IEEE 802.11 (Wi-Fi) Addressing: Transit, Multicast, & Mesh

Donald E. Eastlake 3rd (Futurewei)

d3e3e3@gmail.com

Disclaimers

- IEEE 802.11 is a very complex standard. Sometimes it seems like it has every option you can think of. Latest full version (802.11-2020) has 4,377 pages. Many details are omitted in this presentation. (You can get a copy through https://standards.ieee.org/products-services/ieee-get-program.html)
- The opinions, comments, endorsements, and other such information provided here are not those of the IEEE Inc. or IEEE 802 or IEEE 802.11, they are solely the opinion of their author.
- I was the Chair of the IEEE 802.11s Task Group for approximately the first half of its existence. But that was quite a while ago. There may be errors in this presentation.

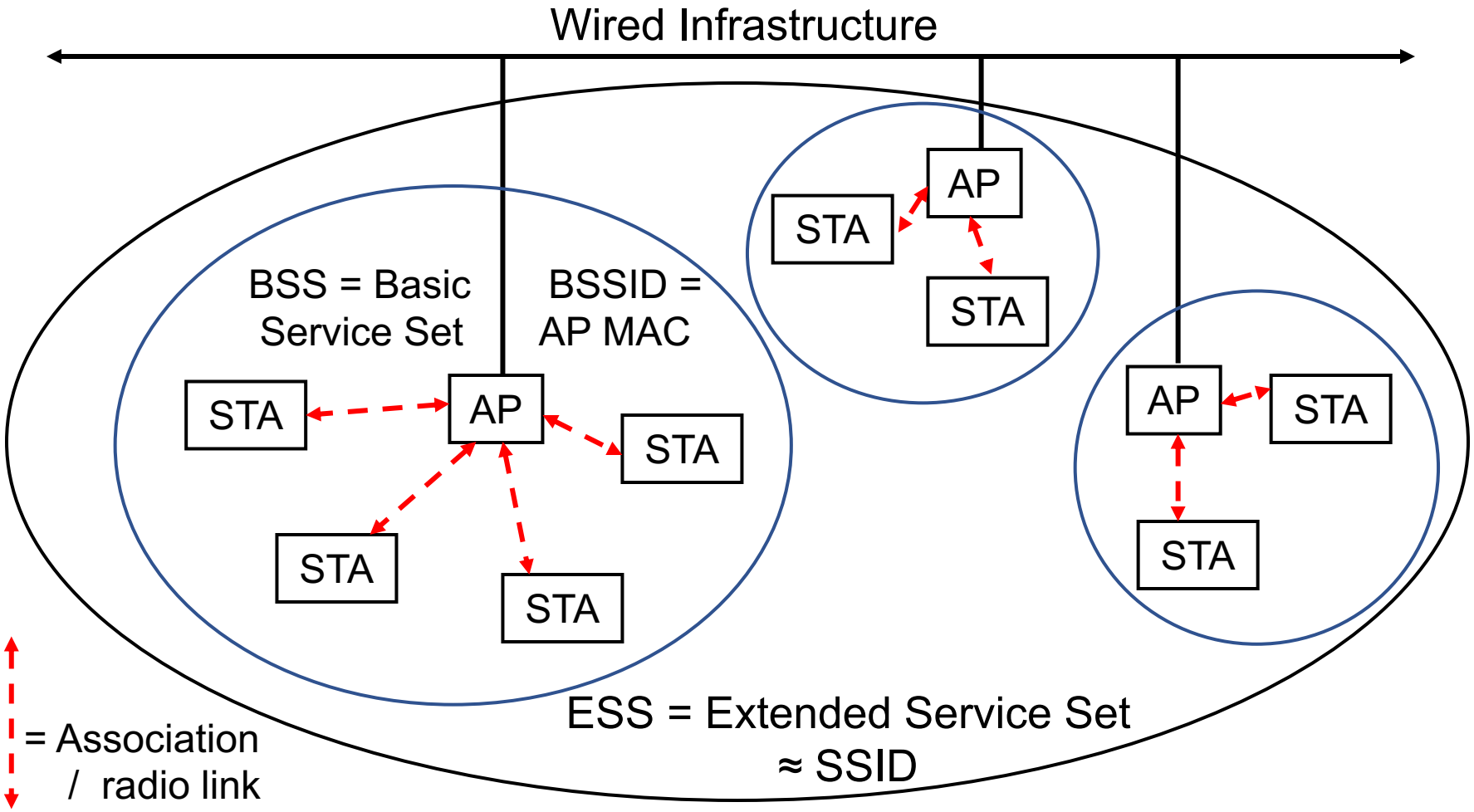
802.11 (Wi-Fi) Miscellaneous

- 802.11 (Wi-Fi) has a lot going for it:
  - Negotiates and adjusts data rates, beam forming, channel switching, national spectra, licensing regimes, etc.
  - Has a multiple levels of aggregation for higher speed / less noisy links and fragmentation for slower speed / more noisy links.
  - Has link level (one-hop) acknowledgement / retransmission (can be defeated with the No Acknowledgement header bit).
  - Radio communication being assumed insecure, encryption and authentication normally implemented in hardware / firmware so there is almost no cost or slowdown in using it.
  - Billions of 802.11 chip sets ship annually.

