ISSN 2320-9984

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

An Improved Technique for Dynamic Source Routing DSR

Deshraj Ahirwar
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email :deshrajahirwar.sati@gmail.com

Mukesh Kumar Dhariwal
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : er.mukesh2008@gmail.com

Neeraj Tantubay
Assistant Professor
Department of Information Technology
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : neerajtantubay2007@gmail.com

Azher Ahmed Khan
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal (M.P.) [INDIA]
Email : khanazher@yahoo.co.in

Abstract—*This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).*

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

Keywords:— *Adhoc network, IPv6, radio nodes, WLAN, TTL etc.*

1. INTRODUCTION

Dynamic Source Routing (**DSR**) is a routine protocol for wireless mesh network. It is similar to AOD in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routine instead of relying on the routing table at each intermediate device.

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cache by nodes processing the route discovery packet. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

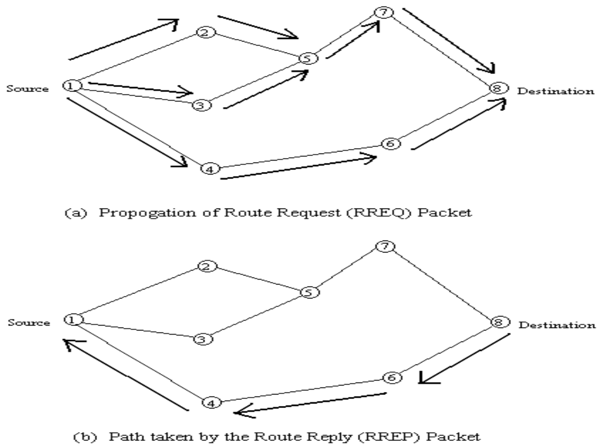
Source
Destination
1
2
3
4
5
6
7
8
(a) Propogation of Route Request (RREQ) Packet
Source
Destination
1
2
3
4
5
6
7
8
(b) Path taken by the Route Reply (RREP) Packet

Figure 1: Propogation of RREQ and RREP packet.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received.

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a RouteRequest packet. This RouteRequest is flooded throughout the network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded.

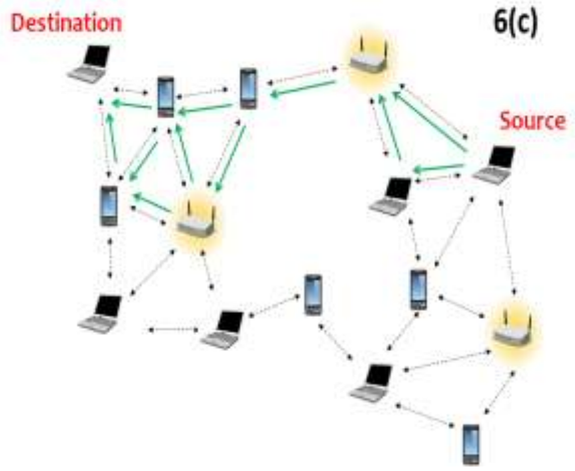

Figure 2: Transmission of packets from source to destination

Each RouteRequest carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate RouteRequest. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase. A destination node, after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase.

2. RELATED WORK

A **wireless mesh network** (**WMN**) is a communications network made up of radio node organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one nod can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. The animation below illustrates how wireless mesh networks can self form and self heal. Wireless mesh networks can be implemented with various wireless technology including 802.1, 802.1, 802.1, cellular technologies or combinations of more than one type.

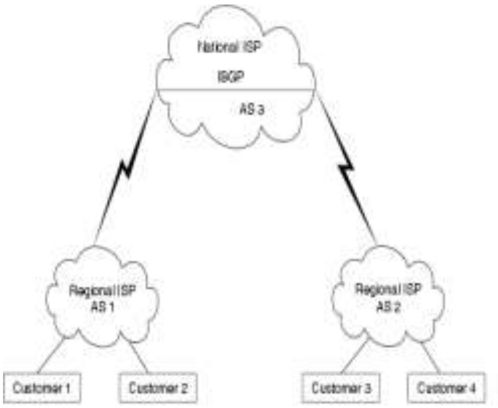

Figure 3: Conection of ISP and customers

Wireless mesh architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing. Such an architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The path of traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes. [1]

IPv6 is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013.[1] As of September 2013, the percentage of users reaching Google services over IPv6 surpassed 2% for the first time.[2]

Every device on the Internet must be assigned an IP address in order to communicate with other devices. With the ever -increasing number of new devices being connected to the Internet, the need arose for more addresses than IPv4 is able to accommodate. IPv6 uses a 128-bi address, allowing 2^{128}, or approximately 3.4×10^{38} addresses, or more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses. IPv4 allows only approximately 4.3 billion addresses. The two protocols are not designed to be interoperable, complicating the transition to IPv6.

IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:1000:8a2e:0370:7334, but methods of abbreviation of this full notation exist.

3. LITERATURE REVIEW

This type of infrastructure can be decentralized (with no central server) or centrally managed (with a central server),[2] both are relatively inexpensive, and very reliable and resilient, as each nod needs only transmit as far as the next node. Nodes act as router to transmit data from nearby nodes to peer that are too far away to reach in a single hop, resulting in a network that can span larger distances. The topology of a mesh network is also reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors can quickly find another route using a routing protocol.

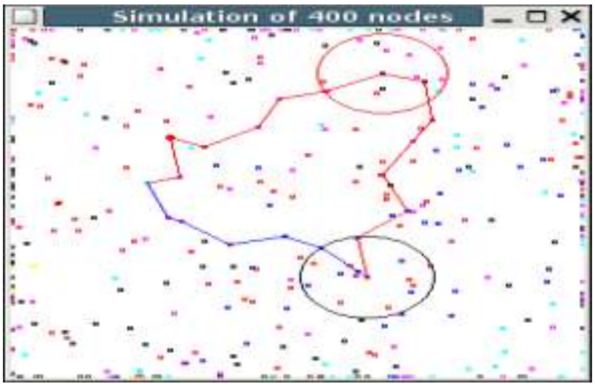

Figure 4: Dynamic source routing in simulation software

Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high speed mobile video applications on board public transport or real time racing car telemetry. An important possible application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh.

Some current applications:

- U.S. military forces are now using wireless mesh networking to connect their computers, mainly ruggedized laptops, in field operations.
- Electric meters now being deployed on residences transfer their readings from one to another and eventually to the central office for billing without the need for human meter readers or the need to connect the meters with cables.[3]
- The laptops in the One Laptop per Child program use wireless mesh networking to enable students to exchange files and get on the Internet even though they lack wired or cell phone or other physical connections in their area.
- The 66-satellite Iridium constellation operates as a mesh network, with wireless links between adjacent satellites. Calls between two satellite phones are routed through the mesh, from one satellite to another across the constellation, without having to go through an earth station. This makes for a smaller travel distance for the signal, reducing latency, and also allows for the constellation to operate with far fewer earth stations that would be required for 66 traditional communications satellites.
- Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This is a true mesh link where you can achieve maximum performance without bandwidth degradation in the mesh and without adding latency. Thus voice and video applications work just as they would on a wired Ethernet network. In true 802.11 networks, there is no concept of a mesh. There are only Access Points (AP's) and Stations. A multi-radio wireless mesh node will dedicate one of the radios to act as a station, and connect to a neighbor node AP radio.

Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long and number about 4.3×10^9 (4.3 billio).[34] IPv6 addresses are 128 bits long and number about 3.4×10^{38} (340 undecillion). IPv6's addresses are deemed enough for the foreseeable future.[35]

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, such as 2001:0db8:85a3:0000:0000:

8a2e:0370: 7334. IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit (sub-) network prefix, and a 64-bit interface identifier.[36]

For stateless address autoconfiguration (SLAAC) to work, subnets require a /64 address block, as defined in RFC 429 section 2.5.1. Local Internet registries get assigned at least /32 blocks, which they divide among ISPs.[37 The obsolete RFC 317 recommended the assignment of a /48 to end-consumer sites. This was replaced by RFC 617, which "recommends giving home sites significantly more than a single /64, but does not recommend that every home site be given a /48 either". /56s are specifically considered. It remains to be seen if ISPs will honor this recommendation; for example, during initial trials, Comcast customers were given a single /64 network.[38]

IPv6 addresses are classified by three types of networking methodologies: unicast addresses identify each network interface, anycast addresses identify a group of interfaces, usually at different locations of which the nearest one is automatically selected, and multicast addresses are used to deliver one packet to many interfaces. The broadcast method is not implemented in IPv6. Each IPv6 address has a scope, which specifies in which part of the network it is valid and unique. Some addresses are unique only on the local (sub-)network. Others are globally unique.

