NETGEAR®
Connect with Innovation™

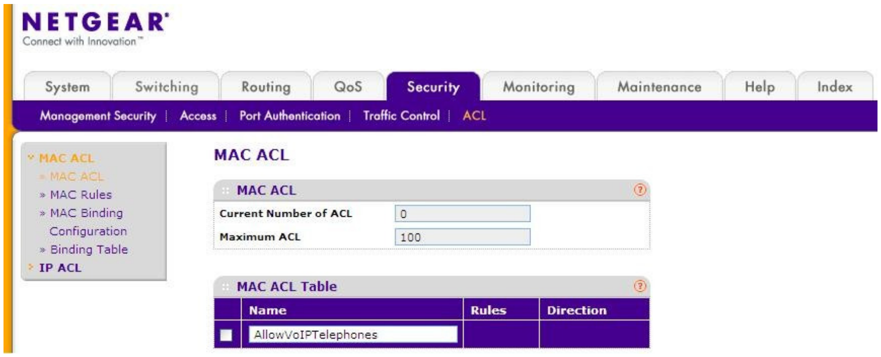
Configuring MAC Access Control Lists (ACLs)

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



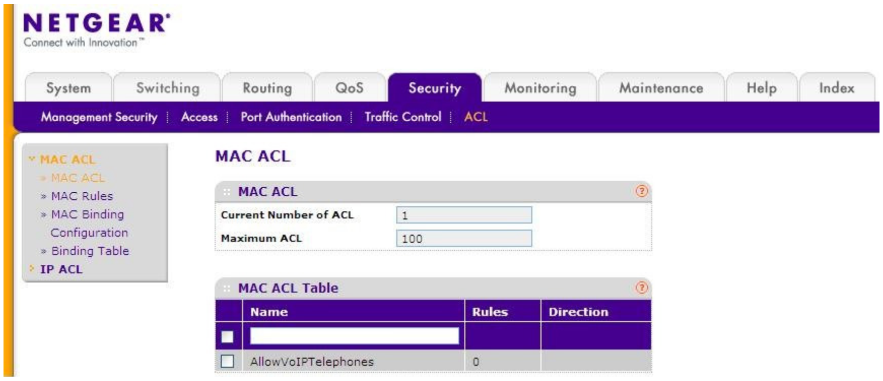
MAC ACL

MAC ACL	
Current Number of ACL	0
Maximum ACL	100

MAC ACL Table

	Name	Rules	Direction
☐	AllowVoIPTelephones		

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



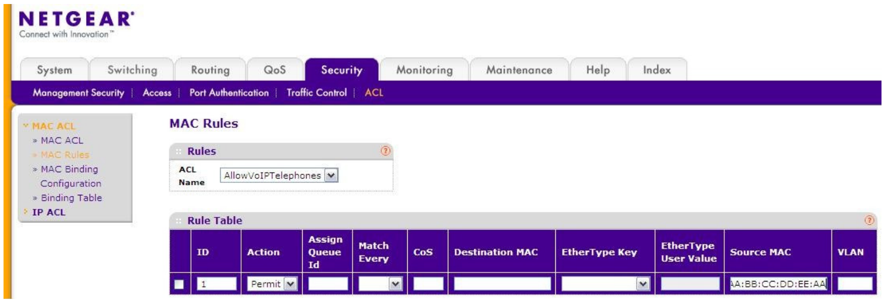
MAC ACL

MAC ACL	
Current Number of ACL	1
Maximum ACL	100

MAC ACL Table

	Name	Rules	Direction
☐			
☐	AllowVoIPTelephones	0	

- AllowVoIPTelephones appears in the MAC ACL Table



MAC Rules

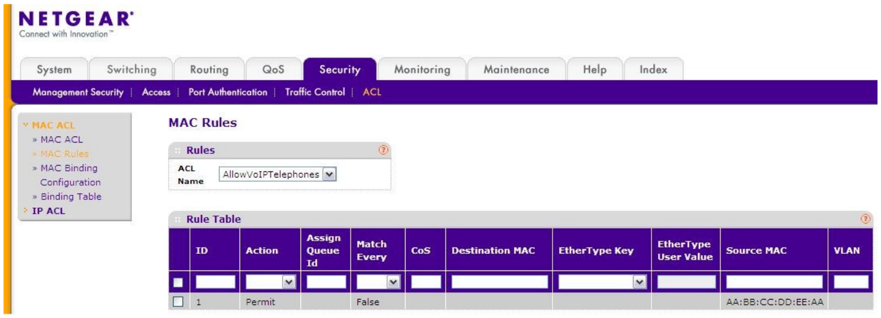
Rules

ACL Name: AllowVoIPTelephones

Rule Table

	ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	EtherType Key	EtherType User Value	Source MAC	VLAN
□	1	Permit							AA:BB:CC:DD:EE:AA	