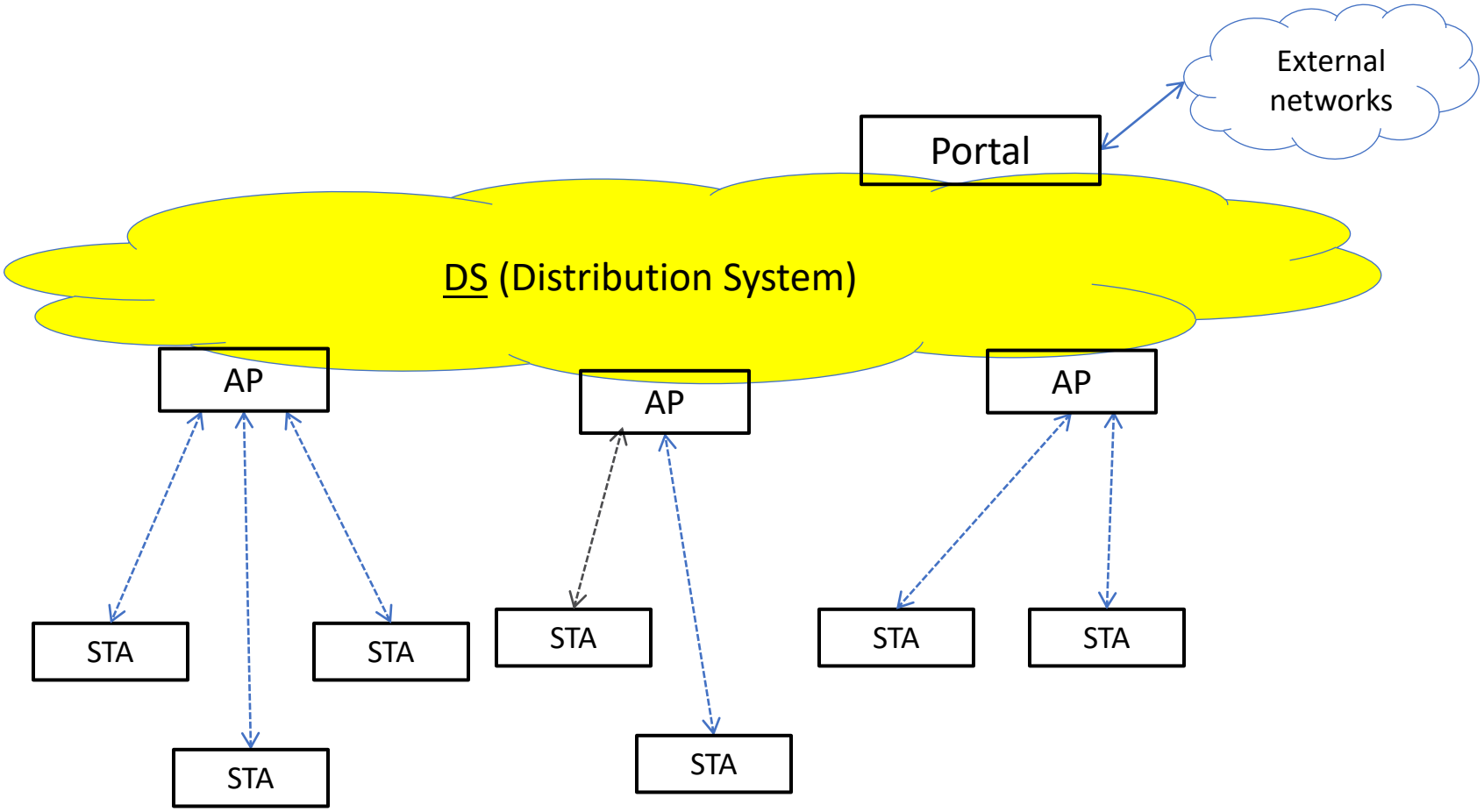
Contents

- Wi-Fi Infrastructure Mode
- Wi-Fi Frame Format, Addressing
- Four Address (Transit Link) Mode
- Wi-Fi Mesh

Wi-Fi Infrastructure mode
The most common mode currently in use



Wi-Fi Infrastructure mode
The most common mode currently in use



Wi-Fi Multicast Reliability

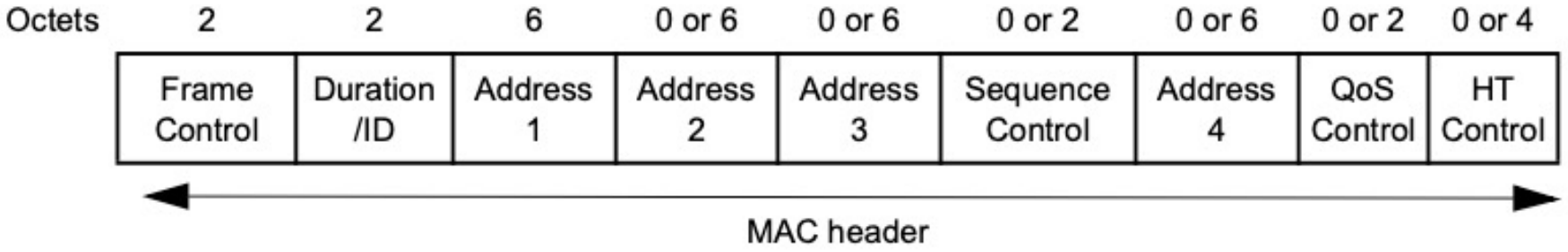
- There are lots of features in 802.11 to improve the reliability of multicast
  - Use of a lowest common denominator bit rate for improved noise resistance
  - Use of serial unicast (except for discovery applications)
  - Multiple transmissions of the same data
  - Block acknowledgements

Contents

- Wi-Fi Infrastructure Mode
- Wi-Fi Frame Format, Addressing
- Four Address (Transit Link) Mode
- Wi-Fi Mesh

Wi-Fi Frame Format

- Wi-Fi uses a unified complex header with many options/flags rather than a sequence of nested headers.



