MANET Autoconfiguration (AUTOCONF)
Internet-Draft
Intended status: Informational
Expires: May 6, 2009

C. Bernardos
M. Calderon
I. Soto
UC3M

November 2, 2008

Requirements for IP Autoconfiguration Mechanisms in Backbone Wireless Mesh Network scenarios
draft-bernardos-autoconf-backbone-mesh-reqs-01

Status of this Memo

Abstract

This Internet Draft presents the multi-hop Backbone Wireless Mesh Network scenario, summarising its basic characteristics and describing the requirements and desired properties of an IP Autoconfiguration mechanism aimed at being used in this kind of networks.

Once that the AUTOCONF WG has almost finalised the documents that describe the general architecture of MANETs and the IP autoconfiguration problem statement in MANETs, the WG is expected to start working on solutions. This document describes an ad-hoc

scenario that is getting a lot of attention from both telecommunication operators and end-users: Backbone/infrastructure Wireless Mesh Networking. This document identifies and explains the requirements posed by this particular scenario to an IP autoconfiguration mechanism. The goal is to help the AUTOCONF WG identify the requirements that need to be taken into account when designing IP autoconfiguration solution(s) suitable for this Wireless Mesh environment.

Table of Contents

1. Introduction and motivation

The multi-hop nature of ad-hoc networks and its lack of a single multicast-capable link for signalling prevents current IP address autoconfiguration related protocol specifications (such as RFCs 2461, 2462, etc.) to be used as-is in ad-hoc networks. Some limitations of these existing solutions are stated in [1] and they mainly concern: the lack of multi-hop support, the lack of dynamic topology support, the lack of network merging support and the lack of network partitioning support.

The main purpose of the AUTOCONF WG is to standardise mechanisms to be used by ad-hoc nodes for configuring unique local and/or globally routable IPv6 addresses. The ad-hoc nodes under consideration are, once configured, expected to be able to support multi-hop communication by running MANET routing protocols as developed by the IETF MANET WG.

Once that the AUTOCONF WG has almost finalised the documents that describe the general architecture of MANETs [2] and the IP autoconfiguration problem statement in MANETS [1], the WG is chartered to start working on the standardisation of IP autoconfiguration solutions. In this context, this document reviews and describes a particular ad-hoc scenario that is getting a lot of attention from both telecommunication operators and end-users: Backbone/Infrastructure Wireless Mesh Networking. This document identifies and explains the requirements posed by this particular scenario to an IP autoconfiguration mechanism. The goal is to help the AUTOCONF WG identify the requirements that need to be taken into account when designing IP autoconfiguration solution(s) suitable for the Wireless Mesh environment.

2. The Wireless Mesh networking scenario

Wireless networks are evolving to provide better services with lower deployment costs. Ad-hoc networking as shown itself as one promising technology in many applicability scenarios. The ad-hoc term is highly overloaded nowadays and it usually comprises many different network architectures, with disparate characteristics and requirements. As an example, today we can find several instances of ad-hoc networks: Mobile Ad-hoc Networks (MANETs), sensor networks, Vehicular Ad-hoc Networks (VANETs), Wireless Mesh Networks (WMNs), etc. All of them share their multi-hop, unmanaged and decentralised nature, but also present very important differences. In this document, we pay attention to Wireless Mesh Networks, as one particular type of ad-hoc network that today is gaining momentum, mainly due to the interest from both end-users and telcos.

In a Wireless Mesh Network [3], nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host, but also as a router, forwarding packets on behalf of other nodes that are not within direct wireless reachability of their destinations. WMNs are dynamically self-organised and self-configured, with their nodes automatically setting-up and maintaining mesh connectivity among themselves. WMNs are considered to be a very promising technology for a broad number of applications, such as community and neighbourhood networks, building automation, emergency networks, broadband home networking, carrier backhaul solutions, etc.

