ANSI E1.17 – 2015 (R2020) Architecture for Control Networks – EPI 13. Allocation of Internet Protocol Version 4 Addresses to ACN Hosts

E1.17 Profile for Interoperability

Part of ANSI E1.17 – 2015 (R2020) approved by the ANSI Board of Standards Review on 23 March 2020.
This part has no substantive changes from the 2010 edition.

TSP document ref. CP/2004-1024-R2-draft-439:454M

ANSI E1.17 - 2010
Architecture for Control Networks – EPI 13. Allocation of Internet Protocol Version 4 Addresses to ACN Hosts

E1.17 Profile for Interoperability

TSP document ref. CP/2004-1024-R2-draft-439:454M

Revision History	
Revision R2-draft-439:454M	2011-04-29
Revision R2pre4	2005-10-13
Revision R2pre3	2005-06-21
Revision R2pre1	2005-06-16
Revision R1	2004-11-09

Abstract

Required techniques for allocation of *IPv4* addresses are specified. Some issues and pitfalls are discussed.

Table of Contents

ACN EPIs

ANSI E1.17-2010 is the “Architecture for Control Networks” standard [ACN]. It specifies an architecture – including a suite of protocols and languages which may be configured and combined with other standard protocols in a number of ways to form flexible networked control systems.

E1.17 Profiles for Interoperability (EPIs) are standards documents which specify how conforming implementations are to operate in a particular environment or situation in order to guarantee interoperability. They may specify a single technique, set of parameters or requirement for the various ACN components. They may also specify how other standards (including other EPIs) either defined within ACN or externally are to be used to ensure interoperability.

1. Introduction

This EPI specifies rules for three different standards which operate together to provide reliable automatic assignment of operable addresses to hosts which may be frequently moved between different networks and systems. These standards are Dynamic Host Configuration Protocol [DHCP], Dynamic Configuration of IPv4 Link-Local Addresses [IPv4LL] and Detecting Network Attachment in IPv4 [DHC-DNA].

While DHCP is well established, the other two standards are newly standardised versions of older techniques. Many systems implement something similar to IPv4LL they are often not fully compliant with the standard and will probably work in the majority of cases but may fail in some. DNA is even newer and while invaluable for equipment which is frequently moved between networks it is not implemented in any real sense in major operating systems at the time of writing.

2. Levels of Compliance

Since full compliance with the three standards involved is impractical until more implementations are available, this EPI defines three levels of compliance. These are denoted *EPI13-Full*, *EPI13-B* and *EPI13-C*. Separate rules may be specified for compliance to each of the different levels. Rules which do not explicitly state a level of compliance or which simply state "*EPI13*" or "*EPI13-Any*" shall apply for all compliance levels.

3. Rules

3.1. Detecting Network Attachment

The DNA specification [DHC-DNA] discusses issues concerned with detecting changes of network environment and specifies behavior. This is particularly relevant in ACN systems where devices may be moved often and where private addresses [PrivateIP] are commonplace. Many different networks are likely to be running the same private IP address range and a device being moved from one to another needs to detect the fact that its network environment has changed, despite the fact that its IP address may still appear valid (and may even be successfully renewed via DHCP).

Equipment conforming to *EPI13-Full* shall implement Detection of Network Attachment (DNA) in accordance with [DHC-DNA].

Equipment conforming to *EPI13-B* shall take action to detect whether existing IP configurations are valid at network attachment change events.

Equipment conforming to *EPI13-C* should take action to detect whether existing IP configurations are valid at network attachment change events.

Network change events shall include:

- Power on or system reset
- Cable plugged in
- Waking from sleep, suspend or hibernate
- Address conflict detection

3.2. DHCP Client

[DHCP] allows configuration and allocation of fully routable addresses in networks of small devices which do not necessarily have a user interface of their own.

Equipment conforming to *EPI13-Any* shall implement DHCP Client functionality for address assignment in accordance with [DHCP].

3.3. Link-Local Addressing

Link Local address allocaton [IPv4LL] allows working addresses to be automatically configured in the absence of any servers or centralised control.

Many operating systems including many versions of Apple MacOS and Microsoft Windows implement Link-Local address autoallocation schemes which are only partially compliant with the specification. These schemes will work in most cases but do not provide such a rigorous assurance of interoperability, particularly when many of them are mixed together on a network.

Equipment conforming to *EPI13-Full* shall assign IPv4 Link Local addresses in full compliance with [IPv4LL].