  - FCS = 32-bit Frame Check Sequence

Wi-Fi Frame Format
Usual Frame Control Field

- Protocol Version normally 0.
- Many, many types/subtypes including subtypes of management, control, and data.
- DS = Distributions System (sort of what's behind the Aps)
- More Fragments and Retry are what they say.
- Power Management relates to various power save and sleep modes.
- More Data is only used in some specialized modes.
- Protected Frame means frame body cryptographically protected during over-the-air hop.
- HTC = High-Throughput Control. Includes aggregation, beam forming, etc.

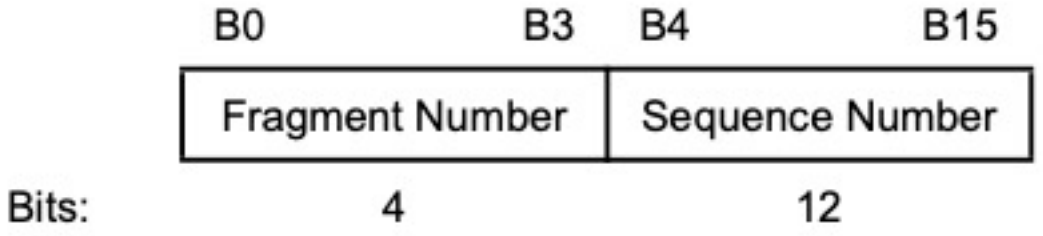
	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
	Protocol Version	Type	Subtype	To DS	From DS	More Frag-ments	Retry	Power Management	More Data	Protected Frame	+HTC
Bits:	2	2	4	1	1	1	1	1	1	1	1

Wi-Fi Data Frame Format
To/From DS Bits, Sequence Control

- The “To DS” and “From DS” bits for Infrastructure.

To DS	From DS	Meaning
0	0	Not part of infrastructure or mesh.
0	1	From AP to STA.
1	0	From STA to AP.
1	1	Transit link.

- The Sequence Control field. Sequence number has to do with detecting duplicates from retransmission within an access (priority) class.



Wi-Fi Data Frame Format To/From DS Bits

- Use of Address Fields
  - DA = Destination Address (might be a multicast address)
  - SA = Source Address
  - RA = Receiver Address (multicast if the DA is multicast)
  - TA = Transmitter Address

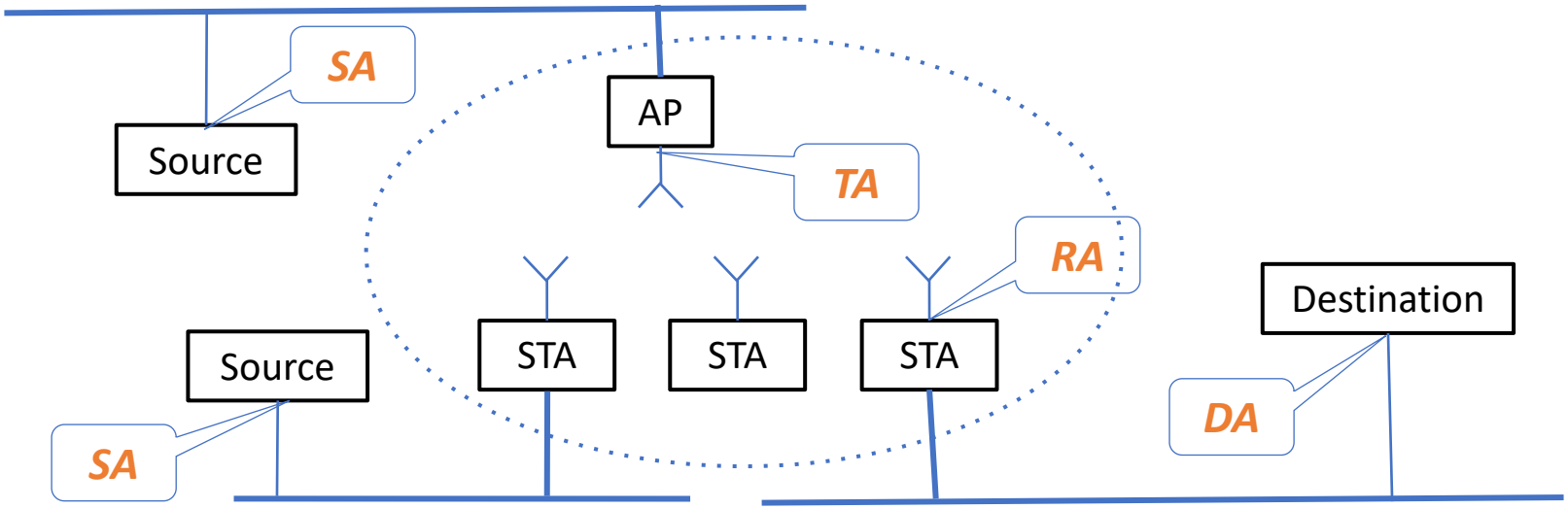
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA=SA	BSSID	Omitted
0	1	RA (STA)	TA (AP)	SA	Omitted
1	0	RA (AP)	TA (STA)	DA	Omitted
1	1	RA	TA	SA	DA

