Appendix A

Residential Network Services
University of California, Irvine
White Paper Prepared for the
Graduate Student Residential Technology Committee

Past, Present and Future
Prepared by Ted Roberge
Manager, Residential Network Services
November 30, 2005

Introduction

Residential Network Services (Resnet) provides network connectivity for all University of California, Irvine residential communities. Additionally, Resnet is the first line support office for the cable television system that was recently installed.

Prior to the creation of Resnet, only three portions of the housing community were provided network access.

- Arroyo Vista – ~800 users
- Middle Earth II - ~ 900 users
- Palo Verde I - ~ 375 users

In 1998 the "Light Every Pillow" project was initiated to provide network access to every resident. After the project was started, Resnet was created. The first year Resnet was run by a volunteer student. The next year (1999) a full time position was created to provide support for the approximately 6,000 users. The position was supported by about six part time student workers.

A second full time position was created in 2002, and the student staff was increased to about 10. Present staffing remains at two full time staff, and an empty third position that is currently being advertised, and approximately 18 student workers.

After the "Light Every Pillow" project was completed, housing continued to expand, adding Middle Earth III, Mesa Court Expansion, Arroyo Vista Infill, Gabrielino Apartments and Las Lomas. The latest addition added Palo Verde expansion. The current user base for Resnet now stands at approximately 7,500 with over 9,000 devices on the network.

Staffing

Attachment (c) is an organizational chart of Housing Information Technology department, and Resnet is included. Attachment (e) is a job description of the duties and responsibilities of the student staff (Residential Network Consultants).

Service Delivery

Resnet's goal is to return or answer every trouble call within 24 hours. Trouble calls come into our office either by e-mail, on line work order, or most commonly, by telephone. This does not necessarily mean that a reported problem would be fixed in 24 hours as it may take several days to schedule an appointment if the problem needs a visit by an RNC. This standard, however, does not work well during move-in week, or if there is a major problem that generates hundreds of phone calls. With the current staffing, it is easy to become swamped, as we are every year. During the normal year, the goal easily attained.

Infrastructure

Arroyo Vista and Middle Earth II infrastructure was serviced by NACS, and network administration was handled by the Business Manager of each unit. Palo Verde was connected to the network by the one housing IT employee and several graduate students. Only bedrooms were wired, not living rooms although a couple were done where capacity allowed. The wiring for Palo Verde is the original telephone wiring, where two pairs were "borrowed" from each telephone cable. This wiring is the oldest and worst, and may be rated at Category 2. Housing Administrative Services is current looking at upgrading the wiring for Palo Verde I to install Category 5e or Category 6, and adding Ethernet connections for every bedroom and living room.

All wall jack and wiring repairs in Arroyo Vista and Middle Earth II were done by NACS except for Palo Verde.

The current infrastructure is as follows, with attachment (a) giving a graphic representation of the network, taken from a screen shot from Ciscoworks, Resnet's network hardware management system.

Core Routers – two Cisco 6513's. Resnet is actually two completely independent networks, where one router is located in Central Plant and the other at the Anteater Recreation Center LIM site. We simply refer to them as the Central Plant or ARC routers.

Further located at each core site are our two Packetshapers (Model 10000/ISP) Each Packetshaper is directly in line between our core router and NACS's core router. All traffic from Resnet passes through the packetshapers. All connections to and from our routers are Gigabit connections.

Distribution and Edge Equipment.

The vast majority of our equipment consists of Cisco Catalyst layer 2 switches such as 5500's, 2900's and 1900's at the edge. Most user connections are 10mbs. The newer buildings have newer equipment such as Catalyst 6500 layer 2 switches (Palo Verde Expansion and Arroyo Vista Infill), and 2950's at the edge. The following table is a list of all Resnet routers and switches:

Catalyst Model	Amount
1912	62
1924C	192
1924A	190
2912MFXL	4
2924CXLV	16
2950G-24	6
2950G-48	23
2950ST-24 LRE	2
2950T-24	29
5505	8
6006	1
6506	2
6513 (Layer 3)	2
Total	537

Cable Television

Campus Televideo was contracted to install a cable television system throughout all six housing complexes. Once this was complete, the system was delegated to Resnet. It was unforeseen that the system would cause over 400 trouble calls within the first few months of installation. Most of the trouble was from the original coaxial wiring and poor quality of connections, bad splitters, missing wiring and areas that were never connected. Although fairly stable at present, the CATV system still requires hours and hours of wiring maintenance and repair work by our student staff.

Resnet ramped up to become CATV knowledgeable, and needed a supply of tools, test equipment, and replacement parts for wiring. All student staff was then trained and now perform all non-warranty repairs on wiring, including addition of needed splitters, replacing bad coaxial connectors, and trouble shooting audio and video line levels. They do not, however, repair or fix problems relating to video quality, fiber optics or video amplifiers.

Maintenance and repairs

All network equipment, wall jacks, wiring, fiber optics, cross connects, and punch-down blocks are maintained by Resnet. Fiber optic repair is generally contracted out, as is installation of additional wiring, if needed. Resnet has trained all student workers to trouble shoot and repair many layer 1 wiring problems, including wire mapping, installation of switches and jumpers, and especially repairing and replacing broken RJ-45 wall jacks. Each year several hundred wall jacks are broken and need replacing. Resnet has well over 12,000 RJ-45 wall jacks. During the summer months, student workers are sent into the empty dorms and test every wall jack, and repair them as needed before fall move-in.

The two full time employees monitor and repair/replace all broken network equipment. It should be noted here that the majority of network equipment is considered "legacy", and is approaching nine years old. Most of it is unsupported by Cisco, and can no longer be purchased except from secondary markets.

Network Management

Once the Light Every Pillow project was started and users began using the network, performance was superb. Resnet was encouraging residents to bring in computers and to hook up. As time went by, it became evident that the network needed to be managed. The only system in place was Ciscoworks, which monitored network equipment, but not bandwidth. Resnet had no way of knowing who was on the network. Because of this, a registration system was needed and implemented. The registration system went through several phases, each one improving upon the previous.

- The first registration system was a simple web-based system where users would be asked to enter their personal information and their computer's hardware address. This was initially fine, however many users chose not to register, or register with false information. There was no way to validate users, or require registration. This became a problem when Resnet needed to contact a user for any number of reasons, i.e., virus infection, complaint, misconfigured device etc. At the same time, DHCP was implemented using a simple Windows NT DHCP server.
- The second registration system was modeled after a popular University's "NetReg" system. We contracted with NACS, Distributed Computing Support (DCS) to develop and maintain this system. DCS provided us with a new system that also included DHCP services. The new system, (now obsolete) directed users to a registration page before they could get on-line. This was very successful, but not without its problems. First, it was very easily bypassed, and second, was not totally compatible with Windows XP. Windows XP users would periodically be redirected back to the registration page even though they were registered. This was an ongoing problem, caused hundreds of trouble calls, and was only resolved

by having the user bypass the registration system. Further, this system was a "single point of failure".

- The newest registration system is a component of the Cisco Clean Access system, and will be discussed later.

Hardware Management

Ciscoworks 2000 is currently the system we use for monitoring the health and status of our network equipment. Using both Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP), we constantly check and monitor the health of hundreds of pieces of network equipment, minute by minute. This system, although in need of upgrading, has proven invaluable. One note of interest regarding Ciscoworks is that it can tell us the location of every hardware address on the network, including the IP address.

Bandwidth Management

After the Light Every Pillow project was implemented, a shift in bandwidth use was becoming prevalent, not only at UCI but world wide. This became know as Peer-to-peer file sharing and came in many forms, the original being Napster. As network connectivity became the norm for residents, we found that performance was beginning to suffer greatly; not only across Resnet but on the UCI Campus as well.

After months of evaluation and testing, it was evident that the amount of P2P traffic that was flowing through all of UCI's networks, including Resnet, was simply "clogging the pipe". We initially installed a Packetshaper to simply monitor what kind of traffic was flowing, and found that P2P traffic was so great that the normal uses of the network were suffering. We now have two Packetshapers and are quite successful in controlling network traffic and managing our bandwidth. Without Packetshapers, the network would be unusable and bandwidth costs would be astronomical.

