Grafting an ATM Network onto an Existing Ethernet Network

William Tucker, Computer Science Department, University of the Western Cape
Derek Keats, Botany Department, University of the Western Cape
Private Bag X17, Bellville 7535, South Africa

Telephone: 27 21 9593008 Fax: 27 21 9593055
E-mail: btucker@uwc.ac.za, dkeats@uwc.ac.za

Abstract

Grafting an ATM network onto an existing Ethernet network is a non-trivial exercise in network configuration. The process of mating ATM technology to an Ethernet network without tampering the underlying backbone and network configuration gives rise to a variety of networking issues including addressing, compatibility, security, efficiency, administrative effort, and scalability. Examples of actual situations serve to illustrate these issues. We have designed several scenarios to tackle the topological problems of an ATM graft. A dual IP approach works but suffers from a lack of scalability. We expect an edge routing solution, with subnetting, will be the most elegant and scalable.

Introduction

The Center of Excellence (CoE) research program in ATM and broadband networking and their applications at the University of the Western Cape (UWC) has a situation that requires grafting an Asynchronous Transfer Mode (ATM) network onto an existing campus Ethernet network. The experience has enabled us to present and categorize a host of technical networking issues involved with the grafting process. We find ourselves revising our ATM deployment strategy as we become more familiar with the peculiarities of ATM and grapple with constraints imposed by grafting issues. These issues are quite general in nature, and are not peculiar to the UWC situation. Furthermore, these problems are practical in nature and therefore do not receive much attention in the literature devoted to running TCP/IP over ATM (Kercheval 1997). This paper identifies the networking issues and presents them in the context of the ongoing UWC experience with them. The constraints and issues fall into the following categories concerning the network: addressing, compatibility, security, efficiency, administrative effort, and scalability. We have devised several scenarios to solve the grafting problems. This paper provides details on each scenario, as well as advantages and disadvantages. We have successfully deployed one of these scenarios and provide implementation details and results. We then discuss the steps to take for the implementation of a more ideal and comprehensive solution. Throughout the paper, we show that the problems and issues of a local ATM graft also apply to a multi-campus grafting situation. When multiple institutions connect their campus-grafted ATM circuits to provide a high-speed broadband ATM wide area network (WAN), all of the issues presented in this paper come into full force at a higher level. An elegant solution deployed at the local level will lead to a more scalable solution as institutions connect.

Grafting

What does "grafting an ATM network onto an existing Ethernet network" mean? For the purposes of this discussion, the ATM circuit is not mean to replace the existing backbone. Rather, the ATM circuit becomes an extension of the existing network structure [see Figure 1]. It would be relatively trivial to isolate all of the machines on an ATM circuit and provide a single gateway to the rest of a campus network [see Figure 2]. In this case, the ATM circuit could take on its own network or even a subnet, with access governed by a router or gateway. This scenario is not what we would call a "graft". Instead, a graft scenario grants ATM access to machines that are already participating in the campus network. Furthermore, the machines must remain part of their existing networks and/or subnets. In a graft scenario, the machines have a choice: to get to other ATM-connected machines, use the ATM link; to get to the rest of the world, use the existing network infrastructure. In other words, grafting an ATM network means leaving the existing network alone.

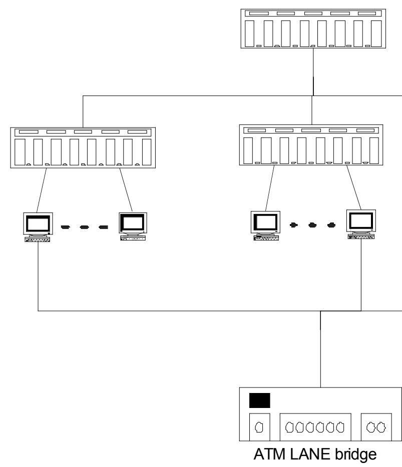

Figure 1. ATM graft: selected nodes join ATM circuit but remain attached to original network

