Apple Internet Router 3.0, IP Extension, & Public Zone (3/93)

Article Created: 12 March 1993

TOPIC ---

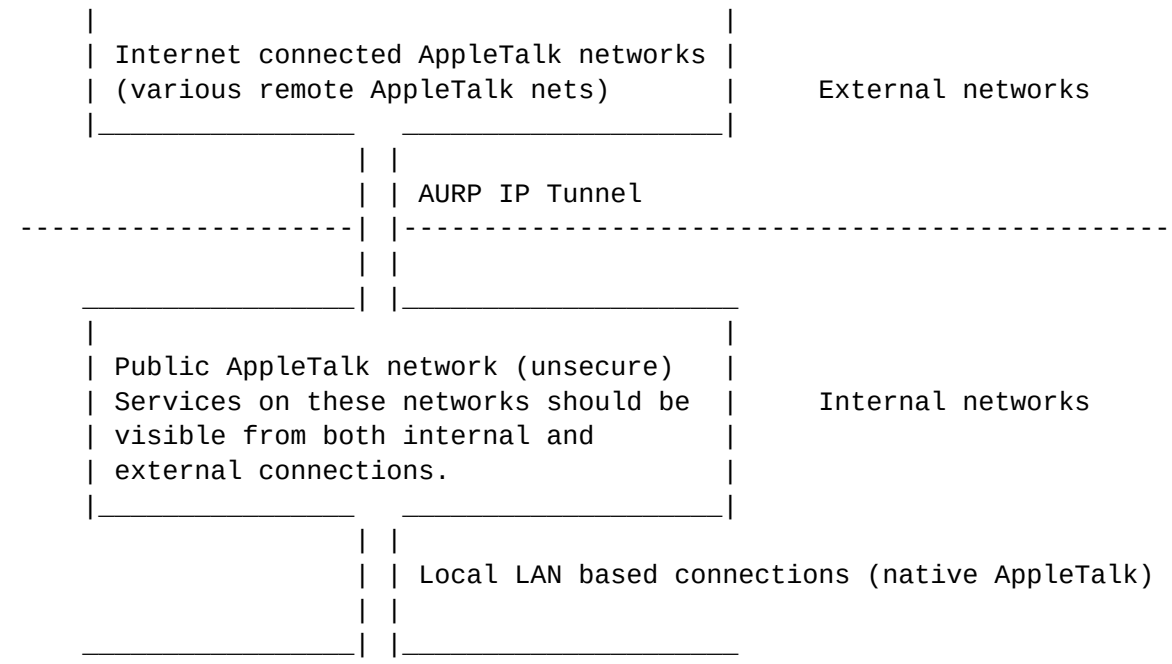
I want to allow remote and local AppleTalk networks to connect to a "public network". I want the "clients" attaching to this public network to see the services on that public network only and to have no knowledge of the peer networks attached to the public network. I may not have control of those who wish to connect to my network, so I need a method to manage the "filtering" of the inbound and outbound AppleTalk traffic.

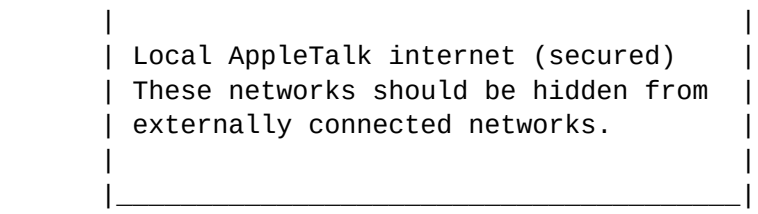
How can I set this service up using AIR 3.0 with the IP extension?

