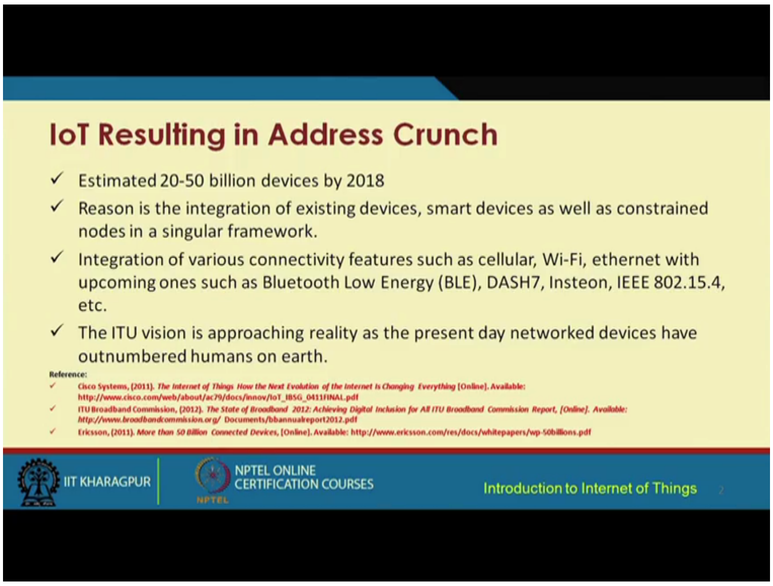
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 02
Introduction to IoT-Part- II

So, now we are going to continue in this lecture with the other basic instructions Basics of Internet of Things.

(Refer Slide Time: 00:34)



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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of Things

So, we have already seen that in the future, it is estimated that the number of things are going to be many, the number of internet of things that are going to be connected are going to be many. So, it is estimated as per one of the studies that by 2018, almost we are going to have 20 to 50 billion devices that are connected that are going to be internetworked.

So, many different applications, so many different devices and these devices are going to be made smart in these applications. So, that is the reason why we are going to have an explosion or in the number of these internetwork things, number of devices connected to the internet of things.

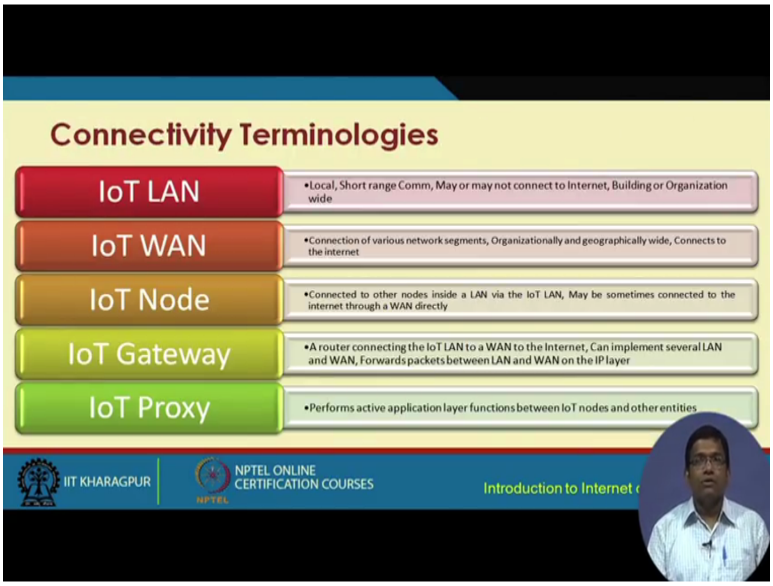
So, as we can understand that if you WANt to internetwork, if you WANt to form a network, a big network, a joint network of internet of things, that means these things being connected, then one fundamental problem that is going to happen is there is going to be an address crunch. We are going to soon run out of the number of addresses that we can assign to each of these devices, the different addresses for example the IP address and so on.

So, IPV4 is defiantly not good enough. People have explored the use of IPV6, but what is required is to come up with a completely new type of addressing scheme which can take care of these issues because of this address crunch.

The next thing is the connectivity. At present there are different various sources, different various ways of offering connectivity. Cellular is one Wi-Fi Ethernet, then Bluetooth Low Energy, Dash 7, Insteon, IEEE 802.15.4, 802.15.6, 80.2.16 so and so forth. So, many different connectivity mechanisms, connectivity standards are available.

So, this is going to be another challenge with respect to network. So, how you are going to have some kind of handshaking between each of this different isolated standards. So, this handshaking has to be, handshaking mechanism has to be devised.

