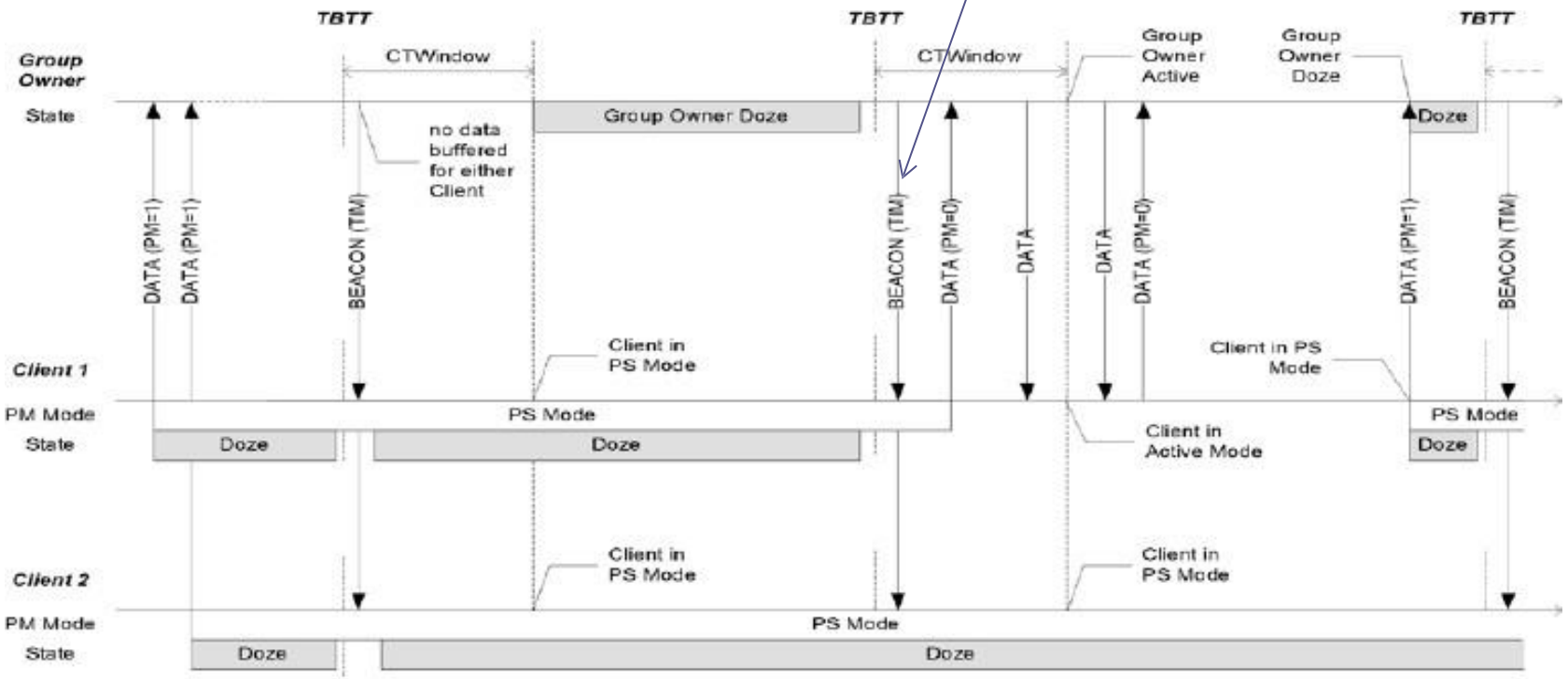
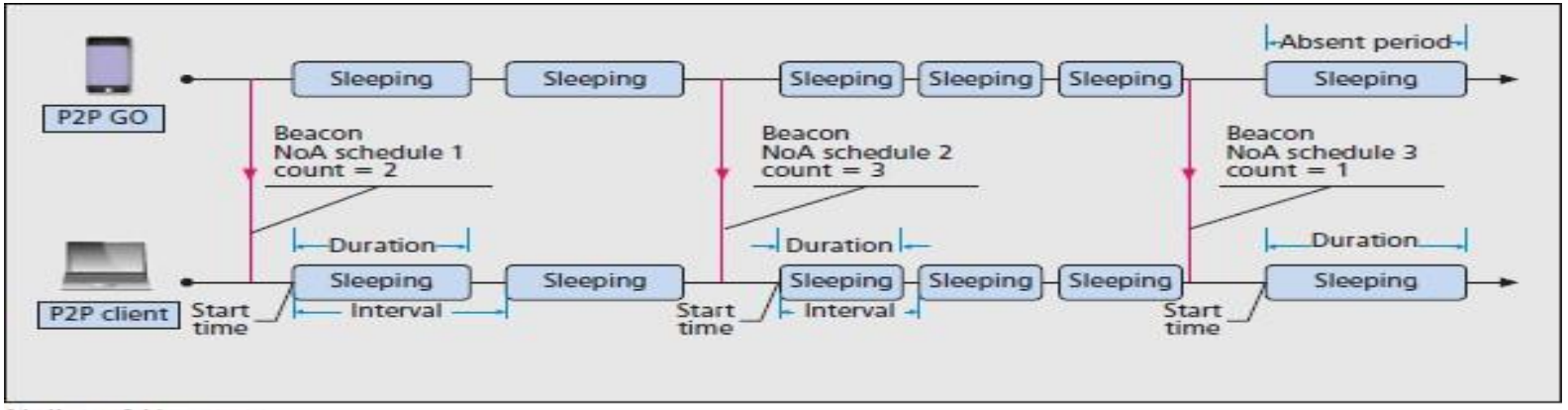


