Naming and addressing:

Naming and addressing are two fundamental issues in networking. Names are used to denote things (nodes, data, transactions) where as addresses supply information to find these things.

Fundamental use of addresses and names in (sensor) networks

In sensor networks the following types of names, addresses, and identifiers can be found.

→ Unique node identifier (UID): It is a persistent data item unique for every node. UID may or may not have any function in protocol stack.

→ MAC address: MAC address helps in distinguishing bet? one hop neighbors of a node and is used for contentionbased MAC protocols. It decides which packets not destined to a node and allow the node to enter sleep mode. This facilitates overhearing avoidance and conserves energy at MAC layer

→ Network address: Network address is used to find and denote a node over multiple hops and hence n/w addresses are often connected to routing.

→ Network identifiers: Networks operating in same frequency band or geographically overlaping area distinguished from each other by the help of n/w identifiers.

→ Resource identifiers:- It provided the user some information that "means something" to user. For example www.xemacs.org gives user an information about web browser

Address management tasks.

The fundamental tasks of addres management which are independent of type of addresses are:

(i) Address allocation: It provides address assignment to an entity from an address pool.

(ii) Address deallocation: The address space for on demand addressing is small in size. In WSN nodes may die, leave from the n/w, hence their addresses need to put into address pool for reuse, else the address pool will be exhausted and no addresses could be allocated to

new nodes. The address deallocation can be (graceful or abrupt.)
In graceful deallocation. the node sends out control packets to give up its address.
In abrupt deallocation, the node disappears or crashes and doesn't send appropriate control packets and in this case the ~~node~~ network takes the responsibility to detect and deallocate the node's address to the n/wk.

(iii) Address representation (Address formating): Here a format for representing address need to be negotiated and also implemented. (format is variable)

(iv) ~~Address~~ conflict detection/resolution: In distributed assignment and on-demand processing network faces address conflicts. These conflicts need to be resolved.

(v) Binding (Address mapping): If many addressing layers used, then mapping between different layers to be provided. Example: The IP in IP n/works the IP address has to be mapped to MAC address through Address resolution protocol (ARP).

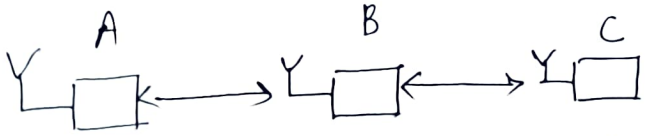
Uniqueness of addresses:
Uniqueness of network names and addresses are defined as:

(i) Globally unique: This type of address or identifier occur in world. Ex: A 48-bit IEEE MAC addresses used in Ethernet and Token Ring networks The binary representation of such address must be large enough to accomodate all devices worldwide.

(ii) Network unique: This type address is unique with in a given network, but the same address can be used in different networks. In general for networks A and B, there is no pair of nodes $a \in A$ and $b \in B$ that can communicate

(iii) Locally unique: this address might occur several times in the same network but need to be unique within a neighborhood. Hence, these addresses are unique only to the neighborhood of a node.

for example



→ for MAC addresses it is required that they are unique within a two hop neighborhood. If A and C have same MAC addresses, B is unable to infer the transmitter of incoming packet, also B is unable to send packet to unique intended receiver.

→ Also considering a WSN with diff sensors such as temp, humidity moisture sensors. It is required that no two temperature sensors have same address but a temperature and humidity sensor may.

Address allocation and assignment: A priori / on demand → Centralized (one node take care of address pool) / Decentralized (Any node take care of address pool)

→ Address assignment can happen a priori (before n/w deployment) or on demand with the help of address assignment Protocol.

→ The on demand assignment can be centralized or distributed. For centralized, one node takes care of address pool i.e a fusion center(FC). Whereas in distributed there is no specific node, i.e all nodes play same role in address assignment. Hence, for on demand type addressing, address deallocation is essential to have network wide or locally unique addresses.

Distributed address assignment → Strong DAD / Weak DAD

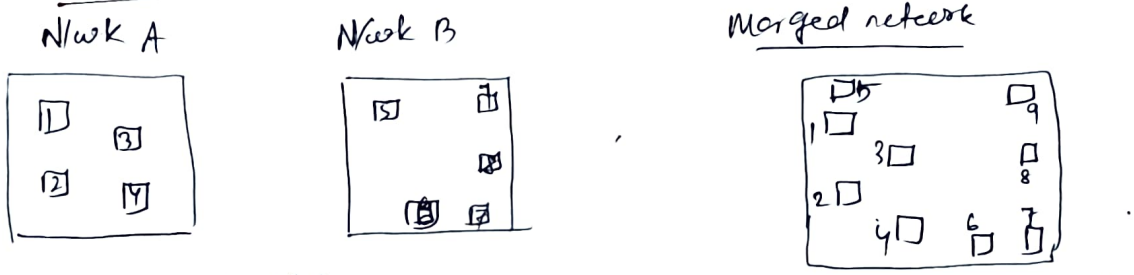
→ The distributed address assignment may not guarantee a network wide uniqueness all time. Hence few address conflicts can be detected or resolved through Duplicate Address Detection (DAD):

DAD is two types: Strong DAD & Weak DAD.

