

Bridging Wireless Bandwidth

Document ID: 71478

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Equal-Cost Load Balancing

Routing Protocols

Switching Paths

Fast Switching vs. CEF Switching

Other Design Considerations

- Quality of Service

- Full Duplex

- Dual Unidirectional Links

- EtherChannel

The Test Design

- Routers

- Switches

- Bridges

Tech Tips

Related Information

Introduction

Wireless bridging provides a simple method for connecting building sites without cabling or can be used as a backup to existing wired links. If you have hundreds of nodes or bandwidth-hungry applications and data transmitting between sites, bridging your networks will require more than 11 Mbps provided by the 802.11b standard. However, by using the following Cisco-tested design, you can easily and effectively aggregate and load balance the bandwidth of three 802.11b-compliant Cisco Aironet® bridges to support up to a 33-Mbps half-duplex connection between bridge locations.

The use of standard technology and protocols including virtual LANs (VLANs), VLAN trunks, equal-cost load balancing, and routing protocols makes this design easy to configure and troubleshoot. More importantly, it makes support from the Cisco Technical Assistance Center (TAC) possible.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Equal-Cost Load Balancing

Load balancing is a concept that allows a router to take advantage of multiple best paths (routes) to a given destination. When a router learns multiple routes to a specific network — via static routes or through routing protocols — it installs the route with the lowest administrative distance in the routing table. If the router receives and installs multiple paths with the same administrative distance and cost to a destination, load balancing will occur. In this design, the router will see each wireless bridge link as a separate, equal-cost link to the destination.

Note: The use of equal-cost load balancing and the routing protocols mentioned in this article are a Cisco-supported means of aggregating Cisco Aironet bridges for additional throughput between sites or as a redundant failover wireless bridge link.

Routing Protocols

If your design requires failover capabilities, the use of a routing protocol is required. A routing protocol is a mechanism to communicate paths between routers and can automate the removal of routes from the routing table, which is required for failover capabilities. Paths can be derived either statically or dynamically through the use of routing protocols such as Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP, and Open Shortest Path First (OSPF). The use of dynamic routes for load balancing over equal-cost wireless bridge routes is highly recommended because it is the only means available for automatic failover. In a static configuration, if one bridge fails, the Ethernet port of the other bridge will still be active and packets will be lost until the problem is resolved. Therefore, the use of floating static routes will not work for failover purposes.

With routing protocols there is a tradeoff between fast convergence and increased traffic needs. Large amounts of data traffic between sites can delay or prevent communication between routing protocol neighbors. This condition can cause one or more of the equal-cost routes to be removed temporarily from the routing table, resulting in inefficient use of the three bridge links.

The design presented here was tested and documented using Enhanced IGRP as the routing protocol. However, RIP, OSPF, and IGRP could also be used. The network environment, traffic load and routing protocol tuning requirements will be unique to your situation. Select and configure your routing protocol accordingly.

Switching Paths

The active forwarding algorithm determines the path that a packet follows while inside a router. These are also referred to as *switching algorithms* or *switching paths*. High-end platforms have typically more powerful forwarding algorithms available than low-end platforms, but often they are not active by default. Some forwarding algorithms are implemented in hardware, some are implemented in software, and some are implemented in both, but the objective is always the same — to send packets out as fast as possible.

Process switching is the most basic way of handling a packet. The packet is placed in the queue corresponding to the Layer 3 protocol while the scheduler schedules the corresponding process. The waiting time depends on the number of processes waiting to run and the number of packets waiting to be processed. The routing decision is then made based on the routing table and the Address Resolution Protocol (ARP) cache. After the routing decision has been made, the packet is forwarded to the corresponding outgoing interface.

Fast switching is an improvement over process switching. In fast switching, the arrival of a packet triggers an interrupt, which causes the CPU to postpone other tasks and handle the packet. The CPU immediately does a lookup in the fast cache table for the destination Layer 3 address. If it finds a hit, it rewrites the header and forwards the packet to the corresponding interface (or its queue). If not, the packet is queued in the corresponding Layer 3 queue for process switching.

The fast cache is a binary tree containing destination Layer 3 addresses with the corresponding Layer 2 address and outgoing interface. Because this is a destination-based cache, load sharing is done per destination only. If the routing table has two equal cost paths for a destination network, there is one entry in the fast cache for each host.

