Orig copy

IEN: 58
Section: 2.3.3.19

ACCESS CONTROL
An Informal Discussion

Radia Perlman, BBN

October, 1978

WHAT IS ACCESS CONTROL

In "The Catenet Model for Internetworking" by Vint Cerf, access control is defined as "permitting traffic to enter or leave a particular network." If access control were really just a mechanism for restricting traffic from leaving the source net, or restricting traffic from entering a destination network, access control would be conceptually simple and easy to implement. It would merely require an access controller on a network communicating with the gateways on that net. However, access control is also to be used for through traffic. Some examples where certain nets would be unusable for certain kinds of through traffic are:

1) An important demo on a packet radio net would require that at the time of the demo, no through traffic would be allowed on that net.

2) The ARPANET might restrict through traffic from a particular hobby net to certain hours of the day.

3) Certain secret traffic might not be allowed on nets that go outside the U.S.

4) Certain traffic, because of delay time requirements or reliability requirements, might not be able to traverse certain nets.

WHY ACCESS CONTROL AFFECTS ROUTING

If access control were only invoked at the source or destination network of a packet, access control would not affect routing. If the destination network is not going to accept a packet, it will not allow it in no matter what route the packet takes. It might be more efficient for the first gateway to realize the packet will get rejected at the final gateway, and have the first gateway therefore reject the packet, but it is not crucial. When access control gets invoked for through traffic, however, routing is affected. There might be two possible routes for a packet to travel from source to destination, and it might be allowed on only one of those paths. Every gateway has to know somehow which way to send the packet so that if there is a legal way for the packet to reach the destination they will send it that legal way. A packet cannot get turned back in the middle of its path and hope to grope its way through the internet. (Without some sort of record in the packet of where it has been, gateways will just route it the old, failed way again, and loops would form. Even if some method were devised of keeping a record attached to the packet of how it shouldn't be routed, routing should not be done by trial and error!)

Thus access control is not something that can be implemented with access controllers local to each net informing the gateways on their own net about whether to accept or reject packets. It has to be something that all gateways know about for all links.

ROUTING

The current proposed internet routing method is based on ARPANET routing. This very efficient (in terms of computation, storage, and traffic requirements) scheme assumes that gateways do not need to know the path a packet will take--they merely have to know which neighbor to give the packet to. Neighbor gateways exchange information about how far they are from all destination nets, and when a gateway receives this information from its neighbors it calculates its own distance from each destination net as the minimum over neighbors N of the sum

D(G,N)+D(N,dest)

where D(G,N) is the distance from the gateway to neighbor N, and D(N,dest) is the distance neighbor N declares is between itself and destination "dest". A gateway routes a packet to the neighbor gateway closest to the destination network.

Without modification to this scheme, gateways could not do anything with information such as "Don't use net 3 for through traffic of any kind", since gateways do not know what path the packet will take once they hand it off to their neighbor.

Another proposed method of internet routing involved having gateways pass around information about the state of links in the catenet. Using this information, each gateway would calculate a complete distance matrix for the catenet, and use the distance matrix to decide which of its neighbors was closest to a destination (and therefore should be sent traffic for that destination). In this scheme, since gateways have all the relevant information, they could, in principle, look at a packet, decide which links are illegal for that packet, construct a modified connectivity matrix with those illegal links marked as down, and calculate a new distance matrix for packets of that type. The only problem is that it is a costly thing to do, and cannot be done on a per packet basis.

CATEGORIES

One way to accommodate a large number of the requirements for access control is to recognize that packets are partitioned into categories according to which nets they are allowed to traverse, and access control can be done on a category (as opposed to per packet) basis. Let S be a subset of the nets in the internet. Define category CS as internet packets that should not traverse nets in S, regardless of whether the nets in S are up or down. Which category a packet is in is time dependent, since nets can change their access control requirements (as in the case where a demo, for which through traffic on a net was banned, ends). If a packet is in category {A,B,D,F}, meaning it is not allowed to traverse nets A,B,D, or F, and F decides it is now OK to allow packets like that packet, the packet will then be in category {A,B,D}. If there are n nets there are 2↑n possible categories.

Routing under access control consists of routing with respect to each category of traffic. If the ARPANET routing is used, it would imply having neighbors pass around their distance to each destination net for each category. If the link state routing is used, since it is too costly to calculate a distance matrix for each packet, it would imply a distance matrix should be calculated and stored for each category.

ATTACKING THE PROBLEM

The basic problem is to keep the number of categories down to a manageable size. To do this we should list all the reasons for disallowing various kinds of traffic on various nets. Then we should choose a set of categories that suit most cases. If there are too many needed categories, nets can be grouped together in the sense that if one net decides not to allow some sort of packets, the other nets in the group will not be sent those sorts of packets either.

Then there is the problem of deciding which category a packet is in. There are many approaches to this:
1) The category could be a simple computation involving just a few fields in the internet header, such as source and destination nets, and type of service, and the gateways would match a packet with the appropriate category.
2) Access controllers could inform a gateway as to which category a packet was in. This would require each gateway to ask an access controller about each packet.
3) Access controllers could inform a gateway as to which category a packet was in, and fill in an appropriate header field with the information, so that subsequent gateways would not have to inquire.

Clearly the first approach is the most reasonable. In order for this to be implemented, however, it is necessary to decide what sort of tables gateways would need in order to calculate categories from the internet header. As conditions change requiring different category assignments for different kinds of packets, access controllers would be responsible for assuring gateways received the information necessary to update their tables. Gateways should probably pass this information around to their neighbors in addition to routing information, and some protocol must be established to assure the latest information would propagate.

POSSIBLE CHANGE OF ROUTING STRATEGY

Depending on the number of categories, and the relative importance of costs of traffic overhead, computation time in the gateways, and storage in the gateways, a link state routing algorithm might be preferable to an ARPANET routing scheme. With C categories, the ARPANET routing scheme requires C times as much traffic with access control as without. With a link state scheme, the amount of traffic between gateways is not increased with the number of categories, but computation time and storage needs are increased.

SECURITY

If care is not taken, this scheme would allow tampering with little effort by any malicious internet user. Anyone could send a packet to any gateway informing it that ARPANET traffic, for instance, should not be allowed on any other net, or any similar offensive message.

Without any maliciousness, simple gateways might be a problem. Someone might implement a gateway that did not implement access control, and it is well known that all nodes must agree on the route choice or loops will form.