Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 7, 2016

B. Lv
Y. Jia
M. Liang
H. Xie
CAEIT

July 6, 2015

Service Centric Networking Architecture for Smart Homes
draft-lv-homenet-service-centric-architecture-00

Abstract

We propose a general service centric homenet architecture, which can handle the diversity of devices, services, applications and context. Especially, we focus on building an overall home network topology, routing and naming structures, to fit SCN into a home network. In the future, we will discuss homenet caching, mobility and security in details.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 7, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Terminology and Abbreviations 2
2. Homenet Architecture 3
2.1. General Principles 3
2.2. Homenet Architecture 3
2.3. Homenet Naming 5
2.4. Homenet Routing 6
2.5. Use Cases 7
2.5.1. Smoke Monitering Service 7
2.5.2. Video Streaming Service 8
2.5.3. Command Delivering Service 8
2.6. Other Considerations 9
3. IANA Considerations 10
4. Informative References 10
Authors' Addresses 10

1. Introduction

Many researchers believe that the legacy IP network architecture is not suitable for Internet of Things due to IPv4 address depletion and various concerns such as security, overhead and efficiency. Smart home networking is a special scenario of Internet of Things. We believe that the legacy IP network architecture is not suitable. Inspired by the recently proposed concept of the content centric network, we strongly believe that a simpler but more appropriate networking architecture is necessary and important for the success of homenets.

In the homenet, the networked devices have heterogeneous ways of connecting to the Internet, often with severe resource constraints and many of which are mobile. Interactions between the applications and devices are often real-time and dynamic, requiring strong security and privacy protections. In order to address these challenges, we propose a service-centric networking architecture to achieve efficient, secure, and reliable networking services for smart homes.

1.1. Terminology and Abbreviations

Region router: inner routers to deliver contents.

Homnet gateway: a connection between homenet and outside networks. It also performs pre-processing and aggregation of contents.

ISP gateway: An entity that provides access to the Internet.

Device: in a smart home network scenario, there are two main kinds of devices. Some of the devices can generate instant content or stream content like smoke sensor and surveillance. The rest devices can only perform commands from users or application and change their states such as lights, air conditions and fridge.

CCN: Content Centric Network

SCN: Service Centric Network

ISP: Internet Service Provider

PIT: Pending Interest Table

CS: Content Storage

APP: application

MAC: Media Access Control

2. Homenet Architecture

2.1. General Principles

Home network has driven a huge amount of attentions from both researchers and industries. While home network grows in complexity as more smart appliances, sensor and network devices join in, we would like to use SCN to fit into home network's scenario which has plenty of control information as well as data information.

