

D-Link Single IP Management (SIM)

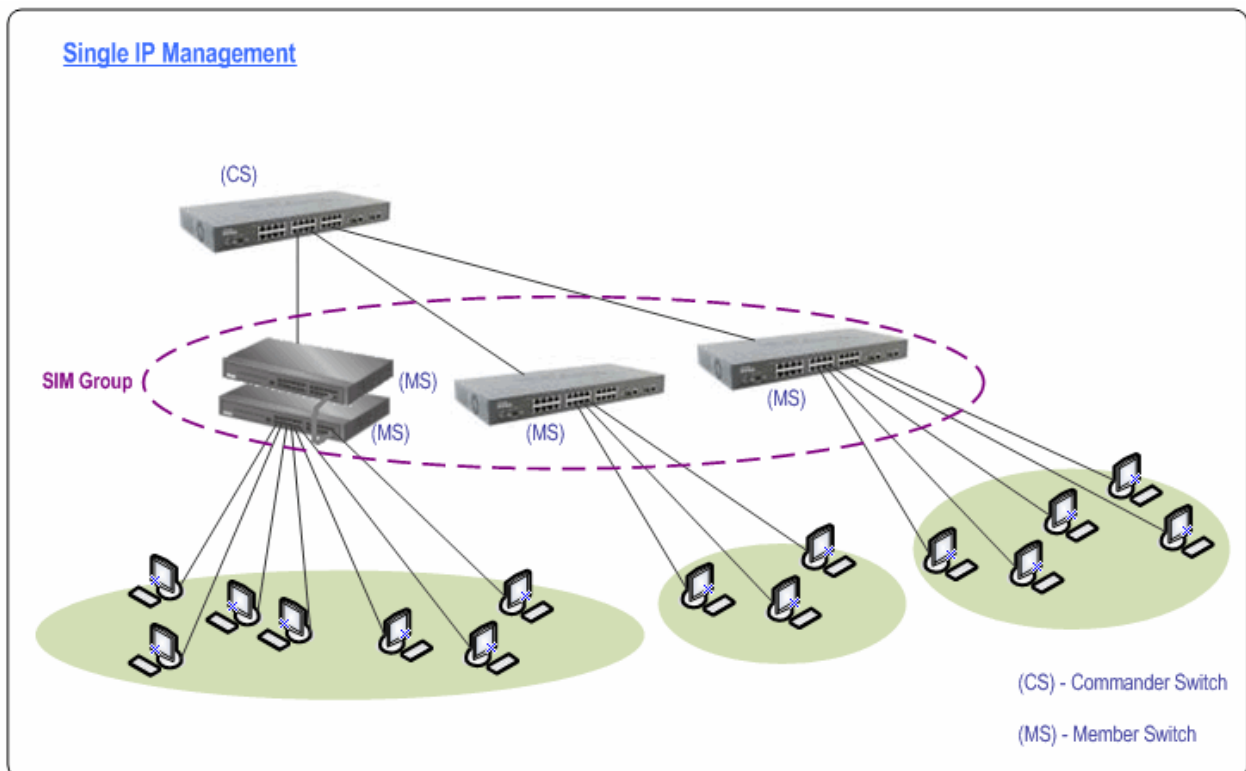
The purpose of this document is to help users comprehend the D-Link Single IP Management (SIM) feature and compare relative versions of the SIM feature.

Overview

Single IP Management (SIM), a simple and useful method to optimize network utilities and management, is designed to manage a group of switches as a single entity, called an SIM group. Implementing the SIM feature will have the following advantages for users:

- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduce the number of IP addresses needed on the network.
- Virtual stacking structure - Eliminate any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

The architecture of SIM is depicted in the following illustration:



Three components constitute an SIM group: Commander Switch (CS), Member Switch (MS), and Candidate Switch (CaS). Each SIM group consists of one CS, and up to 32 MSs. The following section introduces the role and characteristics for these three components.

The **Commander Switch (CS)** is used to be an agent to manage all switches in the same SIM group, and has the following characteristics:

- It has an IP address.
- It is not a Commander Switch or Member Switch of another Single IP group.

- It is connected to Member Switches through its management VLAN.

