Course Takeaways IPV6

1. IoT network characteristics and specificities

The Internet of Things (IoT) differs from conventional computer networks by several specific characteristics and constraints, notably due to the limited resources of connected objects and the wireless nature of the network.

- **Scalability**: IoT networks need to scale up to accommodate many inexpensive smart objects or things that interact with the physical world.
- **Constrained Nodes**:
  - Memory and Processing Constraints: Limited ROM/Flash and RAM, limited processing power.
  - Energy Constraints: Devices may be event energy-limited, period energy-limited, lifetime energy-limited, or have no limitations.
  - Physical Constraints: Size, cost, and user interface/accessibility constraints.

- **Constrained Networks**:
  - Production and Operational Costs: Efforts to reduce costs impact network design.
  - Physical Constraints: Environmental constraints, media constraints (e.g., underwater operation), and regulatory constraints (e.g., limited spectrum availability).
  - Technological Constraints: Older and lower-speed technologies may still be in use.
- **Can Conventional Computer Networks be Used as IoT Networks?**
  - Assumptions of Conventional Networks:
    - Hosts are always on, have decent resources, one interface, and no mobility.
    - Physical networks are deployed in software environments with decent frame size, high throughput, low packet loss, symmetric communications, and decent RTT.
  - IoT Networks:
    - IoT networks are low-power and lossy networks (LLNs) with nodes that have tight limits on power, energy, memory, and processing resources.
    - Links are typically wireless and exhibit considerable loss at the physical layer, with significant variability in delivery rate and short-term unreliability.
- **Node Constraints and Network Design**:
  - Energy Perspective:
    - Communications consume a significant portion of a device's total energy, influenced by transmission duration, reception time, and waiting time for reception.

        - Energy constraints impact low-layer protocols and higher-layer protocols should also be energy-friendly.
    - Resource Perspective:
        - Severely constrained nodes may outsource functions to a network gateway.
        - Constrained nodes can use a protocol stack designed for constrained environments (e.g., CoAP over UDP).
        - Less constrained nodes can support a full conventional protocol stack but benefit from lightweight and energy-efficient protocols.
- **Communication Patterns in IoT Applications**:
    - Device-to-Device Communication: Typically involves devices from the same vendor.
    - Device-to-Cloud Communication: Involves application service providers and smart objects from the same vendor.
    - Device-to-Gateway Communication: Gateways allow the use of less-widely-used radio technologies and provide application-level functionality.
- **IoT Trends**:
    - Decreasing Size and Power Needs: IoT objects are becoming smaller and more power efficient.
    - Increasing Processing and Communication Capabilities: IoT objects can now perform processing and off-load tasks to more resourceful devices (e.g., edge, fog, cloud).
    - Standardization of Communication Technologies: There is a move towards infrastructure-based wireless technologies.

IoT networks are fundamentally different from traditional networks because they must operate with limited resources, in constrained environments, while minimizing energy consumption. This particularity translates into lightweight protocols, intermittent connectivity, and the use of low-throughput but high-energy-efficiency technologies such as LP-WPANs.

2. Rationale for adopting an IPv6 based architecture to support the communications of an IoT system or use case

- **Scalability:**
    - The vast address space (128 bits) of IPv6 supports the large number of devices in IoT networks, ensuring that each device can have a unique address.
- **Auto-Configuration:**
    - IPv6's auto-configuration capabilities simplify network setup and management, reducing the need for manual configuration and enabling devices to join the network seamlessly.
- **Efficient Neighbor Discovery:**

    - The Neighbor Discovery Protocol (NDP) in IPv6 replaces ARP and provides mechanisms for address resolution, duplicate address detection, and router discovery.
- **Better Support for Mobility:**
    - IPv6's mobility features allow IoT devices to move across different networks without losing connectivity, which is essential for mobile IoT applications.
- **Future-Proofing:**
    - Adopting IPv6 ensures that IoT networks are prepared for future growth and technological advancements, avoiding the limitations of IPv4 address exhaustion.