Bandwidth management can also be a factor in the amount of Copyright complaints that UCI receives. Although UCI still receives complaints, we receive very few. Most can be traced to the use of Bit Torrent. We receive 1-2 complaints each week, and all initial complaints are handled by one of the two Resnet staff. Repeat offenders will be referred to the Dean of Students, although we have only had one repeat in the last four years. We do not expect this issue to go away, but by careful use of bandwidth management we seem to be able to keep ahead of the copyright complaints. There are, however, new P2P technologies that are constantly being developed that require us to stay educated and aware so as to keep our network from becoming unusable again.

The Road to Clean Access

Up until fall of 2004, many computers were infected with viruses. Although the numbers were high, these were more of a nuisance than a problem that would take down complete networks. The major turning point came with Blaster and Sasser and their variants. The development of these viruses, and the problems they caused were a quantum leap ahead of anything experienced in the past. Not only were we facing an onslaught of viruses, but these were engineered to open back doors on computers that next lead to Trojan's, worms, spam zombies and BotNet controllers by the thousands.

In an attempt to keep our network clean before Fall 2004 move in, we began a long process of communications and education to help our residents prepare their computers before arriving at UCI. An outbreak of Blaster and Sasser could be 100% prevented by users simply updating their windows operating system and running an up to date anti-virus program.

Massive mailings and e-mails were sent out prior to move in of 2004. 6,000 copies of Windows Service Pack 2 was purchased and placed in every room. Web sited developed, and workshops were held. Graduate housing was included in the distribution of the CD's and literature.

The effort failed miserably. Not only did UCI fail, but universities across the country failed in their voluntary education attempt. We were extremely disappointed. Immediately after fall 2004 move in, our network became a cesspool of infected, misconfigured and compromised computers. Literally thousands of systems were infected and we had no process to handle these except manually, one by one. As attachment (b) shows, from Sept 20, 2004 to November 5, 2004, Resnet staff disconnected over a thousand users, and for the academic year, well over 2,400.

As each incident required manual intervention, well in excess of 10,000 e-mails were generated as a result. Not only were e-mails and action required by Resnet staff, but by the affected resident, and from NACS network security personnel that do the actual monitoring and reporting of attacks, infections and security problems.

The hundreds of hours and tens of thousands of dollars required to remediate these incidents were just part of the overall picture of the negative and unacceptable performance hits the network takes. The following are some bullet points regarding these:

- Residents disconnected for lengthy periods
- Residents frustrated at being infected, many times blaming the network
- Residents (and families) unsure how to fix their problems
- Residents demanding Resnet solve this problem
- NACS and Resnet staff spending full time on the problem, to the detriment of other required work and projects
- 100% preventable
- Resident's computers and personal information compromised
- Resident's computers performing badly due to infections, including spyware and malware.
- Network performance degraded by virus activity
- Network equipment performance severely degraded by attacks, scans and probes

A solution was required that would clean up the network. Several options were investigated.

- Do nothing, or maintain the Status Quo. Unacceptable
- Remove all controls, bandwidth, registration and policies. Would revert back to the original wide open, uncontrolled network and result in chaos. Any modern network the size of Resnet must be managed and controlled.
- Education – Tried and failed
- Firewall Resnet – Collaborated with NACS and were put behind the University firewall in September 2005.
- Virus activity detection systems – Detected virus-like activity on the network and shut off the user. Although workable on the surface, did not provide much management capability. User could be shut off and we would not know who they were or why.

- Clean Access (formally Perfigo). Was tested and found to best fit our needs.

Clean Access System

We needed, and our residents demanded and deserved, a system that would prevent computers from getting on the network before they were up to date and virus checked. They deserved a system that would not simply disconnect them without interaction and explanation. Further, Clean Access offered solutions to inter-dependent systems that were part of Resnet such as registration and DHCP services. Users may sometimes get the Cisco Clean Assess Agent confused with the total system. Here are some bullet points relating to the "System", and not just to the "Agent"

- Clean Access System consists of five servers and one manager. The manager talks to each server and collects information and also disseminates data to the servers.
- Each Server runs on a Dell Poweredge 750 server. Three servers are connected to the ARC router, and two to the Central Plant Router.
- Each server runs on a Linux Redhat OS and is actually a full blown router.
- Each server handles a portion or the total network, for instance Mesa Court has its own server, etc.
- The 5th server is in development and will off-load Arroyo Vista and Middle Earth from Verano and Palo Verde servers, respectively. This will help load balance our ARC servers and keep the total users-per-server within design limits.
- Each server is a full blown DHCP server. These replaced the old registration/DHCP system, and eliminated a critical single point of failure.
- Each server is a Web Server, as is the Manager.
- Except for the initial setup of each server, all configurations, management and reporting is done via the Manager.
- Each server is connected to a router via two Gigabit interfaces, one on the user side and one on the core network side.
- CCA is compatible with the campus authentication system, making registration of computers automatic when a user logs in.
- Clean Access Agent is required to be downloaded by windows operating systems except Windows 95, which is not allowed on the network.
- Depending on the ruleset per VLAN, Clean Access requires the following:
  - All users log in with a valid UCINetID and password
  - Windows requires downloading the agent
  - Non windows require nothing more
  - Windows machines in all complexes are checked by the agent and must have Windows updates turned on and updates must be current
  - Windows machines in undergraduate complexes only are checked for an Anti Virus program and that those are updated. Four AV programs are currently supported, and if a resident needs one, we provide McAfee free of charge.
- In the event of a major Virus outbreak and infection, we can simply move graduate housing networks to a ruleset that will require a check for an Anti Virus program. We are reluctant to do so at the present time for the following reasons
  - Public outcry

- Virus infections are less of a problem now, whereas Windows operating system vulnerabilities and exploits are a huge and ongoing problem.
- Virus infected computers within Graduate Housing can individually be shunted over to a VLAN that will require an AV program and updates.
- Virus infected computers can be redirected to a website that notifies the user that they are infected/compromised

Problems with Clean Access

Clean Access was installed, tested and put into production during the summer of 2005. As with all new technologies, it was not without its start-up problems. Most unfortunately, at the same time Clean Access was put into production, other unrelated problems arose and were attributed to Clean Access. This, of course, gave Clean Access a very negative start-up reputation and soon, everything was blamed on Clean Access.

- Login problems – Many users with accounts years old were required to change their passwords. Many did not want to, but had to in order to login. After an initial time period of great anxiety, this problem faded away.
- Grayed out Login Box problem – This only happened on the one server that serviced Palo Verde and Middle Earth II. The problem was persistent, intermittent, and frustrating. Resnet staff was monitoring the server virtually 24/7, while at work or at home and late into the night. Whenever the condition arose, sometimes three to four times a day, the server required rebooting. This, of course, caused repeated outages on that particular network segment. Again, this was attributed to Clean Access, and was finally traced to one user's computer sending out "malformed packets". Clean Access was modified by the developers to prevent this, and the user notified.
- During the first weeks of Clean Access, Cisco pushed out unannounced updates, several that were not adequately tested. This finally settled down as the system was updated and made more stable. There were several instances where a server would stop working, and it was, again, the one that provided service to Palo Verde and Middle Earth II.
- Misconfigured Routers
  - Rogue DHCP servers. Although Resnet originally prohibited routers, this became an "unenforceable" policy with the popularity of small home wireless routers. A combination of events caused many routers to be set up incorrectly, resulting in them becoming Rogue DHCP Servers. In an attempt to help residents set up their routers and still be able to register their computers, Resnet published guidelines on how to set them up as Access Points. This became a double edged sword. When configured correctly, they worked great. However, any reset, power failure, or disconnect resulted in the device defaulting back to its original configuration and then became a DHCP server. We removed all guidelines for configuring wireless routers and simply state that they must be set up in accordance with manufacturer instructions. We further went on to state that we would not support any routers, and removed all policies relating to the prohibition of routers on the network. We will not respond to any trouble call relating to home routers or wireless.

