



Avaya SDN HealthCare Solution 1.0.1.0 Release Notes

Nov 25, 2016

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits

installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Contents

Purpose	5
Intended audience	5
About Avaya SDN HealthCare Solution	5
Terminology.....	6
Supported features for this Release	7
Avaya SDN HealthCare Solution hardware and software requirements	7
Network Switches.....	8
Other software/hardware requirements.....	10
Supported browsers	10
Known Limitations & Workarounds.....	12
Configuration Procedures	13
Configuring a HP ProCurve 2650 to Deploy into the SDN 1.0.1.0 Solution	13
Configuring a Juniper Switch to Deploy into the SDN 1.0.1.0 Solution.....	16
Configuring Cisco switches to Deploy into the SDN 1.0.1.0 Solution	21
Documentation list	23

Purpose

These Release Notes provides the following information about Avaya SDN HealthCare Solution 1.0.1.0 GA release.

- General information about the Avaya SDN HealthCare Solution
- Release distribution
- Supported devices
- Known problems and workarounds
- Operational notes
- List of documents
- Support contact information

Intended audience

The primary audience for this document is anyone who is involved with deployment, administration, maintenance and troubleshooting for the Avaya SDN HealthCare Solution. The audience includes, but is not limited to, implementation engineers, field technicians, business partners, solution providers, and customers. This document does not include optional or customized aspects of a configuration.

About Avaya SDN HealthCare Solution

The Avaya SDN HealthCare Solution delivers the simplicity needed to help connect, secure, and manage the growing number of medical devices and technologies to reduce breaches, implement new healthcare innovation rapidly, and improve IT staff efficiency. The solution provides the following features:

- Advanced network segmentation to reduce catastrophic breaches.
- Automated and secure onboarding of medical devices.
- Inventory management of hundreds of devices.
- Ability to assign flow priority by device and traffic type.

The Avaya SDN HealthCare Solution is an implementation of Avaya SDN Fx architecture. The solution combines Open vSwitch (OVS)-enabled Avaya IoT device called Open Network Adaptor (ONA) with the Avaya SDN Controller and user level workflows to provide isolation and segmentation of medical devices in healthcare facilities.

Along with the Avaya SDN Controller, the Avaya SDN HealthCare Solution provides the Avaya SDN

Healthcare Application. The Avaya SDN Healthcare Application enables you to configure and manage the network of ONA devices, along with the medical devices to which the ONAs connect over the network. The Avaya SDN Healthcare Application is an SDN Application for ONA device configuration, device management, flow configuration, and diagnostics.

Terminology

Term	Description
SDN Controller	An appliance based solution consisting of two rack mountable single unit servers running the software components of the Avaya SDN HealthCare Solution
Leader Node	The node which provides acts as the Active node in the Active-Standby high availability setup
Master Node	The node which provides acts as the Standby node in the Active-Standby high availability setup
ONA	Open Networking Adapter 1101 GT
SDN Controller UI aka Platform UI aka Admin UI	The software component in the Avaya SDN HealthCare Solution that allows configuration of the SDN Controller functions
Avaya SDN HealthCare Solution App	The software component in the Avaya SDN HealthCare Solution that allows licensing of ONAs and provisioning of the flows in the ONA
ADM	Appliance Device Manager
KVM	Kernel-based Virtual Machine aka Hypervisor
VM	Virtual Machine

Supported features for this Release

The following features are supported:

- New support for Cisco switches
- New support for Hewlett Packard Enterprise switches
- New support for Juniper Switches
- New support for Avaya FA and non-FA enabled switches: ERS 5600, ERS 5900, ERS 4500, ERS 4800, ERS 4900
- New support for a Standalone SDN Controller deployment
- New support for OAuth 2.0
- New support for Northbound APIs

Avaya SDN HealthCare Solution hardware and software requirements

The solution is shipped with two components:

- Open Networking Adapter (ONA): Is a pocket-sized intelligent appliance that is paired with a medical device.
- A preconfigured hardware appliance HP DL360p G9: This appliance has all the required hardware and software for the Avaya SDN HealthCare Solution to work properly.