A number of variants of WMNs exist today, basically differing from the intended end-use and the mobility of their nodes. As an example, a well known classification of WMNs distinguishes among the following types:

- Infrastructure/Backbone WMNs. Basically, this type of WMN is composed of wireless mesh routers providing an infrastructure for clients to connect to them. One of the possible applications of this type of WMNs is to serve as a carrier backhaul for a telecommunications operator, providing backbone for conventional clients. While mesh-based solutions can be used both in temporary and permanent scenarios, their usage is particularly advantageous in situations where the network infrastructure is only needed for short time periods. In these situations, the deployment of a backhaul infrastructure based on current solutions requires a very high investment which is usually uneconomical for such a short duration; a mesh-based solution provides a much more cost effective way of satisfying this short-term demand. A good example of such a temporary scenario that can greatly benefit from a mesh-based solution is the London 2012 Olympic Games. Besides this kind of "planned wireless mesh deployment", we may consider also an additional and very interesting example of application of backbone WMN: the Neighbourhood/Community Networks, which can be considered as an example of "unplanned wireless mesh deployment".
- Client WMNs. This type of WMNs provides peer-to-peer networks among client devices. Therefore, in this architecture, the client nodes are the ones constituting the actual network to perform routing, configuration and service provisioning to customers. This type of networks does not require mesh routers. Compared to the previous type of WMNs, this imposes more requirements on the end-users, since they must perform additional functions such as routing and self-configuration. Examples of client WMNs include: meeting networks, file sharing networks, entertainment networks for gaming, etc.
- Hybrid WMNs. This architecture is actually the combination of the previous two ones (Infrastructure and Client WMNs), in which mesh clients can access the network both through mesh routers and directly through other clients.