Example:

IPv4 Address:

- Address: 143.95.2.219
- Netmask: 0xfffff800
- Broadcast: 143.95.7.255

IPv6 Address:

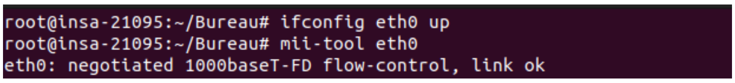
- Link-Local Address: fe80::ca2a:14ff:fe30:4940%en0
    - Prefix Length: 64
    - Scope ID: 0x8
- Global Unicast Address: 2001:667:6672:4:ca2a:14ff:fe30:4940
    - Prefix Length: 64

3. IPv6 basics

1) IPv6 Initialization Steps

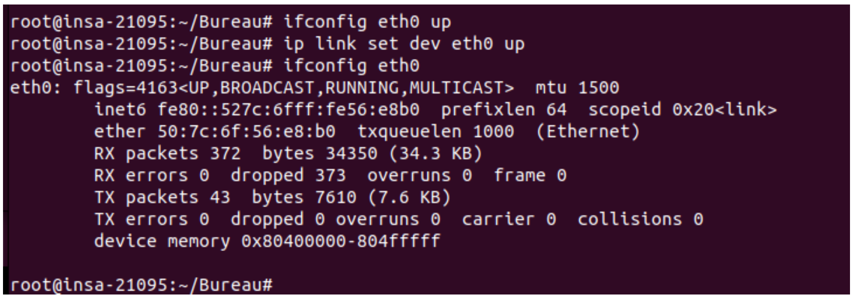
From the experiments and traffic captures during TD1, the following steps outline the IPv6 initialization process that a host goes through when switched on:

1. **Interface Activation:**
    - Command: **ifconfig eth0** up or ip link set dev eth0 up



```
root@insa-21095:~/Bureau# ifconfig eth0 up
root@insa-21095:~/Bureau# mii-tool eth0
eth0: negotiated 1000baseT-FD flow-control, link ok
```

    - Description: The network interface eth0 is activated.
2. **Auto-Configuration of Link-Local Address:**
    - Command: **ifconfig eth0** or **ip -6 addr ls dev eth0**

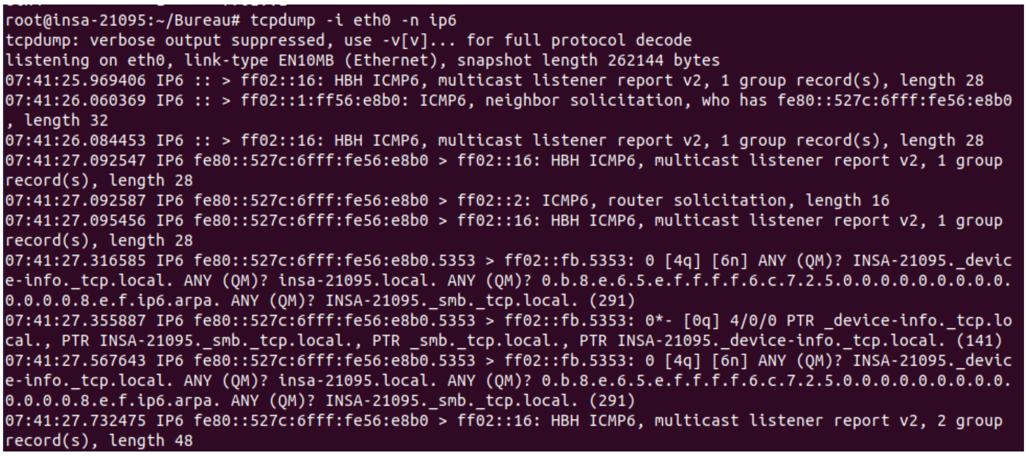


```
root@insa-21095:~/Bureau# ifconfig eth0 up
root@insa-21095:~/Bureau# ip link set dev eth0 up
root@insa-21095:~/Bureau# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::527c:6fff:fe56:e8b0  prefixlen 64  scopeid 0x20<link>
        ether 50:7c:6f:56:e8:b0  txqueuelen 1000  (Ethernet)
        RX packets 372  bytes 34350 (34.3 KB)
        RX errors 0  dropped 373  overruns 0  frame 0
        TX packets 43  bytes 7610 (7.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x80400000-804fffff

root@insa-21095:~/Bureau#
```