- 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



MAC Rules

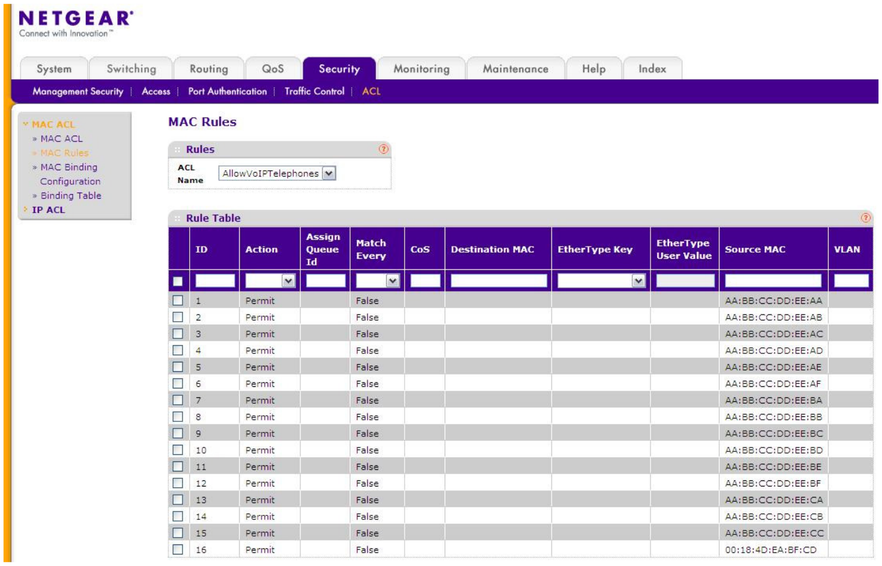
Rules

ACL Name: AllowVoIPTelephones

Rule Table

	ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	EtherType Key	EtherType User Value	Source MAC	VLAN
□										
□	1	Permit		False					AA:BB:CC:DD:EE:AA	

- 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



MAC Rules

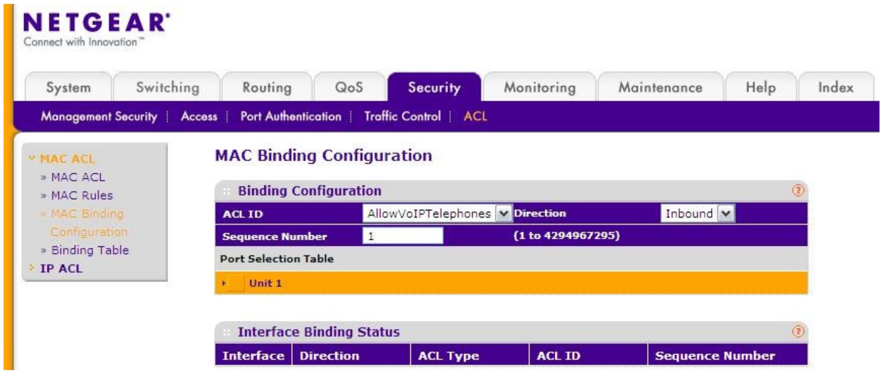
Rules

ACL Name: AllowVoIPTelephones

Rule Table

	ID	Action	Assign Queue Id	Match Every	CoS	Destination MAC	EtherType Key	EtherType User Value	Source MAC	VLAN
□										
□	1	Permit		False					AA:BB:CC:DD:EE:AA	
□	2	Permit		False					AA:BB:CC:DD:EE:AB	
□	3	Permit		False					AA:BB:CC:DD:EE:AC	
□	4	Permit		False					AA:BB:CC:DD:EE:AD	
□	5	Permit		False					AA:BB:CC:DD:EE:AE	
□	6	Permit		False					AA:BB:CC:DD:EE:AF	
□	7	Permit		False					AA:BB:CC:DD:EE:BA	
□	8	Permit		False					AA:BB:CC:DD:EE:BB	
□	9	Permit		False					AA:BB:CC:DD:EE:BC	
□	10	Permit		False					AA:BB:CC:DD:EE:BD	
□	11	Permit		False					AA:BB:CC:DD:EE:BE	
□	12	Permit		False					AA:BB:CC:DD:EE:BF	
□	13	Permit		False					AA:BB:CC:DD:EE:CA	
□	14	Permit		False					AA:BB:CC:DD:EE:CB	
□	15	Permit		False					AA:BB:CC:DD:EE:CC	
□	16	Permit		False					00:18:4D:EA:BF:CD	

- 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)



