



Key Differentiating Features of the Cisco Catalyst 3850/3650 Series



DR161201G
July 2017

Miercom
www.miercom.com

Contents

1 - Executive Summary	3
2 - Product Overview	4
Catalyst 3850 Stackable Switch	4
Catalyst 3650 Switch	5
Catalyst 3560CX Compact Switch.....	5
3 - Test Bed: How We Did It.....	6
Test Bed Configuration.....	6
4 - Power Options	8
5 - Controlling the Internet of Things (IoT).....	9
6 - Application Visibility and Control.....	11
7 - Segmentation	13
8 - Traffic Capture and Analysis.....	16
9 - Wired/Wireless Convergence With Services (mDNS)	19
10 - Supported Cisco Features (16.3.1 Release).....	20
11 - About Miercom Performance Verified Testing	21
12 - About Miercom.....	21
13 - Use of This Report.....	21

1 - Executive Summary

Miercom was engaged by Cisco Systems to independently configure, operate and then assess select advanced features of the Catalyst 3850/3650 Series Switches. Support for a spectrum of useful high-level features, which our testing found, adds considerable value to this switch series.

Deciding which advanced features to test was a joint undertaking by Miercom and Cisco. More than a half-dozen diverse features were distilled and selected from literally hundreds. These provided a good cross-section of the impressive, inherent capabilities of the product.

Key Findings and Observations:

- **Power options** – We exercised the Catalyst 3850's impressive power options. In addition to UPoE there's also Perpetual PoE support – where power to down-range PoE devices continues uninterrupted even when the switch reboots. There is also shared stack power, where stacked switches share the power from all power supplies.
- **Internet of Things (IoT)** – The Catalyst 3850 supports the Constrained Application Protocol (CoAP), an emerging standard for controlling IoT devices. We used it to control a third-party light fixture; CoAP is also used now for light, sensors, cameras, etc.
- **Application visibility and control (AVC)** – Can dynamically identify applications and spot bottlenecks and monitor, rate-limit, re-direct or block non-business-critical or malicious traffic.
- **Segmentation** – Campus Fabric providing policy-based secure segmentation with enhanced host mobility and MPLS providing traditional VPN Based Segmentation.
- **Security Sensor** – Using the Network as a Sensor with NetFlow allows for network traffic visibility. Based on user-specified criteria in StealthWatch, the user can obtain real-time situational awareness of any users, devices and traffic on the network attempting, for example, a denial of service attack.
- **Remote traffic copy over GRE** – The latest form of SPAN (Switched Port Analysis), called ERSPAN (Encapsulated Remote SPAN), copies traffic from any port or VLAN and sends it via a secure GRE tunnel to any port in the network, where tools like Virtual Network Analysis Module (vNAM) or any other collector can conduct deep-packet inspection and analysis.
- **Programmability** – Cisco supports using the standard Netconf API with the YANG data modeling language to configure and troubleshoot the Catalyst 3850.

Based on the results of our feature analysis, we proudly award the **Miercom Performance Verified Certification** to Cisco's Catalyst 3850/3650 series of switches.

Robert Smithers
CEO
Miercom



2 - Product Overview

The test bed included several models of the Cisco Catalyst 3850/3650 Series switches. All of the switches in this series support mGig – multi-gigabit Ethernet, including what is now known as IEEE 802.3bz – which deliver bandwidths beyond 1 Gbps, up to 10 Gbps, over legacy Cat5e and Cat6 copper cabling. The models tested were:

- The 3850, a best-in-class stackable switch model with optional uplink-port modules and Stackpower
- The 3650, similar to the 3850 but with fixed uplinks and FRU-able power supplies
- The 3560CX, a lightweight, compact, desktop (or rackable) version with fewer ports

Catalyst 3850 Stackable Switch

This switch supports 24 and 48 RJ-45 or fiber/SFP+ (small form-factor pluggable) ports, in various configurations. Ports can operate up to 10 Gbps. The 3850 also features an integrated wireless controller that can manage up to 100 APs (Access Points) and up to 2,000 wireless clients.

The switch accepts any of five optional uplink modules. These provide four GE (1-Gigabit Ethernet) via SFP/fiber ports; two or four 10-GE SFP+ ports, two 40-GE QSFP+ ports or eight 10-GE ports.

The switch supports the Cisco StackWise-480 technology – supporting up to 480 Gbps of collective stack throughput.

Also, the 3850 supports a host of power options over copper links. These include: full IEEE 802.3at (PoE+) with 30W power on all copper ports; Cisco Universal Power over Ethernet (Cisco UPOE, with 60W power); and Perpetual Power over Ethernet (PPoE), which was tested for this report. Additional power innovations include dual redundant modular power supplies and power stacking among stack members for power redundancy.

The photo shows four stacked Catalyst 3850 units, as they were tested.



Catalyst 3650 Switch

This switch is nearly the same as the 3850, in the same 1U rack unit form factor, except with fixed uplinks and lower scale/performance. Like the 3850, the 3650 also features an integrated wireless controller, but with less overall wireless capacity; it can manage up to 50 APs and up to 1,000 wireless clients.

The 3650 supports 24 and 48 RJ-45 ports, mGig bandwidth; various fixed fiber/SFP+ uplink modules with various density options, dual (FRU) power. Stack Power is only available on the Catalyst 3850.

In most other respects - software features, and so on – the 3650 is the same as the 3850. The below picture shows four 3650 switches.