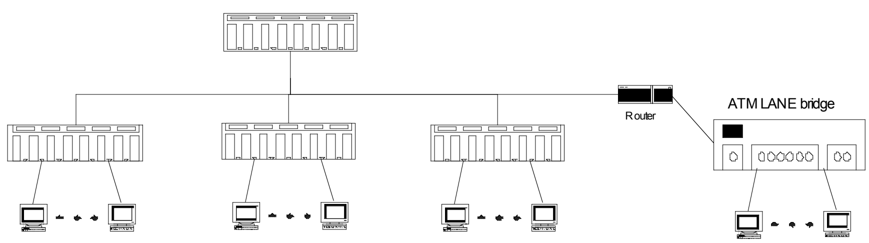

Figure 2. ATM addition: nodes moved to ATM-exclusive segment

The UWC Graft

The UWC CoE research teams' machines must be simultaneously ATM-connected and Internet-connected. The ATM connectivity is only provided between CoE teams on campus. In the future, the ATM connectivity is expected to extend off campus to other CoE members. Most of the teams' machines are already connected to the greater campus network for Internet and email access (UNINET). One team has an independent Internet Service Provider (ISP). Each team has a different set of network IP addresses. There is no subnetting on campus and departments often share portions of Class C networks. As we will see later, the dominance of Novell IPX traffic over the campus backbone introduces additional complications.

In order to provide access to as many computers as possible, the UWC CoE opted for non-native ATM delivery to the desktop. The UWC CoE purchased a core ATM switch and three satellite LANE bridges. Each LANE bridge provides 25 Ethernet UTP ports with an ATM uplink to the core ATM switch. The hardware solution allows placing a LANE bridge in a departmental hub stack cabinet, and merely reconnecting UTP lines from the current LAN hubs to the new LANE bridge. The LANE bridge automatically provides TCP/IP over ATM (Kercheval 1997, 3Com 1997).

Physically, the graft is as follows: three departments took a LANE bridge and laid optic fiber to the main ATM core switch. Computer Science (CS) and Physics share a LANE bridge. The South African National Bioinformatics Institute (SANBI) has the ISP connection. Botany's LANE bridge has an optional Ethernet fiber connector. A native ATM video conferencing center will be deployed when UWC gains ATM connectivity off campus. The video conferencing facility must also integrate with the existing network infrastructure. It must also be compatible with native ATM video conferencing hardware and software at other CoE institutions. Refer to Figure 3 for the overall picture.

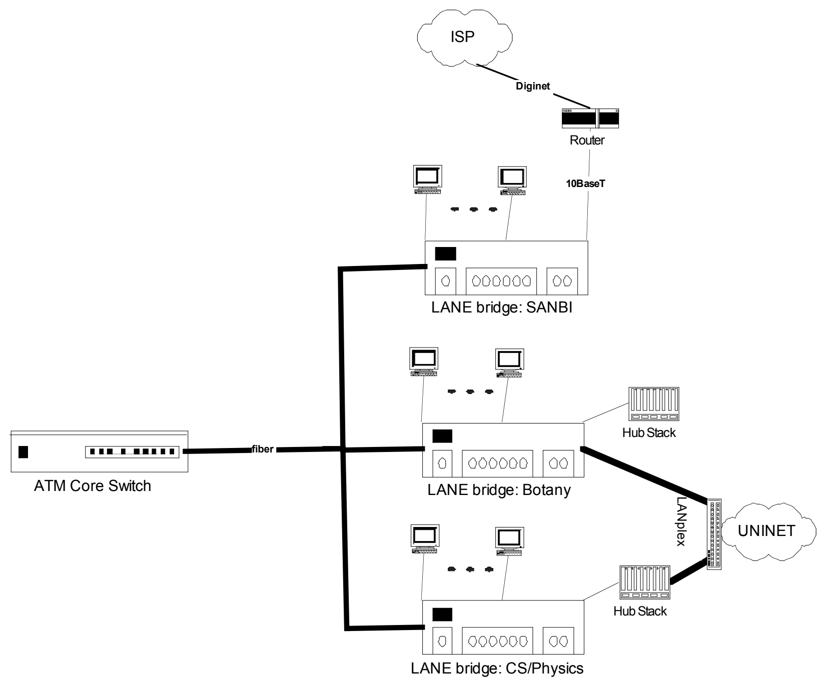

Figure 3. Original ATM graft topology for UWC CoE

Grafting Issues

This section categorizes networking issues involved with a grafting process. These issues are addressing, compatibility, security, efficiency, administrative effort, and scalability. To bring the problem out of the theoretical, and into the real world, we illustrate each issue with more details of the UWC CoE grafting experience.