Component	Specification	
CPU	Processor Name	Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
	Processor Speed	2600 MHz
	Execution Technology	14/14 cores; 56 threads
	vCPU(s)	56
	CPU socket(s)	2
	Core(s) per socket	14
	Thread(s) per core	2
Memory	128 GB	
HDD	4 x 600GB 15000 rpm SAS drive configured with RAID 5	
Network	4 x 1 Gig Broadcom NetXtreme BCM5719	
	2 x 10 Gig Broadcom NetXtreme II BCM57810	

Network Switches

The following switches and switch versions are supported:

Juniper EX4300 PoE and non-POE

Cisco 2950

Cisco 3560

Cisco 3560G PoE48

Cisco 3750

Cisco 3850 48 PoE+

HP ProCurve 2650

HP ProCurve 2824

ERS5900 releases 7.2.0.213, 7.2.0.009, 7.3.0

ERS4900 releases 7.2.0.213, 7.2.0.009, 7.3.0

ERS4500 releases 5.7.3.030/031, 5.7.2.012/013

ERS5500/ERS5600 releases 6.3.6.016/017, 6.3.5.024/025

ERS5600 releases 6.6.3.014/015, 6.6.2.012/013

ERS3500 releases 5.3.2.206/207, 5.3.2.016/017, 5.3.3

ERS4800 releases 5.9.3.022/023, 5.9.2.046/047, 5.10.0

VSP7000 releases 10.4.1.009, 10.4.0.003, 10.4.2

Standalone Controller (Non-HA)

There are 2 deployment models in current release, Standalone Mode and HA Mode (Leader and Master). Standalone mode is deployment model only for single host system. Hence, there is no clustering nor high availability feature in place. The mode can be selected during the configuration process after the installation. Once the deployment model is decided, changing one mode to other mode is not supported in current release. To change the deployment mode, installer shall perform factory reset and reconfigure the appliance.

Standalone Mode

Standalone Mode is deployment model using same HW platform that is used in high-end HA Mode except for the redundancy. Other than that the system carries over same characteristic including performance. In current release, "Standalone Mode" cannot be converted into "HA Mode". Hence the "Standalone Mode" is suitable for following deployment cases:

1. Single node without High-Availability Requirement
2. Customer Demo or Proof-of-Concept
3. Partners Lab Setup

Virtual Network Design

Deployment Node	Virtual Bridge	Virtual Machine	IP Address
Standalone Node	Management (NIC1)	Hypervisor	Required
		Platform	Required
		Monitoring	Required
		Load Balancer	N/A
		Load Balancer Virtual IP	N/A
		iLO	Required
	Device (NIC2)	Hypervisor	Required
		ODL	Required
		MSC	Required
		Load Balancer	N/A
		Load Balancer Virtual IP	N/A
	Integration (NIC3)	Hypervisor	Required
		Load Balancer	N/A
		Cluster Engine	Required
		Cluster Engine Mgmt IP	Required
		Load Balancer Virtual IP	N/A

Note: The SDN HealthCare App will be accessible through Management Hypervisor IP address

OAuth 2.0

OAuth provides to clients a "secure delegated access" to server resources on behalf of the resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. This is designed specifically to work with [Hypertext Transfer Protocol](#) (HTTP), OAuth allows [access tokens](#) to be issued to third-party clients by an authorization server, with the approval of the resource owner.