The **Member Switch (MS)** is a switch that has joined a single IP group, is accessible from the CS, and it takes on the following characteristics:

- It is not a CS or MS of another IP group.
- It is connected to the CS through the CS management VLAN.

The **Candidate Switch (CaS)** is a switch that is ready to join an SIM group but is not yet a member of any SIM group. The Candidate Switch may join the SIM group through an automatic function employed in SIM ready switches, or by manually configuring it to be an MS of an SIM group. A switch, configured as a CaS, is not a member of an SIM group and will take on the following characteristics:

- It is not a CS or MS of another Single IP group.
- It is connected to the CS through the CS management VLAN.

Versions of SIM

The different versions of the SIM feature are version 1.0 (SIMv1.0), version 1.5 (SIMv1.5), and version 1.6 (SIMv1.6). The following is a comparative overview of these versions.

SIMv1.0 and SIMv1.5:

The SIMv1.5 provides the following advantages over SIMv1.0:

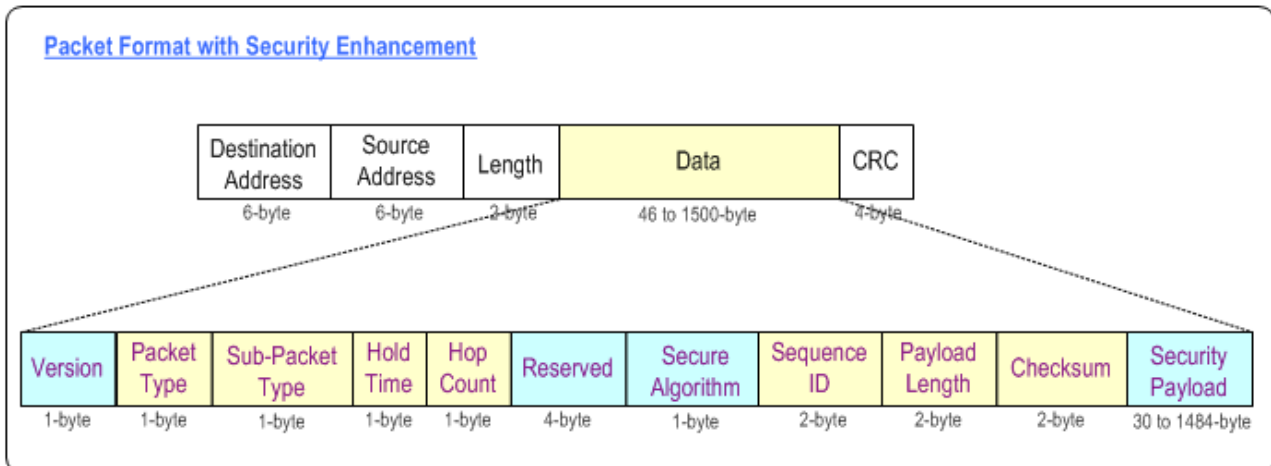
- Enable saving all members of the Commander Switch to non-volatile memory.
In SIMv1.0, the Commander Switch (CS) was not able to save Member Switch information to its memory, and thus, once a Member Switch was rebooted, it reverted back to CaS status, and all pertinent information was lost. In SIMv1.5, if the MS was saved to the CSs member list, the Switch will be automatically re-added to the member list of the CS. The topology map information will be re0collected, when the CS reboots.
- Now displays trunk information on topology map.
In SIMv1.0, only the port speed is shown, regardless of its trunking setting, SIMv1.5 is designed to show trunk speed instead of port speed. When a port belongs to a trunk, the topology map will display multiple lines to illustrate the trunking links.
- Reduce network resources, such as the RAM and FLASH memory space needed for SIM.
- Support topology map zooming on Web.
- Support multiple firmware/configuration file upload/download.

SIMv1.5 and SIMv1.6:

SIMv1.5 provides the substantial functional enhancement as above, yet still lacks the necessary security features. Most of the security problems are due to the transmission of packets without encryption. Thus, SIMv1.6, was developed to enhance security, by adding encryption/ decryption mechanisms. Moreover, devices with the SIMv1.6 security feature can operate with devices that have been upgraded to at least SIMv1.5 (no security facility), and are capable of automatically distinguishing packets with and without security enhancement. Therefore, there is no backward compatibility issue for the implementation of SIMv1.6.

