Router Security Features

This article last reviewed: 26 November 1990

TOPIC ---

My company is having problems with our Ethernet backbone. Everyone is on the
Ethernet, but one division controls all access to the net.

People from different divisions can see into the corporate office's zone and
services. They can also print on corporate's LaserWriters. The corporate
office wants to block transmission into their area but let everyone in the
corporate office see services outside of their area. The corporate office
needs access to the IBM hosts and VAX systems which are all on the backbone
but in different divisions. Thus, total isolation is out of the question.

Right now, we connect our local divisions together with VitaLink boxes and T1
lines. I thought the VitaLink could do some of the above. But, even if they
could, the one division controls them. The best solution for corporate is to
find a router/bridge that has the above blocking/filtering features. If this
is not possible, is there a device that at least allows controlled access to
LaserWriters?

DISCUSSION ---

There are several options available to allow zone and device hiding, but most
of these products are LocalTalk to Ethernet routers like the Shiva FastPath or
the Cayman GatorBox. There is one product that may provide the type of
security you require; the NRC Macintosh-based Multigate router provides
Ethernet-to-Ethernet routing and provides the ability to define parts of your
network as insecure.

See the explanation below for a complete description of the options available
for each device. Here is a summary of AppleTalk router security features:

LOCALTALK TO ETHERNET ROUTERS

Cayman Systems GatorBox

Zone Filtering:
Zone filtering prevents users in the filtered zone from seeing other zones on
the network to which they are connected. This also prevents users in zones
outside of the filtered zone from seeing devices in the filtered zone.

Laser Filtering:
Laser filtering is, in a sense, a subset of zone filtering. Where the zone
filtering shields all of the devices from the outside, laser filtering lets
you hide just the LaserWriters from anyone outside of its AppleTalk zone. This
also prevents users in the filtered zone from seeing LaserWriters in other
zones.

Tilde Filtering:
Tilde filtering lets you hide any device with a tilde character at the end
of its name, so that it cannot be seen by anyone outside of its zone.

Shiva FastPath

Stay in Zone:
The stay-in-zone option prevents users in the filtered zone from seeing other
zones on the network to which they are connected. This also prevents users in
zones outside of the filtered zone from seeing devices in the filtered zone.

LaserWriter Security:
LaserWriter security is, in a sense, a subset of zone filtering. Where the
zone
filtering shields all of the devices from the outside, laser filtering lets
you hide just the LaserWriters from anyone outside of its AppleTalk zone. This
also prevents users in the filtered zone from seeing LaserWriters in other
zones.

Tilde Security:
Tilde filtering lets you hide any device with a tilde character at the end
of its name, so that it cannot be seen by anyone outside of its zone.

NRC 2000

Insecure:
The insecure option lets you define sections of your Internet as "insecure."
An insecure network's routing information is not propagated to any other
section of the network, thus providing a way to control who can access the
secure sections of the Internet.

APT

APT has announced an update to their AppleTalk routers. They now support
device security across zones. Users can, for example, hide their LaserWriter
from anyone not in their zone. You can also hide other devices, like file
servers and NetModems.

The user can let other users on different zones and create different sets of
access to different devices. For example, Zone A may have no access to your
LaserWriter, but still have access to a File Server, while Zone B has access to
all LaserWriters, but not AppleTalk ImageWriters or NetModems.

APT routers connect multiple LocalTalk, Ethernet, WAN, and Serial networks
together, and supports Phase II AppleTalk. DDP/IP encapsulation is in the

works.

ETHERNET TO ETHERNET ROUTERS

NRC Multigate Macintosh

Insecure:
The insecure option lets you define sections of your Internet as "insecure."
An insecure network's routing information is not propagated to any other
section of the network, thus providing a way to control who can access the
secure sections of the Internet.

Cisco (CGS/MB/AGS)

The cisco router offers the ability to set up access lists that permit
controlled access to your network. Access lists are set up to filter all
in-bound network traffic from any network listed in the access list. Only
traffic from networks not listed in the access lists is permitted into your
network. Traffic from your network is still propagated to all other segments
of your Internet.
Copyright 1990 Apple Computer, Inc.

Keywords: <None>

==

This information is from the Apple Technical Information Library.

19960215 11:05:19.00
Tech Info Library Article Number: 6408