- Description: The interface eth0 is automatically assigned a link-local IPv6 address (fe80::527c:6fff:fe56:e8b0). This address is used for communication within the local network segment and is derived based on the interface's MAC address.

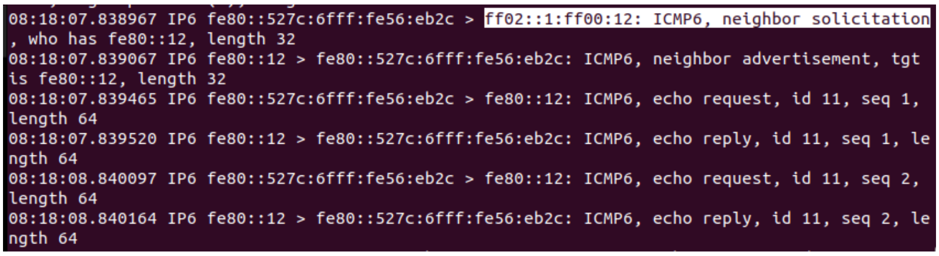
3. **Neighbor Discovery Protocol (NDP):**
   - **Router Solicitation (RS):**
     - Command: **tcpdump -i eth0 -n ip6**



```
root@insa-21095:~/Bureau# tcpdump -i eth0 -n ip6
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:41:25.969406 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
07:41:26.060369 IP6 :: > ff02::1:ff56:e8b0: ICMP6, neighbor solicitation, who has fe80::527c:6fff:fe56:e8b0
, length 32
07:41:26.084453 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
07:41:27.092547 IP6 fe80::527c:6fff:fe56:e8b0 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
07:41:27.092587 IP6 fe80::527c:6fff:fe56:e8b0 > ff02::2: ICMP6, router solicitation, length 16
07:41:27.095456 IP6 fe80::527c:6fff:fe56:e8b0 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
07:41:27.316585 IP6 fe80::527c:6fff:fe56:e8b0.5353 > ff02::fb.5353: 0 [4q] [6n] ANY (QM)? INSA-21095._devic
e-info._tcp.local. ANY (QM)? insa-21095.local. ANY (QM)? 0.b.8.e.6.5.e.f.f.f.f.6.c.7.2.5.0.0.0.0.0.0.0.0.0.
0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? INSA-21095._smb._tcp.local. (291)
07:41:27.355887 IP6 fe80::527c:6fff:fe56:e8b0.5353 > ff02::fb.5353: 0*- [0q] 4/0/0 PTR _device-info._tcp.lo
cal., PTR INSA-21095._smb._tcp.local., PTR _smb._tcp.local., PTR INSA-21095._device-info._tcp.local. (141)
07:41:27.567643 IP6 fe80::527c:6fff:fe56:e8b0.5353 > ff02::fb.5353: 0 [4q] [6n] ANY (QM)? INSA-21095._devic
e-info._tcp.local. ANY (QM)? insa-21095.local. ANY (QM)? 0.b.8.e.6.5.e.f.f.f.f.6.c.7.2.5.0.0.0.0.0.0.0.0.0.
0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? INSA-21095._smb._tcp.local. (291)
07:41:27.732475 IP6 fe80::527c:6fff:fe56:e8b0 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group
record(s), length 48
```