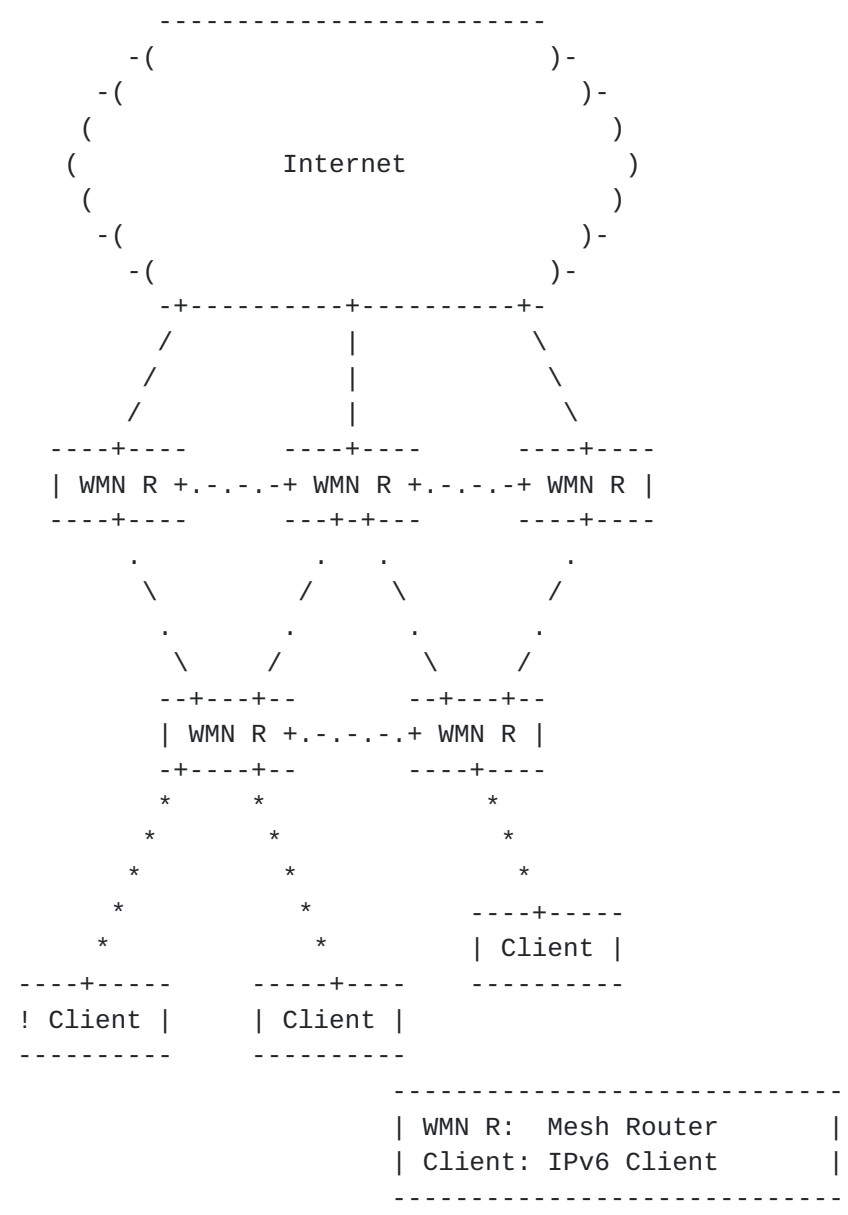

Figure 1: Backbone WMN scenario

Since Infrastructure/Backbone WMNs are a very relevant and common type of WMN -- which is receiving a lot of attention today --, that differs from general MANET scenarios, this document will focus on this type of WMN (Figure 1).

While a Backbone WMN share many common characteristics with classical ad-hoc networks, we may highlight the following key differences:

- Low/null node mobility. Mesh routers will usually present minimal (if any) mobility. Changes in the network topology will be mainly caused by variations in the wireless radio link characteristics and by WMN routers being switched on/off (that is, joining/leaving

the network).

- Infrastructure-connected. While we can differentiate between standalone and connected when considering generic ad-hoc networks, WMNs are expected to be always connected to the Internet. Backbone WMNs (or parts of them) could be temporarily disconnected, but only because some kind of trouble, and therefore the standalone mode of operation does not need to be necessarily considered.
- Multiple gateway nature. Since Backbone WMNs are characterised for its Internet connectivity, they will likely require to benefit from deploying multiple Border Routers/Internet gateways to provide attached nodes with Internet connectivity.
- Compatibility with existing wireless networks, Internet protocols and legacy nodes. Backbone WMNs are expected to provide connectivity to non ad-hoc/legacy clients. Therefore, existing IPv6 nodes should be able to attach to a Backbone WMN (using an unmodified wireless/wired access protocol) and gain Internet connectivity through it.
- Scalability. Although it is difficult to predict and it will be mostly dependant on the particular deployment, Backbone WMNs may be composed of up to hundreds (even thousands) of devices and, therefore, special attention should be paid to the scalability of the protocols designed to work in Backbone WMNs.
- Low power-consumption constraints. Mesh routers usually will not have any strong constraint on power consumption.
- Multiple types of access. While generally speaking ad-hoc networking technologies do not impose any restriction on the technologies deployed within the network, backbone WMNs will likely benefit from disparate heterogeneous wireless and wired access technologies to efficiently provide services to end-users.

3. IP autoconf requirements posed by the Backbone WMN scenario

This section describes in more detail the requirements that the Backbone WMN scenario poses on the design of an IP autoconfiguration solution aimed at working in this kind of environment. This analysis is based on the main characteristics that define Backbone WMNs (described in Section 2). To perform this analysis, we make use of the evaluation considerations defined in [4], by assessing each evaluation consideration from the point of view of a solution targeting Backbone Wireless Mesh Network scenarios.

3.1. Scenarios

This characteristic concerns the multi-hop network environment. In this context, two possible scenarios of ad-hoc networks are identified in [1]: Standalone MANETs and Connected MANETs. WMNs are

expected to be connected to the Internet. This means that the IP autoconfiguration solution will have to deal with the issue of getting global IPv6 addresses that allow nodes to get Internet connectivity.

