

# Installing and Configuring

## Advanced Hardware Setups

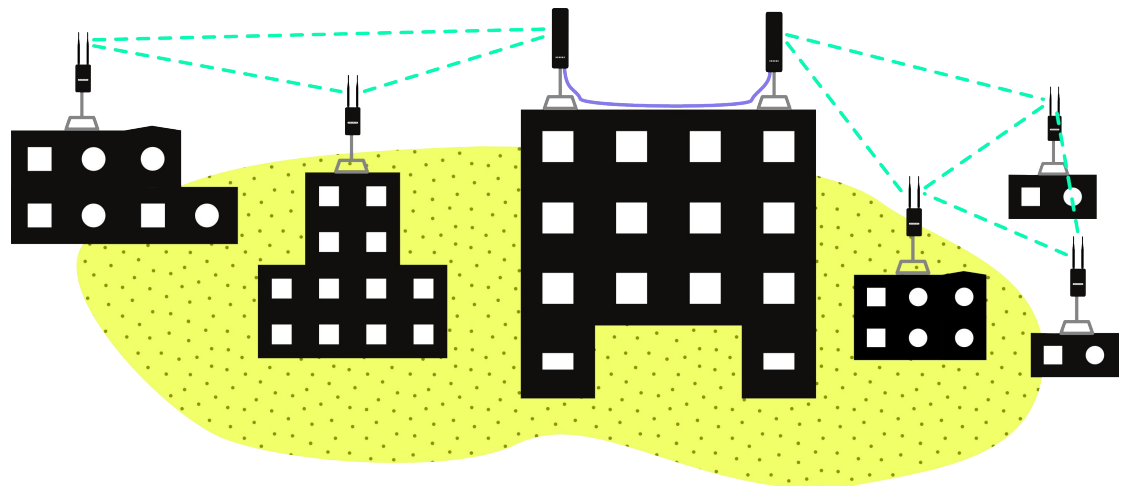
### Introduction

For most community wireless networks, installing a few rooftop and window nodes will fit the needs of the neighborhood or town. For others, more complex installations and configurations will be required. This guide follows and is an advanced companion to **Common Hardware Setups**, which covers the most common and basic Commotion configurations.

Sometimes you will need to connect multiple nodes together at a single site, and this guide will help you do that. Some of the instructions below require some familiarity with networking concepts, so we recommend reading through **Learn Networking Basics** first.

In this document, three types of hardware setups are discussed:

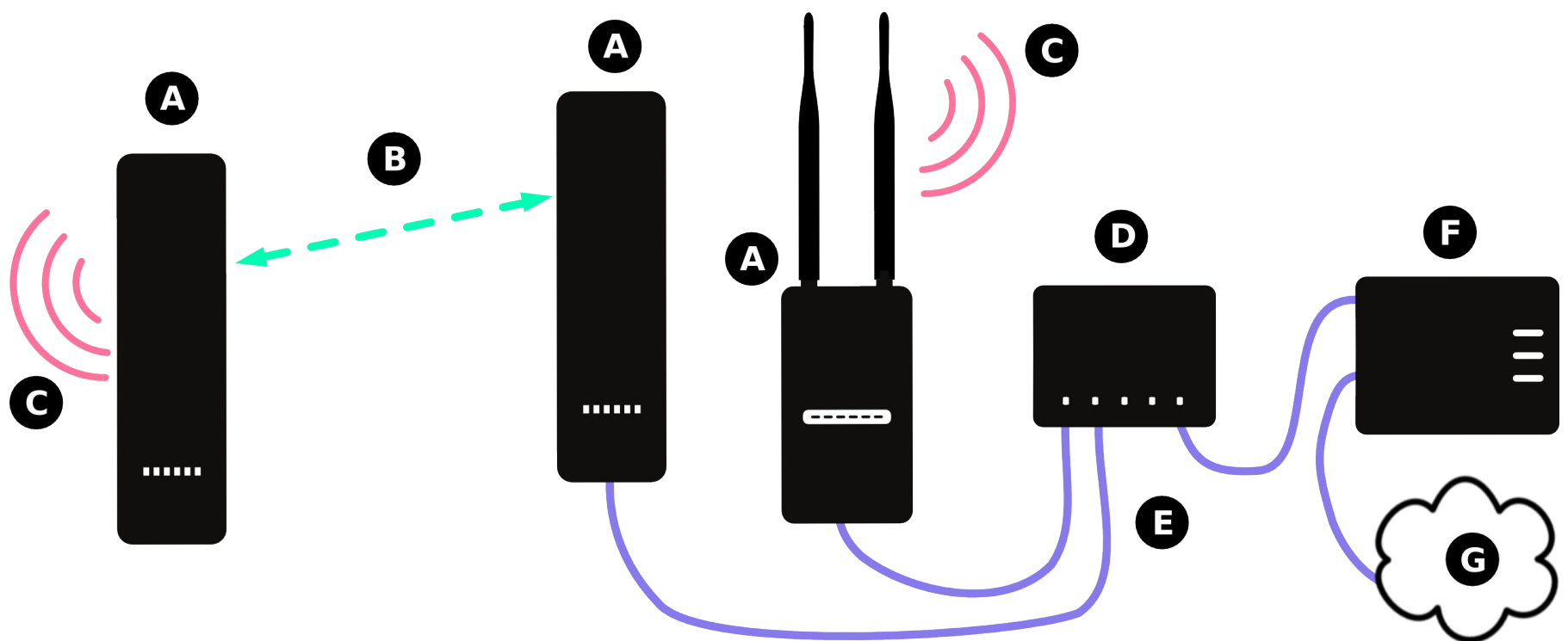
1. Meshing with Ethernet with DHCP
2. Meshing with Ethernet with Static IPs
3. Meshing with Ethernet with a Static Gateway



# Mesh with Ethernet using DHCP

## Using a gateway to the Internet with DHCP for automatic assignment of IP addresses

If you want to provide a gateway connection to the Internet on your mesh network, it helps to use several nodes at the location hosting that connection. This should reduce bottlenecks that would occur if there were only one node connected to that gateway.