Catalyst 3560CX Compact Switch

This is a lightweight, fanless offering in the Catalyst family, which we deployed in the testing as a gateway and for a streaming audio/video test. Depending on model, the 3560CX supports eight or twelve GE (1-Gbps Ethernet) ports, or six GE plus two mGig (multi-Gigabit Ethernet over copper cabling) ports. Alternately, two 10GE uplink ports can be optical SFP+.

The 3560CX boasts line-rate performance on all ports. The power options supported by this smaller Catalyst switch are similar to the higher-end 3650 and 3850 models, delivering up to 240 watts of PoE power. The below picture shows a fixed-configuration Catalyst 3560CX switch.

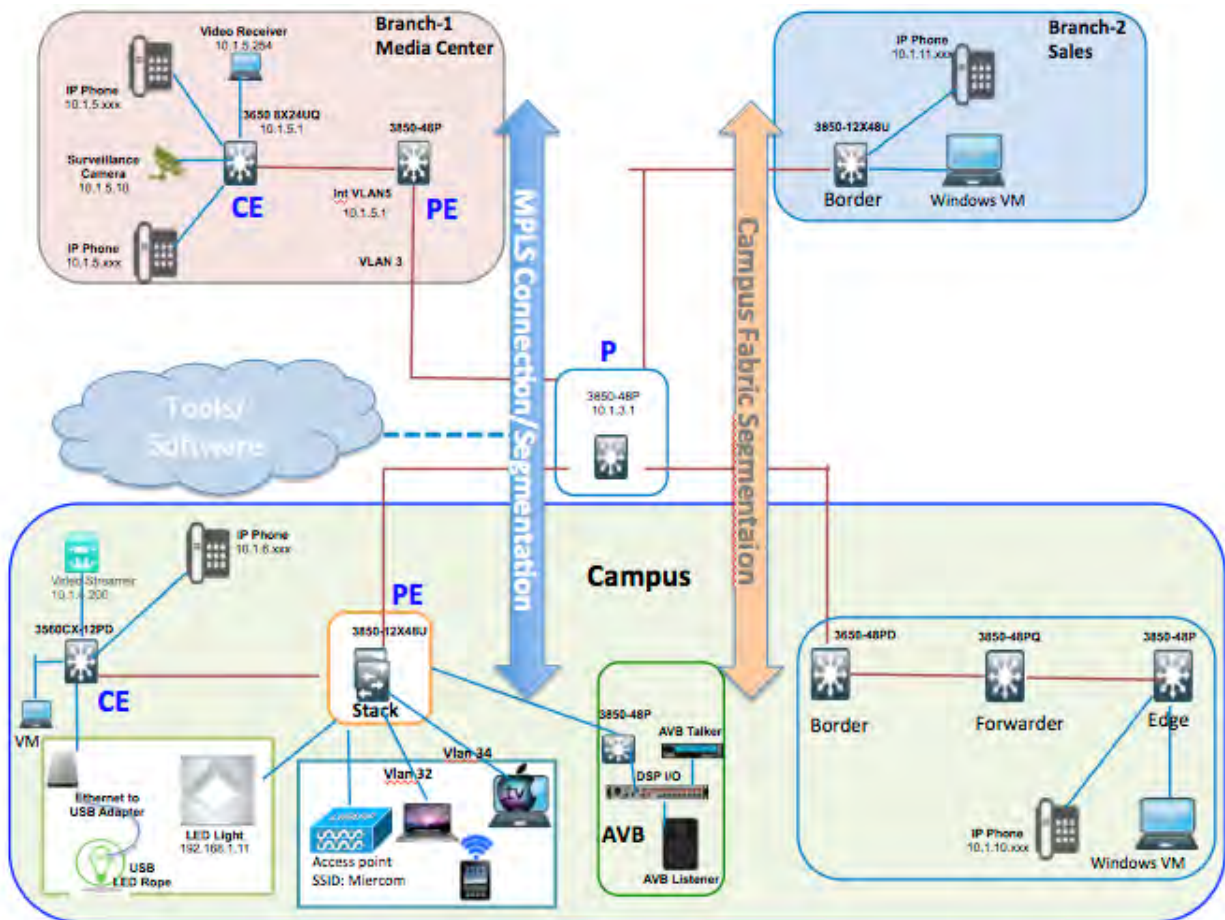


3 - Test Bed: How We Did It

The test bed set up for testing the Catalyst 3850 Series features was as diverse as the features themselves. As shown below, the theme of the testbed was to build a campus simulating a central location and extending two branch locations using different Layer 3 Segmentation technologies that the Catalyst 3850 switch can support due to its advanced programmable ASIC and feature rich software. Each site was centered around one or more Catalyst 3850 switches. Another 3850, at the center of the test bed, provided connectivity between the different sites, endpoints, VLANs, and so on.

A variety of trunk connections were configured, which are discussed more in the following feature sections. In one case IP traffic traversed an MPLS (Multi-Protocol Label Switching) facility. MPLS is in wide use among carriers and service providers, and provides a segregated transport for simultaneously accommodating all manners of traffic to achieve multi-tenancy between customers and necessary isolation throughout the network.

Test Bed Configuration



MPLS transport is featured because the Catalyst 3850/3650 series switches lets the user “segment” and maintain isolation among different traffic types from the very edge/access layer all the way to the destination network. The network topology no longer requires another device to provide the necessary isolation on top of the access switches. Segmentation and isolation can be based upon different customers in Service Provider environments, different Departments in an organization or handling of different user traffic priorities. The QoS (Quality of Service), and other traffic-handling policies, can be applied to these segments to assure adequate transport quality and capacity for any business-critical operation requiring a guaranteed set of resources for performance or privacy reasons.