- After a few weeks, we aggressively tracked down and shut off every rogue server, and the incidents of Rogue Servers has decreased to the point of them being quite rare now.
- Port Flappers – Again, this problem, (falsely attributed to Clean Access) has been around a long time, and became particularly troublesome during move in, and only in Verano Place and Palo Verde I. This is a condition where a resident sets up a router that advertises to the network that it is the "Gateway" to the network. It essentially takes the same address as our router gateway, thereby causing about 50-60% of the network traffic on that particular subnet to be misdirected and dropped. Although the actual problem with the resident's router is difficult to determine, we were really only interested in stopping the problem and restoring network performance. One instance of port flapping was caused by a user in the 5100 building in Palo Verde, and was shut of at least four separate times for the same problem; taking that whole network segment down to a crawl.
- As with Rogue DHCP servers, we were relentless in tracking down these problems and shutting off those users. Port flapping is particularly hard on our network equipment as the "flapping" condition is equivalent to a denial of service attack that causes the CPU on our switches to max out trying to keep up with thousands and thousands of requests per second. Of course, this condition can literally bring a segment of the network to a dead stop. This condition is now experienced less and less and we are carefully monitoring those particular segments to prevent this as it occurs.

Benefits of Clean Access

In spite of the problems associated with Clean Access start-up, and the subsequent bad name it received, Clean Access has been a huge success. We are very aware that there is small core of students that do not like it, will not support it, and want it gone at any cost.

In spite of this, Clean access gives our residents what they demand; a clean network. As previously mentioned, and shown by attachment (b), for the same period as last year, Resnet has had only 43 disconnections for compromised computers. The majority is in graduate housing and can be attributed to the fact that no anti-virus programs are checked for by Clean Access or required. Because of the small numbers, they can be easily handled on an individual basis as explained above.

Additionally, many problems are being routinely blocked by being behind the campus firewall, although the numbers are hard to quantify.

Several benefits are also being seen by the implementation of Clean Access. We notice that the network as a whole is running better. We are not experiencing equipment CPU overloads, and a host of other problems we find with compromised and infected machines. The balance of packets moving in and out of interfaces is almost perfect, and the amount of "bad" packets has decreased to an acceptable level. Complaints about the dreaded "lag" for gamers has stopped, and we rarely receive complaints about massive packet loss. The volume of trouble calls, both via phone and e-mail has dropped off to a record low. For instance, this past holiday weekend (Veteran's Day), when we arrived on Monday morning we only had two voice mail trouble calls and one e-mail. Two of the calls were for Cable TV.

Clean Access is working for UCI's residential network. We realize that we will always have problems keeping a network the size of Resnet running at 100%, but there is no network in the world that runs at 100%. Our outages are limited to small segments of the network, and never had we had an instance where "the whole network is down". Is there room for improvement and upgrading? Absolutely. I will cover my vision of what I see as the future of Resnet in the following section.

Part II, Resnet, A Vision of the Future.

Graduate housing with a network capable of meeting the research needs of the University

In the past, researchers would typically do research from their labs or other "on campus" facilities. Over the past several years we found that more and more graduate and post-graduate students are doing more and more research from their residences. We find that many use their home connection as an extension of their research labs, and will conduct experiments, computations and file transfers as if they were actually in their research environment.

Much higher port speeds to every user

Most of the present infrastructure is limited to 10 mbs per port. Newer equipment is not running at 100 mbs as a minimum standard, even with simply home networking equipment. Our next generation of equipment needs to be 100 mbs minimum to provide better performance for our users.

Network equipment and management that will detect and stop problems as they arise

Newer network switches and routers have built-in safeguards for many problems that never existed when out current network was designed and built. For instance:

- Rogue DHCP servers can be blocked using the newer technology in switches (DHCP Snooping). This gives the network administrator the ability to stop all unauthorized DHCP traffic at the port level.
- Newer generation of switches also are being developed to stop Virus-like activity at the port level. This would be remarkable in that individual computers would have all virus-like activity blocked before it could leave the port. Further, newer technologies can push out anti-virus definitions to keep the equipment current.
- A network that is robust so as to provide the Quality of Service (QoS) required for reliable VoIP Telephony. VoIP Quality of Service requires that all VoIP traffic move at a higher priority than other traffic, even though it is not band-width intensive. In order to have a quality voice service, all packets must move quickly to the head of the queue. (Fair Weighted Queuing). Further, in order for this to work correctly, every piece of equipment in the network must be capable of FWQing to eliminate any bottleneck. There are additional legal concerns regarding VoIP telephony. Who is liable if the network is unable to support VoIP and a resident only has an IP phone and cannot call 911? What would be the ramifications regarding the use of IP phones on a "non-certified" network when it comes to locating the caller should the need arise?

AVID capable

I feel that in order to meet the growing demands for distance learning and streaming Video we should strive for a network that is fully Audio/Video capable. Not only do the newer technologies provide full Cable TV via computer networks, it also should be capable of providing streaming or stored video from UCI or other educational institutions to the desktop. I feel that many sources of educational materials in the near future can and will be available via video feed.

A network that is secure, clean of virus activity, and firewalled.

Current network design requires firewalls, anti-virus programs, and network controls, both voluntary and required. We should look at newer technologies as they become available that would provide clean networks with an absolute minimum user interaction. We should strive for a network that simply “works” every time a user is connected. We should also explore the need to provide redundant or fail-over systems to further increase network reliability.

An Affordable Network

Of course, any network needs to be affordable. Kevin Ansel shared with us an item of interest he brought back from the 2005 Educause conference in Orlando, Florida. It seems that the number one issue across Universities and Colleges in the United States is funding for Information Technology. As we see today here at UCI, with an outdated, under funded and understaffed residential network and no funds budgeted for improvement, that we are not the only university that is facing this problem. Computing in a residential setting is a major deciding factor for all students as they decide to attend UCI for Undergraduate, Graduate or Post-graduate work. I contend that improving the residential network to meet the research needs of the University would be a positive addition to the already positive and well known advantages of attending UCI. In order to accomplish this, funding must be pursued, obtained and provided. Resources must be provided to support this in the way of adequate staffing and work space design. It is becoming exceeding difficult to keep a high level of service to such a large network with the current level of staffing and funding. We need to be innovative to be competitive, and capital investment is the catalyst for innovation.

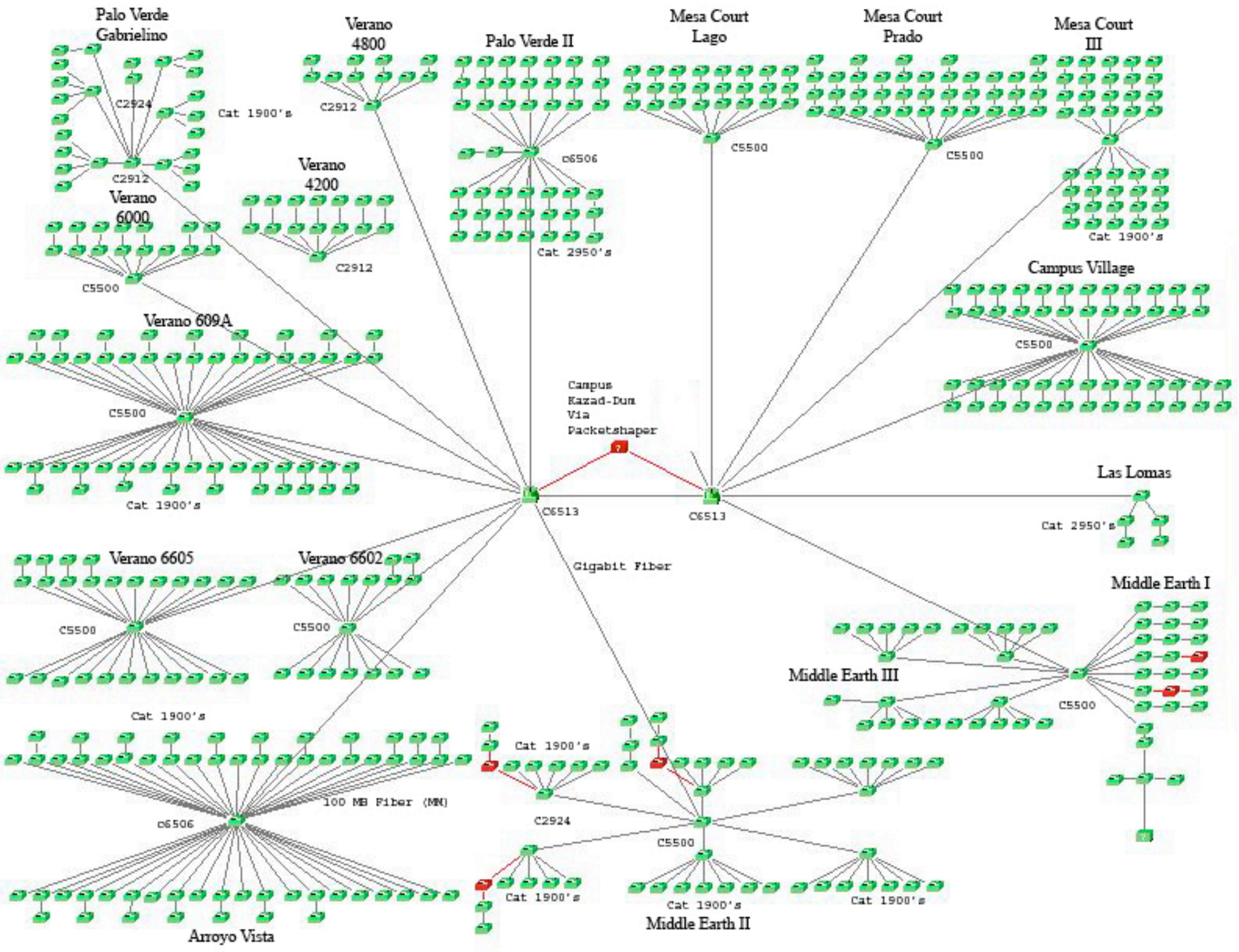
I would encourage my fellow team members to provide the committee with their thoughts and comments. I look forward to working with the committee in developing an innovative and strategic plan for the future of computing at UCI in a residential setting.

