



TELECOM INFRA PROJECT

TIP OOPT DCSG

Requirements Document

TIP Greenlight

Technical Requirements For Disaggregated Devices Life-cycle Management

Authors

Victor López, PhD.

Technological Expert, Telefonica

victor.lopezalvarez@telefonica.com

José Antonio Gómez Atrio

Optical Transport & SDN Architect, Vodafone.

jose-a.gomez@vodafone.com

Manuel Julián López Murillo

IP&SDN Distinguished Engineer, Vodafone

manuel-julian.lopez@vodafone.com

João Gabriel Aleixo

Technology Specialist - Innovation & Technology, TIM Brazi

jaleixo@timbrasil.com.br

Samier Barguil Giraldo

Technological Expert, Telefonica

samier.barguilgiraldo.ext@telefonica.com

Juan Rodriguez Martinez

Technological Expert, Telefonica

juan.rodriguezmartinez@telefonica.com

Murat Mugan

Connectivity Deployment Manager, Facebook

muratm@fb.com

Contributors

Washington Correia

Senior Specialist - Innovation & Technology, TIM Brazil

wcorreia@timbrasil.com.br

Gokul Murali

Network Engineer, Facebook

gokulmurali@fb.com

Andy Furnell

Connectivity Technologies and Ecosystems Manager, Facebook

andyfurnell@fb.com

Luis Martin Garcia

Network Technologies and Ecosystems Manager, Facebook

luismg@fb.com

Diego Marí Moretón

Connectivity Technologies and Ecosystems Manager, Facebook

dmmorten@fb.com

Mahak Arora

Network Engineer, Facebook

mahakar@fb.com





Change Tracking

Date	Revision	Author(s)	Comment
25/02/2021	V1.0	All	Consolidated Version

Table of Contents

1.0 Introduction	8
1.1 Zero-Touch Provisioning (ZTP) Overview	9
1.2 Current ZTP Challenges	10
2.0 Disaggregated Devices Lifecycle	13
2.1 ZTP Use Case	13
2.2 Upgrade and Replacement Use Cases	15
3.0 Technical Solution Description	17
3.1 Functional Requirements for Disaggregated Devices	17
3.2 DHCP Mode of Operation	18
3.3 DHCP Server Discovery	20
3.4 DHCP Client Options	22
3.4 DHCP Server Options	23
3.5 DHCP Relay	26
4.0 ZTP Mode of Operation	28
4.1 HW Vendor ZTP Solution	28
4.2 SW Vendor ZTP Solution	30
5.0 References	33
Glossary	34
TIP Document License	35
Disclaimers	37



List of Figures

Figure 1. Traditional manual approach to device provisioning	10
Figure 2. ZTP-based automated provisioning	10
Figure 3. Configuration-centric	12
Figure 4. Inconsistent approach	12
Figure 5. Topology dependencies	12
Figure 6. Stage 1: Network OS installation	14
Figure 7. Stage 2: Software configuration	15
Figure 8. Layer 3 DHCP relay via in-band production network	18
Figure 9. Layer 2 DHCP via out-of-band network	19
Figure 10. DHCP over L2 VPN	19
Figure 11. DHCP over L3 VPN	20
Figure 12. ZTP Workflow	28

List of Tables

Table 1: Key characteristics of Automated Life-cycle Technologies	10
Table 2: DHCP Client Options	22
Table 3: DHCP Server Options	23



Introduction

Telecom Infra Project (TIP) operators are deploying thousands of disaggregated network devices to meet exponentially increasing demand for connectivity across the world. Increasingly, these deployments are happening in a variety of environments and locations; rural, urban, datacenters, street furniture and mast sites ...



1.0 Introduction

Traditional approaches to device provisioning are labor intensive, time consuming and prone to human error. They are no longer fit for purpose given the velocity and diversity of today's network deployments, and often require complex planning and co-ordination across multiple teams, functions, and organizations.

TIP Greenlight addresses these issues by the application of common and standards-based technologies:

- This first release of TIP Greenlight focuses on the initial deployment of network elements with disaggregated hardware (e.g. a router or a transponder) and software components ("disaggregated devices")
- Future iterations of TIP Greenlight will build upon the flexible and extensible mechanisms contained in this document to deliver additional use cases.

These full lifecycle management use cases will be developed in collaboration with TIP ecosystem partners, and will include other aspects such as automated upgrades, migrations and replacement of Network Operating Systems (NOS). A brief description of the use cases can be found below:

- **Zero-Touch Provisioning (ZTP)** is the process to deploy a NOS and a base configuration to a disaggregated device, so the device can enter in production without any human configuration. The ZTP process is done for the first time the device is turned on in the network.
ZTP is the first TIP Greenlight use case, and is described in this document.
- **NOS Upgrade.** NOS vendors periodically release new versions necessary to add new features/functionality, and to address possible software bugs and defects. These software artifacts can have several releases during a year; this demands the network operators are continually changing and upgrading a device's software to the latest stable version. The process to automatically move from one software release to another is what we define as the NOS Upgrade process.
NOS Upgrade will be covered in a future release of this document.
- **NOS Migration.** Disaggregated devices use common hardware infrastructure components that allow those devices to work as a carrier-grade network element.