Some IPv6 addresses are reserved for special purposes, such as loopback, 6to tunneling, and Teredo tunneling, as outlined in RFC 515. Also, some address ranges are considered special, such as link-local addresses for use on the local link only, Unique Local addresses (ULA), as described in RFC 419, and solicited-node multicast addresses used in the Neighbor Discovery Protocol.

IPv6 in the Domain Name System

Main article: IPv6 address#IPv6 addresses in the Domain Name System in the Domain Name System, hostname are mapped to IPv6 addresses by *AAAA* resource records, so-called *quad-A* records. For reverse resolution, the IETF reserved the domain ip6.arpa, where the name space is hierarchically divided by the 1-digit hexadecimal representation of nibble units (4 bits) of the IPv6 address. This scheme is defined in RFC 359.

Address representation

The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as 4 hexadecimal digits and the groups are separated by colons (:). The address 2001:0db8:0000:0000:0000:ff00:0042: 8329 is an example of this representation.

For convenience, an IPv6 address may be abbreviated to shorter notations by application of the following rules, where possible.

1. One or more leading zeroes from any groups of hexadecimal digits are removed; this is usually done to either all or none of the leading zeroes. For example, the group *0042* is converted to *42*.

2. Consecutive sections of zeroes are replaced with a double colon (::). The double colon may only be used once in an address, as multiple use would render the address indeterminate. RFC 595 recommends that a double colon must not be used to denote an omitted single section of zeroes.[39]

An example of application of these rules:

- Initial address: 2001:0db8: 0000:0000:0000: ff00:0042:8329
- After removing all leading zeroes: 2001:db8:0:0:0:ff00:42:8329
- After omitting consecutive sections of zeroes: 2001:db8::ff00:42:8329
- The loopback address,

0000:0000:0000:0000:0000:0000:0000:0001, may be abbreviated to ::1 by using both rules.

- As an IPv6 address may have more than one representation, the IETF has issued a proposed standard for representing them in tex.[40]

Transition mechanisms

Until IPv6 completely supplants IPv4, a number of transition mechanisms[41] are needed to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure.

Many of these transition mechanisms use tunneling to encapsulate IPv6 traffic within IPv4 networks. This is an imperfect solution, which may increase latency and cause problems with Path MTU Discover.[42] Tunneling protocol are a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

Dual IP stack implementation

Dual-stack (or *native dual-stack*) refers to side-by-side implementation of IPv4 and IPv6. That is, both protocols run on the same network infrastructure, and there's no need to encapsulate IPv6 inside IPv4 (using tunneling) or vice-versa. Dual-stack is defined in RFC 421.[43]

Although this is the most desirable IPv6 implementation, as it avoids the complexities and pitfalls of tunneling (such as security, increased latency, management overhead, and a reduced PMT),[44] it is not always possible, since outdated network equipment may not support IPv6. A good example is cable T-based internet access. In modern cable TV networks, the core of the HF network (such as large core router) is likely to support IPv6. However, other network equipment (such as a CMT) or customer equipment (like cable modem) may require software updates or hardware upgrades to support IPv6. This means cable network operators must resort to tunneling until the backbone equipment supports native dual-stack.

Tunneling

Because not all networks support dual-stack, tunneling is used for IPv4 networks to talk to IPv6 networks (and vice-versa). Many current internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as *tunneling*, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IP protocol 41 indicates IPv4 packets which encapsulate IPv6 datagrams. Some routers or network address translation devices may block protocol 41. To pass through these devices, you might use UDP packets to encapsulate IPv6 datagrams. Other encapsulation schemes, such as AYIY or Generic Routing Encapsulation, are also popular.

Conversely, on IPv6-only internet links, when access to IPv4 network facilities is needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

Automatic tunneling

Automatic tunneling refers to a technique by which the routing infrastructure automatically determines the tunnel endpoints. Some automatic tunneling techniques are below.

6to is recommended by RFC 305. It uses protocol 41 encapsulation.[45] Tunnel endpoints are determined by using a well-known IPv4 any cast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

Teredo is an automatic tunneling technique that uses UDP encapsulation and can allegedly cross multiple NAT nodes.[46] IPv6, including 6to4 and Teredo tunneling, are enabled by default in Windows Vista[47] and Windows. Most Unix systems implement only 6to4, but Teredo can be provided by third-party software such as Mired.