Ted Roberge

Attachments

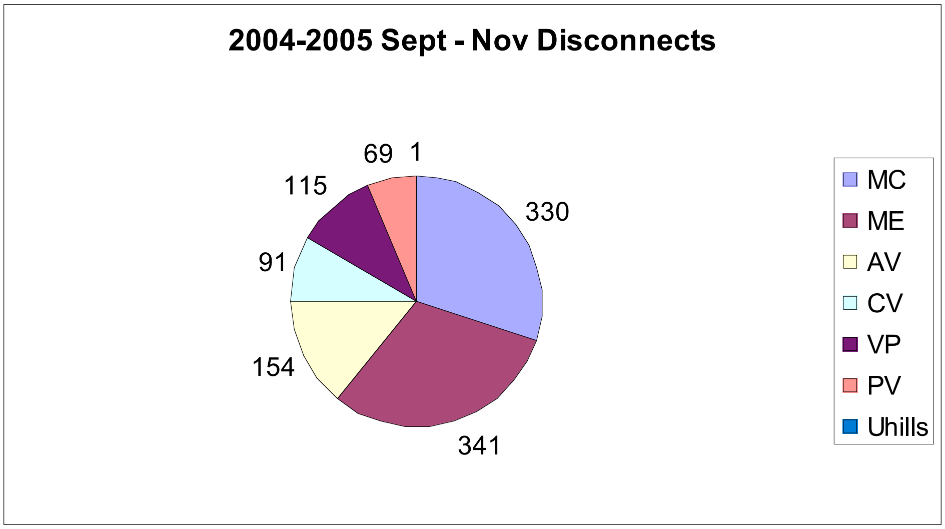
Attachment (a): Graphic of Resnet Topology
Attachment (b): Comparison charts of disconnects, 2004 vs 2005
Attachment (c): Housing IT Organization Chart
Attachment (d): Residential Network Policy
Attachment (e): RNC Job Description
Attachment (f): Performance Graphs, ARC
Attachment (g): Trouble Ticket data

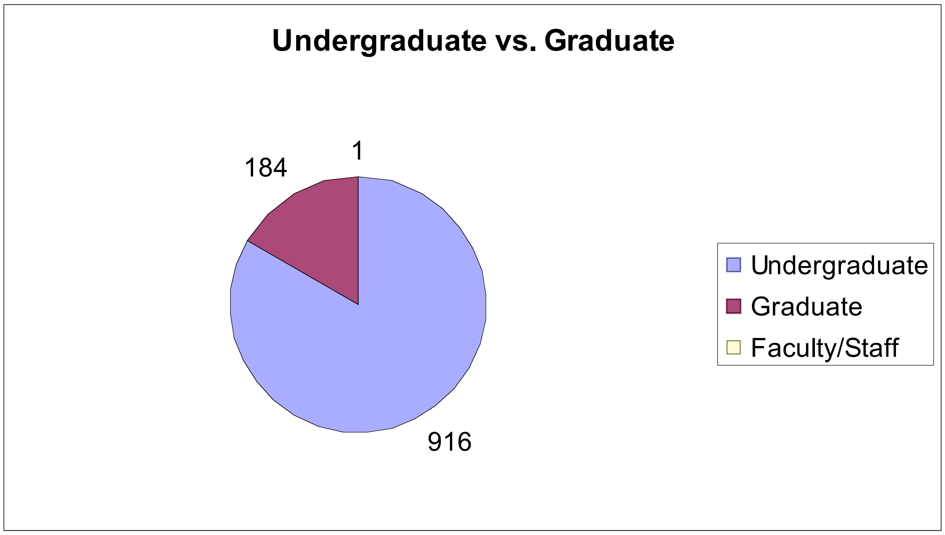
Attachment (a)



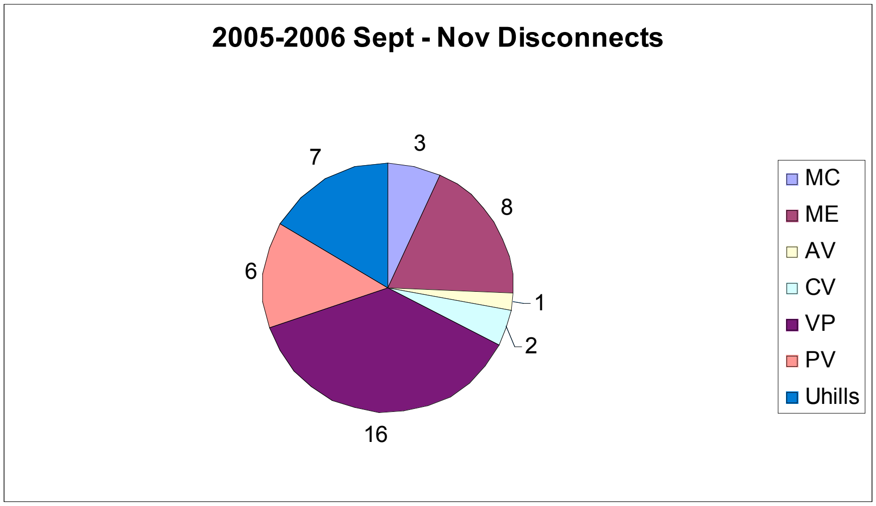
Attachment (b)

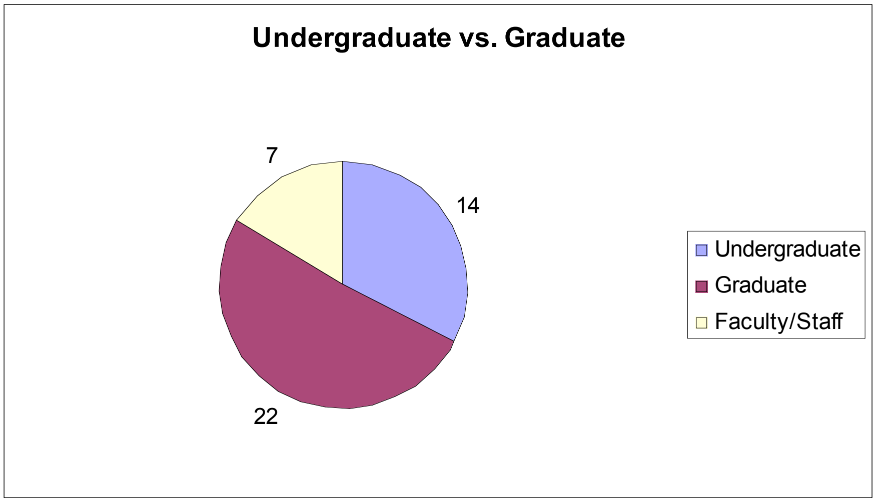
2004-2005				
Complex	**Sept. 20-30**	**October**	**Nov. 1-5**	**Total for Academic Year**
MC	193	131	6	558
ME	184	146	11	537
AV	54	89	11	339
CV	34	48	9	309
VP	27	80	8	474
PV	11	51	7	214
Uhills	0	1	0	20
	Sept-Nov Total		**1101**	44.92%
Undergraduate	465	414	37	1743
Graduate	38	131	15	688
Faculty/Staff	0	1	0	20
Total	**503**	**546**	**52**	**2451**