However, several software vendors can provide the NOS running on top of that hardware infrastructure. Each NOS contains features such as Command Line Interface (CLI), NETCONF, or transport protocols support that can be common or unique between the vendors. The selection of the features included in each NOS highly relies on the technology's maturity: e.g. the IETF-defined IP/MPLS protocols such as LDP 20 years ago, while, newer technologies like EVPN are still under active development. Thus, an operator may need to migrate to a different NOS family to enable new feature support to meet specific demands from planning or sales teams. The NOS Migration use case allows the operator to automatically change the NOS software without any change in the physical element. *NOS Migration will be covered in a future release of this document.*

1.1 Zero-Touch Provisioning (ZTP) Overview

Traditional manual approach to device provisioning



Figure 1

ZTP-based automated device provisioning

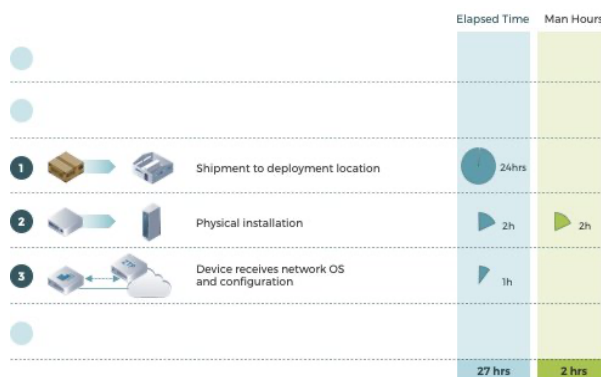


Figure 2

Automated life-cycle technologies make it simpler and more cost effective for operators to build and expand their networks, enabling greater velocity by making initial provisioning, upgrading and replacement of network devices more efficient.

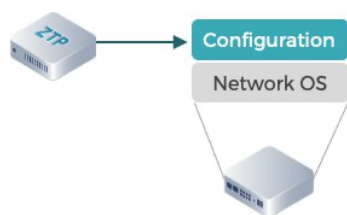
	Operator benefits	OEM benefits	Net outcome
Dynamic discovery of network connectivity	Eliminates manual configuration by field engineers	Minimizes factory pre-provisioning and customization	Network devices can be deployed more quickly
Use of machine to machine (M2M) interfaces	Reduces the risk of human errors due to command-line interactions	Reduced support burden due to avoidable configuration errors	Improved right first time outcomes
Automatic application of configuration	Physical install can occur without operator intervention	Simplified scope for FLM and other field activities	Increased volume and velocity of deployments

Table 1: Key characteristics of Automated Life-cycle Technologies

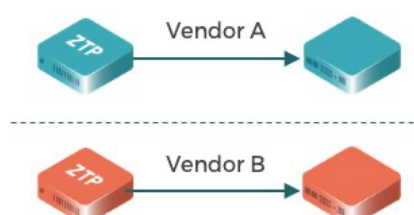
1.2 Current ZTP Challenges

While there are many existing implementations of ZTP, they are proprietary and not well suited for an increasingly diverse and complex range of deployment scenarios:

Configuration-centric



Inconsistent approach



Topology dependencies

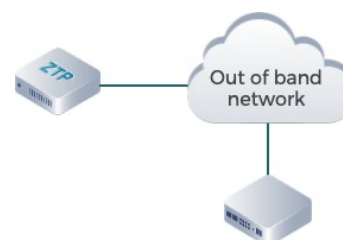




Figure 3

ZTP solutions have traditionally been focused on applying configuration only. The disaggregation of hardware and software means that ZTP must now also support provisioning of operating system software

Figure 4

A lack of standardization and consistency between implementations means operators must deploy and maintain multiple ZTP instances, increasing the cost and complexity of onboarding new vendors and solutions

Figure 5

Dependency on Out of Band (OOB) connectivity, which makes current ZTP solutions unsuitable for rural or access network deployments where a dedicated OOB network cannot feasibly be deployed

Industry has made some attempts to overcome these challenges (e.g. [RFC8572]), but these approaches are complex to implement, requiring a high degree of process integration between operators and OEMs. This TRS proposes a pragmatic, standards-based approach that addresses the specific challenges of disaggregated and agile networks, and which has been 'right sized' to minimize overhead for OEMs and operators alike.

2

Disaggregated Devices Lifecycle

TIP Greenlight lifecycle management enables the automated deployment, upgrade and migration of Network Operating System (NOS) and a base configuration to a disaggregated device....

2.0 Disaggregated Devices Lifecycle

Lifecycle management of disaggregated devices allows for the automated deployment, upgrade and migration of NOS and a base configuration to a disaggregated device. Thus, a router, transponder or other network element can enter the production network without any human manipulation.

2.1 ZTP Use Case

Zero-Touch Provisioning (ZTP) is the process to deploy a Network Operating System (NOS) and a base configuration to a disaggregated device. The ZTP process is automatically started by the device when it first boots and is connected to the existing infrastructure.

The ZTP solution enables the dynamic and automated provisioning of disaggregated devices and follows a two-stage process:

Stage 1: Network OS Installation

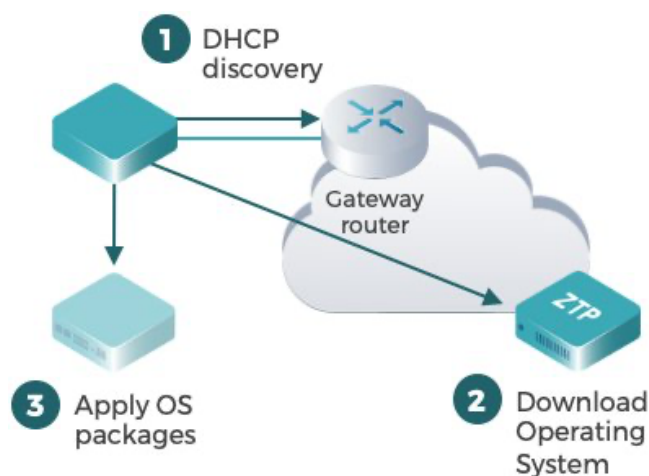


Figure 6

1. Once physical installation of a new or replacement disaggregated device is complete, the device negotiates its network access via DHCP, using any available connectivity. The DHCP server returns a link to the operating system package relevant to that device
2. The disaggregated device downloads the operating system package from the ZTP server using the provided link
3. The disaggregated device applies the software package and boots into the Network OS