(Refer Slide Time: 03:08)



Connectivity Terminologies

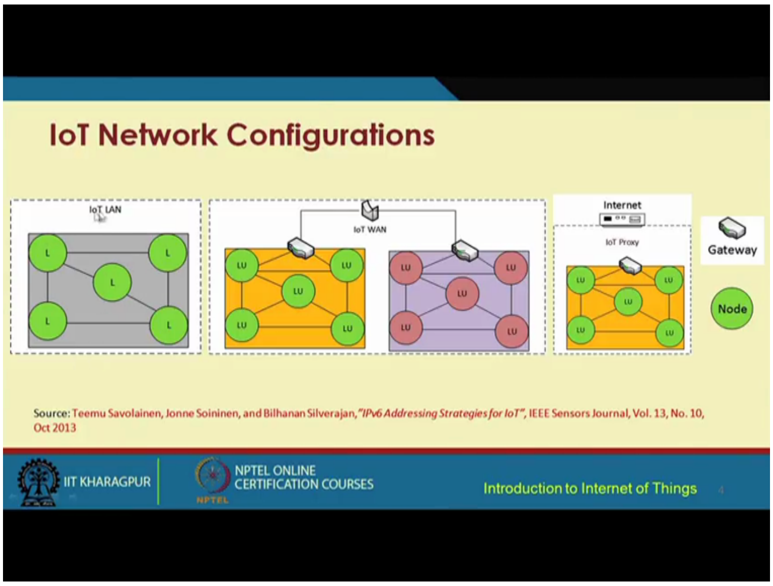
IoT LAN	•Local, Short range Comm, May or may not connect to Internet, Building or Organization wide
IoT WAN	•Connection of various network segments, Organizationally and geographically wide, Connects to the internet
IoT Node	•Connected to other nodes inside a LAN via the IoT LAN, May be sometimes connected 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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet o

So, in terms of connectivity, we are talking about concepts called Unique Building Blocks, such as the LAN IoT, WAN IoT, Node IoT, Gateway IoT, Proxy and so on and so forth. So, all most analogist to what we have as different components of the internet, the capital I internet means the internet of computers analogously. We are also going to have these different components, the LAN, the WAN, the Node, the Gateway, the Proxy, these different components.

So, the concepts are very similar to we have in the internet. So, IoT LAN is very similar to IoT, the internet LAN. So, this is for Local Short Range communication may be building wide or campus wide and so on. IoT WAN is basically internetworking of two different LANs, you know inter connecting of two different LANs, connecting different various network segments organizationally or maybe geographically wide and these can be connected to the internet IoT Node which is the connectivity of the different Nodes inside a LAN or maybe a WAN also directly. Sometimes the LAN you know, the Nodes in the WAN can also be connected IoT. Gateway is basically sort of like you know a router or something very similar which connects to the IoT LAN. So, it is sort of like the outside world, the Gateway beyond a LAN and typically connecting to the WAN. So, we can have in WAN, you know several LANs connected to each other through the individual Gateways and Proxy very similar to what we use proxies for security proxies for sub networking and so on.

(Refer Slide Time: 05:15)



IoT Network Configurations

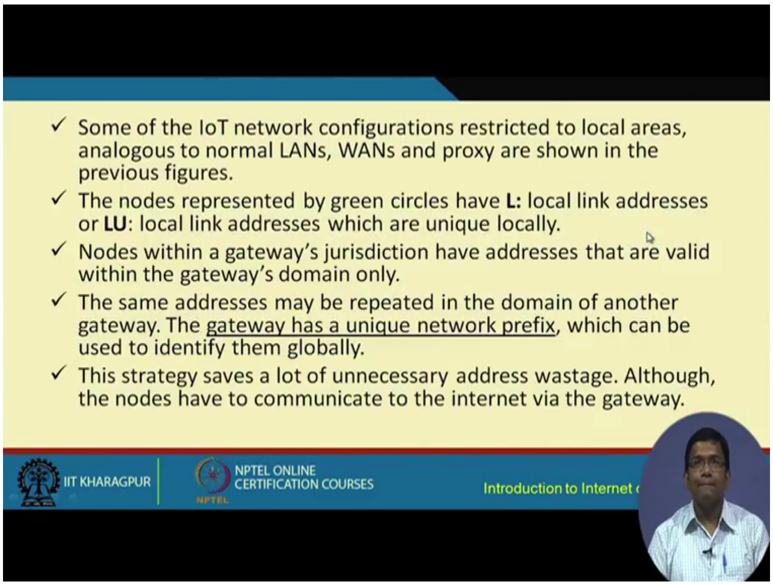
Source: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan, *"IPv6 Addressing Strategies for IoT"*, IEEE Sensors Journal, Vol. 13, No. 10, Oct 2013

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Introduction to Internet of Things

So, if you look at the first picture over here, what we see is IoT LAN. So, you know IoT LAN we have this different IoT devices and each of these devices has its own unique address, local address and these addresses are uniquely local. So, unique that what I am trying to say over here is within a particular LAN, these addresses are unique, these local addresses are unique and similarly, within another LAN, IoT LAN these addresses are unique. So, these are locally unique addresses. So, it might so happen that a particular address might be unique to this LAN, but may be reused in another LAN.

So, the other thing is that these two different LANs, they can connect via two different Gateways. These are the Gateway Nodes and also, we have seen that there is a concept of Proxy. So, Proxy basically helps to connect to the external internet. So, Proxy helps to connect to the internet. So, it is beyond the Gateway and connecting to the internet that is offered by the Proxy.