Addressing

Whenever additions are made to a network, whether they be network devices or workstation nodes, the issue of network addressing always crops up. For the purposes of this discussion, let us focus on IP addressing, since the main purpose of the UWC CoE ATM graft is to run TCP/IP over ATM. The ideal solution to IP address members on a grafted ATM segment is to allocate them a fresh, unused cluster of IP addresses. However, the scarcity and cost of a new network, e.g. Class C, immediately restricts that possibility. Another solution is to allocate unused numbers on an existing network. This can be done with or without subnetting. Without subnetting, unused addresses remain on the existing network. Subnetting, on the other hand, allows logical isolation of network portions (Douba 1995, Black 1998). Locally, subnets behave as separate networks. If a network is already subnetted, perhaps there exists a subnet that has yet to be used. If a network is not already subnetted, the subnet masks have to be changed for all of the participants on the network. A subnet mask specifies that bits from the node portion of an IP address be used to extend the network address. More importantly, machines may have to be renumbered to participate in the new subnets since the most significant bits in the node address now identify membership in a subnet.

A significant advantage of subnetting is that traffic can be contained within local logical subnets behind gateways (Douba 1995). Also, subnets appear as a single network to the rest of the world. In other words, an external node does not need to know that a network is subnetted in order to access a machine inside a given subnet. In the case of an ATM graft, ATM-connected machines can live in their own subnet yet still belong to the parent network as far as the outside world is concerned. Without logical separation, all traffic seen on the campus network also flows onto the ATM circuit, and vice versa. As we will see later, this can have disastrous effects.

Another option for IP addressing is to use dual IP addresses. Each machine already has an IP address for its attachment to the campus network. To "dual IP" a machine is to assign a second address for the purpose of filtering traffic, similar to how a subnet solution filters traffic. Each ATM-connected machine receives a dual IP. An ATM-connected machine uses the original IP address to talk to the Internet. However, a machine uses the second IP address to talk to another ATM-connected machine. Because of this, traffic meant for ATM-connected machines does not travel beyond the logical dual IP network. But where do the dual IP addresses come from? Again, a fresh network address would be ideal. However, the dual IP scenario lends itself to using "fake" IP addresses. A fake IP network would be one that an institution does not own. Judicious masking and keeping the dual IP addresses out of the Domain Name Service tables avoids the problem of having two machines on the Internet with the same IP address. The ATM-connected machines use the fake IP addresses to talk to one another, and actual IP addresses to communicate with the outside world. The dual IP scenario described below provides an illustrated example of this approach.

Another issue is that a graft will have to contend with multiple Internet access points. There are two levels where this happens: campus and inter-campus. At the campus level, the ATM graft connects machines that were previously on disparate networks. Each network has its own connection to the Internet. Each network could also conceivably have its own ISP. After an ATM graft, a machine is given multiple routes to the Internet. The route chosen is easily configured with a static routing table or by the definition of a particular default gateway. At the inter-campus level, campus A now has access to campus B's Internet access points. ATM-connected machines not only have access to multiple access points on campus, they also have some degree of access to every campus connected to the greater ATM circuit. The implications of these configurations are taken up in more detail in the Security and Scalability sections below.

Addressing at UWC

As with most institutions, UWC has a limited number of Class C networks and node addresses are at a premium. Multiple departments in a given geographical area share a Class C network. Departments are usually allocated contiguous blocks of IP addresses. The campus is not subnetted. UWC uses fiber connected to a LANplex to route traffic to networks. Three of the UWC CoE teams live on three different Class C networks. It may be possible to subnet these Class C networks to put CoE machines on logical subnets, but this would impact non-CoE machines. Furthermore, recall that SANBI uses an ISP and therefore lives in a completely different domain. These issues were a major motivation behind attempting a dual IP solution to the grafting problem. Figure 4 depicts the pre-ATM graft network.

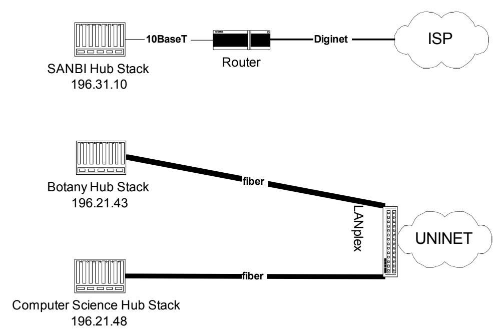

Figure 4. CoE teams' departments before ATM graft

Compatibility

In a graft situation, an ATM-connected machine retains its existing network connectivity. The ATM hardware and networking configuration must support transparent access between the machine and the campus. This is accomplished with LAN emulation, or LANE (Kercheval 1997, Lohse 1997)). Consider a campus network based on Ethernet. The ATM equipment chops up an Ethernet packet and moves it across the fiber inside smaller ATM packets. Before delivering the data to an Ethernet connection on the other side, another LANE bridge reassembles the Ethernet packets. As such, LAN emulation occurs without the knowledge of Ethernet hardware and without any specific cooperation with the network layer of the campus network. On the hardware side, the ATM equipment supports standard Ethernet-type hookups such as UTP RJ-45. The Ethernet packets flow into a LANE bridge just as they would into an Ethernet hub. The network does not know anything different. LANE actually supports any network protocol that runs over Ethernet because the emulation takes place at Layer 2 in the OSI stack. The network protocols at Layer 3 and higher, such as TCP/IP, are insulated from the emulation at the lower level. Note that ATM LANE also supports Token Ring, and consequently any Layer 3 protocol that runs over Token Ring.