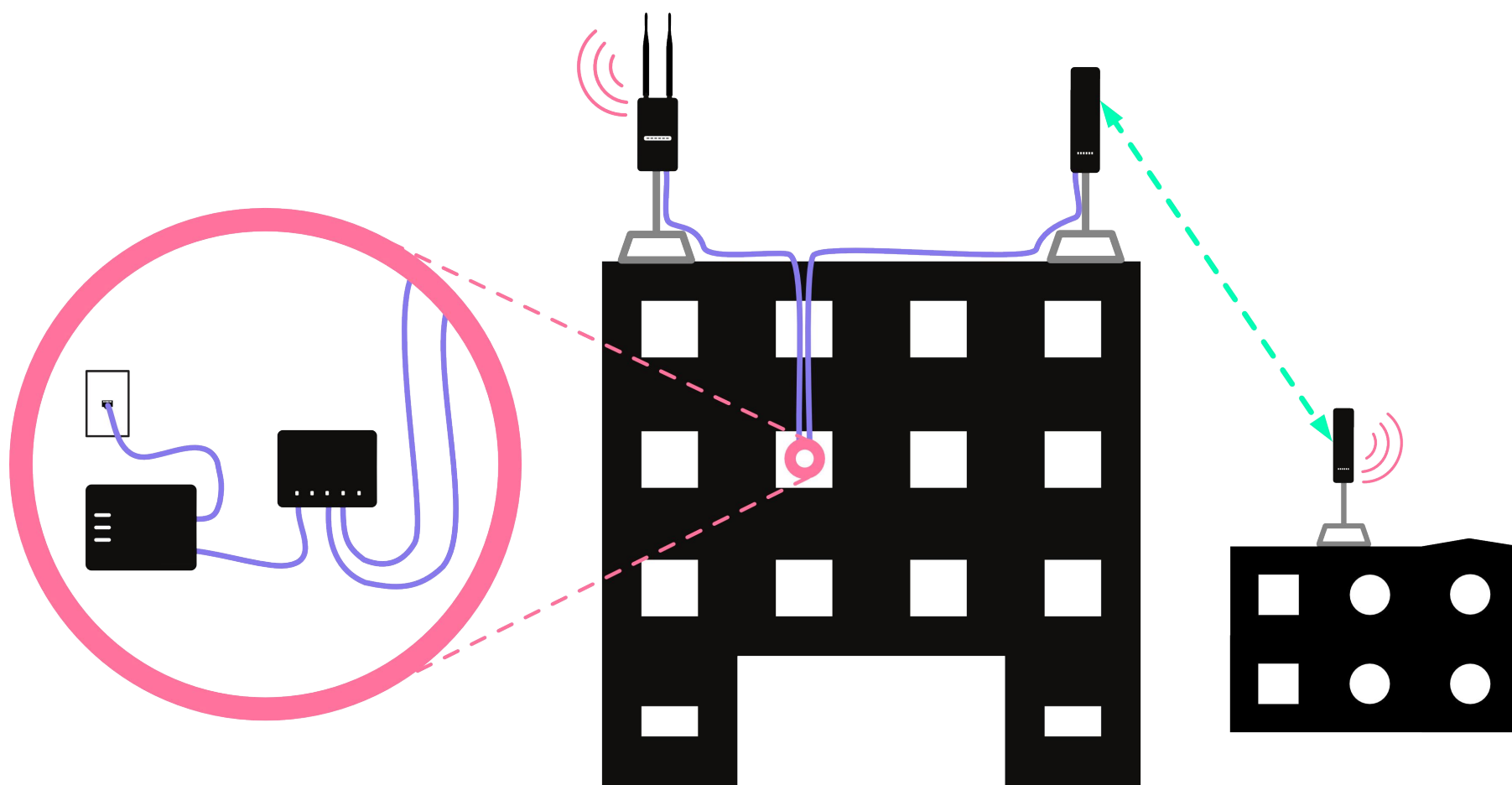


In the diagram above:

- **(A)** Represents a node running the Commotion software.
- **(B)** Represents the wireless mesh links between the nodes.
- **(C)** Represents the Access Point generated by the Commotion node for users to connect to.
- **(D)** Represents an Ethernet switch, which transfers data between all connected devices.
- **(E)** Represents Ethernet cabling connecting the modem and nodes to the Ethernet switch.
- **(F)** Represents the modem or router from the Internet Service Provider (ISP), connected to the Internet. It provides IP addresses on the local port with DHCP.
- **(G)** Represents the Internet.

## Multiple nodes on a building with a gateway

The diagram below demonstrates what this would look like with equipment installed on a building:



**Tip:** Mounting wireless routers very close to each other can cause interference. For best performance, we recommend mounting equipment on separate poles, with two or three meters (6 to 10 feet) between them AND using metal shields on the back of directional nodes. These reduce the wireless signal radiated from the back of the equipment, reducing the interference. You can buy these commercially, or make your own from metal building studs.

## Steps to configure:

First, ensure the Commotion nodes mesh with wireless neighbors. Run the Setup Wizard on the first boot, with the same **Mesh network name**, **Wireless channel**, and **Mesh encryption password**. The passwords must match across the network. You can also disable encryption across the network.

You should also configure the node to allow connections on the Ethernet port to the Administration interface. Follow the instructions for “Opening the firewall for remote Administration” in **Configure Commotion**.

### SET TO RECEIVE DHCP ON THE WAN PORT

Now, set the nodes to “gateway only” to prevent issues with the nodes booting before the modem. Browse to the Administration panel on the node. Navigate to the **Basic Configuration » Network Settings » Additional Network Interfaces** menu.

The screenshot displays the Commotion Administration interface. On the left, a sidebar contains navigation options: 'Status', 'Basic Configuration' (selected), 'Node Settings', 'Network Settings' (with sub-items 'Mesh Network', 'Wireless Network', and 'Additional Network Interfaces'), 'Applications', 'Client Controls', 'Security', 'Advanced', and 'Logout'. The main content area is titled 'Internet Gateway' and includes the following settings:

- Internet Gateway**: If desired, you can configure your gateway interface here.
- Will you be meshing with other Commotion devices over the ethernet interface?
- Gateway Configuration**: A dropdown menu currently set to 'Automatically configure gateway on boot.'
- Advertise your gateway to the mesh.

A 'Save' button with a checkmark icon is located at the bottom right of the configuration area.

1. In the “Gateway Configuration” pull-down menu, select “This device should ALWAYS try to acquire a DHCP lease”, and make sure “Advertise your gateway to the mesh” is checked.
2. **Save**, then **Save and apply** these settings.

## ENABLE MESHING OVER THE ETHERNET PORT

Next, enable meshing over Ethernet for the nodes connected to the switch. Navigate to the **Advanced » Services » OLSR** menu. At the bottom of the page, under the interfaces section, click on the “Add” button.

default 1.0

? Multiply routes with the factor given here. Allowed values are between 0.01 and 1. It is only used when LQ-Level is greater than 0. Examples:  
reduce LQ to 192.168.0.1 by half: 192.168.0.1 0.5  
reduce LQ to all nodes on this interface by 20%: default 0.8

### INTERFACES

Enable	Network	Mode	Hello	TC	MID	HNA	
<input checked="" type="checkbox"/>	R2R:	mesh	5.0s / 40.0s	2.0s / 256.0s	18.0s / 324.0s	18.0s / 108.0s	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

1. On the next page, click radio button for the “WAN” interface under “Network”.
2. In the “Mode” pull down menu, select “Ether”.

Plugins HNA Announcements Display

### OLSR Daemon - Interface

The OLSR daemon is an implementation of the Optimized Link State Routing protocol. As such it allows mesh routing for any network equipment. It runs on any wifi card that supports ad-hoc mode and of course on any ethernet device. Visit [olsrd.org](http://olsrd.org) for help and documentation.

### INTERFACE

General Settings IP Addresses Timing and Validity

Enable  
 ? Enable this interface.

Network

R2R:

lan: (no interfaces attached)

wan:

? The interface OLSRd should serve.

Mode

ether

? Interface Mode is used to prevent unnecessary packet forwarding on switched ethernet interfaces. valid Modes are "mesh" and "ether". Default is "mesh".

Scroll to the bottom of the page and “Save and Apply” these changes.

## CHANGE FIREWALL SETTINGS

Finally, adjust the Firewall so mesh traffic can pass through in both directions. Navigate to the **Advanced » Network » Firewall** menu. Scroll down to the bottom of the page, to the section that is titled “Zones”. It should look like this:

**ZONES**

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
mesh: R2R: → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: → DROP	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

Click the “Edit” button in the WAN row – it should open up the *Firewall – Zone Settings – Zone “wan”* page. Scroll down until you see the section that says “Inter-zone forwarding”. It should look like this:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

Allow forward from *source zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)



## 7 UNIT: INSTALLING AND CONFIGURING MODULE: ADVANCED HARDWARE SETUPS


Under “Allow forward to destination zones”, click the boxes next to “lan” and “mesh”. This will enable traffic to pass from WAN to LAN and MESH. The screen should now look like:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:


lan: lan: 

mesh: R2R: 

vpn: (empty)

Allow forward from *source zones*:

lan: lan: 

mesh: R2R: 




vpn: (empty)

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

Hit “Save & Apply”. Click on “General Settings” at the top of the page. You should be returned to the “Firewall – Zone Settings” page. Scroll down and look at the table of zones. It should look like this:

