Introduction to IoT - 2

Dr. Sudip Misra
Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

IoT Resulting in Address Crunch

- ✓ Estimated 20-50 billion devices by 2018
- ✓ Reason is the integration of existing devices, smart devices as well as constrained nodes in a singular framework.
- ✓ Integration of various connectivity features such as cellular, Wi-Fi, ethernet with upcoming ones such as Bluetooth Low Energy (BLE), DASH7, Insteon, IEEE 802.15.4, etc.
- ✓ The ITU vision is approaching reality as the present day networked devices have outnumbered humans on earth.

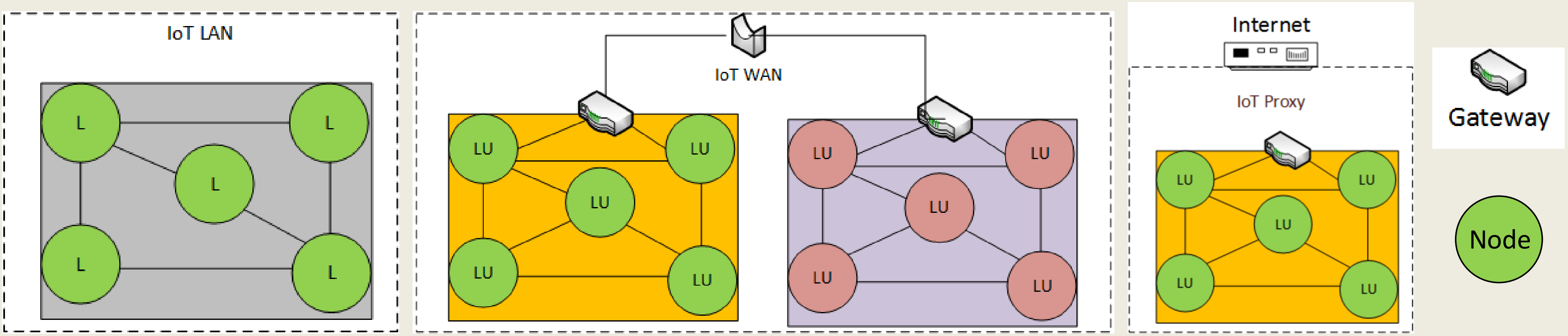
Reference:

- ✓ Cisco Systems, (2011). *The Internet of Things How the Next Evolution of the Internet Is Changing Everything* [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- ✓ ITU Broadband Commission, (2012). *The State of Broadband 2012: Achieving Digital Inclusion for All ITU Broadband Commission Report, [Online]. Available: http://www.broadbandcommission.org/* Documents/bbannualreport2012.pdf
- ✓ Ericsson, (2011). *More than 50 Billion Connected Devices,* [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/wp-50billions.pdf

Connectivity Terminologies

IoT LAN	• Local, Short range Comm, May or may not connect to Internet, Building or Organization wide
IoT WAN	• Connection of various network segments, Organizationally and geographically wide, Connects to the internet
IoT Node	• Connected to other nodes inside a LAN via the IoT LAN, May be sometimes connected to the internet through a WAN directly
IoT Gateway	• A router connecting the IoT LAN to a WAN to the Internet, Can implement several LAN and WAN, Forwards packets between LAN and WAN on the IP layer
IoT Proxy	• Performs active application layer functions between IoT nodes and other entities

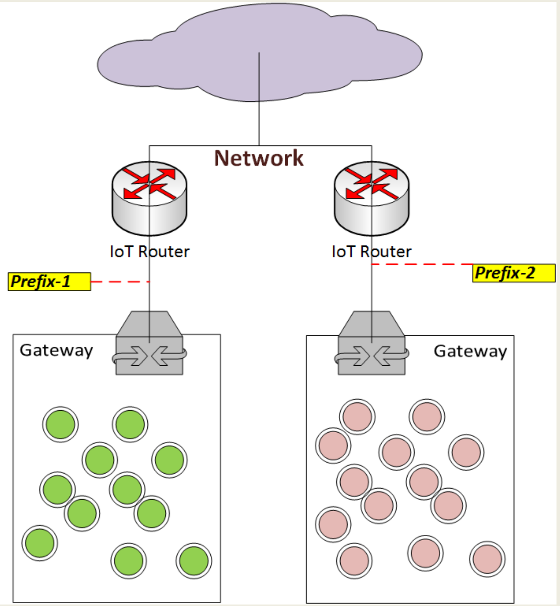
IoT Network Configurations



Reference: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan,*"IPv6 Addressing Strategies for IoT"*, IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013

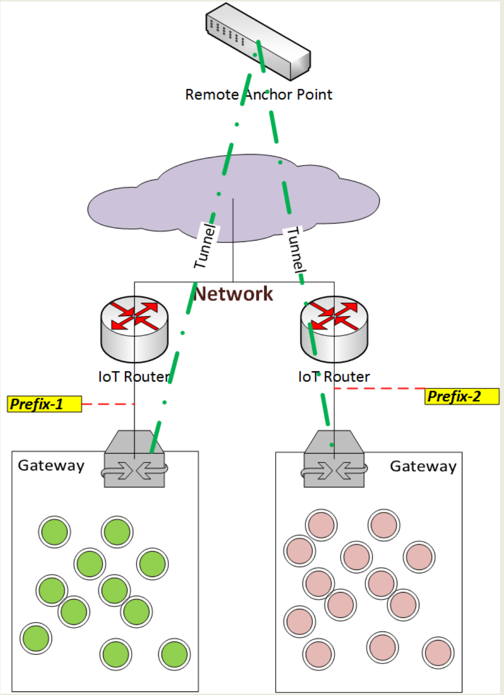
- ✓ Some of the IoT network configurations restricted to local areas, analogous to normal LANs, WANs and proxy are shown in the previous figures.
- ✓ The nodes represented by green circles have **L:** local link addresses or **LU**: local link addresses which are unique locally.
- ✓ Nodes within a gateway’s jurisdiction have addresses that are valid within the gateway’s domain only.
- ✓ The same addresses may be repeated in the domain of another gateway. The gateway have a unique network prefix, which can be used to identify them globally.
- ✓ This strategy saves a lot of unnecessary address wastage. Although, the nodes have to communicate to the internet via the gateway.

