August 2021

ZERO TOUCH PROVISIONING OF RESILIENT ETHERNET PROTOCOL RINGS

Ramesh R

Sonal Shah

Nipun Joy

ZERO TOUCH PROVISIONING OF RESILIENT ETHERNET PROTOCOL RINGS

AUTHORS:
Ramesh R
Sonal Shah
Nipun Joy

ABSTRACT

When a network device comes online, a fair amount of manual configuration needs to take place before the device is fully functional. Day Zero techniques automate such processes, bringing network devices into a functional state with minimal- to no-touch. However, today a resilient Ethernet protocol (which for convenience may be referred herein to as 'REP') does not support Day Zero technologies, since by design there is no support for this requirement at the protocol level. Consequently, current REP ring provisioning requires manual intervention, is time consuming, and involves high operational cost. To address these types of challenges, techniques are presented herein that support configuring REP rings with zero-touch technologies. Aspects of the techniques presented herein introduce a new type-length-value (TLV) encoding scheme to the existing REP Link Status Layer (LSL) protocol data unit (PDU) to carry special flags and Plug and Play (PnP) information.

DETAILED DESCRIPTION

In the narrative that is presented below, reference is made to a Resilient Ethernet protocol. Such a protocol, which for convenience may be referred to as 'REP,' may provide a number of benefits (such as, for example, fast network and application convergence) and may provide an alternative to the Spanning Tree Protocol (STP).

When a network device like a router or a switch comes online, a fair amount of manual configuration needs to take place before the device is fully functional. Day Zero techniques automate these processes, bringing network devices into a functional state with minimal- to no-touch.

Vendor-supplied Plug and Play (PnP) solutions provide a simple, secure, unified, and integrated offering for enterprise and industrial network customers to ease device

rollouts for provisioning updates to an existing network. A device's operating system (OS) may support different Day Zero technologies including, for example, network PnP, Zero Touch Provisioning (ZTP), and the Preboot eXecution Environment (PXE). However, none of those technologies support the REP configuration today in the industry. Such a requirement becomes more pertinent in today's environment where it is important to avoid 'truck roll' situations and bring up the network as much as possible. The REP today will not be able to support Day Zero technologies since by design it blocks the REP ports which have no REP neighbors during the neighbor discovery phase (to be discussed in detail below).

Challenges such as those that were described above are addressed by aspects of the techniques presented herein which support, for example, making the REP configurable with Day Zero technologies.

It is important to note that during the balance of the narrative that is presented below, the specific Day Zero technology that is referred to will be PnP. Additionally, the solution that is offered by aspects of the techniques presented herein is applicable to all Day Zero technologies that wish to deploy REP.

When a new device is onboarded with PnP a number of steps are typically required. Various of those steps are described below and illustrated in Figure 1.

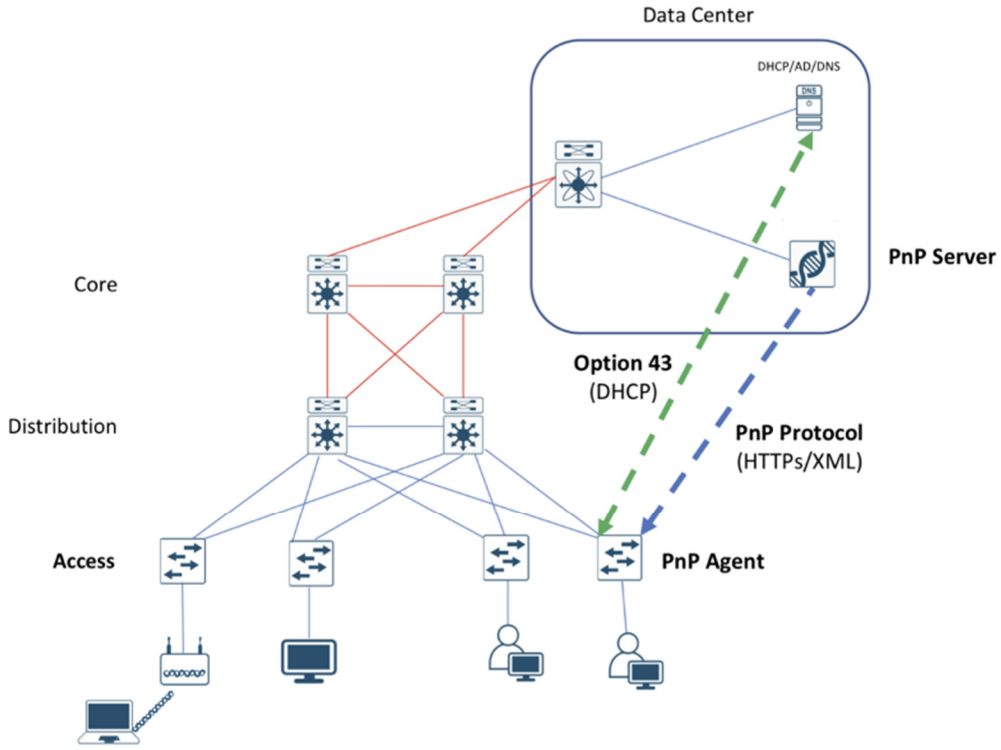

Figure 1: Illustrative Device Onboarding Activities

A device with no startup configuration in the device's Non-volatile random-access memory (NVRAM) triggers a PnP agent to initiate a Dynamic Host Configuration Protocol (DHCP) discovery process which acquires from a DHCP server the Internet Protocol (IP) configuration that is required for the device.

