Active and Passive Scanning

Scanning:

Before joining any network first client/station needs to find it first.

In the wired world, just plugging the cable or jack will help you find the network.

In the wireless world, it requires identification of the compatible network before joining process can begin.

The identification process of the N/W or discovering the N/W is referred to as scanning.

The reason for client scanning is to determine a suitable AP to which the client may need to connect/ roam now or in the future.

Types of Scanning

1. Active Scanning
2. Passive Scanning

Overview:

* During an active scan, the client radio transmits a probe request and listens for a probe response from an AP.
* With a Passive scan, the client radio listens on each channel for beacon sent periodically by an AP.

Limitations:

* A passive scan generally takes more time, since the client must listen and wait for a beacon frame to find an AP
* Another limitation is that with a passive scan, if the client does not wait long enough on a channel, then the client may miss an incoming beacon frame from the AP.

Passive Scanning:

With passive scanning, the wireless client tunes its radio to each possible channel in turn and listens for signals from access points. The speed and duration of dwelling time on each channel depends on the wireless client vendor driver and is defined in each driver MIB by the MaxChannelTime parameter.

*Beacon frames* are used by the access points (and stations in an IBSS) to communicate throughout the serviced area the characteristics of the connection offered to the cell members. This information is not only used by potential clients during passive scanning but also by clients that are already associated to the BSS.

Beacon frames are sent periodically, at a time called target beacon transmission time (TBTT) and at a rate defined by the dot11BeaconPeriod parameter.

The dot11BeaconPeriod parameter is by default 100time units (TUs), that is, 102,400 microseconds, which is a little over 102 milliseconds. This interval can be configured on some access points.

The access point tries to send the beacon at each defined TU interval and announces.

when the next beacon is expected to be sent. Nevertheless, access points are just like any wireless device in the cell. They cannot send if the network is busy. When the time comes for an AP to send a beacon, if the network is busy, the AP will delay its beacon transmission until it can gain access to the media. Although the beacon is slightly delayed, the AP will still try to send the next beacon at the originally planned interval. For example, suppose that a beacon is to be sent every 102.4 milliseconds, at times 0, 102.4, and 204.8.

The first beacon is sent on time, but suppose the network is busy at time 102.4. The second beacon has to be delayed and can then be sent, for example, at time 103.2 millisecond and therefore 0.8 millisecond late. The AP will still try to send the third beacon at time 204.8 and will not delay that third beacon even if the previous one was late.

All stations in the cell use the AP beacon as a time reference. Each beacon contains a time stamp and also an indication about when the next beacon will be sent. Each station uses the time stamp with what the 802.11 standard calls the timing synchronization function (TSF) to make sure that their clock uses the same tempo as the access point.

A beacon can contain mandatory element but also optional and vendor specific elements. The size of the beacon body can vary depending on the type of information carried by the beacon.

A beacon frame contains in total 41 elements. The mandatory ones are:

1. Timestamp
2. Beacon interval
3. SSID
4. Capability Information
5. Supported rates

Active Scanning:

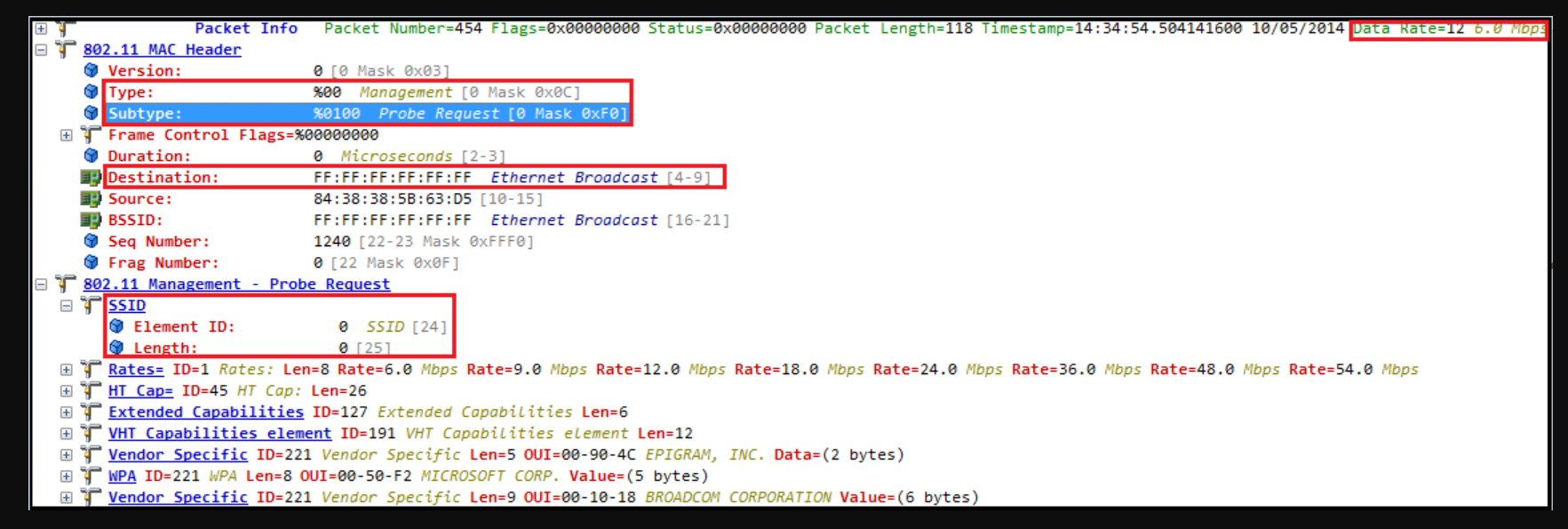
Discovering the network by scanning all possible channels and listening to beacons is not considered to be very efficient. At the scale of a wireless NIC, this process is seen as slow.