Gateway Prefix Allotment



- ✓ One of the strategies of address conservation in IOT is to use local addresses which exist uniquely within the domain of the gateway. These are represented by the circles in this slide.
- ✓ The network connected to the internet has routers with their set of address and ranges.
- ✓ These routers have multiple gateways connected to them which can forward packets from the nodes, to the internet, only via these routers. These routers assign prefixes to gateways under them, so that the gateways can be identified with them.

Impact of Mobility on Addressing



- ✓ The network prefix changes from 1 to 2 due to movement, making the IoT LAN safe from changes due to movements.
- ✓ IoT gateway WAN address changes without change in LAN address. This is achieved using ULA.

- ✓ The gateways assigned with prefixes, which are attached to a remote anchor point by using various protocols such as PMIPv6 (mentioned previously) are immune to changes of network prefixes.
- ✓ This is achieved using ULA. The address of the nodes within the gateways remain unchanged as the gateways provide them with locally unique address and the change in gateway’s network prefix doesn’t affect them.
- ✓ Sometimes, there is a need for the nodes to communicate directly to the internet. This is achieved by tunneling, where, the nodes communicate to a remote anchor point instead of channeling their packets through the router which is achieved by using tunneling protocols such as IKEv2:internet key exchange version 2

Gateways

- ✓ IoT gateways with or without proxies responsible mainly for:
  - Internet connectivity
  - IoT LAN intra-connectivity
- ✓ Upstream addresses prefixes are obtained using mechanisms like DHCPv6 and delegated to the nodes using SLAAC.
- ✓ ULA addresses are maintained independently of globally routable addresses, in cases were internal address stability is of prime concern.

Reference: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan,*"IPv6 Addressing Strategies for IoT"*, IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013

- ✓ Despite of providing address stability, ULA cannot communicate directly with the internet or the upper layers, which is solved by implementing an application layer proxy.
- ✓ Application layer proxies may be additionally configured to process data, rather than just passing it.
- ✓ In nodes with no support for computationally intensive tasks, IoT proxy gathers data sent to the link-local multicast address and routes them globally.

- ✓ Presently, the internet is mainly IPv4 based with little or no IPv6 uplink facilities or support.
- ✓ Due to the lack of a universal transition solution to IPv6, lots of un-optimized solutions are being used for IoT deployment.
- ✓ These makeshift solutions mainly address:
  - IPv6 to IPv4 translation
  - IPv6 tunneling over IPv4
  - Application layer proxies (e.g: data relaying)

Multi-homing

- ✓ In cases of small IoT LANs, where allotment of address prefixes is not feasible and possible, a proxy based approach is used to manage multiple IP addresses and map them to link local addresses.
- ✓ In another approach, IoT gateways with their own address prefixes are used for assigning link local addresses to the nodes under it.

Reference: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan,*"IPv6 Addressing Strategies for IoT",* IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013

- ✓ Providing source addresses, destination addresses and routing information to the multi-homed nodes is the real challenge in multi-homing networks.
- ✓ In case the destination and source addresses originate from the same prefix, routing between gateways can be employed for IoT gateway selection.
- ✓ Presently, IEFT is still trying to standardize this issue.

IPv4 versus IPv6

	IPv4	IPv6
Developed	IETF 1974	IEF 1998
Length (bits)	32	128
No. of Addresses		
Notation	Dotted Decimal	Hexadecimal
Dynamic Allocation of addresses	DHCP	SLAAC/ DHCPv6
IPSec	Optional	Compulsory

IPv4 versus IPv6

	IPv4	IPv6
Header Size	Variable	Fixed
Header Checksum	Yes	No
Header Options	Yes	No
Broadcast Addresses	Yes	No
Multicast Address	No	Yes

IPv4 Header Format

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr>
<tr><td colspan="3">Ver</td><td colspan="5">IHL</td><td colspan="8">Type of Service</td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Source Address (32 bit)</td></tr>
<tr><td colspan="32">Destination Address (32 bit)</td></tr>
<tr><td colspan="24">Options</td><td colspan="8">Padding</td></tr>
</table>

IPv4

- ✓ The IPv4 emphasizes more on reliable transmission, as is evident by fields such as type of service, total length, id, offset, TTL, checksum fields.

IPv6 Header Format

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr>
<tr><td colspan="3">Ver</td><td colspan="9">Traffic Class</td><td colspan="20">Flow Label</td></tr>
<tr><td colspan="18">Payload Length</td><td colspan="9">Next Header</td><td colspan="5">Hop Limit</td></tr>
<tr><td colspan="32">Source Address (128 bit)</td></tr>
<tr><td colspan="32">Destination Length (128 bit)</td></tr>
</table>

IPv6

- ✓ The IPv6 header structure is more simpler as it mainly focuses on the addressing part of the source and destination.
- ✓ It is concerned more with addressing than with reliability of data delivery.

Thank You!!