DISCUSSION --

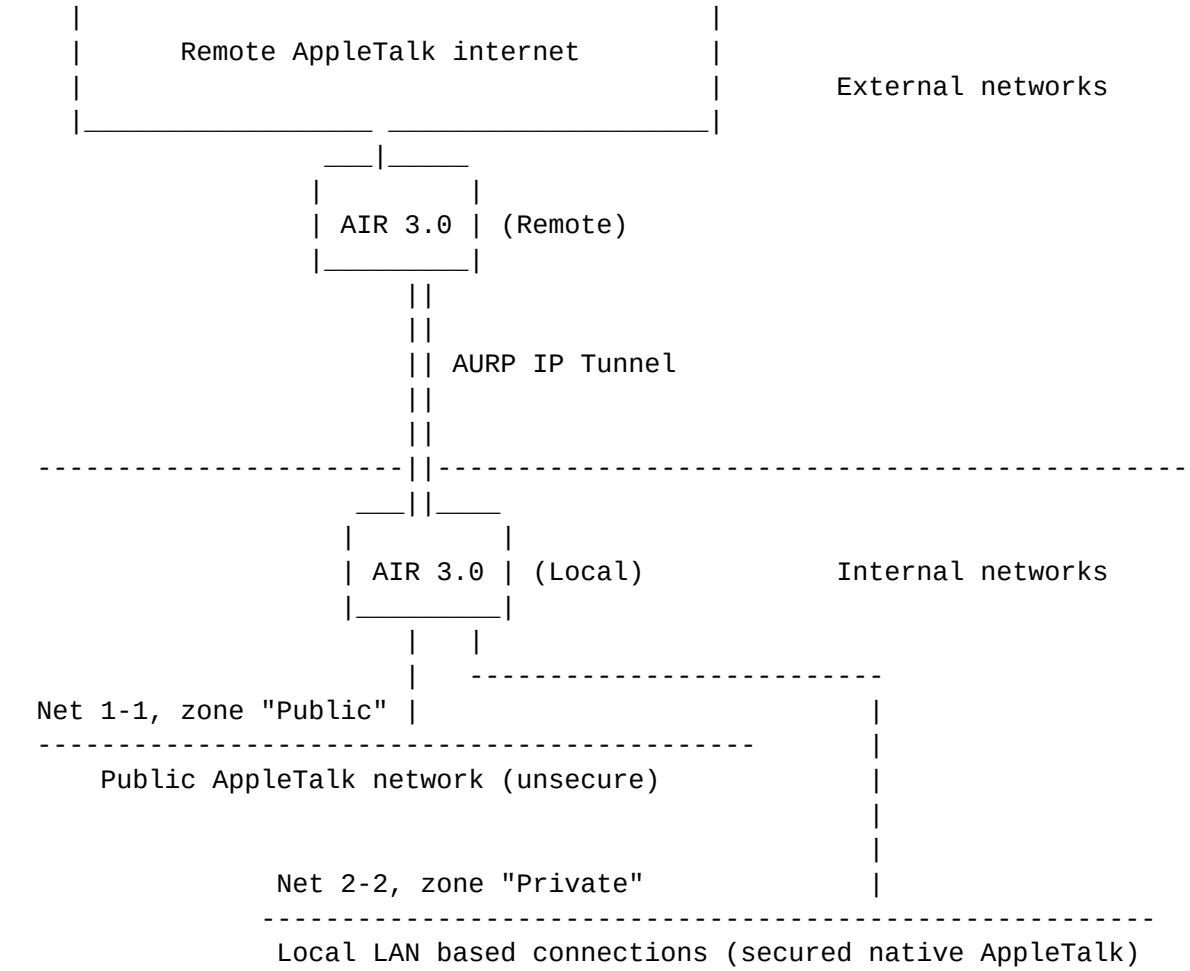
The information provided below will give you with the type of functionality you're looking for.

First, the following diagrams.





The first diagram lays out the basic design of the network; more detail is added below to show a more workable solution.



The Local Apple Internet Router

Given this configuration, you would follow these steps to configure the routers:

1) In the port info box for the IP tunneling port, deselect "Use only host ID's listed. This would allow any remote site to connect to this router to establish an AURP tunnel.

2) Select "Allow more than 15 hops". This takes care of any problems associated with remote networks that are more than 15 hops away from the

public network.

3) Select "Remap remote network numbers". This will allow remote networks which use the same network number as the public network to establish an AURP connection. Chose a range of networks large enough to satisfy the expected number of remote networks you'll have to remap. This will vary from situation to situation, but with a possible range 65,279 - (local network numbers used) you should be able to spare a few thousand numbers for remote remapping purposes.

4) Select "Cluster remapped networks". This is optional and only necessary if you are concerned about the size of the routing table or RTMP packets sent to the local networks.

5) Select "Hide all networks except those listed" from the "Hide from this network" pop-up menu. Input the network number of the public network in the list of networks not to hide, in this example you would list 1-1. This would hide all your local networks to any of your AURP connected remote internets.

6) Configure all other local network numbers and zone assignments.

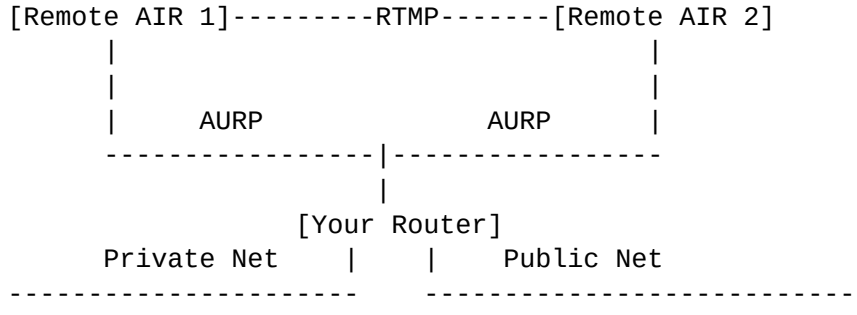
The Remote Apple Internet Router(s)

The remote router would only need to supply the address of your router and set up any options specific to their site (network number remapping, clustering, etc.).

Considerations given this configuration:

- Zones from remote sites will show up in the zone list on the local (secure) AppleTalk internet. Even though zones will show up, no services should be visible because the secure networks are hidden and thus no path exists for remote devices to respond to NBP requests.

- No routing loops can be present. In other words, no remote site could have multiple connections to your public network and also have RTMP-based connectivity between themselves.