### ZONES

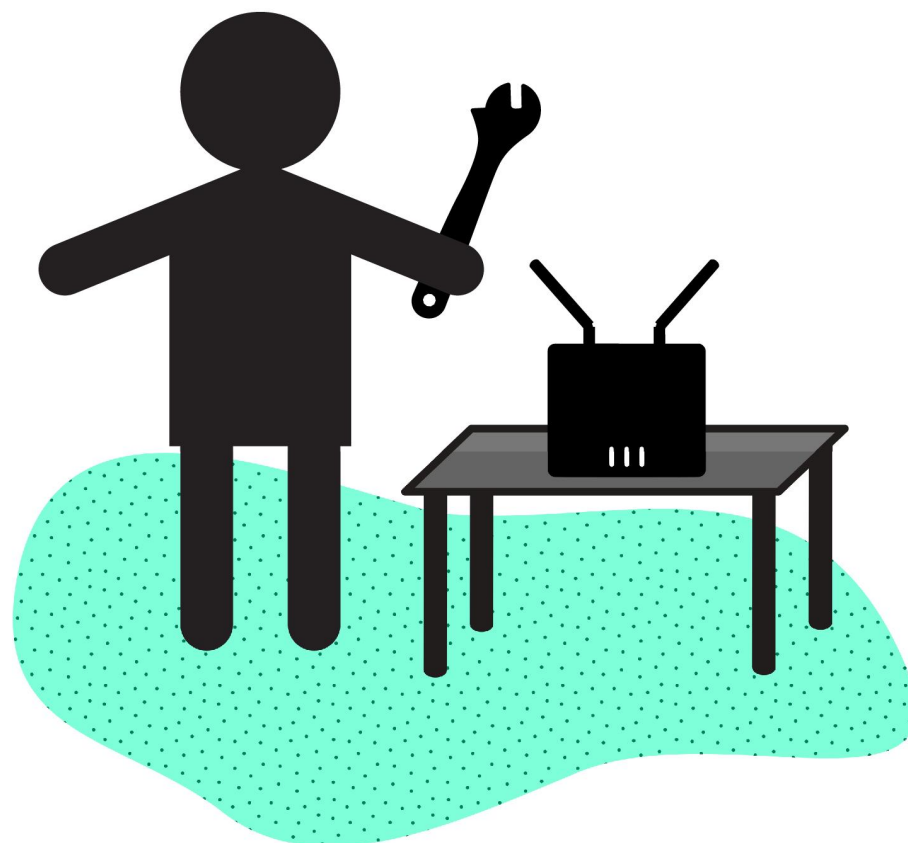
Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan:  → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
mesh: R2R:  → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
wan: wan:  → mesh lan	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

## REBOOT AND VERIFY

Reboot the router to verify the settings.

1. Browse to **Advanced » System » Reboot**.
2. Click “Perform reboot” and wait for the device to restart.

Do these steps for each Commotion node connected to the switch. When all the nodes have been configured, you can confirm that they are meshing over the wired Ethernet connections by connecting to one of the nodes and browsing to the **Basic Menu » Status**. Then click on “Nearby Mesh Devices” and look under the “OLSR Links” section. You should see entries for all of the nodes connected to the switch, and they should have IP addresses on the same subnet, as given out by the modem or router. These will look like 192.168.x.y, or 10.0.x.y, or something similar. That entry will have an ETX value of 0.100. If this is the case, the nodes are successfully meshing with Ethernet.

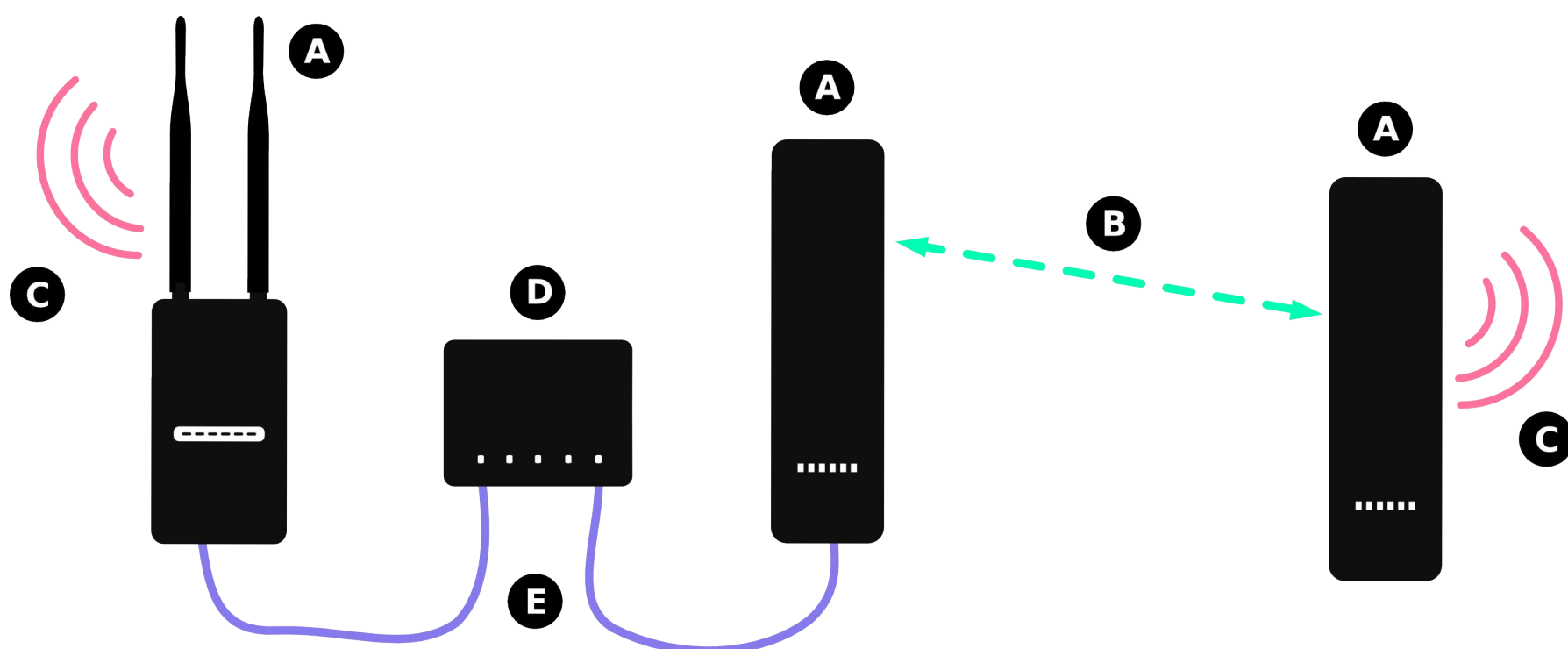




# Mesh with Ethernet + Static IPs

## Static IP addresses, without a Gateway to the Internet

Even if a tall or centrally located site doesn't have a gateway to the Internet, it may help to mount several wireless nodes there to act as a "supernode" on the network. This can increase throughput on the network and reduce bottlenecks for very busy nodes or nodes with many, many connections on the mesh.