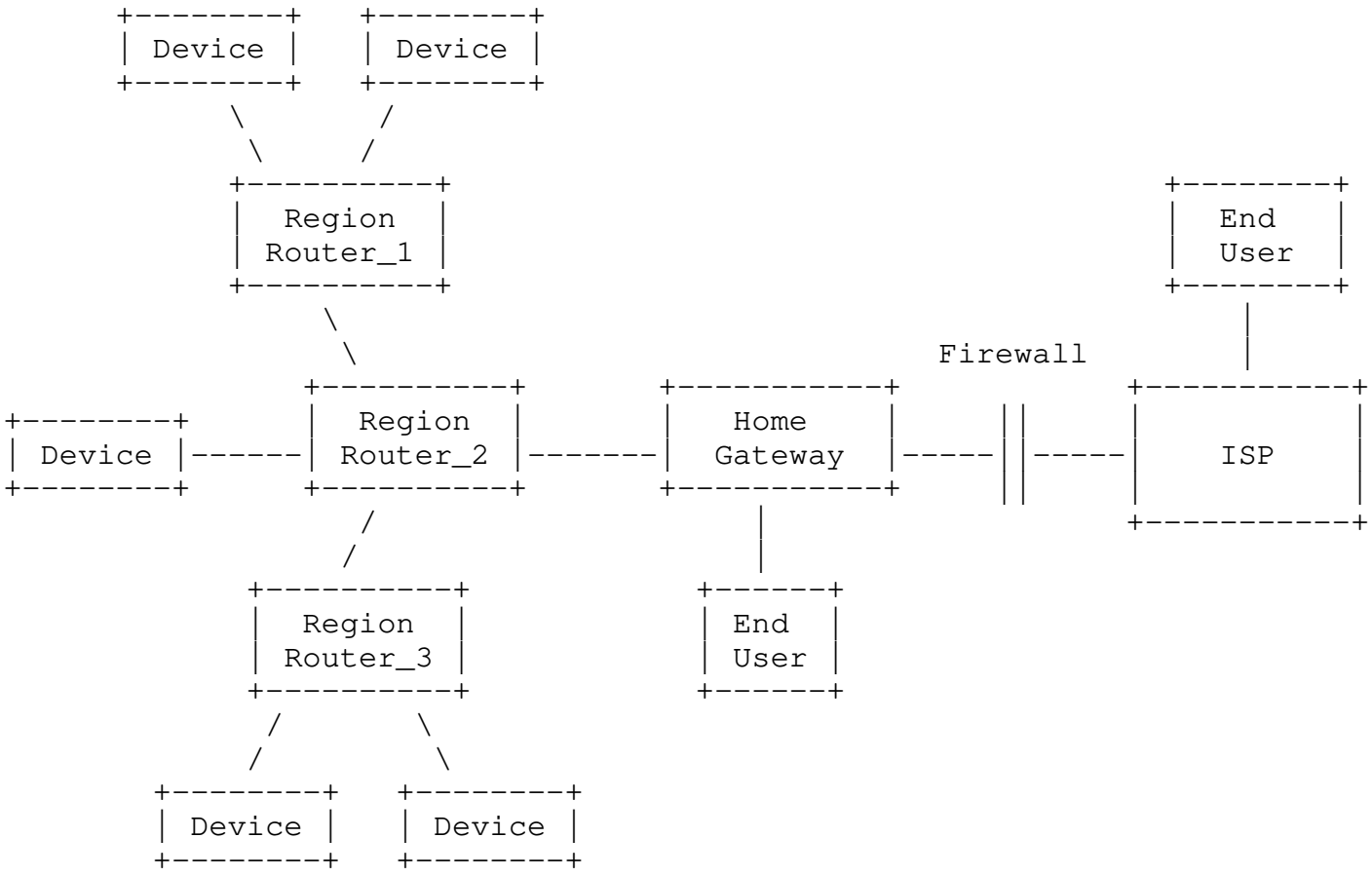
2.2. Homenet Architecture

Based on a state-of-the-art study, we propose following homenet topology as a basic model.

Homenet Gateway has the ability to pre-process and aggregation data and then sending to those interested devices. Homenet gateway will hold PIT, FIB and CS tables for sending corresponding message to region routers, consumers and outside networks.

Region routers are located at different regions which could be different rooms or floors. Normally one region will have one sub controller as long as the total number of devices is under the

capacity of the region router. Region routers only perform the role of collecting information and then send them all to the homenet gateway for further processing. They will have PIT, FIB and CS tables for sending corresponding message to devices.



Devices (sensors, applications, users, actuator and so on) are connected to their nearest region routers. Some of them, like sensors and users, will produce real time data packet and push them to their region routers. Some of the devices, such as applications and users which have special concern, will register their interests to region routers and home gateway. The rest kinds of end devices, like furniture and electric appliances, will wait for commands to adjust their behaviours. An end device can perform several roles, take a user as an example, the user can push heart beat rate as well as ask for room temperature information and then send control information to manipulate air condition.

ISP gateway: The homenet gateway connects to the Internet service provider (ISP) gateway, through which the homnet can connect to

application and end users, who have been authorized, at outside internet.

Devices that generate real time data, such as smoke sensor and temperature sensor, will be configured to periodically upload their data to a neighbouring region router. At the same time, those sensors can also respond to an interest massage to report their current readings.

Other devices that generate stream content, such as surveillance, will store stream data with sequence numbers and waiting for command from end user or application.

A client or application sends interests messages for services to be invoked and the results from service execution or state transitions are returned in data packet.

2.3. Homenet Naming

In smart home network scenario, data is not just retrieved, but can be processed before being presented to the user. Also end users and applications can deliver command content. So we propose to extent names not only for content but also for services to be invoked. Information generated inside a smart home has finite kinds of types. So it is sensible to tailor the naming strategy into the following structure:

'Access scope/service type/device scope/service API/'

In a service centric network, services may be restricted to only local access and/or set for global access through the Internet. Also, a service may have strict access control, and temporal or physical restrictions in terms of where it can accessed in the smart home network. So the first segment 'access scope' indicates who can access this service. The second level 'service type' shows the type of data and it can be instant content, stream content and command content. The third level 'device scope' can accurately locate device or a group of devices that provide this service. The final scope 'service API' identifies the functional primitives and attributes used to interact with the service which can be upload(), switch_on(), mode_1() and so on.

