IPv4/IPv6 Basics

opensourcedomotics

Basic concepts of modern IP networking

28/09/14

Goesta Smekal
http://osdomotics.com

Smart-SARAH Definition

opensourcedomotics

Smart-SARAH is a proposed standard for home automation systems, defined by the OpenSourceDomotics Group.

It contains all aspects from the user interface down to the low level hardware layout of example devices. The entire design is based on freely available standards:

- OpenSource Software for firmware, low level interfaces, middleware and user interface
- OpenHardware making reference implementations freely available
- Internet standard protocols regulate communication

Smart-Sarah by Layer

opensourcedomotics

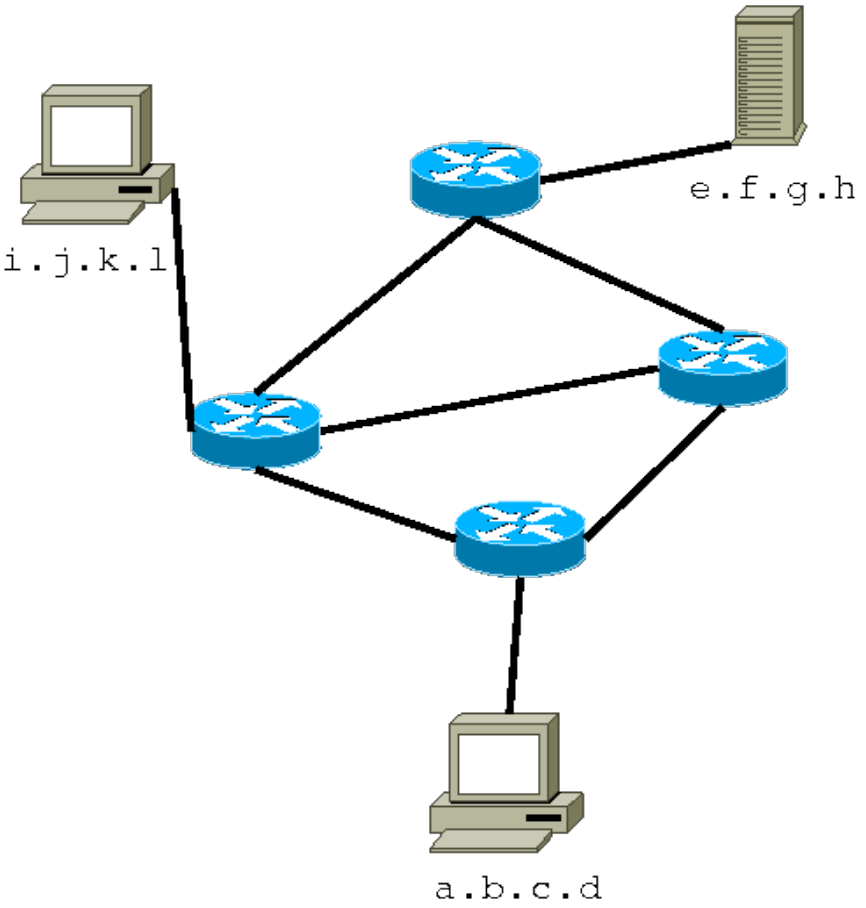
OSI Layer	Smart-SARAH	Comment
7 - application	KnxWeb	Web based GUI
6 - presentation	Linknx / OpenHAB	
5 - session	CoAP	Restful services
4 - transport	UDP	Low overhead
3 - network	IPv6	End to end communication, including encryprion/authentication
2 - data link	6LoWPAN	Low power radio
1 - physical	IEEE 802.15.4	2.4 GHz wireless communication

IP = Endpoint to Endpoint

opensourcedomotics

1980:

- IPv4 is the first network protocol to interconnect different networks regardless of the medium used
- globally unique addressing scheme
- any two nodes can communicate directly



Goesta Smekal
http://osdomotics.com

IPv4 Addressing

opensourcedomotics

- every node is identified by a four byte address
- networks are divided by subnet classes
  each class has a fixed number of network bits
- communication between nodes on different networks is established by routers

Class	Mask	Nets total	Nodes /net
A	/8	128	16777214
B	/16	16384	65534
C	/24	2097152	254

```
ns4.univie.ac.at
IP address: 131.130.249.82
network: 131.130.0.0/16
131.130.0.1-131.130.255.255
```

IPv4 Addressing

opensourcedomotics

CIDR “Classless Inter-Domain Routing”

- replaced classes in 1993
- subnets are divided by masks of any length (usually 8-29)
- reduces routing table size