The DHCP server can be configured to insert additional information, using the vendor-specific option code 43, upon receiving option code 60 from the device with the string 'vendor pnp' to pass on the IP address or the hostname of the PnP server to the requesting device. When the DHCP response is received by the device, the PnP agent extracts the option code 43 information from the response to obtain the IP address or the hostname of the PnP server. The PnP agent may then use the IP address or hostname to communicate with the PnP server. Finally, the PnP server downloads the required Day Zero configuration details on to the device to complete the provisioning.

Figure 2, below, further illustrates aspects of the onboarding steps, in particular the site provisioning steps (e.g., after a remote installer completes mounting and cabling a

device and then powers it on), the Day Zero steps (e.g., various pre-provisioning activities), and the Day One steps (e.g., a network administrator remotely monitoring a device's health).

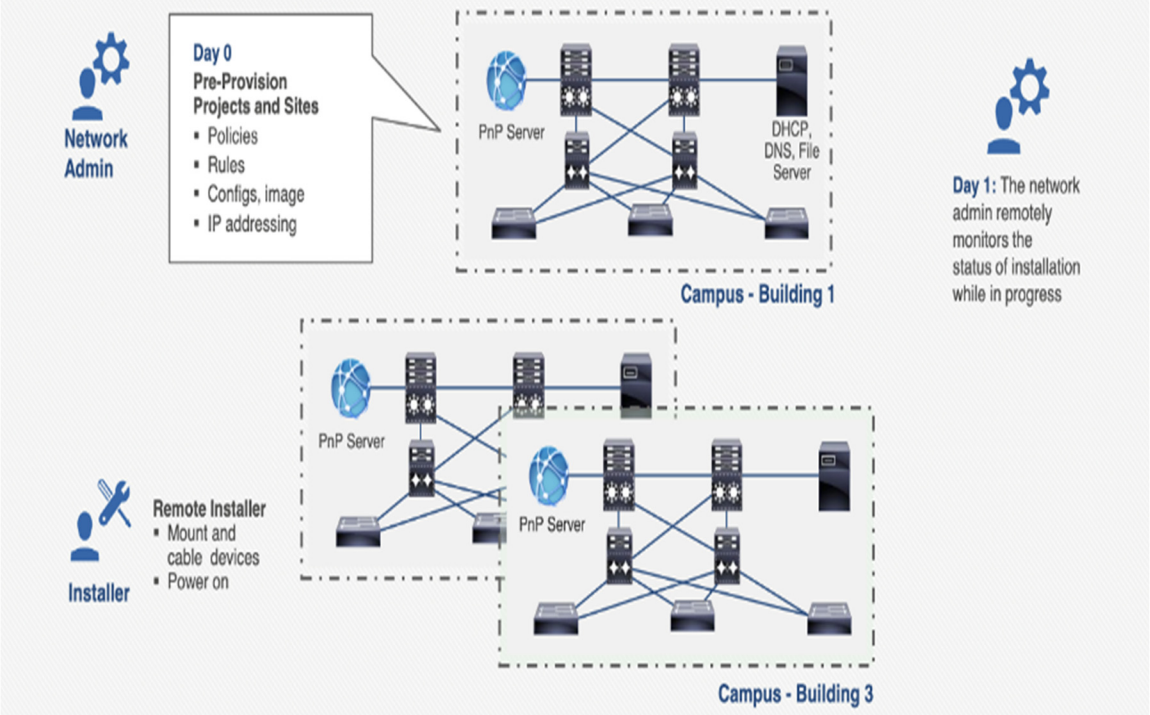

Figure 2: Illustrative Device Onboarding Steps

Figure 3, below, depicts various of the steps that may be included during Day Zero provisioning.

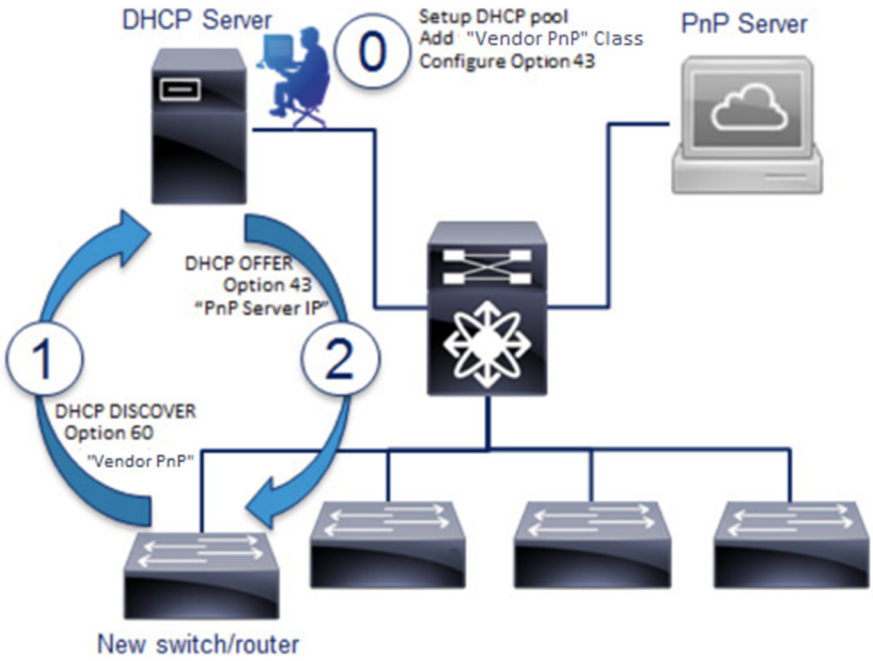

Figure 3: Exemplary Day Zero Provisioning Steps

As illustrated in Figure 3, above, and as described previously, Day Zero provisioning may encompass a series of steps. Various of those steps are described in the following narrative.