Packet Format

The following diagram illustrates the packet format with security enhancement. With the exception of the Topology packets, this packet format is applied to Discovery Packets, Report Packets, Maintenance Packets, Configuration Packets, and Redirection Packets. Please also note that when a device without security enhancement receives a packet with security enhancement, the device will drop the Discovery/Report packets.



The definition of fields in the secure packet format is much the same as the packet format without security except in the following fields: (1) Version, (2) Reserve, (3) Secure Algorithm, and (4) Payload.

(1) Version - The version of the Single IP Management packet. The version of this packet format is 0x02.

(2) Reserve - The length of this field is changed from 5 bytes to 4 bytes. Always 0x00.

(3) Secure Algorithm -

- 0x00 - no secure enhancement
- 0x01 – D-Link internal algorithm (XOR)
- 0x02 to 0xFF - reserved for future usage

(4) Payload - The encrypted payload.

Operation of SIMv1.6

The operation of SIMv1.6 contains three stages: Collection, Maintenance, and Management.

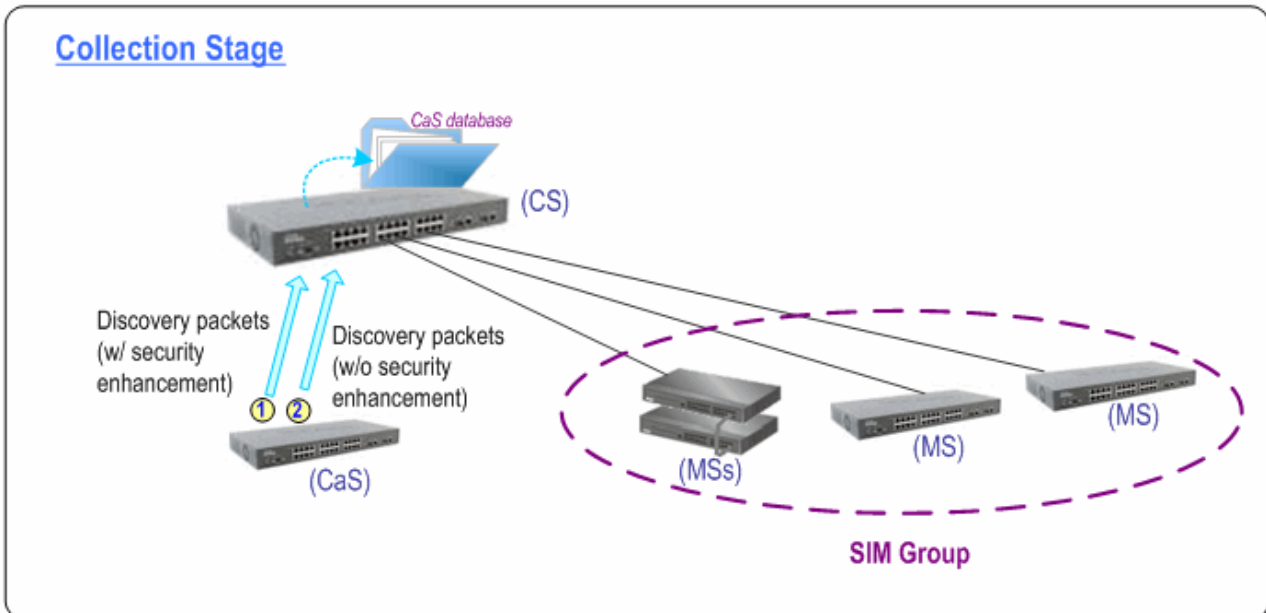
Collection Stage

In the Collection stage, the CS will send Report packets with and without secure enhancement to CaSs periodically, and the CaS will also send Discovery packets with and without secure enhancement periodically during the same time period. The Report/Discovery packets with secure enhancement will be encrypted by a default algorithm. Also, some information about secure enhancement is encoded in the payload as well. This information is about maximum and preferred secure levels that the device supports.

