



# SonicOS and SonicOSX 7

## Switching

Administration Guide  
for the NSa and NSsp Series

SONICWALL®

# Contents

<b>About Switching</b> .....	<b>4</b>
SonicOS/X 7 Switching .....	4
Benefits of Switching .....	5
How Switching Works .....	5
Glossary .....	5
<b>Configuring VLAN Trunking</b> .....	<b>7</b>
NETWORK   Switching > VLAN Trunking .....	7
About Trunking .....	7
Viewing VLANs .....	8
<b>Managing L2 Discovery and LLDP/LLTDV</b> .....	<b>12</b>
About Layer 2 Discovery and LLDP .....	12
Supported LLDP Modes .....	13
Type-Length-Values .....	13
Effect of Interface Link on LLDP Functions .....	15
Associating an LLDP Profile with a L2 Discovery Interface .....	16
Refreshing the Page .....	16
Globally Enabling/Disabling LLDP .....	16
Discovering Neighbors .....	17
Viewing L2 Discovery and LLDP/LLTD Interfaces .....	17
Displaying Peer Information .....	18
Displaying Statistics .....	19
Searching the L2 Discovery Table .....	19
<b>Configuring Link Aggregation</b> .....	<b>20</b>
About Link Aggregation .....	20
Static LAG .....	20
Dynamic Lag .....	21
Viewing Link Aggregation .....	22
Viewing Status .....	22
Viewing Link Aggregation Ports .....	23
Creating a Logical Link (LAG) .....	23
Deleting a LAG .....	24
<b>Configuring Port Mirroring</b> .....	<b>25</b>
Viewing Mirrored Ports .....	25
Configuring a Port Mirroring Group .....	26
Enabling a Mirrored Group .....	27
Editing a Port Mirroring Group .....	27

Deleting Port Mirroring Groups .....	28
Removing Port Group Members .....	28
Removing Multiple Port Mirror Groups .....	28
Removing All Port Mirror Groups .....	28
<b>SonicWall Support</b> .....	<b>29</b>
About This Document .....	30

# About Switching

- ① **NOTE:** References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.
- ① **NOTE:** This section describes advanced switching in SonicOS/X, which is different from managing a Dell X-Series switch from a firewall. For more information about managing X-Series switches, look for the *X-Series Deployment Guide* at <https://www.sonicwall.com/support/technical-documentation>.

SonicWall appliances can manage two different switch product lines: the X-Series extended switches and the SonicWall SWS-series switches. For details refer to the *SonicOS/X System Administration Guide* at <https://www.sonicwall.com/support/technical-documentation>.

For complete details, refer to the *SonicWall Switch Getting Started Guide* at <https://www.sonicwall.com/support/technical-documentation>.

## Topics:

- [SonicOS/X 7 Switching](#)
- [Benefits of Switching](#)
- [How Switching Works](#)
- [Glossary](#)

## SonicOS/X 7 Switching

SonicOS/X provides Layer 2 (data link layer) switching functionality that supports these switching features:

- **VLAN Trunking** – Provides the ability to trunk different VLANs between multiple switches.
- **Layer 2 Network Discovery** – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.
- **Link Aggregation** – Provides the ability to aggregate ports for increased performance and redundancy.
- **Port Mirroring** – Allows you to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.
- **Jumbo Frames** – Supporting jumbo frames allows the SonicOS/X to process Ethernet frames with payloads ranging from 1500-9000 bytes.

# Benefits of Switching

SonicOS/X provides a combined security and switching solution. Layer 2 switching features enhance the deployment and interoperability of SonicWall devices within existing Layer-2 networks.

## How Switching Works

Some switching features operate on PortShield Groups and require preliminary configuration on the **NETWORK | System > PortShield Groups** page. Some operate on existing **NETWORK | System > Interfaces** configurations. For more information about configuring these related features in SonicOS/X, see:

- [Configuring VLAN Trunking](#)
- [Managing L2 Discovery and LLDP/LLTDV](#)
- [Configuring Link Aggregation](#)
- [Configuring Port Mirroring](#)

## Glossary

<b>BDPU</b>	Bridge Protocol Data Unit – Used in RSTP, BPDUs are special data frames used to exchange information about bridge IDs and root path costs. BPDUs are exchanged every few seconds to allow switches to keep track of network topology and start or stop port forwarding.
<b>CoS</b>	Class Of Service – Cos (IEEE 802.1p) defines eight different classes of service that are indicated in a 3-bit user_priority field in an IEEE 802.1Q header added to an Ethernet frame when using tagged frames on an 802.1 network.
<b>DSCP</b>	Differentiated Services Code Point – Also known as DiffServ, DSCP is a networking architecture that defines a simple, coarse-grained, class-based mechanism for classifying and managing network traffic and providing Quality of Service (QoS) guarantees on IP networks. RFC 2475, published in 1998 by the IETF, defines DSCP. DSCP operates by marking an 8-bit field in the IP packet header.
<b>IETF</b>	Internet Engineering Task Force – The IETF is an open standards organization that develops and promotes Internet standards.
<b>L2</b>	OSI Layer 2 (Ethernet) – Layer 2 of the seven layer OSI model is the Data Link Layer, on which the Ethernet protocol runs. Layer 2 is used to transfer data among network entities.
<b>LACP</b>	Link Aggregation Control Protocol – LACP is an IEEE specification that provides a way to combine multiple physical ports together to form a single logical channel. LACP allows load balancing by the connected devices.