Since Backbone WMNs are expected to be always connected to the infrastructure (i.e. the Internet), an IP autoconfiguration solution aimed at working in Backbone WMNs must provide support for Connected MANETs, whereas support for standalone operation is not required. This is a critical difference from the general ad-hoc/MANET scenario -- in which supporting Standalone MANETs is usually required -- and might have a noticeable impact on the solution space for this kind of environments, since solutions may assume that the infrastructure is always reachable and benefit from that fact (e.g., availability of servers).

3.2. Mobility type

This characteristic concerns the nodes behaviour in multi-hop network. In fact, nodes' mobility type depends on the application type.

Backbone WMNs are composed of wireless mesh routers, characterised by presenting very low (if any) mobility. Typically, in a Backbone WMN scenario, mesh routers are located at fixed positions (being these locations also very stable over the time), and therefore a low topology dynamism is expected. Most topological changes would be originated by the degradation of radio link conditions and by the switching on/off of wireless mesh routers.

3.3. Address uniqueness

The Address Uniqueness characteristic concerns two points: i) Duplicate Address Avoidance, and ii) Non-unique Address Detection. Duplicate Address Avoidance is a mandatory characteristic in any autoconfiguration mechanism. It consists in making all autoconfiguration mechanisms' functionalities configure addresses only after their uniqueness have been verified. On the other hand, Non-unique Address Detection is the process used to detect address collisions -- that may appear during the normal life-time of the network -- and resolve them.

A solution designed aimed at working in these scenarios must ensure that the IP addresses configured in the mesh routers are unique (therefore, support for Duplicated Address Avoidance is mandatory). Although it is not very likely that several nodes would turn using duplicated addresses during the normal operation of a Backbone WMN, it is interesting to provide also Non-unique Address Detection, in

order to avoid potential disruptions in the IP connectivity due to address conflicts.

3.4. Merging support

This characteristic basically deals with the ability of an autoconfiguration mechanism to detect network merging and the functionalities that are required in order to avoid IP address conflicts and connectivity problems in case several networks merge. To illustrate an example of merging in Backbone WMNs, we might think of a community network formed by several neighbours of a 10-stories building. In this scenario, depending on the availability of the neighbours' routers, it is possible that several isolated WMNs networks are formed (e.g. a WMN cloud formed by routers on 1st to 5th floor and another one formed by routers on 7th to 10th floor). These isolated networks may merge if a router on the 6th floor is switched on. However, given the connected nature of Backbone WMNs (every mesh router needs to be provided with a globally unique IPv6 address), it is very unlikely that after such a merging, an IPv6 address collision happens.

Therefore, an IP autoconfiguration solution aimed at working in Backbone WMNs does not require to provide support for handling network merging.

3.5. Partitioning support

An IP autoconfiguration mechanism may present the ability to detect network partitioning and provide functionalities to avoid connectivity problems in such a case. The same reasoning used in the previous section also applies here. Only temporal, sporadic disconnections -- caused by some kind of trouble -- are expected in backbone networks.

Therefore, an IP autoconfiguration solution aimed at working in Backbone WMNs is not expected to provide support for handling network partitioning.

3.6. Prefix delegation support

An IP autoconfiguration mechanism may support the delegation of IPv6 prefixes to the connected nodes, so they can use these prefixes for further delegation to "traditional" or legacy attached nodes.

Since Backbone WMNs are expected to provide legacy clients with IP and Internet connectivity, supporting the delegation of IPv6 prefixes to the mesh routers is a very interesting feature (although it is not the only possibility to assist legacy clients gaining IP

connectivity). Therefore, an IP autoconfiguration solution aimed at working in Backbone WMNs should support IPv6 prefix delegation.