Contents

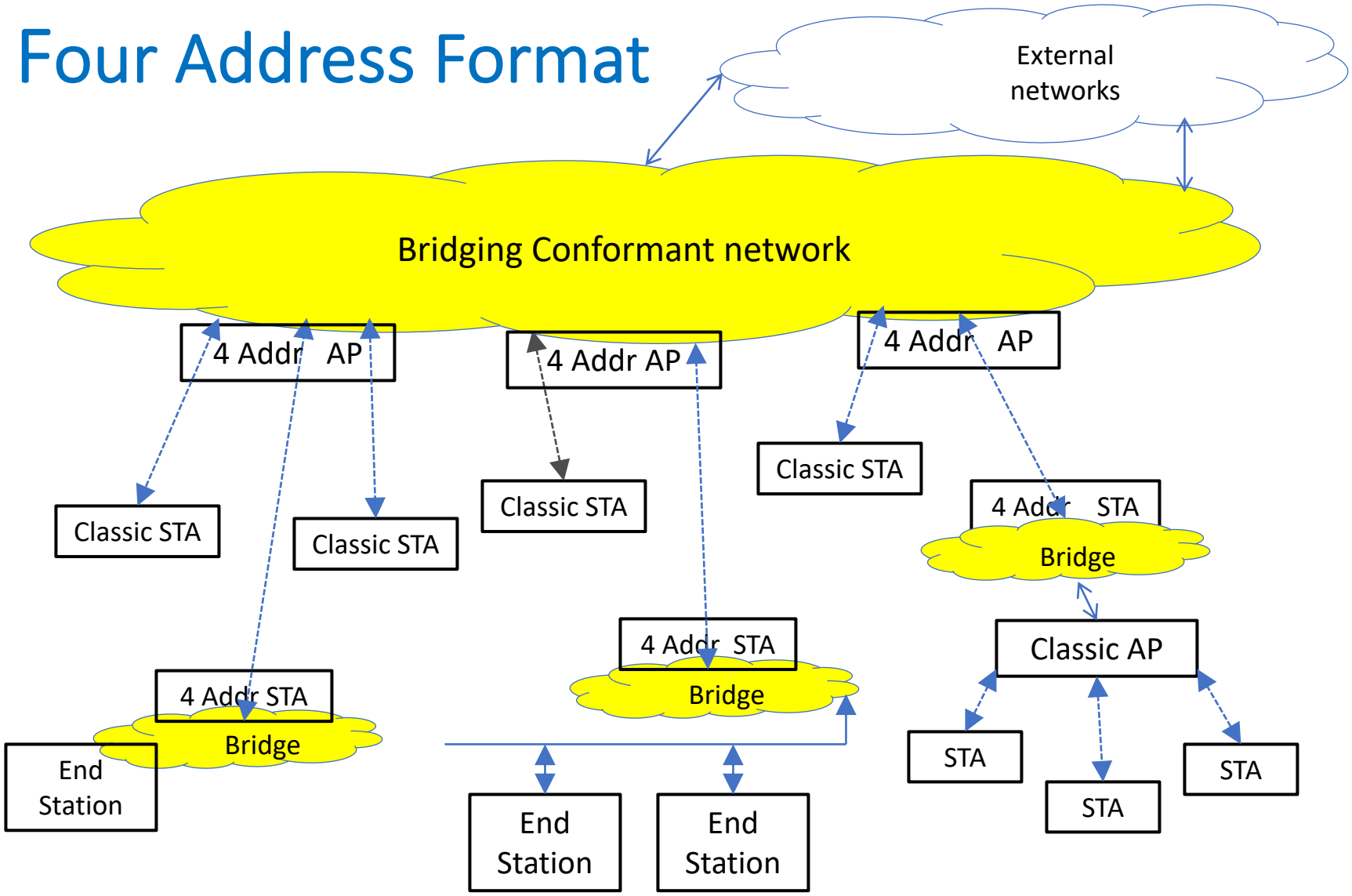
- Wi-Fi Infrastructure Mode
- Wi-Fi Frame Format, Addressing
- Four Address (Transit Link) Mode
- Wi-Fi Mesh

Wi-Fi Data Frame Format
Four Address Format

- Example of four address format use. Done by setting the FromDS and ToDS bits in the header.
  - This provides for the 4 addresses in the overall header or
  - If using an aggregated frame, the overall header has the TA and RA and the aggregated sub-frames have the SA and DA.