(Refer Slide Time: 06:56)

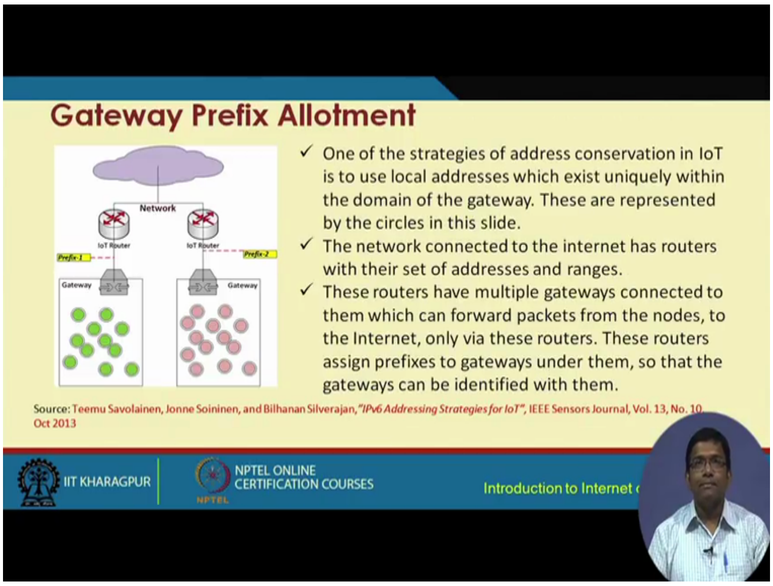


- ✓ Some of the IoT network configurations restricted to local areas, analogous to normal LANs, WANs and proxy are shown in the previous figures.
- ✓ The nodes represented by green circles have **L:** local link addresses or **LU**: local link addresses which are unique locally.
- ✓ Nodes within a gateway's 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 has 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.

So, some of the IoT network configurations are restricted to local areas, very analogous to what we have as internet LANs, WANs and Proxy and this is what we have seen in the previous figure.

So, the Nodes that are within the Gateways jurisdiction have addresses that are valid within the Gateways domain only and the same address maybe repeated in another domain as I was telling you before in the previous slide in the previous diagram. So, the Gateway has a unique network prefix which can be used to identify them globally. So, there is a unique network prefix as well and we are going to look at it shortly. So, this strategy basically saves a lot of unnecessarily address wastage and although the Nodes have to communicate to the internet via the Gateway.

(Refer Slide Time: 07:50)



Gateway Prefix Allotment

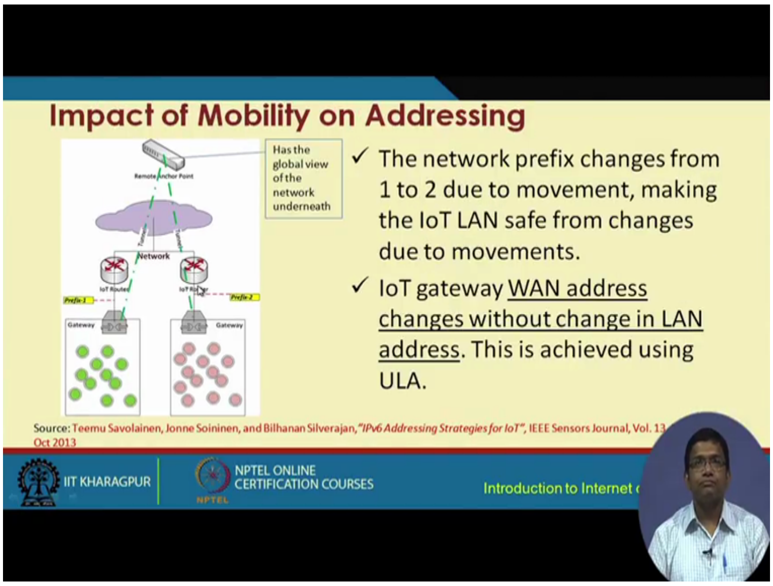
- ✓ One of the strategies of address conservation in IoT is to use local addresses which exist uniquely within the domain of the gateway. These are represented by the circles in this slide.
- ✓ The network connected to the internet has routers with their set of addresses and ranges.
- ✓ These routers 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.

Source: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan, *"IPv6 Addressing Strategies for IoT"*, IEEE Sensors Journal, Vol. 13, No. 10, Oct 2013

So, for address conservation as we have seen, these addresses are unique locally, but they can be reused in another domain, but these networks are connected to the internet, this IoT networks are connected to the network through the Gateway and these IoT routers the network is connected to the internet and these are connected through the routers and these have their own set of addresses and ranges and that means the address ranges.

So, these routers have multiple Gateways and they are connected to them which can forward packets from the Nodes to the internet only via these routers and these routers assign the prefixes to the Gateways that are under them. So, we have this prefix 1 and prefix 2, two different prefixes that I used that are assigned by their corresponding routers to the Gateway. So, prefix 1 is assigned by this router to this Gateway and prefix 2 is assigned by this router to this particular Gateway.