Following are examples of naming messages.

In order to collect all the smoke condition in the house, Fire Alarm broadcasts an instant content interest packet to the network with the name of

’/smarthome/instance/smoke/’

Smart home Application wants to get access to all the cameras on the second floor, a stream content interest is broadcasted to Router B with the name of

’/smarthome/stream/camera/2F’

Smart home Application wants to send a command to turn off all the lights on the second floor

’/smarthome/command/light/2F/set_state{OFF}’;

2.4. Homenet Routing

In this architecture, a router maintains a pending interest table (PIT) for outstanding forwarded requests, which enables request aggregation, to make sure that a router would normally not forward a second interest for a specific content in a particular time span. The PIT maintains state for all interests and maps them to MAC addresses, which are used as unique node identifiers. Data is then routed back on the reverse request path using this state. Service centric network architecture also supports on-path caching and name-based security.

The novelty of this architecture’s routing is reflected in the following aspects:

(1) Content pushing is more important than content pulling in some smart home scenarios, such as periodically uploading humidity data collected by sensors or flooding emergency messages triggered by fire alarms. These contents must be quickly disseminated toward the intended locations even though there is no request. Assuming that some sensors lack of storage capacity, the data collected by sensors are sent to the nearest router periodically via wire or wireless channel to leverage the large storage space of routers.

(2) A consumer uses interest packet to request content from the network. Following the naming scheme, the consumer declares the service type in the name of the interest. Interest packet is broadcasted to all the neighbouring routers. Different service types do not influence the maintenance of PIT table and the forwarding scheme, so the architecture has a good compatibility with other information centric architectures.

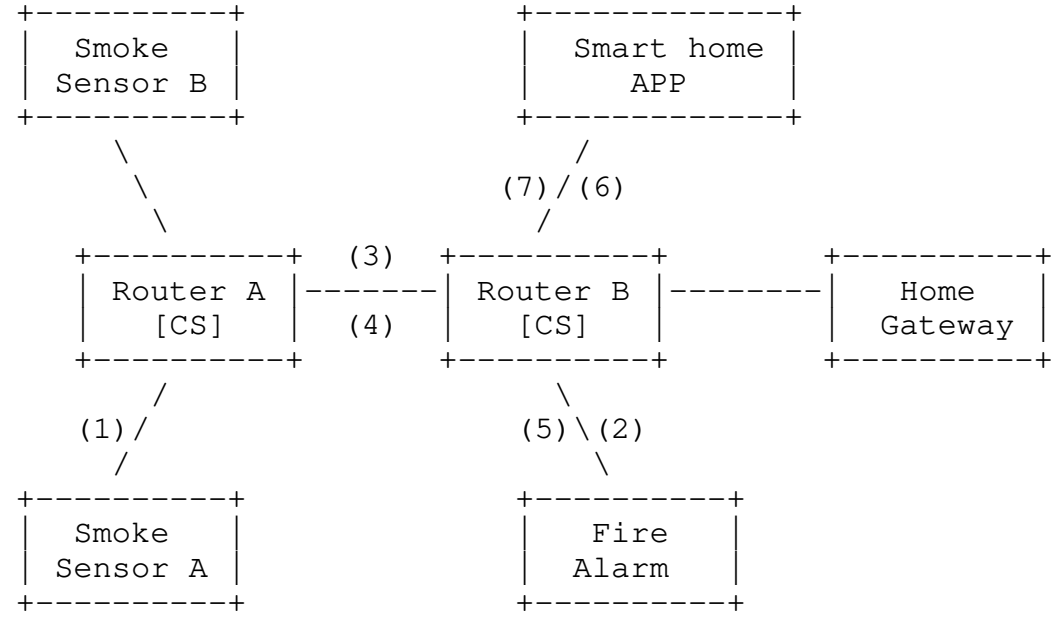
(3) To solve the problem of control message delivering, a novel mechanism is introduced. A command message generated by a controller is seen as an interest packet, known as command content interest.

