Managing Multiple Networks with Configuration Templates

Configuration templates can allow many Cisco Meraki devices to be deployed following a single base configuration. This makes it much easier to roll out new sites/users and maintain consistency across each site’s configuration. It is most useful in cases where a large number of sites exist that share a common network design. Such as a retail deployment with many stores, or a large number of home users with Z1s connecting to a corporate network over VPN. Sites as part of a template can have exceptions to the configuration, and devices that need to be treated differently can be bound to a template. However, it’s important to note that not all settings can be changed on a site bound to a template.

Note that configuration templates cannot be used on networks with Systems Manager or MV Cameras.

Creating a Configuration Template

To begin, a configuration template must be created. This template will then be used as the base for all of the networks that are bound to it.

To create the configuration template:

1. Navigate to Organization > Configuration templates.
2. Click **Create a new template**.

 Configuration templates

 ![Image of configuration templates](Image)

3. To create a template based on an existing template or network, choose **Copy settings from** and select the appropriate network or template.
Or to create a blank template, choose Create new and name the template.

4. Provide a Template name.
5. Click Add.
6. Select any Target networks that should be bound to use this template, then click Bind. 
   *If no networks should use this template yet, skip this step by clicking Close.*
7. Click **Save Changes**.

### Modifying a Template

Once a network has been created, any changes desired for all of the bound networks must be made to the template. To edit the template's configuration, select it from the **Network** dropdown under "Select a template", and make any desired changes. The tabs on the left-hand side of the page can be used to navigate configuration options as normal. Some settings may exist which aren't relevant for all devices in bound networks, such as Wireless settings on a bound MX100, or extra port configurations. Extraneous settings will be ignored on devices not able to use them.

### MR - Wireless Network Templates

MR access points can be managed and deployed in bulk using network templates. It may be helpful to group into common deployment types, such as retail locations or branch offices, so APs deployed at different locations all use the same SSIDs and authentication methods. This way, a user at one location can seamlessly join wireless networks at another location without needing to provide a different PSK or credentials.

### MX - Template VLAN IP Address Range Allocations

While **Configure > Addressing & VLANs > VLANs** is set to "Disabled", all bound security appliances will use the same subnet. This allows for a high level of consistency across all sites, but it inherently disallows the use of Site-to-site VPN, as each site would result in a duplicate route. This means that VLANs must have unique subnets to allow for Auto VPN, as VPN subnet translation is not enabled by default.

Note that, in order to avoid subnet overlap issues, Auto VPN is disabled for cloned networks when using templates.
To allow for the use of Site-to-site VPN, set the **VLANs** field to Enabled. This will then provide several new configuration options specific to templates:

- **Subnetting**: Determines how addressing for the VLAN will be handled on each bound network.
- **Same**: All networks will use the same **Subnet** and **Appliance LAN IP** for this VLAN. Not eligible for site-to-site VPN.
- **Unique**: Each network will get a uniquely assigned **Subnet** and **Appliance LAN IP** based on the **Subnet** options.
- **Subnet**: The network addressing for this VLAN, based on the **Subnetting** selection.
- **Same**: The subnet in CIDR notation to be used for all networks bound to this template.
- **Unique**: Select a subnet mask in CIDR notation, and the private address range for it to come from.

When selecting a subnet allocation, it’s important to keep in mind how many unique networks can be created with that selection. More networks cannot be bound to a template than can be supported by the number of unique allocations available. To calculate the number of unique subnets, take the number after the "/" in the second box and subtract it from the number after the "/" in the first box. Then use the result as a power of 2.

**Ex.** /24 from 192.168.0.0/16 would allow for 256 unique subnets.

**Ex.** /23 from 10.0.0.0/8 would allow for 32,768 unique subnets.

If a network is unbound from a template, its subnet is made available for use by other future networks.

For more information on IP addressing and subnet masks, refer to the following articles on IP addressing and subnetting and subnetting fundamentals.

**Note**: When selecting Unique subnets, ensure that the address space being provided for use by the template is not currently in use by other networks. Otherwise, networks utilizing the template may overlap with other individually configured networks.

**MX - Firewall Rules and DHCP Reservations for Templates**

You have additional source and destination options when configuring layer 3 firewall rules for a configuration template. Because the subnet for a given VLAN may be different in each template child network, VLAN objects allow you to create firewall rules using the VLAN names as source and destination network objects, rather than actual IPs or CIDR subnets. These VLAN objects are automatically translated by each child network into the local subnet associated with that VLAN.

If you wish to use only a certain IP within a VLAN in a firewall rule, you can add a host bit. For instance, let us imagine that you have a firewall rule containing the source Data.50 representing the Data VLAN, host bit 50. If a child network has subnet 192.168.100.0/24 for the Data VLAN, this source will be interpreted in this network as 192.168.100.50.

Mousing over the VLAN dropdown when entering a Source or Destination will display a hover list of available VLANs and their addressing.
DHCP reservations can be configured in much the same way. The VLAN name for each DHCP scope will be autopopulated, and only the host bits of the reserved range needs to be set.

**MS - Switch Templates and Profiles**

MS Switch templates consist of two components: Template networks and switch profiles. Whereas a template network is a standard template as defined above, a switch profile is a port configuration that can be shared by multiple switches of the same model.

For more information about MS templates and profiles, please refer to our [Switch Templates Deployment Guide](#).

**Binding Networks to a Template**

Once a template has been created, networks that are bound to it will utilize its configuration as a base. Any changes made to the template will then be pushed out to all bound networks.