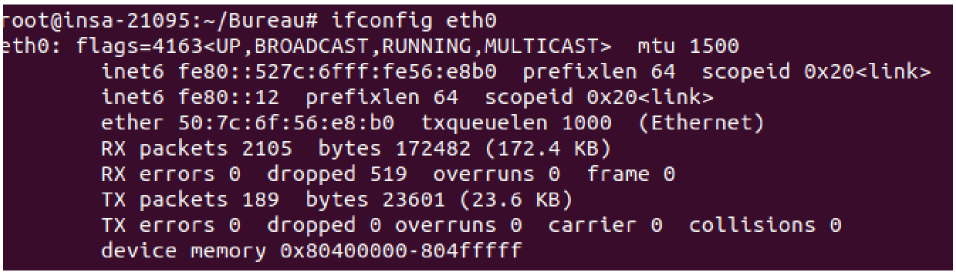
     - Description: We used tool tcpdump to capture and analyze the ICMPv6 messages exchanged between the router and the end-hosts. These messages indicate the neighbor solicitation and router solicitation processes, for the auto-configuration of unicast global IPv6 addresses. The neighbor solicitation message is used to discover the link-layer address of a neighbor or to verify that a neighbor is still reachable.
       The router solicitation message is sent by an end-host to request a router advertisement from a local router, which contains the necessary information for the end-host to configure its global IPv6 address.

   - **Router Advertisement (RA):**
     - Description: Routers respond with Router Advertisement messages containing network configuration information, such as the network prefix and default gateway.
   - **Duplicate Address Detection (DAD):**
     - Description: The host performs DAD to ensure the uniqueness of its IPv6 address by sending Neighbor Solicitation messages to the multicast address ff02::1:ff00:12.



```
08:18:07.838967 IP6 fe80::527c:6fff:fe56:eb2c > ff02::1:ff00:12: ICMP6, neighbor solicitation
, who has fe80::12, length 32
08:18:07.839067 IP6 fe80::12 > fe80::527c:6fff:fe56:eb2c: ICMP6, neighbor advertisement, tgt
is fe80::12, length 32
08:18:07.839465 IP6 fe80::527c:6fff:fe56:eb2c > fe80::12: ICMP6, echo request, id 11, seq 1,
length 64
08:18:07.839520 IP6 fe80::12 > fe80::527c:6fff:fe56:eb2c: ICMP6, echo reply, id 11, seq 1, le
ngth 64
08:18:08.840097 IP6 fe80::527c:6fff:fe56:eb2c > fe80::12: ICMP6, echo request, id 11, seq 2,
length 64
08:18:08.840164 IP6 fe80::12 > fe80::527c:6fff:fe56:eb2c: ICMP6, echo reply, id 11, seq 2, le
ngth 64
```

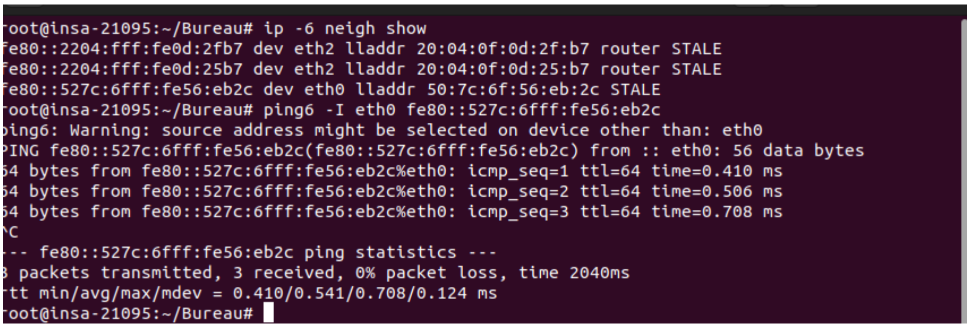
4. **Global Unicast Address Configuration:**
   - Command: **ifconfig eth0**



```
root@insa-21095:~/Bureau# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::527c:6fff:fe56:e8b0  prefixlen 64  scopeid 0x20<link>
        inet6 fe80::12  prefixlen 64  scopeid 0x20<link>
        ether 50:7c:6f:56:e8:b0  txqueuelen 1000  (Ethernet)
        RX packets 2105  bytes 172482 (172.4 KB)
        RX errors 0  dropped 519  overruns 0  frame 0
        TX packets 189  bytes 23601 (23.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x80400000-804fffff
```

   - Description: The host is assigned a global unicast address (fe80::12) based on the network prefix received from the Router Advertisement.