Stage 2: Software Configuration Script

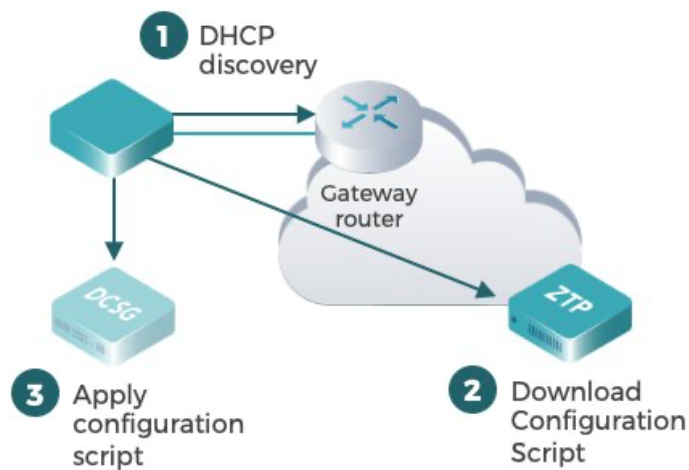


Figure 7

1. Once the Network OS has booted, the device negotiates a new DHCP session, and the DHCP server returns a link to the configuration script relevant to that node
2. The disaggregated device follows the link to download configuration script from the ZTP server using the provided link
3. The disaggregated device applies the configuration script and the ZTP process is complete

2.2 Upgrade and Replacement Use Cases

Nowadays, the NOS upgrade/replace process is a vendor dependent process, and the procedure differs between each vendor solution or specific NOS release. Future releases of TIP Greenlight will extend the ZTP process to support NOS upgrade and NOS replacement scenarios, allowing operators to automatically move from one software release to another in a standard way for open white-box scenarios.

3

Technical Solution Description

The requirements provided in this section describe client-side operations to be implemented by HW and SW vendors.

3.0 Technical Solution Description

This document captures the detailed requirements for Hardware Vendors (HW) and Software Vendors (SW) to participate in Zero Touch Provisioning (ZTP). These requirements cover not only the device configuration but also the NOS (Network Operating System) download and installation process.

The requirements provided in this section describe client-side operations to be implemented by HW and SW vendors. Associated server-side implications and implementation notes are also provided for consideration by operators.

3.1 Functional Requirements for Disaggregated Devices

The following requirements apply to all HW and SW vendor implementations of the ZTP solution:

1. The disaggregated device must send the DHCP options per the specification in this document, to allow the device to be identified uniquely by the DHCP server
2. The disaggregated device must support ZTP on both in-band and OOB interfaces
3. The disaggregated device must generate informative logging and debugging messages at all stages of the ZTP process
4. Logging messages about the ZTP process must be stored to local disk for later retrieval/transfer, and available in real-time via operator console, and export to a remote syslog server as specified during the DHCP discovery process
5. The disaggregated device must support manual operator intervention to stop the ZTP process via the console
6. The disaggregated device must support DHCP relay once configured to provide DHCP to other in-band connected disaggregated devices

3.2 DHCP Mode of Operation

The following section describes the DHCP topologies supported by the ZTP solution, the DHCP server discovery process, and the use of DHCP options to discover the ZTP server.

DHCP Topologies

To facilitate the ZTP process, operators must provide network connectivity for the disaggregated device towards the DHCP and ZTP servers. In some cases, this connectivity is provided using a dedicated out-of-band network. Where such out-of-band connectivity is unavailable, disaggregated devices more commonly rely on 'in-band' connectivity provided by existing network elements.