<b>LLDP</b>	Link Layer Discovery Protocol (IEEE 802.1AB) – LLDP is a Layer 2 protocol used by network devices to communicate their identity, capabilities, and interconnections. This information is stored in a MIB database on each host, which can be queried with SNMP to determine the network topology. The information includes system name, port name, VLAN name, IP address, system capabilities (switching, routing), MAC address, link aggregation, and more.
<b>LLTD</b>	Link Layer Topology Discovery (Microsoft Standard) – LLTD is a Microsoft proprietary protocol with functionality similar to LLDP. It operates on wired or wireless networks (Ethernet 802.3 or wireless 802.11).
<b>PDU</b>	Protocol Data Unit – In the context of the Switching feature, the Layer 2 PDU is the frame. It contains the link layer header followed by the packet.
<b>RSTP</b>	Rapid Spanning Tree Protocol (IEEE 802.1D-2004) – RSTP was defined in 1998 as an improvement to Spanning Tree Protocol. It provides faster spanning tree convergence after a topology change.

# Configuring VLAN Trunking

## Topics:

- [NETWORK | Switching > VLAN Trunking](#)
- [About Trunking](#)
- [Viewing VLANs](#)
- [Editing VLANs](#)
- [Adding a VLAN Trunk Port](#)
- [Enabling a VLAN on a Trunk Port](#)
- [Deleting VLAN Trunk Ports](#)

## NETWORK | Switching > VLAN Trunking

Reserved VLAN Information	VLAN Table	VLAN Trunks
		Starting VLAN ID 3968 Ending VLAN ID 3999

## Topics:

- [About Trunking](#)
- [Viewing VLANs](#)
- [Editing VLANs](#)
- [Adding a VLAN Trunk Port](#)
- [Deleting VLAN Trunk Ports](#)
- [Enabling a VLAN on a Trunk Port](#)

## About Trunking

Unassigned switch ports on SonicOS/X can function as VLAN trunk ports. You can enable or disable VLANs on the trunk ports, allowing the existing VLANs on SonicOS/X to be bridged to respective VLANs on another switch connected through the trunk port. SonicOS/X support 802.1Q encapsulation on the trunk ports. A maximum of 32 VLANs can be enabled on each trunk port.

The VLAN trunking feature provides these functions:

- Change VLAN ID's of existing PortShield groups
- Add/delete VLAN trunk ports
- Enable/disable customer VLAN IDs on the trunk ports

The allowed VLAN ID range is 1-4094. Some VLAN IDs are reserved for PortShield use, and the reserved range is displayed on **NETWORK | Switching > VLAN Trunking**.

You can mark certain PortShield groups as "Trunked." If the PortShield group is dismantled, the associated VLAN is automatically disabled on the trunk ports.

VLANs can exist locally in the form of PortShield groups or can be totally remote VLANs. You can change the VLAN ID of PortShield groups on SonicOS/X. This allows easy integration with existing VLAN numbering.

SonicOS/X does not allow changing port VLAN membership in an ad-hoc manner. VLAN membership of a port must be configured through PortShield configuration in the SonicOS/X management interface.

A virtual interface (called the VLAN Trunk Interface) is automatically created for remote VLANs. When the same remote VLAN is enabled on another trunk port, no new interface is created. All packets with the same VLAN tag ingressing on different trunk ports are handled by the same virtual interface. This is a key difference between VLAN sub-interfaces and VLAN trunk interfaces.

The **Name** column in **NETWORK | System > Interfaces** displays the VLAN IDs of the VLAN Trunk Interfaces for the VLAN trunks.

You can enable any VLAN, local or remote, on a VLAN trunk to allow bridging to two respective VLANs on another switch. For example, local VLAN 345 can be enabled on the VLAN trunk for port X2, which also has two remote VLANs enabled on it. Example of VLAN table with VLAN enabled shows the VLAN Table on the **NETWORK | Switching > VLAN Trunking > VLAN Table** page displaying the Member Port, X9, as a member of local VLANs after the VLAN is enabled on the VLAN trunk.

VLAN trunking interoperates with the Link Aggregation and Port Mirroring features. A VLAN trunk port can be mirrored, but cannot act as a mirror port itself.

Ports configured as VLAN trunks cannot be used for any other function and are reserved for use in Layer 2 only. For example, you cannot configure an IP Address for the trunk ports.

When a Trunk VLAN interface has been configured on a particular trunk port, that trunk port cannot be deleted until the VLAN interface is removed, even though the VLAN is enabled on multiple trunk ports. This is an implementation limitation.