3.7. Protocol overhead

This characteristic concerns the additional signalling required by the IP autoconfiguration mechanism. Such signalling is considered as protocol overhead that might have a significant performance impact. This characteristic might have an impact on the convergence time, on the scalability of the autoconfiguration mechanism and on the power consumption.

Backbone WMNs are expected not to be power nor resource constrained and they will not typically suffer from very low and poor radio link interconnections. Therefore, although the protocol overhead should always be minimised as much as possible, this is not a very critical issue in this kind of environments.

3.8. Robustness

One important characteristic/property of an autoconf mechanism is its robustness. Given the particular multi-hop characteristics of ad-hoc scenarios, it might be important to analyse the underlying assumptions that an IP autoconfiguration mechanism might make.

IP autoconfiguration mechanism aimed at working in Backbone WMNs should be robust in terms of resiliency to sporadic transmission problems (wireless links are unreliable). However, typical radio and stability conditions in Backbone WMNs will be not much worse than in a single-hop networking scenario, and therefore the use of additional dedicated mechanisms is not expected.

3.9. Convergence time

Another important characteristic, that can be related to the robustness as well, is the convergence time of an autoconf solution. Depending on the scenario and/or the application, we may define the convergence time as the time required by a single node to get a usable (and unique) IPv6 address or as the time required by the whole network to have all its nodes configured with correct addresses.

Given the level of stability of Backbone WMNs (topological changes are mainly caused by radio link degradation and wireless mesh switching on/off), convergence time is not a critical issue. It is expected that only during bootstrapping many nodes will be configuring an IP address simultaneously, and the time that this "power-up" takes is not considered a concern.

3.10. Scalability

An important issue to deal with during autoconfiguration mechanisms design is the scalability of mechanisms to different networks sizes. An autoconfiguration mechanism is not scalable, if its performance degrades significantly when the network size increases. The MANET Architecture I-D [2] defines as Small a MANET composed of 2-30 peer MANET routers, Moderate a MANET composed of 30-100 peer MANET routers, Large a MANET composed of 100-1000 peer MANET routers, and Very Large those MANETs larger than 1000 peer MANET routers.

Given the application scenarios that usually involve Backbone WMNs, an IP autoconfiguration solution aimed at working in these kind of environments should scale in such a way that it works in Large (hundreds to thousands nodes) Backbone WMNs deployments.

3.11. Address space utilisation

This characteristic basically analyses how an autoconf solution makes use of the available address space.

An IP autoconfiguration solution aimed at working in WMNs should make an efficient use of the IP address space available, given its connected nature and its potentially large size.

3.12. Distributed/Centralised approach

There are different possible approaches that an IP autoconfiguration mechanism might follow to provide IP addresses to all the nodes of an ad-hoc network, from the deployment a centralised server that is in charge of the IP address configuration (e.g., DHCPv6) to sharing the IP address configuration task among all the participant nodes.

The Backbone WMN scenario does not impose itself any constraint/ requirement on the particular type of solution to be used (centralised or distributed). However, given the connected nature and reasonable topological stability of Backbone WMNs, the use of centralised solutions is not as discouraged as in a general MANET environments. Therefore, approaches that make use of centralised servers located at the infrastructure can be considered.

3.13. Trust and security

Security is a critical issue in any communication protocol. In the design of autoconfiguration mechanisms, attacks in ad hoc multi-hop environments should be considered. Given the typical application scenarios of WMNs, it might be even possible to assume the existence of trust relationships between each communicating pair of nodes that

are involved in the autoconfiguration process.

An IP autoconfiguration solution aimed at working in Backbone WMNs should be provided with a level of security similar to today's fixed Internet. Because of the connected nature and taking into account the potential application scenarios that are being considered today for Backbone WMNs, it could be assumed the existence of trust relationships (or mechanisms enabling its establishment on-demand) between the participant nodes.