Layer 3 DHCP relay via in-band production network

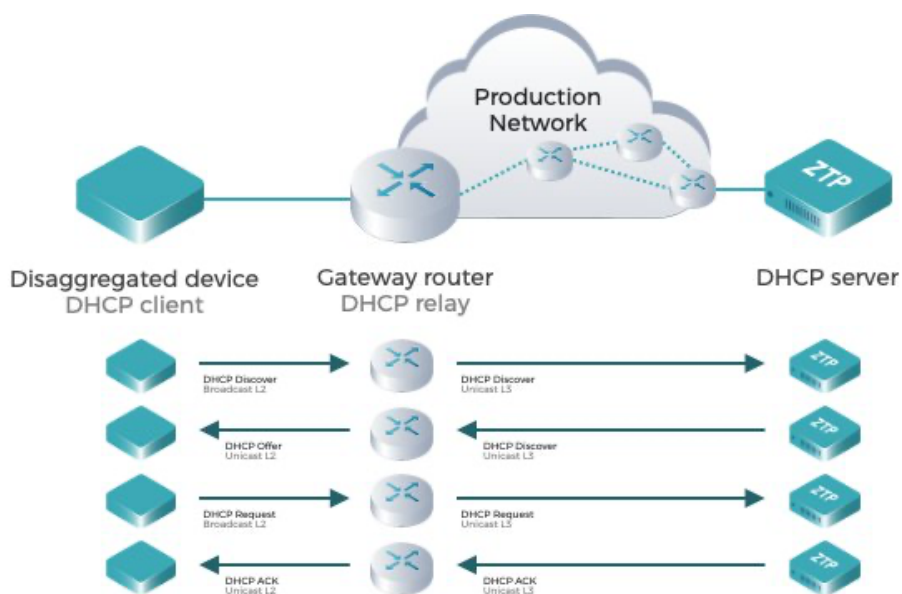


Figure 8

Layer 2 DHCP via out-of-band network

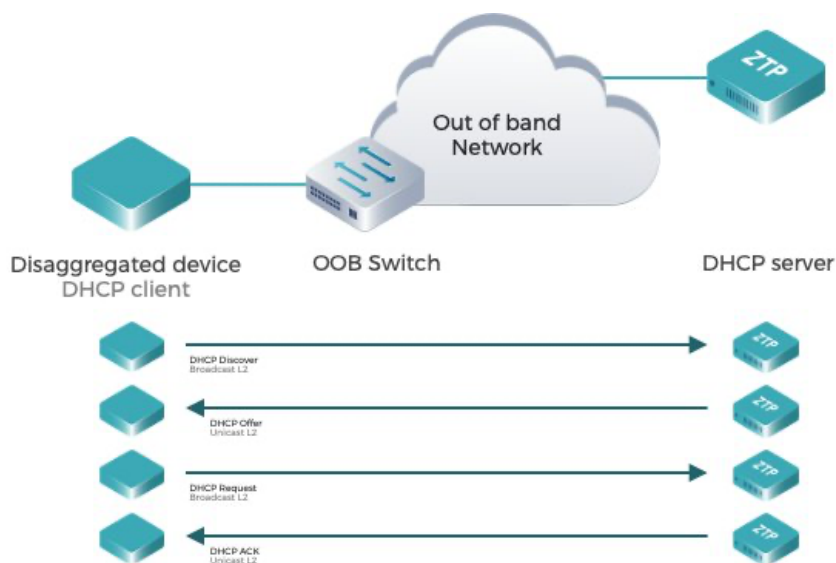


Figure 9

Depending on the topology of the network, the DHCP server may be visible directly at layer 2, or may be reachable via an intermediate layer 3 DHCP relay function according to one of the scenarios depicted below:

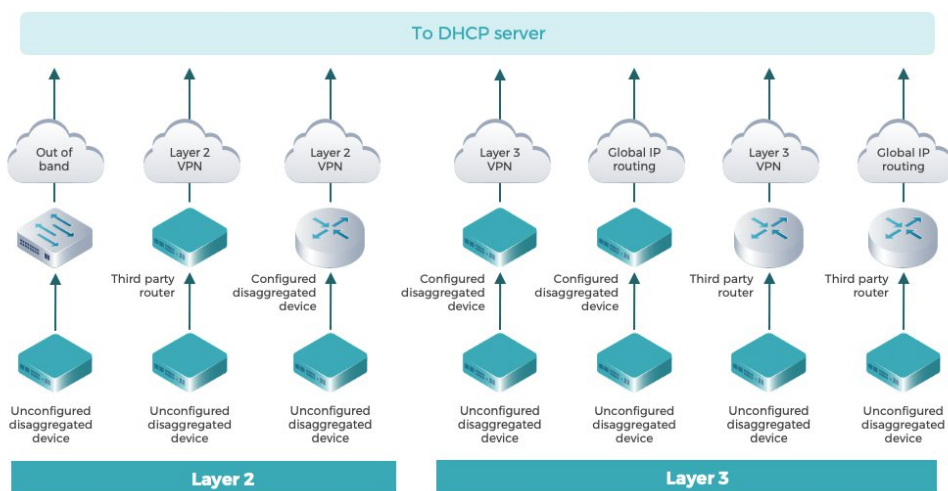


Figure 10: DHCP over L2 VPN

Layer 2 connectivity is most typically associated with out of band via an existing out of band switch but may also be provided using an L2VPN over in-band connectivity. The layer 3 scenario enables the use of in-band connectivity to mitigate the need for additional devices (e.g. management switches) and/or dedicated out of band connectivity to complete the ZTP process. Layer 3 connectivity may be provided in an L3VPN, or via the global routing table. The DHCP relay function may be provided by an existing third-party network element, or via an existing disaggregated device. Accordingly, NOS vendors provide DHCP relay agent functionality in accordance with the relevant technical requirements specification to support this use case.

3.3 DHCP Server Discovery

The DHCP server may be reachable by any port on the device, depending on operator requirements and design. To promote deterministic behaviors, disaggregated devices must first attempt DHCP discovery via the out-of-band interface, and then try in-band ports in ascending numerical order until an IP address has been successfully negotiated.

