Advanced Network Behavior Features

Chapter 4

In this Chapter...

Advanced Network Behavior Features

In addition to the Basic Managed Switch Features detailed in Chapter 3, the **Stride** SE2 series Managed switches include a full list of features that will be valuable to particular networks. This chapter describes the more advanced network features found in the **Stride** managed switches.

Traffic Priority (Priority Queuing QoS, Quality of Service)

Without enabling special handling, a network provides a “best effort” service to all applications. This means that there are no assurances regarding the Quality of Service (QoS) for any particular application because all packets are treated equally at each switch or router.

However, certain applications require deterministic response from the network to assure proper operation.

Consider a drilling machine in a plant that is controlled by a computer on a local network.

The depth of the machine’s drill is critical; if the hole is drilled too deep, the material will have to be thrown out. Under normal conditions, the drill process is running smoothly (controller and computer are communicating efficiently over the network) but when another user on the network accesses records from an online database, the large volume of traffic can interfere with timely communication with the drill. A delay in communications between the drill and controller causes the drill to go too far and the material has to be thrown away. To prevent this from happening, we need to provide a certain QoS for all drill controller communications so delay is avoided.

Traffic priority is shaped based on three principals:

1. Identify the type of traffic. This is encoded in the message headers built by the END DEVICE. The end device will encode according to either 802.1p or DSCP rules for creating that header.
2. Manage congestion - Queue traffic then forward it according to the scheduling algorithm as configured on the QoS configuration page.
3. Avoid congestion – apply rules for dropping traffic to alleviate congestion on the network as configured on the Port Rate configuration page.

In this section, we’ll discuss the QoS options for MANAGING network congestion.

Since the SE2 switches do not assign priority to traffic, we’ll simplify our discussion to consider traffic between switches. That is, traffic at a port that is connected to an end device will have a priority assigned by that end device and we’ll assume the network design has considered the rate requirements of that device.

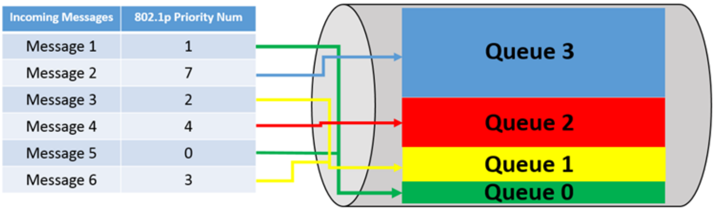
For traffic received at the switch (Ingress), the SE2 managed switches support three types of queue mapping modes to identify traffic priority: port, DSCP and 802.1p

- If the Ingress Type is **Port**, the rules for port ingress rate limiting as configured on the Port Rate configuration page govern traffic priority. Simply put, incoming traffic is accepted until the "bucket" is full, then is dropped. See the Port Rate configuration section in this manual for details.
- If the Ingress Type is **DSCP**, the priority and queue relationship can be configured according to the ToS/DSCP field in the traffic that is received at that port. The choice between DSCP and 802.1p depends on the end devices and how those devices construct the message headers. Configuration of the switch requires understanding of the requirements and behaviors of the end devices. The priority may be managed across the switch by configuring the 64 DSCP priorities as they map to the 4 queues (DSCP Priority table on the switch QoS configuration page).
- If the Ingress Type is **802.1p**, the priority and queue relationship can be configured and will apply to traffic that arrives at the switch tagged in the DSCP field. Untagged traffic will be assigned priority and queue according to 802.1p rules. The priority may be managed across the switch by configuring the 8 priorities as they map to the 4 queues (802.1p Priority table on the switch QoS configuration page).

For traffic that will be transmitted by the switch (Egress), the SE2 managed switches support two types of QoS queue scheduling: Weighted Round Robin (WRR) and Strict Priority (SP).

- If the Egress type is **SP**, high priority messages will be guaranteed preferential forwarding. This is especially useful when network traffic includes sensitive signals. Once a message is added into the high priority queue, the SP mechanism stops traffic from the lower priority queues and processes the data in the high priority queue. Only when the high priority queue is empty will the switch return to processing data in the lower priority

- If the Egress type is **WRR**, traffic will be scheduled according to the configured weight ratio; Queue 3 is allotted half the bandwidth, Queue 2 is allotted 1/4 the bandwidth, Queue 1 and Queue 0 split the remaining quarter. More bandwidth (traffic) is allocated to the queue with the largest ratio. See the graphic below.



Incoming Messages	802.1p Priority Num
Message 1	1
Message 2	7
Message 3	2
Message 4	4
Message 5	0
Message 6	3

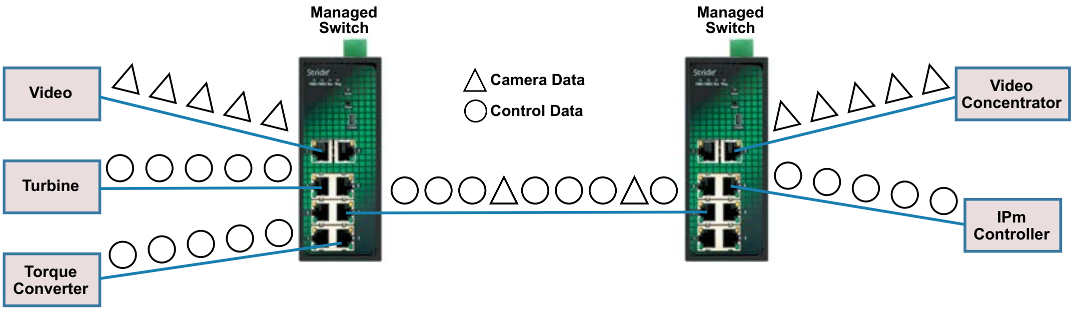
802.1p Example

The 802.1p configuration requires the end device to insert an Ethernet frame header containing the priority embedded in an 802.1p tag. It will contain a value of 0 (lowest) – 7 (highest). The 802.1p Priority configuration allows for translation of the 802.1p priority levels to the switch's queueing levels.

The DSCP configuration is similar in concept to the 802.1p configuration but uses a different Ethernet frame header with a priority level ranging from 0 – 63. The DSCP priority table allows for configuration of the 0 – 63 range of the DSCP header to the 0 – 3 Queue levels of the switch.

Let's consider an example network. There is a power plant that is controlled by a central control system. In addition, because of security concerns, cameras have been mounted and installed at each location of mechanical control. The mechanical control devices and video cameras at each site communicate via Ethernet to their own switch. (For reasons of simplicity and clarity, we will assume that only video and control data reside on the network).