5. **Verification:**
   - Command: **ip -6 addr ls dev eth0 or ifconfig eth0**
   - Description: Verify the assigned IPv6 addresses and their types (link-local, global unicast).



```
oot@insa-21095:~/Bureau# ip -6 neigh show
e80::2204:fff:fe0d:2fb7 dev eth2 lladdr 20:04:0f:0d:2f:b7 router STALE
e80::2204:fff:fe0d:25b7 dev eth2 lladdr 20:04:0f:0d:25:b7 router STALE
e80::527c:6fff:fe56:eb2c dev eth0 lladdr 50:7c:6f:56:eb:2c STALE
oot@insa-21095:~/Bureau# ping6 -I eth0 fe80::527c:6fff:fe56:eb2c
ing6: Warning: source address might be selected on device other than: eth0
ING fe80::527c:6fff:fe56:eb2c(fe80::527c:6fff:fe56:eb2c) from :: eth0: 56 data bytes
4 bytes from fe80::527c:6fff:fe56:eb2c%eth0: icmp_seq=1 ttl=64 time=0.410 ms
4 bytes from fe80::527c:6fff:fe56:eb2c%eth0: icmp_seq=2 ttl=64 time=0.506 ms
4 bytes from fe80::527c:6fff:fe56:eb2c%eth0: icmp_seq=3 ttl=64 time=0.708 ms
C
-- fe80::527c:6fff:fe56:eb2c ping statistics ---
 packets transmitted, 3 received, 0% packet loss, time 2040ms
tt min/avg/max/mdev = 0.410/0.541/0.708/0.124 ms
oot@insa-21095:~/Bureau#
```

Transmission Capabilities:

- **Minimum MTU**: IPv6 requires a minimum MTU of 1280 bytes to ensure efficient packet transmission across various network links.
- **Multicast Support**: IPv6 extensively uses multicast addresses for Neighbour Discovery, reducing the need for broadcast traffic.

Host Availability:

- **Always On Connectivity:** Devices that are always on can maintain continuous network connectivity without the need for frequent reattachment.
- **Low Power Devices:** Devices that operate on limited power may need to optimize their communication patterns to conserve energy, such as using sleep modes and minimizing transmission durations.

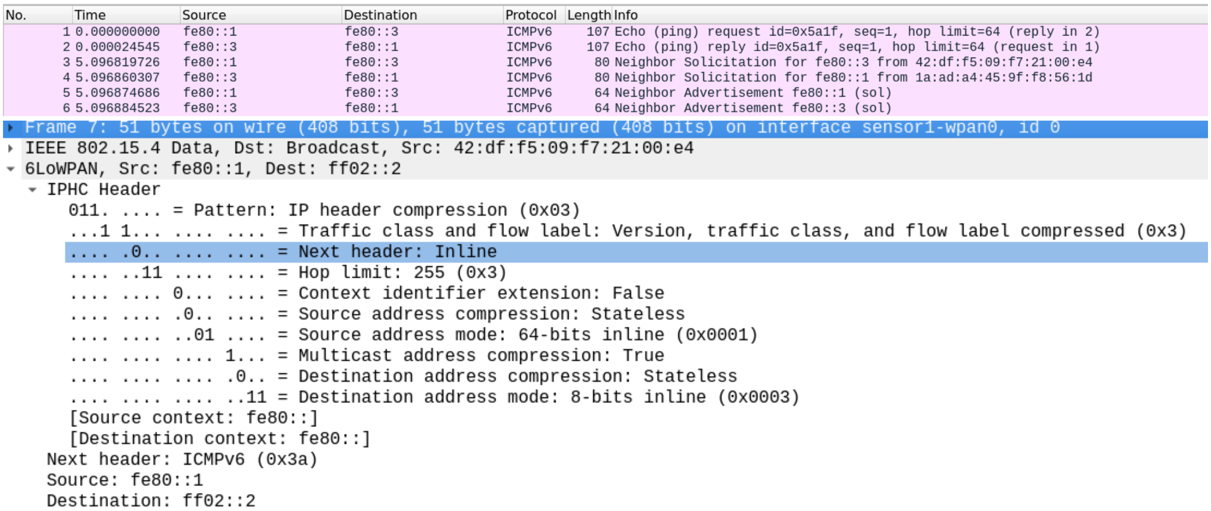
Important Characteristics of IPv6:

- **Large Address Space:** IPv6 provides a vast address space, allowing for unique addresses for a large number of IoT devices.
- **Security:** IPv6 includes built-in support for IPsec, providing end-to-end security for communications.

4. IPv6 adaptation and extensions in order to enable its use atop a physical IoT network

Based on the experiments conducted during TD2, the following are the main additions, adjustments, and optimizations of IPv6 that were defined for application in the context of an IoT network:

- **6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks):**
  - **Header Compression:**
    - **Objective:** Reduce the size of IPv6 headers to fit the limited frame size of low-power wireless networks.
    - **Mechanism:** Compresses IPv6 headers by eliminating redundant information and using shorter representations for addresses.
    - **Example:** Compressing the 51-byte IPv6 header to a much smaller size by removing the network prefix and using link-local addresses.
  - **Benefits:** Efficient use of bandwidth, reduced transmission time, and lower energy consumption.



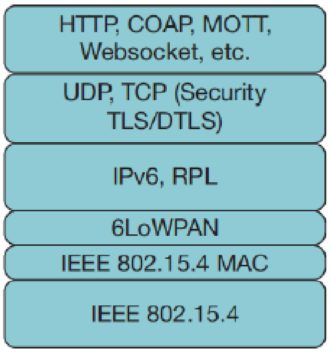
```
No.   Time          Source     Destination  Protocol  Length Info
    1 0.000000000   fe80::1    fe80::3      ICMPv6     107 Echo (ping) request id=0x5a1f, seq=1, hop limit=64 (reply in 2)
    2 0.000024545   fe80::3    fe80::1      ICMPv6     107 Echo (ping) reply id=0x5a1f, seq=1, hop limit=64 (request in 1)
    3 5.096819726   fe80::1    fe80::3      ICMPv6      80 Neighbor Solicitation for fe80::3 from 42:df:f5:09:f7:21:00:e4
    4 5.096860307   fe80::3    fe80::1      ICMPv6      80 Neighbor Solicitation for fe80::1 from 1a:ad:a4:45:9f:f8:56:1d
    5 5.096874686   fe80::1    fe80::3      ICMPv6      64 Neighbor Advertisement fe80::1 (sol)
    6 5.096884523   fe80::3    fe80::1      ICMPv6      64 Neighbor Advertisement fe80::3 (sol)

▸ Frame 7: 51 bytes on wire (408 bits), 51 bytes captured (408 bits) on interface sensor1-wpan0, id 0
▸ IEEE 802.15.4 Data, Dst: Broadcast, Src: 42:df:f5:09:f7:21:00:e4
▾ 6LoWPAN, Src: fe80::1, Dest: ff02::2
  ▾ IPHC Header
      011. .... = Pattern: IP header compression (0x03)
      ...1 1... .... .... = Traffic class and flow label: Version, traffic class, and flow label compressed (0x3)
      .... .0.. .... .... = Next header: Inline
      .... ..11 .... .... = Hop limit: 255 (0x3)
      .... .... 0... .... = Context identifier extension: False
      .... .... .0.. .... = Source address compression: Stateless
      .... .... ..01 .... = Source address mode: 64-bits inline (0x0001)
      .... .... .... 1... = Multicast address compression: True
      .... .... .... .0.. = Destination address compression: Stateless
      .... .... .... ..11 = Destination address mode: 8-bits inline (0x0003)
      [Source context: fe80::]
      [Destination context: fe80::]
    Next header: ICMPv6 (0x3a)
    Source: fe80::1
    Destination: ff02::2
```