During a first step, a networking device is cabled and powered on. Since the startup configuration in the device's NVRAM is empty, a PnP agent is triggered and sends a 'vendor pnp' in a DHCP option code 60 in a DHCP DISCOVER message.

During a second step, an administrator configures a DHCP server to send the PnP server IP address in an option code 43. For example:

```
ip dhcp pool PNP-POOL
network 172.19.210.0 255.255.255.0
default-router 172.19.210.1
option 43 ascii "5A;K4;B2;I172.19.210.215;J80"
```

During a third step, the DHCP server matches the 'vendor pnp' in option code 60 and sends the configured string (as shown in Step 0 in Figure 3, above) in an option code 43. Such a string is interpreted by the PnP agent and the PnP server IP address is decoded.

During a fourth step, the PnP server then pushes the desired Day Zero configuration on to the device. A typical Day Zero network, which will be illustrated below, may

comprise daisy-chained switches mostly running some flavor of a spanning tree protocol. But PnP does not support the zero-touch provisioning of the REP. Due to the way REP is designed, there is no way to roll out such a protocol with PnP today on Day Zero. Accordingly, aspects of the techniques presented herein support a solution that takes care of the Day Zero provisioning of REP rings using a new type-length-value (TLV) encoding scheme.

Aspects of the techniques presented herein may be explicated through the following description of a typical use case scenario for provisioning REP ring.

Under the illustrative use case, the first nodes that are to be provisioned are Access 1 and Access 2, as depicted in Figure 4, below.

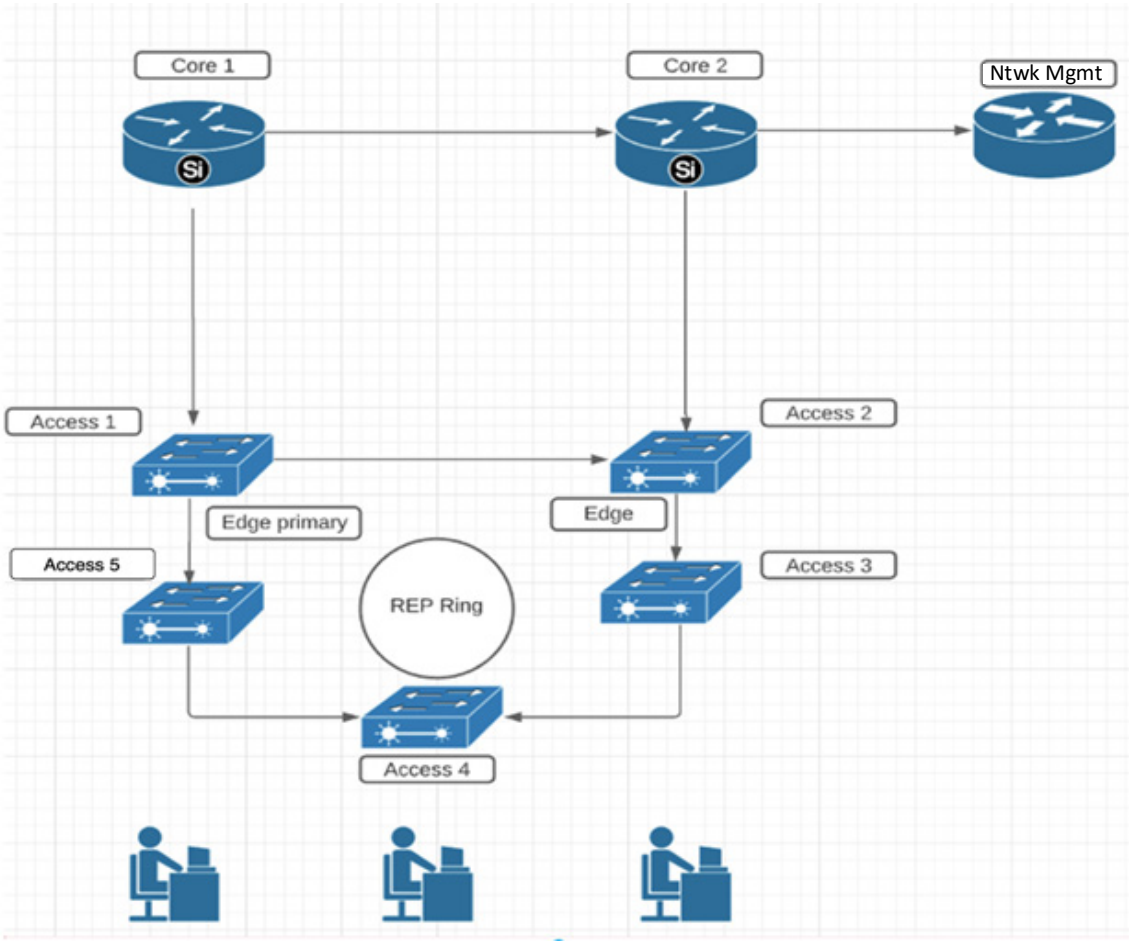

Figure 4: Illustrative REP Ring Environment

As illustrated in Figure 4, these are the two edge nodes of REP ring. Note that PnP has configured a downlink port as a primary edge on Access 1 and an edge on Access 2.