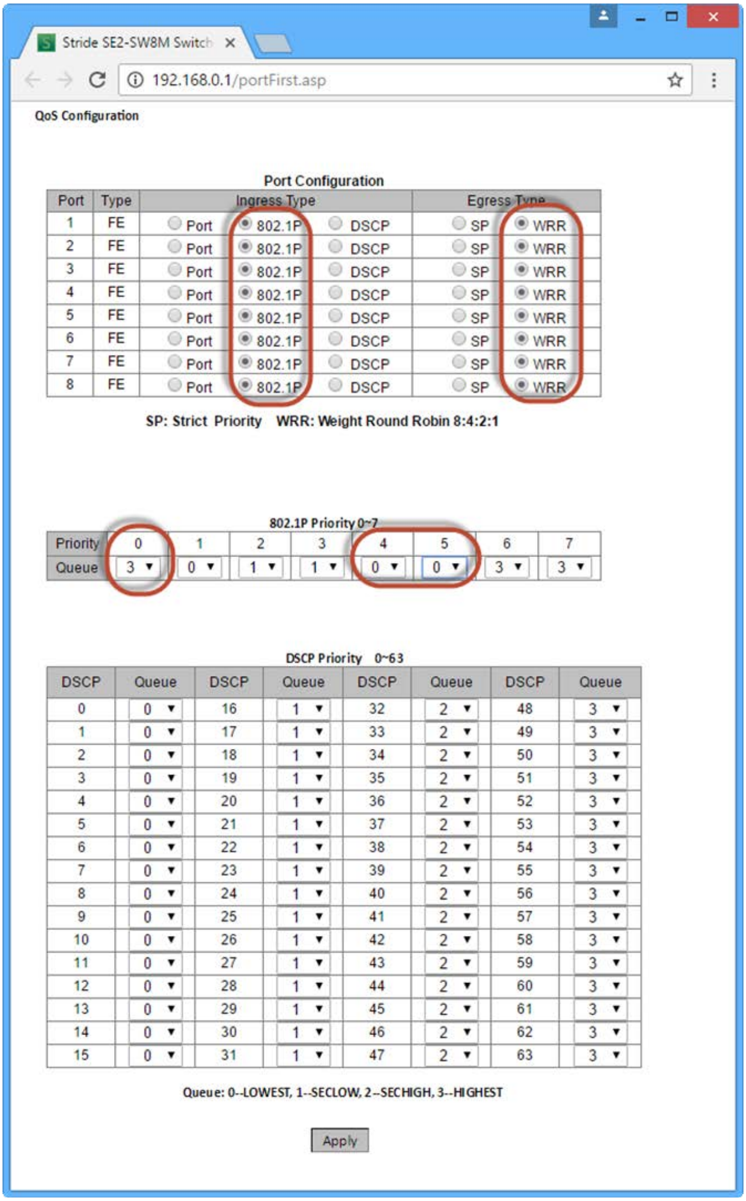
Should any of the mechanical control devices receive delayed control data from the central control system, the power plant can't generate the maximum energy that it is capable of. Customers will experience brown outs, and the plant will be looked upon with negative scrutiny. It is therefore very important that the video traffic created by the cameras not delay critical data.



Unless we configure the switch's priority queuing abilities, our switches perform to the best-effort network model. This means that the network will try to deliver all packets of information, but will not allocate switch resources according the timeliness of data for specific applications. Considering our control/video example, there is no guarantee that we can get the response time needed for control data if the video cameras are sending data at the same time. Our switches, though, are capable of prioritizing network traffic even if the devices (video cameras and control systems) do not support configuration of Quality of Service parameters

In our network, the control traffic is highest priority and the video traffic is low priority. In a more general network (commercial or enterprise rather than industrial control,) video traffic is usually given a high priority (4 or 5.) We'll adjust this by configuring the 802.1 priority-to-queue mapping. We'll map Priority 4 and 5 to the lowest priority queue, Queue 0.

For our example, the devices creating communication traffic do not have an assigned priority, that is, the control devices don't add a priority tag to the packets. So that traffic has Priority 0. By default in our switches, Priority 0 maps to the lowest priority queue. We will change this to map Priority 0 to the highest queue, Queue 3.



QoS Configuration

Port Configuration

Port	Type	Ingress Type			Egress Type	
1	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
2	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
3	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
4	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
5	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
6	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
7	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
8	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR

SP: Strict Priority WRR: Weight Round Robin 8:4:2:1

802.1P Priority 0~7

Priority	0	1	2	3	4	5	6	7
Queue	3 ▾	0 ▾	1 ▾	1 ▾	0 ▾	0 ▾	3 ▾	3 ▾

DSCP Priority 0~63

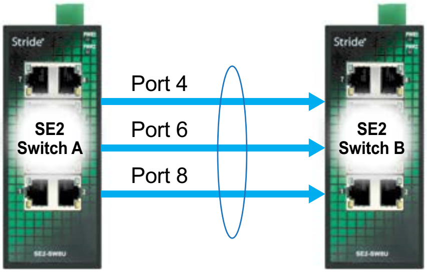
DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	0 ▾	16	1 ▾	32	2 ▾	48	3 ▾
1	0 ▾	17	1 ▾	33	2 ▾	49	3 ▾
2	0 ▾	18	1 ▾	34	2 ▾	50	3 ▾
3	0 ▾	19	1 ▾	35	2 ▾	51	3 ▾
4	0 ▾	20	1 ▾	36	2 ▾	52	3 ▾
5	0 ▾	21	1 ▾	37	2 ▾	53	3 ▾
6	0 ▾	22	1 ▾	38	2 ▾	54	3 ▾
7	0 ▾	23	1 ▾	39	2 ▾	55	3 ▾
8	0 ▾	24	1 ▾	40	2 ▾	56	3 ▾
9	0 ▾	25	1 ▾	41	2 ▾	57	3 ▾
10	0 ▾	26	1 ▾	42	2 ▾	58	3 ▾
11	0 ▾	27	1 ▾	43	2 ▾	59	3 ▾
12	0 ▾	28	1 ▾	44	2 ▾	60	3 ▾
13	0 ▾	29	1 ▾	45	2 ▾	61	3 ▾
14	0 ▾	30	1 ▾	46	2 ▾	62	3 ▾
15	0 ▾	31	1 ▾	47	2 ▾	63	3 ▾

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Port Trunk – Link Aggregation

The **Stride** SE2 series switches include a port trunk (link aggregation) feature that allows multiple ports on a switch to share traffic and provide instant fail over recovery in case one port fails.

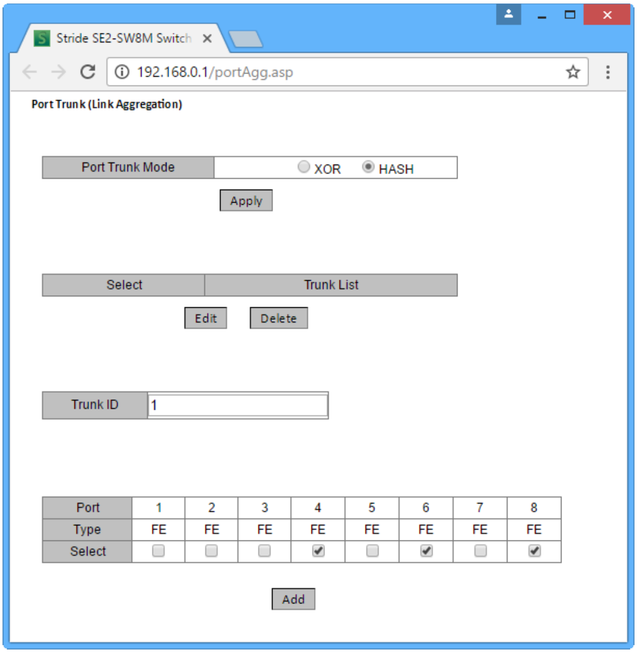
The total bandwidth of the Trunk Group is the combined bandwidth of the ports in the group.



When Switch A transmits to Switch B, Switch A will conduct a flow allocation algorithm to select one member port to transmit the messages. If the connection on one port in the group fails, the traffic borne by the port is reallocated to the other connected port(s) by the recalculated flow algorithm, XOR or HASH.

The allocation algorithms are not configurable. Typically, one would expect the XOR option to result in all traffic from a specific source (for example PLC1) to a specific destination (for example Remote IO 2) to always be allocated to the same port. In a network where two devices have significantly more traffic between them than other traffic on the network, the HASH option may provide more balanced traffic allocation. Neither method will result in a perfectly even distribution of traffic across the ports.