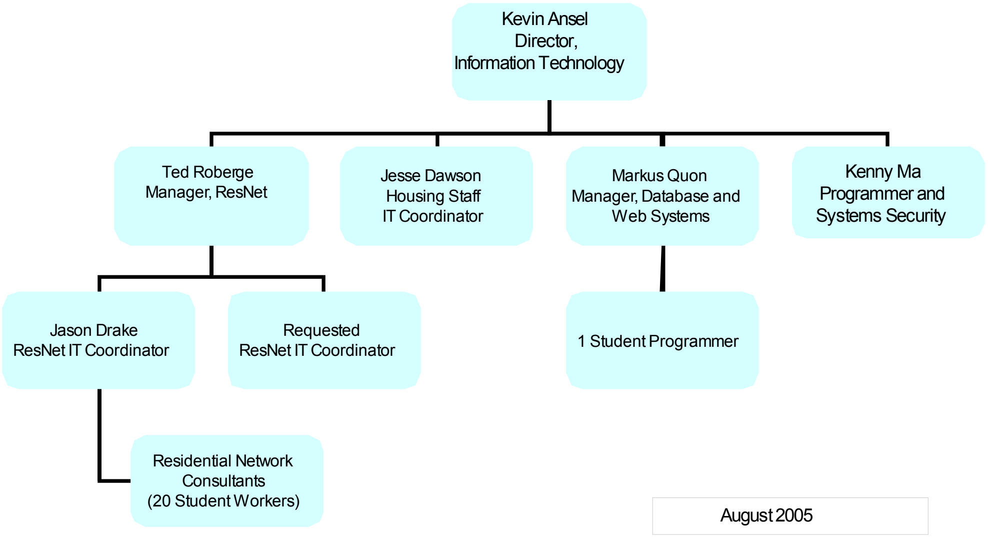
2005-2006				
Complex	Sept. 20-30	October	Nov. 1-5	Total for Academic Year
MC	0	1	2	3
ME	3	5		8
AV	0	0	1	1
CV	0	2		2
VP	5	11		16
PV	4	2		6
Uhills	4	3	0	7
Undergraduate	3	8	3	14
Graduate	9	13	0	22
Faculty/Staff	4	3	0	7
Total	**16**	**24**	**3**	**43**


2005-2006 Sept - Nov Disconnects


Undergraduate vs. Graduate

Attachment (c)

Housing Information Technology



Kevin Ansel
Director,
Information Technology

Ted Roberge
Manager, ResNet

Jesse Dawson
Housing Staff
IT Coordinator

Markus Quon
Manager, Database and
Web Systems

Kenny Ma
Programmer and
Systems Security

Jason Drake
ResNet IT Coordinator

Requested
ResNet IT Coordinator

1 Student Programmer

Residential Network
Consultants
(20 Student Workers)

August 2005

Attachment (d)

Computer Use Policy and Connection Guidelines

Bringing the World to Your Room

November 14, 2005
UCI Policy on Student Use of Computing Resources

The University of California, Irvine (UCI) provides computing resources and worldwide network access to members of the UCI electronic community for legitimate academic and administrative pursuits to communicate, access knowledge, and retrieve and disseminate information. All members of the UCI community (faculty, staff, students, and authorized guests) sharing these resources also share the rights and responsibilities for their use.

Please visit http://www.policies.uci.edu/adm/pols/714-18.html to view UCI's complete computing and Information Systems Policies.

Residential Network Acceptable Use Policy and Connection Guidelines (Revised Novenber 14, 2005)

General Guidelines

The UCI Computer Use Policy binds users of computing or communications resources at UC Irvine. (http://www.policies.uci.edu/adm/pols/714-18.html). The following information pertains to University of California, Irvine, Residential Network Services and establishes policies and guidelines specific and unique to residential computing. By connecting to the Residential Network and logging on with a valid UCINetID and password, each user understands and agrees to abide by these guidelines.

Every computer or network device on the Residential Network will be subject to the Clean Access System. Please visit the Cisco Clean Access website for more info or details.

Policies

P.07-01 Responsibility

Users are responsible for all traffic originating from their computer, including user activity, regardless of whether or not:

1. They generated it;
2. They know what they are doing, and;
3. They realize that they have violated any specific policies.

It is REQUIRED that all computers on the Residential Network;

Have Cisco Clean Access Agent, Anti Virus Protection that is updated (McAfee will be provided by UCI free of charge) and the latest Microsoft security updates (Windows operating systems only);

1. Is properly logged onto the network; and
2. Has an IP Address assigned by Resnet.

Clean Access is about having "Clean Machines" on the network. If anyone masks any computer to look like a different operating system to bypass the Clean Access Agent, the machine and user will immediately be banned from the network and disciplinary action pursued.

It is RECOMMENDED that all computers on the Residential Network that are running Windows operating systems have the following:

1. An updated version of Microsoft's free Anti Spyware program for the removal of spyware.
2. Enable windows Personal Firewall to protect the computer.
3. Change the Administrator Account to another name and use a strong password with both numbers and letters.
4. Disable the Guest Account.

P.07-02 Registration

Registration is an automatic process where all users will be directed to a simple log on screen. Users must log onto the network using their usual UCINetID and Password. (There will no longer be a registration page to enter information). If you do not have a UCINetID, you must contact NACS to activate your account or obtain a guest account. For details on registering X-boxes and other non-browser devices, please visit http://resnet.uci.edu.

P.07-03 Use of IP Addresses

All IP addresses within Resnet are assigned through an automatic process. IP addresses are dynamic, and are subject to change without any prior notice. Residents should have no expectation that their IP address will remain the same for any length of time. Under no circumstances may computers be configured with a static IP address.
Using an IP address that you have not been assigned is grounds for losing your network privileges and immediate disconnection without notice. Additionally, users may not mask the hardware address of their machines. Any computer that is found with a masked hardware address, or consisting of all zeros will be disconnected until it is reconfigured.

P.07-04 Hacking and Port Scanning

Any unauthorized attempt to access another computer is considered hacking. It doesn't matter whether the computer being hacked into is on or off campus. Any report received by the Office of Residential Network Services that a computer on the housing network attempted to hack into or scanned the ports of another will result in the immediate disabling of the network connection until the matter is resolved. Port scanning is considered by the vast majority of network administrators to be a “hostile” act and a precursor to an actual hacking attempt. In light of the recent rash of highly publicized incidents by the news media, it should be remembered that network administrators are tracking attempts to hack into their systems, and report those attempts immediately to the University when they occur.

P.07-05 Security and Privacy

Network traffic is considered private; users are completely responsible for the security and integrity of their systems. In cases where a computer is "hacked into", it is recommended that the system be either shut down or be removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. In such cases, if the owner cannot be contacted in a reasonable time the network administrator reserves the right to disable the network connection. Once the owner is made aware of the situation and agrees to take reasonable steps to ensure that the computer is not compromised, network privileges may be restored.

Any computer with shared drives or directories that are passworded are considered private, even if others that do not own the computer know the password. Accessing passworded directories without the express permission of the owner is considered hacking, and may result in permanent loss of network privileges.

P. 07-06 Server Services

UCI’s Residential Network is designed as a CLIENT network, and as such the use of servers will be carefully controlled. Computers running any type of server that uses excessive bandwidth will either be disconnected from the network or have their bandwidth limited. Examples of server services include, but are not limited to: Peer-to-Peer services (Ares, BitTorrent, Gnutella, Kazaa, DC++, Filetopia, etc) Web or IIS; FTP; Shoutcast; WAREZ; Chat; Gaming servers; and mIRC chat servers, including file servers.

From time to time it may be necessary to block or stop certain server services if they adversely affect the performance of the network, or if they become security threats.