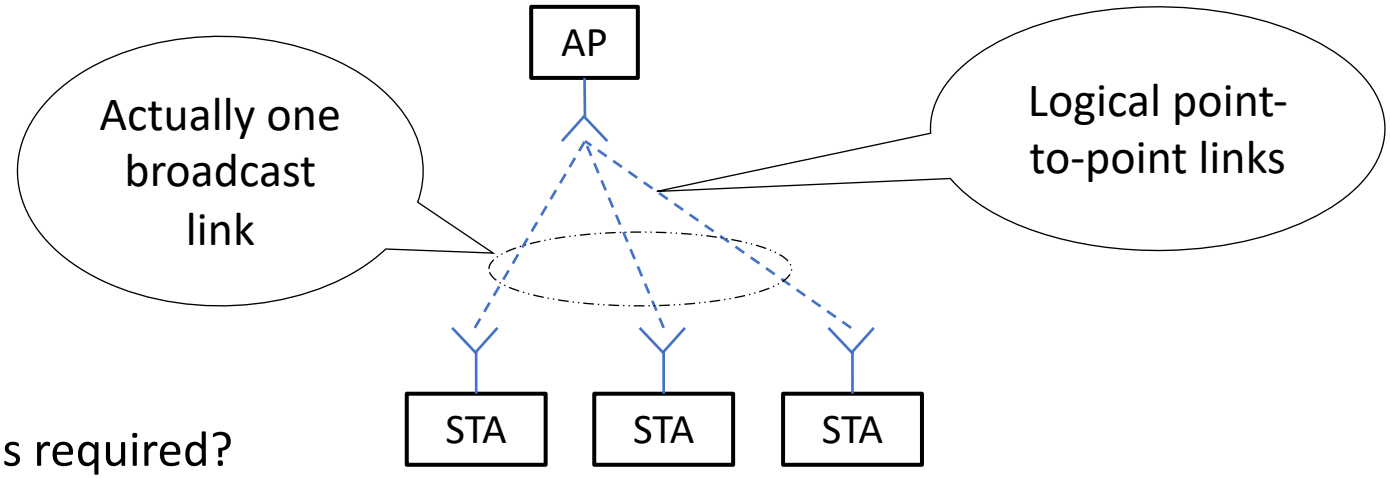


Wi-Fi Data Frame Format
Four Address Format



Wi-Fi Data Frame Format
Four Address Format

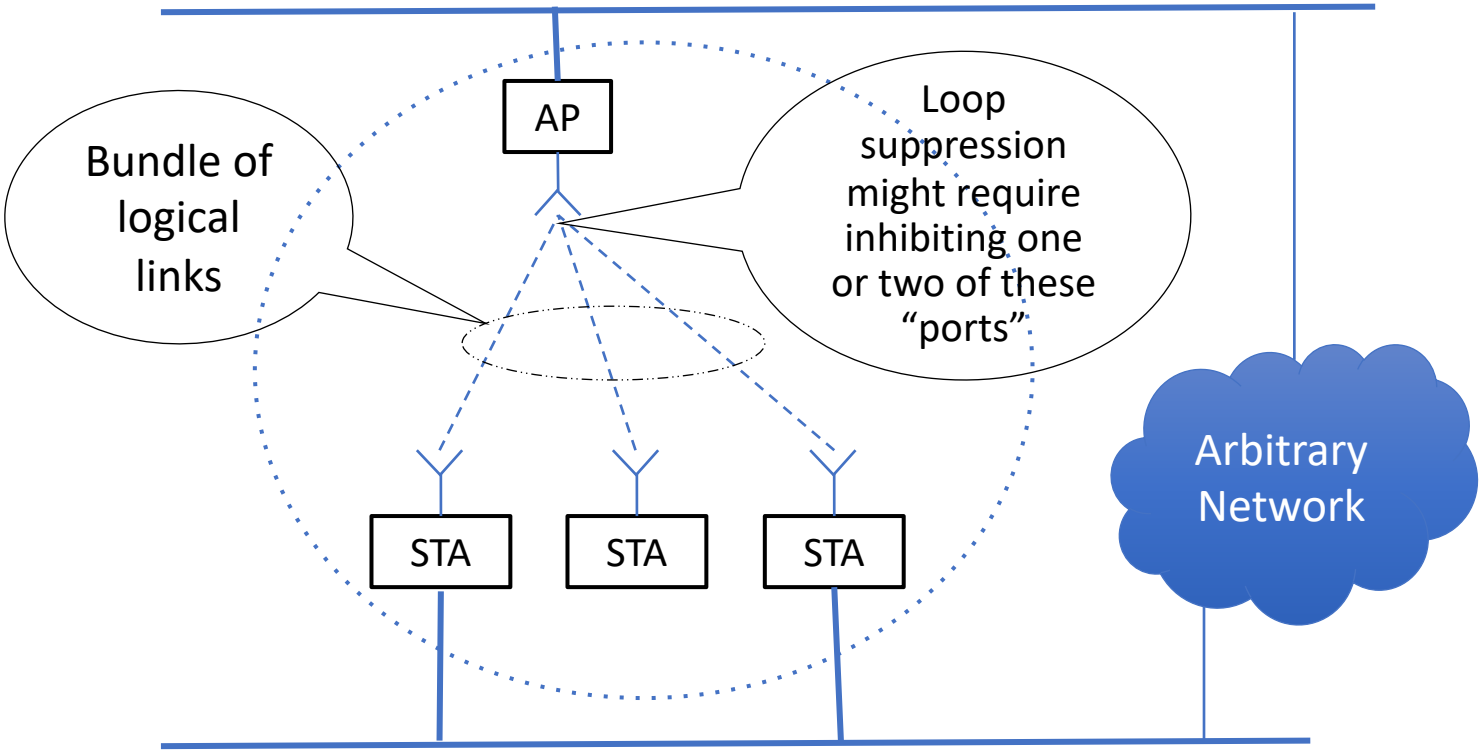
- As far as it can, 4 address mode makes the broadcast channel between an AP and its associated STAs look like point-to-point connections.



- Why is this required?
  - IEEE bridging protocols, including spanning tree, work best with point-to-point links.
  - To implement loop suppression in the general case.
  - To enforce the Ethernet requirement that when a station sends a frame, it does not come back to that station.