1. Port trunk and the following features are mutually exclusive. That is, to configure a port to participate in a Trunk Group, Disable the following features:
   - Port Monitoring
   - RSTP/STP
   - AD-Ring and AD-RP
   - DHCP Snooping Trust port
   - IGMP
   - GVRP
   - Port static multi-cast, Port static unicast
2. Gigabit ports may not be configured to participate in a Trunk Group.
3. A port may join only one Trunk Group.



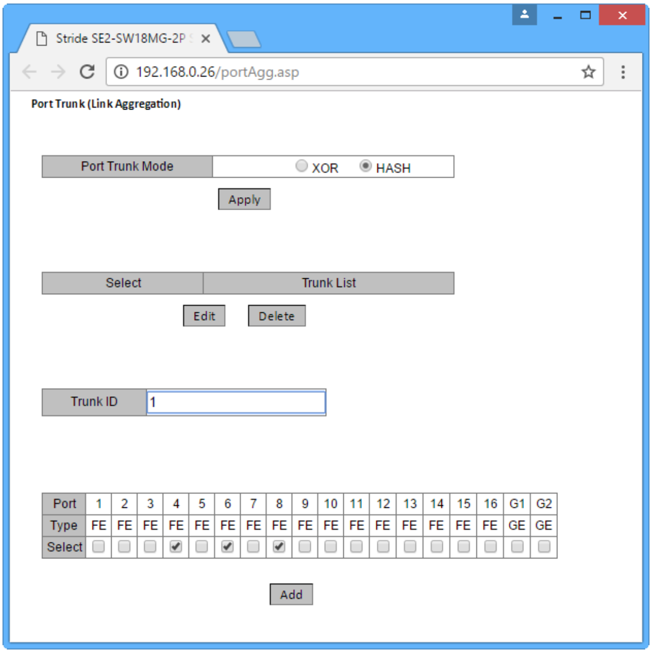
Port Trunk (Link Aggregation)

Port Trunk Mode	○ XOR ● HASH

Select	Trunk List

Trunk ID	1

Port	1	2	3	4	5	6	7	8
Type	FE	FE	FE	FE	FE	FE	FE	FE
Select	□	□	□	☑	□	☑	□	☑



Port Trunk (Link Aggregation)

Port Trunk Mode	○ XOR ● HASH

Select	Trunk List

Trunk ID	1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	G1	G2
Type	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	GE	GE
Select	□	□	□	☑	□	☑	□	☑	□	□	□	□	□	□	□	□	□	□

Port Rate

In addition to QoS, Port Rate limiting may be used to manage network traffic flow. Ingress ports limit the rate of selected message types and Egress ports limit the rate of all messages.

Rate limitation can be configured to apply to the following types of messages on Ingress ports:

Unknown Unicast Frame (UUF): messages whose destination MAC has not been learned and has not been statically added to the FDB.

Unknown Multicast Frame (UMF): messages whose destination MAC has not been learned by IGMP Snooping or GMRP and has not been added to the Static FDB Multicast table.

Broadcast Frame (BF): messages with the destination MAC FF: FF: FF: FF: FF: FF.

Multicast Frame (MF): messages whose destination MAC has been learned by IGMP or GMRP, or has been statically added to the Static FDB Multicast table.

Unicast Frame (UF): Messages whose destination MAC address has been learned or has been added to the FDB.

Imagine switch traffic as tokens that are added to a bucket in the switch. Tokens are added to the bucket at a certain rate and the bucket has a certain capacity. If the number of tokens exceeds the capacity of the bucket, the bucket will overflow and the mechanism will stop accumulating tokens.

Each token allows sending a certain number of bits. When a message is transmitted, a number of tokens equal to the length of the message are removed from the bucket. If there aren't enough tokens in the bucket, the message may be held until there are sufficient tokens or the message may be dropped.

Port rate configuration uses token buckets to control flow. If Port Rate is set for a port, the messages at this port will be processed by the token bucket method before forwarding. If there are sufficient tokens, the messages will be transmitted, or else they will be dropped.

AD-Ring

By default, RSTP is Enabled on all ports. When configuring a pair of ports to participate in an AD-Ring, RSTP must be Disabled on those ports.

Like RSTP, an AD-Ring increases network reliability by providing an alternate path for message flow in the event of a network segment failure. When a ring port detects a communications break, it quickly notifies the other switches in the ring. Messages are automatically rerouted through the alternate ring path within milliseconds.

RSTP/STP (Rapid Spanning Tree Protocol) is more flexible than a ring configuration, but recovery times for spanning trees may be in the hundreds of milliseconds. The AD-Ring protocol exchanges topological flexibility for recovery times in the tens of milliseconds.

There are two types of AD-Rings: port-based (AD-Port-Ring) and VLAN-based (AD-VLAN-Ring).

AD-Port-Ring: specifies a port to forward or block packets.

AD-VLAN-Ring: specifies a port to forward or block the packets of a specific VLAN. This allows multiple VLANs on a tangent port, that is, one port is part of different redundant rings based on different VLANs.

AD-Port-Ring and AD-VLAN-Ring cannot be used together.

Concepts

Master station: A ring has only one master station. The master station forwards AD-Ring packets and detects the current status of the ring.

Master port: On the master station, the first port whose link status changes to up is called the master port. It is in forwarding state.

Slave port: On the master station, the port whose link status changes to up if a failure is detected is called the slave port. When the ring is closed, the slave port is in blocking state. When a ring is open due to a link or port failure, the status of the slave port changes to forwarding.

Slave station: A ring can include multiple slave stations. Slave stations listen to and forward AD-Ring packets and report fault information to the master station.

Backup port: The port for communication between AD-Rings is called a backup port.

Master backup port: When a ring has two backup ports, the backup port with the larger MAC address is the master backup port. It is in forwarding state.

Slave backup port: When a ring has two backup ports, the backup port with the smaller MAC address is the Slave backup port. It is in blocking state.

Forwarding state: If a port is in forwarding state, the port can both receive and send data.

Blocking state: If a port is in blocking state, it can only receive data, but not send data.

Implementation of AD-Ring

The master port on the master station periodically forwards AD-Ring packets to detect ring status. If the slave port of the master station receives the packets, the ring is closed; otherwise, the ring is open.

When a ring is closed, the master port of the master station is in forwarding state, the slave port in blocking state, and all ring ports of slave stations are in forwarding state.

A ring may be open in the following cases:

- The master port of the master station fails. The statuses of the slave port on the master station and all ring ports of slave stations change to forwarding.
- The slave port of the master station fails. The statuses of the master port on the master station and all ring ports of slave stations change to forwarding.
- Another port or link fails. The statuses of the two ports of the master station and all up ports of slave stations change to forwarding.

