Tech Info Library

AppleTalk: Filtering AppleTalk Traffic From Remote Links

Revised: 4/7/92
Security: Everyone

AppleTalk: Filtering AppleTalk Traffic From Remote Links

==========

Article Created: 31 March 1992
Article Last Reviewed:
Article Last Updated:

TOPIC -----

This article explains how to identify and filter AppleTalk packets from remote links.

DISCUSSION -----

Many organizations, particularly those whose data processing centers are run on DEC VAX computers, use Ethernet as their primary data communications link. When these organizations need to connect remote sites to their networks, it is quite common to extend a local Ethernet to the remote site using a transparent learning bridge and a leased digital telecommunications line, such as a 56K bps or a T1 line.

If AppleTalk nodes are connected anywhere on this extended Ethernet, any broadcast traffic they generate is forwarded across the remote link and may cause unwanted traffic on this line. And, if AppleTalk routers are present on both sides of the link, they exchange routing tables. As long as no configuration conflicts are present, they reliably route AppleTalk traffic between the two sites, which can be useful if you want to interconnect distant AppleTalk networks. However, if are not prepared to administer an AppleTalk WAN, or you don't want to have the two sites connected, this situation can cause problems.

For these reasons, you may want to filter AppleTalk traffic from the remote link, either to save transmission bandwidth on the link and/or to separate two AppleTalk networks that should not be connected. This is usually done by configuring the bridges to discard AppleTalk packets rather than forwarding them.

Here's how to do filter AppleTalk packets for both AppleTalk Phase 1 and

Phase 2 networks:

To filter AppleTalk traffic from a remote link, the bridges on both ends need to be set up to filter two kinds of packets. It is important that both ends of the link are set up for filtering, since most remote bridges filter only outgoing traffic. If AppleTalk traffic is passing in one direction and not in the other, there will be problems with routers on the end that receives the other's traffic.

Filtering AppleTalk Phase 1 is fairly straightforward. Since AppleTalk Phase 1 uses standard Ethernet headers, you can set the bridge to filter based on Ethernet protocol type (a 2-byte field in the packet that begins at byte 13). The two types to filter are $80F3 (for AARP) and $809B (for all other AppleTalk). Most bridges have a specific protocol filtering capability, so you simply need to specify which packet types to pass and which to discard, and the bridge does the rest.

Because AppleTalk Phase 2 does not use the old-style Ethernet header, you can't filter AppleTalk Phase 2 based on Ethernet protocol type. AppleTalk Phase 2 uses IEEE 802.2 and SNAP (Sub-Network Access Protocol) to provide interoperability with Token Ring networks because Token Ring uses 802.2 as its only means of specifying which protocol is in use. The 802.2 header begins at byte 15 of the Ethernet frame, and for AppleTalk, it looks like this:

```
                |       |
    Byte 15:    |  $AA  | \
                |  $AA  |  |- 802.2 header (3 bytes)
                |  $03  | /
                |  $08  | \
                |  $00  |  \
                |  $07  |   |- SNAP Protocol Discriminator (5 bytes)
                |  $80  |  /
                |  $9B  | /
                |       |
```

Thus, the bridge must be set to discard all packets that have this 8-byte pattern beginning at byte 15. This is usually accomplished as a different filtering function, by specifying the pattern to match and where to look for it. The bridge does not care what the data mean: if it finds the specified pattern at the right place, it discards the packet.

AARP (AppleTalk Address Resolution Protocol), which has a different protocol discriminator from other AppleTalk traffic, must also be filtered. The pattern to filter for AARP looks like this:

```
                |       |
    Byte 15:    |  $AA  | \
                |  $AA  |  |- 802.2 header (3 bytes)
                |  $03  | /
                |  $00  | \
                |  $00  |  \
                |  $00  |   |- SNAP Protocol Discriminator (5 bytes)
```

```
                  |  $80  |  /
                  |  $F3  | /
                  |       |
```


Tech Info Library Article Number:10034