



Bluesocket's Edge-2-Edge Architecture

Introduction

Edge-2-Edge (E2E) is a Bluesocket solution that provides flexibility in the way that Bluesocket APs (BSAP) are deployed with Bluesocket controllers (BSC) and also how wireless client traffic is handled by the BSAP.

In the past, all traffic to and from the BSAP was tunneled to and from the BSC via layer 3 tunnel. E2E enables customers to design their network so that some of their wireless traffic is tunneled to the BSC and some of their wireless traffic is dropped locally onto the layer 2 network. This ability to determine where traffic is forwarded enables network configurations that were previously no possible.

Remote office deployments where the BSC is located at the corporate facility and the BSAP is deployed at the remote office can present a few obstacles especially when a wireless client tries to access devices at the remote office such as a printer. E2E addresses this problem by switching the wireless client's traffic to the local subnet.

Bluesocket decided to have a phased approach for the E2E solution. The initial implementation focuses solely on the data plane functionality (i.e. how the traffic should be switched at the BSAP). As we get feedback on this solution, we are working on the control plane functionality which outlined in the "Future Work" section below.

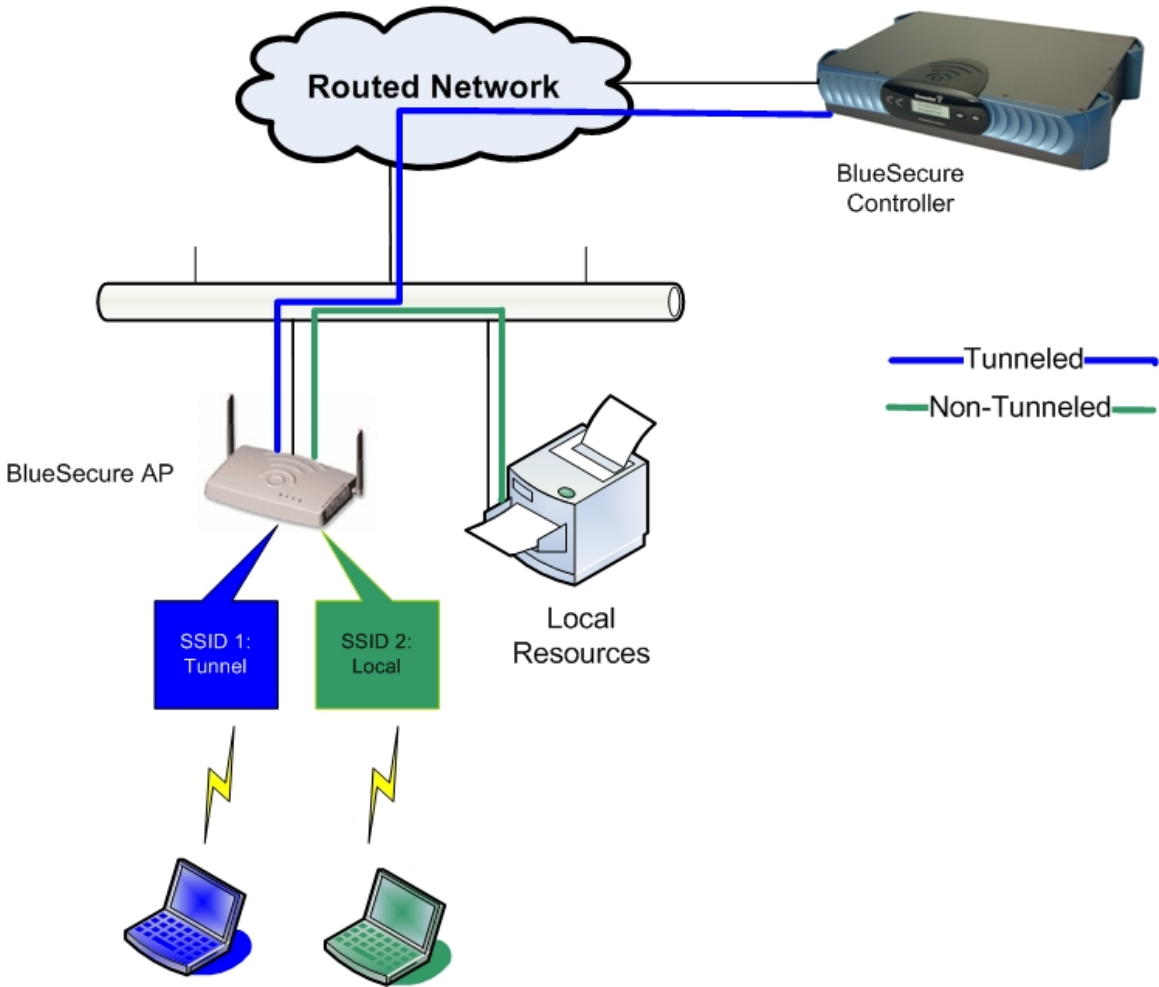
Software Versions

E2E support is fully supported in BSC releases 6.1 and later. The following matrix shows support in previous releases:

Platform	5.2	5.3	6.0	6.1
BSC	Not Supported	Bluepatch required + special	Enable as a special	Supported
BSAP15x0	Not Supported	5.3.2.0 and later	Not Supported	Supported
BSAP1700	Not Supported	Not supported	Not Supported	Supported

How Edge-2-Edge Works

E2E is configured on a per SSID basis. Traffic from a wireless client which is connected to an E2E-enabled SSID (i.e. Local) is bridged directly to the local subnet. Traffic from a tunneled SSID (i.e. Tunnel) is encapsulated in an EtherIP tunnel and forwarded to the BSC. The following diagram depicts the two scenarios.



In order to better understand the architecture, here are common questions about the E2E solution.

Do the BSAPs need to be connected on the BSC's managed-side?