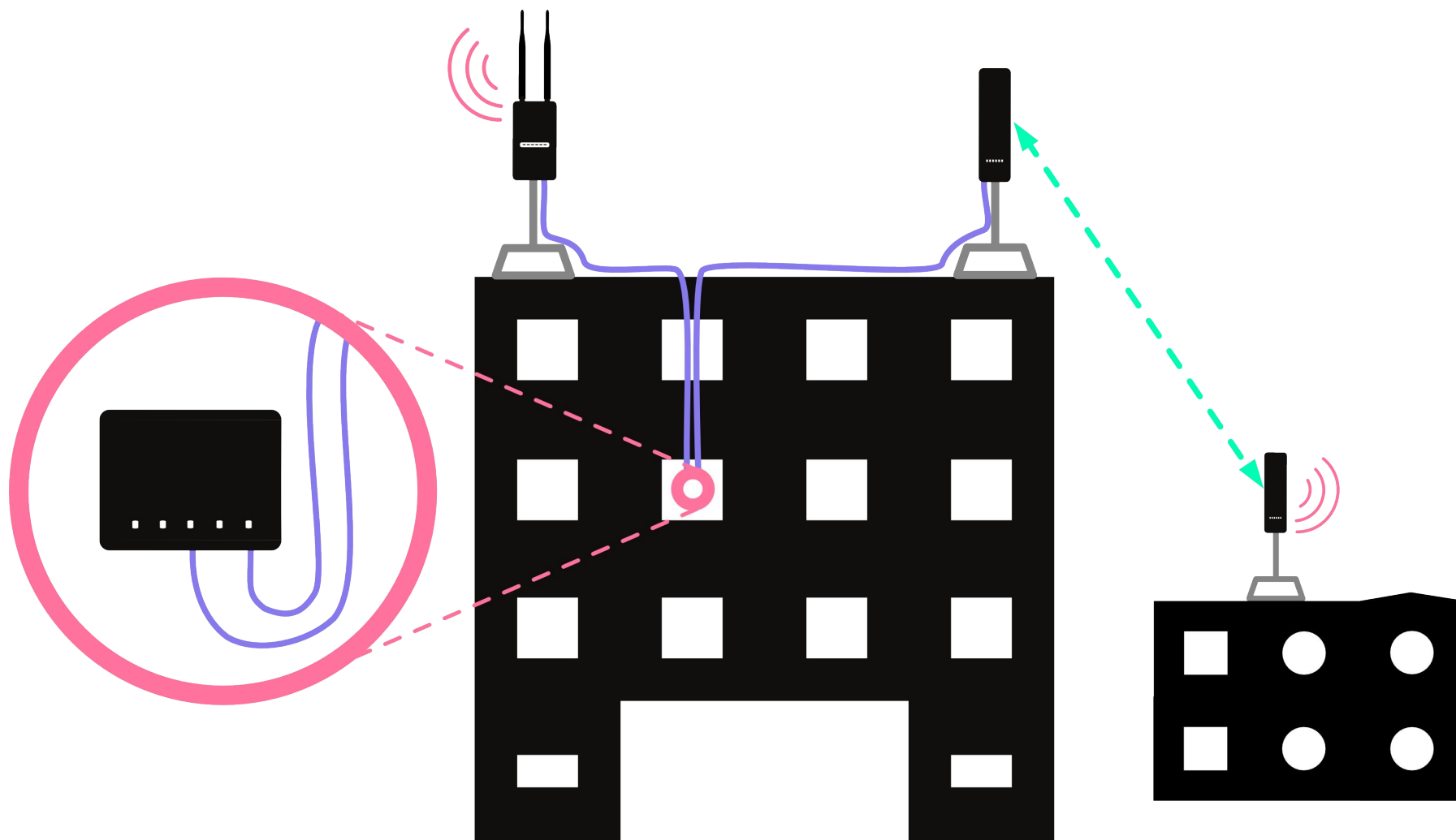


In the diagram above:

- (A) Represents a node running the Commotion software.
- (B) Represents the wireless mesh links between the nodes.
- (C) Represents the Access Point generated by the Commotion node for users to connect to.
- (D) Represents an Ethernet switch, which transfers data between all connected devices.
- (E) Represents Ethernet cabling connecting the modem and nodes to the Ethernet switch.

## Multiple nodes on a building

The diagram below demonstrates what this would look like with equipment installed on a building:



**Tip:** Mounting wireless routers very close to each other can cause interference. For best performance, we recommend mounting equipment on separate poles, with two or three meters (6 to 10 feet) between them AND using metal shields on the back of directional nodes. These reduce the wireless signal radiated from the back of the equipment, reducing the interference. You can buy these commercially, or make your own from metal building studs.

## Steps to configure:

First, ensure the Commotion nodes mesh with wireless neighbors. Run the Setup Wizard on the first boot, with the same **Mesh network name**, **Wireless channel**, and **Mesh encryption password**. The passwords must match across the network. You can also disable encryption across the network.

You should also configure the node to allow connections on the Ethernet port to the Administration interface. Follow the instructions for “Opening the firewall for remote Administration” in **Configure Commotion**.

### CHANGE THE WAN PORT TO USE STATIC ADDRESSING

Browse to the Administration panel on the node.

1. In the Basic Configuration menus, go to the **Network Settings » Additional Network Interfaces** menu
2. Select the box under “Will you be meshing with other Commotion devices over the Ethernet interface?”. The page will change and two fields will appear.
3. Put in a static IP address and Netmask for this router.

The screenshot displays the 'Internet Gateway' configuration page in the Commotion Administration interface. On the left, a sidebar menu shows 'Basic Configuration' selected, with 'Additional Network Interfaces' highlighted. The main content area features a form with the following elements:

- Internet Gateway** header with a sub-note: "If desired, you can configure your gateway interface here."
- A checkbox labeled "Will you be meshing with other Commotion devices over the ethernet interface?" which is checked.
- An "IP Address" input field containing "172.16.100.20".
- A "Netmask" input field containing "255.255.255.0".
- A "Save" button with a checkmark icon.

If you are adding the router to the same switch with others that are meshing over Ethernet, use an IP address in the same range. For example, if a node had the address 172.16.10.5, you could use 172.16.10.6.

If you are setting up mesh over Ethernet at a new site, use an IP address range that isn't in use somewhere else. For example, if the 172.16.10.x range is in use somewhere, don't use it again – this will cause problems on the network. You could use 172.16.11.x, 10.50.0.x, or something else. It is recommended not to use 192.168.x.x since many home and office routers use these ranges.

The Netmask will almost always be 255.255.255.0.

## ENABLE MESHING OVER THE ETHERNET PORT

Next, enable meshing over Ethernet for the nodes connected to the switch. Navigate to the **Advanced » Services » OLSR** menu. At the bottom of the page, under the interfaces section, click on the “Add” button.

default 1.0

? Multiply routes with the factor given here. Allowed values are between 0.01 and 1. It is only used when LQ-Level is greater than 0. Examples:  
reduce LQ to 192.168.0.1 by half: 192.168.0.1 0.5  
reduce LQ to all nodes on this interface by 20%: default 0.8

### INTERFACES

Enable	Network	Mode	Hello	TC	MID	HNA	
<input checked="" type="checkbox"/>	R2R:	mesh	5.0s / 40.0s	2.0s / 256.0s	18.0s / 324.0s	18.0s / 108.0s	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

1. On the next page, click radio button for the “WAN” interface under “Network”.
2. In the “Mode” pull down menu, select “Ether”.

Plugins HNA Announcements Display

### OLSR Daemon - Interface

The OLSR daemon is an implementation of the Optimized Link State Routing protocol. As such it allows mesh routing for any network equipment. It runs on any wifi card that supports ad-hoc mode and of course on any ethernet device. Visit [olsrd.org](http://olsrd.org) for help and documentation.

### INTERFACE

General Settings IP Addresses Timing and Validity

Enable  
 ? Enable this interface.

Network

R2R:

lan: (no interfaces attached)

wan:

? The interface OLSRd should serve.

Mode

ether

? Interface Mode is used to prevent unnecessary packet forwarding on switched ethernet interfaces. valid Modes are "mesh" and "ether". Default is "mesh".

Scroll to the bottom of the page and “Save and Apply” these changes.