The name of the interest is the device name which intends to be controlled. The content requested by the controller is the state of the device after the command is successfully delivered. The command content interest follows the same procedure as an ordinary interest to realize the delivery of a command. The command content can also be seen as the acknowledgement of a command message.

2.5. Use Cases

Three scenarios are discussed to demonstrate the feature of SCN when handling different services.

2.5.1. Smoke Monitering Service



STEP 1: Smoke Sensor A periodically uploads the instant smoke data to its neighbouring router to leverage the large storage space of Router A;

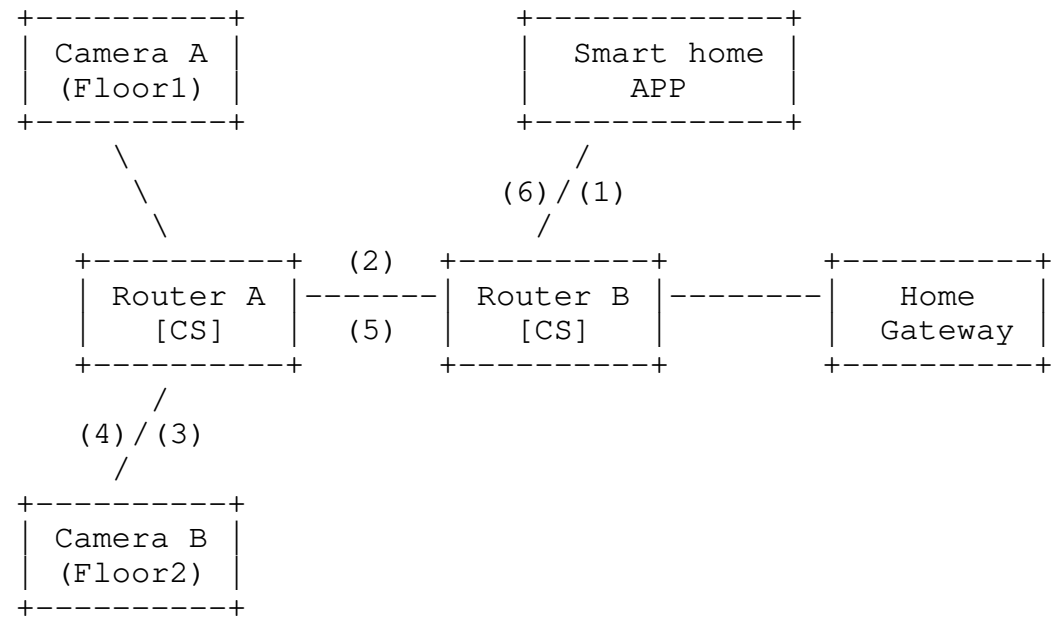
STEP 2: In order to collect all the smoke condition in the house, Fire Alarm broadcasts an instant content interest packet to the network with the name of '/smarthome/instance/smoke/';

STEP 3: On receiving the interest packet from Fire Alarm, Router B updates its PIT table and forwards it to Router A;

STEP 4 and 5: After Router A receives the interest packet from Router B, the instant smoke content is forwarded to Router B and Fire Alarm using the backward route;

STEP 6 and 7: Suppose that Smart home APP want to request all the instant monitoring data in the house, an interest packet is sent to Router B with the name of '/smarthome/instance/'. The smoke content data uploaded by Smoke Sensor A is forwarded to APP directly from Router B, thanks to the caching scheme of SCN.