The segmentation capability can be addressed using Campus Fabric, a building block for Cisco’s next generation Enterprise architecture. Campus Fabric interconnects endpoints such as hosts and applications by using a virtual network and enforcing access control policies with a policy-driven segmentation model.

As more and more IOT devices are connected to the network, segmentation is an essential component to keep them separate from the user community.

The computers pictured in the test-bed diagram are all VMs (Intel-based Virtual Machines) running on UCS (Unified Computing System) machines.

Features Tested:

The observations and conclusions of our feature testing are detailed in the following six sections in this report. The sections and specific features examined in each one are:

Section 4: Power Options, including Perpetual PoE and Stack-Shared Power Supplies.

Section 5: Controlling the Internet of Things (IoT), including support for the Constrained Application Protocol, or CoAP.

Section 6: Application Visibility and Control, to monitor, restrict, rate limit applications, identify performance issues and insure appropriate QoS settings are applied.

Section 7: Segmentation, using Campus Fabric and MPLS features to segment and maintain path isolation among business-critical applications.

Section 8: Traffic Capture and Analysis, using NetFlow, StealthWatch, ERSPAN, and vNAM to monitor and analyze traffic.

Section 9: Wired and Wireless Convergence with Services (mDNS), including Audio and Video Bridging.

4 - Power Options

Feature tested

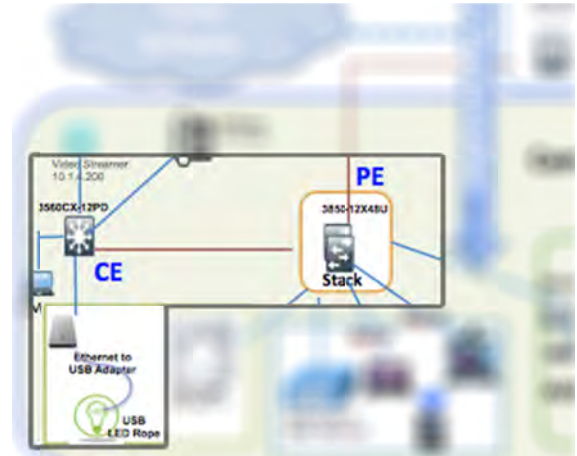
- **Stack Power:** power is shared across the stack. Therefore if one power supply fails, the remaining power supplies will keep all switches in the stack running, provided there is sufficient power to satisfy the power requirements of all the switches in the power stack. This is not only for redundancy purposes, but can also be used when more PoE power is required on one switch in the power stack due to PoE endpoint consumption.

How we did it

The graphic to the right shows the area of the test bed involved in this testing.

For testing the stack power, we set-up two 3850 switches in a stack, each cross-connected to stack power supplies. Power is shared across the stack, so that if one power supply fails, the remaining power supplies will keep all switches in the stack running.

After properly connecting the switches and power supplies, one of the power supplies was abruptly disconnected.



For testing Perpetual Power-over-Ethernet (PPoE), an LED rope light was connected via an RJ-45 copper Ethernet link on a PPoE port, as seen in the pictures below. The switch powered up and the light came on. Then the switch was rebooted and the LED rope light and the PPoE-connected light both remained lit through the re-boot process. Next, we failed one power supply and the remaining supply continued to provide sufficient power for the lights to remain lit.

Conclusion

Performed as expected. Because the Cisco 3850's were configured as a stack of two systems with cross-connected power supplies, the power is shared between the systems and if one power supply goes down, the remaining power supplies continue to power both boxes. After failing one power supply, both switches continued working. In addition, the rope light on the PPoE port remained lit as long as one or more power supplies remained powered up.

The LED rope light came on when its PPoE port activated as the switch powered up. With high availability enabled on the PPoE port, the light stayed on while the switch rebooted.



Light off

Light on

5 - Controlling the Internet of Things (IoT)

Cisco planners surmise that currently, 99 percent of physical objects that may one day join the Internet are still unconnected. A collaborative research effort, made up of DHL Trend Research and Cisco Consulting Services, estimates in its *Internet of Things in Logistics* report that 15 billion devices were connected to the Internet as of 2015, and projects it will grow more than 250 percent, to over 40 billion, by 2020 because of the Internet of Things (IoT).

One of the more promising protocols that is gaining traction for the IP-based management of IoT devices is the Constrained Application Protocol, or CoAP, embodied in IETF proposed standard 7252, issued in June 2014. CoAP is a Web transfer protocol – that is, it provides a simple request/response interaction model between endpoints. It has a built-in discovery capability, low overhead, and was recently enhanced with the ability to move large blocks of data, such as for software downloads.

All that's required in such devices is an 8-bit microprocessor and a little RAM and ROM.

Feature tested

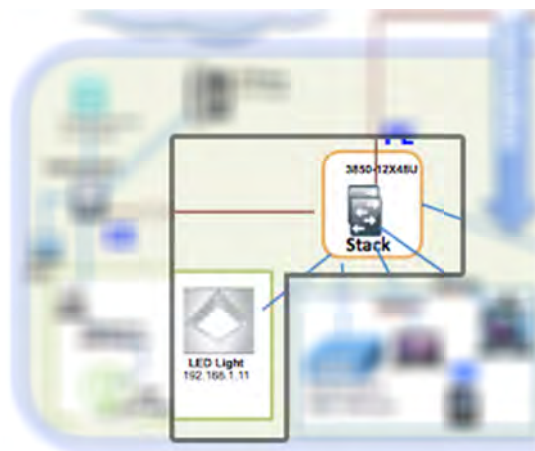
- **CoAP support:** the ability of the 3850 switch to securely communicate with the IoT devices using the Constrained Application Protocol

How we did it

The graphic to the right shows the test bed involved in this testing.