(Refer Slide Time: 09:11)



Impact of Mobility on Addressing

Has the global view of the network underneath

- ✓ 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.

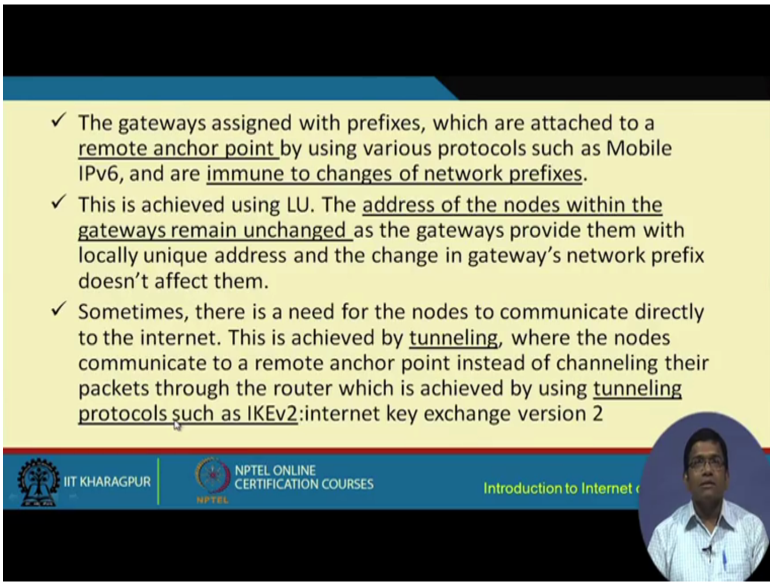
Source: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan, *"IPv6 Addressing Strategies for IoT"*, IEEE Sensors Journal, Vol. 13 Oct 2013

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Introduction to Internet

Now, this is a very important concept that has been proposed because it helps to solve the problem of mobility. So, basically what is going to happen is when a particular Node changes its position from a particular network to another network, let us say from this network is Node moves and comes to this particular network, then the prefix is also going to change from 1 to 2 and this is going to make the IoT LAN safe from changes due to mobility. So, IoT Gateway, basically the IoT Gateway WAN takes care of the address changes without change in the LAN address. So, within the LAN, the address remains the same, but with the help of assignment of this unique prefix, the WAN address changes and that is how the mobility addressing aspect of mobility is taken care of.

So, in this particular figure, we see that there is this concept of the remote anchor point and these particular entity in this network is the one which has the global view of the network that is underneath. That means, this entire network comprising of these LANs, this WAN, the Gateway, then this thing routers and so on. So, this particular entity is considered to be the one which has the unique global view of this network underneath.

(Refer Slide Time: 10:54)



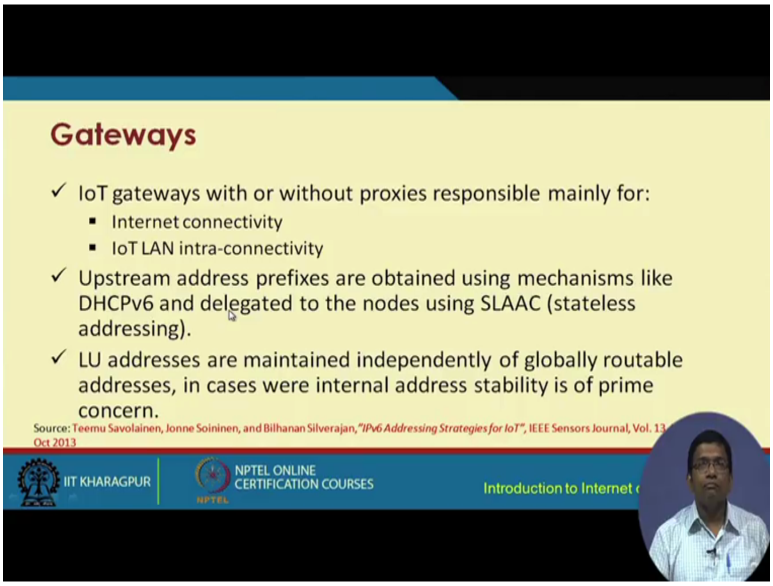
- ✓ The gateways assigned with prefixes, which are attached to a remote anchor point by using various protocols such as Mobile IPv6, and are immune to changes of network prefixes.
- ✓ This is achieved using LU. The address of the nodes within the gateways remain unchanged as the gateways provide them 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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet o

So, now let us try to understand few other concepts surrounding it. So, we have already seen that there is a remote anchor point and if there is a change in the network prefix that can be taken care of automatically and technologies or protocols, such as mobile IPV6 can come helpful in this particular scenarios assuming that IPV6 based addressing is being used.