The following diagram illustrates CS operations once information has been received from the CaS:

The CaS will send two Discovery packets at the same time, one with security enhancement, and the other without security enhancement. When the CS receives the Discovery packet without security enhancement

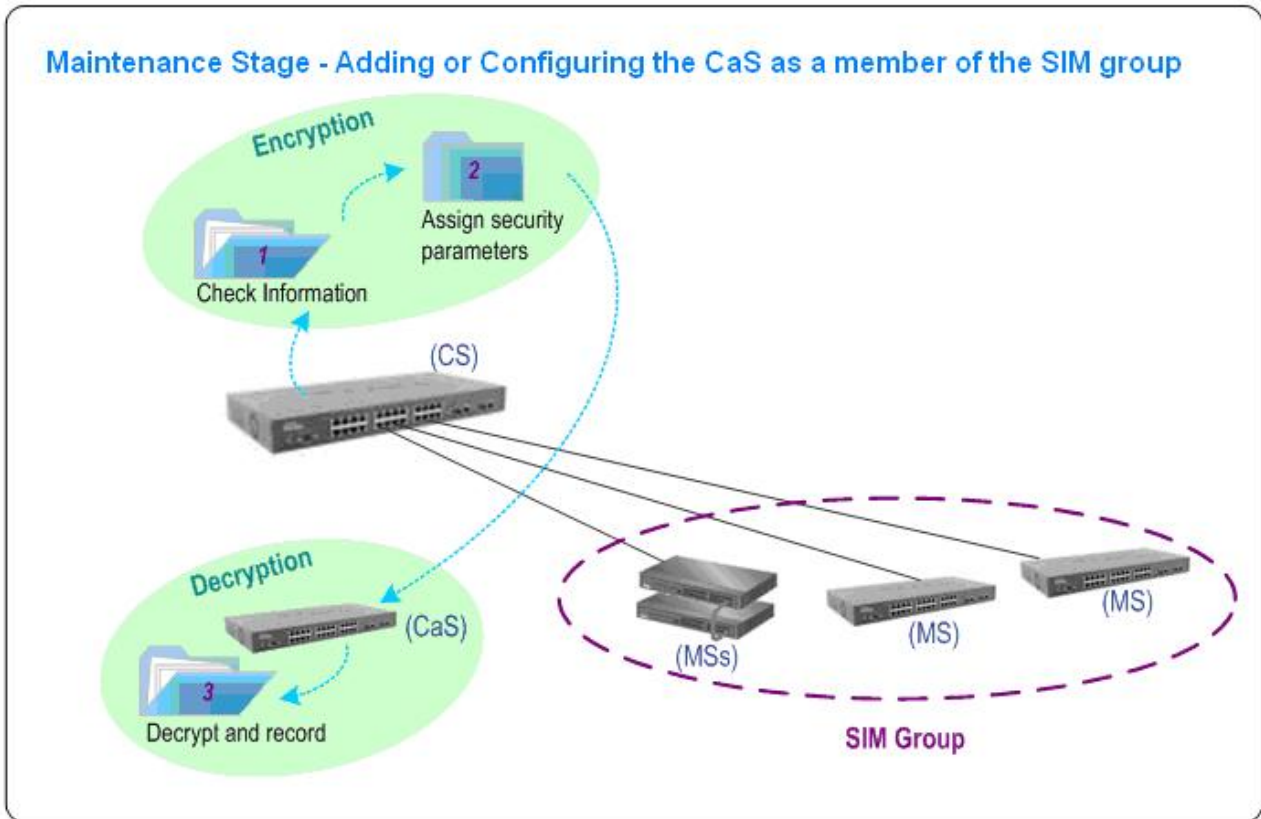
from the CaS, the CS will wait 20 seconds to receive the Discovery packet with security enhancement. If the CS receives the Discovery packet with security enhancement within this period (20-second), the CaS will be recognized as supporting security enhancement. Otherwise, the CaS will be recognized as lacking security enhancement. Then the security capability of the CaS will be recorded in the CaS database of the CS.