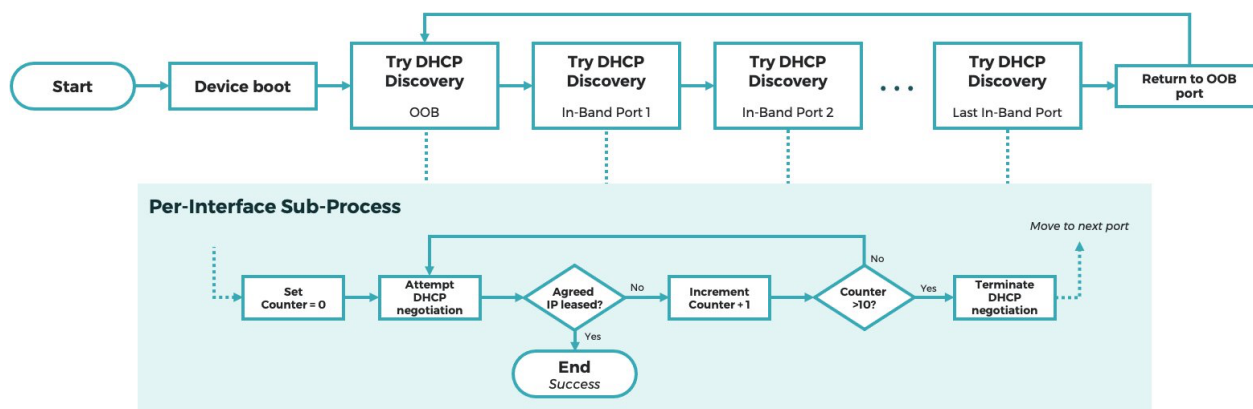


Figure 11: DHCP over L3 VPN

The following requirements apply to the DHCP discovery process:

- Disaggregated devices must only attempt DHCP discovery on interfaces with an active link



- Where a given interface can support multiple line protocols (e.g. 1GE/10GE/25GE on SFP28 interfaces, 40GE/100GE on QSFP28 interfaces), supplier documentation must state the default line protocol configuration applied to each interface
- Disaggregated devices must attempt 10 DHCP discover messages on each interface, implementing the retransmission algorithm according to [RFC2131] (section 4.1)
- Where no IP address has been negotiated on a given interface after 10 retries, the DHCP discovery process must be terminated before attempting the next interface
- Where no IP address has been negotiated for any interface, the discovery process should restart, beginning once again with the out-of-band interface.
- The DHCP Server could be configured to provide fixed or infinite lease expiration time.

DHCP Options and ZTP Server Discovery

The ZTP solution uses DHCP options to signal information to/from the disaggregated device. This approach inherits many characteristics from the [ONIE image discovery and execution](#) process and has been tailored to meet the specific needs of disaggregated network devices.

3.4 DHCP Client Options

Disaggregated devices send the following DHCP options when initiating DHCP discovery:

DHCP Option Code	DHCP Option Name	Description
60	Class Identifier	Vendor type information describing the make and model of the disaggregated device
61	Client Identifier	Unique identifier for each disaggregated device
55	Parameter Request List	Set of fields requested by DHCP client from the DHCP server.

Table 2: DHCP Client Options

DHCP Client Option 60 - Class Identifier

The DHCP client uses option 60 to send vendor type information to the DHCP server. The DHCP server then uses this value to determine which NOS should be returned to the disaggregated device. The class identifier string must be compliant with the [ONIE specifications](#) and is the concatenation of two strings, separated by the colon (:) character:

1. The static string `onie_vendor`
2. `<arch>-<vendor>-<machine>-r<machine_revision>`

For example: `onie_vendor:x86_64-VENDOR_MACHINE-r0`

DHCP Client Option 61 - Client Identifier

The DHCP Client uses option 61 to send the client identifier to the DHCP Server. The client identifier contains a unique identity for the disaggregated device and is assigned by the vendor. The client identifier is defined as the concatenation of a unique vendor

identifier, and a unique device identifier:

1. The vendor identifier used is the IANA-allocated enterprise ID for the device
2. The device identifier used is the serial number associated with the device:

The two identifiers are separated by the colon character and encoded into a single string. For example: 52587:WE61A7.

DHCP Client Option 55

The DHCP client uses option 55 to send a list of parameters it expects from the DHCP. The parameter list must include all relevant DHCP server options from the section below.

3.4 DHCP Server Options

The DHCP server returns the following values to the disaggregated device:

DHCP Option Code	DHCP Option Name	Description
1	Subnet Mask	Subnet Mask information.
3	Default Gateway	Default Gateway information
7	Logging server	Syslog server IP address information
28	Broadcast Address	Broadcast Address information.
51	IP Address Lease Time	IP Address Lease Time information
54	DHCP Server Identity	DHCP Server Identity information
114	Default NOS URL (HW solution only)	URL to the ZTP server to download the Network Operating System (NOS)
240	Default Config URL (SW solution only)	URL to the ZTP server to download the SW configuration script

Table 3: DHCP Server Options



DHCP Server Option 1

The DHCP server uses option 1 to send the subnet mask information associated with the assigned client address. The disaggregated device uses this information to configure the network interface.

DHCP Server Option 3

The DHCP server uses option 3 to send default gateway information. The disaggregated device uses this information to configure a default route that will be used to access the ZTP server.

DHCP Server Option 7

The DHCP server uses option 7 to send details of the ZTP syslog server. If the DHCP server sends option 7, the disaggregated device must export its ZTP logs remotely to the server specified using the syslog protocol defined in [RFC5424]. UDP encapsulation (specified in [RFC5426]) must be used by default. Where no option 7 value is provided, the disaggregated device only stores logs locally.

DHCP Server Option 28

The DHCP server uses option 28 to send broadcast address information. The disaggregated device uses this information to configure the network interface.

DHCP Server Option 51

The DHCP server uses option 51 to send IP address lease time information. The disaggregated device must initiate appropriate DHCP renewal behaviors (in accordance with [RFC2131]) with respect to this lease time.

DHCP Server Option 54

The DHCP server uses option 54 to send DHCP server identity information. The

disaggregated device uses this information for DHCP renewal and release activities.

