Robust real-time IP-based multimedia communication

Peter van der Stok
Philips Research
Prof. Holstlaan 4
NL - 5656 AA Eindhoven
Peter.van.der.Stok@philips.com

Michael van Hartskamp
Philips Research
Prof. Holstlaan 4
NL - 5656 AA Eindhoven
Michael.van.Hartskamp@philips.com

Abstract

The home network will be an IP-based local area network that originates from a desire to share the Internet connection. Eventually, it will have to deliver real-time audio and video to its users.

The IP-based nature of the home network gives a mismatch between the original assumptions of the IP-protocol and the practice of a home network.

In this paper we focus on several of the components of the IP stack that disturb the real-time behavior of the network in a more profound way than might be expected.

For this we provide three scenarios that show what happens in the case that new devices are added, existing devices are removed or networks are merged.

We conclude by showing directions on how to remedy the indicated problems.

1. Multimedia Communication

Networks slowly penetrate our homes. The most common path to a home network is via the addition of a second PC to share the Internet connection with the first PC. Viewing video and listening music of streams coming from a provider over the Internet to our homes is becoming more and more popular. The natural continuation of this trend is a home in which many boxes are interconnected by a network. This in-home network of devices will provide the so-called DICE functionalities

- *Domotica,* the control of the infrastructure facilities in the home like light, gas, heating.
- *Information*, the acquisition of pieces of (encyclopedic) information, e.g. from the Internet.
- *Communication*, the exchange of information between humans e.g. video conferencing.
- *Entertainment*, the enjoyment of activities within the home or family surroundings, e.g. viewing a film.

Given that the network in the home grows from the second PC that heavily relies on the Internet Protocol (IP) and given that many standards compete for acceptance (if not dominance), the IP stack seems a likely candidate to form the basis for the network in the home.

A network that provides entertainment in the home should support the streaming of video or audio over the network. Video streaming to the TV puts very stringent requirements on the robustness of the network. Although people in general accept that video over the Internet has flaws, people are not ready to accept frame skips, sudden reductions in quality, still pictures, or noise on their TV set.

In this paper we first discuss some of the important components of an IP network. The behavior of these components that makes the network less robust than tolerable for real-time use is discussed in Section 3. Finally we discuss possible ways to remedy or circumvent these problems.

2. IP components

The IP stack is composed of several protocols that are described in Request For Comments (RFC). These RFCs prescribe how a protocol should be implemented to deliver a given functionality. Many implementation choices are left open because the needs for the Internet protocol at the time of creation of the RFC was different from the needs today. One of the more dramatic changes is the size of the Internet that makes the configuration by hand difficult if not impossible. Laptops with wireless communication cards that move from sub-net to sub-net have made it necessary to render the network more dynamic. Therefore, IP addresses are leased to devices for a limited period. However, stability is wanted as well, because we want to address a specific item with a specific name that identifies the device uniquely within a given context (e.g. your home). Components that can yield unwanted behavior in the home context are:

- *DHCP*, the DHCP distributes IP addresses to network interfaces. Several DHCP servers can propose an address. One address with a finite validity interval is chosen.

- *DNS,* the DNS server attributes names to addresses. Names change when addresses change.
- *ZeroConf,* the IPv4 zeroconf working group proposes to allocate link-local addresses within 6 seconds after an address conflict.

3. Network behaviors

In a perfectly stable network, The IP stack will provide stable addresses and names to network interfaces. However, the home network is not a stable network. Devices are added to the network when people return home from work or school. Devices may be switched off, when the user does not see the value of leaving the device on.

At the moment devices are switched off or networks are merged, the reconfiguration activities of the IP-stack may result in video streams being interrupted for several seconds for no clear reason to the user.

One of the essential elements for acceptability of a home network is that there is a clear cause and effect relationship between actions in the network. The freezing of an image on the TV set because 20 minutes ago a new device was inserted, and only now another device fails in refreshing the IP addresses it had leased, is quite unacceptable. Nevertheless such unwanted behavior is perfectly possible and even likely with today's IP stack.

