L-Notebook

IEN-181

Van Gateway: Some Routing and Performance Issues

Jack Haverty

Bolt Beranek and Newman Inc.

May 1981

The VAN gateway is a new facility currently under development for the internet community. Its intended purpose is to allow interconnection of the ARPANET and therefore the Internet with Telenet, but it also introduces a new mechanism whose failure or misuse can seriously affect the system. The key problem with use of the VAN gateway is to allow and encourage using it for legitimate purposes, while preventing utilization by unauthorized users or as a result of a software or hardware failure in the networks involved.

There are two aspects to this problem. The first control on the gateway usage must be to assure that the packets being handled are legitimate, in that they are associated with authorized users. This is a specific example of the need for mechanisms which have been discussed at various times as "restricted routing" mechanisms.

The second control problem is to assure that the gateway is being used as intended, with a reasonable level of traffic for the function being performed. Even if packets are being processed for authorized users, it is possible for failures within the routing system or host software, for example, to cause packets to loop endlessly. Failures of the network protocols could similarly cause duplicate packets to be sent needlessly.

In both cases, the concern results from the highly visible impact which use of Telenet incurs, since charges are computed on a per-packet basis. However, the same issues are inherent in the Catenet itself, in that misuse of the network consumes resources which are then unavailable for legitimate use. Thus the problem of managing use of the gateway is most critical for the VAN gateway, but applies as well to all gateways, and in fact to any shared resource.

In the initial implementation of the VAN gateway, resource management is being provided by use of tables which enumerate the authorized users of the gateway. These users are simply the addresses of the hosts, both on the ARPANET (Catenet) side and on the Telenet side, which will be acceptable as valid source and destination addresses of packets which transit the gateway. All other packets which are received by the gateway will be discarded.

In the internet architecture, the Telenet side of the gateway appears as a single network to the internet mechanisms. The gateway contains a table which maps artificial host addresses on that network into real 14-digit Telenet/X.25 addresses, in much the same way as other networks convert internet addresses into addresses for their particular attached network. X.25 virtual circuits are only permitted between the gateway and X.25

hosts which are present in this translation table, which effectively defines the set of authorized gateway users in the X.25 community.

No similar table is necessary for translation of addresses on the ARPANET side of the gateway, since this translation is well defined by the internet protocol. Without any additional mechanisms, this would permit any ARPANET host to use the VAN gateway. In addition, since gateways to other networks are simply ARPANET hosts, this would permit any host on the Catenet to use the VAN gateway.

To restrict the user community of the VAN gateway, a second table is provided, which enumerates all internet addresses which are acceptable as sources or destinations on the ARPANET side of the gateway. Each internet datagram which arrives from the ARPANET or Telenet is checked to assure that the source and destination addresses in the internet header are listed in one of the two tables which define the set of hosts which are permitted to use the VAN gateway.

The table entries will be set up directly by DARPA. In selecting the set of valid hosts, the reliability of the data presented to the gateway should be considered.

In particular, we note that there is a significant difference in the addresses presented at the gateway in the internet header of each packet. If such an address is in fact on the ARPANET, the gateway can verify it by comparison with the address supplied by the IMP in the ARPANET leader of the packet. For packets sent to the ARPANET, one can similarly expect the IMP subnet to deliver the packet to the host specified in the ARPANET leader.

If the address of a packet handled by the gateway is on another component network of the Catenet, the packet is necessarily handled through one or more gateways. The internet structure permits gateways to freely enter the system. Gateways are in general under the control of the organization which owns them and/or the attached network. Gateways in general do not check the addresses in the internet headers of packets which they process, so it is possible for malfunctioning hardware or software to emit packets with incorrect addresses. If such addresses happen to be present in the VAN gateway tables, these packets will be processed by the VAN gateway.

The impact of this situation on the policy for allowing use of the VAN gateway is that hosts on networks other than the ARPANET are to be considered somewhat less reliable in terms of enforcement of the usage policy. The mechanisms in the initial

VAN gateway implementation will provide some degree of control over the use of the gateway, but these mechanisms are not to be considered appropriate or complete in the general sense, and they are not proof against failures. These mechanisms are intended only as an interim measure.

We suggest that further development work on the internet gateway system, of which the VAN gateway is a component, should address the problems of resource control at the internet system level. Any mechanism which restricts the usage of a gateway must be designed in conjunction with other network mechanisms, such as routing, flow control, load sharing, and error control.

As an example, we can consider a hypothetical configuration in which two VAN gateways are connected to Telenet, one from ARPANET, and the other from SATNET, to support traffic between Telenet users and hosts on ARPANET or SATNET. Only these user/hosts would be listed in the VAN gateway tables.

Since the VAN gateways are participants in the internet routing mechanisms, failure of the gateway between ARPANET and SATNET would cause the system to recognize the path through TELENET, as a transit network, as a viable route for ARPANET-SATNET traffic. However, this traffic would be discarded at the VAN gateway because the addresses are not listed in its tables.

This scenario will be avoided by preventing the two VAN gateways from being "neighbors" for routing purposes, which is acceptable only in restricted configurations. The general problem results from the usage restrictions at the VAN gateway, which makes the path a valid route for one class of packets, but invalid for other classes. The current routing mechanism cannot handle this situation.

In addition, the effect of the usage restrictions on future mechanisms for handling partitioned networks, and load sharing of gateway paths, must be investigated.

We have two mechanisms to propose for consideration as mechanisms to attack this problem. The first is a resource control model which is a result of the TIP Login work. The second involves the use of performance models, which monitor use of resources to determine if unexpected behavior occurs. These two mechanisms can be introduced to work more effectively in the VAN gateway problem.

The architecture for the TIP Login system identifies several abstract modules which interact to implement the resource control functions. A "Control Point" is the module which directly controls the use of a resource. It is responsible for detecting an attempt to use some resource, collecting such information which identifies who is trying to use the resource and what they are trying to do, and then permitting or denying use of the resource. The decision concerning whether or not a particular usage is allowed is made by a "Decision Module." This module takes the information supplied by the Control Point, and applies the algorithm which defines the resource usage policy. Typically, and particularly in the Tip Login case, the Decision Module will obtain more information about the particular user and/or resource involved in the decision, by using a distributed database system.

In the TIP Login system, the Control Point is at each TIP. Decision Modules are located in special-purpose hosts. The database system is present in those hosts as well as on larger database-maintenance hosts, where tools to manipulate and modify the database exist. Typically the Decision Module identifies the particular individual attempting to use a TIP, and retrieves a record of information specific to that individual, which defines his authorizations (or lack thereof).

Much of this mechanism should prove to be useful as a basis for control of gateways as well. In such a system, the control points would be at the gateways. Decision Modules might also be at the gateways, if decisions must be made on each packet. Decisions might be based on source or destination addresses, or on the identify of the individual responsible for the packet. We suggest that this approach be considered for further research.

A problem which is not being addressed currently is the second control problem mentioned earlier, namely the monitoring of the use of some resource by an authorized user, to guarantee that the resource is being used as intended. In the VAN gateway case, for example, a malfunctioning TCP might cause many unnecessary packets to be handled, but since they are associated with authorized addresses, no control is applied. In addition to the obvious cost and performance penalties, lack of monitoring precludes the use of policies which grant limited use of resources to, for example, allow some users to handle only low-throughput traffic, or low priority traffic. We believe that the use of performance models, embedded within the gateways and for hosts, is a promising direction for attacking this problem.

Limitations of the current LSI-11 implementation of the VAN gateway are likely to preclude any significant testing of these approaches. We have been pursuing these ideas as research issues, which have surfaced during the current implementation efforts.