To enhance this discovery process, stations often use what is called active scanning. In this mode, stations still go through each channel in turn, but instead of passively listening to the signals on that frequency, stations send a *probe request* management frame aimed at asking what network is available on this channel. If any AP or active station in an IBSS is present on that frequency, they should answer with the requested information

The probe request

frame body contains the element and fields listed:

1. SSID
2. Supported rates
3. Request information
4. Extended supported rates
5. Vendor specific



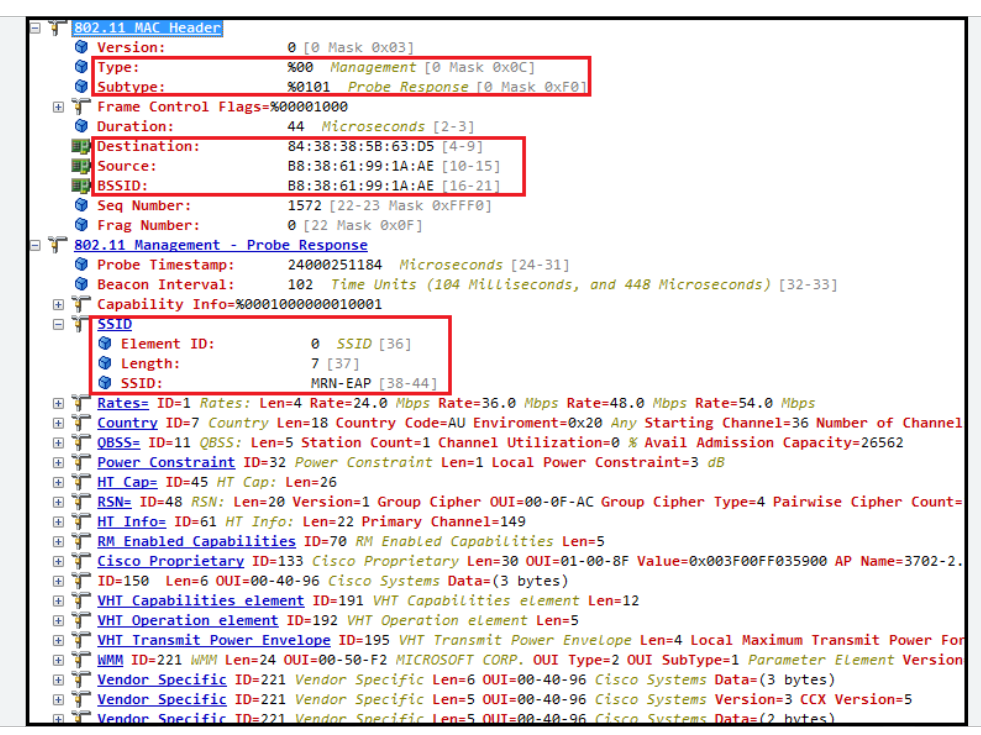
The probe requests are usually sent to the broadcast DA address (ff:ff:ff:ff:ff:ff). The frame is sent using the common CSMA/CA procedure. Once the probe is sent, the emitting station starts a ProbeTimer countdown and waits for answers. This ProbeTimer value is decided by each vendor, but it is usually a lot shorter than a beacon interval. Common values are in the 10 millisecond range. At the end of the timer, the station processes the answers it has received. If no answer was received, the station moves to the next channel and repeats the discovery process.

Stations sending probe requests may specify the SSID they are looking for (in that case the probe request is called a *directed probe request*). Only those IBSS stations or APs supporting the requested SSID will answer. The SSID value can also be set to 0 (that is, the SSID field is present but empty). This is called a wildcard SSID, and the frame is a null probe request. In that case, an IBSS station or AP on the probed channel should send a probe response indicating the SSID it supports and the characteristics of the cell.

The purpose of a probe request is typically to discover APs and their supported networks (SSIDs and/or BSSIDs).

The station performing the discovery indicates the rates it supports so that the AP or IBSS station answering the probe request can determine the best data rate to use for the answer. The requesting station may also use the probe request to discover specific elements about the network (for example, “What are the local country parameters?”). To allow for this additional information discovery, the probe request can contain a Request Information element. The Request Information element is optional.

Upon receiving a probe request frame, a station in an IBSS or an AP will respond with a *probe response* frame, which contains information about itself and the cell.



The format of the probe response is very close to the format of a beacon, because both frames essentially answer the same question: what are the specs of the cell?

The probe response is sent as a unicast frame. The DA field is the MAC address of the station from which the probe request was sent.

The probe response is sent at the lowest common rate supported by both the station sending the probe request and the answering AP (or IBSS station). The probe response should be acknowledged by the receiving station, just like any other unicast frame.

If you compare this list to the beacon frame body component list, you will see that both frame bodies are very similar, with the following differences:

* The beacon frame contains a TIM field; the probe response does not.
* The beacon frame can contain a QoS Capability Information element that announces basic QoS support to the cell.
* The probe response also contains the Requested Information elements that may have

been requested by the probing station.