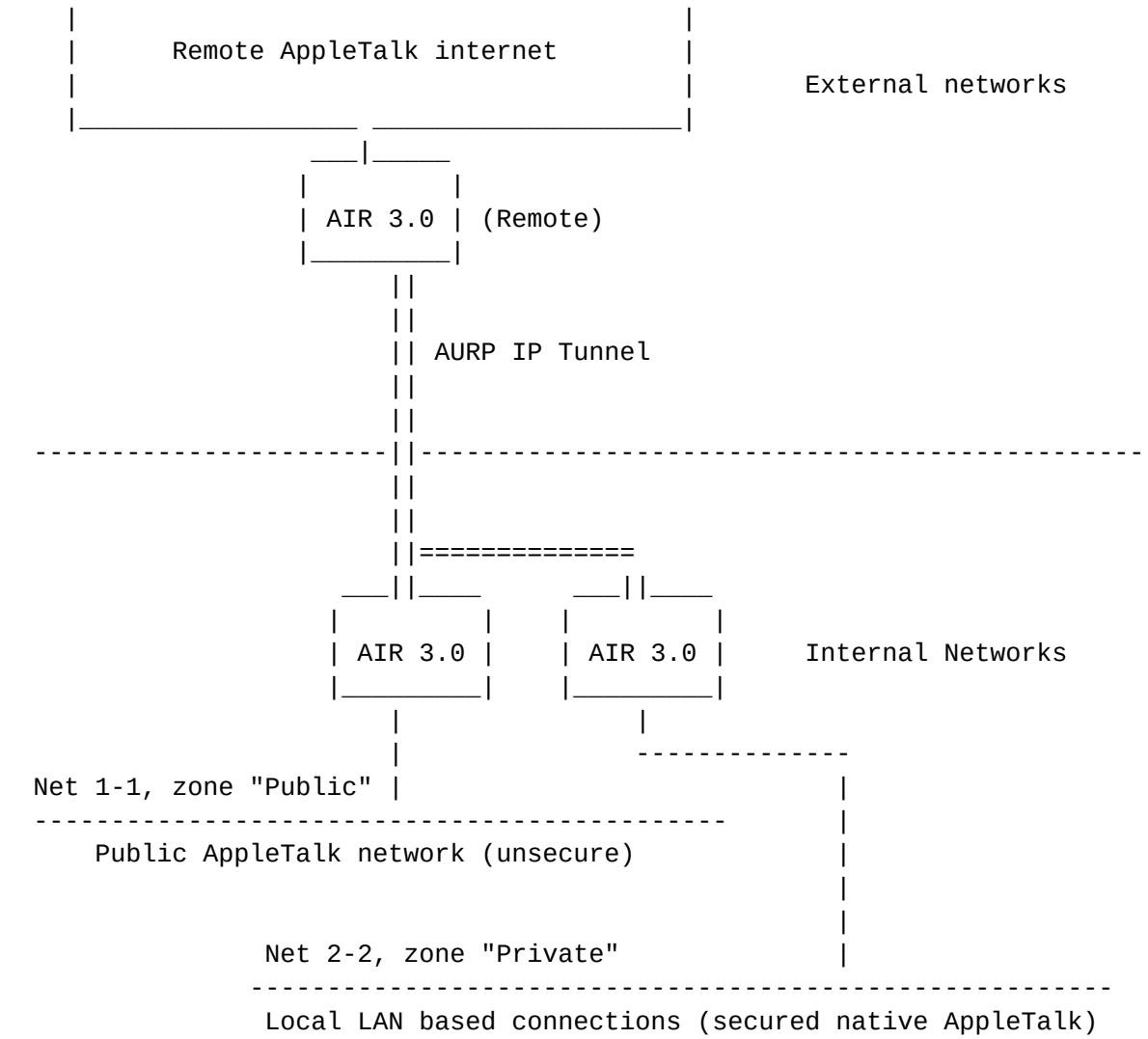
This type of configuration will not work unless you don't use network

number remapping.

Private (Secured) Network

Your private (secured) network nodes would not be able to connect to other "public" networks which may be advertised on the Internet without adding another interface to the router, or by adding another router, and changing the security configuration. We just can't come up with a good general way to provide the best of both worlds such as is possible using IP.

Now let's see if I can make it a little better:



What We're trying to show here is a second Apple Internet Router connected via IP to the local public network. This configuration offers some advantages over the first configuration.

- The biggest advantage is that your local users wouldn't be bothered seeing random zones appear because you would be connected to the public

network via an IP tunnel over which you would only see a single route to network 1, and a single zone "Public". This would, for the same reason, only increase the size of a local RTMP packet by a single network entry.

- You could easily configure the second router to also connect to other "public" Internet networks -- although security would still have to be carefully thought through for your private network users. Security would need to be considered because in order to enable your private network-based users to connect to remote "public" networks, you have to supply a route back into your private networks which means they cannot be hidden. You could hide your file servers and your printers using the device hiding features of the Apple Internet Router. But NBP-based security is really not all that secure since the devices could still be attacked if someone was able to discover their network and node information.

Keywords: <None>

==========

19960215 11:05:19.00

Tech Info Library Article Number: 11777