

Pacific Net Memorandum of Understanding

Version 6.4 4/12/04

With the creation of Pacific Net, and its stewardship by OIT's Network Engineering Services (NES), it is important to address service levels. Providing reliable information technology services to meet the pedagogical and administrative needs of all University units is the overriding objective. This Memorandum of Understanding (MoU) will mutually assure the provision of high quality network services that meet Pacific's business needs. This information will enable all parties to achieve a common understanding of expectations and operations. However, the nature of modern networking, especially in a complex and security conscious environment, does not allow for service level guarantees. Therefore, this is not a service level agreement.

This is the master document. Should the requirements (logistical, technological, and/or pedagogical) of individual schools or units substantially differ from what is specified below, appropriate accommodations will be mutually agreed to and noted in this MOU or added as attachments to the MOU that override or modify the master specifications.

Definitions

Office of Information Technology (OIT), The University of the Pacific's (Pacific) central information technology services provider.

Network Engineering Services (NES). The unit of OIT charged with stewardship (i.e., engineering, provisioning (of additions, deletions, changes), management and support) of Pacific Net. NES has stewardship over all network components regardless of the initial purchaser.

OIT Systems (Systems). The unit of OIT charged with stewardship of centrally owned or co-located servers. Systems often supports central Network Applications, as defined below, and as opposed to the network itself.

Network Applications. There are certain applications that critically depend on Pacific Net. These include, but are not limited to, email, the web, video-conferencing, video distribution, streaming, and telephony applications (as Pacific moves to VoIP). Because these applications may require Quality of Service or other considerations, their performance may depend on network technical details, such as traffic prioritization.

Pacific Net or Network: The University of the Pacific's central digital data communications network infrastructure. It is further defined as all network wiring and electronics from the wall plate or equivalent demarcation point to any other wall plate or equivalent demarcation point (ex. a server room port) in any Pacific facilities on all three campuses, including the WAN, connection to the Internet or other external networks, any wireless equipment and network monitoring and/or network administration systems. This means, amongst other things, that cables and Network Interface Cards (NIC) are not part of Pacific Net, nor are systems that do not connect directly or indirectly to Pacific Net, (i.e. stand-alone systems). However, NES reserves the right to set standards for NIC cards and cables, with the approval of recommendations to the Information Technology Planning Committee.

Local Technical Support Providers (local TSPs, or TSPs) are the technical support staff, charged with supporting discipline specific applications, desktop and local server support in their respective schools or units. TSPs are envisioned as partnering with NES in the support of Pacific Net. Much of this document is intended to lay out the parameters of that partnership.

HEAT is Pacific's standard distributed help desk trouble ticketing and work management system, supported by OIT's Customer Support Center (CSC), a.k.a. the Help Desk.

Operational Understandings

1. Mutual cooperation between OIT and TSPs is assumed. OIT(including NES) and the TSPs will mutually cooperate and support each other in a timely manner within the context and limitations of this

MOU. OIT will sponsor TSP meetings on a regular basis in addition to the online TSP forum, tsp@lists.pacific.edu and ptug-i@lists.pacific.edu . OIT will discuss changes of any significance on the list and in the meetings. Significant outages will be announced on ptug-a@lists.pacific.edu . Attendance and participation is highly encouraged. Not communicated, unilateral action, including additions or changes to Network Applications, and/or unnecessary delays by OIT staff or unit TSPs will be construed as lack of cooperation.

2. Mutual Cooperation with the Units is expected. NES and the Units will make every effort to understand and meet each other's requirements. In particular, this will include the desires of the faculty, staff and students served by Pacific Net. The Units and NES will cooperate on issues including standardization efforts and operational procedures necessary to enable the meeting of obligations under this MoU. However, NES will rely heavily on the TSPs to provide an accurate appraisal of the needs of their respective Units. This implies that TSPs will truly gather and understand local needs as opposed to relying on mental models of perceived needs. Likewise, NES will not presume to know the requirements of the local units.