The problem starts when either Access 2 or Access 3 in Figure 4, below, are powered on. The REP edge primary port starts the REP protocol negotiation and discovers that the neighbor port is not the REP enabled port (note that the switch will be added to the REP ring only after PnP provisioning, for which it needs to first contact the DHCP server as explained earlier). When an upstream parent switch port has REP configured and the downstream switch is being onboarded with PnP, the REP port goes into a NO_NEIGHBOR state as it is not able to discover its downstream REP switch. In the NO_NEIGHBOR state, the REP blocks all of the virtual local area networks (VLANs) on that port. This means that the DHCP DISCOVER message from the new switch will be dropped in the upstream parent switch and the same sequence will continue for all the other nodes that will be added to the ring (e.g., Access 4).

In order to solve the problem that was described above, the existing REP Link Status Layer (LSL) protocol data unit (PDU) may be enhanced to notify the upstream switch about PnP execution on the downstream switch. Aspects of the techniques presented herein introduce a new TLV to the existing LSL REP PDU that can carry special flags and PnP VLAN information. Such a TLV indicates to the neighbors that PnP provisioning is underway and enables the upstream parent node to unblock the PnP VLAN on the REP port for subsequent DHCP and PnP communications.

For purposes of exposition, the function flow to enable REP rings at zero-touch, according to aspects of the techniques presented herein, will be illustrated through a series of figures that will be presented below.

Figure 5, below, depicts aspects of REP ring configuration with PnP on element S1.

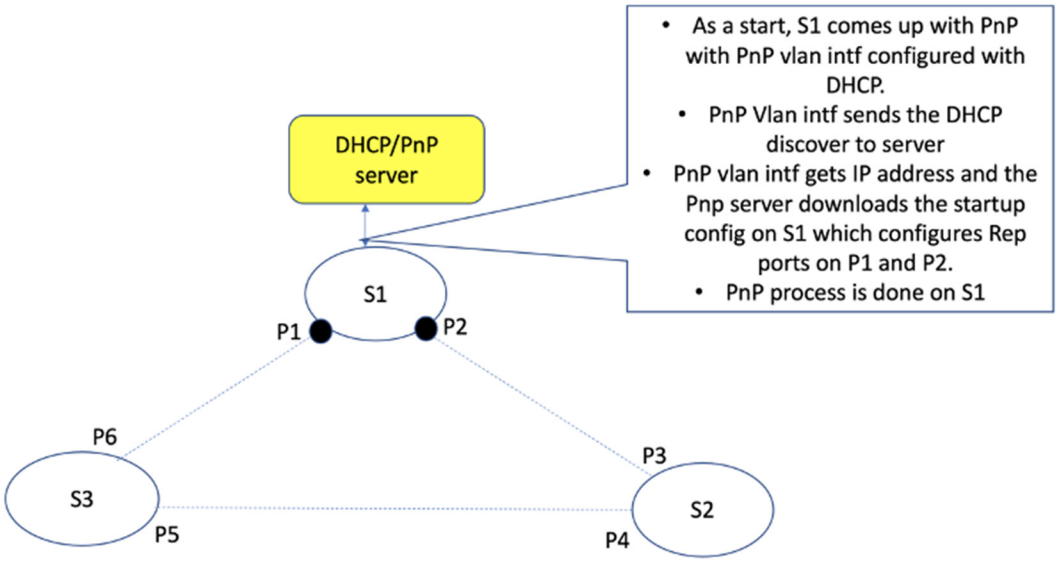

Figure 5: Exemplary Configuration with PnP on S1

Figure 6, below, depicts aspects of a first step of REP ring configuration with PnP on element S2.