ISATA (Intra-Site Automatic Tunnel Addressing Protocol)[48] uses the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address. Unlike 6to4 and Teredo, which are *inter-site* tunneling mechanisms, ISATAP is an *intra-site* mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organization.

Configured and automated tunneling (6in4)

6in4 tunneling requires the tunnel endpoints to be explicitly configured, either by an administrator manually or the operating system's configuration mechanisms, or by an automatic service known as a tunnel broke;[49] this is also referred to as *automated tunneling*. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, well-administered networks. Automated tunneling provides a compromise between the ease of use of automatic tunneling and the deterministic behavior of configured tunneling.

Raw encapsulation of IPv6 packets using IPv protocol number 41 is recommended for configured tunneling; this is sometimes known as 6in tunneling. As with automatic tunneling, encapsulation within UDP may be used in order to cross NAT boxes and firewalls.

Proxying and translation for IPv6-only hosts

After the regional Internet registries have exhausted their pools of available IPv4 addresses, it is likely that hosts newly added to the Internet might only have IPv6 connectivity. For these clients to have backward-compatible connectivity to existing IPv4-only resources, suitable IPv6 transition mechanism must be deployed.

One form of address translation is the use of a dual-stack application-layer proxy serve, for example a web proxy.

NAT-like techniques for application-agnostic translation at the lower layers in routers and gateways have been proposed. The NAT-PT standard was dropped because of criticisms,[50] however more recently the continued low adoption of IPv6 has prompted a new standardization effort of a technology called NAT6.

IPv6 readiness

Compatibility with IPv6 networking is mainly a software or firmware issue. However, much of the older hardware that could in principle be upgraded is likely to be replaced instead. The American Registry for Internet Number (ARIN) suggested that all Internet servers be prepared to serve IPv6-only clients by January 2012.[51] Sites will only be accessible over NAT6 if they do not use as well.

4. WORKING

The principle is similar to the way does not exist)"packet travel around the wired Interne-data will hop from one device to another until it reaches its destination. Dynamic routing algorithms implemented in each device allow this to happen. To implement such dynamic routing protocols, each device needs to communicate routing information to other devices in the network. Each device then determines what to do with the data it receives — either pass it on to the next device or keep it, depending on the protocol. The routing algorithm used should attempt to always ensure that the data takes the most appropriate (fastest) route to its destination.

Several proposals appeared for an expanded Internet addressing system and by the end of 1992 the IETF announced a call for white papers.[8] In September 1993, the IETF created a temporary, ad-hoc *IP Next Generation* (IPng) area to deal specifically with IPng issues. The new area was led by Allison Mankin and Scott Bradner, and had a directorate with 15 engineers from diverse backgrounds for direction-setting and preliminary document review:[5][9] The working-group members were J. Allard (Microsoft), Steve Bellovin (AT&T), Jim Bound (Digital Equipment Corporation), Ross Callon (Wellfleet), Brian Carpente (CERN), Dave Clar (MIT), John Curra (NEARNET), Steve Deering (Xerox), Dino Farinacci (Cisco), Paul Francis (NTT), Eric Fleischmann (Boeing), Mark Knopper (Ameritech), Greg Minshall (Novell), Rob Ullmann (Lotus), and Lixia Zhang (Xerox).[10]

The Internet Engineering Task Force adopted the IPng model on 25 July 1994, with the formation of several IPng working groups.[5 By 1996, a series of RFC was released defining Internet Protocol version 6 (IPv6), starting with RFC 188. (Version 5 was used by the experimental Internet Stream Protocol.)

It is widely expected that the Internet will use IPv4 alongside IPv6 for the foreseeable future. IPv4-only and IPv6-only nodes cannot communicate directly, and need assistance from an intermediary gateway or must use other transition mechanisms.

5. CONCLUSION

This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

6. PROPOSED WORK

Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

RECERENCES:

[1] DSR Specificatio (RFC)

[2] piconet an open source POSIX implementation

[3] J. Jun, M.L. Sichitiu, "The nominal capacity of wireless mesh networks, in IEEE Wireless Communications, vol 10, 5 pp 8-14. October 2003

[4] S.M. Chen, P, Lin, D-W Huang, S-R Yang, "A study on distributed/ centralized scheduling for wireless mesh network" in Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, pp 599 - 604.