We set-up a video surveillance camera connected to our test-bed network to watch the state of a Molex CoAP-compatible light fixture that was connected to a Power-over-Ethernet port of the Catalyst switch. The light fixture has a center light beacon that we used to demonstrate communication using CoAP IoT protocol.

Using an available Firefox browser plug-in, we sought to change the light colors using the plug-in's simplistic interface (shown on next page). The center beacon on the network-connected light fixture was controlled via a simple RESTful API calls which used JSON (JavaScript Object Notation) as the data-interchange format.

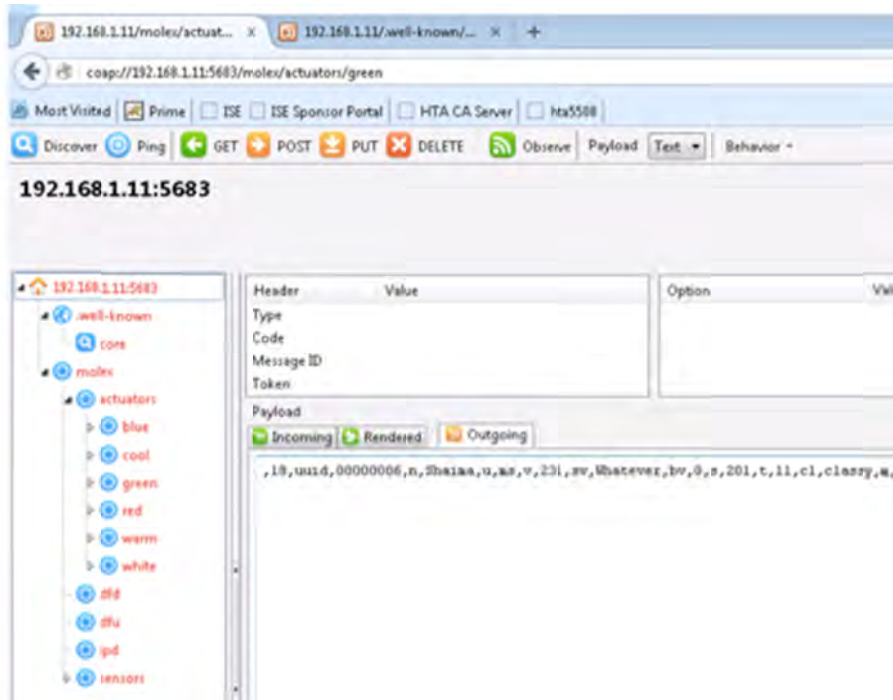


Conclusion

Performed as expected. In fairly short order, we were able to remotely control the light fixture via the CoAP protocol, using the Firefox CoAP plug-in referencing the IP address of the LED light.

As shown on next page, we successfully changed the light fixtures center beacon color.

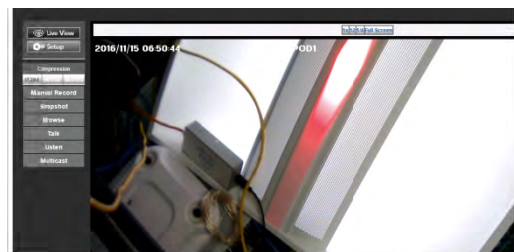
The Firefox browser plug-in provides this simple interface that we used to change the color of a remote, CoAP-supporting, IP- and PoE-connected light panel.



Via this interface we successfully changed the color of the central light panel from purple, to red and to green, and recorded the changes via the video surveillance camera.



Light panel changed via CoAP from purple



to red



to green

6 - Application Visibility and Control

Collectively called AVC, for Application Visibility and Control, the Cisco Catalyst 3850 Series offers several related features for tracking traffic by application and defining network configurations to expedite important business-critical traffic and relegate or block the rest.

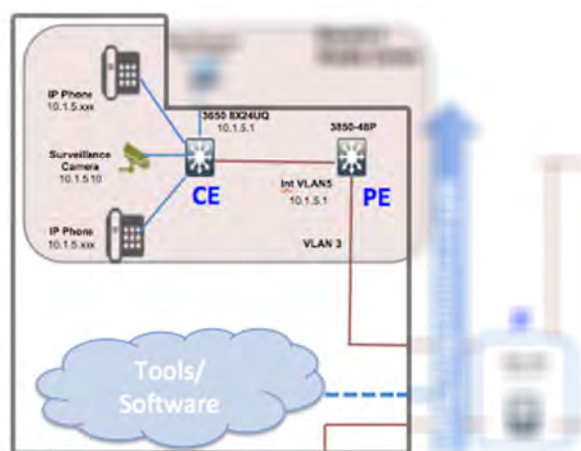
Feature(s) tested

- **Application Visibility and Control (AVC):** monitoring application traffic, restricting and rate-limiting malicious applications and traffic from accessing the network, identify application performance degradation and insure that the appropriate QoS treatment is applied.

How we did it

The Cisco Application Visibility and Control is a suite of services integral to the Catalyst 3850/3650 Series. It is also included in select Cisco ISRs (Integrated Services Routers) and many Cisco Wireless LAN Controllers.

AVC uses multiple technologies to recognize, analyze, and control over 1500 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools.