Strong DAD: If address x is assigned to node A and B at times t_0 and t_1 respectively, then this duplicate assignment must be detected latest at time t_1+T where T is the fixed time bound.

Weak DAD: Here duplicate addresses are tolerated as long as they don't distort ongoing sessions. For example after merging two networks A & B and addressing both networks with address x. Here no

action need to be taken as long as all packets from nodes of previous n/wk A destined to x reach the node in A with address x and not the node with same address in other network.



Let 1,2,3,4, 5,6,7,8,9 have same address x, the packet destined to node 1 of previous n/wk A must not delivered to node 9 in merged n/wk.

x centralized possible don't scale with sensor n/works. The DHCP protocol needs to renew node address periodically to detect abrupt deallocations.

Addressing overhead → dependent on frequency size

The addressing require the number of bits needed for their representation this is called as overhead. The overhead and energy required for transmitting addressing information related to two factors (i) The freq. with which addresses are used, ii) size of their representation.

→ In some MAC Protocol like TRAMA or SMACS where links bet? neighboring nodes are established through conflict-free time slots or frequencies. If these links are used for data packet, then there is no requirement to carry address information in these packets. (scheduled based) (no requirement to carry address information with data packets)

→ However, in contention based MAC Protocols there is always a conflict bet? transmitting nodes and addressing information is vital to identify source and destination and to achieve overhearing avoidance. Fewer bits spent per address, it better. Some trade-offare.

→ For globally unique address IEEE 802.3/ Ethernet, 48 bits are used to accomodate current and anticipated number of devices. A priori

→ N/wk wide unique address have sufficient no. of bits to accomodate all nodes in the n/wk. In sensor n/wk with 10000 nodes, addresses of 14 bit suffices. However, to minimize the no. of address bits, the size of n/wk must be known in advance. assignment remove requirement of address assignment protocol.

→ A locally unique address must be unique within a certain neighborhood, which is typically smaller than the entire network.

* For example MAC address should be unique within a two hop neighborhood which consist of dozen of nodes depending on node density. Due to less knowledge about exact topology address assignment protocol needed.

Distributed assignment of locally unique addresses: (addresses are not directly fixed, rather encoded & fixed as code words.

In this protocol nodes are assigned with locally unique MAC addresses. Using this localized protocol node communicate only with immediate neighbors.

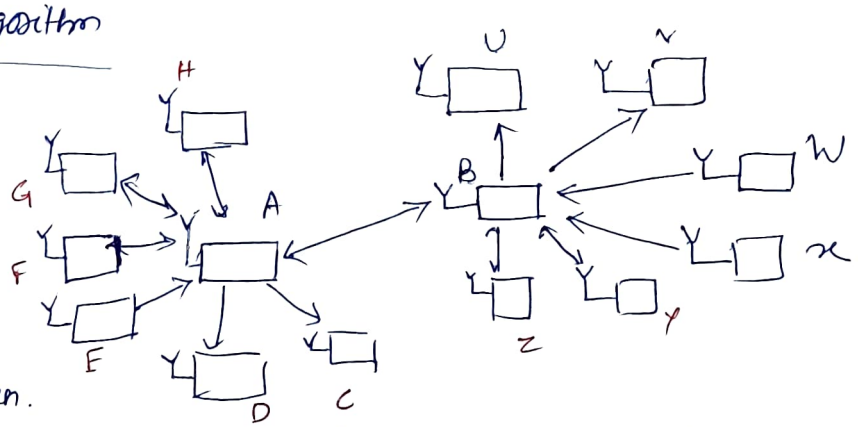
→ (If the neighborhood is made small), (fewer bits are needed) for address representation than network wide or globally unique address.

→ The locally unique addresses, can be reused several times in the overall n/work. The address reuse uses greediness by allocating a node with that address with numerically lowest non allocated address.

→ With this approach lower addresses are used often than higher addresses. Therefore, addresses are not directly transmitted rather by encoding them according to Huffman coding for transmitting code words. The mapping of addresses to codes is called codebook.

→ In Huffman coding short codes are assigned with frequent addresses and longer codes are assigned with less frequent ones.

Address assignment algorithm



→ In this scenario the assumption is each node has knowledge of bidirectional and inbound neighbors from previous run.

→ Inbound neighbors of A are the neighbor whose transmission is heared by A but not vice versa. Outbound neighbor of node A is the node that receives A's information but not vice versa. Considering this situation, the addresses to node A and B is assigned. The requirements are:

(i) Node A and B are assigned different addresses.

(ii) Address of node A is different from the inbound neighbor nodes of B as these nodes direct packets to B.

(iii) Similarly B's address must be different from inbound neighbors of A.