Vancouver, British Columbia, Canada. 2006

[5] ZigBee.org Smart Energy Overview

[6] Pathak, P. H.; Dutta, R. (2011). "A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks". *IEEE Communications Surveys & Tutorials* **13** (3): 396–428. do:10.1109/ SURV.2011.060710.0006.

[7] V. Kawadia, P. R. Kumar (February 2005). *A Cautionary Perspective on Cross-Layer Design in IEEE Wireless Communications*. pp. 3–11.

[8] Perkins, C.; Belding-Royer, E.; Das, S. (July 2003). *Ad hoc On-Demand Distance Vector (AODV) Routing*. IET. RFC 3561. Retrieved 2010-06-18.

[9] David Frost (20 April 2011). "Ipv6 traffic volumes going backwards. iTWire. Retrieved 19 February 2012.

[10] Roberts, Phil (24 September 2013). "IPv6 Deployment Hits 2%, Keeps Growing. Internet Society. Retrieved 27 September 2013.

[11] : RFC 246, *Internet Protocol, Version 6 (IPv6) Specification*, S. Deering, R. Hinden (December 1998)

[12] *Google IPv6 Conference 2008: What will the IPv6 Internet look like*. Event occurs at 13:35.

[13] RFC 175 *The Recommendation for the IP Next Generation Protocol*, S. Bradner, A. Mankin, January 1995.

[14] Rashid, Fahmida. "IPv4 Address Exhaustion Not Instant Cause for Concern with IPv6 in Wings. eWeek. Retrieved 23 June 2012.

[15] Ward, Mark. "Europe hits old internet address limits. BBC. Retrieved 15 September 2012.

[16] RFC 155, *IP: Next Generation (IPng) White Paper Solicitation*, S. Bradner, A. Mankin (December 1993)

[17] "History of the IPng Effort. Sun.[*dead link*]

[18] The Internet Engineering Task Force. Apendix B. http://tools.ietf.org/html/ rfc1752#appendix-

[19] RFC 172, *Technical Criteria for Choosing IP The Next Generation (IPng)*, Partridge C., Kastenholz F. (December 1994)

[20] "U.S. Census Bureau. Census.gov. Retrieved 20 January 2012.

[21] "Moving to IPv6: Now for the hard part (FAQ). *Deep Tech*. CNET News. Retrieved 3 February 2011.

[22] RFC 207, *Network Renumbering Overview: Why would I want it and what is it anyway?*, P. Ferguson, H. Berkowitz (January 1997)

[23] RFC 207, *Router Renumbering Guide*, H. Berkowitz (January 1997)

[24] RFC 486, *IPv6 Stateless Address Autoconfiguration*, S. Thomson, T. Narten, T. Jinmei (September 2007)

[25] RFC 111, *Host extensions for IP multicasting*, S. Deering (August 1989)

[26] RFC 395, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*, P. Savola, B. Haberman (November 2004)

[27] RFC 290, *The Internet Multicast Address Allocation Architecture*, D. Thaler, M. Handley, D. Estrin (September 2000)

[28] RFC 330, *Unicast-Prefix-based IPv6 Multicast Addresses*, B. Haberman, D. Thaler (August 2002)

[29] RFC 289, *Router Renumbering for IPv6*, M. Crawford, August 2000.

[30] RFC 430, *IPv6 Node Requirements", J. Loughney (April 2006)*

[31] RFC 643, "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)

[32] RFC 396, *Network Mobility (NEMO) Basic Protocol Support*, V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert (January 2005)

[33] RFC 267, *IPv6 Jumbograms*, D. Borman, S. Deering, R. Hinden (August 1999)

[34] Statement on IPv6 Address Privacy, Steve Deering & Bob Hinden, Co-Chairs of the IETF's IP Next Generation Working Group, 6 November 1999.

[35] "Neues Internet-Protokoll erschwert anonymes Surfen. Spiegel.de. Retrieved 19 February 2012.

[36] T. Narten, R. Draves (2001-01). "Privacy Extensions for Stateless Address Autoconfiguration in IPv6.

[37] IPv6 Essentials by Silvia Hagen, p. 28, chapter 3.5.

[38] Privacy Extensions (IPv6, Elektronik Kompendium.

[39] Overview of the Advanced Networking Pack for Windows X, Revision: 8.14

[40] IPv6: Privacy Extensions einschalten, Reiko Kaps, 13 April 2011

[41] "Comment #61 : Bug #176125 : Bugs: "procps" package: Ubuntu. Bugs.launchpad.net. Retrieved 19 February 2012.