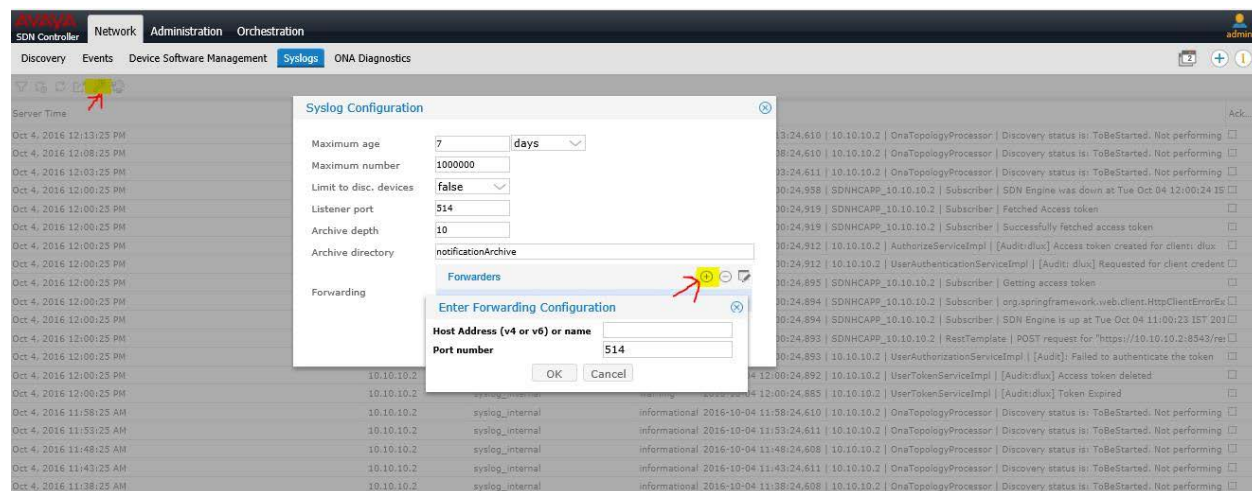
OAuth 2.0 is being used for all SDN Fx Controller and SDN App NB APIs. All REST API framework shall be compliant to OAuth 2.0 standard

External Syslog server Support

All syslog messages generated by the SDN controller can be forwarded to external syslog servers.

Procedure:

- 1) Login to Platform UI and navigate to Network -> Syslogs menu
- 2) Click on "Settings" icon (highlighted in yellow in attached screenshot)
- 3) On the "Syslog Configuration" window, click on "Add" button
- 4) Add the external Syslog Host details and the syslog messages get forwarded to that server.



Other software/hardware requirements

- A DNS/DHCP server is required and must be set up prior to the Application installation
- Avaya SDN HealthCare Solution Application version 1.0.1.0.2016316
- For Fabric Attach Network Devices
 - VOSS 5.0.0.0 and up
 - BOSS 5.9.2.047 and up
 - ONA 1101GT running VEGA v2.0.1.1GA

Supported browsers

SDN Healthcare Application:

- Chrome - version 40 and above

SDN Controller UI:

- Internet Explorer – version 10, version 11
- Firefox – version 40 and above

Known Limitations & Workarounds

The following are limitations for the 1.0.1.0 release:

Issue ID	Summary	Description / Workaround
SDN-2786	Cancel button on Edit Security Flow screen is disabled for Clinical engineer	Cancel button in Edit Security Flow screen is disabled for clinical engineer. Clinical engineer can use the close icon to exit out of edit flow screen, instead of the Cancel button. By clicking on the close icon, the Clinical engineer can redirect to the Device Inventory screen
SDN-2755	The SDN Health Care login user name is saved in lowercase format	When creating a new user with uppercase alphabets, the username is saved with all lowercase characters.
SDN-2753	iLO-IPMI v2.0 Password Hash Security Disclosure	The following known vulnerability was reported on the HP iLO The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC. There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : <ul style="list-style-type: none"> - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.
SDN-2630	Some ONAs may remain INACTIVE state after a broadcast storm in the management VLAN	Reset the ONA by disabling then enabling the POE support.
SDN-2359	Topology Manager – ACTIVE ONAs show up with a caution symbol/icon	After the “Start Network Discovery”, ACTIVE ONAs show up in with a “Caution” symbol when ERS switches are configured as Fabric Server mode.
SDN-2386	SDN Fx Controller software upgrade menu (SSD) does not return browser handle back to user	During the SDN Controller software upgrade, after "precheck" is completed, the Web UI does not return browser handle back to user to perform the upgrade . The screen shows spinning-wheel and never comes back.