3.14. Integration with standard IPv6 nodes

Certain autoconf mechanisms may allow/be compatible to support IPv6 nodes to get addresses using standard mechanisms defined in IPv6, while others may be totally incompatible with today's IPv6 nodes, therefore preventing these nodes to inter-operate with these autoconf solutions, unless the IPv6 nodes are properly modified to support them.

Enabling the connectivity of legacy clients is a key characteristic of a Backbone WMN, Therefore an IP autoconfiguration solution aimed at working in this kind of environments must be compatible with standard IPv6 nodes, allowing them to attach and get IP connectivity through the WMN.

3.15. Gateway involvement

Internet gateways (also known as MANET Border Routers) are responsible of providing nodes with the connectivity to the fixed infrastructure. Additionally, these gateways might also have a role/ involvement in the IP address configuration procedure (e.g., in some solutions, the gateway might only be responsible of forwarding packets to the infrastructure, while in other solutions it may also be involved in the task of providing nodes with addresses/prefixes).

An IP autoconfiguration solution aimed at working in Backbone WMNs does not impose any particular role to the Internet Gateways in the IP address configuration process. Again, given the always-connected nature of this kind of WMNs, a particular solution may become simpler when collocating the gateway and IP address functionalities on the same entities.

3.16. Routing protocol dependency

An IP autoconfiguration mechanism may depend on a particular routing protocol in order to work properly or may need some specific information from the routing protocol stack, whereas another autoconfiguration mechanism may be completely independent of the

routing protocol used in the network.

Potentially, it is preferred to keep the IP autoconfiguration solution as much independent as possible from the MANET routing protocol used in the network. However, since Backbone WMN scenarios usually involve relatively closed user groups (e.g., community networks) or domains administered by a single entity (e.g., backhaul operator networks), the MANET routing protocol dependency is not an issue as critical as in generic ad-hoc scenarios.

3.17. Multiple interfaces support

One characteristic that might have an impact on the IP autoconfiguration mechanism is the number of interfaces that should be provided with IP addresses. Although from a conceptual point of view solutions should not be affected by this, if we look at the solution space, this could have an impact on the IP autoconfiguration mechanism.

Wireless mesh routers will typically have more than one single physical interface. Therefore, an IP autoconfiguration solution aimed at working in a backbone WMN should support the operation on multiple-interfaced mesh routers, being able to provide IP addresses to more than one single interface.

4. Security Considerations

None.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgements

Patrick Stupar provided text for an earlier version of this draft.

This work has been partially supported by the Spanish Government under the POSEIDON (TSI2006-12507-C03-01) project.

This work has also been partially supported by the EU through the ICT FP7 European Project CARMEN (INFSO-ICT-214994). Apart from this, the European Commission has no responsibility for the content of this Internet-Draft. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for

any particular purpose. The user thereof uses the information at its sole risk and liability.

7. References

7.1. Normative References

[1] Baccelli, E., Mase, K., Ruffino, S., and S. Singh, "Address Autoconfiguration for MANET: Terminology and Problem Statement", draft-ietf-autoconf-statement-04 (work in progress), February 2008.

[2] Chakeres, I., Macker, J., and T. Clausen, "Mobile Ad hoc Network Architecture", draft-ietf-autoconf-manetarch-07 (work in progress), November 2007.

7.2. Informative References

[3] Akyildiz, I., Wang, X., and W. Wang, "Wireless mesh networks: a survey", Computer Networks, vol. 47, no. 4, March 2005, pp. 445-487 , 2005.

[4] Moustafa, H., Bernardos, C., and M. Calderon, "Evaluation Considerations for IP Autoconfiguration Mechanisms in MANETs", draft-bernardos-autoconf-evaluation-considerations-03 (work in progress), November 2008.

Appendix A. Change Log

Changes from -00 to -01:
- New release to keep the document alive.
- Update of some references.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es

Maria Calderon
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 8780
Email: maria@it.uc3m.es

Ignacio Soto
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 5974
Email: isoto@it.uc3m.es

Full Copyright Statement

Intellectual Property