DHCP Server Option 114

Note, DHCP option 114 is only required for the HW vendor solution.

The DHCP server uses option 114 to send the URI to the ZTP server to download the Network Operating System (NOS). This usage is in line with the ONIE specification (see [ONIE-Discovery]). The option 114 value is formatted in accordance with [RFC3986], and disaggregated devices must support a minimum of HTTP, HTTPS and TFTP URI schemes, and use of IP-addressed hosts. By extension, the ZTP server may use HTTP, HTTPS or TFTP. The following are example of valid option 114 strings:

```
http://192.0.2.0/TIP/HW-Vendor-x/VENDORx_NOS_INSTALLER
https://192.0.2.0/TIP/HW-Vendor-x/VENDORx_NOS_INSTALLER
tftp://192.0.2.0/TIP/HW-Vendor-x/VENDORx_NOS_INSTALLER
```

Where an HTTPS URI is returned, the disaggregated device must support a minimum of TLS version 1.2 as defined in [RFC5246]. Other TLS versions and/or implementations may be provided in addition to TLS 1.2 should vendors wish to do so. HTTPS clients must allow for the use of self-signed SSL certificates on the ZTP server.

DHCP Server Option 240

Note, DHCP option 240 is only required for the SW vendor solution.

The DHCP server uses option 240 to send the URI to the ZTP server to download the configuration script. The option 240 value is formatted in accordance with [RFC3986], and disaggregated devices must support a minimum of HTTP, HTTPS and TFTP URI schemes, and use of IP-addressed hosts. By extension, the ZTP server may use HTTP, HTTPS or TFTP. The following are example of valid option 240 strings:

```
http://192.0.2.0/TIP/SW-Vendor-y/VENDORY_CONFIG_SCRIPT.py
https://192.0.2.0/TIP/SW-Vendor-y/VENDORY_CONFIG_SCRIPT.py
tftp://192.0.2.0/TIP/SW-Vendor-y/VENDORY_CONFIG_SCRIPT.py
```

Where an HTTPS URI is returned, the disaggregated device must support a minimum of TLS version 1.2 as defined in [RFC5246]. Other TLS versions and/or implementations may be provided in addition to TLS 1.2 should vendors wish to do so. HTTPS clients must allow for the use of self-signed SSL certificates on the ZTP server.

3.5 DHCP Relay

Disaggregated devices must support DHCP relay functions as specified in [RFC2131]. DHCP relay can be configured by operators to provide in-band connectivity to a remote DHCP server in support of the [Layer 3 scenario](#) described earlier in this document.

4

ZTP Mode of Operation

The following sections describe the processes implemented by disaggregated devices. This includes NOS download and installation by HW vendor solutions, and configuration script download and execution by SW vendor solutions ...

4.0 ZTP Mode of Operation

The following sections describe the processes implemented by disaggregated devices. This includes NOS download and installation by HW vendor solutions, and configuration script download and execution by SW vendor solutions.

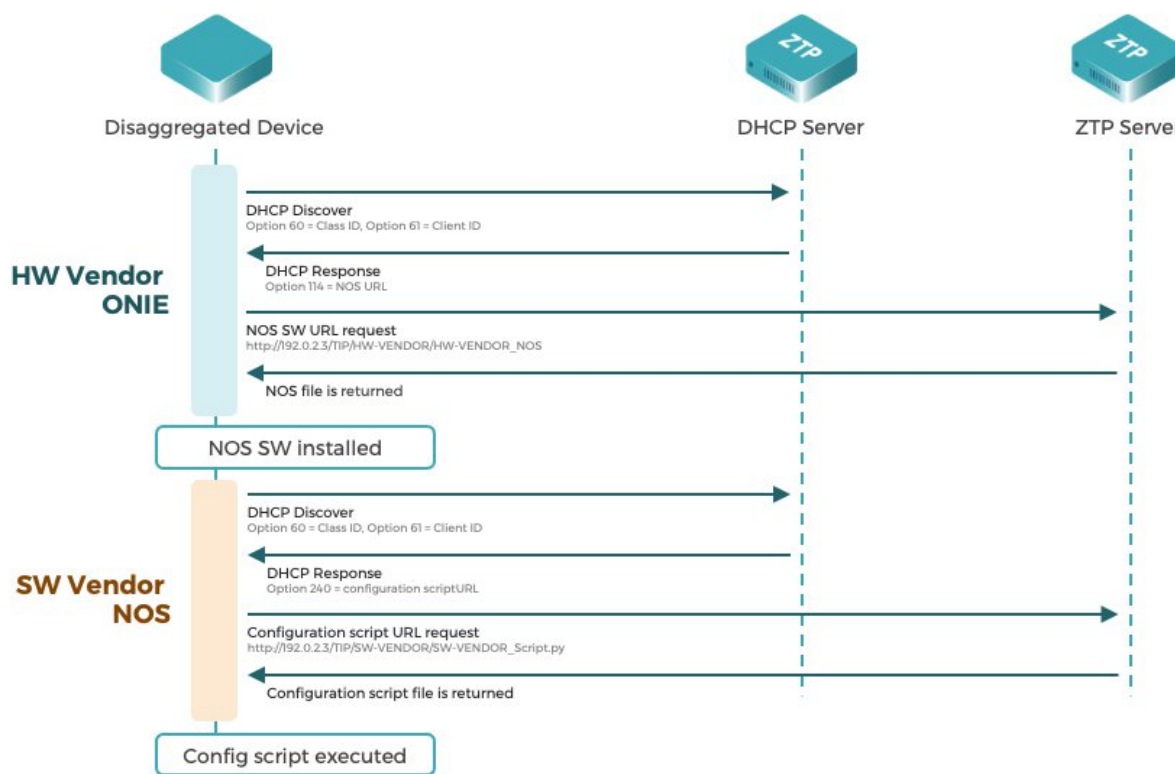


Figure 12: ZTP Workflow

4.1 HW Vendor ZTP Solution

Entry state: The disaggregated device comes shipped with ONIE installed but does not yet have a Network Operating System (NOS). The disaggregated device boots with the pre-loaded Open Network Install Environment (ONIE) from the HW vendor.