For the most part, the ATM/Ethernet interface is physically plug and play. However, experience tends to show that the real world can be much different. There are often multiple protocols running on top of Layer 2 systems. For example, both TCP/IP and IPX run over Ethernet. Because the LANE emulates Ethernet, it is automatically buffered from having to deal with IP or IPX. The IP and IPX datagrams are already encapsulated inside Ethernet packets. However, the topologies that characterize higher levels in the OSI stack may not agree with the topology provided by its lower levels.

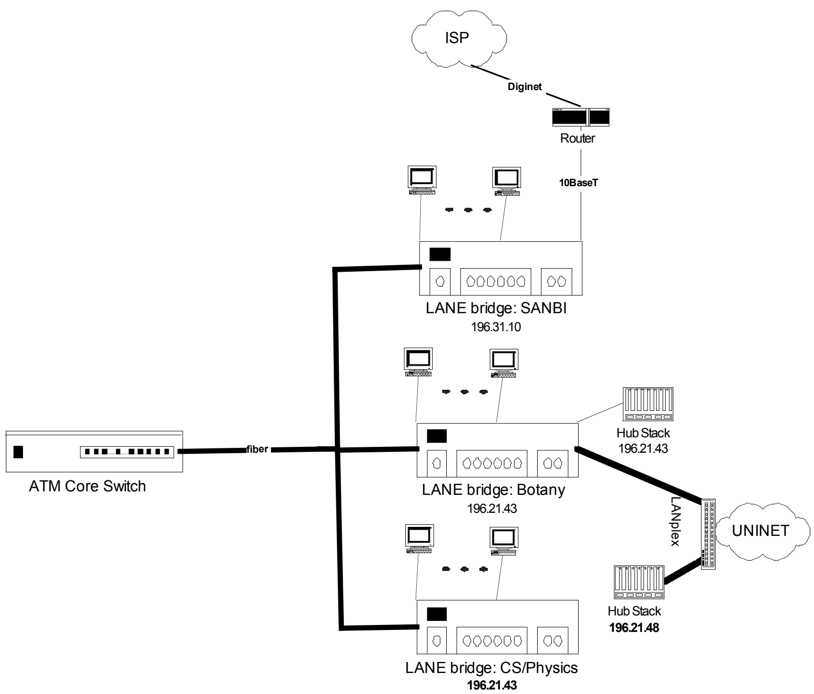

Figure 5. Revised ATM graft topology

Compatibility at UWC

At UWC, we encountered such a problem with IPX traffic. When we connected the ATM hardware up as in Figure 3, we crashed the entire campus network. The reason was that the LANE bridges do not support the Spanning Tree Protocol (STP) over ATM (3Com 1997). The graft of the ATM circuit onto the network introduced additional avenues for the IPX traffic. The Novell system could not cope and fell over. To remedy the situation, we disconnected the CS/Physics LANE bridge from the CS hub stack. In order to access the Internet, the Computer Science and Physics machines now take on Botany IP addresses (196.21.43.x) and route through Botany's LANE bridge to reach the UNINET. Figure 5 shows the modified topology. This approach unfortunately introduces quite a roundabout way for CS and Physics machines to communicate with their respective peers. It also removes some of the CoE machines from their departmental groupings. As such, the solution was accepted as a temporary measure until a better solution could be deployed.

Security

An ATM graft allows an ATM-connected machine access to resources it could not previously reach. Before the graft occurs, network resources are typically restricted to network segments. For example, a departmental printer lives on a given Class C network. Only machines on the same network have access to that printer. Access is easily controlled with network topology, e.g. routers. An ATM graft violates the separation of networks [see Figure 1]. The graft links up machines on multiple network segments, providing paths between networks where there previously were none. When different networks use (and pay) different ISPs, the potential for abuse arises.