Further, residents that are running any Peer to Peer program that is creating excessive connections on the network may be disconnected without notice. Excessive connections are defined as any computer within the Residential Network that has in excess of 500 connections at any given time to other computers off campus. Excessive connections cause problems on the network, degrades performance and efficiency of equipment, and causes slow-downs and lag for hundreds of residents.

P.07-07 Music, Movies, Software and other Copyrighted Files

It is common knowledge that many students are copying and illegally distributing copyrighted songs and movies. Please be aware that this activity is a violation of the Federal Copyright laws and you could be arrested and prosecuted in a criminal case or sued in a civil case. The University of California in no way condones or encourages this illegal activity and will take action to terminate Residential Network privileges of any resident breaking University regulations, State or Federal laws.

The University of California, Irvine is obliged to cooperate with any criminal investigation regarding these matters. Please be aware that according to copyright law, you do not need to be making a profit to be prosecuted for distributing copyrighted materials such as these Music, Movie and Software files.

P.07-08 Routers and DHCP Servers

Small home routers have become extremely popular, and as such, are allowed on our network. Routers must be set up in accordance with manufacturer instructions to work correctly. Resnet will not provide technical support for any router and it is the responsibility of each user to install and configure it correctly.

Any routing device that is misconfigured set up for home networking that assigns IP addresses to the residential network causes severe outages of the network and will be immediately disconnected.

P.07-09 Network Traffic and Bandwidth

Residential connections to the campus network are provided to allow students to fully participate in the legitimate educational and research missions of the University of California, Irvine. In general, we encourage individuals to provide useful, interesting, and inventive content to the Internet community, so long as it remains feasible for us to do so.

It may not remain feasible to provide unlimited connectivity for systems that are not strictly serving the University's missions. Because of this possibility, we reserve the right to regulate the flow of traffic on the residential network to ensure that all users receive a fair and equitable use of bandwidth. This may include Traffic Shaping, limiting or blocking certain types of network traffic. The University may also request that users reduce the amount of traffic being caused by their service, or where necessary, to remove such systems from the residential network. In all but extreme cases, we will contact the owner of the system before removing it from the network.

P.07-10 Misconfigured Services or Virus Infected Computers

There may be times when a computer is unintentionally misconfigured or infected with a virus that causes problems on the network. In order to preserve the best service possible for the majority of the users, every infected computer will be disconnected from the network immediately. We will attempt to notify the owner of the system by electronic mail that the computer has been disconnected and why.

Computers will be allowed back onto the network after the owner notifies the Office of Residential Network Services that they have reconfigured the computer or removed the virus and resolved the problem. Any computer that is infected a second time may be disconnected for two weeks, and subsequent infections may result in being disconnected for a full quarter or permanently.

P.07-11 Accounts

Some operating systems, specifically UNIX operating systems, allow the system administrator to create accounts for other users. While this is not, there are some things that should be considered. All users must be accurately identifiable. The user name field for any given account should contain the user's real name. There is no valid reason to allow a user to have a fictitious name for their account. Off-campus users with no affiliation the University of California, Irvine are explicitly prohibited from having accounts on computers connected to the residential network.

P.07-12 Commercial Use

Under no circumstances will any individual be permitted to use their network connection or computing privileges for commercial purposes. You may not advertise any commercial products. Any commercial use of University facilities is explicitly prohibited and is grounds for loss of residential network privileges.

Any computer that provides services for a commercial operation (e.g. a web site selling commercial products), provides services of a commercial nature (e.g. provides web services to Non-university users, whether or not a fee is charged), or has a domain name with a commercial designation (currently .COM or .NET) is explicitly prohibited from the campus network.

P.07-13 Anonymous Mailers and Spam Zombies

All electronic communications at UC Irvine must accurately identify the sender. Anonymous mail forwarders are prohibited. Running an anonymous mail forwarding service is grounds for removal from the residential network. This includes computers that have been hacked into and are being used as spam zombies.

P.07-14 Intentional Abuse

Systems found to be intentionally running programs that disrupt network activity or attack specific computers on the network will be subject to immediate removal and disciplinary action. The UCI Computer Use Policy further details this issue. The full policy may be found at http://www.policies.uci.edu/adm/pols/714-18.html

Attachment (e)

Residential Network Consultant (RNC) Job Description

Statement: The Residential Network Consultant is the primary computer and cable TV student support for all housing complexes. Working alone and with other network consultants, the RNC will help install, maintain, and support residential computers and residential computer networks (and where applicable residential computer labs). They will educate residents on all aspects of computing at UCI, consult with residents on computer related problems, and support in-room network connections. RNCs work directly for the Manager, Residential Network Services.

Duties:

- Assist residents with the installation and configuration of network software.
- Configure all computers to connect to DHCP server for automatic IP assignment.
- Keep office hours to answer phones, update web pages, maintain office computers, and participate in various training sessions regarding networks, hardware, and software.
- Provide consultation regarding hardware requirements to use the network.
- Troubleshoot and help correct problems related to connectivity to the network throughout all housing complexes, including Cable TV problems.
- Maintain accurate logs of **all** service requests; enter work done in the on-line database.
- Provide educational services regarding the use of network resources to enhance academic and co-curricular activities on a group and individual basis.
- Assist with the development of documentation materials, flyers and newsletters.
- Assist with special projects as may be assigned from time to time.

Requirements:

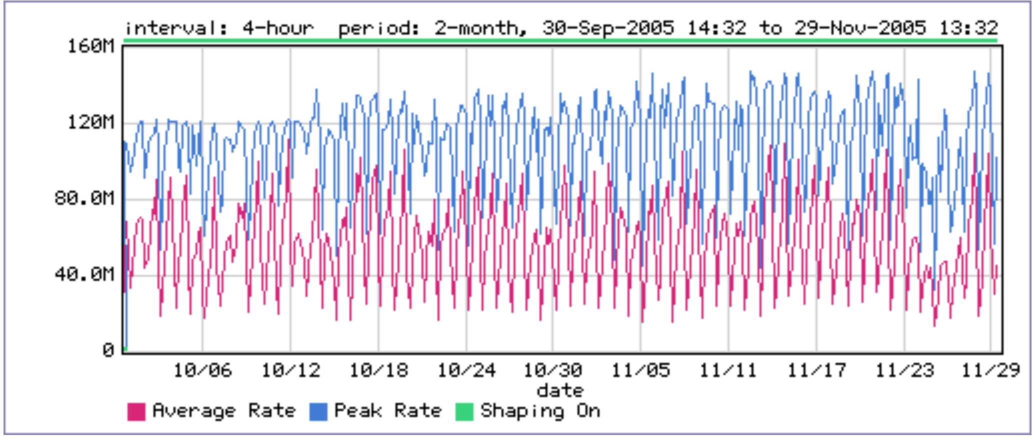
- Attend mandatory quarterly RNC meetings at the beginning of each academic quarter.
- Attend mandatory ResNet training sessions held a week prior to move in.
- Full-time UCI student, with a minimum cumulative 2.2 GPA throughout the employment period. Grades to be provided to the supervisor quarterly.
- Knowledge of networking software and configuration for both PC and Macintosh computers.
- Knowledge of UCI computer resources.
- Demonstrate full support and a working knowledge of both the University and Housing Computer Use Policy.
- Proven leadership and customer service experience/capabilities with effective telephone and personal communication skills.
- Ability to work in a professional environment and interact with a diverse population of students and staff, and to function as part of a team.

Expectations: Accept the appointment for the entire agreed upon period. Incumbents are University Housing Staff and are expected to conduct themselves accordingly. Be available for training to be scheduled just prior to move-in. Abide by all Housing and University policies. Check and respond to calls on the RNC duty voice mail line, RNC E-mail and RNC On-line work orders. Return all calls within 24 hours. Submit accurate and timely work orders. Accurately document all service calls.

