61200500L1-29.1A
May 2004

ADTRAN

Configuration Guide

Spanning Tree Protocol

Eliminating Looping in Redundant-Topology Networks

This Configuration Guide explains the concepts behind configuring your ADTRAN OS product for Spanning Tree Protocol support. For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* on your *ADTRAN OS System Documentation* CD.

This guide consists of the following sections:

- *Understanding the Purpose of Spanning Tree Protocol* on page 2
- *How Does STP Work?* on page 4
- *Spanning Tree Protocol Variations* on page 5
- *Configuring Your NetVanta AOS Product* on page 6

Understanding the Purpose of Spanning Tree Protocol

As Ethernet networks become more and more business-critical, the need for higher levels of reliability and sophistication increases dramatically. Building more dependable networks requires a reduced reliance on individual pieces of equipment and/or links, and an increased dependency on protocols intelligent enough to automatically detect and recover from inevitable network failures.

Simply adding equipment to serve as a backup in case of hardware or software failure is not a complete solution. For example, a redundant switch network may provide a means of backing up the network in the event that one switch fails; however, without the proper protocols in place, a network can easily be overwhelmed by broadcast storms and redundant looping.

Spanning Tree Protocol (STP) was created to solve this problem. By identifying and blocking redundant paths, STP prevents loops from forming in a switch network. The protocol is also intelligent enough to restore an alternate path when a primary link goes down, eliminating downtime.

The following examples illustrate STP capabilities:

Example 1: Broadcasting Packets in a Non-Redundant Topology

In Figure 1, when **A1** initially sends data to **C2**, **Switch A** is not yet aware of the location of **C2**. To find the location, **Switch A** broadcasts the packet out all other active (non-receiving) ports. **Switch B** and **Switch C** receive the packet and continue the broadcast in search of **C2**. When **C2** receives the packet, it responds back to **A1** and the switches in between learn the locations of **A1** and **C2**.

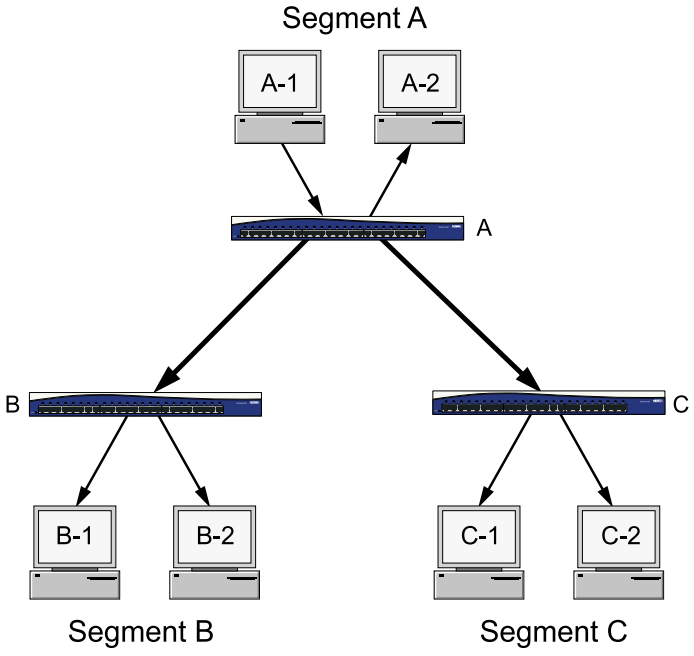

Figure 1. Non-Redundant Topology

Example 2: Broadcasting Packets in a Redundant Topology

In Figure 2, the looping problem becomes an issue when a direct connection is made between **Switch B** and **Switch C**. If the same initial transfer of data between **A1** and **C2** takes place, the search for **C2** begins the same. However, now when **Switch B** and **Switch C** forward the broadcast out all (non-receiving) ports, they create redundant data transmissions that last indefinitely, as the switches inadvertently retransmit the broadcast to each other over and over again. Spanning Tree Protocol is used by the switches to prevent this never-ending broadcast loop (i.e., broadcast storm).

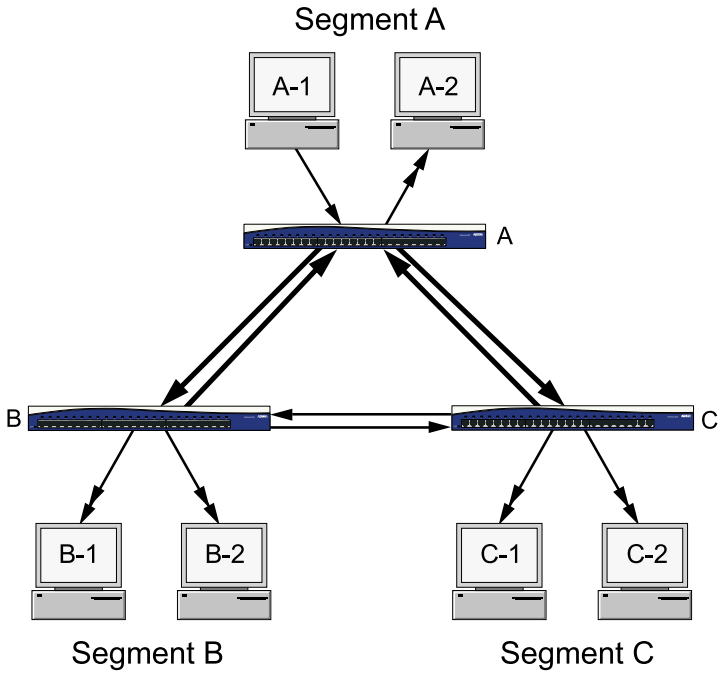

Figure 2. Redundant Topology

How Does STP Work?