3. Staff coordination across campuses. NES is accountable for Pacific Net's operation, specifically meeting its user's reasonable requirements and the obligations under this MOU. Every reasonable engineering step and management control will be used to stabilize the network and reduce the need for any intervention. By scrupulous adherence to standards and significant appropriate management controls, NES will largely mitigate the distance across the Stockton campus as well as the distance between Stockton and the San Francisco and Sacramento campuses. That having been said, distance and rapid response remains a concern. NES and the appropriate TSPs will need to coordinate support as necessary to meet the reasonable requirements of Pacific Net users as specified in this MoU. NES may need to provide and train TSPs in troubleshooting procedures. TSPs and NES are expected to promptly exercise troubleshooting procedures. NES and TSPs will utilize each other as necessary to achieve MoU goals, especially responsiveness.

4. Local testing and monitoring. NES will supply the TSPs with networking tools (for example port testers). Where possible, NES will provide monitoring capability to network equipment that serves the respective units and or Pacific Net as a whole, NES will enable other capabilities as appropriate within the context and limits of this MoU to see that TSPs are successful in fulfilling their respective missions.

5. TSPs will provide 1st level troubleshooting. It is expected that end-users in units with TSPs will call them first to ensure the validity of network issues or alleged outages. TSPs will then contact NES by phone and/or via HEAT ticket.

6. Support incidents. In the event that a reported network problem is alleged not to have been resolved within the parameters of this MoU, there will be an investigation by NES management to determine the root cause. This determination is not to assign blame. It is mutually understood that human error can and does happen from time to time. Once the root cause has been determined, such determination will be reported to the administration of the impacted units. Procedures or processes may be changed, engineering solutions may be implemented and/or changes may be made to the MoU. However, human error may result in additional training and repeated human error may be grounds for corrective action. The idea behind this approach is to mitigate or eliminate similar future support incidents.

7. TCP/IP is the only supported protocol on Pacific Net. Legacy systems using non-IP connectivity may be accommodated during their conversion to IP or phase-out.

8. No NIC card or application support. NES is responsible for troubleshooting IP connectivity issues to the port level in consultation with TSP's. NES will not be able to diagnose NIC card issues or application level issues. NIC card and application issues are the sole responsibility of the system and/or application owner and/or local TSPs unless the network is considered to be a Contributing Factor.

9. Contributing Factors. In order to manage and secure modern networks, certain network traffic based activities may be temporarily or permanently prohibited or throttled. Network security hardware and software is becoming increasingly aware of the nature of network activity and increasingly intervening in an active manner. In addition, personal firewalls or server/client based intrusion prevention software may interact with network traffic. The result is that static and dynamic network rules may affect applications and computer systems in complex ways. NES will work closely with OIT Systems and the TSPs to mitigate and/or eliminate adverse interaction, but interference should be expected from time to time.

Certain key services, such as DHCP or DNS, while not strictly speaking part of Pacific Net, are considered for the purposes herein to be possible contributing factors, even though they are the responsibility of OIT Systems. NES and OIT Systems will work closely with the TSPs should contributing factors be added, deleted or changed.

10. Provisioning (port adds, changes, deletes). Provisioning with, or over, existing infrastructure will occur in accordance with the prioritization guidelines (paragraph 27). Phone calls or email may follow, but will not substitute for notification. Provisioning that requires additional or altered infrastructure will occur as soon as cabling and switch space is made available, but typically not more than 5 business days from the date of work order entry into HEAT. Units requesting provisioning must give NES sufficient notice as actual time to install may rely on contractor or other third party availability. NES is the sole avenue for provisioning; working with TSPs and appropriate unit administrators, to ensure that all critical University needs are met. TSPs will request provisioning, including new ports, port activation (except as outlined below), DNS (a responsibility of OIT Systems, not NES) and IP translation requests, by entering a HEAT ticket.