Equipment conforming to *EPI13-B* or *EPI13-C* should assign IPv4 Link Local addresses in full compliance with [IPv4LL] but may instead assign IPv4 Link Local addresses in the 169.254.x.x address space by a compatible scheme as implemented in recognised mainstream operating systems.

3.4. DHCP Server

Equipment is not required to implement DHCP server and a compliant system can function without one but DHCP gives benefits and DHCP servers will be found in many systems. However, a DHCP server which suddenly appears on a network can cause disruption if it leads to equipment losing functioning addresses (see Change of IP address below) and this must be preventable.

For example, a controller which includes a DHCP server is very likely to be introduced in some systems when they are already functioning – often at a critical time. The, operator needs to be in control of when that DHCP server becomes active and any ensuing disruption occurs.

To conform to *EPI13-Any*, equipment which provides DHCP server functionality on a network shall be configurable to disable that functionality.

3.5. Static Address Configuration, BOOTP, RARP

Addresses which are static and manually assigned, or are assigned via BOOTP or RARP can give rise to interoperability failures requiring re-configuration locally at each component. Assignment by these methods are therefore *not* compliant with *EPI13-Any*. However, many considerations here are still relevant in such non-compliant systems.

3.6. Choice of Address

To comply with *EPI13-Any*, system implementers/administrators shall not allocate addresses which are reserved or otherwise disallowed by IANA. They should allocate permitted addresses as assigned by IANA and where no specific IANA assigned addresses are available, they should either allocate private addresses [PrivateIP] to create private internets or can allow Link local addresses to be assigned by [IPv4LL].

4. Changes of IP Address

Change of IP address – and particularly loss of an IP address, even if another is substituted – is very disruptive in a working system. Connections which are broken may take time to re-establish and it may not be possible to re-establish them at all. In a control network this can mean sudden loss of control.

The kind of networks in which ACN operates however, are often subject to frequent changes, equipment is turned on and off, moved around and re-configured. Larger controllers which often implement the network server functions may also be turned off and on, or replaced. Use of backup controllers to provide security in the event of failure of the primary controller is common. In this environment, implementers must be careful and aware of the issues which can lead to disruption.

4.1. Abandoning an Address

Whether or not for specific reasons discussed here, to comply with *EPI13-Any* a host which ceases using a working IP address shall close any ACN connections using that address in an orderly manner (except if the address has already ceased functioning).

A reason code for this purpose is provided in SDT which indicates that sessions are being closed because of changes in the underlying protocol. This code indicates to other components that they may look for the same service via the discovery mechanism if they need to continue the interaction.

The host must ensure that any services advertised via any discovery mechanism (e.g. SLP, DNS-SD) using a discontinued address are revoked or changed to reflect a new working address.

In a system implemented according to the rules above, there are a number of reasons why an IP address which is in use may need to be abandoned. The principle ones are given below.

4.2. Loss of DHCP Address

Renewal Fails or is Refused

This can happen because the DHCP server has gone offline and the lease expires or because it refuses a renewal request.

It is usual to attempt renewal well before a lease expires. At this intermediate time being unable to find a DHCP server is not sufficient reason to stop using a valid address, but once the expiry time has elapsed, or if the server actively refuses a lease the address must be relinquished after closing connections and deregistering advertisments in accordance with Section 4.1, “Abandoning an Address”.

Those implementing or configuring DHCP servers should be aware of this and must consider the implications if the server goes offline or changes configuration. Do not re-configure servers so that leases will be refused except when any ensuing loss of connections on the network will do no harm. In general a server with a stable configuration and which is always available is the most satisfactory solution.

4.3. Local Configuration Change

Local changes (e.g. configuring a static address, forcing the release of a lease or other reconfiguration) are beyond the scope of this EPI. Operators should nevertheless be aware that they cannot simply change configuration without potential disruption.

4.4. Link-local Address Conflict

If equipment properly conforms to the Link-local specification, loss of address due to conflict will not occur with equipment coming on and off line one host at a time. Large numbers of hosts being powered up at once may give rise to clashes leading to extended time searching for an address, but this should not disrupt equipment which is already functioning unless network conditions lead to loss of lots of packets.

The one time when address conflict leading to re-allocation is probable is when two functioning networks with Link-local addresses are joined. This can happen not just by physical actions such as plugging two switches together, but also due to software actions which bridge networks together.

4.4.1. Spanning Tree

A particular case to be aware of is spanning-tree networks. The spanning tree algorithm can take sufficiently long that some sectors may already have working link-local addresses established before the algorithm completes.