Three possible scenarios illustrate the unwanted behavior.

Device addition. The added device contains a DHCP server. Two cases may be discerned: (1) no DHCP server was present on the network, or (2) at least one DHCP server was present. In the latter case it may be possible that the contact to the originally used DHCP server was also lost. The result is that the IP address of one or more devices needs to change and ongoing IP connections are severed. Changing an IP address can take up to 6 seconds, leading to no TV for at least 6 seconds.

Device removal. The removed device contains a DHCP server. Again two cases can be discerned (1) this was the only DHCP server, and (2) at least one DHCP server is left. Same behavior as under device addition.

Merging networks. Networks are merged with a wireless bridge. Names on the two networks may be the same. Some IP addresses may be the same. The duplicate IP addresses need to be changed, thus leading to connection disruption and interruption of audio/video streaming. Changed IP addresses lead to different names in DNS. Even when no IP address duplication is present, the DNS may adapt the names.

4. Remedies

In this section we consider a few possible remedies for the described problems

Use IPv6 link-local addresses.

Currently, more and more interest is going to IPv6, the protocol succeeding IPv4. The main advantage is that IPv6 has a much larger address space since an address consists of 16 bytes instead of just 4. Given that IPv4 and IPv6 are not compatible and that the Internet is now slowly moving towards IPv6, a solution might be to make the home network already IPv6 based.

Also in IPv6, a distinction is made between so-called link-local and globally unique addresses. The link-local addresses are intended for use on the local link only and may not be forwarded beyond the link.

Because of the abundance of addresses IPv6 enables link-local addresses to be configured by embedding the IEEE addresses of the network card in the IPv6 address. For more information we refer to [6].

Since this is not the only way a link-local address can be obtained there still is a uniqueness requirement to be tested via Neighbor Discovery (see [5]). Here it may be skipped and no delays occur. Concluding, whenever compliant devices are added or removed or networks are merged no IP address changes are necessary.

Observe that the globally unique address is in the end acquired via the Internet Service Provider and may still be subject to change. The consequences, however, are then confined to connections from and to the Internet only.

Use link-local addresses even in the presence of a DHCP server.

The solution above of link-local addresses does require them to be actually used. Often it is posed as a requirement to first query for a DHCP server and if any is found use the addresses as assigned by the server. As described in the scenarios above this may lead to problems. The solution is to allow link-local addressing even in the presence of DHCP servers and not to enforce the use of such servers. When a connection is established, the protocol should verify whether a link-local address can be used. In that case it should use its own link-local address as source address to establish the communication. Within IPv6 the choice of the link-local address is fixed to the hardware address. Within IPv4 this is not the case. Consequently, with IPv4 addresses clashes can occur and link-local addresses need to be reallocated. Maintaining connections with discarded addresses is still needed.

Make switching of IP addresses less disruptive to involved connections.

In practice problems arise because a change in the network layer (IP address) affects the connection at the application level.

Since for instance TCP uses the IP addresses together with port numbers a change in an IP address cannot be confined to the network layer and needs to be propagated to TCP. Otherwise the connection simply breaks. Two cases have to be discerned, the host can be directly addressed or is reached via a router. When the host can be directly addressed, the host can maintain two tables of IP addresses to hardware addresses. One table for current mappings and one table for invalid but still used mappings. The involved port needs to be signaled sending to an invalid but used address. When the packet is passed on for sending, the old invalid table is used to send the packet. At the receiver side, also two tables are needed to accept the packets with out-of date IP addresses. Care must be taken that the invalid table is not used for responses to ARP requests.

Reducing timing

Many protocols include time-outs to wait for messages that do not arrive. For real-time networks, the delay incurred by this waiting may be crucial. Some of these time-outs are based on large-scale networks and might for a home situation safely be decreased.