AD-Ring configurations must meet the following conditions:

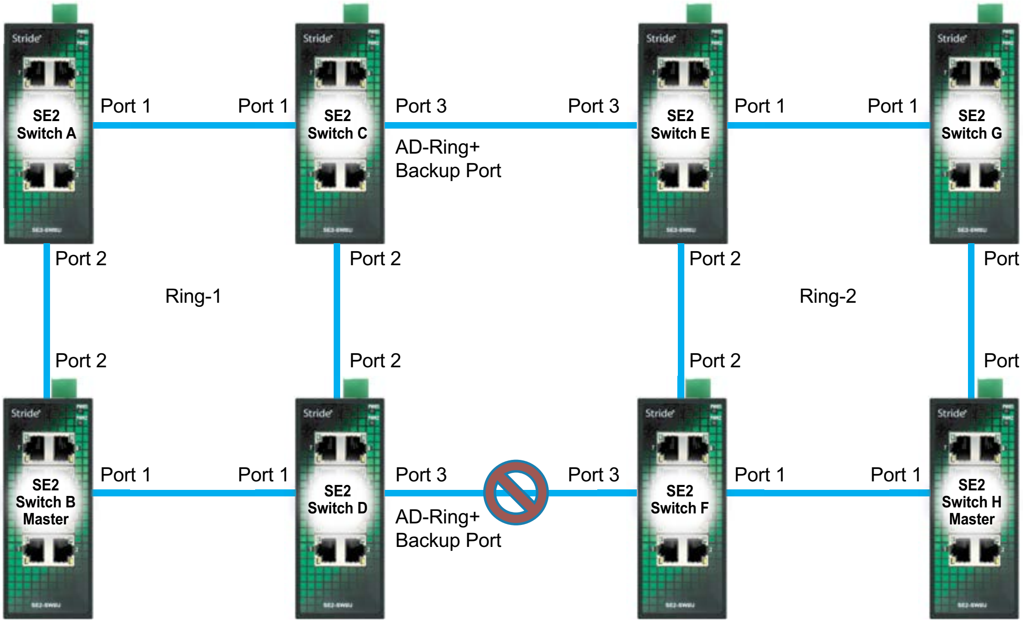
- All switches in the same ring must have the same Domain ID.
- Each ring can have only one master station and multiple slave stations
- Two ports must be configured on each switch for a ring
- For two connected rings, backup ports can be configured only in one ring
- A maximum of two backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring

CAUTION: Port trunk and ring are mutually exclusive. The ports added to a trunk group cannot be configured as a ring port, and a ring port cannot be added to a trunk group.

Implementation of AD-Ring+

AD-Ring+ can provide backup for two AD-rings, as shown below. One backup port is configured on Switch C and on Switch D. Which port performs as the master backup port depends on the MAC addresses of the two ports. If the master backup port or its link fails, the slave backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

See the example at the end of this section for details on configuring this example network.



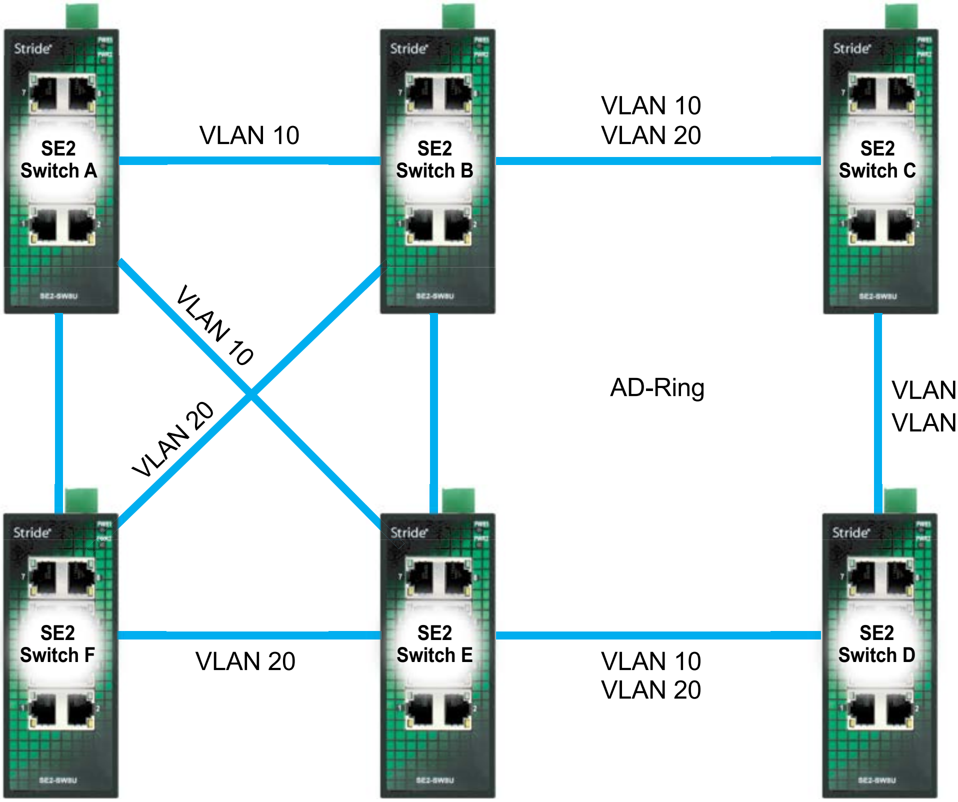
Implementation of AD-VLAN-Ring

AD-VLAN-Ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms an AD-VLAN-Ring. Different AD-VLAN-Rings can have different master stations. As shown below, two AD-VLAN-Rings are configured.

Ring links of AD-VLAN-Ring10: AB-BC-CD-DE-EA.

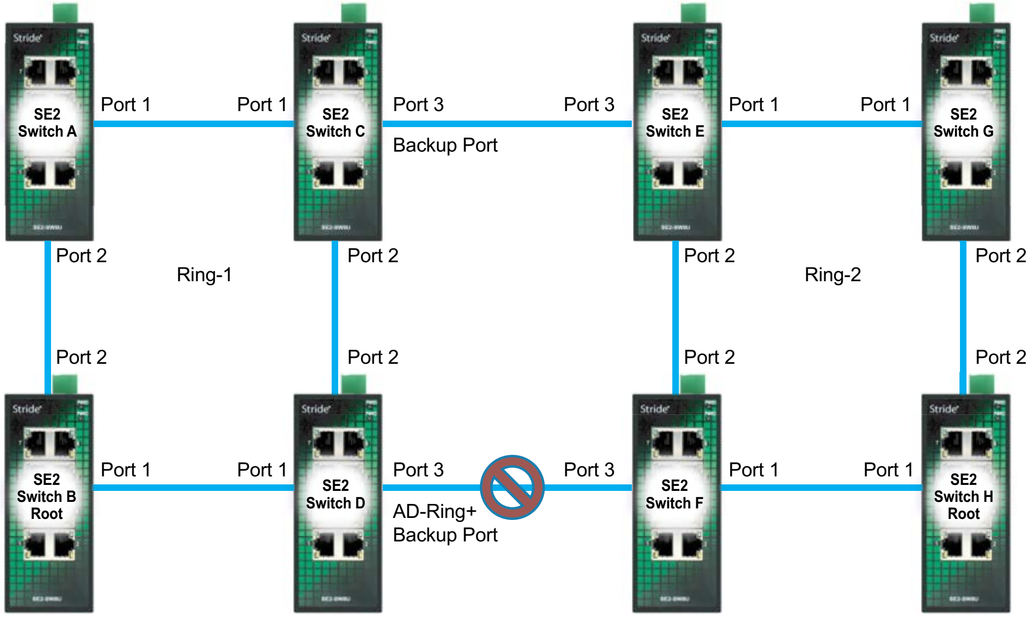
Ring links of AD-VLAN-Ring20: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLAN.