## CHANGE FIREWALL SETTINGS

Finally, adjust the Firewall so mesh traffic can pass through in both directions. Navigate to the **Advanced » Network » Firewall** menu. Scroll down to the bottom of the page, to the section that is titled “Zones”. It should look like this:

**ZONES**

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
mesh: R2R: → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: → DROP	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

Click the “Edit” button in the WAN row – it should open up the *Firewall – Zone Settings – Zone “wan”* page. Scroll down until you see the section that says “Inter-zone forwarding”. It should look like this:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

Allow forward from *source zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

## 14 UNIT: INSTALLING AND CONFIGURING MODULE: ADVANCED HARDWARE SETUPS


Under “Allow forward to destination zones”, click the boxes next to “lan” and “mesh”. This will enable traffic to pass from WAN to LAN and MESH. The screen should now look like:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:


lan: lan: 

mesh: R2R: 

vpn: (empty)

Allow forward from *source zones*:

lan: lan: 

mesh: R2R: 




vpn: (empty)

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

Hit “Save & Apply”. Click on “General Settings” at the top of the page. You should be returned to the “Firewall – Zone Settings” page. Scroll down and look at the table of zones. It should look like this:

### ZONES

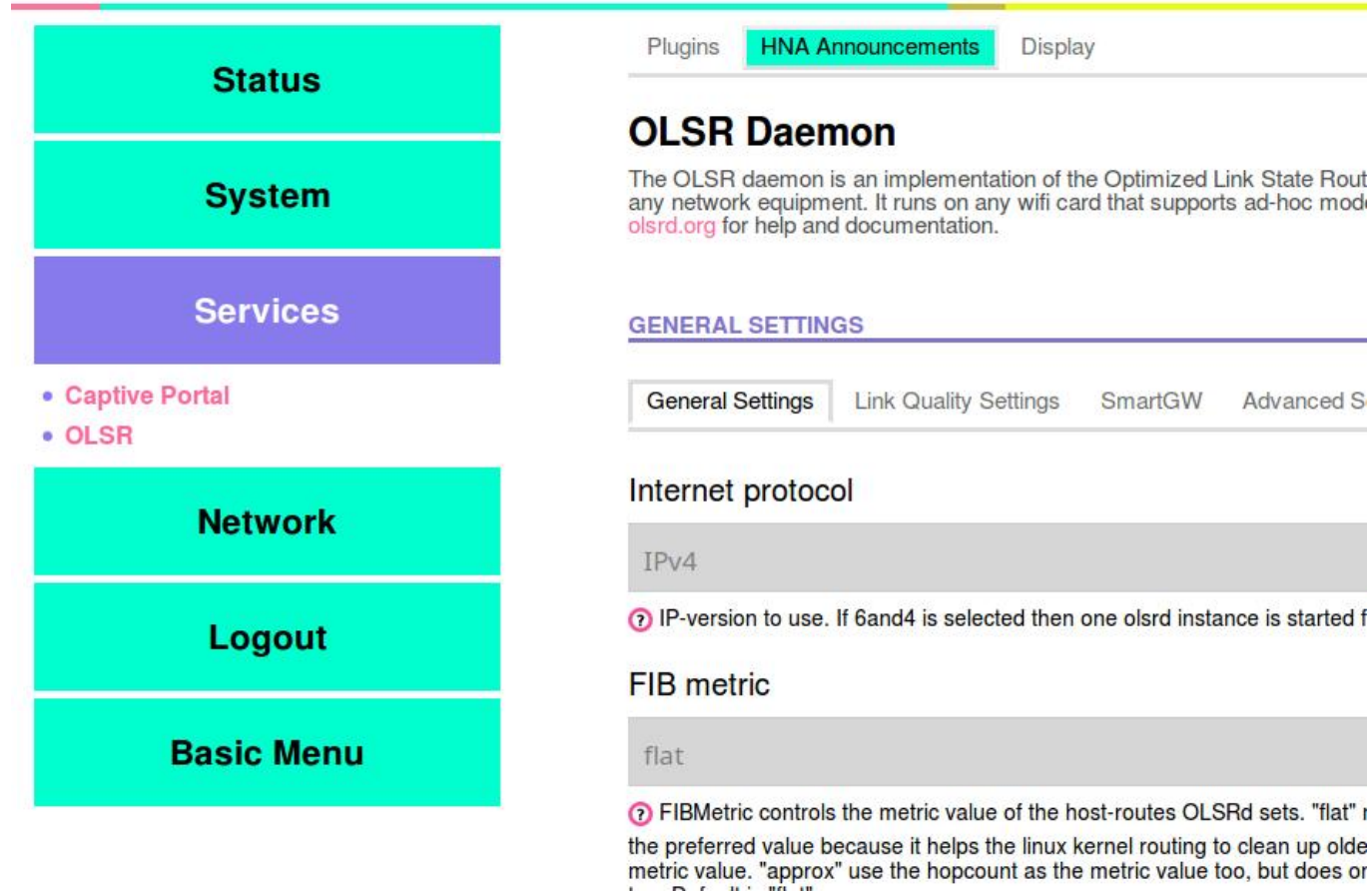
Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan:  → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
mesh: R2R:  → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
wan: wan:  → mesh lan	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>



## ADD A HNA TO THE STATIC IP RANGE

Add a Host Network Announcement (HNA) for the Static IP address range for the nodes. This setting lets the rest of the mesh network know where to find anything attached to the switch that might have those Static IPs.

Go to **Advanced » Services » OLSR**, and click on “HNA Announcements” at the top of the page.



The screenshot shows a web interface for configuring the OLSR Daemon. On the left is a navigation menu with buttons for Status, System, Services, Network, Logout, and Basic Menu. The 'Services' section is expanded to show 'Captive Portal' and 'OLSR'. The main content area is titled 'HNA Announcements' and includes a description of the OLSR daemon, a 'GENERAL SETTINGS' section with tabs for General Settings, Link Quality Settings, SmartGW, and Advanced S, and configuration fields for 'Internet protocol' (set to IPv4) and 'FIB metric' (set to flat). Each field has a help icon and a brief description.

Plugins **HNA Announcements** Display

### OLSR Daemon

The OLSR daemon is an implementation of the Optimized Link State Routing protocol for any network equipment. It runs on any wifi card that supports ad-hoc mode. See [olsrd.org](http://olsrd.org) for help and documentation.

#### GENERAL SETTINGS

General Settings | Link Quality Settings | SmartGW | Advanced S

Internet protocol

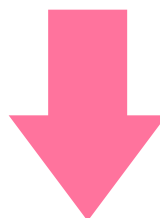
IPv4

? IP-version to use. If 6and4 is selected then one olsrd instance is started for each IPv6 address.

FIB metric

flat

? FIBMetric controls the metric value of the host-routes OLSRd sets. "flat" is the preferred value because it helps the linux kernel routing to clean up older metric value. "approx" use the hopcount as the metric value too, but does not



## 16 UNIT: INSTALLING AND CONFIGURING MODULE: ADVANCED HARDWARE SETUPS

Click the “Add” button to create a new line, and put the following settings into the boxes:

- Network address: your static IP range, ending with a zero
- Netmask: 255.255.255.0

Plugins HNA Announcements Display

---

### OLSR - HNA-Announcements

Hosts in a OLSR routed network can announce connectivity to external networks using HNA messages.

#### HNA4

Both values must use the dotted decimal notation.

Network address	Netmask	
<input type="text" value="10.14.42.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Delete"/>
<input type="text" value="172.16.100.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Delete"/>

At the bottom of the page, hit “Save & Apply”.