So, within a particular LAN, the address of the Nodes remain unchanged because they are within the Gateway and within the Gateway, there is a local unique address and the change in the Gateways network prefix does not affect them, but it might be required for the Nodes to communicate directly to the internet as well and this can be done with the help of concept of tunnelling where the Nodes can communicate to a remote anchor point instead of channelling their packets through the router. This can be done with the help of tunnelling protocol, such as IKV, IKEV2. So, this is how with the help of IKEV2, this tunnelling can be done with the help, with the remote anchor point through the Gateways. So, indirectly from the Gateway to the anchor points, the tunnels can be set up like this.

(Refer Slide Time: 12:25)



Gateways

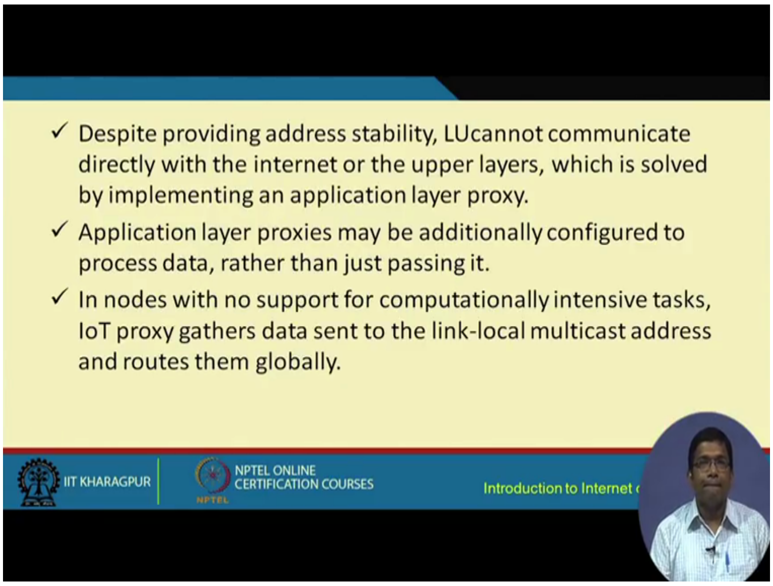
- ✓ IoT gateways with or without proxies responsible mainly for:
  - Internet connectivity
  - IoT LAN intra-connectivity
- ✓ Upstream address prefixes are obtained using mechanisms like DHCPv6 and delegated to the nodes using SLAAC (stateless addressing).
- ✓ LU addresses are maintained independently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

Source: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan, *"IPv6 Addressing Strategies for IoT"*, IEEE Sensors Journal, Vol. 13 Oct 2013

The Gateway has you know associated, they can come with or without proxies and they can offer internet connectivity or intra LAN connectivity. So, within the LAN, they can offer connectivity between the different Nodes within it for up upstream addressing, that means beyond the Gateway.

So, Gateway to the internet mechanisms, such as DHCPV6 assuming that IPV6 technology is being used, DHCPV6 for state based addressing or SLAAC for stateless addressing can be used and the locally unique addresses are maintained independently of the globally routable addresses in cases were internal address stability is of prime concern.

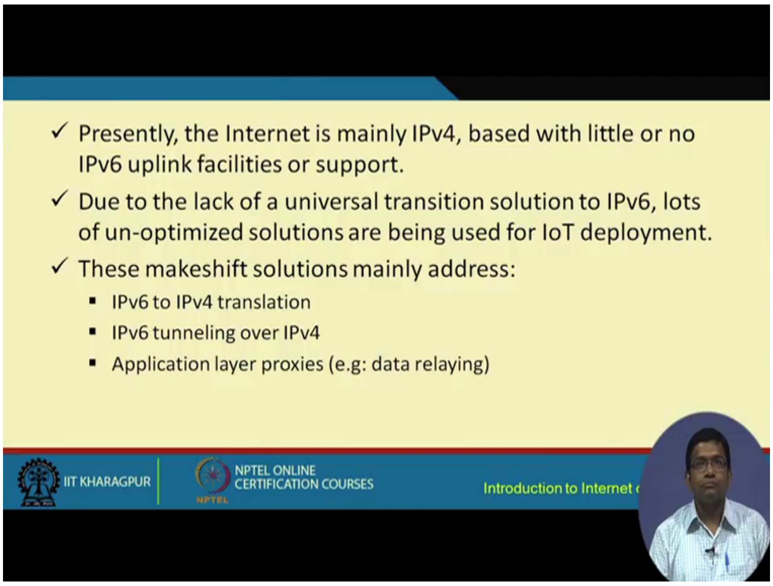
(Refer Slide Time: 13:21)



- ✓ Despite providing address stability, LUcannot 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.

So, we have to keep another thing in mind that despite this mechanism of address stability, the LU cannot communicate directly with the internet or the upper layers which is solved by implementing an application layer Proxy. So, this proxies basically help in achieving connectivity to the upper layers on the internet.