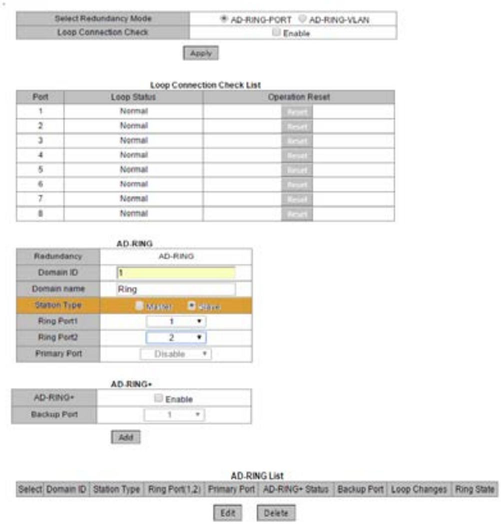


AD-Ring Example

As shown below, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form Ring 2; CE and DF are the backup links of Ring 1 and Ring 2.



Configuration on Switch A:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

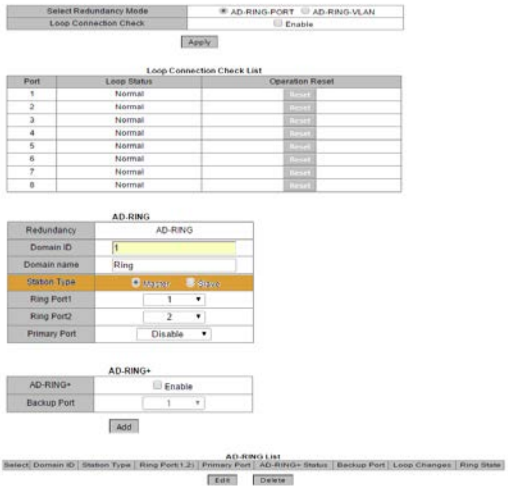
AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switch B:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	● Master ○ Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

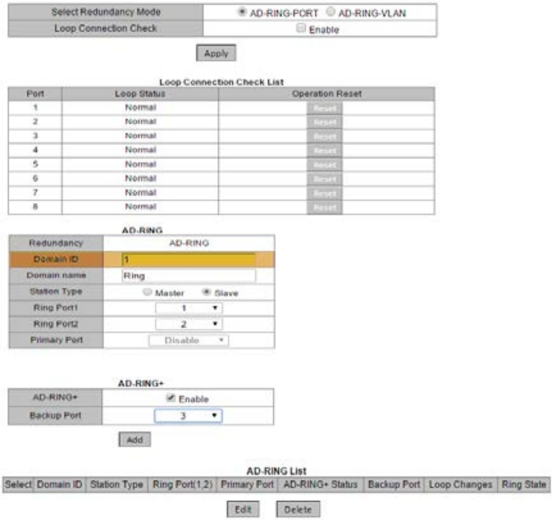
AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switches C and D:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1 ▾
Ring Port2	2 ▾
Primary Port	Disable ▾

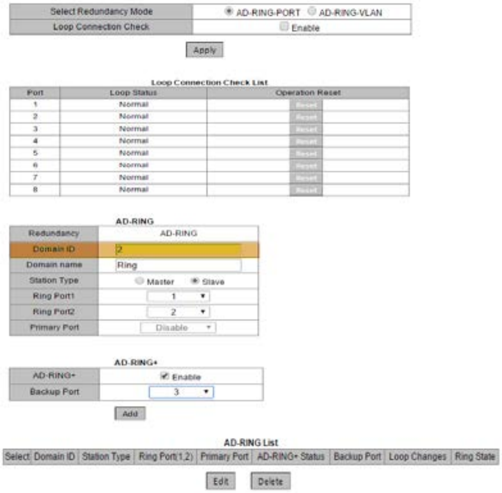
AD-RING+

AD-RING+	☑ Enable
Backup Port	3 ▾

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switches E and F:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1 ▾
Ring Port2	2 ▾
Primary Port	Disable ▾

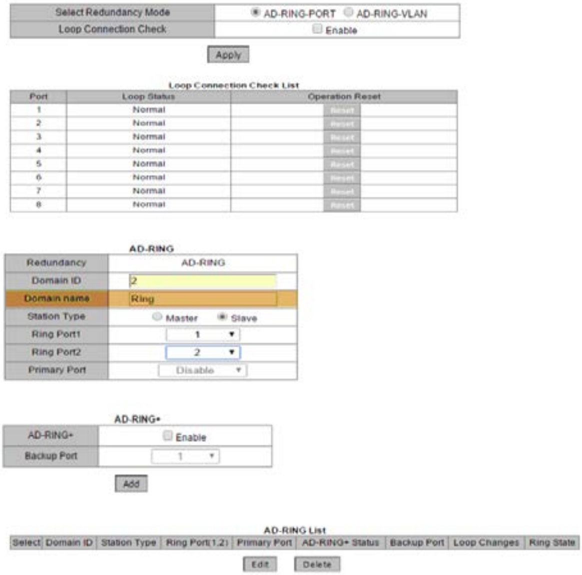
AD-RING+

AD-RING+	☑ Enable
Backup Port	3 ▾

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switches G:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

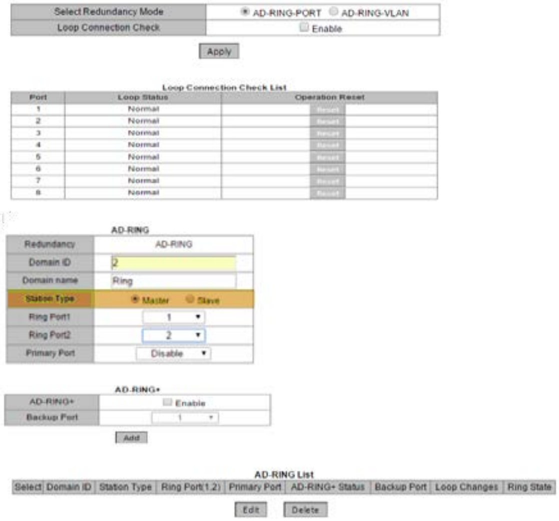
AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switches H:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	● Master ○ Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

AD-RP

AD-RP is an IEC62439-6 compliant redundant ring protocol. It adopts a distributed ring network protection solution for **Stride** SE2 series switches. When a link fails, the network can recover within 20ms to guarantee stable and reliable communication.

One switch may participate in multiple AD-RP rings.

***NOTE:** By default, RSTP is Enabled on all ports. When configuring a pair of ports to participate in AD-RP, RSTP must be Disabled on those ports.*

Concept

INIT: the initial state of the switch

Root: there is one and only one root in the ring network. The root is elected by switches in the network and changes with network topology. The root periodically sends out an Announce message and other devices forward this message to guarantee topology stability.

B-Root: The switch in which a ring port is Link-down, or a ring port deteriorates (which means the number of CRC messages exceeds the threshold)

Normal: Except Root and B-Root, the rest are Normal switches in a normal communication ring network

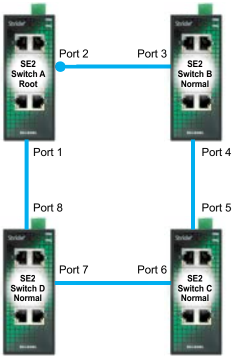
Backup port: the communication ports between AD-RP rings. Two or more backup ports can be configured. All backup ports must be in the same AD-RP ring. The backup port that links up first is the master backup port and is in Forward state, and other backup ports are slave backup ports and are in Block State.

Implementation

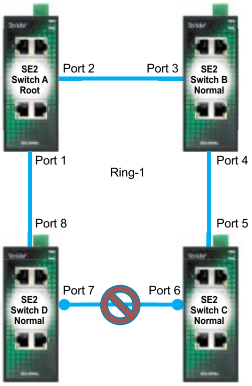
AD-RP protocol determines switch roles by forwarding Announce messages to guarantee a loop-free redundant network.