To bind an existing network to a template:

1. Navigate to Organization > Configuration templates.
2. Click on the row for the template (but not on the name of the template).
3. Click Bind additional networks.
4. In Target networks, select any additional networks that should be bound to this template.
5. Click Bind.
6. Click Save Changes.

*Note: When binding an existing network to a template, its current configuration will be lost and it will begin using the template configuration.*

To bind a new network to a template:

1. Select Create a network from the network dropdown.
2. Enter a Name, and select the appropriate Network type.
3. For Configuration, select Bind to template and the name of the template created earlier.
4. Click **Create network**.

Once bound to a template, individual networks will lose most of their **Configure** menu, and any changes impacting the network's configuration should be made from the template.

### Creating Multiple Template-Bound Networks

Once a template has been created, the [bulk network tool](#) can be used to create multiple networks, bound to the same template (or based on an existing network configuration).

### Moving Networks Between Templates

Once a network has been bound to a template, it can be moved to another template.

To move a network to another template:

1. Navigate to **Organization > Monitor > Configuration Templates**
2. Select the template where the network is currently bound
3. Select the network you wish to move
4. Click **Rebind**
5. Select the new template and then click **Rebind**
Unbinding Networks from a Template

If a network needs to stop following the shared configuration, so that it can be configured independently, it must be unbound from the template.

**Note:** When a network is unbound from a template, all devices within the network will revert to the configuration last used prior to any template binding, regardless of current network.

To unbind a network from a template:

1. Navigate to **Organization > Configuration templates**.
2. Click on the row for the template (but not on the name of the template).
3. Check the box next to the network(s) that must be unbound.
4. Click **Unbind**.
5. Click **Save Changes**.

**Note:** When a network is unbound from a template, it will retain some settings (such as addressing and VLANs) but most settings will revert to their state before binding, if there were any.

Local Overrides

Once a network has been bound to a template, some options can still be configured normally. Any local configuration changes made directly on the network will
override the template configuration.

**Note:** Updating the same options on the template will not clear a network’s local overrides. To clear local overrides, the network needs to be unbound and rebound to the template. The only exception is non-combined MR template, which can be reverted via the Organization > Monitor > Configuration templates page.

Below are overrides that can be configured for networks bounded to a template. Please refer to the product specific guides for more details:

**MX/Z - MX Templates Best Practices**

- Addressing & VLANs subnets
- DHCP exceptions
- Forwarding rules
- SD-WAN & traffic shaping uplink configuration

**MS - Templates for Switching Best Practices**

- Switch ports
- Routing and DHCP
- OSPF Routing
- Port management

**MR Access Points**

- Access control
- Radio Settings

---

**Deleting a Configuration Template**

If a template must be deleted, it can be done so using the instructions below. When a template is deleted, all networks bound to it will be automatically unbound.

1. Navigate to **Organization > Configuration templates**.
2. Check the box next to any templates that should be deleted.

3. Click Delete.

4. Read the important information on the next page, and confirm deletion. Once a template has been deleted, it cannot be recovered.

5. Click **Delete networks**.

---

**MX Port Numbers/Mappings**

Port numbering can differ between MX models, which can cause confusion when assigning a configuration to a specific port number in a template. For example, a configuration on LAN 2 in a template doesn't affect any ports on an MX65.

This table outlines template port numbers and their corresponding physical port on some MX models *(red fields indicate ports used for secondary WAN connections)*:

<table>
<thead>
<tr>
<th>Model</th>
<th>Z1</th>
<th>Z3</th>
<th>MX60/W</th>
<th>MX64/W</th>
<th>MX67/C/W</th>
<th>MX68/W/CW</th>
<th>MX80</th>
<th>MX84</th>
<th>MX90</th>
<th>MX100</th>
<th>MX400</th>
</tr>
</thead>
<tbody>
<tr>
<td>#WAN_Ports</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>#LAN_Ports</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>2(+)</td>
</tr>
</tbody>
</table>
# Fiber Ports

## Physical Ports

<table>
<thead>
<tr>
<th>WAN2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
<th>Inet 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN 2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>LAN 3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>LAN 4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>LAN 5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>LAN 6</td>
<td>5(PoE)</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>LAN 7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>LAN 8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>LAN 9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>LAN 10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>8(SFP)</td>
<td>8(SFP)</td>
<td>8(SFP)</td>
<td>8(SFP)</td>
<td>8(SFP)</td>
<td>8(SFP)</td>
</tr>
<tr>
<td>LAN 11</td>
<td>11(PoE+)</td>
<td>11(PoE+)</td>
<td>11(SFP)</td>
<td>9(SFP)</td>
<td>11(SFP)</td>
<td>11(SFP)</td>
<td>11(SFP)</td>
<td>11(SFP)</td>
<td>11(SFP)</td>
</tr>
<tr>
<td>LAN 12</td>
<td>12(PoE+)</td>
<td>12(PoE+)</td>
<td>12(SFP)</td>
<td>12(PoE+)</td>
<td>12(SFP)</td>
<td>12(SFP)</td>
<td>12(SFP)</td>
<td>12(SFP)</td>
<td>12(SFP)</td>
</tr>
</tbody>
</table>

* (+) : Model is capable of being modified to include additional LAN ports by installing interface modules.

## Modifying/Setting Secondary WAN Ports

You can toggle the LAN2 port between **LAN** and **Internet**, through **Uplink configuration** under the **Local status** tab on the Local Status Page.