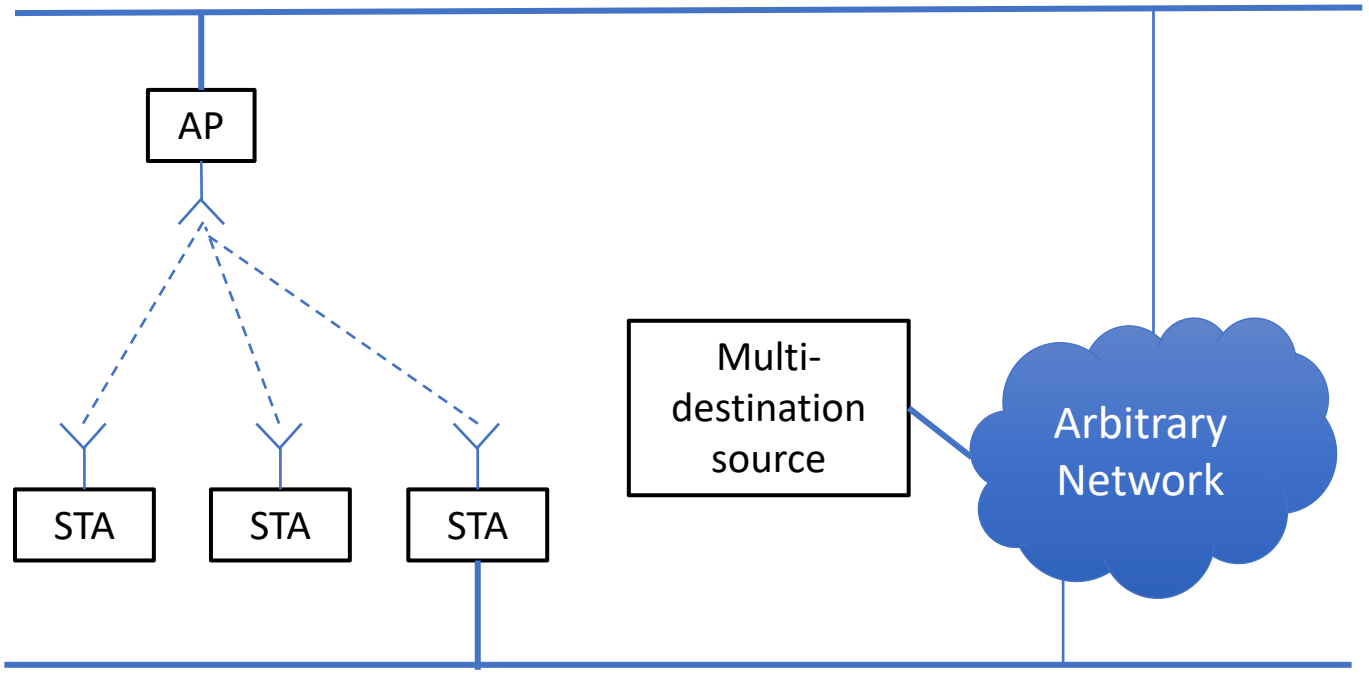
Wi-Fi Data Frame Format
Four Address Format

- Loop suppression may require inhibiting individual logical “ports” at an AP.



Wi-Fi Data Frame Format
Four Address Format

- Ethernet requires that a frame not come back to the sender.
  - Not a problem with 3-address infrastructure because a STA can recognize frames it sent by seeing itself as the SA.
  - In the 4-address case, only the AP knows so if it receives a multi-destination MPDU from a STA, it must not send it back to that STA.



Contents

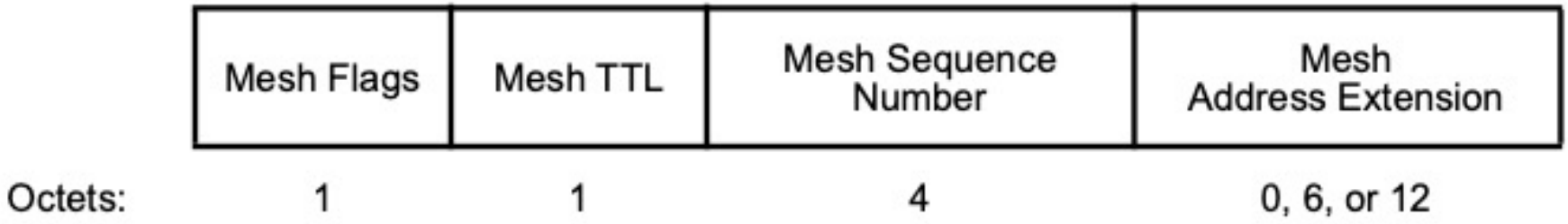
- Wi-Fi Infrastructure Mode
- Wi-Fi Frame Format, Addressing
- Four Address (Transit Link) Mode
- Wi-Fi Mesh

Wi-Fi Mesh

- Links between mesh stations are peer-to-peer.
- Mesh stations have a mesh profile, which must be the same for two mesh station to peer, consisting of the following:
  1. Mesh ID
  2. Path selection protocol identifier
  3. Path selection metric identifier
  4. Congestion control mode identifier
  5. Synchronization method identifier
  6. Authentication protocol identifier