No. The BSAP can be deployed across a routed network either on the protected or managed (i.e. remote managed subnets), directly on the protected-side subnet, or directly on the managed-side subnet.

Does the BSC do client authentication for wireless clients on an E2E-enabled SSID?

It depends on where the BSAP is connected and what resources the wireless client is trying to access.

If a BSAP is on the protected-side of the BSC, wireless clients connected to an E2E-enabled SSID won't authenticate with the BSC.

If the BSAP is on the managed-side of the BSC, wireless clients connected to an E2E-enabled SSID only authenticate with the BSC if they need to gain access to resources that are on the protected-side of the BSC (i.e. corporate resource, internet access, etc). If the wireless client only needs access to resources are on the managed-side, the wireless client never authenticates with the BSC. This is the model that is synonymous with Fat APs (i.e. Cisco 1100/1200)

In order to fully leverage BSC's security capabilities, the recommended deployment is on the managed-side either on a remote managed subnet or the same subnet.

Are wireless clients that are connected to an E2E-enable SSID tracked by the BSC?

Again, it depends on where the BSAP is connected and what resources the wireless client is trying to access.

If a BSAP is on the protected-side of the BSC, wireless clients connected to an E2E-enabled SSID won't be in the connection table. They will show-up under the AP Status as associated clients, but they are not tracked by the BSC.

If the BSAP is on the managed-side of the BSC, wireless clients connected to an E2E-enabled SSID will show-up in the BSC connection status since they pull an IP address from the BSC's DHCP server. However, they will remain in the unregistered role status if they only access resources on the managed side of the network.

Does the BSAP support VLAN trunk links when E2E is enabled?

The BSAP supports 802.1Q trunk links and can drop non-tunneled wireless traffic on any VLAN either native or non-native.

Since the non-tunneled traffic isn't being handled by the BSC, it is recommended that VLAN switches are used to control access. An SSIDs with E2E enabled should be configured with a non-native VLAN so the traffic is sent through an 802.1Q trunk link to a VLAN switch, where it can be distributed based on policies setup the by customer.