Maintenance Stage

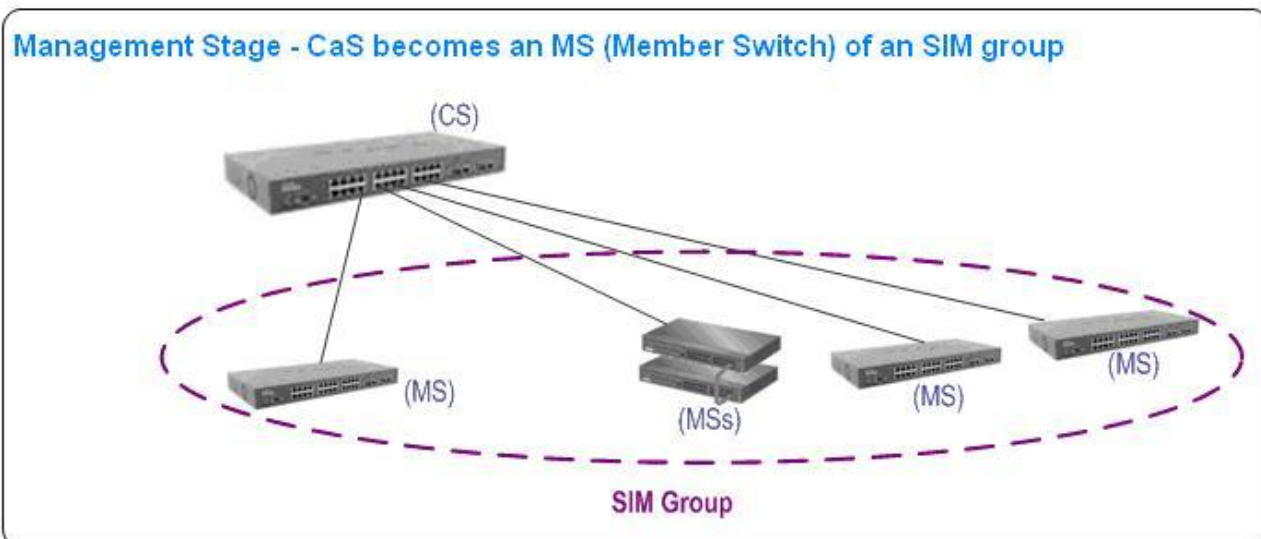
After the Report/ Discovery packets are exchanged, the membership and communication method between the CaS and the CS will be done and decided in the Maintenance stage. The following illustrations depict operations in the CS on adding and configure the CaS as a member of its group and operations in the CaS on receiving the join group command from the CS.

When configuring a CaS as a Member Switch through a user interface, the SIM kernel will look up the information of the indicated CaS to determine security parameters. This process can be viewed as an encryption. After the encryption, the CS will send Configuration Packets with these corresponding parameters to configure the CaS. After receiving the Configuration Packets from the CS, the CaS will decrypt the packet and save these security parameters. Then the CaS will become a MS of the SIM group and use the security setting to communicate with CS in the future, see the following diagram labeled "Management Stage".