AD-RP configuration must meet the following conditions:

- All switches in a ring must have a same domain ID
- There is one and only one Root in a ring, but there may be multiple B-Roots or Normals.
- There are only two ring ports in each switch in a ring
- For two connected rings, backup ports can only be set in one ring
- A ring allows multiple backup ports
- Each switch in a ring can only set one backup port



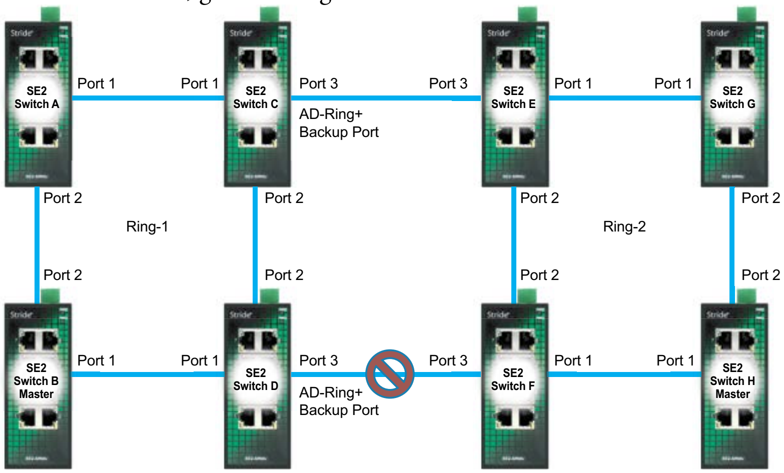
1. In the initial state, all switch are in INIT state
2. In the ring network, switches compare the Announce message forwarded between them, and then elect Switch A to be Root due to its optimum configuration. The ring port 1 in Root that links up first is the Forwarding port, while the ring port 2 is blocked. Other switches are B-Root or Normal. The two ring ports in B-Root/Normal are both in Forward state.



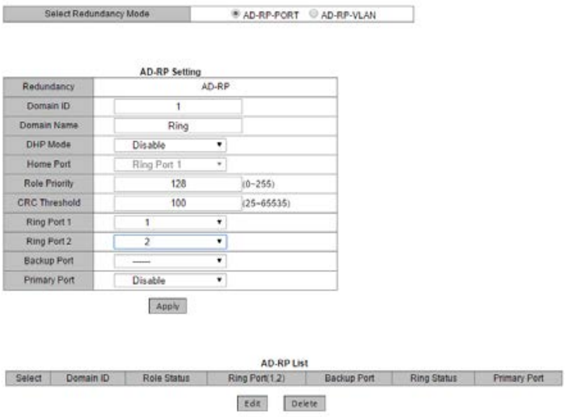
3. If the link between switches C and D fails, for example, immediately switch A will change from Root to Normal AND either switch C or D will be elected the new Root. Ports 6 and 7 will be blocked. If D is root, then C will be B-Root.

CAUTION: Link state changes affect the status of all ring ports.

AD-RP protocol can provide backup between two AD-RP rings; each switch can have a Backup Port configured. The master backup port is the forwarding port, and the other backup ports are blocked. If the master backup port/link fails, the system will select a slave backup port to forward data, guaranteeing the normal communication between redundant rings.



Switch A and Switch B configuration:



Select Redundancy Mode	● AD-RP-PORT ○ AD-RP-VLAN

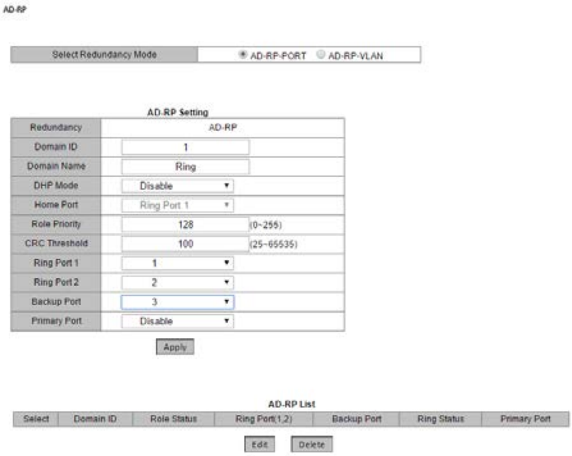
AD-RP Setting

Redundancy	AD-RP
Domain ID	1
Domain Name	Ring
DHP Mode	Disable
Home Port	Ring Port 1
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	1
Ring Port 2	2
Backup Port	——
Primary Port	Disable

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

Switch C and Switch D configuration:



AD-RP

Select Redundancy Mode	● AD-RP-PORT ○ AD-RP-VLAN

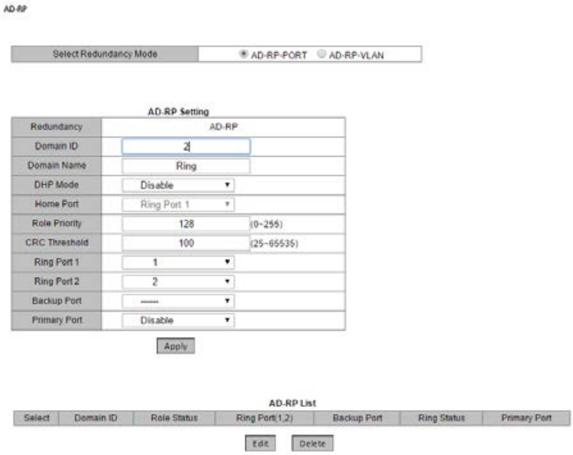
AD-RP Setting

Redundancy	AD-RP	
Domain ID	1	
Domain Name	Ring	
DHP Mode	Disable	
Home Port	Ring Port 1	
Role Priority	128	(0~255)
CRC Threshold	100	(25~65535)
Ring Port 1	1	
Ring Port 2	2	
Backup Port	3	
Primary Port	Disable	

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

Switch E, F, G, H configuration:



AD-RP

Select Redundancy Mode	● AD-RP-PORT ○ AD-RP-VLAN

AD-RP Setting

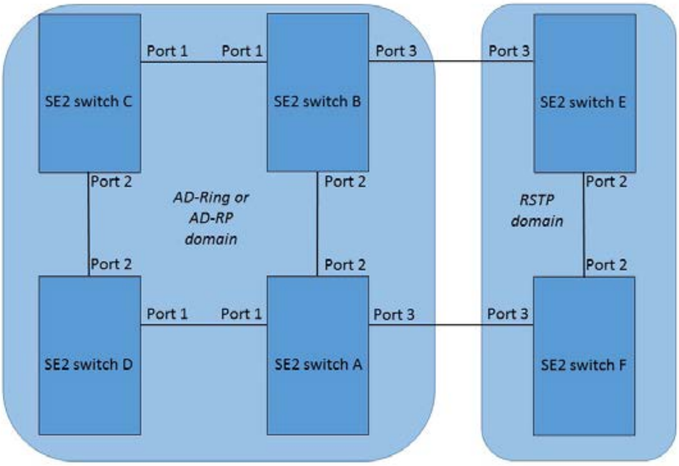
Redundancy	AD-RP	
Domain ID	2	
Domain Name	Ring	
DHP Mode	Disable	
Home Port	Ring Port 1	
Role Priority	128	(0~255)
CRC Threshold	100	(25~65535)
Ring Port 1	1	
Ring Port 2	2	
Backup Port	------	
Primary Port	Disable	

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

RSTP/STP Transparent Transmission

AD-Ring and AD-RP are proprietary redundancy solutions and as such can't coexist with RSTP/STP on a network. But to accommodate traffic to/from an AD-Ring or AD-RP, the **Stride** SE2 series switches provide an RSTP/STP Transparent Transmission feature that will transmit RSTP/STP BPDUs across the ports participating in AD-Ring or AD-RP.