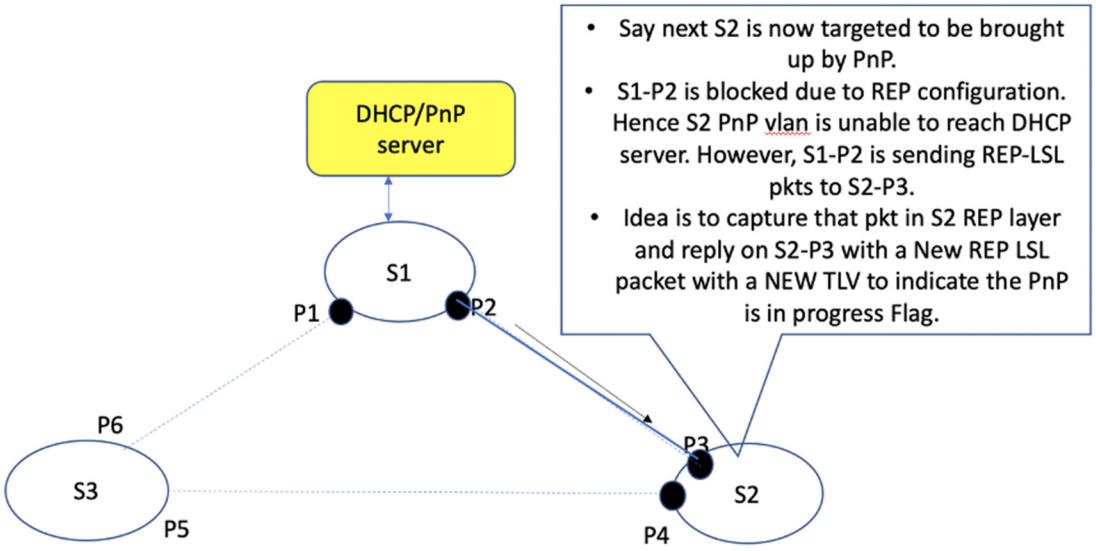

Figure 6: Exemplary Configuration with PnP on S2 – Step 1

Figure 7, below, depicts aspects of a second step of REP ring configuration with PnP on element S2.

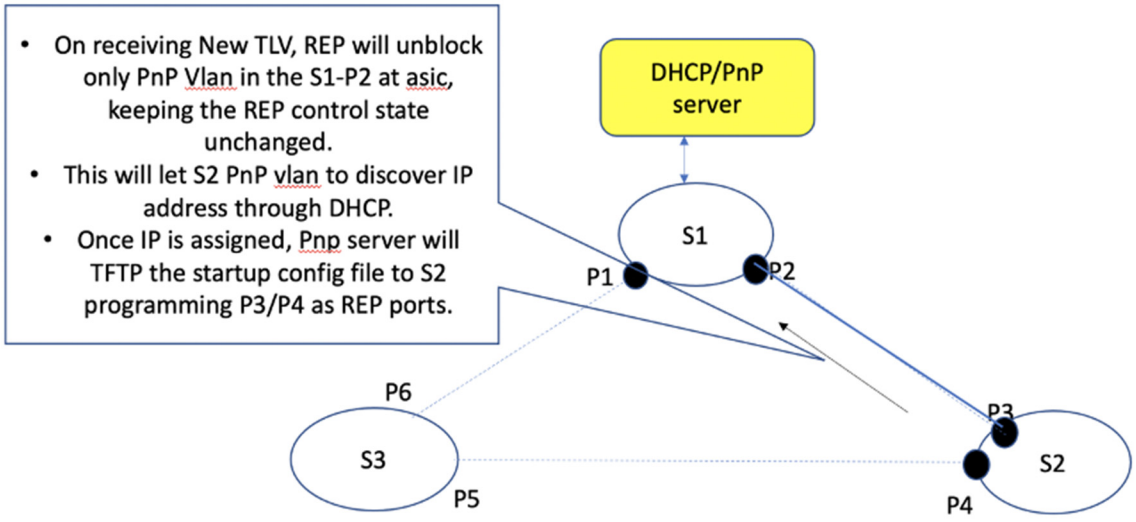

Figure 7: Exemplary Configuration with PnP on S2 – Step 2

Figure 8, below, depicts aspects of a third step of REP ring configuration with PnP on element S2.

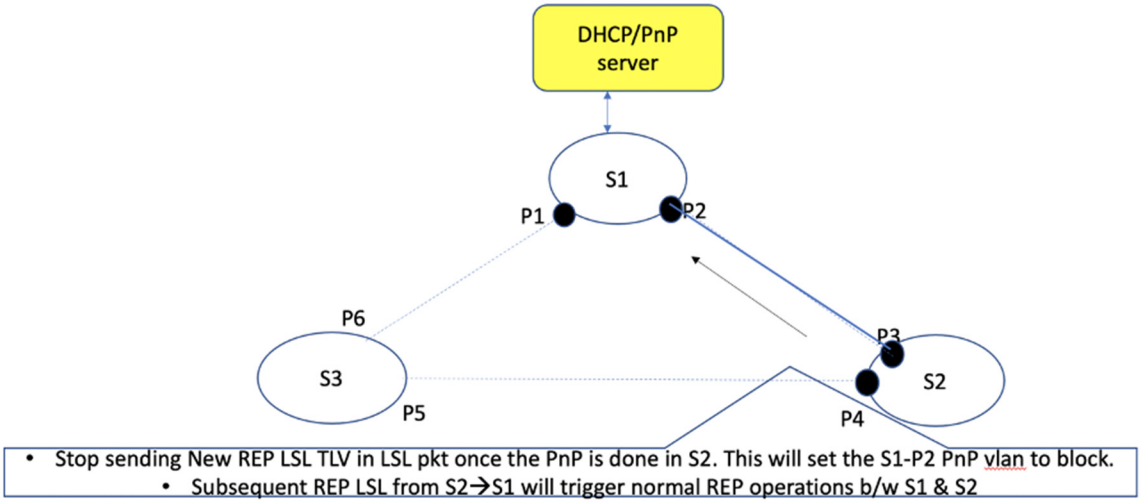

Figure 8: Exemplary Configuration with PnP on S2 – Step 3

Figure 9, below, depicts aspects of a first step of REP ring configuration with PnP on element S3.