Security at UWC

Most UWC CoE teams access the Internet via the UNINET. However, SANBI pays an external ISP for dedicated bandwidth. A security issue emerges because other groups can abuse this ISP connection: anyone on the ATM island can easily change their IP address to join the ISP network. Of course, the perpetrator would need to use a valid unused IP address. Another possibility would be to set up a static route to the ISP network and then use the ISP router as a default gateway. This would allow a machine to transmit information using the ISP's bandwidth. Note however, that incoming traffic would still come in via normal routes. Regardless, firewall measures can be put in place to negate both types of abuse.

Efficiency

Of the many ways to measure network efficiency, speed is usually considered most crucial. One of the primary motivations for introducing an ATM circuit is to gain the incredible speeds that ATM is capable of, currently ranging from 155Mbps to 622Mbps (Kercheval 1997). A graft is meant to deliver these speeds to participating machines. However, when an ATM-connected machine communicates over its original campus network, the speeds necessarily drop back down. Since the amount of time, or length of cable, that such a connection spends on the ATM link is insignificant, other measures are more pivotal.

First of all, consider the number of hops that a packet or datagram must make between a source machine and its intended destination. At each hop, the packet needs to travel up and down the network protocol stack, incurring overhead all the while, in order to be sent to the next hop. One way to insulate ATM-connected machines in a graft situation is to surround the ATM circuit with routers. Each time a packet travels in toward the ATM circuit or outward from it, the hop count increases. Each extra hop count delays communications. Also, recall that the LANE bridge is also incurring some overhead at the border between the ATM and the surrounding Ethernet network as it fragments and reassembles Ethernet packets.

Another efficiency issue specific to the ATM graft situation is the overflow of traffic from the non-ATM segments onto the ATM circuit. If unshielded by routers, broadcasts made from outside the ATM circuit find their way onto the ATM fiber. Depending on the characteristics of the campus network, the degree to which this unnecessary traffic impinges upon the overall ATM throughput may or may not be negligible.

Efficiency at UWC

At UWC, the machines on a given network share Ethernet bandwidth of 10Mbps. This pales in comparison to the 155Mbps over the ATM circuit, and the dedicated 10Mpbs that machines receive when they direct-connect to a LANE bridge. The efficiency of the ATM-connected machines, then, is not an issue. However, the introduction of the ATM graft does inhibit efficiency when the ATM-connected machines communicate with the campus and the Internet. Due to the Spanning Tree problem, all ATM-connected machines (except SANBI machines) route through the Botany LANE bridge and out through Botany's port on the LANplex. Before the ATM graft, CS machines were on the same physical LAN. Now, a CS machine on the ATM circuit must make a large trip through two LANE bridges, the core switch, and the LANplex before connecting to a CS peer on the original network. That is four hops where there were none before. Also, if we introduce routers to reconfigure the ATM graft, there would still be a router hop between peers on the same Class C network (but on a different subnet). This is discussed in detail below.

The other issue of efficiency is the spurious traffic introduced to the ATM circuit from the campus network. At UWC, this traffic is mainly composed of predominantly IPX broadcasts and a negligible amount of Appletalk. With a packet sniffer, we found IPX traffic averaging 3% of the bandwidth, with spikes up to 50% or more. Understandably, these numbers have created some concern among CoE ATM participants. Efforts to filter the IPX traffic with LANE bridge configuration failed. It may be that the packets are coming across as Ethernet-level broadcasts so that disabling IPX has no effect.

Administrative Effort

An often overlooked issue regarding network configuration is simply the amount of administrative effort required to plan, configure, implement, and maintain network changes. With respect to an ATM graft onto an Ethernet network, the most significant types of changes are physical network connections and the configuration of networking parameters. The first stage of any graft process is to plan out the introduction of the ATM circuit into the existing network. A useful beginning is to start by drawing diagrams. The simplicity of a network diagram is a good measure of its usefulness. Complicated network diagrams are a strong indicator that the implementation is either not well thought out or will require too much effort.

Another useful technique is to draw up multiple scenarios to force oneself to approach the problem from different angles. A stepwise implementation through the scenarios allows the careful recording of implementation issues and details. The physical connectivity and network configuration are intricately interdependent and must be considered simultaneously. This complicates the conception of implementation scenarios. Again, the general rule of thumb here is "Keep it simple".

Another administrative issue that one will not find in the ATM literature is that in a research situation where the ATM hardware is managed by a research team and the campus network managed by a dedicated IT staff, there is bound to be plenty of opportunity for network configuration contention. Fortunately, this can be overcome by inviting all involved parties to the table from the very beginning. This involves choosing and purchasing the hardware as well as planning the actual integration of the ATM circuit into the campus network.