		The issue exist in latest IE patch and Firefox v47 and above. The workaround is to downgrade the browser. The issue is only applicable for those customer who are upgrade from 1.0 and 1.0.0.25 and 1.0.0.26 patches. The issue is resolved starting from SDN 1.0.1.0 release.
SDN-2557	SDN Standalone server should not be allowed to convert to SDN HA cluster	SDN Standalone server cannot be converted to SDN HA cluster. This is not supported.
SDN-2279	ONA upgrade getting error and fail to create task with 40 ONA devices	Workaround is to remove existing tasks containing ONA's. When an upgrade task is removed, the associated license will be given up for each ONA associated to the task. A new task can be created to add new ONA's to go with the upgrade.
SDN-2418	Support to provision ONA Device port speed and duplex mode	Upgrading to ONA release 2.0.1.1, the ONA Ethernet port will now additionally support port speeds of 10MB and 100MB. It will also support half duplex with these port speeds, however, there is no UI for customer to select specific mode.

Configuration Procedures

Configuring a HP ProCurve 2650 to Deploy into the SDN 1.0.1.0 Solution

Before you begin:

- Identify ONA Management VLAN.
- Identify the port or trunk which will be used for uplink.
- Identify the ports where ONAs will be connected.
- Identify the VLANs which will be used to connect Medical Devices.

In this example, following are the inputs:

- VLAN 600 is used for ONA Management.
- Trunk 'Trk1' is used for uplink, port 49 and 50 are part of this trunk.
- Port 1 and 2 are the ports where ONAs will be connected.
- VLAN 3401 and VLAN 3402 are used for connecting the Medical Devices.

Procedure

1 Access the switch.

2 Create ONA Management VLAN.

```
ProCurve Switch 2650-PWR(config)# vlan 600
ProCurve Switch 2650-PWR(vlan-600)# name "ONA-Mgmt"
```

3 Add the ONA ports as untagged ports to this VLAN.

```
ProCurve Switch 2650-PWR(vlan-600)# untagged 1-2
```

4 Add the uplink trunk to this VLAN as tagged ports.

```
ProCurve Switch 2650-PWR(vlan-600)# tagged Trk1
```

5 Create VLAN 3401.

```
ProCurve Switch 2650-PWR(config)# vlan 3401
ProCurve Switch 2650-PWR(vlan-3401)# name ONA-1_VLAN
```

6 Add the ONA port (Port-1) and uplink trunk (Trk1) as tagged ports to this VLAN.

```
ProCurve Switch 2650-PWR(vlan-3401)# tagged 1,Trk1
```

7 Create VLAN 3402.

```
ProCurve Switch 2650-PWR(config)# vlan 3402
ProCurve Switch 2650-PWR(vlan-3402)# name ONA-2_VLAN
```

8 Add the ONA port (Port-2) and uplink trunk (Trk1) as tagged ports to this VLAN.

```
ProCurve Switch 2650-PWR(vlan-3402)# tagged 2,Trk1
```

Additional Information

Following shows how to create a trunk

```
ProCurve Switch 2650-PWR(config)# trunk 49-50 Trk1 Trunk
```

When a Trunk is created, by default LACP is disabled, user can configure LACP based on the configuration on the UP-Link Switch. When connecting the trunk to Avaya's MLT/SMLT link, LACP can be disabled.