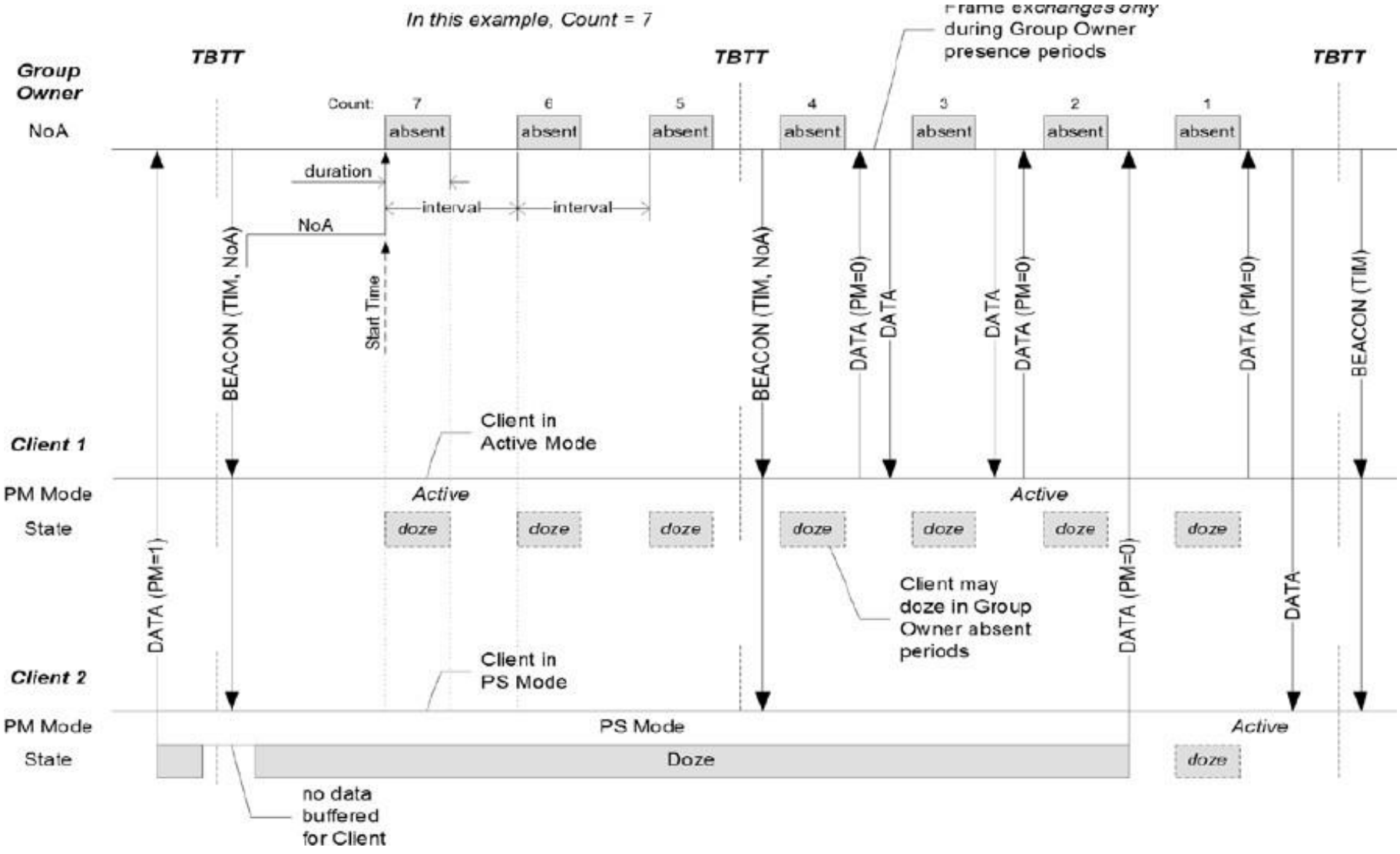
Fig.5. Opportunistic Powersave Operation