Switches A, B, C, and D form an AD-Ring. When RSTP/STP Transparent Transmission is enabled on Switch A and B ports, Switches E and F can receive RSTP BPDUs from each other, detect loops, and calculate spanning trees.

Link Check

The Link Check feature verifies that ports participating in a redundancy protocol (RSTP/STP, AD-Ring or AD-RP) transmit data normally. Note that only ports configured to participate in a redundancy protocol may enable Link Check.

When Link Check is enabled on a port, the status may be monitored using Modbus TCP, EtherNet/IP or SNMP.

Status:

Normal Link: Link Check is enabled and the port is transmitting/receiving data properly.

Receive Fault: Link Check is enabled and the port is NOT transmitting/receiving data properly.

Disable: Link Check is not enabled on this port.

Virtual Cable Check

The Virtual Cable Tester uses Time Domain Reflectometry to detect twisted pair status. It transmits a pulse signal along the cable and detects the reflection of the pulse signal. If a failure has occurred in the cable, the pulse will be reflected back to the switch port and the user interface will display the distance to the failure in the Distance to Fault column, shown in meters.

The following types of cable faults can be detected and displayed in the status column:

Short: short circuit, two or more wires are shorted.

Open: open circuit, there may be broken wires in the cable.

Imped: impedance mismatch. The characteristic impedance of Cat5e cable is 100 ohms. The impedance of the terminators at both ends of the cable must be 100 ohms to avoid wave reflection and data errors.

Port Security

Port Security is a MAC-address-based security mechanism for network access control. This mechanism compares the source MAC address of received messages to the list of allowable MAC addresses. A message with a source MAC addresses that isn't included in the Allowable MAC address table is dropped.

The switch supports 32 allowable MAC addresses on each port.

Port CRC Protect

The switch can be configured to protect itself from expending effort tending traffic on a port that's experiencing problems. CRC errors are symptoms of a problem with traffic. This may result from a problem with the integrity of the physical condition (failing cable or connector).

- a malfunctioning Network Interface Controller
- software problems on a connected device
- port configured for Half Duplex rather than Full Duplex communications
- other network problems

Loop Detect

If a port is **not** configured to participate in a redundancy protocol, loop detect protects the network from failing due to unintended loops. When loop detect is enabled on a port, the switch will disable that port if traffic indicating a loop in the network is detected. When auto recover is enabled, the switch will re-enable the port and check for loops after a pause.

MAC Address Forwarding Database

Ordinarily the switch will automatically learn the MAC addresses of connected devices by examining the messages it receives. These automatically learned addresses will be deleted from the MAC table if no messages have been received from or transmitted to them for a duration defined by the MAC Aging Time. The MAC Aging Time may be configured between 15 and 3600 seconds, but it must be a multiple of 15.

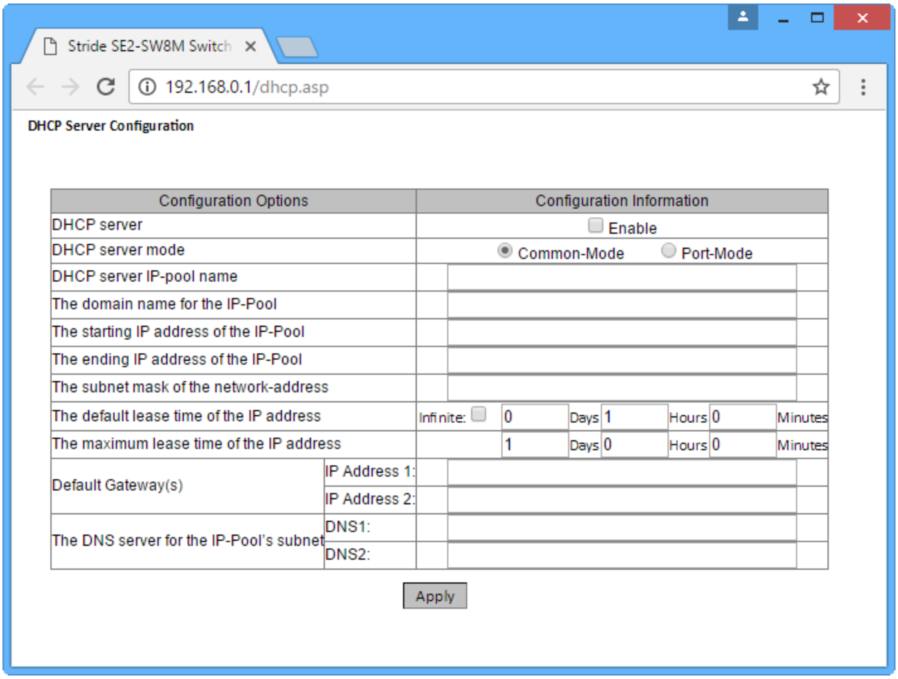
DHCP Server

As networks grew in scale and complexity, DHCP (Dynamic Host Configuration Protocol) was developed as a mechanism to automatically assign IP addresses and subnet masks to devices as they connect to the network.

DHCP employs a client-server communication model. The client sends a configuration request to the server, and then the server replies with configuration parameters such as IP address and subnet mask.

A **Stride** SE2 series switch may be configured to be the DHCP server to a network.

CAUTION: Remember that in DHCP, messages are transmitted as broadcasts, so the DHCP client and the Stride SE2 series switch acting as the DHCP server must be in the same network segment.



DHCP Server Configuration

Configuration Options		Configuration Information
DHCP server		☐ Enable
DHCP server mode		● Common-Mode ○ Port-Mode
DHCP server IP-pool name		
The domain name for the IP-Pool		
The starting IP address of the IP-Pool		
The ending IP address of the IP-Pool		
The subnet mask of the network-address		
The default lease time of the IP address		Infinite: ☐ 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
Default Gateway(s)	IP Address 1:	
	IP Address 2:	
The DNS server for the IP-Pool's subnet	DNS1:	
	DNS2:	

DHCP supports two types of IP address allocation mechanisms, Port-Mode and Common -Mode.

Port Mode: the network administrator statically binds a fixed IP address to a port. This is helpful for clients such as a router port configured as a Gateway.

Common Mode: DHCP server dynamically allocates an IP address to a client. The IP address can be allocated to a client permanently or with a limited lease period. When the lease expires, the client needs to request a new IP address.

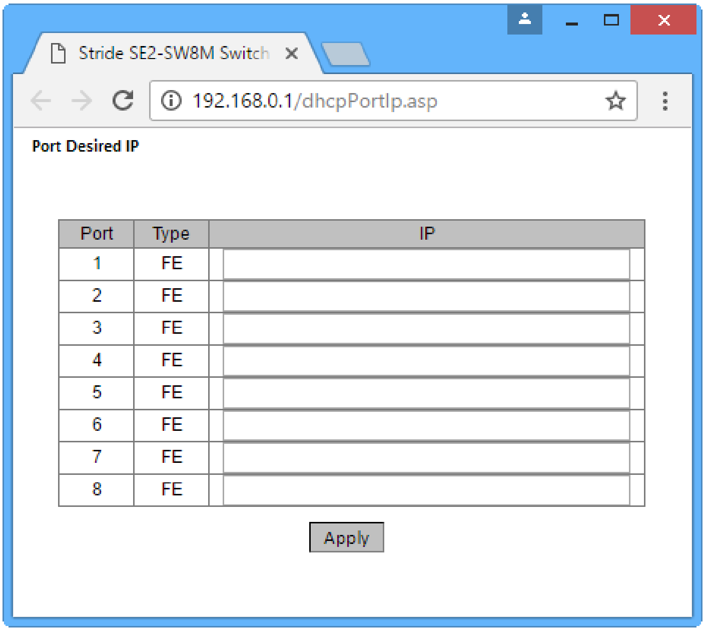
The DHCP server selects an IP address from an address pool and allocates it together with other parameters to the client. The IP address allocation sequence is as follows:

1. The IP address statically bound to the client MAC address or the port ID connecting to the server.
2. The IP address that is recorded in the DHCP server that was previously allocated to the client.
3. The IP address that is specified in the request message sent from the client.
4. The first allocable IP address found in the address pool.