Config Dump of the switch after completion

```
ProCurve Switch 2650-PWR# show running-config
```

```
Running configuration:
```

```
; J8165A Configuration Editor; Created on release #H.08.98
```

```
hostname "ProCurve Switch 2650-PWR"
interface 49
    no lacp
exit
interface 50
    no lacp
exit
trunk 49-50 Trk1 Trunk
vlan 1
    name "DEFAULT_VLAN"
    untagged 3-47,Trk1
    no ip address
    no untagged 1-2
    exit
vlan 3401
    name "ONA-1_VLAN"
    tagged 1,Trk1
    exit
vlan 3402
    name "ONA-2_VLAN"
    tagged 2,Trk1
    exit
vlan 600
    name "ONA-Mgmt"
    untagged 1-2
    tagged Trk1
    exit
spanning-tree Trk1 priority 4

ProCurve Switch 2650-PWR#
```

Verifying Connectivity

After boot up ONA's status LED should change to fast blinking "GREEN", and ONA should register on the SDN HealthCare APP.

User can connect a Laptop/PC at port 1 or 2, it should get DHCP Lease, and it should be able to ping "avayasdncontroller".

Quick recovery

If medical device needs to be connected directly to the port, user can turn off tagging using the following command, and connect the device.

```
ProCurve Switch 2650-PWR(config)# vlan 3401
ProCurve Switch 2650-PWR(vlan-3401)# untagged 1
```

Configuring a Juniper Switch to Deploy into the SDN

1.0.1.0 Solution

The following Juniper switches were tested:

- Juniper EX4200 PoE
- Juniper EX4300 PoE

Before you begin:

- Identify ONA Management VLAN.
- Identify the port or trunk which will be used for uplink.
- Identify the ports where ONAs will be connected.
- Identify the VLANs which will used to connect Medical Devices.

In this example, following are the inputs:

- VLAN 300 is used for ONA Management.
- Redundant Link: In a network composed of distribution and access layers, a redundant trunk link provides a simple solution for trunk interface network recovery. When a trunk interface fails, data traffic is routed to another trunk interface, thereby keeping network convergence time to a minimum.
- Ports 09 and 10 are part of the redundant link.
- Port 06 and 07 are the ports where ONAs will be connected.
- VLAN 3010 and VLAN 3020 are used for connecting the Medical Devices.

Procedure

1 Login to the Juniper switch.

2 Create an ONA Management VLAN.

```
root@Juniper-EX4200-PWR(config)# set vlans MGMT-vlan vlan-id 300
```

3 Create ONA Data VLAN for 2 ONAs.


```
root@Juniper-EX4200-PWR(config)# set vlans ONA1 vlan-id 3010
root@Juniper-EX4200-PWR(config)# set vlans ONA2 vlan-id 3020
```

4 Configure the ports to which the 2 ONAs to be connected to as trunk ports allowing the management VLAN and the corresponding data VLAN.

```
root@Juniper-EX4200-PWR(config)#
set interfaces ge-0/0/09 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/09 unit 0 family ethernet-switching vlan members
ONA1,ONA2
set interfaces ge-0/0/09 unit 0 family ethernet-switching vlan members MGMT-
vlan
set interfaces ge-0/0/09 unit 0 family ethernet-switching native-vlan-id 300
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members
ONA1,ONA2
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members MGMT-
vlan
set interfaces ge-0/0/10 unit 0 family ethernet-switching native-vlan-id 300
```

5 Configure the redundant links which is connecting to the uplink.

```
root@Juniper-EX4200-PWR(config)#
set ethernet-switching-options redundant-trunk-group group rtg0 interface ge-
0/0/9.0 primary
set ethernet-switching-options redundant-trunk-group group rtg0 interface ge-
0/0/10.0
```

6 Optional - Change the length of time (from the default 120 seconds) that a re-enabled primary link waits to take over for an active secondary link.

```
root@Juniper-EX4200-PWR(config)#
set ethernet-switching-options redundant-trunk-group group rtg0 preempt-
cutover-timer 60
```

Additional Information

Rapid Spanning Tree Protocol (RSTP) is enabled by default on EX Series switches to create a loop-free topology, but an interface is not allowed to be in both a redundant trunk group and in a spanning-tree protocol topology at the same time. You will need to disable RSTP on the two distribution switches in the example, Switch 1 and Switch 2. Spanning-tree protocols can, however, continue operating in other parts of the network—for example, between the distribution switches and also in links between distribution switches and the core.