POWER SAVING: Notice of Absence

- This protocol (NoA) allows a P2P GO to announce time intervals, referred to as absence periods, where P2P Clients are not allowed to access the channel.---Beacons, probe response
- P2P GO defines a NoA schedule using four parameters:
  - Duration that specifies the length of each absence period
  - Interval that specifies the time between consecutive absence periods
  - Time that specifies the start time of the first absence period after the current Beacon frame
  - Count that specifies how many absence periods will be scheduled during the current NoA schedule.



Notice of Absence


In this example, Count = 7
Frame exchanges only during Group Owner presence periods
TBTT
TBTT
TBTT
Group Owner
NoA
Count: 7 6 5 4 3 2 1
absent
duration
interval
interval
NoA
Start Time
BEACON (TIM, NoA)
BEACON (TIM, NoA)
BEACON (TIM)
DATA (PM=0)
DATA
DATA
DATA (PM=0)
DATA (PM=0)
Client 1
Client in Active Mode
PM Mode
State
Active
Active
doze
Client may doze in Group Owner absent periods
DATA (PM=1)
DATA (PM=0)
DATA
Client 2
Client in PS Mode
PM Mode
State
PS Mode
Active
Doze
doze
no data buffered for Client

Provisioning Discovery – Overview

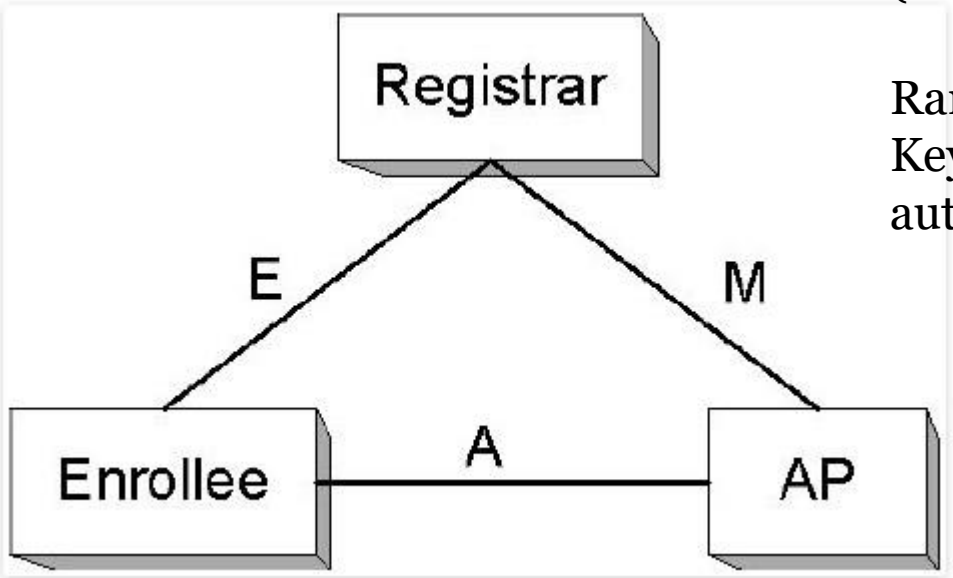
- Occurs after GO negotiation and before WPS provisioning.
- Devices decide on the method for secure group formation (e.g., PIN, PBC).
- Exchange of Provision Discovery Request and Response frames.
- Frames include device info and supported WPS methods.
- No credentials are exchanged at this stage.