[42] RFC 429, *IP Version 6 Addressing Architecture*, R. Hinden, S. Deering (February 2006)

[43] "The sheer size of IPv6. Pthree.org. 8 March 2009. Retrieved 20 January 2012.

[44] RFC 429, p. 9

[45] "IPv6 Address Allocation and Assignment Policy. RIPE NCC. 8 February 2011. Retrieved 27 March 2011.

[46] "Comcast Activates First Users With IPv6 Native Dual Stack Over DOCSIS. Comcast. 31 January 2011.

[47] RFC 595, *A Recommendation for IPv6 Address Text Representation*, S. Kawamura (August 2010), section 4.2.2: http://tools.ietf.org/html/rfc5952#section-4.2.

[48] RFC 595, *A Recommendation for IPv6 Address Text Representation*, S. Kawamura (August 2010)

[49] "IPv6 Transition Mechanism / Tunneling Comparison. Sixxs.net. Retrieved 20 January 2012.

[50] "RFC 6343–Advisory Guidelines for 6to4 Deployment. Tools.ietf.org. Retrieved 20 August 2012.

[51] "RFC 4213, Basic Transition Mechanisms for IPv6 Hosts and Routers. Tools.ietf.org. Retrieved 20 August 2012.

[52] "IPv6: Dual stack where you can; tunnel where you must. www.networkworld.com. 5 September 2007. Retrieved 27 November 2012.

[53] RFC 305, *Connection of IPv6 Domains via IPv4 Clouds*, B. Carpenter, February 2001.

[54] RFC 438, *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*, C. Huitema, Februari 2006

[55] "The Windows Vista Developer Story: Application Compatibility Cookbook. Msdn2.microsoft.com. 24 April 2006. Retrieved 20 January 2012.

[56] RFC 521, *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*, F. Templin, T. Gleeson, D. Thaler, March 2008.

[57] RFC 305, *IPv6 Tunnel Broker*, A. Durand, P. Fasano, I. Guardini, D. Lento (January 2001)

[58] RFC 496, *Reasons to Move the Network Address Translator-Protocol Translator (NAT-PT) to Historic Status*

[59] *Web sites must support IPv6 by 2012, expert warn*. Network World. 21 January 2010. Retrieved 30 September 2010.

[60] "RFC4291. Tools.ietf.org. Retrieved 20 January 2012.

[61] "OpenBSD inet6(4) manual page. Openbsd.org. 13 December 2009. Retrieved 20 January 2012.

[62] "RFC 3493, Basic Socket Interface Extensions for IPv6. Tools.ietf.org. Retrieved 20 January 2012.

[63] "DOCSIS 2.0 Interface. Cablemodem.com. 29 October 2007. Retrieved 31 August 2009.

[64] "RMV6TF.org (PDF). Retrieved 20 January 2012.[*dead link*]

[65] "DOCSIS 3.0 Network Equipment Penetration to Reach 60% by 2011 (Press release). ABI Research. 23 August 2007. Retrieved 30 September 2007.[*dead link*]

[66] Mullins, Robert (April 5, 2012), *Shadow Networks: an Unintended IPv6 Side Effec*, retrieved March 2, 2013

[67] Cicileo, Guillermo; Gagliano, Roque; O'Flaherty, Christian et al. (October 2009). *IPv6 For All: A Guide for IPv6 Usage and Application in Different* Environment (pdf). p. 5. Retrieved March 2, 2013.

[68] "IPv4 Address Report. Potaroo.net. Retrieved 20 January 2012.

[69] Mike Leber (2 October 2010). "Global IPv6 Deployment Progress Report. Hurricane Electric. Retrieved 19 October 2011.

[70] "Beijing2008.cn leaps to next-generation Net (Press release). The Beijing Organizing Committee for the Games of the XXIX Olympiad. 30 May 2008.

[71] Das, Kaushik (2008). "IPv6 and the 2008 Beijing Olympics. *IPv6.com*. Retrieved 15 August 2008. "As thousands of engineers, technologists have worked for a significant time to perfect this (IPv6) technology, there is no doubt, this technology brings considerable promises but this is for the first time that it will showcase its strength when in use for such a mega-event."

[72] Derek Morr (9 June 2009). "Verizon Mandates IPv6 Support for Next-Gen Cell Phones. CircleID.

[73] theipv6guy (31 July 2012). "T-Mobile USA Launches External IPv6