MAC Binding Configuration

Binding Configuration

ACL ID: AllowVoIPTelephones
Direction: Inbound
Sequence Number: 1 (1 to 4294967295)

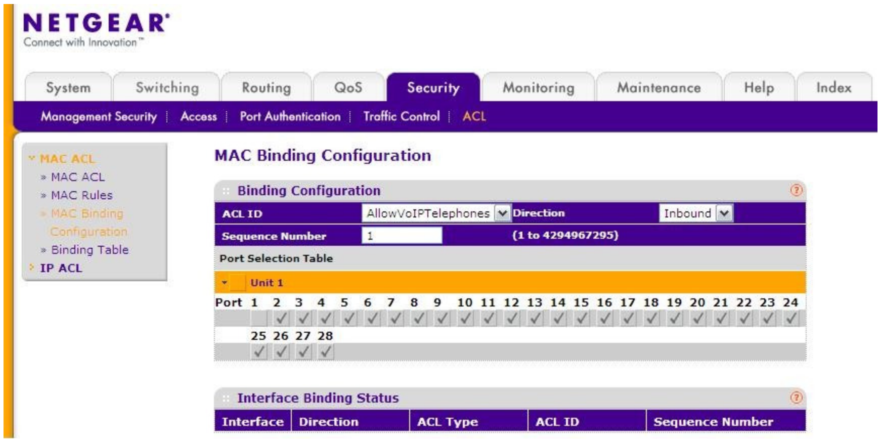
Port Selection Table

Unit 1

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

- 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



MAC Binding Configuration

Binding Configuration

ACL ID	AllowVoIPTelephones	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

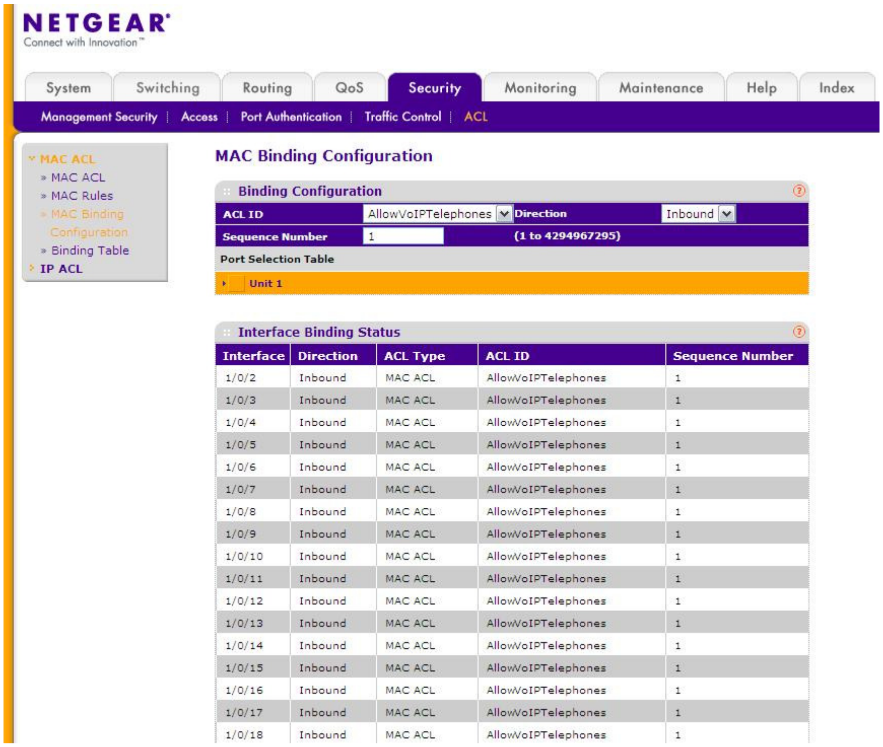
Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	25	26	27	28																				
	✓	✓	✓	✓																				

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number

- We will add the ACL to ports 2 through 28
- Check ports 2 through 28
- Press Apply
- Port 1 will not have the ACL added to it for test purposes



MAC Binding Configuration

Binding Configuration

ACL ID	AllowVoIPTelephones	Direction	Inbound
Sequence Number	1	(1 to 4294967295)	

Port Selection Table

Unit 1

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/0/2	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/3	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/4	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/5	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/6	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/7	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/8	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/9	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/10	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/11	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/12	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/13	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/14	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/15	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/16	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/17	Inbound	MAC ACL	AllowVoIPTelephones	1
1/0/18	Inbound	MAC ACL	AllowVoIPTelephones	1

- The Interface Binding Status list displays a summary of the ports we have applied the ACL to
- The configuration is now complete and can be saved through Maintenance -> Save Configuration

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.