All of the Spanning Tree Protocol implementations are based on the 802.1D IEEE algorithm. By exchanging messages with other switches to detect loops, and then removing the loops by shutting down selected bridge interfaces, this algorithm guarantees that there is *one and only one* active path between two network devices.

Simply stated, the IEEE 802.1D Spanning Tree Protocol algorithm does the following:

- Eliminates loops in a redundant-link network by selectively disabling links.
- Monitors for failure of active links and reactivates redundant links in order to restore the network to full connectivity (while preserving the loop-free topology).

The three basic steps in the execution of the STP algorithm are as follows:

1. **Identify Root Bridge.** A root bridge is a switch that has all ports actively forwarding information. A root bridge is typically chosen automatically, based on bridge priority. The root bridge serves as the center of the network and should be placed near the focal point of all network traffic (i.e., near the servers).

All switches with factory default settings intact will have the same bridge priority. If the setting is not changed on any of the switches, the root bridge will be the switch with the lowest MAC address. You can adjust this setting using the ***(config)#spanning-tree priority*** *command. If you are predetermining the root bridge, choose a switch that is the most centralized in the network. See the section Configuring Your NetVanta AOS Product on page 6 for more information.*

2. **Identify Root Port.** Every bridge which is not the root bridge must determine which of its ports is closest to the root bridge. This port is designated as the root port.
3. **Identify Designated Ports.** Every LAN segment must designate a port from among all the ports on all the bridges connected to that segment. Traffic from that segment will head towards the root bridge through the designated port.

Once the root bridge, root ports, and designated ports are all identified, all other ports are blocked. In the event that a primary link fails, ports will be reactivated as needed to restore network connectivity.

Spanning Tree Protocol Variations

Although Spanning Tree functions on any given device are typically invisible to VLAN users or members of the subnet, the protocol's presence or absence will always have a significant effect on the packet switching and overall switch performance. This is because the protocol is responsible for selecting the links and switches used by user traffic as the traffic travels on a subnet or VLAN. Therefore, it is important to clearly understand whether each Spanning Tree setting can coexist and operate with other vendor's products deployed in the same network.

In a typical networking environment, each switch could encounter and must be compatible with any of the multiple industry-defined Spanning Tree Protocol varieties, as well as proprietary ones. The following list identifies a number of Spanning Tree variants as defined by IEEE standards and leading-brand proprietary implementations.

- Common Spanning Tree (CST) assumes one Spanning Tree instance for the entire bridged network, regardless of the number of VLANs. This implementation reduces CPU load since only one Spanning Tree instance is maintained for the entire network. This implementation is typically used when only one Layer 2 topology is needed in the network.
- MISTP (802.1S) is an IEEE standard that allows several VLANs to be mapped to a reduced number of Spanning Tree instances. This is possible since most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer 2 topology.
- Per-VLAN Spanning Tree (PVST) maintains a Spanning Tree instance for each VLAN configured in the network. It uses ISL Trunking and allows a VLAN trunk to forward some VLANs while blocking for others. Since PVST treats each VLAN as a separate network, it can load balance traffic (at Layer 2) by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop.
- Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster Spanning Tree convergence after a topology change.
- Per-VLAN Spanning Tree Plus (PVST+) provides the same functionality as PVST using 802.1Q trunking technology rather than ISL. PVST+ is a proprietary enhancement to the 802.1Q specification.

Configuring Your NetVanta AOS Product

For most setups, the default settings for STP are sufficient. However, the following examples provide information on situations when you may wish to adjust your STP configuration.

Designating Root Bridge Using Switch Priority Setting

As discussed previously, a root bridge is a switch that has all ports actively forwarding information. If you wish to manually determine which unit will be the root bridge switch (instead of allowing STP to determine it automatically), set the switch's **spanning-tree priority** to **0**. This prevents any other switch from becoming the root bridge.

Table 1. Step-by-Step Configuration: Designating a Root Bridge

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	#**configure terminal**
3	Set priority to 0.	(config)#**spanning-tree priority 0**

Filtering BPDU Messages During Troubleshooting

During network troubleshooting, it is sometimes useful to turn off BPDU (bridge protocol data unit) messages on a port. This is helpful when analyzing network traffic (other than BPDUs) by reducing the amount of data captured. You can do this globally (as shown in Table 2) or on a per-interface basis (as shown in Table 3).

Table 2. Step-by-Step Configuration: Turning BPDU Messages Off (Global Level)

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	#**configure terminal**
3	Disable BPDU messages for all interfaces.	(config)#**spanning-tree edgeport bpdufilter default**

Table 3. Step-by-Step Configuration: Turning BPDU Messages Off (Interface Level)

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	#**configure terminal**
3	Access configuration parameters for the Ethernet port.	(config)#**interface eth 0/1**
4	Disable BPDU messages on the Ethernet port.	(config-eth 0/1)#**spanning-tree edgeport bpdufilter**

Configuring the Unit to Forward Traffic Immediately

If STP is not of value in your network setup, you can configure your AOS device to be an edgeport device by default. When connecting the device directly to a computer, this configuration allows you to avoid the delay of waiting for STP to enable the port. You can issue this command globally (as shown in Table 4) or on a per-interface basis (as shown in Table 5).

Table 4. Step-by-Step Configuration: Configuring Unit as Edgeport

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	#**configure terminal**
3	Configure unit to be an edgeport by default.	(config)#**spanning-tree edgeport default**

Table 5. Step-by-Step Configuration: Configuring Interface as Edgeport

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	#**configure terminal**
3	Access configuration parameters for the Ethernet port.	(config)#**interface eth 0/1**
4	Configure the Ethernet port to be an edgeport by default.	(config-eth 0/1)#**spanning-tree edgeport**