The AVC suite of services include: NBAR2 (second generation of Cisco's Network Based Application Recognition), NetFlow v9 and IPFIX for collecting and exporting metrics, Cisco Quality of Service controls, Deep Packet Inspection, and management and reporting software such as Cisco Prime or third-party packages. These AVC capabilities, when combined with Cisco StealthWatch security system, turns the 3850/3650 switches into Security Sensors, capable of detecting denial-of-service attacks, anomaly detection, and automatic quarantining of malicious endpoints.

The combined capabilities of Cisco AVC are impressive, and include:

- Application identification and classification
- Monitoring by-application flow statistics like latency and response time
- Setting QoS priorities based on application such as YouTube, Facebook, CNN, etc.
- Collection and export of application performance metrics

The test was executed with detailed test profiles and performed by streaming continuous video feed through the switch and then the switch with virtue of AVC/NBAR2 configuration not only identified the traffic rate but also identified video format and application it was receiving. Then we created a QoS policy to police video application traffic (specifically, in an MPEG-2 transport stream format) and observed degraded video quality. The policy was then removed, using the YANG Explorer (YTool). Video traffic was then restored to its original quality.

Conclusion

Performed as expected. We observed that AVC identified and correctly reported the video traffic played and the traffic slowing down on the GE interface, in accordance with the policy and class map set as part of the AVC configuration.

Configuration and provisioning of the Catalyst 3850 was straightforward and more automatable with the Campus Fabric.

7 - Segmentation

Network breaches have become common for enterprise customers. Network Segmentation is one of the key components to secure and isolate users or services. It is also one of the key features, which provides security and containment from any attacks that occur on a particular network segment. If the attack does occur on a network segment, by the virtue of segmentation, other network elements will not be affected. The Catalyst 3850/3650 Series switches provide multiple segmentation options: VRF Lite, Campus Fabric and MPLS.

Feature(s) tested

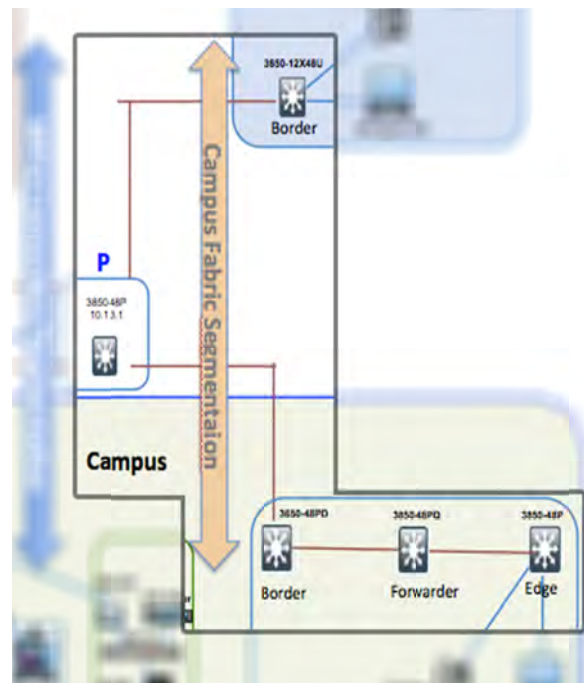
- **Campus Fabric:** Provides network virtualization with path isolation and policy-based segmentation within the virtual network using Scalable Group Tag's and Security Group ACLs (Access Control Lists).

How we did it

The graphic to the right shows the area of the test bed involved in this testing.

Cisco's Campus Fabric architecture is comprised of the underlay and overlay network. The underlay network is made up of physical switches with IP connectivity established via any routing protocol. The overlay network consists of the control plane (standards-based LISP map-service), and the data plane. The control plane maintains the location mapping of the underlay endpoints and assigns roles to the endpoints based on their location in the fabric and their functions. The data plane (VXLAN based encapsulation), is responsible for forwarding in the fabric. Policy Segmentation comes from the TrustSec implementation of Scalable Group Tag (SGT). An SGT is assigned to each user defined group and the Security Group ACL's restricts the communication between them.

The overlay network also assigns specific roles to the switches based on their location in the fabric and their functions; Fabric Edge is typically where encapsulation/decapsulation occurs for the connected end points, Forwarder/intermediate node forwards the traffic based on IP underlay protocol and it does not have to be fabric aware (no VXLAN encapsulation), and Border node is the demarcation point for the fabric and non-fabric site.



Test bed section involved in Campus Fabric/segmentation testing.

The test was performed by defining two virtual networks called *IP Phones* and *Multimedia*. Each Virtual Network could have multiple user groups, we had VoIP end points, Contractors and Guest user groups in the *IP Phones* Virtual Network and video end points; Executives and Employee user groups in the *Multimedia* Virtual Network. Network segmentation and virtualization was achieved by virtue of virtual networks (like VRF's), and Policy based segmentation was achieved within the virtual networks by setting different level of permissions based on roles assigned to individual user groups, i.e., in the *IP_Phones* VN, Contractors were permitted access to VOIP services but Guest were denied access and similarly in the *Multimedia* VN, Executives were permitted access to the video resources but not the Employee.