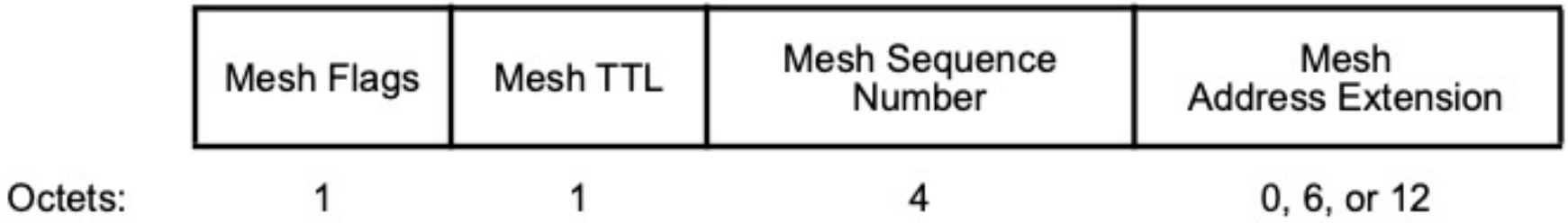
Wi-Fi Mesh

- All 802.11 Mesh Data frames are required to be “QoS Frames”. So, the header extension required for mesh is indicated by a field within the QoS Control field.
- This extension is the Mesh Control Field shown below which is considered to be the first part of the frame body. The main effect of this is that it is encrypted over the air.



Wi-Fi Mesh

- Mesh Flags = currently only used for addressing extension mode.
- Mesh TTL = Set by Mesh Source STA, counted down by subsequently mesh STAs, frame dropped if zero.
- Mesh Sequence Number = Set by Mesh Source STA. Used to discard duplicates based on cached <Mesh Source SA, Mesh Sequence Number> pairs.



Wi-Fi Mesh

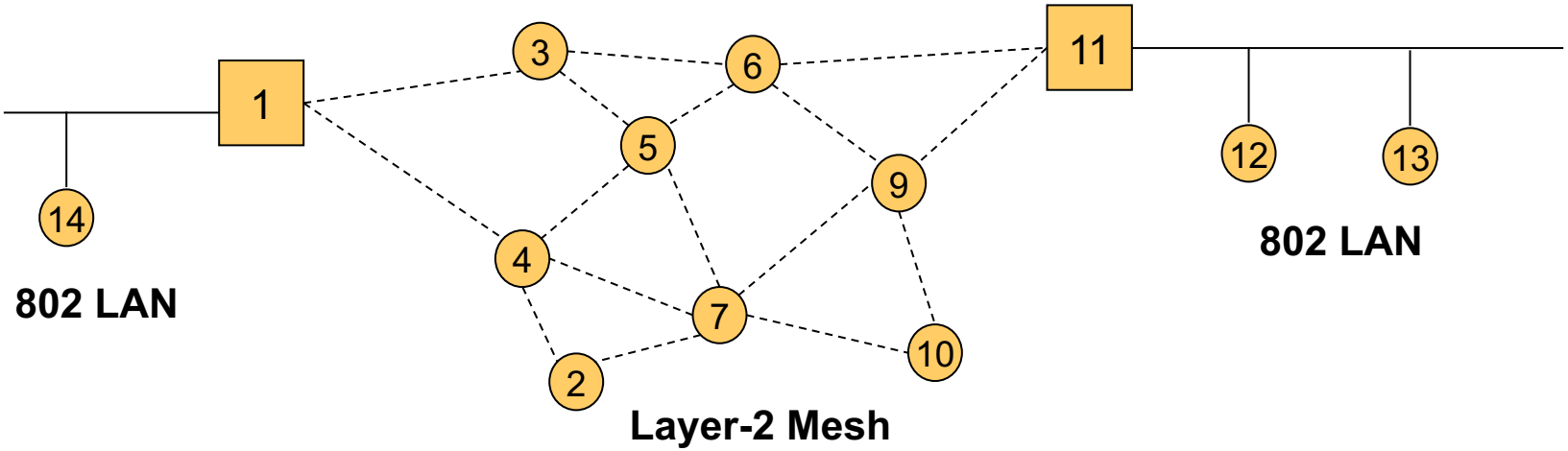
- An 802.11 Mesh appears, from an external point of view, to be a single multi-access link. A mesh can connect to networks that are not 802.11 meshes via mesh stations that are mesh gates and portals.
  - Mesh stations can also be Access Points (APs).
  - Any two or all of the AP, mesh gate, and Portal functions could by co-located in one mesh station device.

Wi-Fi Mesh

- Address Field
  - RA, TA, DA, SA as before
  - Mesh SA is address of first Mesh STA
  - Mesh DA is address of last Mesh STA