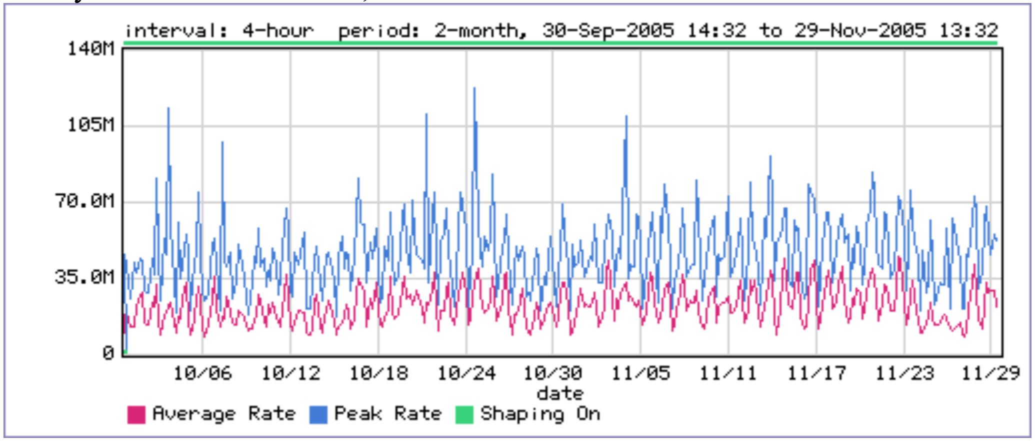
Hours: Flexible, approximately 10 hours per week. Expect more than 10 hours per week from fall move in through the winter quarter. Less hours after spring break. RNC's will work all hours for the ResNet office.

Attachment (f)

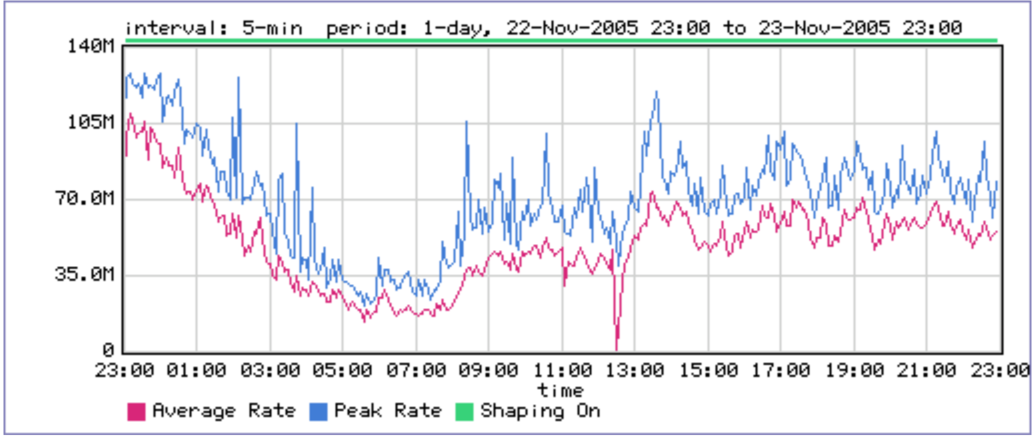
60 day inbound bandwidth, ARC network



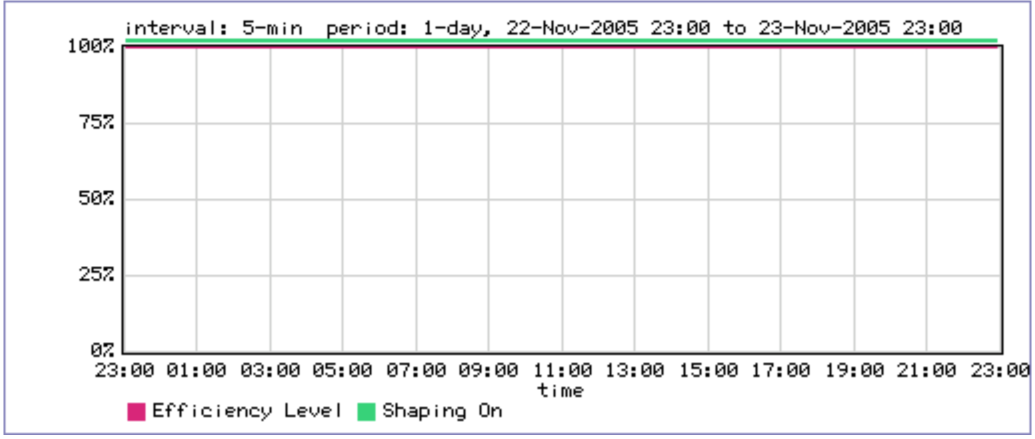
60 day outbound bandwidth, ARC network



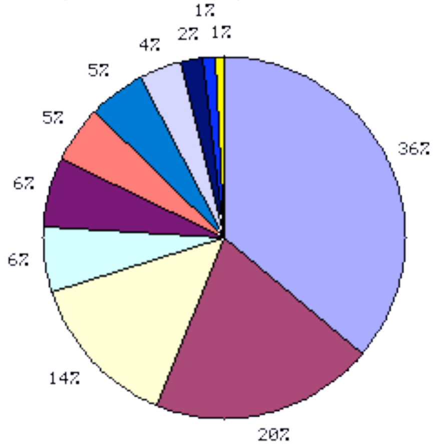
24 hour graphs for 11/23/2005 for ARC traffic, which includes Verano, Palo Verde, Arroyo Vista, and Middle Earth II, Shows outage at ~1230

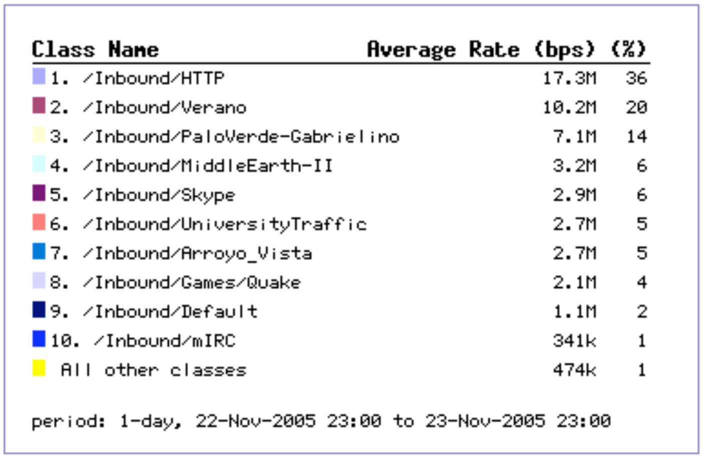


Typical graph showing network efficiency, (tcp retransmits)