Port Desired IP Configuration

When DHCP Server is Enabled, and Port-Mode is selected as the Server Mode, the Port Desired IP table setting statically assigns an IP address to a port. When a port receives a request message from a client, the IP address bound to the port will be allocated to the client. This IP allocation mode has the highest priority and the lease period is 1000 days 23 hours and 59 minutes.

Caution: The IP address assigned to a port and the DHCP server must be in same segment.



Port Desired IP

Port	Type	IP
1	FE	
2	FE	
3	FE	
4	FE	
5	FE	
6	FE	
7	FE	
8	FE	

If a subnet mask and Default Gateway(s) are entered in the DHCP Server Configuration table, these values will be assigned to devices requesting host configuration from the switch.

The DNS-server for the IP-Pool's subnet

When an address is provided as a name, the name needs to be resolved to an IP address. A DNS server will accomplish this. DHCP address pool can configure max two DNS addresses.

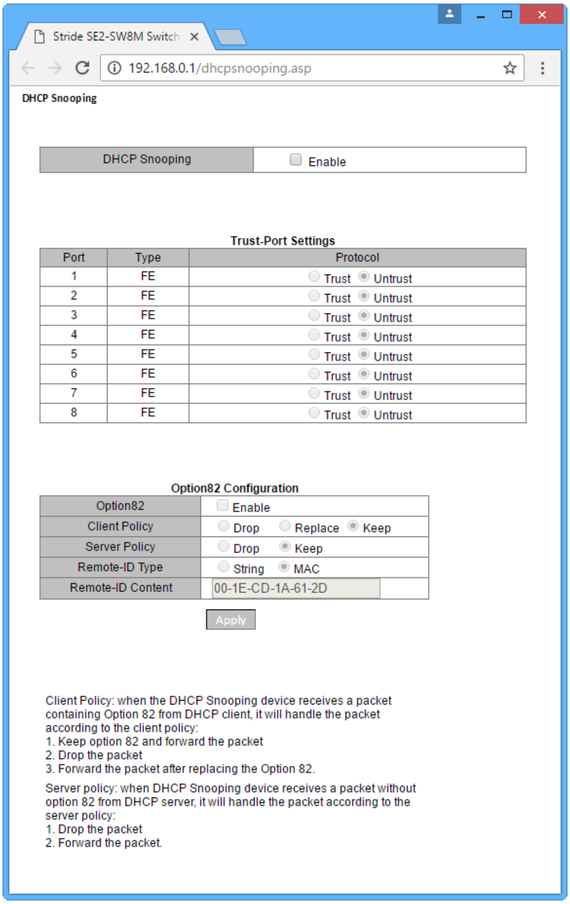
DHCP Snooping

DHCP snooping is a feature to prevent unexpected DHCP servers from providing IP addresses to DHCP clients. Unacceptable DHCP messages will be dropped at Untrusted ports.

Trusted port: a port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: any port that is not connected to a known DHCP server. Untrusted ports will not forward DHCP requests and responses.

Note 1: *A switch configured to perform DHCP snooping may not be configured as a DHCP server.*
Note 2: *A switch configured to perform DHCP snooping may not be configured to obtain its IP address by DHCP*
Note 3: *A switch configured to perform DHCP snooping may not be configured to participate in a Trunk Group.*



DHCP Snooping

DHCP Snooping	□ Enable

Trust-Port Settings

Port	Type	Protocol
1	FE	○ Trust ● Untrust
2	FE	○ Trust ● Untrust
3	FE	○ Trust ● Untrust
4	FE	○ Trust ● Untrust
5	FE	○ Trust ● Untrust
6	FE	○ Trust ● Untrust
7	FE	○ Trust ● Untrust
8	FE	○ Trust ● Untrust

Option82 Configuration

Option82	□ Enable
Client Policy	○ Drop ○ Replace ● Keep
Server Policy	○ Drop ● Keep
Remote-ID Type	○ String ● MAC
Remote-ID Content	00-1E-CD-1A-61-2D

Apply

Client Policy: when the DHCP Snooping device receives a packet containing Option 82 from DHCP client, it will handle the packet according to the client policy:
1. Keep option 82 and forward the packet
2. Drop the packet
3. Forward the packet after replacing the Option 82.

Server policy: when DHCP Snooping device receives a packet without option 82 from DHCP server, it will handle the packet according to the server policy:
1. Drop the packet
2. Forward the packet.

Option 82 Configuration

Option 82 (Relay Agent Information Entry) allows DHCP traffic from switches that are not directly connected to a DHCP server to successfully negotiate network settings across a more complicated network while maintaining the security that DHCP snooping provides.

Client Policy: when the DHCP Snooping device receives a packet containing Option 82 from DHCP client, it will handle the packet according to the client policy:

1. Keep option 82 and forward the packet
2. Drop the packet
3. Forward the packet after replacing the Option 82.

Server policy: when DHCP Snooping device receives a packet without option 82 from DHCP server, it will handle the packet according to the server policy:

1. Drop the packet
2. Keep the packet and forward it.

The Option 82 field on **Stride** SE2 series switches includes two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

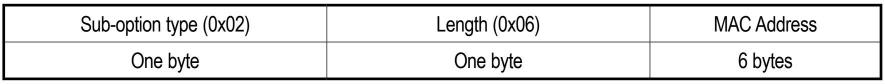
Sub-option 1 contains the VLAN ID and number of the port that receives the request message from the DHCP client. The format of the sub-option 1 field within the message is:

Sub-option type (0x01)	Length (0x04)	VLAN ID	Port Number
One byte	One byte	Two bytes	Two bytes

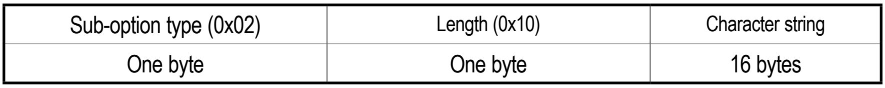
VLAN ID: On a DHCP Snooping device, the VLAN ID of the port that receives the request message from the DHCP client

Port number: On a DHCP Snooping device, the number of the port that receives the request message from the DHCP client

The content of Sub-option 2 includes the MAC address of the DHCP Snooping device that receives the request message from the DHCP client, or the character string configured by users, as shown in below



Sub-option type (0x02)	Length (0x06)	MAC Address
One byte	One byte	6 bytes



Sub-option type (0x02)	Length (0x10)	Character string
One byte	One byte	16 bytes

Sub-option type: 2

Length: the number of bytes that Sub-option 2 content occupies. The MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the MAC address of the DHCP Snooping device that receives the request message from the DHCP client.

Character string: 1-16 characters. This character string is configured. on the DHCP Snooping page.