Management Stage

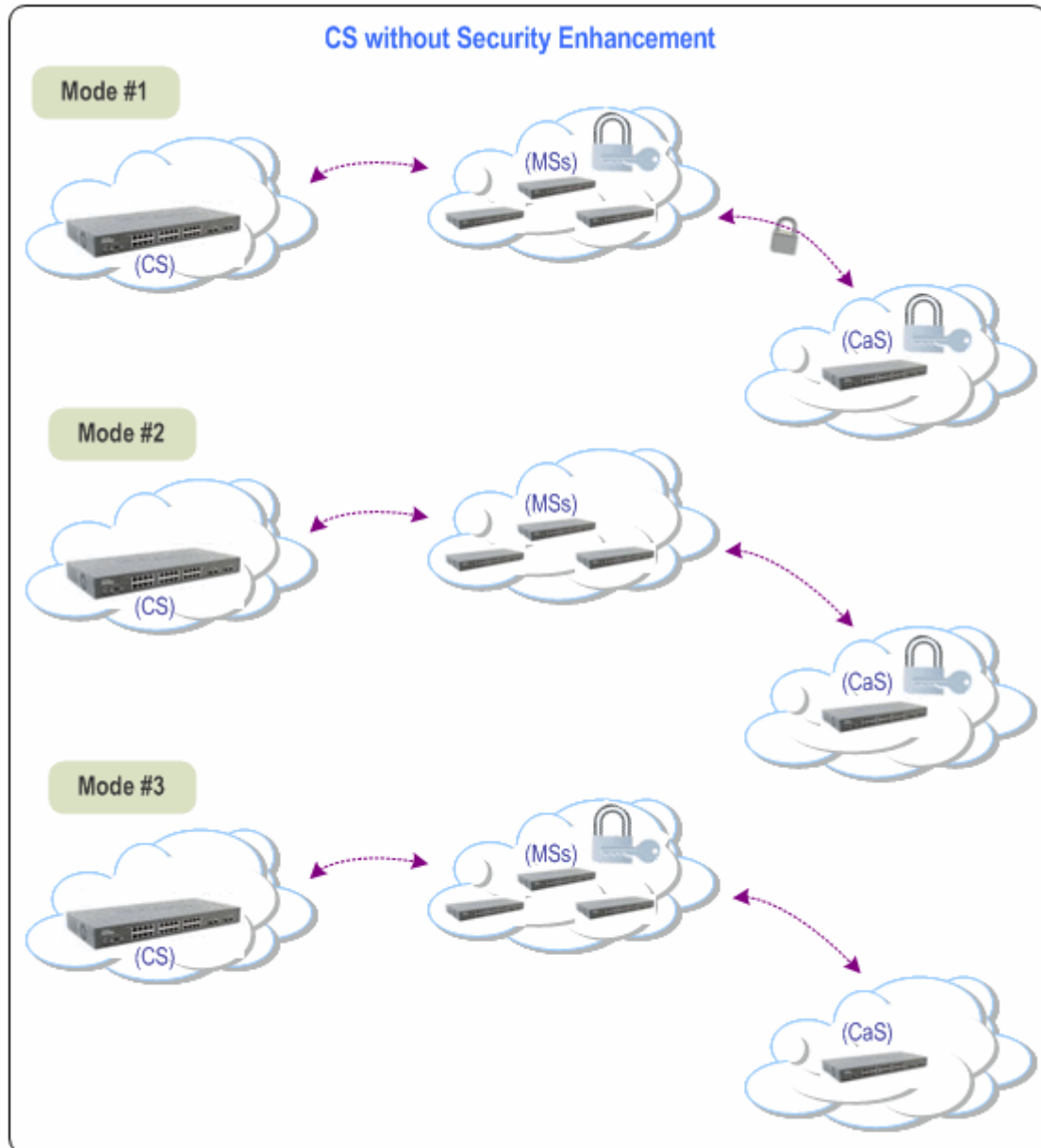
Finally, the membership is completely established between the CS and the new member. The role of the CaS becomes MS in this stage. The new MS will adopt and follow the communication method (encrypted or not), decided in the Maintenance Stage, in order to communicate with the CS as other Member Switches do within the same group.



