Configuring MAC Access Control Lists (ACLs)

This document describes how to set up MAC ACLs. In this example we will use MAC ACLs to restrict access to ports on a switch based on the MAC address of connected clients (i.e. the source MAC address of a packet received at a port on the switch).

Specifically, our example will demonstrate how to restrict access to a set of VoIP telephones and a single management PC. Other devices will not be allowed access ensuring that bandwidth is preserved for the VoIP phones.

This example uses a Netgear ProSafe FSM7328PS layer 3 managed switch.

1. Configuration

- Go to Security -> ACL -> MAC ACL
- Enter a name for the ACL, in our example ‘AllowVoIPTelephones’
- Press Add

- AllowVoIPTelephones appears in the MAC ACL Table
Configuring MAC ACLs

- Go to MAC Rules
- Enter the first rule with an ID of 1
- Set the Action to Permit
- Under Source MAC enter the MAC address of one of the ‘trusted’ devices
- Press Add

- Rule ID 1 appears in the Rule Table list
- Next, add rule ID 2 which will permit the MAC address of the next ‘trusted’ device
- Repeat this process for the rest of the MAC addresses

- This shows the Rule Table with all required MAC addresses added (VoIP phones are IDs 1 through 15 and the management PC is ID 16)

- Next, we will add the ACL we created to the required ports on the switch
- Go to MAC Binding Configuration
- Choose the ACL ‘AllowVoIPTelephones’ from the ACL ID list
- Click on ‘Unit 1’ to show the ports of the switch
2. Testing

To test, connect one of the devices from the ‘trusted’ list to one of the ports which has the ACL applied. This device will be allowed access to the network.

Connecting a ‘non-trusted’ device to the same port will result in this device being denied access.

To verify this operation further, connect the ‘non-trusted’ device to port 1 (which does not have the ACL applied to it) and confirm that it is then allowed access to the network.