Configuration of the switch after completion

```
root@Juniper-EX4200-PWR>show configuration| display set

set interfaces ge-0/0/6 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members ONA1,ONA2
set interfaces ge-0/0/6 unit 0 family ethernet-switching native-vlan-id 300
```

```

set interfaces ge-0/0/7 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members ONA1,ONA2
set interfaces ge-0/0/7 unit 0 family ethernet-switching native-vlan-id 300

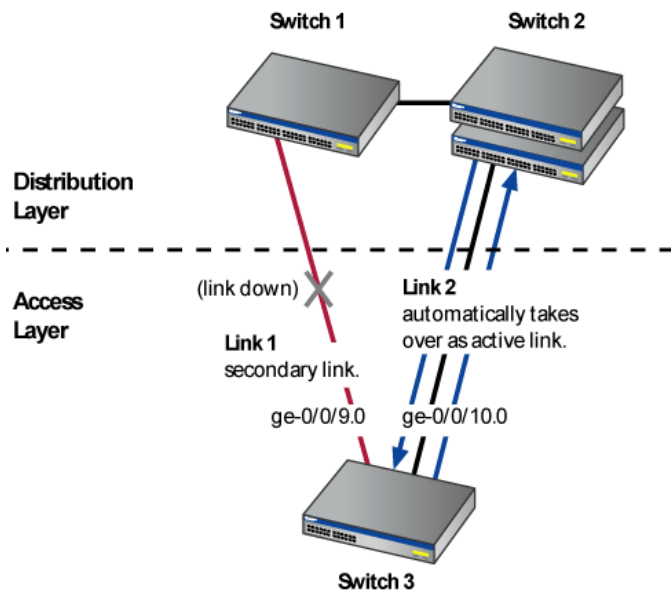
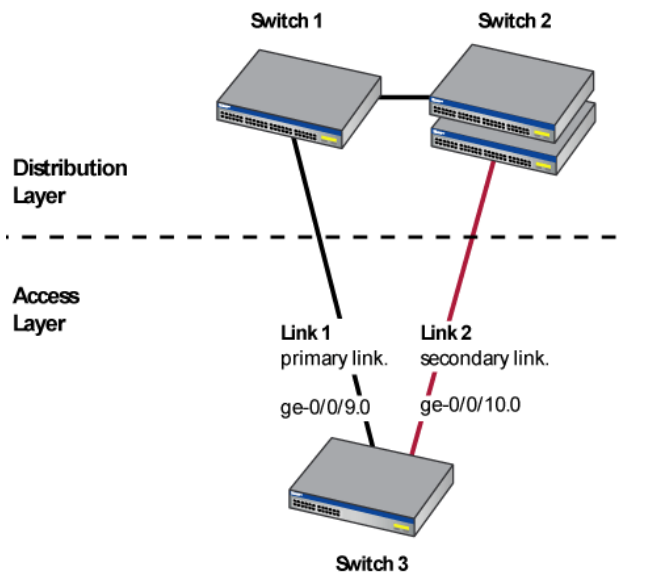
set protocols stp interface ge-0/0/9.0 disable
set protocols stp interface ge-0/0/10.0 disable
set protocols rstp interface ge-0/0/9.0 disable
set protocols rstp interface ge-0/0/10.0 disable

set interfaces ge-0/0/09 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/09 unit 0 family ethernet-switching vlan members
ONA1,ONA2
set interfaces ge-0/0/09 unit 0 family ethernet-switching native-vlan-id 300
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members
ONA1,ONA2
set interfaces ge-0/0/10 unit 0 family ethernet-switching native-vlan-id 300

set ethernet-switching-options redundant-trunk-group group rtg0 preempt-
cutover-timer 60
set ethernet-switching-options redundant-trunk-group group rtg0 interface ge-
0/0/9.0 primary
set ethernet-switching-options redundant-trunk-group group rtg0 interface ge-
0/0/10.0
set ethernet-switching-options storm-control interface all
set vlans MGMT-vlan vlan-id 300
set vlans ONA1 vlan-id 3010
set vlans ONA2 vlan-id 3020
set poe interface all