2.5.2. Video Streaming Service



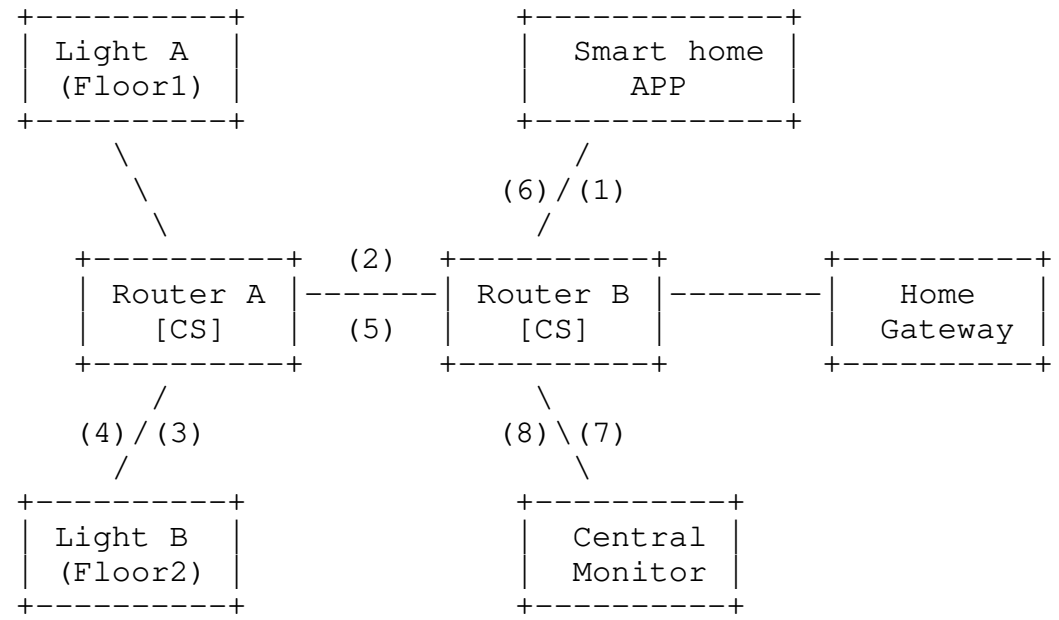
STEP 1: Smart home Application wants to get access to all the cameras on the second floor, a stream content interest is broadcasted to Router B with the name of '/smarthome/stream/camera/2F';

STEP 2: On receiving the interest packet, Router B updates its PIT table and forwards it to Router A;

STEP 3 and 4: On receiving the interest packet, Camera B send video stream content to Router with the name of '/smarthome/stream/camera/2F/caremaB' and an increasing sequence number;

STEP 5 and 6: The stream content is forwarded to Smart home Application using the backward route and is saved by Router A and Router B.

2.5.3. Command Delivering Service



STEP 1: Smart home Application wants to send a command (eg. turn off) to all the lights on the second floor, a command content interest is broadcasted to Router B with the name of '/smarthome/command/light/2F/' and with the service API's value of 'set_state{OFF}';

STEP 2: On receiving the interest packet, Router B updates its PIT table and forwards it to Router A;

STEP 3: On receiving the interest packet, Light B changes its state into OFF and return a content packet with the name of '/smarthome/command/light/2F/lightB' and with the service API's value of state{OFF}';

STEP 4, 5 and 6: The content packet is forwarded to Smart home Application using the backward route and is saved by Router A and B;

STEP 7 and 8: If the Central Monitor want to know the state of all the lights in the house, an interest packet is broadcasted with the name of '/smarthome/command/light/'. The state of Light B is forwarded to Central Monitor directly from Router B, thanks to the caching scheme of SCN.

2.6. Other Considerations

Mobility:

Sensor or end user move around (step between different networks or move between different regions), they may need to connect to different region routers. Mobility support for both service

producers and consumers is required to ensure best connectivity at all times. This includes nomadic movement, seamless mobility to handle real-time applications, and vertical handovers between different access networks as residents move in and out of their region premise.

Scalability:

One of the benefits for applying SCN rather than IP is that SCN could support as many devices as needed, while IPV4 or IPV6 could run out of available addresses.

Security:

A new device joins in (public key encrypt, private key decrypt to guarantee authority), information or data generated inside the smart home should keep confidential and private, and accessible through strict access control; it is safer to use SCN than IP architecture.

3. IANA Considerations

This document makes no specific request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

4. Informative References

[1] Braun, T. and V. Hilt, "Service-Centric Network", June 2011.

[2] Chown, T., "Home Networking Architecture for IPv6 (RFC7368)", October 2014.

Authors' Addresses

Bo Lv
CAEIT
11 Shuangyuan Road
Beijing, Beijing 100041
China

Email: lv1985bo@163.com

Yue Jia
CAEIT
11 Shuangyuan Road
Beijing, Beijing 100041
China

Email: jiayuebupt@163.com

Min Liang
CAEIT
11 Shuangyuan Road
Beijing, Beijing 100041
China

Email: liangmin82@163.com

Yaiyong Xie
CAEIT
11 Shuangyuan Road
Beijing, Beijing 100041
China

Email: caeitic@163..com