In the Zeroconf workgroup of IETF, progress is made in reducing the waiting time for Zero-configuration. Currently it is 6 seconds. The time-out and the number of packets sent to establish whether an address is already in use can be adapted to the reliability of the network. In [7] a calculation based on Markov chains shows that under specific conditions only one packet needs to be sent with time-outs of a few 100 ms to establish that an IP address is unique with a reasonable reliability.

More coordination between DHCP servers

When a host sends a DHCP request, it waits for the first answer. When several DHCP servers are present, the first answer to a query need not always come from the same DHCP server. Taking the first returned answer may hence lead to frequent, but unnecessary, IP address changes. There exists an option to wait for several answers and not take the first one. The waiting for all answers needs to be the recommended option for home networks.

In the DHCP request, the host also must indicate a preference for a given IP address connected to its hardware address. Addresses returned by DHCP servers from different IP service providers may nevertheless differ. Under such circumstances it is useful to setup IP addresses as function of the DHCP server. The IP address selection algorithm becomes more complex than the earlier suggestion of using two tables of invalid and valid addresses.

Network split/merge

In the former solutions, we suggest to keep several IP addresses and use the appropriate IP address to maintain old connections. This is a valid approach as long as no routers are passed. Connections passing through a bridge may not be maintainable anyway. When merging networks through a link-layer bridge, the bridge may still wait up to 30 seconds before starting to forward frames. Dependent on the amount of time that the network is disconnected, no real-time streaming will be possible. As the user may well recognize this situation, the disappearance of the images corresponds to the same situation when his TV provider experiences an hiccup. However, these bridge or gateway failures should have no impact on the local streams, as discussed above.

Do not rely on DNS for user-based naming but use other mechanisms.

Applications talk to hosts by using a name and not the IP address. The binding of name to IP-address is done with DNS. DNS is one of the backbones to security in Internet. Problems galore occur when the naming system cannot be trusted. Changing the DNS is not recommended at all. However, the mapping from name to address is a rather fixed one. In a dynamic home network, where IP addresses may change, it would lead to frequent changes to applications and users trying to figure out what device is connected to a given DNS name. Actually no globally unique names are needed in a home network but names that remain stable with a given hardware address. An additional naming system, apart from DNS, that provides mapping from a name to hardware address is recommended. Such a mapping can be used to solve some of the problems above. IP addresses are not used on the local network, but local names are translated to hardware addresses. Next to the tables that translate DNS names to IP address and IP addresses to hardware addresses, another table is proposed that translates local names to hardware addresses. Hardware address may be replaced with an IPv6 link-local address when IPv6 is used.

The local names exist next to the IP addresses and DNS names. Names can be found and their uniqueness can be established using ARP like protocols. Connections over routers and gateways to externals service providers use IP addresses. Local streaming applications use local addresses or IPv6 link-local addresses.

5. Conclusions

We discussed the IP-stack and showed that there are a number of problems in the DHCP, DNS, and Zeroconf protocols that inhibit guaranteed real-time behavior. We also discussed directions towards solving these problems. Problems with network partitioning and merging will in all cases lead to perturbations. Within

the local home network these perturbations can be reduced by a set of measures:

- use IPv6 link-local addresses
- use IPv4 link-local address
- reduce wait times in IPv4 link-local protocols
- send suggestions to DHCP protocols
- maintain connections with invalid addresses.
- Provide a table with local name to hardware address (IPv6 address).

Acknowledgements

This work was partially funded by the European fifth framework program in the context of the Ozone project.

References

1. IETF, zeroconf working group
2. RFC 1034, Domain names – concepts and facilities
3. RFC 1035, Domain names – Implementation and specification
4. RFC 2131, Dynamic Host Configuration Protocol
5. RFC 2461, Neighbor Discovery for IP Version 6 (IPv6)
6. RFC 2462, IPv6 Stateless Address Autoconfiguration
7. Henrik Bohnenkamp, Peter van der Stok, Holger Hermanns, Frits Vaandrager, *Cost optimisation of the IPv4 Zeroconf Protocol,* DNS 2003.