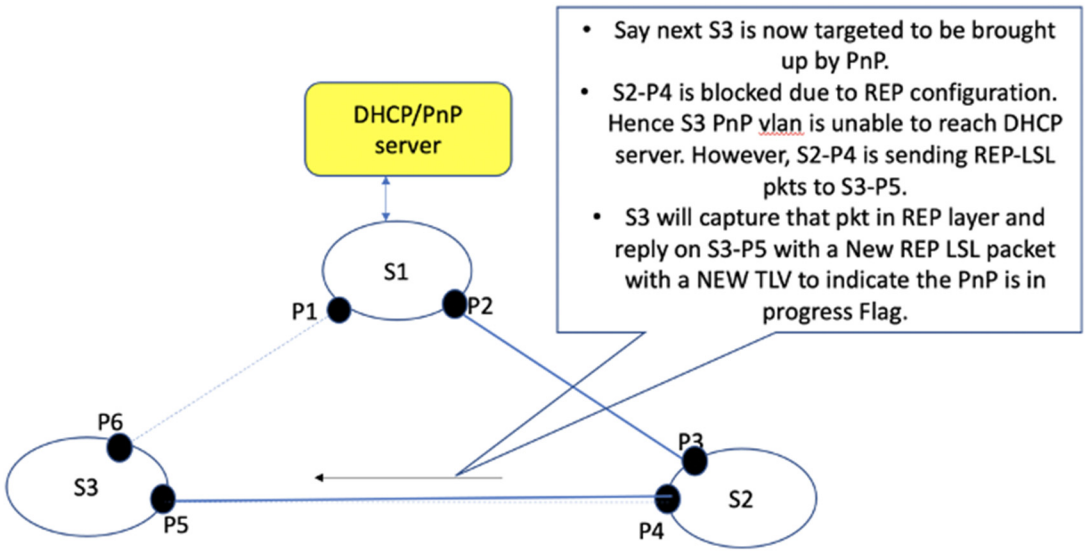

Figure 9: Exemplary Configuration with PnP on S3 – Step 1

Figure 10, below, depicts aspects of a second step of REP ring configuration with PnP on element S3.

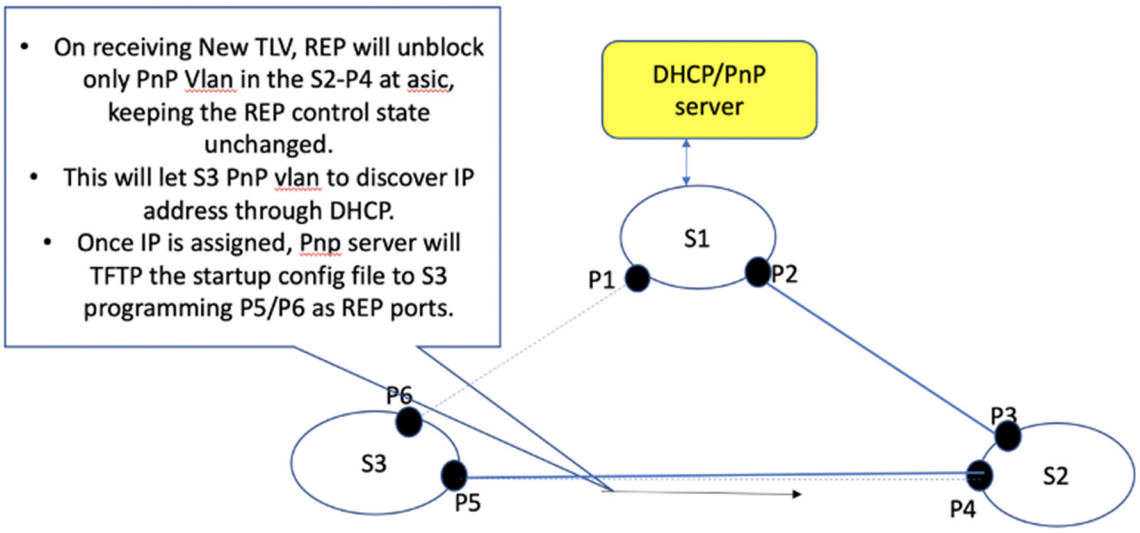

Figure 10: Exemplary Configuration with PnP on S3 – Step 2

It is important to note that it is possible that element S3 can receive a new TLV from element S1 also on port P6. In such a case, the first received new TLV port may be chosen and unblocking the PnP VLAN may be done only on this port. Figure 11, below, depicts aspects of a third step of REP ring configuration with PnP on element S3.