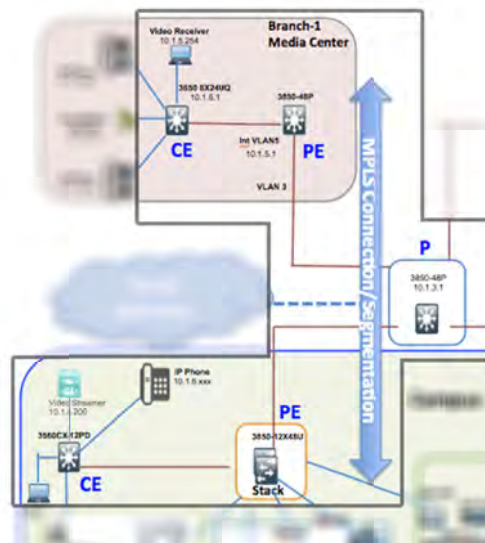
Feature(s) tested

- **MPLS:** Provides network segmentation and maintains path isolation among business-critical applications throughout the L3 network using VRF (virtual routing forwarding) and L3VPN.

How we did it

The graphic on the right is where we tested the MPLS based segmentation, which is the traditional way of segmenting based on VRF's. MPLS Architecture also comprises of underlay and overlay network. The underlay network consists of IP connectivity between the switches via any routing protocol and Overlay network comprises of Label distribution protocol (LDP) and Multi-protocol BGP for L3VPN.

The test was performed by defining the same virtual networks (*IP Phones* with VOIP Services) and (*Multimedia* with Video Services) as above on the provider edge switches (PE) and MPLS was configured on the links between three switches in different buildings as shown in the diagram. Then two L3 VPN tunnels were configured between the PE switches using the MP-BGP for both virtual networks (*IP_Phones* VRF and *Multimedia* VRF). The Provider Switch (P) acts like a core intermediary device, which forwards the traffic based on the label distribution protocol (LDP). This is the traditional form of segmentation, where network virtualization is achieved by MPLS L3 VPN.



Test bed section involved in MPLS/segmentation testing.

Conclusion

Performed as expected.

Campus Fabric provides dual level of segmentation. Network Virtualization is achieved by defining individual virtual networks, Policy based segmentation is ensured by assigning unique SGTs to all user groups and SGACLs are used for selective access between the different user groups within the virtual networks.

Network Virtualization can also be delivered by the traditional way of using MPLS L3VPN.

We found the configuration and provisioning of the Catalyst 3850 very straightforward with both the technologies, albeit more secure and granular control with Campus Fabric.

8 - Traffic Capture and Analysis

The Catalyst 3850/3650 Series supports numerous features to enable network administrators to track, capture and analyze traffic.

Feature(s) tested

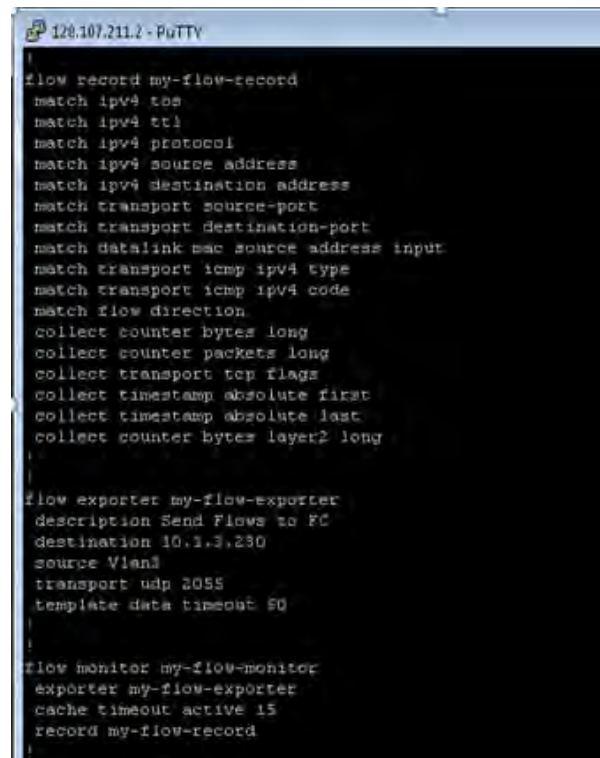
The features tested for this report included:

- **NetFlow:** data capture, which has become the de facto standard mechanism and format for collecting network data according to user-specified criteria.
- **Cisco Lancope StealthWatch:** software including management console for analyzing captured NetFlow-captured data.
- **ERSPAN:** Encapsulated Remote SPAN, or Switched Port Analyzer, the latest enhancement to SPAN and RSPAN (Remote SPAN), where traffic from one or more switch ports or VLANs is mirrored to one or more destination ports on another switch over GRE/IP for analysis.
- **vNAM:** Virtual Network Analysis Module, a component of Cisco Prime network management, provides Layer 2-7 application visibility using Cisco Network-based Application Recognition 2 (NBAR2).

How we did it

The StealthWatch system consists of several individual components. The minimum deployment consists of a StealthWatch FlowCollector and a StealthWatch Management Console (SMC). SMC was installed on a Virtual Machine. We then directed a Catalyst 3850 to configure and execute a NetFlow collection and export (see IOS command-line instructions to the right).