Administrative Effort at UWC

At UWC, the administrative effort for the CoE ATM graft has mostly included the steps outlined above. The ATM hardware was purchased by the CoE with the help of the UWC ITS staff. Upon embarking on the initial stages of planning the graft integration, we attempted to involve all of the involved parties from the CoE, ITS, and the hardware vendor. From this team came the network diagrams, then the scenarios, and at last, the implementation of a scenario and the subsequent observation and tracking of the scenario's successes and failures. Most of this effort is shown in the figures scattered throughout the paper and detailed in Scenarios section below.

Scalability

There are two levels of scalability to consider with an ATM graft: local and external. Local scalability refers to adding nodes to the ATM circuit on campus. Depending on the hardware, this can be both a hardware capacity problem and an exercise in daisy-chaining. These issues are very similar in nature to the usual LAN considerations, such as the number of connections in a hub or switch. In the ATM world, fiber ports tend to be quite expensive. There are only a limited number of optic ports in the core switch. The number of core switch ports limits the number of hubs. In a direct connect ATM circuit, it is possible to chain ATM adapters at the machine level as well. From a practical standpoint, the issue of local scalability is more an issue of budget than physical connectivity.

External scalability, on the other hand, refers to connecting the local ATM circuit to other ATM circuits on an ATM backbone. To scale externally, an ATM graft configuration has to handle connecting to other similarly configured networks. Initially, it may seem that external scalability is a different league, but actually when the issues are worked out at the local level, they should scale up. Obviously, the problem of multiple Internet connections and the IP addressing scheme looms largest with external scalability. The first step towards external scalability is then an elegant and comprehensive solution at the local level. Next, the most favorable circumstances would be that all ATM participants have agreed on similar , if not the same, grafting solutions.

Scalability at UWC

Throughout the grafting process at UWC, we have given careful thought to both levels of scalability. To achieve local scalability, we chose hardware to support large numbers of machines to provide room for the CoE machine count to rise. At the moment, our LANE bridges can support up to 75 machines. We also have 5 unused core ATM switch ports, of which 2 or 3 will be used for the native ATM video conferencing facility. That still leaves at least 2 open ports for up to 50 more machines with LANE bridges.

Even though UWC is not currently ATM-connected to the outside world, we still have spent much time and effort considering the problems of IP addressing and multiple Internet access points. While it has caused us a lot of anguish, having multiple Internet access points on campus has prepared us for this eventuality. Due to the restricted access to fresh IP network addresses, we have been forced to focus on solutions that are not dependent on new addresses. Such solutions will tend to be less dependent on external factors, should as the availability of network addresses as well as their costs. It is hoped that solutions that favor insulation and simplicity will scale once we obtain connectivity to other institutions in the greater South African CoE.

Grafting Scenarios

Dual IP

The Dual IP Scenario allows machines to retain their existing IP addresses and gives them a second IP address so they can communicate directly over the ATM network [see Figure 6]. ATM-connected machines use their original IP address to communicate with the rest of campus and the Internet. To stay within the ATM circuit, however, they use the second IP. It is relatively trivial to alias a single interface to multiple IP addresses on most common platforms (Win95, NT, and UNIX). We chose to use the disused ARPANET Class A 10 network for the "fake" IP addresses. The primary advantage of this scenario is that it requires minimal change to the existing topology. We must only assign the additional "fake" IPs and hook up the fiber between the LANE bridges and the core ATM switch. There is no extra hardware to buy or cabling to lay. It also obviates the need for additional hops from introducing a router. However, it does open up the ISP connection to security problems; but then so will all of the grafting solutions. Dual IPs can also be a