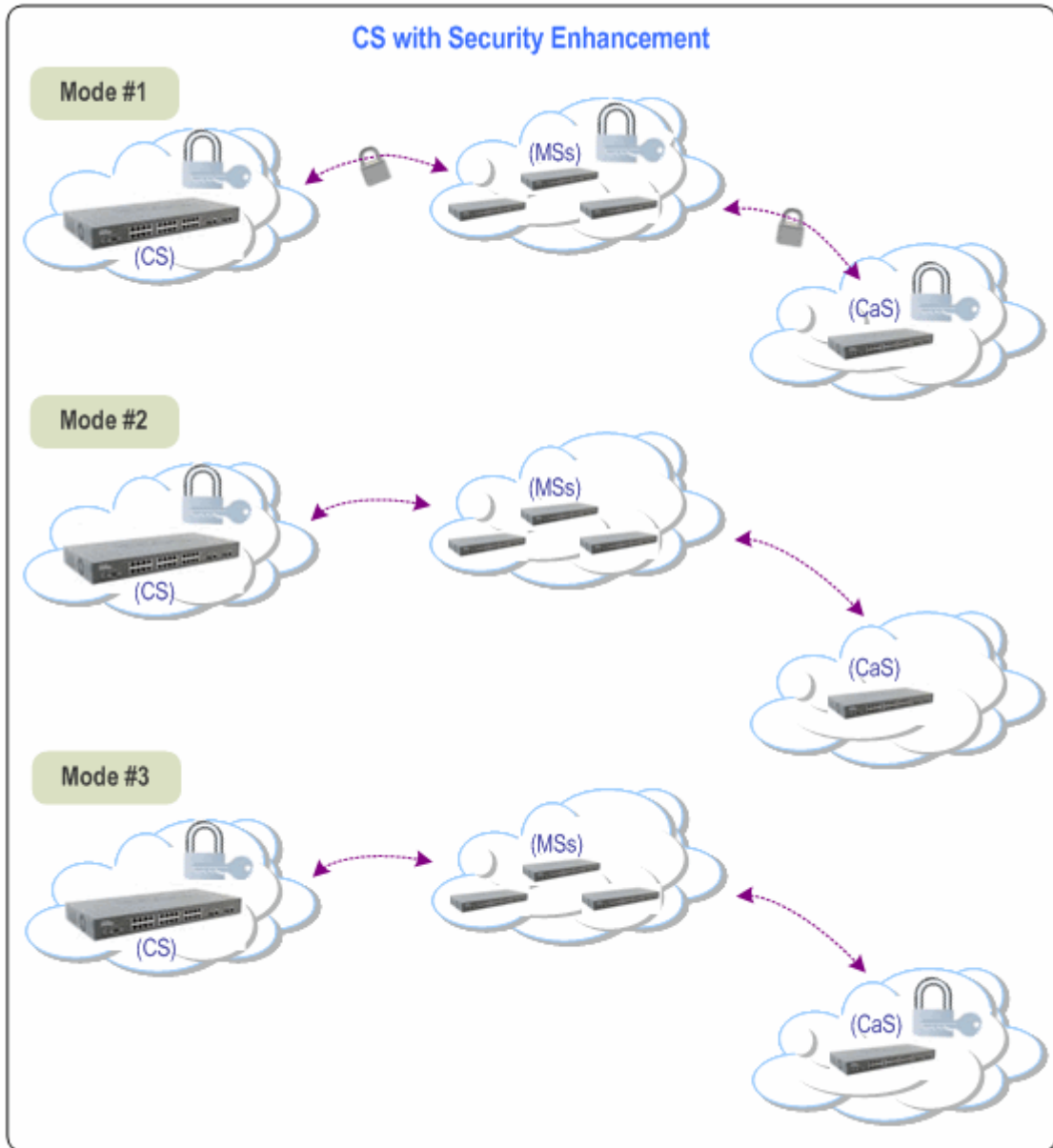
Interactions in SIM Topology

Based on the CS with or without security enhancement, interactions between switches in the SIM topology can be distinguished in five modes.

1. When the CS does not support security enhancement, all membership established between CSs and MSs are without security enhancement. In the following illustrations, the CS will only receive packets without security enhancement, regardless of what capabilities CaSs and MSs have.



2. When all devices (CS, MSs, and CaS) support secure enhancement, the interactions among them are secured. See Mode #1 of the following illustration. If both MS and CaS do not provide secure enhancement, all memberships are established without security enhancement, even if the CS has the security feature (See also the Mode #2). Mode #3 diagram depicts that if the CS is with security enhancement, but the CaS with security enhancement is separated by a device without a security facility, the membership between the CS and the CaS is conducted without security enhancement.



Products with SIM Feature

All D-Link SIM-ready products are listed in the following table.

Mode Name	SIM		
	SIMv1.0	SIMv1.5	SIMv1.6
DES-3010G/3010F/3010FL/3018/3026		R1/R2	R3
DES-3526/3526DC/3550	R1/R2/R3/ R3.5/R3.6 (R3.6 for DES-3526 only)		R4
DES-3828/3828P/3828DC		R1/R2	R3
DES-3852		R2	R3
DGS-3224TGR	R3		
DGS-3426/3427/3450		R1	R1.2
DGS-3426P			R1.2
DGS-3312SR	R2		
DGS-3324SR/3324SRi	R1/R2/R3/R4.0/R4.1/R4.2		R4.3
DXS-3326GSR/3350SR	R1/R2/R3/R4.0/R4.1/R4.2		R4.3
DES-6500	R2		