Setting up a NetFlow capture is a straightforward process. The user needs to first determine what data to meter, and then where to send the captured data. The user sets the parameters for caching the captured data and assigns the NetFlow to a specific 3850 port or VLAN. Via the IOS command line we

A screenshot of a terminal window titled "128.107.211.2 - PuTTY". The terminal displays a series of NetFlow configuration commands in IOS syntax. The commands are:

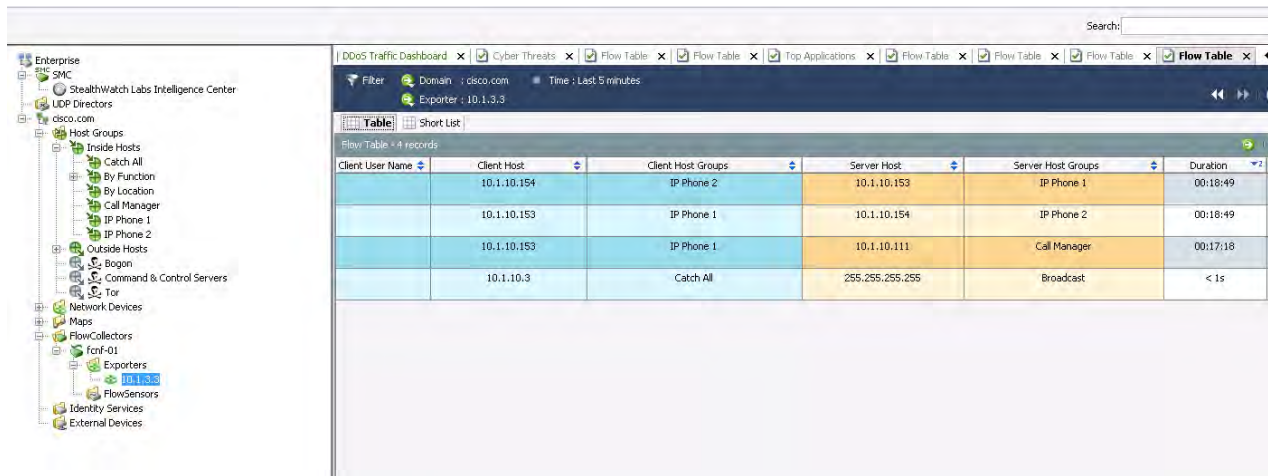
```
flow record my-flow-record
match ipv4 tos
match ipv4 ttl
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match datalink mac source address input
match transport icmp ipv4 type
match transport icmp ipv4 code
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect counter bytes layer2 long

flow exporter my-flow-exporter
description Send Flows to FC
destination 10.1.3.230
source Vlan3
transport udp 2055
template data timeout 50

flow monitor my-flow-monitor
exporter my-flow-exporter
cache timeout active 15
record my-flow-record
```


then verified the flow-monitor cache, and that we were in fact collecting and exporting the data we wanted. We opened a StealthWatch window via Google Chrome, from which we could select and view the captured flows.

An example of selecting flows and header information to capture, which can be viewed through the StealthWatch GUI, is shown below. NetFlow and StealthWatch are heavily used to identify which flows (users and applications) are consuming the most network bandwidth.



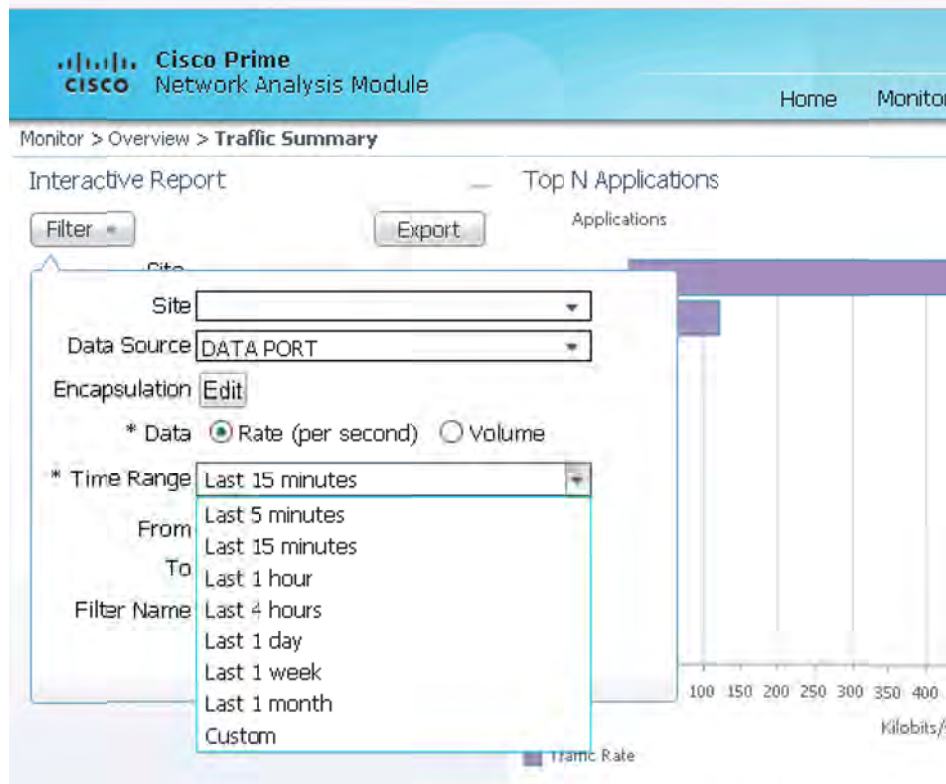
Encapsulated Remote SPAN (ERSPAN) and Virtual Network Analysis Module (vNAM)

ERSPAN and vNAM together perform functions similar to NetFlow and StealthWatch, with some notable differences. ERSPAN, which is also supported integrally by the Catalyst 3850/3650 Series, is designed to mirror all (or subset of) the traffic, in one direction or bi-directionally, of a specified port or ports, or a particular VLAN, and send a copy of the traffic through a secure GRE (Generic Routing Encapsulation) tunnel to one or more destination ports for subsequent analysis. The GRE can even traverse a service provider's MPLS network, as might be the case in retrieving data from a branch office by the head office.