- **RPL (Routing Protocol for Low-Power and Lossy Networks):**
  - **Objective:** Provide efficient routing in networks with constrained nodes and lossy links.
  - **Mechanism:** Constructs a Destination-Oriented Directed Acyclic Graph (DODAG) for routing, optimizing for energy efficiency and reliability.

5. The IETF IPv6 based stack for IoT

The IETF has promoted a network architecture for low-power multi-hop wireless IoT networks that integrates standards and protocols to address the unique requirements of IoT. This architecture is applicable to major IoT network technologies, including BLE, BacNet, Z-Wave, PLC, NB-IoT, LoRaWAN, DECT, and Visible Light Communications.


HTTP, COAP, MOTT, Websocket, etc.
UDP, TCP (Security TLS/DTLS)
IPv6, RPL
6LoWPAN
IEEE 802.15.4 MAC
IEEE 802.15.4

Protocol Stack

- **Physical and MAC Layer: IEEE 802.15.4**
    - **Function:** Defines the physical and media access control (MAC) layers for low-rate wireless personal area networks (LR-WPANs).
- **Adaptation Layer: 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)**
    - **Function:** Adapts IPv6 packets to be transmitted over IEEE 802.15.4 networks by compressing headers and fragmenting packets.
- **Routing Layer: RPL (Routing Protocol for Low-Power and Lossy Networks)**
    - **Function:** Provides efficient routing in networks with constrained nodes and lossy links.
- **Network Layer: IPv6**
    - **Function:** Provides addressing and routing for devices in the network.
- **Transport Layer: UDP (User Datagram Protocol) and TCP (Transmission Control Protocol)**
    - **Function:** Provides transport services for data transmission.
        - **UDP:** Connectionless protocol with minimal overhead, suitable for applications that can tolerate some packet loss.
        - **TCP:** Connection-oriented protocol providing reliable data transmission.
- **Security: TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security)**
    - **Function:** Ensures secure communication between devices.
        - **TLS:** Provides security for TCP connections.
        - **DTLS:** Provides security for UDP connections.
- **Application Layer: CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), HTTP, WebSocket**
    - **Function:** Facilitates communication between IoT devices and applications.
        - **CoAP:** Lightweight protocol designed for constrained environments, enabling RESTful communication similar to HTTP.
        - **MQTT:** Lightweight messaging protocol for small sensors and mobile devices, optimized for low-bandwidth, high-latency, or unreliable networks.
        - **HTTP:** Standard protocol for web communication.
        - **WebSocket:** Provides full-duplex communication channels over a single TCP connection.

6. Existing IPv6 based network technologies for IoT

- **6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)**
  - Application: Home automation, Industrial monitoring
- **Zigbee IP**
  - Application: Smart energy, home automation
- **Thread**
  - Application: Home automation, Lighting systems
- **LoRaWAN (Long Range Wide Area Network)**
  - Application: Smart cities, Industrial IoT
- **BLE (Bluetooth Low Energy)**
  - Application: Health care, home automation

7. Is an IPv6 based stack relevant for your semester project ?

Adopting an IPv6 based stack is relevant for the project, which aims to develop a solution for detecting water leaks in a house. IPv6 provides a vast address space, allowing for unique identification of each sensor in the distributed network, essential for scaling from household leaks to public water infrastructures. Its auto-configuration capabilities simplify the deployment of numerous sensors, while RPL ensures efficient and reliable routing in low-power and lossy environments. Additionally, IPv6's built-in security features enhance data protection, and its energy-efficient protocols prolong sensor battery life. Overall, IPv6 supports the project's need for scalable, secure, and efficient communication in an IoT context.