### REBOOT AND VERIFY

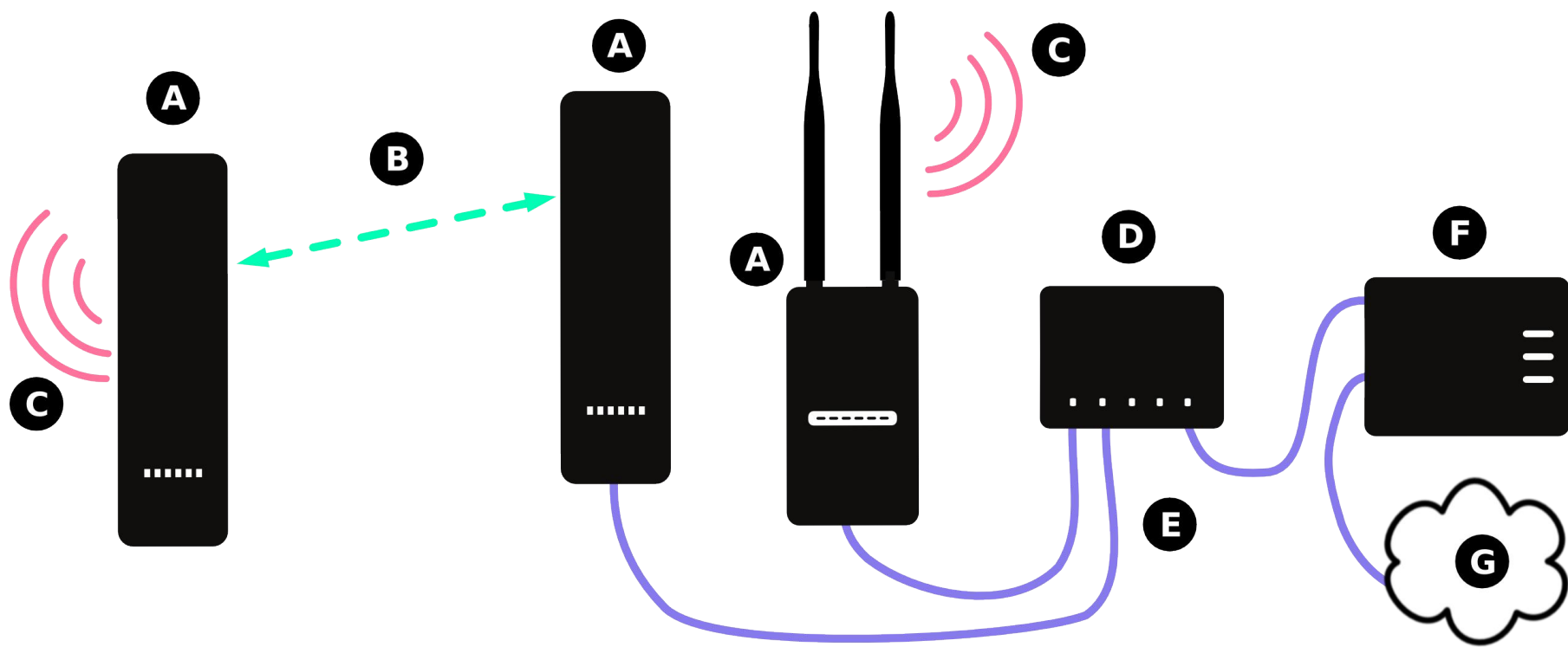
Reboot the router to verify the settings.

1. Browse to **Advanced » System » Reboot**.
2. Click “Perform reboot” and wait for the device to restart.

Do these steps for each Commotion node connected to the switch. When all the nodes have been configured, you can confirm that they are meshing over the wired Ethernet connections by connecting to one of the nodes and browsing to the **Basic Menu » Status**. Then click on “Nearby Mesh Devices” and look under the “OLSR Links” section. You should see entries for all of the nodes connected to the switch, and they should have IP addresses on the same subnet, as given out by the modem or router. These will look like 192.168.x.y, or 10.0.x.y, or something similar. That entry will have an ETX value of 0.100. If this is the case, the nodes are successfully meshing with Ethernet.

# Mesh with Ethernet + a Static Gateway

This example is similar to the other example with a gateway above, but the gateway to the Internet does not provide IP addresses automatically using DHCP. You must configure the addresses for the Commotion nodes manually. In this example the gateway IP address is 192.168.50.1, but you will need to obtain the proper IP address information from your Internet service provider.

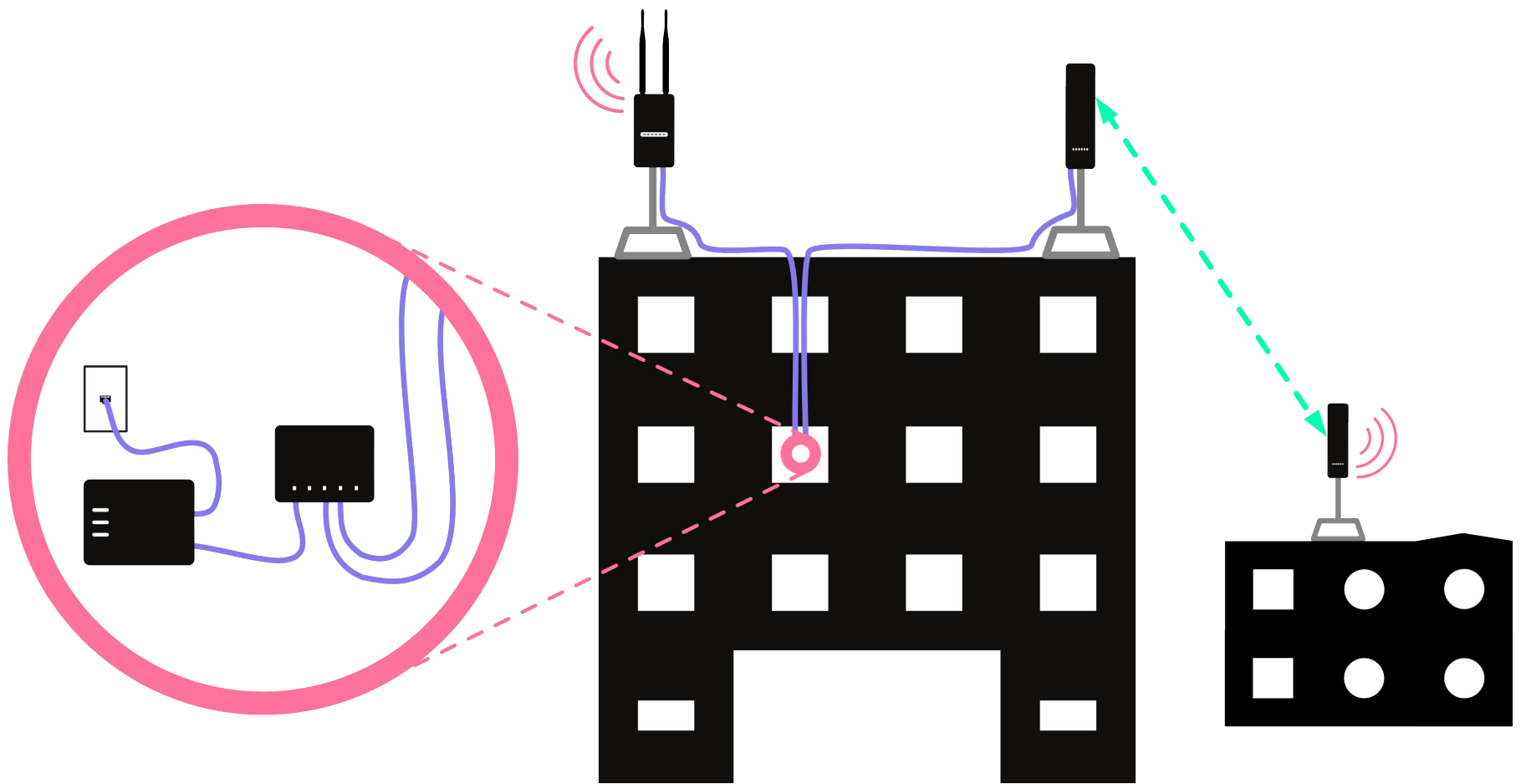


In the diagram above:

- **(A)** Represents a node running the Commotion software.
- **(B)** Represents the wireless mesh links between the nodes.
- **(C)** Represents the Access Point generated by the Commotion node for users to connect to.
- **(D)** Represents an Ethernet switch, which transfers data between all connected devices.
- **(E)** Represents Ethernet cabling connecting the modem and nodes to the Ethernet switch.
- **(F)** Represents the modem or router from the Internet Service Provider (ISP), connected to the Internet. It is configured with a Static IP address, and does not provide IP addresses to clients automatically via DHCP.
- **(G)** Represents the Internet.