The disaggregated device initiates the [DHCP discovery process](#) described above to obtain an IP address, and to discover the URL for the NOS. The URL is returned in DHCP

option 114, and this option must be specified in the DHCP parameter request list (DHCP option 55).

Since the vendor, model and specific device identity are all exchanged during this process, the ZTP URL returned by the DHCP server specifies the most suitable NOS for each device. The DHCP server configuration snippet below demonstrates how vendor class identifier can be used to return a different NOS package for each HW vendor/model:

```
# Apply SW vendor 1 NOS to Edgecore-26x
class "onie-Edgecore-26x" {
    match if substring(option vendor-class-identifier, 0, 40) =
"onie_vendor:x86_64-accton_as7316_26xb-r0";
    option default-url = "http://192.0.2.7/TIP/SW-Vendor1/SW1_dNOS_INSTALLER";
}

# Apply SW vendor 2 NOS to Edgecore-27x
class "onie-Edgecore-27x" {
    match if substring(option dhcp-client-identifier, 0, 40) =
"onie_vendor:x86_64-accton_as7315_27xb-r0";
    option default-url = "http://192.0.2.7/TIP/SW-Vendor2/SW2_CNOS_INSTALLER";
}

# Apply SW vendor 3 NOS to Ufispac-30x
class "onie-Ufispac-30x" {
    match if substring(option vendor-class-identifier, 0, 41) =
"onie_vendor:x86_64-ufispac_s9500_30xs-r0";
    option default-url = "http://192.0.2.7/TIP/SW-Vendor3/SW3_OcNOS_INSTALLER";
}
```

For further background information about the above snippet, see the configuration documentation for ISC DHCP server (<https://www.isc.org/dhcp/>).

The disaggregated device configures its network interface and routing table using the information returned from the DHCP server and downloads the NOS file from the specified URL. Once the NOS file has been downloaded, the file checksum is validated, and the software package is installed to the device.



4.1.1 Exception Handling

In the event the NOS file could not be accessed via the specified URL, or in the event the download is interrupted, the device must retry the download using the same URL. In the event the file has not been successfully downloaded after 5 retries, or in the event the software installation fails for any reason, the device must return itself to a clean state and begin the DHCP discovery process again. Example failure scenarios may include (but are not limited to):

- File corruption/checksum failure
- Incompatibilities between NOS and the HW device
- Interruptions during the NOS installation process (e.g. power failure)

4.2 SW Vendor ZTP Solution

Entry state: The disaggregated device has successfully downloaded and installed its Network Operating System (NOS). The device boots up with the freshly installed NOS.

The disaggregated device initiates the [DHCP discovery process](#) described above to obtain an IP address, and to discover the URL for the configuration script. The URL is returned in DHCP option 240, and this option must be specified in the DHCP parameter request list (DHCP option 55).

Since the vendor, model and specific device identity are all exchanged during this process, the ZTP URL returned by the DHCP server may be specific to the unique device or may be a standardized/templated configuration applied to a given HW vendor/model. The DHCP server configuration snippet below demonstrates how vendor class identifier and client ID values can be used to achieve these different use cases:

```
# Generic configuration script based on vendor class ID
class "onie-Edgecore-26x" {
    match if substring(option vendor-class-identifier, 0, 40) =
"onie_vendor:x86_64-accton_as7316_26xb-r0";
    option 240 = "http://192.0.2.7/TIP/config/GENERIC_CONFIG_SCRIPT.py";
}

# Device-specific configuration script based on client ID (serial number
only)
class "onie-WE61A7" {
    # match 52587:WE61A7
    match if substring(option dhcp-client-identifier, 6, 6) = "WE61A7";
    option 240 = "http://192.0.2.7/TIP/config/WE61A7_CONFIG_SCRIPT.py";
}

# Device-specific configuration script based on client ID (vendor ID + serial
number)
class "onie-52587-WE61A7" {
    # match 52587:WE61A7
    match if substring(option dhcp-client-identifier, 0, 12) = "52587:WE61A7";
    option 240 = "http://192.0.2.7/TIP/config/52587-WE61Q7_CONFIG_SCRIPT.py";
}
```

The disaggregated device configures its network interface and routing table using the information returned from the DHCP server and downloads the configuration script file from the specified URL. Once the file has been downloaded, the script is executed by the NOS. If the configuration script cannot be downloaded from the URL, the disaggregated device must generate informative log messages, and re-attempt the download up to a maximum of 5 times. After 5 times, the ZTP process should be terminated and the device returned to its default configuration and terminal.

For clarity, the default configuration must enable the SSH feature and include default administrator credentials made available to the operator, such that an administrator can log in to restart the ZTP process and/or address any exceptions that may have caused the configuration script to fail.