(Refer Slide Time: 13:50)

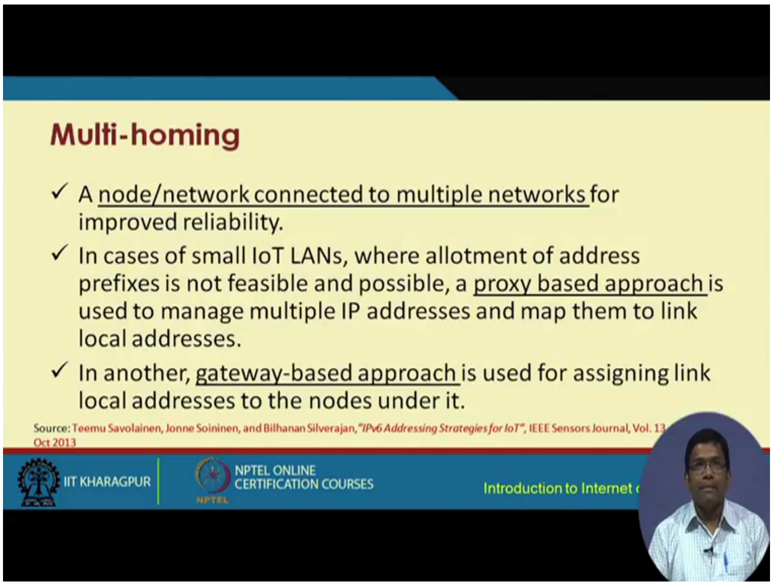


- ✓ Presently, the Internet is mainly IPv4, based with little or no IPv6 uplink facilities or support.
- ✓ Due to the lack of a universal transition solution to IPv6, lots of un-optimized solutions are being used for IoT deployment.
- ✓ These makeshift solutions mainly address:
  - IPv6 to IPv4 translation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

So, most of the IoT based solutions at present still are using IPV4. There are very few IPV6 implementations. So, what is going to happen is if you want to deploy, if you want to approach building IoT by expanding the existing internet, they approach one that I talked about initially as part of lecture 1 for building IoT.

So, in that particular case, what needs to happen is there are different addressing schemes that are followed IPV4 IPV6 and so on. So, something like address translation between IPV4 and IPV6 and vice versa has to happen. This is one until we have a separate addressing scheme, a new type of a addressing scheme. So, handshaking or translation of addresses from IPV4 to IPV6 or from IPV6 to IPV4 number 1, number 2 is tunnelling of IPV6 over IPV4. So, maybe some part of the network uses IPV6. So, these IPV6 PD used can be tunnelled over IPV4 PD used application layer proxies can also be used and these can help in achieving tasks such as data relaying.

(Refer Slide Time: 15:21)



Multi-homing

- ✓ A node/network connected to multiple networks for improved reliability.
- ✓ 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, gateway-based approach is used for assigning link local addresses to the nodes under it.

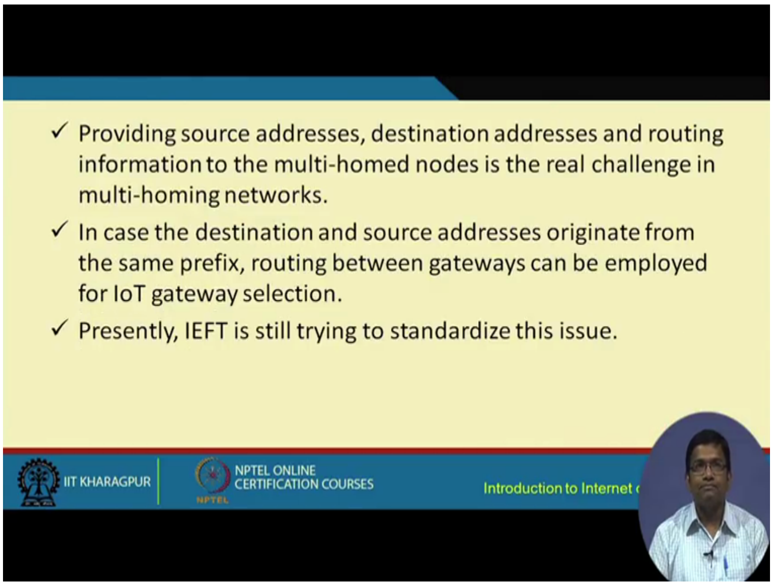
Source: Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan, *"IPv6 Addressing Strategies for IoT"*, IEEE Sensors Journal, Vol. 13 Oct 2013

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet o

Finally, I would like to mention that there is a concept of multi-homing, where a particular Node or an IoT device or the sub network, IoT sub network can be connected multiple networks for improving the reliability. So, basically multi-homing is a concept that is used for improving the overall liability of the network in that way. So, in the same state if some component of the network or maybe a Node has gone down, there is another network that can take over.

So, for these multi homing, there can be two different approaches; a Proxy based approach can be used or a Gateway based approach. I do not need to explain these two approaches in detail, but these names basically tell how the things are going to be managed for multi-homing using these different approaches.