Can the BSAP have a mixture of E2E-enabled SSID and tunneled SSIDs?

Yes. The BSAP can be configured with all tunneled SSIDs, all E2E-enabled SSIDs or a mixture of both.

In addition, a tunneled SSID and an E2E-enabled SSID can share the same VLAN id. For example, a tunneled SSID (i.e. Corp) and a E2E-enabled SSID (i.e. Eng) are configured for VLAN id 2. All wireless traffic on the "Corp" SSID is tunneled to the BSC where the outer packet uses the native VLAN and the inner packet uses the VLAN id of 2; all switches between the BSAP and the BSC handle the traffic on the native VLAN. In the case of wireless traffic on the "Eng" SSID, the BSAP switches the traffic onto a trunk link using VLAN id of 2.

How is layer 2 security handled on the SSIDs which are E2E enabled?

SSIDs which are E2E enabled support all the standard encryption methods including WEP, WPA-PSK, WPA2-PSK, WPA/WPA2 with 802.1x.

Layer 2 encryption of wireless traffic is done by the BSAP; the BSC isn't involved in layer 2 encryption. However, key management of 802.1x sessions is handled the same way regardless of the E2E configuration. All EAP messages from the BSAP to the authentication server (i.e. RADIUS) are encapsulated and forwarded to the BSC over the EtherIP tunnel. Therefore, an authentication server cannot be deployed at a remote office since all the EAP messages are forwarded to the BSC.

How is IPSec traffic handled when E2E is enabled?

If the IPSec session is terminated at the BSC, all traffic must be forwarded to the BSC (obviously). If E2E is enabled on the SSID, the BSAP doesn't tunnel the traffic. If E2E is not enabled, the BSAP tunnels the traffic via EtherIP.

How is client-2-client functionality impacted?

The client-2-client options are limited for E2E-enabled SSID. The client-2-client options are Allow, Block, and Forward to BSC. Here are a few quick descriptions:

Allow:

The BSAP allows wireless clients to communicate without going through the BSC.

Block:

The BSAP drops any traffic from a wireless client that is destined for another wireless client.

Forward to BSC:

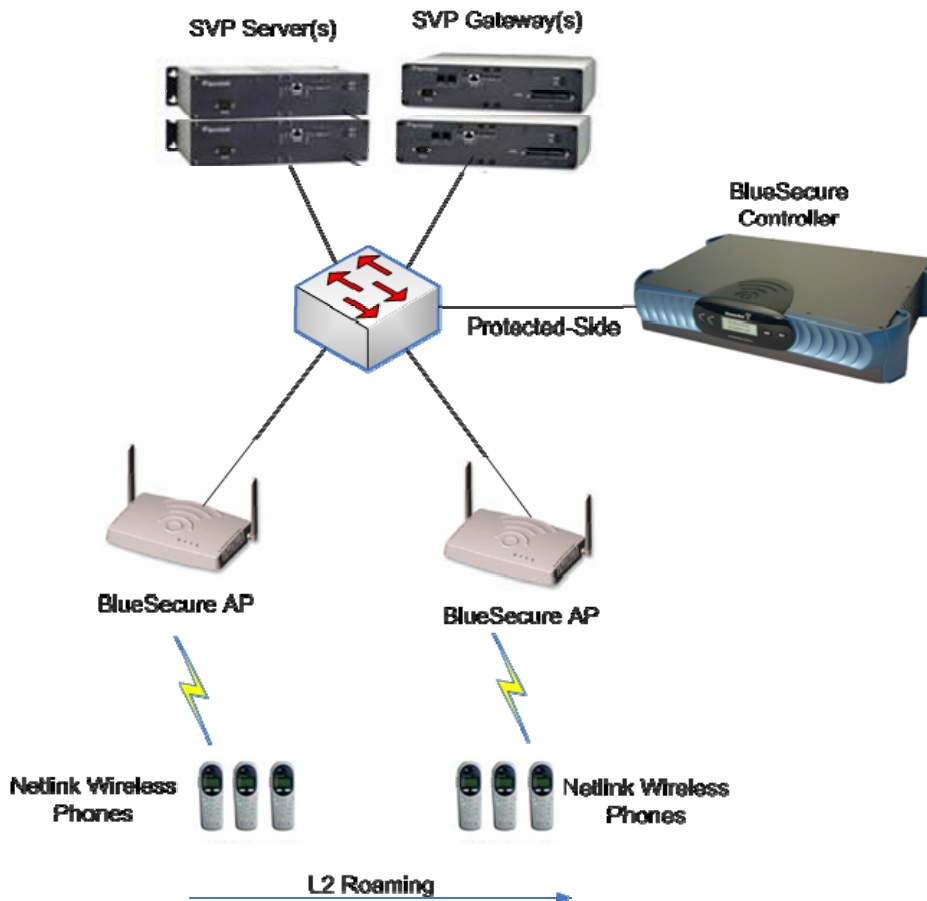
The BSAP forwards all traffic to the BSC and allows the BSC to make the decision whether the wireless clients can communicate.

