Tech Info Library

Networks: Selectively Securing Zones and Devices (6/94)

Revised: 6/29/94
Security: Everyone

Networks: Selectively Securing Zones and Devices (6/94)

==========

Article Created: 29 August 1991
Article Reviewed/Updated: 29 June 1994

TOPIC ----------

Is there any product available that will allow a network administrator to hide zones or services on a selective basis?

I have two divisions on a single network that want to keep their printers separate. Each zone contains printers from only one division.

DISCUSSION ----------

There are several products available to isolate a LaserWriter. Some are hardware, some are software, but most work on the level of zones, hiding devices within a zone to the entire Internet.

There are several options available to allow zone and device hiding, some are LocalTalk-to-Ethernet routers, and some are Ethernet-to-Ethernet routers. To locate a vendor's address and phone number, use the vendor name as a search string.

Apple Internet Router

Apple Internet Router supports three "families" of access methods: AppleTalk, half-routing, and tunneling. Each family may include more than one specific access method. For example, LocalTalk, EtherTalk, and TokenTalk are all AppleTalk access methods.

One of the more interesting features of Apple Internet Router is device hiding, which lets you select any device or devices on your local network to be hidden from users on other networks. Device hiding is configured in the "Hide Devices..." dialog, which is accessed by clicking the "Hide..." button in the Port Info window.

You can elect to hide no devices, all devices, only a specific list of devices,

or all devices except a specific list. You can hide your selection from all other ports or from a specific other port.

The administrator must use good judgment when setting up the list of hidden devices (or the list of not hidden devices). If the list contains more than a few devices, it will adversely affect performance.

In order for device hiding to be effective in a loop environment, all routers on a given network must hide the same devices. Otherwise, a "hidden" device would be accessible through another router that isn't hiding it.

Device hiding is not foolproof. Users could obtain a hidden device's AppleTalk address through some means other than looking for it on their network, such as running Inter•Poll on a portion of the internet that does have access to the device. Armed with that information, a user could access the device programmatically, even though the device is theoretically hidden.

AppleTalk Router Security Features: LocalTalk-to-Ethernet Routers

---

Cayman Systems GatorBox

Zone filtering prevents users in the filtered zone from seeing other zones on the network. This also prevents users in zones outside of the filtered zone from seeing devices in the filtered zone.

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 allows you to hide only LaserWriter printers from anyone outside of its AppleTalk zone. This also prevents users in the filtered zone from seeing LaserWriter printers in other zones.

Tilde filtering allows you to hide any device with a tilde character (~) at the end of its name from being seen by anyone outside of its zone.

Shiva FastPath

The Stay in Zone option prevents users in the filtered zone from seeing other zones on the network. This also prevents users in zones outside the filtered zone from seeing devices in the filtered zone.

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 allows you to hide only LaserWriter printers from anyone outside of its AppleTalk zone. This also prevents users in the filtered zone from seeing LaserWriter printers in other zones.

Tilde Security allows you to hide any device with a tilde character (~) at the end of its name from being seen by anyone outside of its zone.

NRC 2000

The Insecure option allows you to define sections of your Internet as insecure. Insecure network's routing information is not propagated to any other section of

the network, thus providing a way to control who can and cannot access the secure sections of the Internet.

APT

APT Communications 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 hide other devices, such as file servers and NetModems.

You can allow other users on different zones, 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 LaserWriter printers, but not AppleTalk ImageWriter printers or NetModems.

APT routers connect multiple LocalTalk, Ethernet, WAN, and Serial networks and support Phase II AppleTalk.

AppleTalk Router Security Features: Ethernet-to-Ethernet Routers
---

NRC Multigate Macintosh

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

Cisco (CGS/MGS/AGS)

The Cisco router offers the ability to set up access lists that allow controlled access to your network. Access lists are set up to filter all inbound network traffic from any network listed in the access list. It excludes traffic from networks listed in the access lists from your network. Traffic from your network is still propagated to all other segments of your Internet.

International Transware (InterTalk)

This is a 2-port LocalTalk router that lets the user create blind and private zones. Users in a blind zone cannot see or use the resources of the AppleTalk Internet, but users outside of the blind zone can see and access any of the services in the blind zone. Private zone users have access to the entire Internet, but users outside the private zone cannot see or access any of the services of the private zone.

NetCounter

NetCounter limits use of a LaserWriter by using the user name as specified in the Chooser for all accounting and access control. Therefore, NetCounter does NOT provide a secure environment against knowledgeable users who are motivated to circumvent the NetCounter controls. The security can be increased to some degree by removing the Chooser Desk Accessory, if the Chooser is not required.

NetCounter is an application that downloads PostScript code to PostScript printers. Thus, NetCounter does NOT support QuickDraw printers such as the LaserWriter IISC. Because the accounting code executes on the printer rather than on the Macintosh, you install the NetCounter application only on the administrator's Macintosh, not on each Macintosh on the network.

The NetCounter code and log data normally reside in the printer memory. Therefore, in the event of a power failure or printer reset, the log data in the printer memory is lost. A Macintosh running NetCounter can request transfer of log data from the printer to the Macintosh, so the administrator can limit the amount of information lost in the event of a power failure. If the printer has a hard disk attached (like a LaserWriter IINTX with hard disk), the log data is automatically saved to the hard disk, so that no information is lost in the event of a power failure. If the printer has the new PostScript ROMs installed (such as M0445LL/A LaserWriter IINTX Upgrade Kit or M6215/A Printer), you can install the NetCounter PostScript code on the printer's hard disk. This allows NetCounter to start up automatically after a power failure or whenever the printer is turned on, and the code does not need to be manually downloaded. This is the recommended configuration.

Within the constraints described, NetCounter offers the following features:

- Provides a count of the number of pages printed by each user.

- Provides two different approaches to control access to the printer:
  - Grant access to specific users (deny all other users).
  - Deny access to specific users (grant access to all other users).

- Provides miscellaneous control and display of printer parameters
  For example, enable/disable printer startup page, or set the manual feed timeout.

- Prevents the PostScript Trojan horse (which changes the printer's password) from infecting the printer while NetCounter is running.

NetCounter can control multiple printers, but it is awkward, with the current version, to specify a different access control list for each printer.

Article Change History:
29 Jun 1994 - Included the Apple Internet Router.

Support Information Services

Tech Info Library Article Number:8794