## Viewing VLANs

- [Reserved VLAN Information](#)
- [VLAN Table](#)



# Reserved VLAN Information

Reserved VLAN Information VLAN Table VLAN Trunks  
**Starting VLAN ID** 3968  
**Ending VLAN ID** 3999

The **Reserved VLAN Information** table lists the range of reserved VLAN IDs:

- Starting VLAN ID
- Ending VLAN ID

## VLAN Table

Reserved VLAN Information VLAN Table VLAN Trunks Refresh

VLAN ID	INTERFACE	MEMBER PORTS	TRUNKED
3968	X0	X0	false
3969	X1	X1	false
3970	X2	X2	false
3971	X3	X3	false
3972	X4	X4	false
3973	X5	X5	false
3974	X6	X6	false
3975	X7	X7	false
3976	X8	X8	false
3977	X9	X9	false
3978	X10	X10	false
3979	X11	X11	false
3980	X12	X12	false
3981	X13	X13	false
3982	X14	X14	false
3983	X15	X15	false
3984	X16	X16	false
3985	X17	X17	false
3986	X18	X18	false

Total: 19 item(s)

<b>Trunk Port</b>	Interface for the Trunk port and the number of VLAN entries associated with it
<b>VLAN ID</b>	ID(s) of the VLAN(s)
<b>Configure</b>	Contains Delete icons for the VLANs

To display the VLAN ID(s) of the Trunk Port, click the **Expand** icon for the Trunk port. To display the VLAN ID(s) of all the Trunk Ports, click the **Expand** icon in the **VLAN Trunks** table header. To hide the VLAN ID(s), click the appropriate **Collapse** icon.

## Editing VLANs

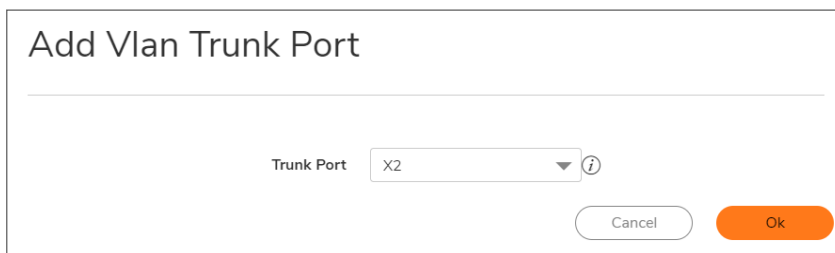
### To edit a VLAN:

1. Navigate to **Switching > VLAN Trunking**.
2. Click the Configure icon in the VLAN Table row for the VLAN ID you want to edit. The Edit VLAN for PortShield Host dialog displays.
3. Do one of the following:
  - Type a different VLAN ID into the VLAN ID field. You can enter any VLAN ID except the original system-specified VLAN ID or any others in the Reserved VLAN Information table.
  - Use the VLAN ID number in the VLAN ID field, which matches the one for which you clicked the Configure icon.
4. To enable trunking for this VLAN, select the Trunked checkbox. To disable trunking for this VLAN, clear the checkbox.
5. Click **OK**.

## Adding a VLAN Trunk Port

### To add a VLAN Trunk Port:

1. Navigate to **Switching > VLAN Trunking**.
2. Under VLAN Trunks, click **+Add**. The **Add VLAN Trunk Port** dialog displays.



The screenshot shows a dialog box titled "Add Vlan Trunk Port". Below the title bar is a horizontal line. Underneath the line, there is a label "Trunk Port" followed by a dropdown menu that currently displays "X2". To the right of the dropdown is a small circular help icon. At the bottom right of the dialog, there are two buttons: "Cancel" and "Ok".

3. Select the port to add from the **Trunk Port** drop-down menu.
4. Click **OK**.

## Enabling a VLAN on a Trunk Port

### To enable a custom VLAN ID on a specific trunk port:

1. Navigate to **NETWORK | Switching > VLAN Trunking**.
2. Under the **VLAN Trunks** table, click **Enable VLAN**. The **Enable VLAN** dialog displays.
3. Select a trunked port from the **Trunked Port** drop-down menu. This is the port that you want to use to trunk the VLAN ID indicated in the **VLAN ID** field.
4. In the **VLAN ID** field, type in the VLAN ID to be trunked. This can be a VLAN ID on another switch.
5. Click **OK**.

# Deleting VLAN Trunk Ports

You can delete one VLAN trunk port, multiple ports at a time, or all ports.

## **To delete a VLAN trunk port:**

1. Navigate to **NETWORK | Switching > VLAN Trunking**.
2. Expand the VLAN trunk port to be deleted.
3. Click the **Delete** icon in the **Configure** column for the VLANs to be deleted. A confirmation message displays:
4. Click **OK**.
5. Click the **Delete** icon in the **Configure** column for the port to be deleted. A confirmation message displays:
6. Click **OK**.

## **To delete multiple VLAN trunk ports:**

1. Navigate to **NETWORK | Switching > VLAN Trunking**.
2. In the **VLAN Trunks** table, expand the VLAN trunk ports to be deleted.
3. Click the **Delete** icon in the **Configure** column for each VLAN to be deleted. A confirmation message displays:
4. Click **OK** for each one.
5. Select the checkboxes for the VLAN trunk ports you want to delete. **Delete** becomes available.
6. Click **Delete**. A confirmation message displays.
7. Click **OK**.

## **To delete all VLAN trunk ports:**

1. Navigate to **NETWORK | Switching > VLAN Trunking**.
2. In the **VLAN Trunks** table, expand the VLAN trunk ports by clicking the **Expand** icon in the **VLAN Trunks** table heading.
3. Click the **Delete** icon in the **Configure** column for each VLAN to be deleted. A confirmation message displays:
4. Select the checkbox in the **VLAN Trunks** table heading. Delete becomes available.
5. Click **Delete**. A confirmation message displays.
6. Click **OK**.