Fast Switching vs. CEF Switching

Both fast switching and Cisco Express Forwarding (CEF) switching were tested with the Cisco Aironet bridge design. It was determined that Enhanced IGRP dropped neighbor adjacencies under heavy loads less often using CEF as the switching path. The main drawbacks of fast switching include:

- The first packet for a particular destination is always process switched to initialize the fast cache.
- The fast cache can become very big. For example, if there are multiple equal-cost paths to the same destination network, the fast cache is populated by host entries instead of the network.
- There's no direct relation between the fast cache and the ARP table. If an entry becomes invalid in the ARP cache, there is no way to invalidate it in the fast cache. To avoid this problem, 1/20th of the cache is randomly invalidated every minute. This invalidation/repopulation of the cache can become CPU intensive with very large networks.

CEF addresses these issues by using two tables: the forwarding information base table and the adjacency table. The adjacency table is indexed by the Layer 3 addresses and contains the corresponding Layer 2 data needed to forward a packet. It is populated when the router discovers adjacent nodes. The forwarding table is an mtree indexed by Layer 3 addresses. It is built based on the routing table and points to the adjacency table.

While another advantage of CEF is the ability to allow load balancing per destination or per packet, the use of per-packet load balancing is not recommended and was not tested in this design. Bridge pairs may have different amounts of latency, which could cause problems with per-packet load balancing.

Other Design Considerations

Quality of Service

Quality of Service (QoS) features can be used to increase the reliability of routing protocols. In situations with heavy traffic loads, congestion management or avoidance techniques can prioritize routing protocol traffic to ensure timely communication.

Full Duplex

Setting the Fast Ethernet bridge ports and associated Layer 2 switch ports to 10-Mbps full duplex will increase reliability by causing congestion to be queued at the switch instead of the bridge, which has limited buffers.

Dual Unidirectional Links

For designs that require the emulation of full duplex links, it's possible to configure the administrative distance of the equal-cost links between sites to create two unidirectional links. With this design, the third

bridge set could be used as a failover link or not be installed at all. Note that this specific design was not tested.

Example:

- **Site 1**

- ◆ Configure bridge pair 1 to have a relatively low administrative distance.
- ◆ Configure bridge pair 2 to have a relatively high administrative distance.
- ◆ Configure bridge pair 3 to have a relatively medium administrative distance.

- **Site 2**

- ◆ Configure bridge pair 1 to have a relatively high administrative distance.
- ◆ Configure bridge pair 2 to have a relatively low administrative distance.
- ◆ Configure bridge pair 3 to have a relatively medium administrative distance.

Traffic will flow from site 1 to site 2 across bridge pair 1 and from site 2 to site 1 across bridge pair 2. In the event that either bridge pair fails, bridge pair 3 will work as the failover link. See your specific routing protocol documentation for more information on how to configure the administrative distance.

EtherChannel

EtherChannel® is another technology that can be used to aggregate bridges into a virtual single link. Using EtherChannel for this purpose is not recommended, however, as it is not a supported design by Cisco and the Cisco TAC. Furthermore, you will be unable to manage some bridges via TCP/IP due to the way EtherChannel works. The port aggregation protocol (PagP) is not a tunable protocol and failover support is limited.

The Test Design

The following information is specifically related to the actual testing of the aggregation of three Cisco Aironet 350 Series bridges. The equipment used included six Cisco Aironet 350 bridges, two Cisco Catalyst® 3512 XL switches, and two Cisco 2621 routers. This design may also be used with two bridge pairs instead of three. The test design used Enhanced IGRP as the routing protocol with equal-cost load balancing, and CEF as the forwarding mechanism.

Most likely you will be using some hardware other than the specific models tested. Here are some guidelines when choosing the equipment to be used to aggregate bridges.

