Research & Vehicle Technology
"Infotainment Systems Product Development"

Feature – Internet Gateway v2

APIM Infotainment Subsystem Part Specific Specification (SPSS)

Version 1.0

UNCONTROLLED COPY IF PRINTED

Version Date: March 12, 2018

FORD CONFIDENTIAL

Revision History

Date	Version	Notes	
March 12, 2018	1.0	Initial Release	

Table of Contents

1 Overview

This document specifies the requirements needed to ensure IP connectivity and networking. It identifies the Internet Engineering Task Force (IETF) Request for Comments (RFC) related requirements. Sync 4 Wi-Fi function provides STA and AP functionality. IP connectivity must be supported to enable in vehicle software update and projection over Wi-Fi and other transports. Although the requirements may be relevant for other functions and entities, the current focus is Wi-Fi function in Sync.

2 Functional Definition

2.1 IG-FUN-REQ-299882/A-Internet Gateway

2.1.1 Requirements

2.1.1.1 IG-FUR-REQ-299885/A-Use of NAT

The system shall support acting as a NAT gateway for connected devices. Relevant RFCs include, but are not limited to, 1631 (The IP Network Address Translator (NAT)), 5382 (NAT Behavioral Requirements for TCP), 4787 (Network Address Translation (NAT) Behavioral Requirements for Unicast UDP), etc…

2.1.1.2 IG-FUR-REQ-299886/A-Network Addressing

The system shall support both IPv4 and Ipv6 network addressing standards.

2.1.1.3 IG-FUR-REQ-299887/A-IPv4 Private Addressing

All private addressing should correlate to the ranges laid out in RFC1918. Preferably, the 192.168.100/24 address space would be the chosen.

2.1.1.4 IG-FUR-REQ-299888/A-IPv6 Unique Local Addressing

All private addressing should correlate to the ranges laid out in RFC4193.

2.1.1.5 IG-FUR-REQ-299889/A-Standards Compliant DHCP

The DHCP server shall be compliant with RFC2131.

2.1.1.6 IG-FUR-REQ-299890/A-DHCP Lease Time

The minimum DHCP lease time shall be 3 days with an address pool size of at least 100.

2.1.1.7 IG-FUR-REQ-299891/A-DHCP service usage

The system shall support DHCP service as per RFC 2131 “Dynamic Host Configuration Protocol.”

2.1.1.8 IG-FUR-REQ-299892/A-Reserved Addresses (IPv4)

The DHCP service shall not assign the following addresses any default or reserved address such as the following addresses 192.168.100/24 Address Space:
192.168.100.1
192.168.100.2 – 192.168.100.50.

2.1.1.9 IG-FUR-REQ-299894/A-IPv4 Link Local Addressing

In instances where DHCP is not used for configuration of IPv4 clients then the system shall implement RFC3927 “Dynamic Configuration of IPv4 Link-Local Addresses” for addressing.

Note: Requirement is needed for applications such as Apple and Microsoft applications.

2.1.1.10 IG-FUR-REQ-299895/A-IPv6 Stateless Address Auto-configuration

In instances where DHCP is not used for configuration of IPv6 clients then the system shall implement RFC4862 “IPv6 Stateless Address Autoconfiguration” for addressing.

Note: Requirement is needed for applications such as Apple and Microsoft applications.

2.1.1.11 IG-FUR-REQ-299897/A-Reserved Addresses (IPv6)

The DHCP service shall not assign a subset of IPv6 addresses in the unique local addressing space selected for implementation.

Note: Requirement is needed for applications such as Apple and Microsoft applications.

2.1.1.12 IG-FUR-REQ-299899/A-DNS Based Service Discovery

The system shall be capable of interacting on a network where DNS Service Discovery is used. As such, the system shall implement RFC6763. This includes advertising of network services that the system itself hosts.

Note: Requirement is needed for applications such as Apple applications.

2.1.1.13 IG-FUR-REQ-299901/A-Ethical hack

A set of network Ethical Hacks shall be performed to explicitly call out the specific vulnerabilities in the networking subsystem. The results of these hacks may lead to further network requirements.

2.1.1.14 IG-FUR-REQ-299902/A-Default Firewall Ruleset

The default firewall rules SHALL be set to ensure the system's security requirements are met as defined by the system's security specification.

2.1.1.15 IG-FUR-REQ-299903/A-Open ports only for services in use

The firewall shall be dynamically modified to open and close specific ports as they are needed.

2.1.1.16 IG-FUR-REQ-299905/A-Threat Models

All network based services shall be threat modeled that is signed off on before deployment to production as specified by the system's security specification.

2.1.1.17 IG-FUR-REQ-299907/A-Ethical Hack for Services

All network based services shall undergo an ethical hack to further understand any security risks associated with the service as specified by the system's security specification.

2.1.1.18 IG-FUR-REQ-299909/A-Fuzz Testing

All network based services shall be fuzz tested to ensure they properly handle invalid and unexpected data as specified by the system's security specification.

2.1.1.19 IG-FUR-REQ-299911/A-IPSec Passthrough

The system shall support the passthrough of IPSec connections. The relevant RFC is RFC3715 (IPsec-Network Address Translation (NAT) Compatibility Requirements).

2.2 IG-FUN-REQ-299934/A-Carplay

2.2.1 Requirements

2.2.1.1 IG-FUR-REQ-299937/A-Management Information Base

The system SHALL support RFC 1213-MIB-II.

2.2.1.2 IG-FUR-REQ-299938/A-RFCs for IP Connectivity

The system SHALL support the relevant parts of the following RFCs

- RFC 791: Internet Protocol (IP), DARPA Internet Program, protocol specification, Sept 1981
- RFC 2460: Internet Protocol, Version 6 (IPv6), Dec 1998
- RFC 4193: Unique Local IPv6 Unicast Addresses, Oct 2005RFC
- RFC 793: Transmission Control Protocol (TCP), Sept 1981
- RFC 768: User Datagram Protocol (UDP), Aug. 1980
- RFC 826: An Ethernet Address Resolution Protocol (ARP),Nov. 1982
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6), Sept 2007
- RFC 2131: Dynamic Host Configuration Protocol (DHCP), Mar. 1997
- RFC 792: Internet Control Message Protocol (ICMP), DARPA Internet Program, Protocol specification, Sept. 1981
- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, Mar 2006
- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Dec. 1998
- RFC 3966: The tel URI for Telephone Numbers, Dec. 2004
- RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010
- RFC 1398: Definitions of Managed Objects for the Ethernet-like Interface Types, Jan. 1993

3 Appendix: Reference Documents

Reference #	Document Title
1	RFC 1631 “The IP Network Address Translator (NAT)”
2	RFC 5382 “NAT Behavioral Requirements for TCP”
3	RFC 4787 “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP”
4	RFC 1918 “Address Allocation for Private Internets”
5	RFC 4193 “Unique Local IPv6 Unicast Addresses”
6	RFC 2131 “Dynamic Host Configuration Protocol”
7	RFC 4862 “IPv6 Stateless Address Autoconfiguration”
8	RFC 6762 “Multicast DNS”
9	RFC 6763 “DNS-Based Service Discovery”
10	RFC 3715 “IPsec-Network Address Translation (NAT) Compatibility Requirements”