# Managing L2 Discovery and LLDP/LLTDV

## Topics:

- [About Layer 2 Discovery and LLDP](#)
- [Associating an LLDP Profile with a L2 Discovery Interface](#)
- [Refreshing the Page](#)
- [Globally Enabling/Disabling LLDP](#)
- [Discovering Neighbors](#)
- [Viewing L2 Discovery and LLDP/LLTD Interfaces](#)

## About Layer 2 Discovery and LLDP

To discover neighboring devices and their capabilities, the SonicWall Security Appliance uses:

- IEEE 802.1AB (LLDP: Link Layer Discovery Protocol)/Microsoft LLTD (Link Layer Topology Discovery)
- IEEE 802.3-2012 protocols
- A switch-forwarding table

LLDP operates at Layer 2 and exchanges LLDP Protocol Data Units (LLDPDUs) between the neighbors containing a sequence of variable length information elements that include type-length-values (TLV). The information is stored in the SNMP MIBs. These Layer 2 protocols are used by networking devices to advertise their identities and capabilities and to identify their directly connected Layer 2 neighbors/peers on wired Ethernet networks; they do not cross a broadcast domain.

More information about these protocols is available at:

- [https://en.wikipedia.org/wiki/Link\\_Layer\\_Topology\\_Discovery](https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery)
- [https://en.wikipedia.org/wiki/Link\\_Layer\\_Discovery\\_Protocol](https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol)

SonicOS/X supports LLDP Transmit and Transmit-Receive Modes.

- [https://msdn.microsoft.com/en-us/library/windows/desktop/dn594471\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/dn594471(v=vs.85).aspx)

LLDP makes troubleshooting easier, especially in cases where peers are not detected by ping or traceroute.

## Topics:

- [Supported LLDP Modes](#)
- [Type-Length-Values](#)
- [Effect of Interface Link on LLDP Functions](#)

# Supported LLDP Modes

These LLDP modes are supported in SonicOS/X:

- LLDP-receive
- LLDP-transmit
- LLDP-transmit-receive
- LLDP-disabled

You can create custom LLDP profiles for individual interfaces.

These interface types and modes support LLDP:

Interface	LLDP Support
<b>L2 Interface</b>	If the physical port is configured in L2 Mode.
<b>L3 Interface</b>	If the physical port is configured in L3 Mode.
<b>Wire-Mode Interface</b>	Supported for secure and inspect mode for wire-mode interfaces, but not for VLAN interfaces.
<b>L2 Bridge Interface</b>	Supported for the physical interface, but not for VLAN interfaces.
<b>VLAN Sub-Interface</b>	Not supported.
<b>LAG/LACP</b>	Supported for learn only on the aggregate port and not a member, but is supported for send on individual interfaces. An aggregate port shows neighbor information for both itself and its members.

# Type-Length-Values

Each LLDP frame starts with three mandatory type-length-values TLVs: Chassis ID, Port ID and TTL. The mandatory TLVs are followed by any number of optional TLVs. The LLDP frame ends with a mandatory End-of-frame TLV.

## Mandatory TLV's

Mandatory TLVs describes the mandatory LLDP TLVs supported for both transmit and receive.

### MANDATORY TLVS

TLV Name	TLV Type	Description	SonicOS/X Usage
Chassis ID TLV	1	Identifies the firewall chassis. Each firewall must have exactly one unique Chassis ID.	SonicOS/X sends the MAC address of the Security Appliance in the Chassis ID field. The MAC address is same as the Security Appliance serial number.
Port ID TLV	2	Identifies the port from which the LLDPDU is sent. The Security Appliance uses the interface's if name as the Port ID. For example, Port ID can be X1, X2, X3.	The Port ID subtype 5 (interface name) is used to identify the transmitting port.
Time-to-live (TTL) TLV	3	Specifies how long (in seconds) LLDPDU information received from the peer is retained as valid in the local Security Appliance (range is 0-65535). The value is a multiple of the LLDP Hold Time Multiplier. When the TTL value is 0, the information associated with the device is no longer valid and SonicOS/X removes that entry from the database.	Calculated internally.
End of LLDPDU frame TLV	0	Indicates the end of the TLVs in the LLDP Ethernet frame.	

## Optional TLVs

Optional TLVs describes the optional LLDP TLVs supported for both transmit and receive.

### OPTIONAL TLVS

Port Description	4		
System Name	5	The Security Appliance name in alpha-numeric format.	

System Description	6	The full name and version identification of the system's hardware type, software operating system, and networking software in alphanumeric format.
System Capabilities	7	<p>This field contains a bit-map of the capabilities that define primary functions of the system. Describes the deployment mode of the interface:</p> <ul style="list-style-type: none"> <li>• An L3 interface is advertised with router (bit 6) capability and the "other" bit (bit 1).</li> <li>• An L2 interface is advertised with MAC Bridge (bit 3) capability and the "other" bit (bit 1).</li> </ul> <p>A virtual wire interface is advertised with Repeater (bit 2) capability and the "other" bit (bit 1).</p>
Management Address	8	<p>IP addresses used for the management of the device:</p> <ul style="list-style-type: none"> <li>• IP address of the management (MGT) interface</li> <li>• IPv4 and/or IPv6 address of the interfaceLoopback address</li> <li>• User-defined address entered in the management address field; If no management IP address is provided, the default is the MAC address of the transmitting interface. The interface number of the specified management address is included. Also included is the OID of the hardware interface with the specified management address (if applicable). If more than one management address is specified, they are sent in the order they are specified, starting at the top of the list.</li> </ul> <p>One Management Address is supported. This is an optional parameter and can be left disabled.</p>