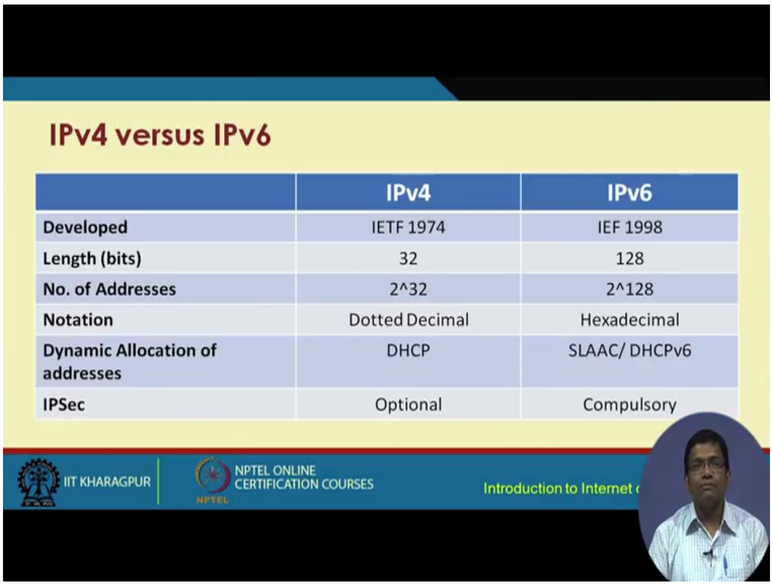
(Refer Slide Time: 16:16)



- ✓ 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.

So, providing source address, destination address and routing information to the multi-homed Nodes is the real challenge in multi-homing networks. So, presently IETF is trying to standardize this particular issue.

(Refer Slide Time: 16:32)

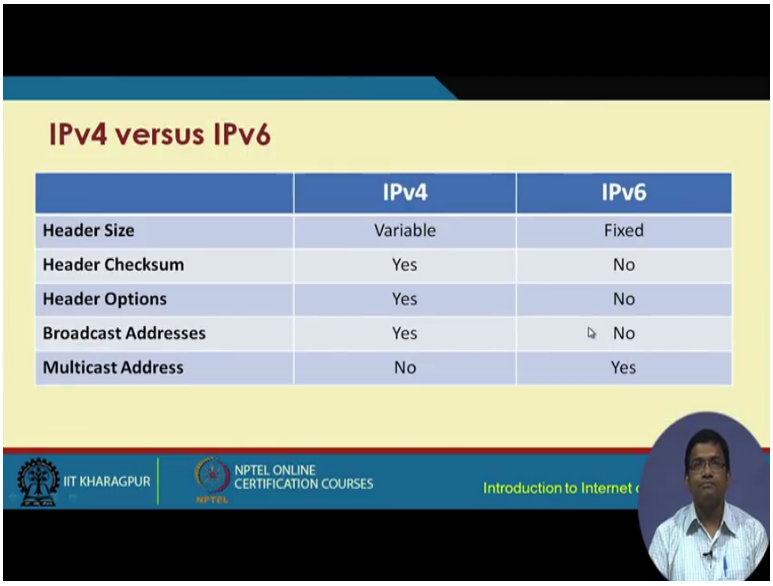


IPv4 versus IPv6

	IPv4	IPv6
Developed	IETF 1974	IEF 1998
Length (bits)	32	128
No. of Addresses	2^32	2^128
Notation	Dotted Decimal	Hexadecimal
Dynamic Allocation of addresses	DHCP	SLAAC/ DHCPv6
IPSec	Optional	Compulsory

So, IPV4 is being used, some parts IPV6 being used. We can use both, but that is not going to be sufficient. We have to come up with a new addressing scheme which we do not know yet what is going to happen. People are still working on it, researches are coming up with different mechanism. There are still lot of research effort on building addressing schemes for IoT, but if IPV4 is used and IPV6 is used, these are the comparison points of comparison between the use of IPV4 and IPV6. The main point of difference is that because the bit length, the length over here in IPV4 is 32 and in IPV6 is 128, the number of addresses in IPV4 is S2 the power 32 only. On the other hand, the address space over here is 2 to the power 128. So, we are going to get a large address space and I think we already know that there is a difference in the notation in IPV4 which is dotted decimal notation and it differs from the IPV6 which has a hexadecimal notation for addressing.

(Refer Slide Time: 17:49)

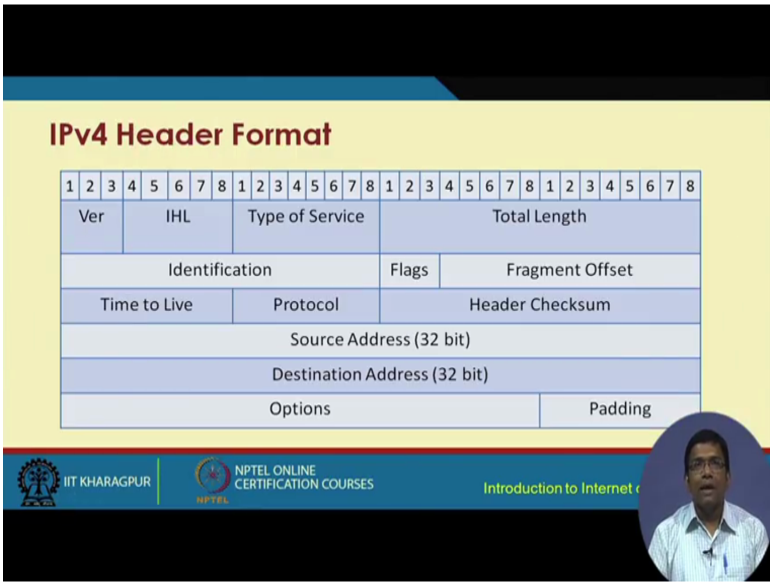


IPv4 versus IPv6

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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet c