4.5. Link-local to Routable Address Transition

If a host is functioning with a Link-Local address and a DHCP assigned or other routable address becomes available, when and how should the host start using the new address? There are rules and guidelines for this transition in [IPv4LL] which must be followed. The best action which is in accordance with [IPv4LL] is to operate both addresses side by side during a transition period. However, there are IP stacks – particularly some small embedded ones – which cannot operate with multiple addresses.

To comply with *EPI13-Any*, a host which can only support a single address on an interface shall change to a properly assigned routable address which becomes available (including those assigned by DHCP and subject to any authentication policy present) but should defer the change while any operations known to be critical are in progress using the former address.

Note that “advertising” an address as mentioned in [IPv4LL] includes service advertisements via any discovery mechanism (e.g. SLP, DNS-SD), therefore to comply with *EPI13-Any* a component with a Link-Local address which receives a routable address (e.g. via a DHCP server coming online) is required to update its service advertisements to the new address, even if it continues to use the Link-Local address as well.

5. Critical Periods

In entertainment technology networks (and many other control networks) there are known critical periods during which disruption of control must be avoided and other times at which some disruption for purposes of re-configuration is quite acceptable. Typically the critical periods are during active processing, for example while a show is running in an entertainment context.

The provisions in this section are guidance and apply to *EPI13-Any*.

5.1. DHCP Servers

Equipment incorporating DHCP server functionality should be configurable to set in advance the periods which are critical for control. In many cases this is a case of declaring a daily cycle.

DHCP servers should not issue leases which expire during critical periods. This should be an automatic default policy programmed by the manufacturer rather than left to the user or administrator configuring the server in the field.

DHCP servers which have been off-line or disabled, should not start offering leases during critical periods without explicit confirmation from an operator (with the exception of servers in multi-server systems which are properly synchronised with an functioning DHCP configuration before going live).

DHCP servers should always honor requests for renewal of leases during critical periods unless explicitly instructed by an operator.

DHCP servers should not offer different addresses in response to requests for renewal during a critical periods unless explicitly instructed by an operator.

5.2. Bridging Separate Link-Local Networks Together

System operators and administrators should be aware of the issue of address conflict when Link-Local addresses are used if two networks become bridged and of the actions which can cause such bridging. Any such action should be avoided during critical periods.

Equipment designers or programmers must be aware of programmed functions which could lead to bridging of previously separate networks and should not allow such actions to happen during critical periods without explicit instructions.

6. Discovery Considerations

To comply with *EPI13-Any* a component shall ensure that it is not advertising services using an address which is no longer functional. It must therefore withdraw or update all services advertised via any discovery mechanism (e.g. by SLP deregistration) which use the discontinued address.

To comply with *EPI13-Any* any component using an IPv4 Link-Local address shall not advertise that address outside the local link. This means that they cannot advertise a Link-Local address in any packet which will be sent off link by themselves or by a discovery mechanism, whether or not that packet is sent using a Link-Local source address. Steps must also be taken to ensure that any servers used in discovery (e.g. SLP's Directory Agents) do not pass advertisements containing link-local addresses outside the link, for example by configuring scopes or TTL values or by checks within the server code itself..

Definitions

IPv4	Internet Protocol version 4.

References

Normative

[ACN] Entertainment Services and Technology Association, [https://tsp.esta.org]. ANSI E1.17 - 2010. *Entertainment Technology - Architecture for Control Networks*.

[DHCP] Internet Engineering Task Force (IETF) [http://ietf.org/]. RFC 2131 [http://ietf.org/rfc/rfc2131.txt]. R. Droms. *Dynamic Host Configuration Protocol*. 1997.

[DHC-DNA] Internet Engineering Task Force (IETF) [http://ietf.org/]. RFC4436 [http://ietf.org/rfc/rfc4436.txt]. B. Aboba, J. Carlson, and S. Cheshire. *Detecting Network Attachment in IPv4 (DNAv4)*. March 2006.

[IPv4LL] Internet Engineering Task Force (IETF) [http://ietf.org/]. RFC3927 [http://ietf.org/rfc/rfc3927.txt]. Stuart Cheshire, Bernard Aboba, and Erik Guttman. *Dynamic Configuration of IPv4 Link-Local Addresses*. 2005.

[PrivateIP] Internet Engineering Task Force (IETF) [http://ietf.org/]. RFC 1918 [http://ietf.org/rfc/rfc1918.txt]. Y. Rekhter, B. Moskowitz, D. Karrenberg, J. de Groot, and E. Lear. *Address Allocation for Private Internets*. 1996.