## Effect of Interface Link on LLDP Functions

LLDP only functions when the interface link is up. When the mode is changed:

- From Receive to Transmit ,
- From Transmit-Only to Receive-Only,
- To Disabled,

A final LLDP shutdown LLDPDU is sent with these mandatory TLVs:

- Chassis ID TLV
- Port ID TLV
- TTL TLV
- End of LLDPDU TLV

The statistics counters are reset after the link goes down.

## Topics:

- [Associating an LLDP Profile with a L2 Discovery Interface](#)
- [Refreshing the Page](#)
- [Globally Enabling/Disabling LLDP](#)
- [Discovering Neighbors](#)

# Associating an LLDP Profile with a L2 Discovery Interface

## *To associate an LLDP profile to a L2 Discovery interface:*

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. Click the **Edit** icon in the **Configure** column for the interface. The **Discover on Interface** dialog displays.  
image
3. Select the default or custom profile from LLDP Profile:
  - Default LLDP Disabled
  - Default LLDP RX (default)
  - Default LLDP TX
  - Default LLDP RX\_TX
  - Custom profile
4. Click **Save**. The name of the profile displays in the **Profile Name** column of the **L2 Discovery** table.

# Refreshing the Page

## *To refresh data displayed on the page:*

1. Click the **Refresh** icon above the **L2 Discovery** table.

# Globally Enabling/Disabling LLDP

By default, LLDP is enabled globally. You can toggle the LLDP switch to enable or disable LLDP transmit and receive globally.

## *To globally enable/disable LLDP:*

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. Click **LLDP** above the **L2 Discovery** table. A confirmation message displays.



# Discovering Neighbors

You can discover neighbors for:

- A single interface.
- Multiple interfaces.
- All interfaces.

① **TIP:** For LAG with trunk mode, all ports can discover neighbors; LAG with PortShield mode learns neighbors only under the aggregator port.

## *To discover neighbors for a single interface:*

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. Click the Refresh icon in the **Configure** column for the interface.  
A processing message displays.  
The information for the interface is updated.

## *To discover neighbors for multiple interfaces:*

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. Select the interfaces in the **L2 Discovery** table.
3. Select **Discover** from **Discover** above the table. This option is dimmed unless an interface is selected.  
A processing message displays.  
The information for the interfaces is updated.

## *To discover neighbors for all interfaces:*

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. Select an interface in the **L2 Discovery** table.
3. Select **Discover All** from **Discover** above the table.  
A processing message displays.  
The information for all interfaces is updated.

# Viewing L2 Discovery and LLDP/LLTD Interfaces

<b>Interface</b>	Lists the Security Appliance's interfaces along with either the number of entries.
<b>Profile Name</b>	Name of the default or custom profile name.
<b>Configure</b>	Contains the <b>Statistics</b> , <b>Edit</b> , and <b>Refresh</b> icons for the interfaces. <b>NOTE:</b> The <b>Refresh</b> icon refreshes only LLTD discovery, not LLDP discovery. To refresh LLDP discovery, click the <b>Refresh</b> icon above the <b>L2 Discovery</b> table.

① **NOTE:** Only the **Interface** and **Profile Name** columns contain information about interfaces, and the **Configure** column icons apply only to the interface. The other columns display information about the entries under an interface; for information about these columns, see [Displaying Peer Information](#).

**Topics:**

- [Displaying Peer Information](#)
- [Displaying Statistics](#)
- [Searching the L2 Discovery Table](#)

## Displaying Peer Information

**To display L2 discovery information:**

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. In the **L2 Discovery** table, click the **Expand** icon for the desired interface. Information about the nodes (entries) discovered for the interface are displayed.

<b>Chassis ID</b>	Identifies the Security Appliance's chassis. Each Security Appliance must have exactly one unique Chassis ID that is a string value consisting of mostly the MAC address of the peer.
<b>Port ID</b>	Identifies the port from which the LLDPDU is sent and is a string value of the port name or number. The Security Appliance uses the interface's <i>ifname</i> as the Port ID. For example, Port ID can be X1, X2, X3.
<b>Management Address</b>	Lists the IP or MAC address of the peer used for the management of the device. If multiple management addresses are returned, only the first address is shown.
<b>System Name</b>	Name of the Security Appliance, in alpha-numeric format.
<b>System Description</b>	Full name and version identification of the Security Appliance's hardware type, software operating system, and networking software, in alpha-numeric format.
<b>More</b>	Contains an Information icon that displays additional peer information.

3. To display additional peer information for a peer entry, mouse over the **Information** icon in the **More** column for that peer. A pop-up displays.

<b>MAC Address</b>	MAC address of the peer.
<b>Vendor</b>	Vendor name from the main menu.
<b>Port Description</b>	String value from the <b>Comments</b> field for the interface on SonicWall Security Appliances.
<b>System Capabilities</b>	String value representing the list of capabilities supported by the peer device.