When an SSID is E2E-enabled, the only two options are Allow and Block. The Forward to BSC option is grayed out.

What is the dependency of E2E with Spectralink?

During VIEW certification, we determine that the Bluesocket system must support multiple SVP servers and SVP gateways in order to achieve VIEW certification. In BSC Release 5.3, the Voice tab only provided the option to enter a single SVP server and gateway. Due to this limitation, we decided to propose the E2E solution since it was available in the BSAP.

The E2E solution works very well with Spectralink since their system was designed for layer 2 deployments rather than layer 3 deployments; therefore we completed the certification with E2E enabled. The Bluesocket Configuration and Deployment guide that is listed on the Polycom (aka Spectralink) website describes the setup using the E2E solution. No other configurations (i.e. through the BSC) are supported by Spectralink at this time. The following diagram shows the deployment scenario of E2E with the Spectralink system.



Should E2E be enabled for all voice applications?

Not necessarily. There is no evidence that the BSC introduces any significant jitter into the voice stream; however the E2E solution does take the BSC out of the equation in certain deployment scenarios.

Recent BSC platforms have been architected to minimize jitter for voice applications, so a customer has the options allow voice traffic to be handled by the BSC or use E2E.

Should E2E be used to offload wireless clients that are passing traffic at 802.11n rates?