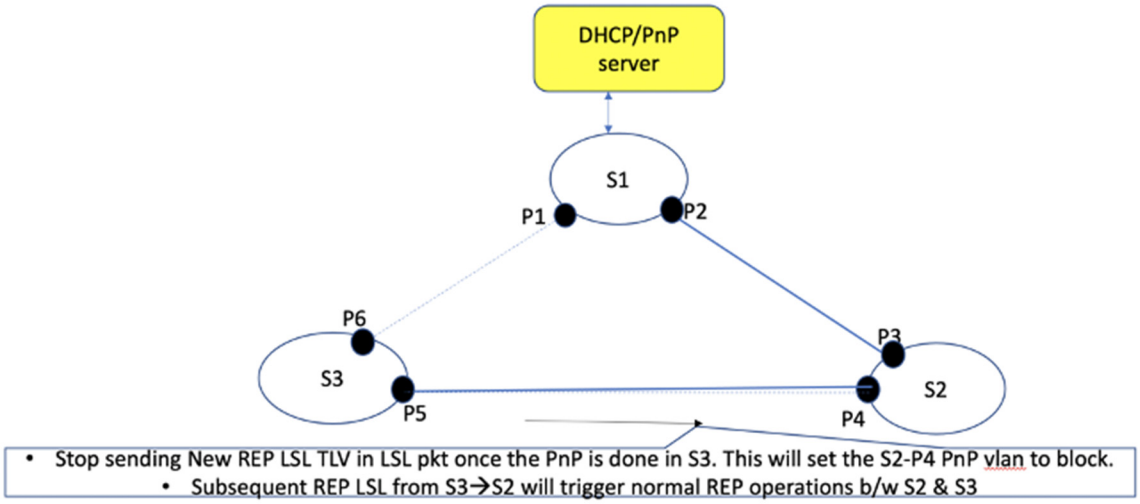

Figure 11: Exemplary Configuration with PnP on S3 – Step 3

Figure 12, below, depicts aspects of a fourth step of REP ring configuration with PnP on element S3.

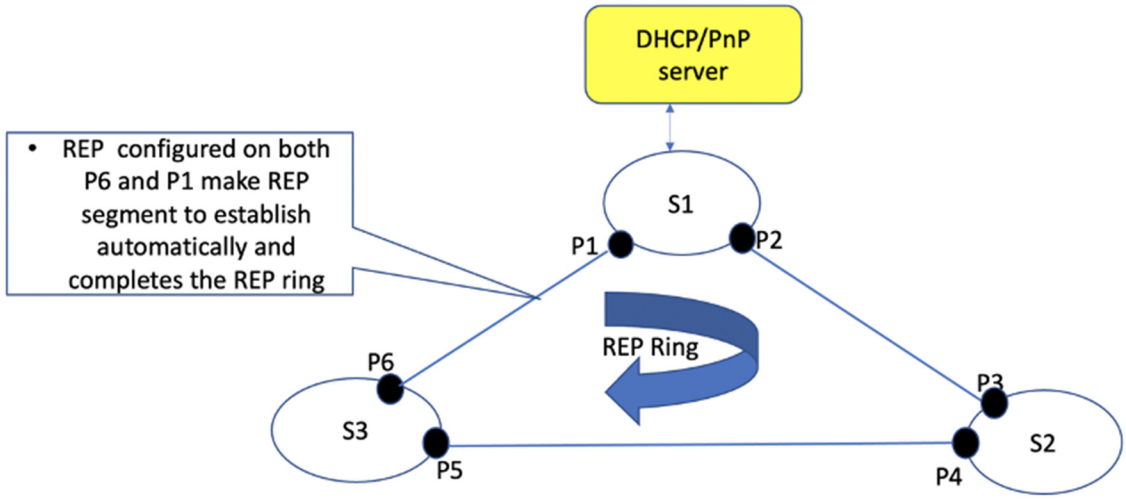

Figure 12: Exemplary Configuration with PnP on S3 – Step 4

When there are two ports in the NO_NEIGHBOR state, the REP protocol state machine places one of the ports into a forwarding state while other port is in a blocking state. However, this built-in logic does not completely solve the challenge of bringing up the REP ring in a network roll out scenario where a predefined sequence is not available.

To further illustrate aspects of the techniques presented herein, consider the model that was employed in the above Figures 5 through 12 (i.e., the three elements S1, S2, and S3) but with an on-boarding sequence of S1, S3, and then S2. Figure 13, below, along with the narrative that is presented below illustrate and describe aspects of such a scenario.

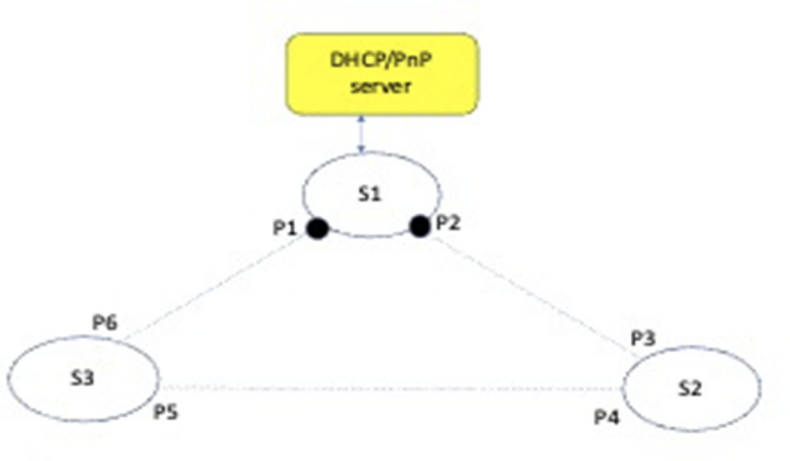

Figure 13: Exemplary Configuration with PnP on S1

The scenario that was described above (and depicted in Figure 13, above) may comprise a number of steps.

During a first step, element S1 is brought up with PnP automation. Ports P1 and P2 are configured with REP. Assume that port P1 is forwarding and that port P2 is blocked by the REP state machine.