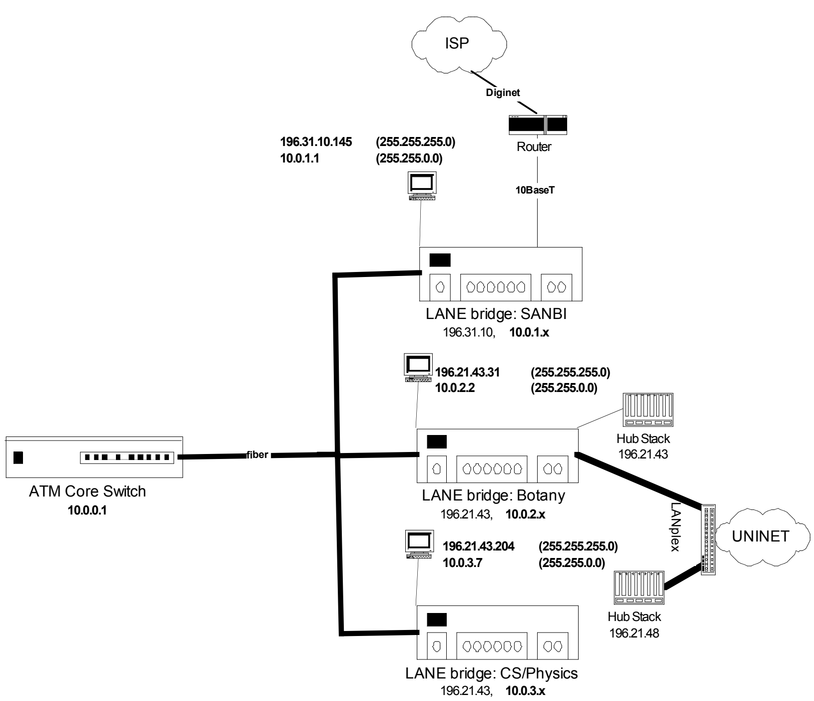

Figure 6. Dual IP with subnet masks

nightmare to administer and keep track of. This scenario also has two different deployment topologies, of which one failed miserably. The first attached each LANE bridge to its respective departmental server. As mentioned above, this crashed the campus network. The second scenario restricts access to a single point for each Internet provider. The last dual IP scenario will not scale when UWC connects to other institutions over ATM because, on a larger scale, it is unreasonable to assign Internet access to a single point.

Dual NIC

The Dual NIC (Network Interface Card, or Ethernet card) Scenario places two Ethernet cards into each box. This scenario keeps the original NIC connected to the respective Internet provider and inserts a second NIC to connect to the local ATM LANE bridge. This solution requires a nontrivial amount of additional hardware. When we introduce another NIC, we must also introduce more IP addresses. We can choose to use a "fake" IP address as in the Dual IP scenario, or perhaps acquire a valid set of network numbers. In this scenario, every machine is basically a gateway between the ATM and non-ATM worlds. Budgetary considerations put this scenario lowest on the implementation list.

Edge Routing

The Edge Routing Scenario isolates the ATM island by surrounding it with routers. Each of the three groups within the CoE retains respective network numbers and Internet connections. We still connect the research machines to the ATM LANE bridge, but we stick a router in between the LANE bridge and the Internet connection. Therefore, the machines can retain their original IP addresses, belong to a departmental domain, and still use the original default gateway to communicate to the Internet. Instead of dual IP'ing the machines, though, we assign these machines to a Virtual LAN (VLAN) with the ATM hardware. With VLAN, the LANE bridges are smart enough to keep VLAN traffic inside the ATM net (Kercheval 1997, 3Com 1997). The edge routers can also firewall and filter IPX traffic from the ATM circuit. Note that SANBI is already protected by an edge router. Only the other two LANE bridges require newly dedicated machinery.