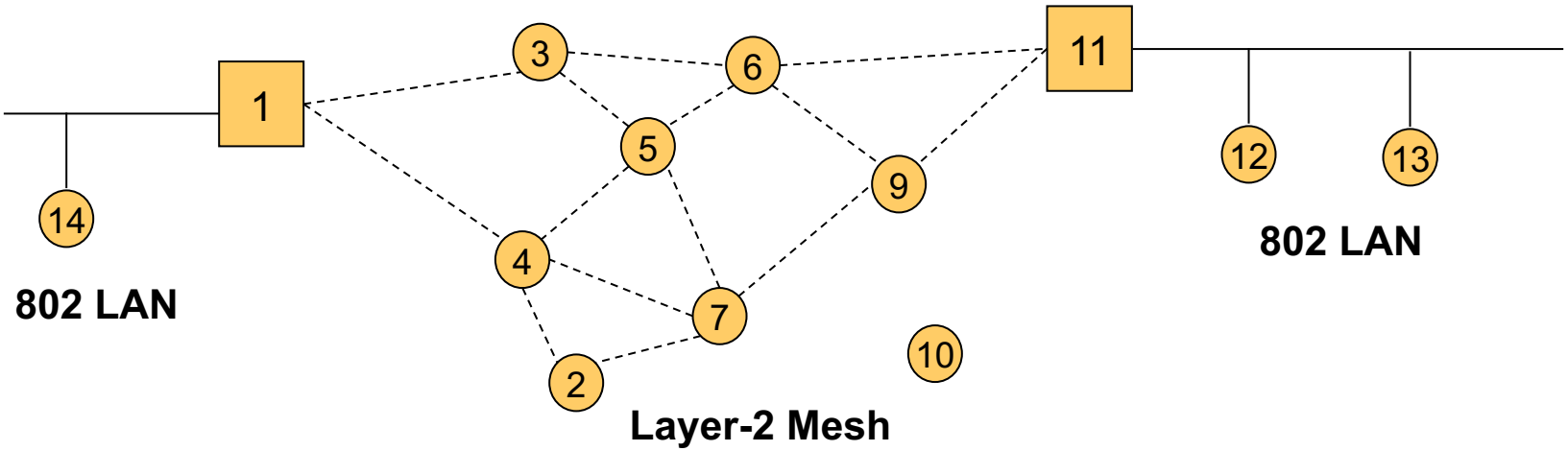
Description	To DS	From DS	Addr Exten	Addr 1	Addr 2	Addr 3	Addr 4	Addr 5	Addr 6
Mesh Data Unicast	1	1	—	RA	TA	DA = Mesh DA	SA = Mesh SA	Omit	Omit
Proxied Mesh Data Unicast	1	1	Addr 5&6	RA	TA	Mesh DA	Mesh SA	DA	SA
Mesh Data Multicast	0	1	—	RA = DA	TA	SA = Mesh SA	Omit	Omit	Omit
Proxied Mesh Data Multicast	0	1	Addr 4	RA = DA	TA	Mesh SA	SA	Omit	Omit

Wi-Fi Mesh



- Mesh looks like a link.
- For data just from 3 to 6
  - SA = Mesh SA = TA = 3, DA = Mesh DA = RA = 6
- For data from 4 to 10
  - SA = Mesh SA = TA = 4, RA = 7, DA = Mesh DA = 10, then
  - SA = Mesh SA = 4, TA = 7, DA = Mesh DA = RA = 10

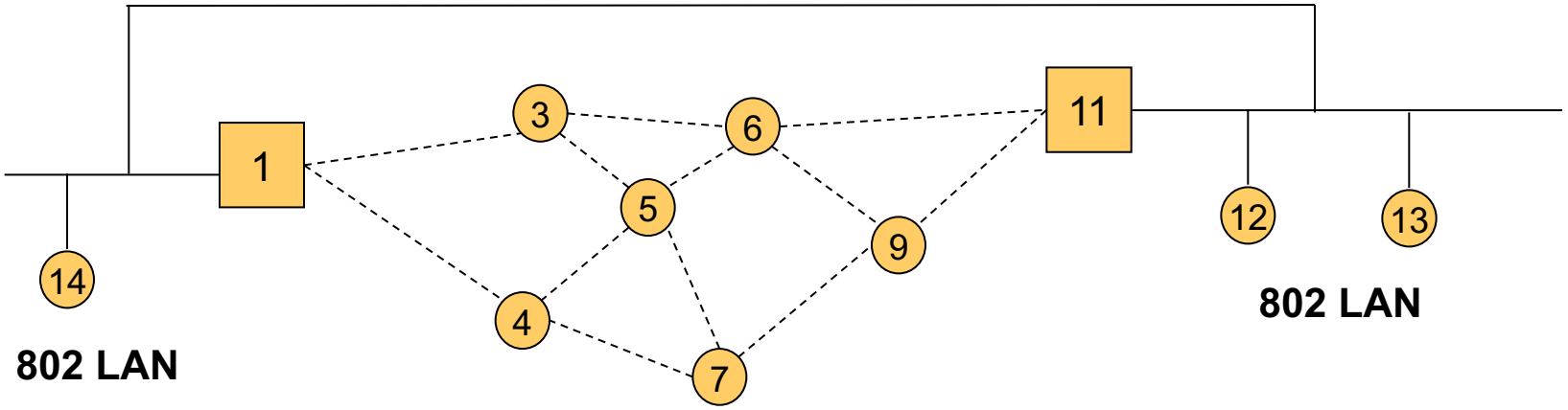
Wi-Fi Mesh



- Data from 14 to 4 (14 to 1 by Ethernet, proxied)
  - SA = 14, Mesh SA = TA = 1, DA = Mesh DA = RA = 4
- Data from 14 to 12 (14 to 1 & 11 to 12 by Ethernet, proxied)
  - SA = 14, Mesh SA = TA = 1, RA = 3, Mesh DA = 11, DA = 12, then
  - SA = 14, Mesh SA = 1, TA = 3, RA = 6, Mesh DA = 11, DA = 12, then
  - SA = 14, Mesh SA = 1, TA = 6, Mesh DA = RA = 11, DA = 12

Wi-Fi Mesh

- Loop prevention inside the mesh is the meshes problem, depends on duplicate discard.
- From outside, the mesh is simply a Layer 2 link. If part of a larger Layer 2 network, loops are broken by spanning tree or the like.
- Beyond IP routers, it is the IP routing algorithm's problem.



END

Donald E. Eastlake 3rd (Futurewei)

d3e3e3@gmail.com