Routers

The routers used for testing had two Fast Ethernet (100-Mbps) ports and supported 802.1q trunking and CEF-based switching. It's possible to use a single 100-Mbps port to trunk all traffic to and from a switch. However, the use of a single Fast Ethernet port was not tested and could interject unknown issues or negatively impact performance. A router with four Fast Ethernet ports would not require the use of a VLAN trunking protocol. Other router considerations include:

- For 802.1q trunking support, Cisco 2600 and 3600 Series routers require Cisco IOS® Software Release 12.2(8)T or higher.
- If the routers don't support 802.1q trunking, check if they support ISL trunking, a Cisco proprietary trunking mechanism that can be used in place of 802.1q. Before you configure the routers, verify that your switch supports ISL trunking.

- For Cisco 2600 and 3600 Series routers, IP Plus code is required for 802.1q trunk support (this would be a cost upgrade from IP code).
- Depending on the hardware and its intended use, the base flash and DRAM may need to be increased. Take into consideration additional memory-intensive processes such as CEF tables, routing protocol requirements, or other processes running on the router that are not specifically related to the bridge aggregation configuration.
- CPU utilization may be a consideration depending on the configuration and features used on the router.

Consult the Feature Navigator (registered customers only) for Cisco IOS Software support for IEEE 802.1q VLAN trunking on your specific hardware platform.

Switches

The switches in the tested design require support for VLANs and 802.1q trunking. Using inline power-enabled switches such as the Cisco Catalyst 3524PWR when using Cisco Aironet 350 Series bridges is recommended, as this will make the setup less cumbersome. To collapse the switch and routing functionality into a single box, the Catalyst 3550 was tested and works quite well.

Bridges

Using Cisco Aironet 340 Series bridges will work as well, but the configuration would be slightly different since the Cisco Aironet 340 uses 10-Mbps half duplex Ethernet ports and a different operating system.

Tech Tips

Prevent duplicate EIGRP router IDs Duplicate Enhanced Interior Gateway Routing Protocol (EIGRP) router IDs can cause problems with the redistribution of EIGRP external routes. This document explains the problem and provides the proper configuration to prevent it.

Use VPN with the Cisco Aironet Base Station A typical use of the Cisco Aironet® Base Station Ethernet (BSE) and Base Station Modem (BSM) is for accessing the Internet over cable or DSL connection using virtual private network (VPN) technology. This document shows how to set up the base station unit for use with VPN.

Support Cisco CatOS SNMP traps Trap operations allow Simple Network Management Protocol (SNMP) agents to send asynchronous notifications that an event has occurred. Learn which traps are supported by the Catalyst® OS (CatOS) and how to configure them.

Lost your password on the Cisco SN 5420 Storage Router? Get it back with this step-by-step procedure for recovering a lost console password on the Cisco SN 5420 Storage Router.

Uninstall Cisco WAN Manager This document explains how to uninstall Cisco WAN Manager (CWM) from your system. Applies to versions 9.2 and 10.x of CWM installed on Solaris.

Get the lowdown on CISCO-BULK-FILE-MIB Learn how to use the CISCO-BULK-FILE-MIB and transfer files created by this Management Information Base (MIB) using the CISCO-FTP-CLIENT-MIB. Starting with Cisco IOS® Software Release 12.0, Cisco has implemented a way to store a Simple Network Management Protocol (SNMP) object or table as a file on the device. This file can then be retrieved using the CISCO-FTP-CLIENT-MIB, allowing you to transfer large amounts of data using a reliable transport method.

Caching in on savings Calculate cache savings using the tools and commands available on Cisco cache engines, content engines, and routers.

Set up shunning on a UNIX director Cisco Intrusion Detection System (IDS) Director and Sensor can be used to manage a Cisco router for shunning. In this how-to, a Sensor is configured to detect attacks on the router "House" and communicate the information to the Director.

Related Information

- [How Does Load Balancing Work?](#)
 - [Performance Tuning Basics](#)
 - [Configuring Switching Paths](#)
 - [Configuring Cisco Express Forwarding](#)
 - [Load Balancing with CEF](#)
 - [Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding](#)
 - [Configuring Fast Switching](#)
 - [Enhanced Interior Gateway Routing Protocol \(EIGRP\) Technology Support](#)
 - [OSPF Technology Support](#)
 - [Routing Information Protocol \(RIP\) Technical Support](#)
 - [Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2](#)
 - [Congestion Management Overview](#)
 - [Congestion Avoidance Overview](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 15, 2006

Document ID: 71478