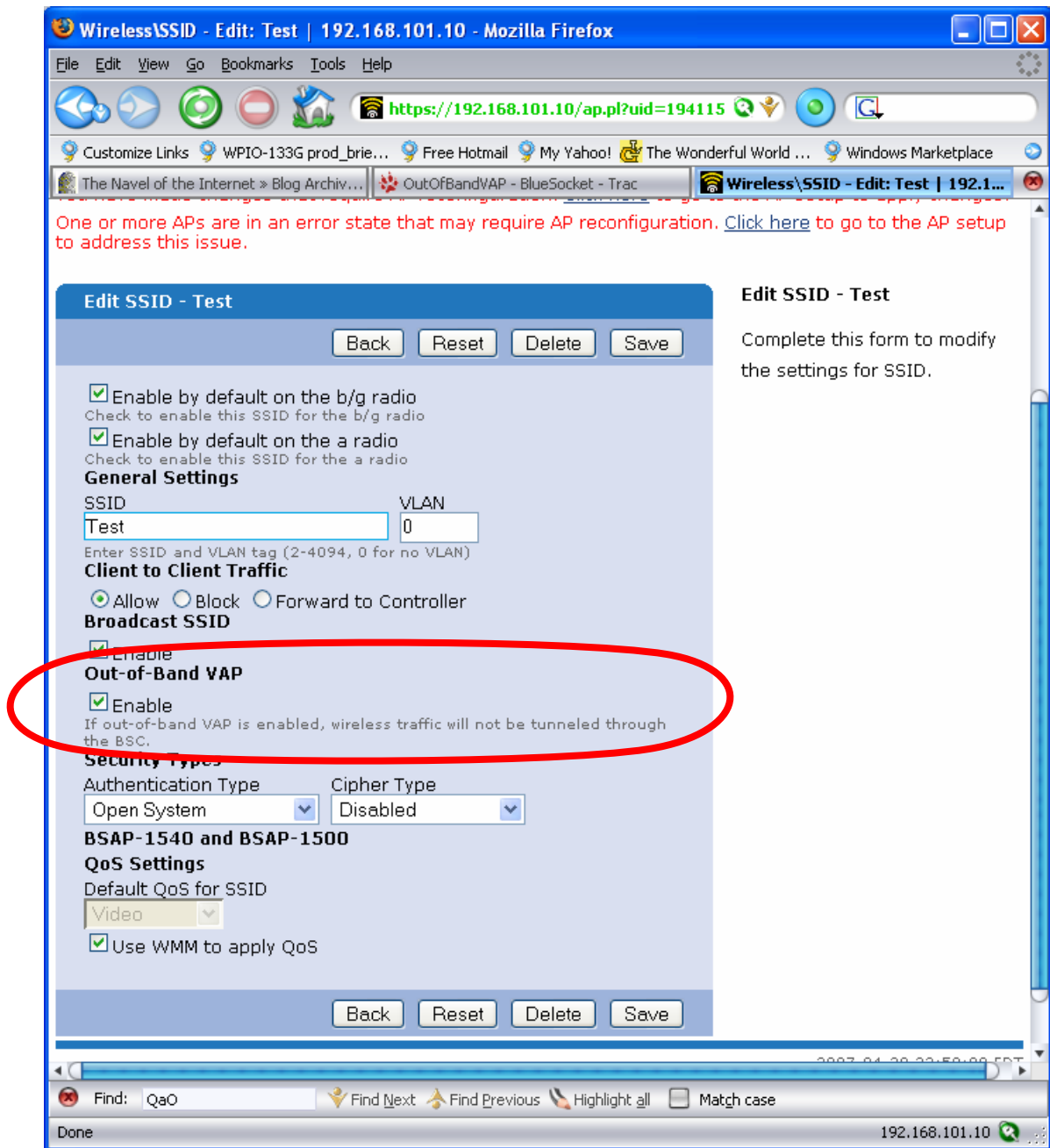
This isn't a big concern in the short-term because there are very few 802.11n clients. Once 802.11n is ratified and the next-generation 1700 is available, appropriate network design will be required and E2E could be a part of the design. It will depend on the BSC model and the number of APs supported.

The current BSAP1700 is capable of a peak throughput of 130Mbps with an appropriate MIMO client. If a customer is interested in testing MIMO speeds on the BSAP 1700 using a BSC 400, they need to enable E2E because the BSC 400 doesn't have a gigabit interface. If the customer is using a BSC 5200, E2E isn't necessary to test MIMO rates.

Configuring E2E on a Bluesocket System

As mentioned previously, the E2E is enabled per SSID. Navigate to the Wireless->SSID tab and select a particular SSID.

The GUI currently refers to the E2E feature as Out-of-Band VAP. Check the Enable box accordingly.



Future Work

Some of the areas that are under consideration are:

1. Always force wireless clients who are on an E2E-enabled SSID to authenticate with the BSC. The BSAP would tunnel the client's traffic regardless of the E2E configuration until the client authenticates. Once authenticated, the BSAP switches traffic to the local network.
2. Switch traffic between tunneled and non-tunneled based on traffic tuple (i.e. source or destination IP and port numbers). Instead of switching traffic per SSID, it would be based on a role or particular user.
3. Enable high available APs with the use of E2E feature.

If the AP loses connectivity to the BSC, the AP will continue to pass traffic on the E2E-enabled SSIDs until the AP discovers another BSC and downloads new configuration. This is particular useful for remote office locations that have a temporary outage on the WAN link.