4.2.1 Exception Handling

Disaggregated devices must log any outputs or errors generated during execution of the configuration script file. Logs are stored locally and may be exported to a syslog server if the DHCP returns an appropriate value DHCP option 7.

5.0 References

- [RFC2131] Dynamic Host Configuration Protocol - <https://tools.ietf.org/html/rfc2131>
- [RFC3315] Dynamic Host Configuration Protocols for IPv6 (DHCPv6) - <https://tools.ietf.org/html/rfc3315>
- [RFC3986] Uniform Resource Identifier (URI): Generic Syntax - <https://tools.ietf.org/html/rfc3986>
- [RFC4361] Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DPCHv4) - <https://tools.ietf.org/html/rfc4361>
- [RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2 - <https://tools.ietf.org/html/rfc5246>
- [RFC5424] The Syslog Protocol - <https://tools.ietf.org/html/rfc5424>
- [RFC5426] Transnission of Syslog Messages over UDP - <https://tools.ietf.org/html/rfc54246>
- [RFC8572] Secure Zero Touch Provisioning (SZTP) - <https://tools.ietf.org/html/rfc8572>
- [ONIE-Discovery] ONIE image discovery and execution specification
<https://opencomputeproject.github.io/onie/design-spec/discovery.html>

Glossary

3R's	Reshaping, Reamplification, Retiming	MNO	Mobile Network Operator
API	Application Programming Interface	NOS	Network Operating System
DCI	Data Center Interconnection	OCP	Open Compute Project
CAPEX	Capital Expenditure	OLS	Open Line System
DCN	Data Communication Network	ONIE	Open Network Install Environment
DWDM	Dense Wavelength Division Multiplexing	OTN	Optical Transport Network
EOE	Electrical-Optical-Electrical	ROADM	Reconfigurable Optical Add-Drop Multiplexer
FEC	Forward Error Correction	SAN	Storage Area Network
GE	Gigabit Ethernet	SDH	Synchronous Digital Hierarchy
HAL	Hardware Abstraction Layer	SDN	Software Defined Network
HW	Hardware	SW	Software
LO/L1	Layer 0 and Layer 1	TAI	Transponder Abstraction Interface
LAN	Local Area Network	TRS	Technical Requirement Specification
MAN	Metropolitan Area Networks	WDM	Wavelength Division Multiplexing
NMS	Network Management System	ZTP	Zero Touch provisioning



TIP CONFIDENTIAL

This document contains TIP Confidential Information as defined in Article 1 of the TIP Bylaws. Subject to Sections 17.1 and 17.2 of the TIP Bylaws, use and disclosure of the document and its contents are strictly prohibited.

Copyright © 2021 Telecom Infra Project, Inc. All rights reserved.

The Telecom Infra Project logo is a trademark of Telecom Infra Project, Inc. (the “Project”) in the United States or other countries and is registered in one or more countries. Removal of any of the notices or disclaimers contained in this document is strictly prohibited.

The publication of this document is for informational purposes only. THIS DOCUMENT IS PROVIDED “AS IS,” AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. UNDER NO CIRCUMSTANCES WILL THE PROJECT BE LIABLE TO ANY PARTY UNDER ANY CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER LEGAL OR EQUITABLE THEORY, FOR ANY INCIDENTAL INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR FOR ANY COMMERCIAL OR ECONOMIC LOSSES, WITHOUT LIMITATION, INCLUDING AS A RESULT OF PRODUCT LIABILITY CLAIMS, LOST PROFITS, SAVINGS OR REVENUES OF ANY KIND IN CONNECTION WITH THE SUBJECT MATTER OR USE OF THIS DOCUMENT.

TIP Document License

By using and/or copying this document, or the TIP document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, display and distribute the contents of this document, or the TIP document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted under the copyrights of TIP and its Contributors, provided that you include the following on ALL copies of the document, or portions thereof, that you use:



1. A link or URL to the original TIP document.
2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice (hypertext is preferred, but a textual representation is permitted) of the form: "Copyright 2019, TIP and its Contributors. All rights Reserved"
3. When space permits, inclusion of the full text of this License should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of TIP documents is granted pursuant to this License. except as follows: To facilitate implementation of software or specifications that may be the subject of this document, anyone may prepare and distribute derivative works and portions of this document in such implementations, in supporting materials accompanying the implementations, PROVIDED that all such materials include the copyright notice above and this License. HOWEVER, the publication of derivative works of this document for any other purpose is expressly prohibited.

For the avoidance of doubt, Software and Specifications, as those terms are defined in TIP's Organizational Documents (which may be accessed at <https://telecominfraproject.com/organizational-documents/>, and components thereof incorporated into the Document are licensed in accordance with the applicable Organizational Document(s).




Disclaimers

THIS DOCUMENT IS PROVIDED "AS IS," AND TIP MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

TIP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name or trademarks of TIP may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with TIP and its Contributors. This TIP Document License is based, with permission from the W3C, on the W3C Document License which may be found at <https://www.w3.org/Consortium/Legal/2015/doc-license.html>.



Copyright © 2020 Telecom Infra Project, Inc. A TIP Participant, as that term is defined in TIP's Bylaws, may make copies, distribute, display or publish this Specification solely as needed for the Participant to produce conformant implementations of the Specification, alone or in combination with its authorized partners. All other rights reserved.

The Telecom Infra Project logo is a trademark of Telecom Infra Project, Inc. (the "Project") in the United States or other countries and is registered in one or more countries. Removal of any of the notices or disclaimers contained in this document is strictly prohibited.



TELECOM INFRA PROJECT