# Displaying Statistics

For each interface, you can display the number of:

- Transmitted, received, erroneous, and discarded frames.
- Discarded and unrecognized TLVs.
- Aged or deleted neighbors.

## ***To display an interface's statistics:***

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. In the **L2 Discovery** table, mouse over the **Statistics** icon for the interface. The **Statistics** pop-up displays.

# Searching the L2 Discovery Table

## ***To limit the interfaces displayed in the L2 Discovery table:***

1. Navigate to **NETWORK | Switching > L2 Discovery**.
2. In the **Search** field, enter the search criterion. The display changes.
3. To clear the search and redisplay the entire table. click the red **Delete** icon in the **Search** field.

# Configuring Link Aggregation

#	PORT	LAG ID	KEY	AGGREGATOR	LACP ENABLE	STATUS	PARTNER	VENDOR	STAT
No Data									
Total: 0 item(s)									

## Topics:

- [About Link Aggregation](#)
- [Viewing Link Aggregation](#)
- [Creating a Logical Link \(LAG\)](#)
- [Deleting a LAG](#)

## About Link Aggregation

Link Aggregation allows port redundancy and load balancing in Layer 2 networks by allowing you to interconnect SonicWall Security Appliances with two or more links between them in such a way that the multiple links are combined into one larger virtual pipe that can carry a higher combined bandwidth. As multiple links are present between two devices, if one link fails, the traffic is transferred through other links without disruption. With multiple links present, traffic also can be load balanced in such a way to achieve even distribution. Load balancing is controlled by the SonicWall Security Appliance, based on source and destination MAC address pairs. The **NETWORK | Switching > Link Aggregation** page provides information and statistics about and allows configuration of interfaces for aggregation.

SonicOS/X supports the two types of LAG:

- [Static LAG](#)
- [Dynamic Lag](#)

## Static LAG

In Static Link Aggregation, ports that are in the same VLAN (same PortShield Group) or are VLAN trunk ports are eligible for link aggregation. Up to four ports can be aggregated in a logical group, and there can be four Logical Links (LAGs) configured. With Static Link Aggregation, all configuration settings are set on both participating LAG components.

Two main types of usage are enabled by this feature:

---

<b>Firewall to Server</b>	Implemented by enabling Link Aggregation on ports within the same VLAN (same PortShield Group). This configuration allows port redundancy, but does not support load balancing in the appliance-to-Server direction because of a hardware limitation on the Security Appliance.
<b>Firewall to Switch</b>	Allowed by enabling Link Aggregation on VLAN trunk ports. Load balancing is performed automatically by the hardware. The Security Appliance supports one load balancing algorithm based on source and destination MAC address pairs.

---

Similarly to PortShield configuration, you select an interface that represents the aggregated group. This port is called an aggregator. The aggregator port must be assigned a unique key. Non-aggregator ports can be optionally configured with a key, which can help prevent an erroneous LAG if the switch connections are wired incorrectly.

① **NOTE:** The key is not the same as the LAG ID, which is the same as the interface number and cannot be changed. The key must be assigned when the LAG group is configured. All the non-aggregator ports should have the same key as the aggregator port.

Ports bond together if connected to the same link partner and their keys match. A link partner cannot be discovered for Static link aggregation. In this case, ports aggregate based on keys alone.

Like a PortShield host, the aggregator port cannot be removed from the LAG as it represents the LAG in the system.

① **NOTE:** After link aggregation has been enabled on VLAN trunk ports, additional VLANs cannot be added or deleted on the LAG.

## Dynamic Lag

SonicOS/X supports Dynamic Link Aggregation using Link Aggregation Control Protocol (LACP defined by IEEE 802.3ad) on all SonicWall Security Appliances that support Advanced Switching features.

### About Dynamic Lag Using LACP

LACP allows the exchange of information related to link aggregation between the members of the LAG group in protocol packets called Link Aggregation Control Protocol Data Units (PDUs). with LACP, errors in configuration, wiring, and link failures can be detected quickly.

The two major benefits of LAG such as increased throughput and link redundancy can be achieved efficiently using LACP. LACP is the signaling protocol used between members in a LAG. It ensures links are only aggregated into a bundle if they are correctly configured and cabled. LACP can be configured in one of two modes:

- **Active mode** - Device immediately sends LACP PDUs when the port comes up.
- **Passive mode** - Port is placed in a passive negotiating state, in which the port only responds to LACP PDUs it receives, but does not initiate LACP negotiation.

If both sides are configured as active, LAG can be formed assuming successful negotiation of the other parameters. If one side is configured as active and the other one as passive, LAG can be formed as the

passive port responds to the LACP PDUs received from the active side. If both sides are passive, LACP fails to negotiate the bundle. Passive mode is rarely used in deployments.

In the configuration, all member ports of the same LAG must be set up on the same VLAN as the Aggregator port. Data packets received on the LAG members are associated with the parent Aggregator port using the VLAN. When the state of the Aggregator/member ports of a LAG reaches a stable Collection/Distribution state, the ports are ready to transmit and receive data traffic.

All information related to LAG, such as the Aggregator ports configured, this information is displayed on the **NETWORK | Switching > Link Aggregation** page:

- Member ports that are part of the LAG.
- Status of each of the ports that form the LAG.
- The Partner MAC address received through LACP.