```

Sample Topology



Show Commands

If medical device needs to be connected directly to the port, user can turn off tagging using the following command, and connect the device.

```
root@Juniper-EX4200-Edge1> show redundant-trunk-group group-name rtg0
```

Interface	State	Bandwidth	Time of last flap	Flap count
-----------	-------	-----------	-------------------	------------

```
ge-0/0/9.0 Up/Pri/Act 1 Gbps 2015-10-15 13:17:00 UTC (5w1d 02:33 ago) 1
ge-0/0/10.0 Up 1 Gbps 2015-10-15 13:17:01 UTC (5w1d 02:33 ago) 1
```

```
root@Juniper-EX4200-Edge1> show ethernet-switching interfaces ge-0/0/6.0
```

```
Interface State VLAN members Tag Tagging Blocking
ge-0/0/6.0 up MGMT-vlan 300 untagged unblocked
          ONA1,ONA2 3010 tagged unblocked
```

```
{master:0}
```

```
root@Juniper-EX4200-Edge1> show ethernet-switching interfaces ge-0/0/7.0
```

```
Interface State VLAN members Tag Tagging Blocking
ge-0/0/7.0 up MGMT-vlan 300 untagged unblocked
          ONA1,ONA2 3010 tagged unblocked
```

```
{master:0}
```

```
root@Juniper-EX4200-Edge1> show ethernet-switching interfaces ge-0/0/9
```

```
Interface State VLAN members Tag Tagging Blocking
ge-0/0/9.0 up MGMT-vlan 300 untagged unblocked
          MGMT-vlan 300 tagged unblocked
          ONA1,ONA2 3010 tagged unblocked
```

```
{master:0}
```

```
root@Juniper-EX4200-Edge1> show ethernet-switching interfaces ge-0/0/10.0
```

```
Interface State VLAN members Tag Tagging Blocking
ge-0/0/10.0 up MGMT-vlan 300 untagged blocked by RTG(rtg0)
          MGMT-vlan 300 tagged blocked by RTG (rtg0)
          ONA1,ONA2 3010 tagged blocked by RTG(rtg0)
```

Port Mirroring: Debugging Purpose

```
set ethernet-switching-options analyzer mon1 input ingress interface ge-0/0/9.0
set ethernet-switching-options analyzer mon1 input ingress interface ge-0/0/10.0
set ethernet-switching-options analyzer mon1 input egress interface ge-0/0/9.0
set ethernet-switching-options analyzer mon1 input egress interface ge-0/0/10.0
set ethernet-switching-options analyzer mon1 output interface ge-0/0/2.0
```

Configuring Cisco switches to Deploy into the SDN

1.0.1.0 Solution

The following Cisco switches were tested:

- Cisco 2950
- Cisco 3560
- Cisco 3560G PoE48
- Cisco 3750
- Cisco 3850 48 PoE+

Before you begin:

- Identify ONA Management VLAN.
- Identify the port or trunk which will be used for uplink.
- Identify the ports where ONAs will be connected.
- Identify the VLANs which will be used to connect Medical Devices

In this example, following are the inputs:

- VLAN 300 is used for ONA Management.
- **Ether Channel:** For the purposes of aggregating available bandwidth and to provide physical redundancy, Avaya had tested the SDN solution with the above switches by using Cisco's EtherChannel mode/feature. In this mode, aggregation is achieved by manually (statically) configuring the ports. Cisco's LACP Active/Passive mode to achieve the aggregation is not yet tested with the SDN solution.

Ether Channel 'Port-channel1' is used for uplink, ports 23 and 24 are used to be part of this ether channel.

- Port 1 and 2 are the ports where ONAs will be connected.
- VLAN 2000 and VLAN 2001 are used for connecting the Medical Devices.