(Refer Slide Time: 17:55)



IPv4 Header Format

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

Ver	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live		Protocol	Header Checksum
Source Address (32 bit)			
Destination Address (32 bit)			
Options			Padding

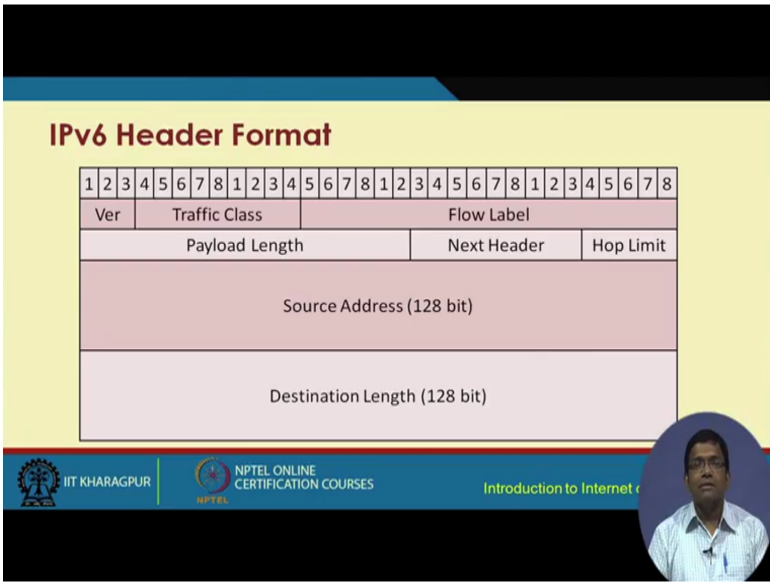
IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Introduction to Internet

So, here are few other points of comparison which I am not going to go through and here is the IPV4 header format.

(Refer Slide Time: 18:01)



IPv6 Header Format

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

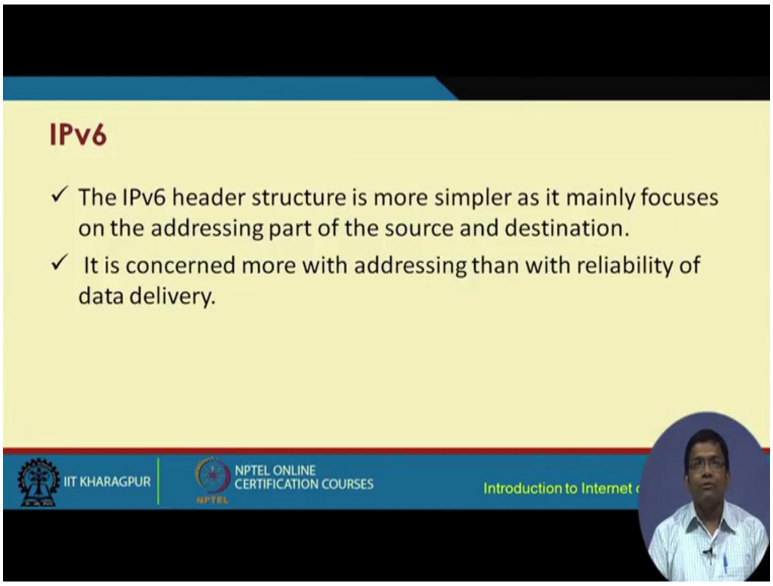
Ver	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address (128 bit)		
Destination Length (128 bit)		

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Introduction to Internet

(Refer Slide Time: 18:06)



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.

Here is the IPV6 header format. So, these IPV4 and IPV6, they have to go hand in hand until there is a new solution for addressing a new mechanism which is completely different from these proposed. So, they have to work hand in hand. So, you know mechanism such as tunnelling or address translation mechanisms have to be used in order for this thing to happen.

So, with this we come to an end of introduction on IoT Internet of Things. We have already understood the motivation for building IoT systems, the different applications of IoT systems, the different characteristics of IoT systems, the different challenges that are involved from networking prospective, what are the different components for building IoT. IoT is a joint network, but then you have to use a modular approach, a step by step approach, a phased approach to building IoT. So, what are the different components from a networking prospective that can be used is what we have already gone through and we have understood.

So, with this we come to an end of the lecture on the Introduction of Internet of Things.

Thank you.