

MeetingPlace Server Network Isolation Recommendations

Document ID: 48264

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Network Isolation

- Broadcast Storms

- Networked Systems

Related Information

Introduction

This document explains network traffic problems that may occur on a Cisco MeetingPlace server and provides some network isolation recommendations.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco MeetingPlace server software (all versions).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Network Isolation

A variety of network traffic–related problems with Cisco MeetingPlace servers may occur, depending on how Cisco MeetingPlace networked systems are set up. This document provides some observations and recommendations for network isolation to deal with these problems.

Broadcast Storms

All Cisco MeetingPlace servers are susceptible to some extent to broadcast storms. The term *broadcast storm* refers to a situation in which a network is flooded with broadcast message packets addressed to the LAN broadcast address. For example, any packet sent to the local Ethernet address ff:ff:ff:ff:ff:ff is received by all

hosts attached to the local Ethernet segment. Low levels of broadcast traffic are normal and expected on any LAN. They are typically used either to advertise service ("I am here") or to find something ("where are you?"). For example, Cisco MeetingPlace conference servers use a broadcast to find the network server. However, when the broadcast traffic gets to the point where it takes a large percentage of the LAN bandwidth, you have a storm.

There are two problems with a broadcast storm. First and most obviously, the storm uses up the LAN bandwidth and crowds out other traffic. Second and more importantly, every broadcast packet must be processed by every machine that receives it, whether the packet is interesting to that machine or not. In a storm, the traffic that comes into a conference server can steal all of the CPU processing time, stopping normal operation and eventually triggering a watchdog timeout. Cisco MeetingPlace is more sensitive to broadcasts than a typical PC because of the real-time nature of the system.

Isolation and Protection

Cisco MeetingPlace can be isolated from broadcast storms through proper use of a router or LAN switch. Any router can easily be configured to filter out all broadcast traffic. In fact, most routers do so by default. Some Ethernet switches have a broadcast filtering mechanism, which shuts out broadcast traffic when it exceeds a configured traffic level. Because switches are considerably cheaper than routers, a switch is normally preferred in this situation, but not all switches have this feature.

Recommendation

All Cisco MeetingPlace systems should be isolated from other traffic on the corporate network. Usually this is most easily done by giving the Cisco MeetingPlace system a dedicated port on an Ethernet switch that has a broadcast filtering mechanism.

Networked Systems

The other possible traffic problem is specific to networked systems. Message traffic must flow unimpeded between the conference servers and the network server for the system to operate correctly. A traffic interruption that lasts more than a few seconds can have a noticeable effect on users. If the traffic is interrupted for a minute or more, conference servers "give up" and shut down.

Networks are typically not designed or managed to meet the requirements of a Cisco MeetingPlace network server. Traffic interruptions may occur due to maintenance activities, and blockage may occur due to high traffic levels. Network administrators may not be aware of the specific needs of the Cisco MeetingPlace system, or of the interruptions to the system that occur.

Recommendation

Cisco MeetingPlace conference servers should be directly connected to the same hub or switch as the network server. This equipment should, in turn, be isolated from the rest of the network as described above. Warnings should be placed on the hub or switch to prevent anyone from altering it. An excellent way to achieve this is to ask the customer to supply a dedicated Ethernet switch, which should be mounted in the same rack as the network server and considered part of the Cisco MeetingPlace system.

Another option is a router. Routers are the most versatile equipment available, and can be configured on a per-port basis. However, a single router port can be more expensive than an entire switch. Although it is unusual to dedicate a router port to a single device, it is necessary to dedicate a router port to Cisco MeetingPlace (or the aggregate set of Cisco MeetingPlace servers) to achieve the desired effect.

All Cisco MeetingPlace components should reside on their own subnet to avoid networking issues (such as broadcast storms) introduced by other, non-MeetingPlace components.

Related Information

- **Voice Technology Support**
 - **Voice and Unified Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **Technical Support – 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: Jan 31, 2006

Document ID: 48264