(iv) Whether node B have different address to the neighbors of A that receive data from A. If these addresses are same then all packets from node A destined to node B is also received by C. If another constraint that nodes B accepts packet from bidirectional neighbors. there it's address shouldn't be different than B. Similarly, A and B can also have same address as w and x. Hence, w & x need not have different address as far as B is connected.

In this requirement node A all bidirectional neighbors have distinct addresses. Also the address of any inbound neighbor must be different from the address of all bidirectional neighbors.

Content-based and geographic addressing

Content-based and geographic addressing: (4.)

Traditional n/works (Independent users)
WSN (dependent nodes)

In traditional fixed and adhoc n/wks it offers services and protocols which allows a number of independent users to exchange data among each other and with the remaining world. However, in WSNs the nodes interact with physical environment and they also collaborate (i.e they are not independent of each other). In overall sense the user of WSN ultimately wants to know about physical environment to which the n/wk interacts but don't care about the sensor nodes.

→ In traditional IP based n/wks, this requirement corresponds to introducing a naming system on top of IP addresses and to introducing appropriate binding services or other directory services providing mapping from names (meaningful to user) to IP addresses (meaningful for the routing Protocol) In WSN these levels of indirection can be eliminated and user specified (attributes) can be directly used to find (group of) nodes. This is referred as data centric addressing. This approach to make the application data meaningful to the operation of n/wk Protocols is also a key enable for in-network processing techniques.

→ Geographic addressing is considered as a special case of content-based addressing. Here, some user specific attributes refer to special coordinates. Geographic addressing assumes that each node knows its own location w.r.t some agreed coordinate system. Therefore locationing techniques are essential for working with geographic addresses. Geographic ~~routing~~ addresses can also help with routing. For example, in directed diffusion Protocol, location information help to make the flooding propagation step directional and reduce the number of interest packets significantly.

Content based addressing:

In a low-level naming mechanism, content based addressing is integrated with directed diffusion routing. In directed diffusion a sink node issues an interest message by specifying attributes for desired data. This message passed in n/wk. The nodes that can produce sensor data matching the interest are

are called source nodes. The data packet generated by source node travels through intermediate nodes to sink. The intermediate node stores the interest along with a (set of) possible upstream neighbors in the interest cache.

After receiving a data packet, intermediate node searches its cathe for an interest matching the data and forwards the packet to the associated upstream neighbor.

→ Both interests and data packets are represented as lists of Attribute value operation (AVO) tuples. The set of attributes is predefined and each attribute possesses a unique well known key as well as an understanding of the data type for corresponding value. The IS operator specifies that corresponding attribute actually has the indicated value & is generated by data source. IS is also called an actual operator. All other operators are called formal operators and are used to specify the interests against which the actual values generated by the source are matched.

Operator	meaning
EQ	matches if actual value is equal to value
NE	" " not " "
IS	specifies a literal attribute.
LT	matches if actual value is smaller than value
GT	" " greater "
LE	" " smaller or equal "
GE	" " larger or equal "
EQ-ANY	" anything, value is meaningless

Ex: If user at sink node wants to know when temp. of certain geographic area exceeds a certain threshold. The user combines several attributes to an interest message. Here attribute type specifies kind of sensor to which the interest is directed (temperature sensor let). The next attribute threshold-from-below specifies the sink is interested in cases where threshold of 20°C is crossed from below. The area under observation is square bet. (0,0) and (20,20). If temp. exceeds this threshold a matching sensor report this event 0.05 s for a duration of 10 s.

The formal attribut class expresses the the AVO tuple is an interest and not a data, message.
Let we have different type of sensor including temp. sensors (interest). Each sensor has set of AVO tuples. If the interest message reaches the temp. sensor and one-way check reveals that self description of sensor matches with the attributes of the interest, then the sensor start to observe the environment and generate data messages when the event of interest occurs. This is an example of data message. The nonmatching sensors store the interest in their interest cache.

Interest message

<type, temperature, EQ>
<threshold-from-below, 20, IS>
<X-coordinate, 20, LE>
<X-coordinate, 0, GE>
<Y-coordinate, 20, GE>
<Y-coordinate, 0, GE>
<interval, 0.05, IS>
<duration, 10, IS>
<class, interest, IS>

Temperature sensor

<type, temperature, IS>
<X-coordinate, 10, IS>
<Y-coordinate, 10, IS>

Data message

<type, temperature, IS>
<X-coordinate, 10, IS>
<Y-coordinate, 10, IS>
<temperature, 20.01, IS>
<class, data, IS>

Geographic addressing

It is easy for users to express queries to sensor n/ws not only in terms of type and modality of data but also the region or location from where the data should originate. Unlike content-based address where users separately specify each node belonging to region of interest geographic addressing prefers to specify a region and allow the n/wk to find out which sensors are appropriate. Furthermore, geographic routing schemes can be used if the sensor node location is known. Different ways to specify a region are

- → Specify a single point.
- → Specify a circle or sphere with centre & radious
- → Specify a rectangle or a parallelpiped by giving 2 or 3 corner points.
- → Specify a polygon (2D) or polytype (3D) by giving a list of points.