24 hour graph showing top 10 classes of bandwidth uses, inbound, ARC Subnets

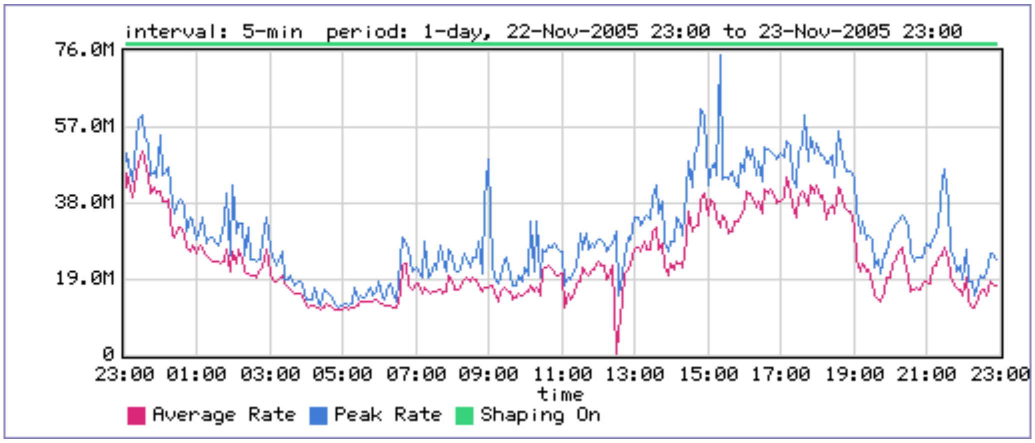




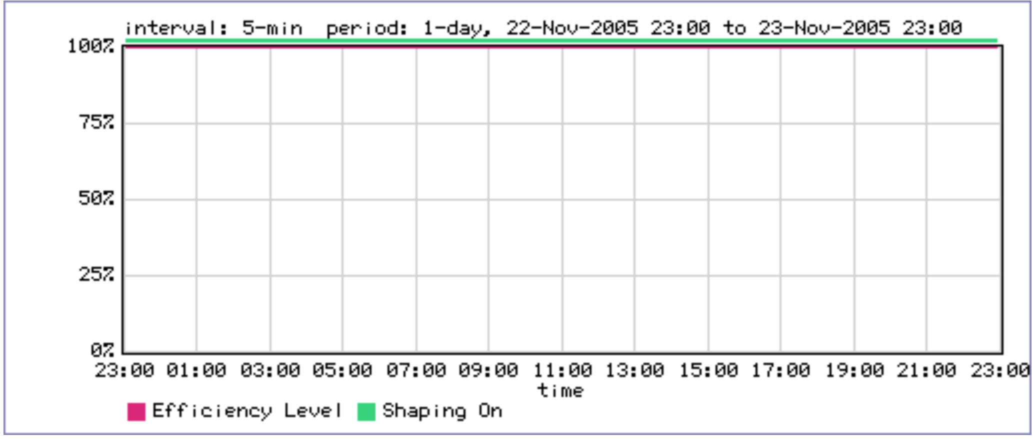
	Class Name	Average Rate (bps)	(%)
■	1. /Inbound/HTTP	17.3M	36
■	2. /Inbound/Verano	10.2M	20
■	3. /Inbound/PaloVerde-Gabrielino	7.1M	14
■	4. /Inbound/MiddleEarth-II	3.2M	6
■	5. /Inbound/Skype	2.9M	6
■	6. /Inbound/UniversityTraffic	2.7M	5
■	7. /Inbound/Arroyo_Vista	2.7M	5
■	8. /Inbound/Games/Quake	2.1M	4
■	9. /Inbound/Default	1.1M	2
■	10. /Inbound/mIRC	341k	1
■	All other classes	474k	1

period: 1-day, 22-Nov-2005 23:00 to 23-Nov-2005 23:00

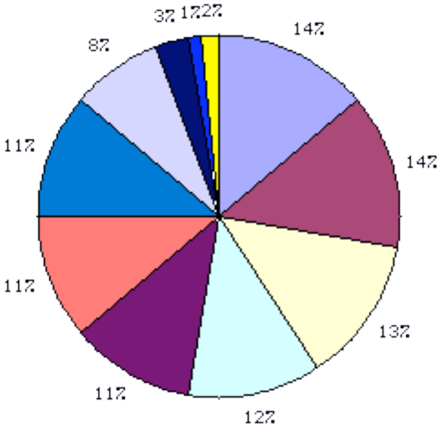
Same 24 hour graphs for 11/23/2005 inbound showing outage at ~1230 for ARC subnets

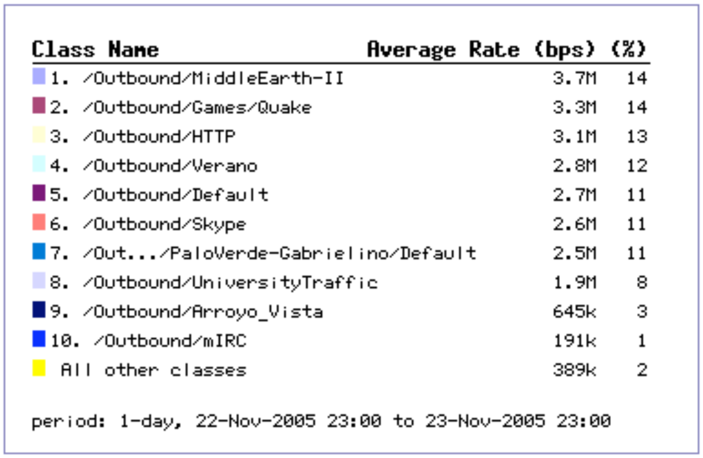


Typical graph showing network efficiency, (tcp retransmits)



24 hour graph showing top 10 classes of bandwidth uses, outbound ARC subnets





Class Name	Average Rate (bps)	(%)
■ 1. /Outbound/MiddleEarth-II	3.7M	14
■ 2. /Outbound/Games/Quake	3.3M	14
■ 3. /Outbound/HTTP	3.1M	13
■ 4. /Outbound/Verano	2.8M	12
■ 5. /Outbound/Default	2.7M	11
■ 6. /Outbound/Skype	2.6M	11
■ 7. /Out.../PaloVerde-Gabrielino/Default	2.5M	11
■ 8. /Outbound/UniversityTraffic	1.9M	8
■ 9. /Outbound/Arroyo_Vista	645k	3
■ 10. /Outbound/mIRC	191k	1
■ All other classes	389k	2

period: 1-day, 22-Nov-2005 23:00 to 23-Nov-2005 23:00

Attachment (g)

Statistics for trouble log

Report generated based on data collected from 9/1/2004 to 11/30/2005.

Total trouble tickets:	5164
Total resolved tickets:	5134
Total outstanding tickets:	30 (0.58%)

Total time spent:	972 hrs (58320 min)
Average minutes spent per trouble ticket:	11.36 min
Average trouble tickets per day:	11.37

Type of Trouble Tickets

Work Order	% of Total	Outstanding	Resolved	Total #
Network	85 %	29	4360	4389
Cable	15.6 %	1	807	808

Number of trouble tickets per complex

Complex	% of Total	Outstanding	Resolved	Total #
Arroyo Vista	10.1 %	1	521	522
Campus Village	7.8 %	3	402	405
Gabrielino Apartment	0.5 %	0	28	28
Las Lomas	2 %	0	103	103
Mesa Court	14 %	2	723	725
Middle Earth	13.3 %	1	686	687
Palo Verde	14.7 %	10	750	760
Unknown	11.3 %	5	579	584
Verano Place	26.1 %	8	1342	1350

Amount of time spent per complex (Network-Related)

Complex	% of Total	Minutes	Hours	Time / Resolved
Arroyo Vista	9 %	5260	87.67	10.1 min
Campus Village	7.1 %	4160	69.33	10.35 min
Gabrielino Apartment	0.5 %	320	5.33	11.43 min
Las Lomas	2.2 %	1300	21.67	12.62 min
Mesa Court	14.4 %	8390	139.83	11.6 min
Middle Earth	13.4 %	7810	130.17	11.38 min
Palo Verde	11.7 %	6840	114	9.12 min
Unknown	5.7 %	3300	55	5.7 min

Verano Place	20.2 %	11760	196	8.76 min

Amount of time spent per complex (Cable-Related)

Complex	% of Total	Minutes	Hours	Time / Resolved
Arroyo Vista	3.2 %	1850	30.83	3.55 min
Campus Village	0.7 %	400	6.67	1 min
Gabrielino Apartment	0 %	0	0	0 min
Las Lomas	0%	0	0	0 min
Mesa Court	1.8 %	1040	17.33	1.44 min
Middle Earth	2.2 %	1270	21.17	1.85 min
Palo Verde	2.9 %	1700	28.33	2.27 min
Unknown	0.1 %	40	0.67	0.07 min
Verano Place	5.9 %	3430	57.17	2.56 min

Statistics for disconnected log

Report generated based on data collected from 9/1/2004 to 11/30/2005.

Total violations:	3649
Total resolved violations:	3627
Total outstanding violations:	22 (0.89%)
Average violations per day:	5.46

Number of violations per complex

Complex	% of Total	Outstanding	Resolved	Total #
Arroyo Vista	13.6 %	0	521	521
Campus Village	12.6 %	3	493	496
Gabrielino Apartment	0.1 %	1	2	3
Las Lomas	0.7 %	0	18	18
Mesa Court	22.6 %	1	760	761
Middle Earth	21.9 %	4	739	743
Palo Verde	8.8 %	4	415	419
Unknown	0 %	0	0	0
Verano Place	19.6 %	9	679	688

Number of violations per category

Category	% of Total	Total #
Bandwidth Abuse	0.1 %	2
Copyright Violation	1.9 %	46
Excessive Connections	1 %	26
Misconfigured Device	6.4 %	159
Spam Complaint	2.7 %	68
Virus Infection	88.1 %	2190

Number of violations per month: 2005

298	126	142	98	79	85	71	37	49	43	15	0
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Number of violations per month: 2004

48	56	239	170	324	443	51	68	503	546	173	85
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

*Graphs not proportioned