Procedure

1 Access the switch.

2 Create ONA Management VLAN.

```
vlan 300
name ONA-DHCP_DNS
```

3 Create ONA Data VLAN for two ONAs.

```
vlan 2000
```

```
name ONA-1_VLAN
!
vlan 2001
name ONA-2_VLAN
```

4 Configure an EtherChannel

```
interface Port-channel1
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 300
    switchport trunk allowed vlan 300,2000,2001
    switchport mode trunk
    switchport nonegotiate
    no ip address
```

5 Configure the ports to which the 2 ONAs to be connected to as trunk ports allowing the management vlan and the corresponding data vlan.

```
interface Port-channel1
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 300
    switchport trunk allowed vlan 300,2000,2001
    switchport mode trunk
    switchport nonegotiate
    no ip address
!
interface GigabitEthernet1/0/2
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 300
    switchport trunk allowed vlan 300,2001
    switchport mode trunk
!
```

6 Configure the uplink EtherChannel ports.

```
interface FastEthernet0/23
    switchport trunk native vlan 300
    switchport mode trunk
    switchport nonegotiate
    channel-group 1 mode on
!
interface FastEthernet0/24
    switchport trunk native vlan 300
```

```

switchport mode trunk
switchport nonegotiate
channel-group 1 mode on

```

!

Verifying Connectivity

After boot up ONA's status LED should change to fast blinking "GREEN", and ONA should register on the SDN HealthCare APP.

User can connect a Laptop/PC at port 1 or 2, it should get DHCP Lease, and it should be able to ping "avayasdncontroller".

Documentation list

The following table lists the documents related to the Avaya SDN HealthCare Solution. Download the documents from the Avaya Support website at <http://support.avaya.com/>.

Document	Description
<i>Avaya SDN Fx Healthcare Solution Description, NN48200-100</i>	This document offers a high-level description of the Avaya SDN HealthCare Solution.
<i>Avaya SDN Fx Healthcare User Guide, NN48200-101</i>	This document describes how to use the Avaya SDN Healthcare Application features.
<i>Locating the software and release notes for Avaya SDN Fx Healthcare, NN48200-103</i>	This document describes where to find critical information to configure and deploy the Avaya SDN HealthCare Solution.
<i>Deploying Avaya SDN Fx Healthcare, NN48200-300</i>	This document contains Avaya Surge™ Healthcare Solution installation, configuration, initial administration, and basic maintenance checklist and procedures
<i>Maintaining Avaya SDN Fx Healthcare, NN48200-500</i>	This document contains the Avaya SDN HealthCare Solution maintenance procedures and best practices for routine maintenance. Routine maintenance practices include regularly scheduled backup and restoration, daily monitoring, and verification testing.
<i>Administering Avaya SDN Fx Healthcare, NN48200-600</i>	This document contains information about how to perform the Avaya SDN HealthCare Solution administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.
<i>Troubleshooting Avaya SDN Fx Healthcare, NN48200-700</i>	This document describes how to use the Avaya SDN HealthCare Solution troubleshooting tools and utilities. The document also describes the procedures to contact Avaya Support and contains typical error messages and resolution tasks.
<i>Avaya Open Networking Adapter 1101GT Installation Job Aid, NN48800-300</i>	This installation job aid provides an overview of the Open Networking Adapter (ONA).
<i>Avaya Open Networking Adapter 1101GT Software Update Requirement, NN48800-302</i>	The software upgrade requirement document provides information about the requirement to

	upgrade your Open Networking Adapter (ONA) devices to the final software version.
<i>Avaya Open Networking Adapter 1101GT Release Notes</i> , NN48800-400	The <i>Avaya Open Networking Adapter 1101GT Release Notes</i> (NN48800-400) provide important information about this release of the Open Networking Adapter (ONA).
<i>Avaya Open Networking Adapter 1101GT Read Me</i> , NN48800-401	The read me document provides a brief description on where to find the documentation for the Open Networking Adapter (ONA) devices.