In addition, vNAM, a component of Cisco Prime network management, performs deep packet inspection and some analytics that StealthWatch does not. For example, vNAM can calculate and report the Mean Opinion Score (MoS) for a site.

We set up an ERSPAN copy from a port on one 3850, to mirror all data in both directions to a port on a remote 3850, to which the vNAM analyzer was connected. We then opened a Google Chrome browser window to vNAM, and we established a VoIP phone call through the 3850 port being mirrored.

The vNAM interface for selecting the phone call of interest is shown below



Interactive Report: Filter Export

Site:
 Data Source: DATA PORT
 Encapsulation: Edit
 * Data: Rate (per second) Volume
 * Time Range: Last 5 minutes
 From: 2016-Nov-16, 04:06
 To: 2016-Nov-16, 04:11
 Filter Name:

RTP Streams

Time	Poor	Fair	Good	Excellent
2016-Nov-16, 04:10:58	0	0	0	2
2016-Nov-16, 04:09:58	0	0	0	2
2016-Nov-16, 04:08:58	0	0	0	2
2016-Nov-16, 04:07:58	0	0	0	2
2016-Nov-16, 04:06:58	0	0	0	2

RTP Conversations

The above vNAM interfaces allow the user to select specific VoIP calls appearing on a remote mirrored port or VLAN. This is incredibly helpful in diagnosing VoIP network problems.

Conclusion

Performs as expected. Once properly set-up, we could effectively use the StealthWatch Management Console to analyze data we specified, which was captured and exported by NetFlow.

Once set-up, ERSPAN and vNAM were able to analyze a specific phone call and provide clear call-quality ratings.

9 – Wired/Wireless Convergence With Services (mDNS)

An integral feature of the Catalyst 3850 is a built-in Wireless LAN Controller. A single high-end 3850 can manage up to 100 APs and up to 2,000 WiFi endpoints. The Catalyst 3650 can manage up to 50 APs and 1,000 WiFi clients. With the integrated nature of the WiFi support, the 3850/3650 Series achieves wired LAN convergence with wireless, transparently interconnecting WiFi and wired endpoints along with VLANs.

Feature(s) tested

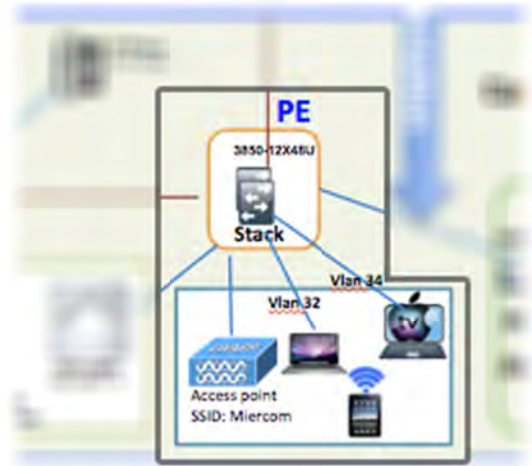
- **Wired to Wireless:** examining quality of video across wired, wireless and multiple VLANs, between Apple endpoints using mDNS Gateway.
- **Audio Video Bridging (AVB):** based on IEEE 802.3ba, provides better audio and video experience through improved time synchronization and QoS.
- **Apple's mDNS Gateway:** to facilitate Apple TV configuration.

How we did it

The graphic to the right shows the test bed involved in this testing. We set up endpoints for the delivery of time-sensitive traffic, in this case audio and streaming video, between WiFi and wired endpoints through the 3850 switch.

Using an iPad as the source, we plugged the "audio out" into a Digital Signal Processor, connected to an IP address of the 3850 switch. The 3850 forwarded the traffic to a digital speaker.

We also then deployed a wireless Apple TV for delivery of streaming video through the 3850, to wired endpoints and across multiple VLANs. This test used Bonjour, Apple's implementation of the mDNS protocol, which facilitates network-device configuration through service and device discovery, address assignment and hostname resolution.



Conclusion

Performs as expected. With built-in support for IEEE 802.3ba AV Bridging (AVB), the 3850 assured clear and continuous audio transmission from WiFi to wired endpoints. Indeed, the test showed that the 3850 could be used as an Audio/Video bridge using DSPs.

Similarly, Apple TV could deliver clear and continuous streamed video between WiFi and wired endpoints and across multiple VLANs through the 3850 switch.

10 - Supported Cisco Features (16.3.1 Release)

Power Differentiators	
Feature(s)	Cisco
UPoE	✓
Fast PoE	✓
Perpetual PoE	✓
Stackpower	✓
Segmentation Differentiators	
Feature(s)	Cisco
MPLS	✓
Campus Fabric with LISP and VXLAN	✓
IoT Differentiators	
Feature(s)	Cisco
CoAP Gateway	✓
Visibility Differentiators	
Feature(s)	Cisco
ERSPAN	✓
NBAR2	✓
Flexible NetFlow	✓
Wired/Wireless Convergence Differentiators	
Feature(s)	Cisco
Wireless Controller in switch with wireless terminated in switch ASIC	✓
AVB	✓
mDNS Gateway	✓

11 - About Miercom Performance Verified Testing

This test was sponsored by Cisco Systems, Inc. The data was obtained independently by Miercom engineers and staff as part of our Performance Verified program. This testing is based on a methodology that is co-developed with the sponsoring vendor. The test cases may be designed to focus on specific performance or features of the product(s), and either validate or repudiate those claims. The results are presented in a report, where the content is independently written by Miercom.

12 - About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

13 - Use of This Report

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems, Inc. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.