`188.118.213.248/29` → `188.118.213.248...255`

Private address ranges (RFC 1918)

- may be used without registration
- will not be routed globally
- `10.0.0.0/8`
  `172.16.0.0/12`
  `192.168.0.0/16`
- may be subdivided as needed

Special IPv4 Addresses

opensourcedomotics

- local addresses:
  - local host: 127.0.0.1 – packets never leave the host
  - Network Address
    all host bits “0”: 131.130.0.0/16 → 131.130.0.0
  - Broadcast Address
    all host bits “1”: 131.130.0.0/16 → 131.130.255.255
- Gateways:
  Hosts can reach foreign networks across routers – every connected network has at least one router
  - Default Gateway: the router, connecting to “the Net” - address depends on the specific network, but must be within the range of the given class

Configuring IPv4

opensourcedomotics

manual configuration:

- local IP address per interface
- network and netmask
- default gateway and optional routes
- name server(s)
- time server(s)
- file server(s)
- ...

dynamic configuration

- DHCP server provides required information (UDP ports 67,68)
- DHCP client sends broadcast packet “DHCP request” with its MAC address
- server answers with “DHCP reply” to clients MAC address

IPv4 Vulnerabilities

opensourcedomotics

- initially security was no concern to IP networks
- source and destination addresses can easily be faked
- packet payload can be read/altered by any intermediate system
- arbitrary amounts of traffic can be sent to any destination (denial of service)
- within a growing internet, privacy and security became an ever growing issue

IPv4 Security

opensourcedomotics

Network Layer:

- Packet filters on routers (“Firewalls”)
  - filter by source/destination
  - by protocol
  - by UDP/TCP port
  - by payload (“deep packet inspection”)

Transport Layer:

- IPSec (IP security extensions)
  - Authentication: cryptographically signed headers
  - Encryption: encrypted payload

Application Layer:

- SSL “secure sockets layer” (aka HTTPS)

IPv4 = Endpoint to Endpoint ?

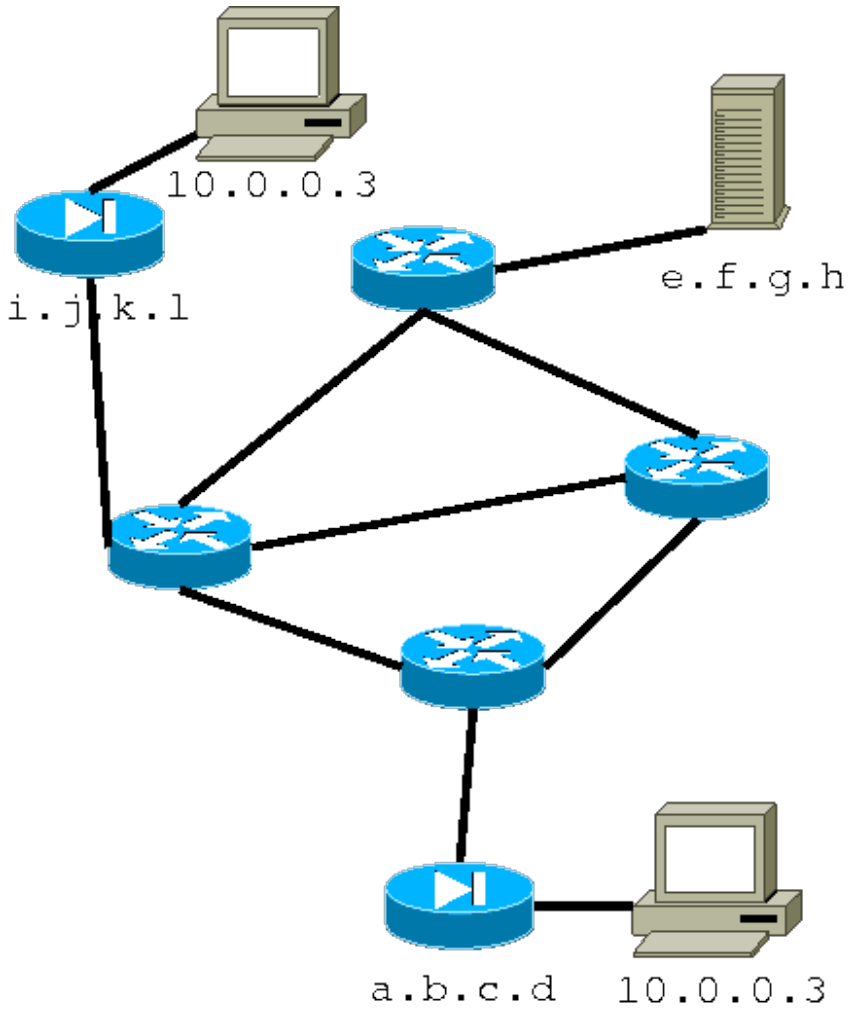
opensourcedomotics

currently:

direct connections are usually prohibited by:

- Firewalls
- NAT (due to shortage of IPv4 addresses)

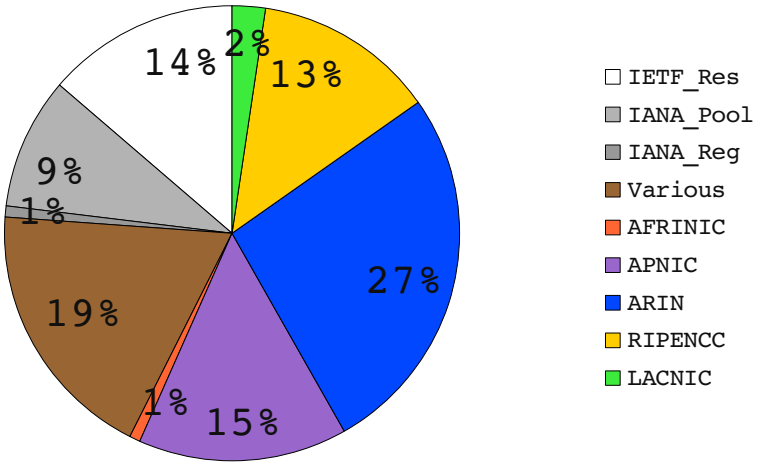
E2E only by assistance of a third party



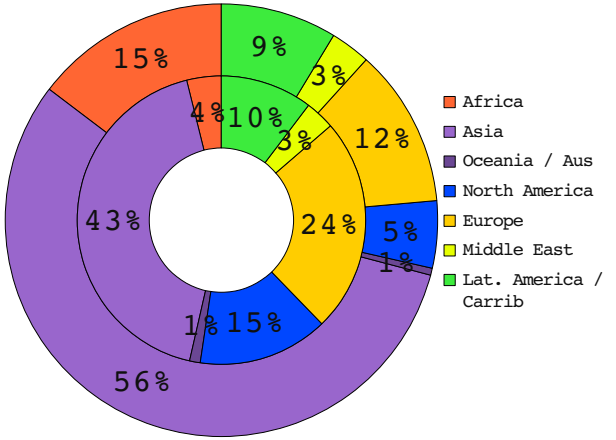
Goesta Smekal
http://osdomotics.com

Internet use vs. IPv4 addresses

opensourcedomotics



World Regions	Pop / Mio	Inet Users / Mio	Penetration (% Population)	Users % of Table
Africa	991,00	**67,37**	6.8 %	3.9 %
Asia	3808,07	**738,26**	19.4 %	42.6 %
Europe	803,85	**418,03**	52.0 %	24.1 %
Middle East	202,69	**57,43**	28.3 %	3.3 %
North America	340,83	**252,91**	74.2 %	14.6 %
Latin America/Caribbean	586,66	**179,03**	30.5 %	10.3 %
Oceania / Australia	34,70	**20,97**	60.4 %	1.2 %
WORLD TOTAL	6767,81	**1733,99**	**25.6 %**	100.0 %



Goesta Smekal
http://osdomotics.com

Anatomy of an IPv6 address

opensourcedomotics

- 128 Bit -> 16 Byte -> 8 blocks hexadecimal
- leading zeroes may be omitted
- one continuous block of zeroes may be replaced by "::"
- shortest IPv6 address: 127.0.0.1(IPv4) -> ::1(IPv6)

examples:

2001:0db8:1104:6100:0000:0000:0000:0001

2001:db8:1104:6100::1 ✓

2001:0db8:1104:0000:0000:4bd3:0000:0ac3

~~2001:db8:1104::4bd3::ac3~~ ✘

2001:db8:1104::4bd3:0:ac3 ✓

Goesta Smekal
http://osdomotics.com

IPv6 Prefixes

opensourcedomotics

like CIDR,IPv6 networks are defined by prefixes and subnet masks:

- `fe80::230:5ff:febe:3084/64`
  `fe80:0000:0000:0000:0230:05ff:febe:3084`
- `2001:858:0002::/48`
  `2001:0858:0002:0000:0000:0000:0000:0000`

the smaller the prefix, the larger the network

end users should typically be provided with:

- /64 -> one network containing 2^64 hosts
- /56 -> 256 networks, 2^64 hosts each

IPv6 Address Types

opensourcedomotics

- link local (`fe80::/10`) only valid within the local
  - network → will never be routed
- unique local IPv6 unicast (`fd00::/7`) (site local)
  - globally unique (40Bit random ID, 16Bit Subnet, 64Bit Interface) but not globally routable (like RFC 1918)

IPv6 Address Ranges

opensourcedomotics

- global unicast (`2000::/3`)

  `2001:0000::/32` Teredo (tunnel broker)
  `2001:db8::/32` documentation only
  `2002::/16` `6to4`

- multicast (`ff00::/8`)
  `ff02::1` all Nodes (link local)
  `ff02::2` all Routers

- anycast
  packet gets delivered to the closest member
  Example: subnet-router anycast: `2001:5c0:1104:6100::`

Goesta Smekal
http://osdomotics.com

Special IPv6 Addresses

opensourcedomotics

- Multicast by Scope:
  `ff01::x` same interface
  `ff02::x` same subnet
  `ff05::x` site local
  `ff0e::x` global
- other multicast groups:
  all nodes: `ff0x::1`
  all routers: `ff0x::2`
  all NTP servers: `ff0x::101`
- IPv4 in IPv6
  `::ffff:192.168.0.21`

Goesta Smekal
http://osdomotics.com

Handling IPv6 Addresses

opensourcedomotics

How to type IPv6 addresses?

- Don't do it. Use DNS ;-)
- `[fe80::210:a4ff:fe88:ecd]:80`
  (z.B. in webbrowsers, beware of shell escapes!
  `'[...]'`)

matching, using regular expressions (i.e. Perl):

- `m/\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}/`
  this won't work!
- `NetAddr::IP->version($IP)`
  use special libraries instead!

ICMPv6

opensourcedomotics

more than just PING ...

- informational messages
  Echo Request, Echo Reply
- error messages
  Dest. unreachable, packet too big, time exceeded, parameter problem
- Neighbour Discovery (ND)
- Autoconfiguration
- Path MTU discovery
- Multicast listener/server discovery (IPv4: IGMP)

ICMPv6: ND

opensourcedomotics

- automatic configuration of addresses
  Neighbour solicitation, neighbour advertisement
  (link local and global unicast)
- resolve local prefix and router
  Router solicitation, Router advertisement
- Duplicate Address Detection (DAD)
- Link-Layer Address Resolution (IPv4: ARP)
- Secure Neighbour Discovery
  Routers use certificates, certification Path,
  cryptographically generated Addresses

ICMPv6: Autoconfiguration

opensourcedomotics

without DHCP: "stateless autoconfiguration"

- link local addr. created (fe80::/10) "tentative"
- join multicast group ff02::1 (all nodes) and "solicited-node"
- neighbour solicitation using tentative address as destination (DAD)
- router solicitation (ff02::2)
- prefix and routes resolved

IPv6 - Security

opensourcedomotics

- global unicast requires new network security concepts:
  - the Firewall is no longer at the perimeter
  - security policy has to be centrally managed across all clients within a network
  - isolation “guest” networks for untrusted hosts
- endpoint to endpoint IPSec – the perimeter is lost - forever
  - bad news for “firewall in a box” vendors

IPv6 - Privacy

opensourcedomotics

- link local and global unicast addresses usually contain clients MAC address
  - may be used for client-tracking
    - user may be identified, even if he uses a different network (notebook in a hotel room)
    - NIC may be identified -> device identified (vendor, model, ...)
  - this can be disabled:
    - DHCPv6 using a short lease time
    - privacy extensions create a pseudo random identifier every time the interface is initialized

IPv4 - IPv6 Transition

opensourcedomotics

- dual stack
  - node uses both protocol versions (especially important for publicly available services)
  - proxy handles connections
- tunnelling
  - 6to4 (requires an official IPv4 address)
  - Teredo/Tunnel Broker (can traverse NAT, uses tunnel server)
  - Tunnel Broker (s.o.)
  - 6RD (RFC 5569, free prefix, assigned by IANA)

Further Reading

opensourcedomotics

- allocated IPv4 netblocks:
  ftp://ftp.ripe.net/pub/stats/ripencc/membership/alloclist.txt
- general statistics about the internet:
  http://www.internetworldstats.com/stats.htm
- why we will run out of IPv4 addresses soon (for a long time now):
  http://www.potaroo.net/tools/ipv4/index.html
- various background information:
  http://www.tcpipguide.com