WPS Provisioning – Overview

- Begins once the WPS method is agreed upon.
- Uses WPS protocol to authenticate and exchange WPA2 keys.
- Methods: Push Button Configuration (PBC) or PIN.
- Establishes secure group and enables data exchange.
- Keys are stored if persistent group is created.

SECURITY

- Wi-Fi Direct devices are required to implement Wi-Fi Protected Setup (WPS) to support a secure connection with minimal user intervention.
- WPS allows establishing a secure connection by introducing a PIN in the P2P Client, or pushing a button in the two P2P Devices.
- Following WPS terminology, the P2P GO is required to implement an internal Registrar, and the P2P Client is required to implement an Enrollee.
- The operation of WPS is composed of two parts.
- **In the first part**, the internal Registrar is in charge of generating and issuing the network credentials, i.e., security keys, to the Enrollee
- **In the second part**, the Enrollee (P2P Client) disassociates and reconnects using its new authentication credentials.



Advanced Encryption Standard (AES)-CCMP as cipher,

Randomly generated Pre-Shared Key (PSK) for mutual authentication

Service discovery protocol

Generic Advertisement Service (GAS) protocol

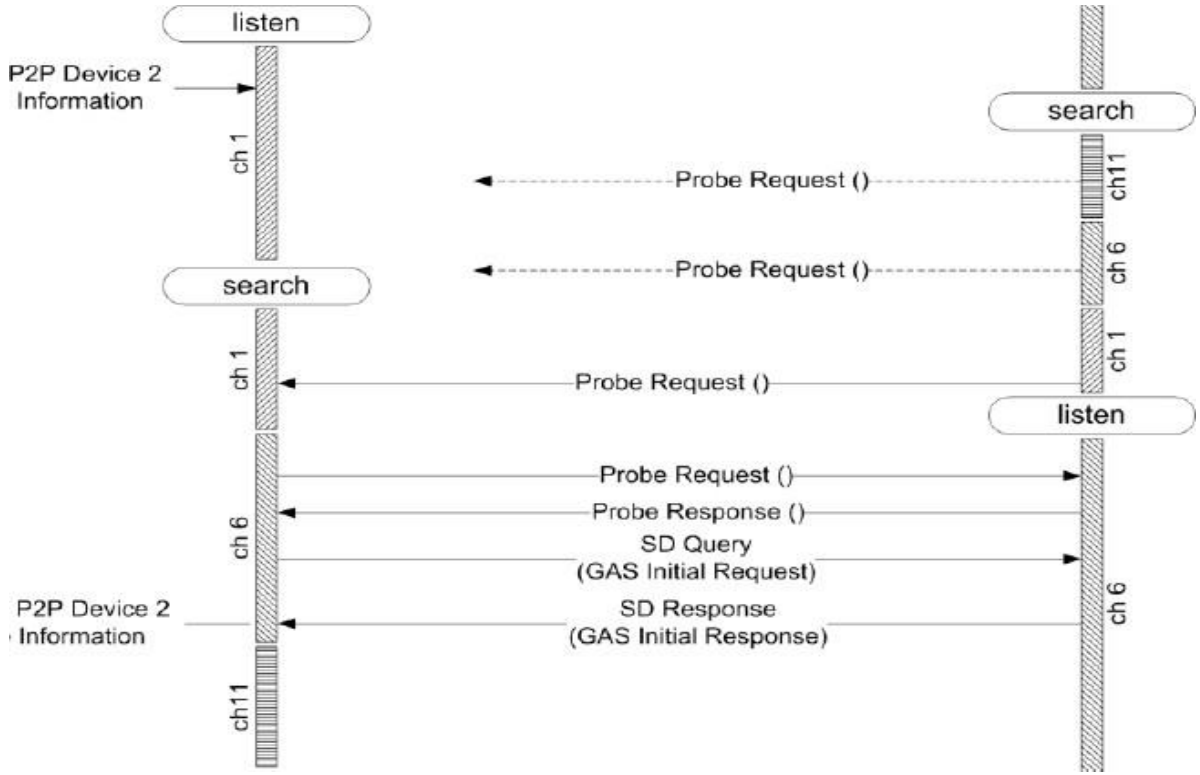
- It may be a single or multiple GAS Initial Request and Response action frame exchange.
- The requesting P2P Device transmits one or more GAS Initial Request frames.
- A target P2P Device that supports Service Discovery responds with one or more GAS Initial Response frames.