Six load balancing options are available for configuration. The load balancing option must be chosen when creating a LAG along with the Aggregator port.

① | **IMPORTANT:** You cannot modify the load balancing option after the LAG is created.

## VLAN Enhancements for LAG

With this enhancement;

- LAG does not have to be dismantled or removed before the VLAN is added/deleted. The configuring allows you to add the VLAN to an existing LAG or delete the VLAN from an existing LAG without disrupting the current traffic related to the LAG or other VLANs configured on the LAG.
- VLAN can be added to/deleted from any member of the LAG and it gets applied to all the other members of the LAG automatically without the need to explicitly add to/delete from other members of the LAG.

## Viewing Link Aggregation

**Topics:**

- [Viewing Status](#)
- [Viewing Link Aggregation Ports](#)

## Viewing Status

The **Status** table displays the MAC address System ID for the firewall.

# Viewing Link Aggregation Ports

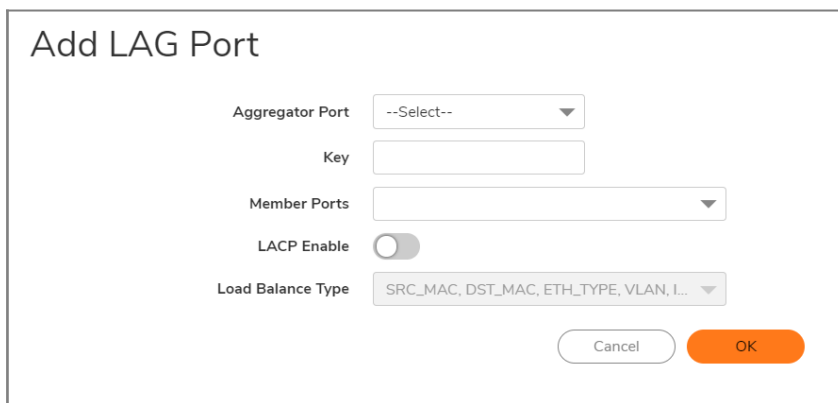
To view Link Aggregation Ports, navigate to **NETWORK | Switching > Link Aggregation**.

<b>Port</b>	Interface used as an aggregator port or a member port.
<b>LAG ID</b>	System-configured link aggregator. A port that is not an aggregator has a LAG ID of the aggregator of which it is a member.
<b>Key</b>	Indicates port membership from the <b>Add LAG Port</b> dialog.
<b>Aggregator</b>	Indicates an aggregator port by a green checkmark; otherwise, it is blank.
<b>LACP Enable</b>	Indicates whether LACP is enabled.
<b>Status</b>	Indicates whether the port is up or down.
<b>Partner</b>	MAC addresses of the link partners after they are physically connected; for <ul style="list-style-type: none"><li>• Static LAG, displays 00:00:00:00:00:00</li><li>• Dynamic LAG, displays the partner's MAC address</li></ul>
<b>Vendor</b>	Displays the name of the equipment manufacturer.

# Creating a Logical Link (LAG)

*To create a Logical Link (LAG):*

1. Navigate to **NETWORK | Switching > Link Aggregation**.
2. Click + (Add). The **Add LAG Port** dialog displays.
3. Select the interface from **Aggregator Port**.



4. Specify the port membership to an LAG group by entering the desired key into the **Key** field. The minimum value is 1, and the maximum value is 255. The field has a default value of 0, which must be replaced.
  5. Select the ports to be aggregated from the **Member Ports** drop-down menu. You can select any number of ports in the list by selecting the checkbox for each port to be aggregated.
- ① | **NOTE:** The listed ports depend on the interface chosen in Step 3.

6. To enable Link Aggregation Control Protocol (LACP) for this port, select **LACP Enable**. This option is not selected by default.
7. From **Load Balance Type**, select the how load balancing is performed:
  - ① | **IMPORTANT:** You cannot modify the load balancing option after the LAG is created.
    - SRC\_MAC, ETH\_TYPE, VLAN, INTF (default)
    - DST\_MAC, ETH\_TYPE, VLAN, INTF
    - SRC\_MAC, DST\_MAC, ETH\_TYPE, VLAN, INTF
    - SRC\_IP, SRC\_PORT
    - DST\_IP, DST\_PORT
    - SRC\_IP, SRC\_PORT, DST\_IP, DST\_PORT
8. Click **OK**.

## Deleting a LAG

### *To delete a member of a LAG:*

1. Navigate to **NETWORK | Switching > Link Aggregation**.
2. Delete the member port of the lag by clicking its **Delete** icon.

### *To delete an aggregator port:*

1. Navigate to **NETWORK | Switching > Link Aggregation**.
2. Delete all the member ports by clicking their **Delete** icons.
  - ① | **NOTE:** All member ports must be deleted from the LAG before deleting the Aggregator port.
3. Delete the aggregator port by clicking its **Delete** icon.



# Configuring Port Mirroring

You can configure Port Mirroring on SonicOS/X to send a copy of network packets seen on one or more switch ports (or on a VLAN) to another switch port called the mirror port. By connecting to the mirror port, you can monitor the traffic passing through the mirrored port(s).