During a second step, element S3 is brought up next with a Day Zero PnP install protocol. Assume that REP is configured on ports P6 and P5. Port P6 will be in a forwarding state (i.e., REP neighbor discovered) and port P5 will be in a blocking state (i.e., no REP neighbor).

During a third step, element S2 may be on-boarded with PnP and will try to acquire an IP address via element S3 port P5.

Since P5 is in blocked state, the DHCP DISCOVER message from element S2 is dropped at element S3 thereby halting the PnP process for bringing up element S2. In the absence of a valid IP address, the auto-install process is stuck at this stage and continues to wait for an IP address assignment from the server. Unless REP port P5 is opened (i.e., in a forwarding state) connectivity to the DHCP server cannot be established. Aspects of the

techniques presented herein address this corner problem by exchanging PnP runtime status information between elements S3 and S2 in REP LSL 'hello' packets. Element S3 continues to send LSL hellos to P4. On receiving such an LSL at the REP layer in element S2, instead of dropping the LSL (in the absence of the REP capable port and active PnP on the switch) a new algorithm under the techniques presented herein append the PnP runtime status to an LSL in a new TLV and acknowledge back to element S3 on P5 a connected link. Element S3's REP layer parses this new PnP status flag and opens up P5 until a further runtime status update from element S2 confirms the successful completion of the PnP-based process of bringing up the devices.

As described above, the logic that is expressed under aspects of the techniques presented herein works in bringing up any sequence of the devices in the REP ring.

As noted previously, aspects of the techniques presented herein introduce a new application-specific TLV – that is, a PnP REP LSL TLV.

The REP LSL PDU has a higher layer TLV embedded within it which may be enhanced to convey a PnP application specific status flag to an upstream REP-enabled parent switch.

Figure 14, below, depicts aspects of an LSL PDU extension to support application-specific requirements in a Day Zero deployment according to aspects of the techniques presented herein.

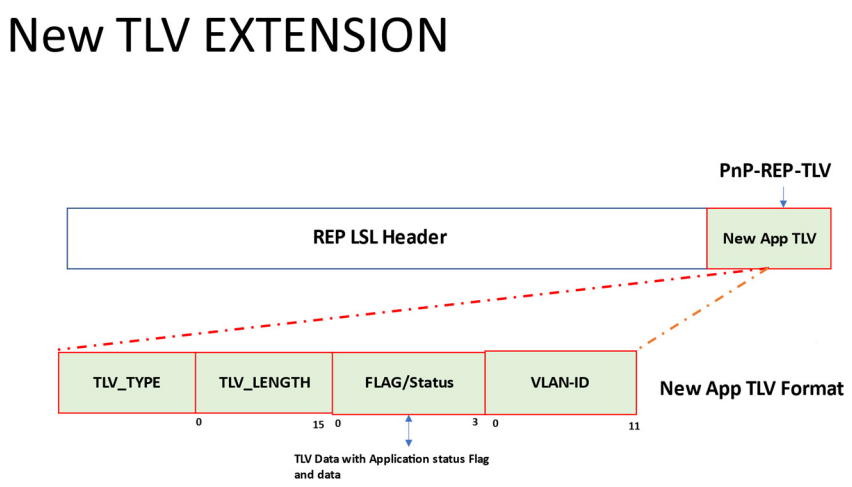

Figure 14: Exemplary TLV

As illustrated in Figure 14, above, a PnP REP LSL TLV may comprise a number of elements, including:

- A TLV_TYPE containing an application name (e.g., a PnP or zero-touch application).
- A FLAG/Status (comprising four bits) containing application or PnP specific flags that are either set or reset to convey application execution status (such as, for example, running, done, etc.). The flag bits will be interpreted by an upstream parent REP state machine to unblock or block the ring port in a VLAN-ID that is received in the TLV during a downstream device on-boarding.
- A VLAN-ID (comprising 12 bits) containing PnP startup VLAN information that is configured on the device. The VLAN identifier will be used to make sure that all the switches are using the same PnP VLAN for the right functionality.

In connection with the techniques that have been presented herein, it is important to note that the Internet Engineering Task Force (IETF) Autonomic Networking Integrated Model and Approach (ANIMA) protocol focuses principally on the automatic provisioning of devices in a customer network to enable remote self-management from the day of roll

out. Auto-install, PnP, and ZTP are similar industrial technologies for autonomic networking. Aspects of the techniques presented herein are more centered around the provisioning of the REP ring in conjunction with Day Zero technologies like ANIMA. The REP is a widely used protocol to achieve link redundancy in a ring topology for many enterprises and industrial Internet of things (IoT) customers. There is also a trend towards network digitization to avoid manual intervention for large scale network deployment. Hence, integrating REP ring provisioning in a secure autonomic networking infrastructure simplifies the deployment for the end users. Aspects of the techniques presented herein support a unique mechanism to blend a classic redundancy protocol, such as REP, with autonomic networking protocols. The result is a new effort in the direction of feature automation with autonomic protocols which has not been supported before and which supports streamlining network operations and provides offsite information technology (IT) teams with optimized remote access and management capabilities.

In summary, techniques have been presented that support configuring REP rings with zero-touch technologies. Aspects of the techniques presented herein introduce a new TLV encoding scheme to the existing REP LSL PDU to carry special flags and PnP information to handshake between upstream and downstream elements to enable REP ring provisioning.