- The Service Discovery procedure can be used to find:

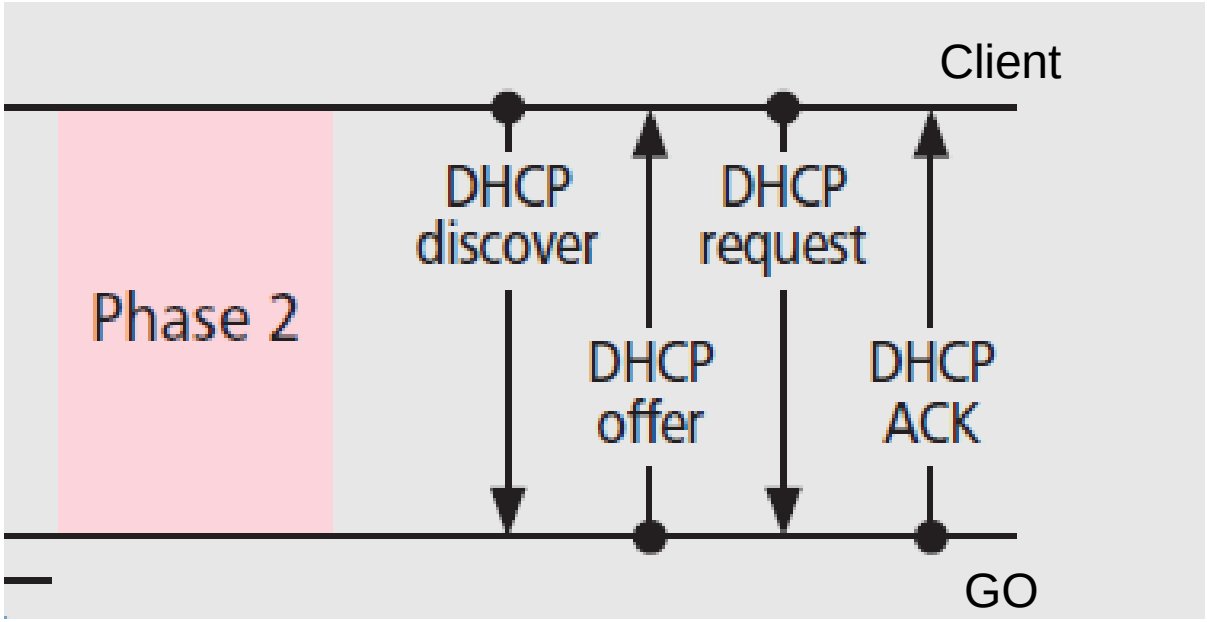
☐ A list of all services offered by a P2P Device
☐ Information about a single service offered by a P2P Device
☐ Information about multiple services offered by a P2P Device
☐ If there has been a change in the services offered by a P2P Device

Service discovery protocol

Generic Advertisement Service (GAS) protocol



Address configuration



Address configuration

Step 1: DHCP DISCOVER (Client → GO)

After association, the P2P Client:

* Broadcasts a DHCP DISCOVER message
* Destination: 255.255.255.255
* Purpose: To find a DHCP server (i.e., the GO)

Step 2: DHCP OFFER (GO → Client)

The GO, acting as a DHCP server, responds with a:

DHCP OFFER message

Includes:

* An available IP address
* Subnet mask
* Gateway (optional)
* Lease time

Address configuration

Step 3: DHCP REQUEST (Client → GO)

The P2P Client:

* Sends a DHCP REQUEST message
* Asks to confirm the IP address offered by the GO

Step 4: DHCP ACK (GO → Client)

The GO sends a DHCP ACK

* Confirms the lease
* The P2P client now officially owns the IP address

CONCLUSIONS

- Wi-Fi alliance has recently developed the Wi-Fi Direct technology that builds upon the Wi-Fi infrastructure mode to enable direct device to device connectivity.
- Thorough overview of the novel technical features specified in Wi-Fi Direct, following by the group formation, and other performance analysis such as power saving and security in this device.
- The NoA protocol could also be re-used to virtualizes the roles of P2P GO/Client over multiple concurrent P2P Groups.
- Concurrent operation together with dynamic nature of the P2P GO/Client roles could be used to improve performance in dense environments, for instance by means of dynamic relays.