## Multiple nodes on a building, with a gateway

The diagram below demonstrates what this would look like with equipment installed on a building:



**Tip:** Mounting wireless routers very close to each other can cause interference. For best performance, we recommend mounting equipment on separate poles, with two or three meters (6 to 10 feet) between them AND using metal shields on the back of directional nodes. These reduce the wireless signal radiated from the back of the equipment, reducing the interference. You can buy these commercially, or make your own from metal building studs.

## Steps to configure:

First, ensure the Commotion nodes mesh with wireless neighbors. Run the Setup Wizard on the first boot, with the same **Mesh network name**, **Wireless channel**, and **Mesh encryption password**. The passwords must match across the network. You can also disable encryption across the network.

You should also configure the node to allow connections on the Ethernet port to the Administration interface. Follow the instructions for “Opening the firewall for remote Administration” in **Configure Commotion**.

### CHANGE THE WAN PORT TO USE STATIC ADDRESSING

Browse to the Administration panel on the node.

1. In the Basic Configuration menus, go to the **Network Settings » Additional Network Interfaces** menu
2. Select the box under “Will you be meshing with other Commotion devices over the Ethernet interface?”. The page will change and two fields will appear.
3. Put in a static IP address and Netmask for this router.

The screenshot shows the Commotion Administration interface. On the left, a sidebar contains menu items: Status, Basic Configuration (selected), Applications, Client Controls, Security, Advanced, and Logout. Under 'Basic Configuration', there are sub-menus for Node Settings and Network Settings, with 'Additional Network Interfaces' highlighted. The main content area is titled 'Internet Gateway' and includes the text: 'If desired, you can configure your gateway interface here.' Below this is a checkbox labeled 'Will you be meshing with other Commotion devices over the ethernet interface?' which is checked. Two input fields are present: 'IP Address' containing '172.16.100.20' and 'Netmask' containing '255.255.255.0'. At the bottom center, there is a circular 'Save' button with a checkmark icon.

The static IP that you choose should be in the same range as the IP address of the router that has the connection to the Internet. For example, if the gateway’s IP is 10.50.0.1, you would choose a static IP for the node in the 10.50.0.x range, where “x” is a number that isn’t in use by any other nodes, servers, or devices.

The Netmask will almost always be 255.255.255.0.

## SET A STATIC GATEWAY

Configure the node with a static route to the Internet. Browse to the Administration panel on the first node. Go to the **Advanced » Network » Static Routes** menu.

**Status**

**System**

**Services**

**Network**

- Interfaces
- Wifi
- DHCP and DNS
- Hostnames
- Static Routes
- Firewall
- Diagnostics
- QoS

**Logout**

**Basic Menu**

### Routes

Routes specify over which interface and gateway a certain host or network can be reached.

#### STATIC IPV4 ROUTES

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	If target is a network			

This section contains no values yet

Add

#### STATIC IPV6 ROUTES

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

Add

Save & Apply Save Reset

1. Click “Add” in the “Static IPv4 Routes” section.
2. In the entry that comes up, select “WAN” in the first pull-down menu.
3. In the “Target” field, enter 0.0.0.0
4. In the “IPv4-Netmask” field, enter 0.0.0.0
5. In the “IPv4-Gateway” field, enter the IP address for the gateway modem or router.
6. Save and apply these settings.

### Routes

Routes specify over which interface and gateway a certain host or network can be reached.

#### STATIC IPV4 ROUTES

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
	Host-IP or Network	If target is a network		
wan	0.0.0.0	0.0.0.0	10.75.100.1	0

Add



## ENABLE MESHING OVER THE ETHERNET PORT

Next, enable meshing over Ethernet for the nodes connected to the switch. Navigate to the **Advanced » Services » OLSR** menu. At the bottom of the page, under the interfaces section, click on the “Add” button.

default 1.0

? Multiply routes with the factor given here. Allowed values are between 0.01 and 1. It is only used when LQ-Level is greater than 0. Examples:  
reduce LQ to 192.168.0.1 by half: 192.168.0.1 0.5  
reduce LQ to all nodes on this interface by 20%: default 0.8

### INTERFACES

Enable	Network	Mode	Hello	TC	MID	HNA	
<input checked="" type="checkbox"/>	R2R:	mesh	5.0s / 40.0s	2.0s / 256.0s	18.0s / 324.0s	18.0s / 108.0s	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

1. On the next page, click radio button for the “WAN” interface under “Network”.
2. In the “Mode” pull down menu, select “Ether”.

Plugins HNA Announcements Display

### OLSR Daemon - Interface

The OLSR daemon is an implementation of the Optimized Link State Routing protocol. As such it allows mesh routing for any network equipment. It runs on any wifi card that supports ad-hoc mode and of course on any ethernet device. Visit [olsrd.org](http://olsrd.org) for help and documentation.

### INTERFACE

General Settings IP Addresses Timing and Validity

Enable  
 ? Enable this interface.

Network

R2R:

lan: (no interfaces attached)

wan:

? The interface OLSRd should serve.

Mode

ether

? Interface Mode is used to prevent unnecessary packet forwarding on switched ethernet interfaces. valid Modes are "mesh" and "ether". Default is "mesh".

Scroll to the bottom of the page and “Save and Apply” these changes.

## CHANGE FIREWALL SETTINGS

Finally, adjust the Firewall so mesh traffic can pass through in both directions. Navigate to the **Advanced » Network » Firewall** menu. Scroll down to the bottom of the page, to the section that is titled “Zones”. It should look like this:

**ZONES**

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
mesh: R2R: → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: → DROP	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

Click the “Edit” button in the WAN row – it should open up the *Firewall – Zone Settings – Zone “wan”* page. Scroll down until you see the section that says “Inter-zone forwarding”. It should look like this:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

Allow forward from *source zones*:

- lan: lan:
- mesh: R2R:
- vpn: (empty)

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

## 23 UNIT: INSTALLING AND CONFIGURING MODULE: ADVANCED HARDWARE SETUPS

Under “Allow forward to destination zones”, click the boxes next to “lan” and “mesh”. This will enable traffic to pass from WAN to LAN and MESH. The screen should now look like:

### INTER-ZONE FORWARDING

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from “wan”**. *Source zones* match forwarded traffic from other zones **targeted at “wan”**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:


lan: lan: 

mesh: R2R: 

vpn: (empty)

Allow forward from *source zones*:

lan: lan: 

mesh: R2R: 




vpn: (empty)

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

Hit “Save & Apply”. Click on “General Settings” at the top of the page. You should be returned to the “Firewall – Zone Settings” page. Scroll down and look at the table of zones. It should look like this:

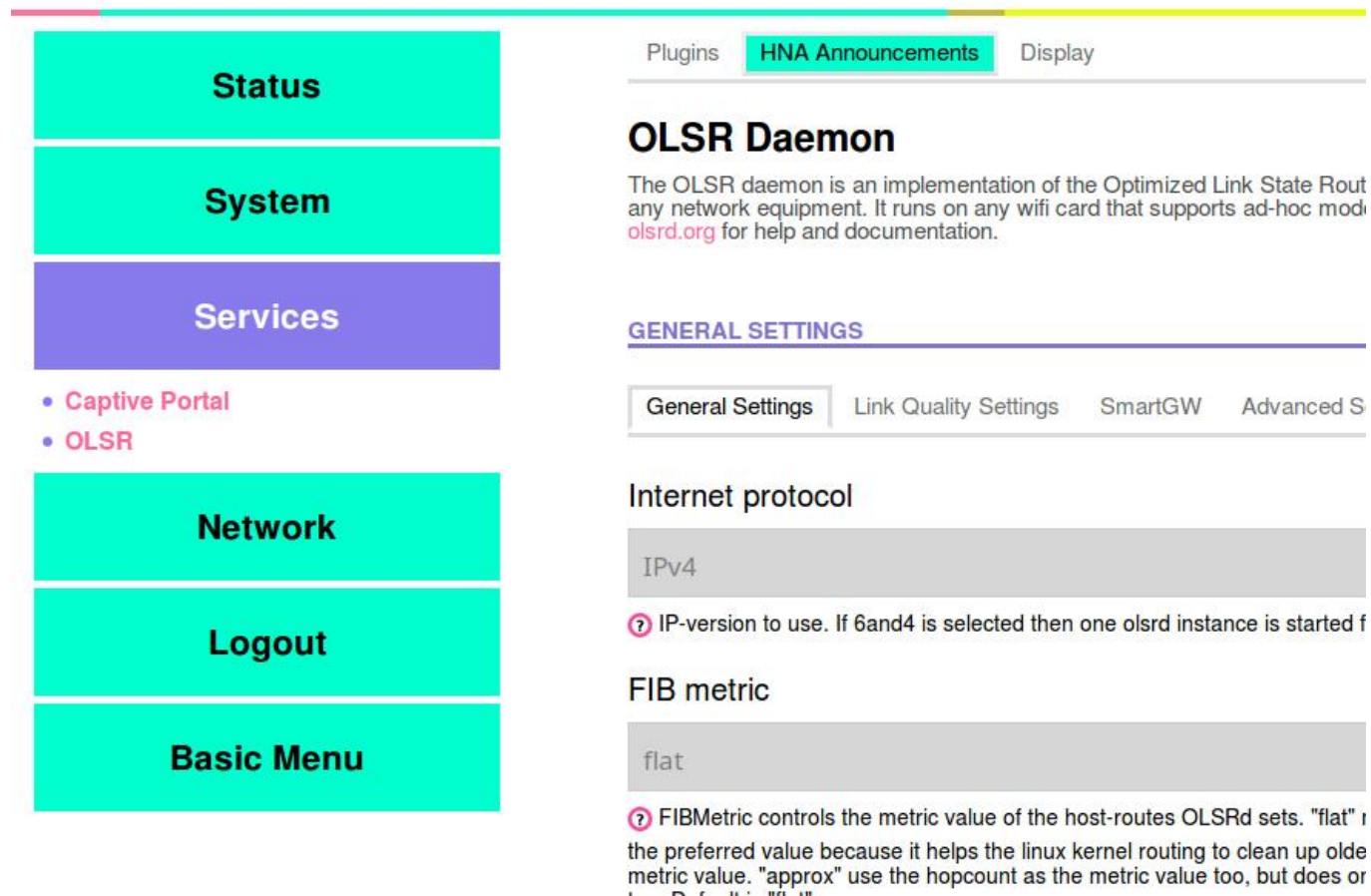
### ZONES

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan:  → lan mesh wan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
mesh: R2R:  → mesh wan lan	accept	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
wan: wan:  → mesh lan	drop	accept	drop	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
vpn: (empty) → DROP	drop	accept	drop	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

## ADD A HNA TO THE STATIC IP RANGE

Add a Host Network Announcement (HNA) for the Static IP address range for the nodes. This setting lets the rest of the mesh network know where to find anything attached to the switch that might have those Static IPs.

Go to **Advanced » Services » OLSR**, and click on “HNA Announcements” at the top of the page.



The screenshot shows a web interface for configuring the OLSR daemon. On the left is a navigation menu with buttons for Status, System, Services, Network, Logout, and Basic Menu. Under the Services menu, 'Captive Portal' and 'OLSR' are listed. The main content area has tabs for Plugins, HNA Announcements, and Display. The 'HNA Announcements' tab is active, showing the 'OLSR Daemon' section with a description and a link to 'olsrd.org'. Below this is the 'GENERAL SETTINGS' section with sub-tabs for General Settings, Link Quality Settings, SmartGW, and Advanced S. The 'General Settings' sub-tab is active, showing 'Internet protocol' set to 'IPv4' and 'FIB metric' set to 'flat'. Both settings have help icons and descriptive text.

Plugins **HNA Announcements** Display

### OLSR Daemon

The OLSR daemon is an implementation of the Optimized Link State Routing protocol for any network equipment. It runs on any wifi card that supports ad-hoc mode. See [olsrd.org](http://olsrd.org) for help and documentation.

#### GENERAL SETTINGS

General Settings | Link Quality Settings | SmartGW | Advanced S

Internet protocol

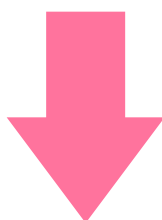
IPv4

? IP-version to use. If 6and4 is selected then one olsrd instance is started for each IPv6 address.

FIB metric

flat

? FIBMetric controls the metric value of the host-routes OLSRd sets. "flat" is the preferred value because it helps the linux kernel routing to clean up older metric values. "approx" use the hopcount as the metric value too, but does not



## 25 UNIT: INSTALLING AND CONFIGURING MODULE: ADVANCED HARDWARE SETUPS

Click the “Add” button to create a new line, and put the following settings into the boxes:

- Network address: *your static IP range, ending with a zero*
- Netmask: 255.255.255.0

Plugins HNA Announcements Display

---

### OLSR - HNA-Announcements

Hosts in a OLSR routed network can announce connectivity to external networks using HNA messages.

#### HNA4

Both values must use the dotted decimal notation.

Network address	Netmask	
<input type="text" value="10.14.42.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Delete"/>
<input type="text" value="172.16.100.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Delete"/>

At the bottom of the page, hit “Save & Apply”.

### REBOOT AND VERIFY

Reboot the router to verify the settings.

1. Browse to **Advanced » System » Reboot**.
2. Click “Perform reboot” and wait for the device to restart.

Do these steps for each Commotion node connected to the switch. When all the nodes have been configured, you can confirm that they are meshing over the wired Ethernet connections by connecting to one of the nodes and browsing to the **Basic Menu » Status**. Then click on “Nearby Mesh Devices” and look under the “OLSR Links” section. You should see entries for all of the nodes connected to the switch, and they should have IP addresses on the same subnet, as given out by the modem or router. These will look like 192.168.x.y, or 10.0.x.y, or something similar. That entry will have an ETX value of 0.100. If this is the case, the nodes are successfully meshing with Ethernet.

# Definitions

## **AP (Access Point)**

A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards

## **DHCP: Dynamic Host Configuration Protocol**

It assigns IP addresses to client devices, such as desktop computers, laptops, and phones, when they are plugged into Ethernet or connect to Wireless networks.

## **Ethernet**

A type of networking protocol - it defines the types of cables and connections that are used to wire computers, switches, and routers together. Most

often Ethernet cabling is Category 5 or 6, made up of twisted pair wiring similar to phone cables.

## **Router**

A device that determines how messages move through a computer network.

## **Node**

An individual device in a mesh network.

## **WAN: Wide Area Network**

Signifies the connection to the global Internet or a different, typically larger, network.