GROUPS						
						+ Add — Remove
<input type="checkbox"/>	GROUP NAME	MIRROR PORT	DIRECTION	INGRESS	EGRESS	ENABLE
No Data						
Total: 0 item(s)						

**NETWORK | Switching > Port Mirroring** allows you to assign mirror ports to mirror ingress, egress or bidirectional packets coming from and/or to a group of ports.

## Topics:

- [Viewing Mirrored Ports](#)
- [Configuring a Port Mirroring Group](#)
- [Configuring a Port Mirroring Group](#)
- [Editing a Port Mirroring Group](#)
- [Deleting Port Mirroring Groups](#)

## Viewing Mirrored Ports

Monitor traffic on the mirrored port(s) by connecting to the mirror port.

<b>Group Name</b>	Name of the interface group.
<b>Mirror Port</b>	Interface used as the mirror port, that is, the port that monitors other ports on the selected direction.
<b>Direction</b>	Direction of the traffic being mirrored: <ul style="list-style-type: none"> <li>• ingress</li> <li>• egress</li> <li>• both (bidirectional)</li> </ul>
<b>Ingress</b>	Number of packets arriving on the mirrored port(s). For egress-only ports, this is always 0.

<b>Egress</b>	Number of packets sent out on the mirrored port(s). For ingress-only ports, this is always 0.
<b>Enable</b>	Indicates whether mirroring is enabled – a checkmark is in the checkbox – or disabled – the checkbox is blank – for the group.
<b>Configure</b>	Contains the <b>Edit</b> and <b>Delete</b> icons for the group entry and a Delete icon for each port in the group.

## Configuring a Port Mirroring Group

*To create a new port mirroring group:*

1. Navigate to **NETWORK | Switching > Port Mirroring**.
2. Click **+Add**. The **Add Mirror Group** dialog displays.

3. Enter a descriptive name for the group into the **Interface Group Name** field. The default name is **New Group**.
4. Enter a descriptive name for the group into the **Interface Group Name** field. The default name is **New Group**.
  - **ingress** – Monitors traffic arriving on the mirrored port(s).
  - **egress** – Monitors traffic being sent out on the mirrored port(s).
  - **both** – Monitors traffic in both directions on the mirrored port(s).

5. From the **All Interfaces** list:
  - a. Select the port to mirror the traffic to. You must use an unassigned port as the mirror port.
  - b. Click the top **Right Arrow** to move the port to the **Mirrored Port** field.
6. From the **All Interfaces** list:
  - a. Select one or more ports to be monitored. You monitor traffic on the mirrored port(s) by connecting to the mirror port.
  - b. Click the lower Right Arrow to move it/them to the **Mirrored Ports** list.
7. To enable port mirroring for these ports, select **Enable**.
  - ① **NOTE:** Only one ingress group and one egress group can be enabled at one time. If a group has both directions and it is enabled, the individual ingress and egress groups or another group with both directions cannot be enabled. The individual ingress and egress groups can be enabled separately.  
This option is dimmed until you specify the mirror port and its mirrored ports.
8. Click **OK**.

## Enabling a Mirrored Group

If you did not enable the mirrored group when you created it, you can enable mirroring on the **Groups** table by selecting **Enable** for the mirrored group.

## Editing a Port Mirroring Group

You can edit all attributes of a mirrored group except the mirror port, which is dimmed.

### *To edit a port mirroring group:*

1. Navigate to **NETWORK | Switching > Port Mirroring**.
2. Click the **Edit** icon of the mirror port. The **Edit Mirror Group** dialog for the group displays.
3. Make the changes to any of the options.
  - ① **NOTE:** You can add or delete mirrored ports, but not the mirror port itself. If you delete a member of the group, no confirmation message is displayed.

4. If mirroring has been enabled for the group, **Enable** is selected. To disable port mirroring for these ports, deselect **Enable**.
  - ① **NOTE:** Only one ingress group and one egress group can be enabled at one time. If a group has both directions and it is enabled, the individual ingress and egress groups or another group with both directions cannot be enabled. The individual ingress and egress groups can be enabled separately.
5. Click **OK**.

## Deleting Port Mirroring Groups

You can delete members of a mirror group, a mirror group, multiple groups, or all groups.

## Removing Port Group Members

You can delete a member of a port group as described in [Editing a Port Mirroring Group](#) or you can delete it in the **Groups** table.

*To remove a port mirror group in the Groups table:*

1. Either:
  - Click the **Delete** icon for the group to be deleted. A confirmation message displays.
  - Select the checkbox for the group and then click **Ungroup**. A confirmation message displays.
2. Click **OK**.

## Removing Multiple Port Mirror Groups

*To remove multiple port mirror groups:*

1. In the **Groups** table, select the checkbox next to the port mirror groups you want to delete.
2. Click **Ungroup**. A confirmation dialog displays.
3. Click **OK**.

## Removing All Port Mirror Groups

1. To remove all port mirror groups:
2. In the **Groups** table, select the checkbox in the table heading.
3. Click **Ungroup**. A confirmation dialog displays.
4. Click **OK** in the confirmation dialog.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS and SonicOSX Switching Administration Guide for the NSa and NSsp Series

Updated - February 2021

Software Version - 7

232-005350-00 Rev B

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request

Attn: Jennifer Anderson

1033 McCarthy Blvd

Milpitas, CA 95035