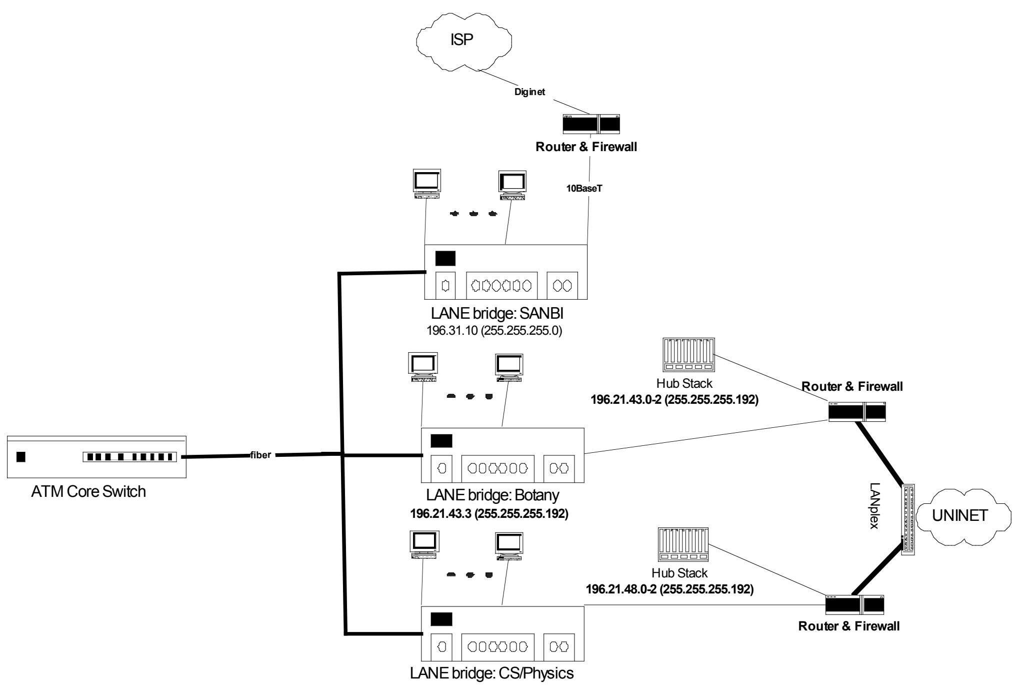

Figure 7. Edge routing with subnets and firewalling

However, there is a major snag with this approach. The ATM-connected machines belong to the same network as machines on the other side of the edge router. Without subnetting, it is doubtful that the router can handle having part of its network on either side of itself. A better solution is to introduce subnets into the local networks and put the ATM-connected machines into a single subnet separated from the rest of the network with the edge router. In this scenario, ATM-connected machines retain membership in the departmental LAN and domain. They are fully accessible from the outside the ATM circuit. The drawback to this scenario is that all of the departmental machines, CoE notwithstanding, must be reconfigured and possibly renumbered. Figure 7 shows one possible implementation using 4 subnets.

Deploying the Dual IP Scenario

We decided to first try out the Dual IP Scenario. The main reason was that two of the CoE teams had already hooked up research machines to their respective LANE bridges, and each LANE bridge was daisy-chained into a departmental hub stack. A complication arose by direct connecting fiber from the Botany LANE bridge to the campus LANplex, and connecting Botany's hub stack into one of the LANE bridge's 10BaseT ports [see Figure 3]. Overall, we didn't have to change much except to alias the network interfaces to a second IP address. This turned out to be trivial for UNIX, Win95, and NT. However, after the ATM uplinks were connected to the core switch, it appeared to crash the entire campus network. A LANE bridge (in this case a 3Com SuperStack II) provides LAN emulation at the OSI Layer 2, emulating Ethernet and effectively any protocol that runs at a higher level. At UWC, our campus backbone is Ethernet (backbone fibers to numerous UTP hubs) running TCP/IP, IPX, and AppleTalk. Broadcast packets fly through a LANE bridge onto the ATM island. The introduction of the ATM circuit into the campus network disrupted the pathways that these protocols were previously allowed to follow. In this case, we believe that the IPX traffic caused the problem, as the LANE bridges do not support the Spanning Tree protocol under ATM. The ATM graft introduced redundant paths, in effect, a loop into the network that Novell's NetWare could not handle.

A workable situation emerged when we severed one of the LANE bridge/hub stack connections [see Figure 6]. To accommodate the machines on the severed LANE bridge, we borrowed IP addresses from the network with the direct fiber connection between the ATM LANE bridge and the campus LANplex. In other words, we reconfigured such that all machines on the ATM island that want UNINET access go through a single avenue from the ATM island. This results in a functional network where broadcast IPX and AppleTalk traffic still finds its way onto the ATM island, but the traffic is tolerable, averaging 2-3% of 10Mbps bandwidth. The main disadvantage to this configuration is that some CoE teams' machines no longer belong to their departments' subnet. This topology also entails excessive routing journey to communicate with non-ATM-connected peers.

Future Efforts

Even though the Dual IP scenario is working, the next step is to introduce the Edge Routing scenario. The topology for this effort appears in Figure 7. We have decided that the costs and setup involved with the Dual NIC scenario are prohibitive and not worth pursuing. To implement the Edge Routing scenario we must first determine all parties that will be affected by subnetting and the consequent changing of subnet masks and IP addresses. Then, we must configure two machines into routing gateways so that we do not have to purchase more hardware. We can easily use NT and/or UNIX machines. The router/gateway must be able to filter IPX traffic. The filtering not only keeps unnecessary traffic off the ATM circuit, it also avoids creating a loop for Novell's IPX STP. The Edge Routing scenario seems to address all of the requirements of the UWC CoE. The issues presented in this paper point toward this type of scenario. Only a careful plan and subsequent implementation will prove its merit.

References

Black, Uyless, *TCP/IP and Related Protocols*, McGraw-Hill, 1998.
Douba, Salim, *Networking UNIX*, SAMS, 1995.
Kercheval, Barry, *TCP/IP Over ATM: A No-Nonsense Internetworking Guide*, Prentice Hall, 1997.
Lohse, Steen B., "Reliable ATM Networking", *BYTE*, April 1997, pp. 55-56.
3Com, *SuperStack II Switch 1000 User Guide*, 3Com, June 1977.