11. Un-planned port activation (Law and Dental only)

- a.) TSPs will contact NES for emergency port activation, 24 x 7.
- b.) TSPs can obtain any necessary cabinet keys from Public Safety.
- c.) TSPs will install a temporary cable, to activate a port, with a label on each end.
- d.) TSPs will submit a HEAT ticket with Cable, Jack, and Port number.
- e.) NES will replace the cable based on HEAT ticket priority.

NES will perform a wiring closet/cabinet audit at least annually to insure procedure adherence and documentation accuracy. The CIO recommends that all ports reasonably expected to be used, be activated (especially in new construction or renovation) and left activated to avoid this scenario.

12. Cost of provisioning. The costs associated with provisioning will be borne by the requesting unit. It is assumed that major provisioning costs will be included, in good faith, within the project cost of renovation and new construction. However, when simply adding a port that does not require additional wiring but requires additional port capacity, NES, at the requesting unit's option, may charge (one-time only) for the port at an annually established per port rate. This is as opposed to the unit buying a whole switch. The Pacific Net MUR will cover the rest of the cost of the unused switch ports. Under this option, NES, at its expense, may reallocate ports over equipment or substitute equipment as it sees fit to meet demand, avoid the purchasing of additional equipment, and/or lower cost to the University.

13. Physical access to buildings and wiring closets. Physical access to all buildings and wiring closets containing Pacific Net components on all University campuses shall be available to NES staff, or their authorized contractors or representatives at all times, within 15 minutes of on-site notification. Keys and alarm codes to secure areas typically accessed in the support of Pacific Net will be maintained on the respective campuses within their respective Public Safety/Security offices and with the appropriate TSPs or their management. Authorized individuals will contact the appropriate campus personnel prior to accessing alarmed areas for alarm deactivation, keys, badges, or access cards. Individuals provided access are further responsible for ensuring that all secured areas are resecured upon any departure and that all alarms are reset (or will be reset) and keys/badges/access cards returned whenever an absence greater than 2 hours occurs. NES is the administrative authority for access to network cabinets (not closets or areas) securing Pacific Net equipment, but NES shares that authority if said cabinets contain non-Pacific Net equipment.

14. Access and configuration restricted. NES, to insure consistency and fidelity of the network, may restrict access to Pacific Net equipment and/or configurations. NES will make every attempt to put systems with fine grained authorization in place to enable TSPs to perform necessary functions.

15. External network equipment prohibited without NES authorization. In order to insure the integrity and manageability of Pacific Net, the attachment of external network equipment, including, but not limited to, hubs, switches, routers, hardware firewalls, and wireless equipment, to the production parts of Pacific Net, is not permitted without prior authorization by NES. Ports supporting unauthorized devices may be disabled or Machine (MAC) Addresses blocked immediately if network performance or management is jeopardized. Otherwise, NES will attempt to notify TSPs, where they exist, prior to any such disconnection.

16. Network experimentation and experimental networks. It is expected that units wanting to experiment with network technology work with NES to arrange for a suitable venue, perhaps even an

experimental network or VLAN. It is expected that units will not offer production services on experimental/test networks, but work with NES, as appropriate, to migrate support of new technology to NES.

17. Standard equipment uptime. NES, as a normal part of provisioning, will supply UPS power systems to support Network components for 40 minutes in the event of electrical power outages. If a unit has additional uptime requirements, they must arrange for the additional provisioning through NES and bear the additional cost.

18. Maintenance and upgrades. At any given time, existing Pacific Net components, including wireless and security components, are the responsibility of NES and costs will be covered by the Pacific Net MUR. Maintenance and upgrade does not include replacement due to theft or inflicted damage, except where due to NES negligence.

19. Port failures. Port failures verified by a TSP, will be addressed in accordance with the prioritization guidelines (paragraph 27). A call directly to NES will assist in moving this forward, but does not establish the notification time. Unverified port failures may take longer to resolve.

20. Emergency port failure procedure (Law and Dental only)

- a.) TSPs will contact NES of a port/switch failure 24x7.
- b.) NES and/or the TSPs will troubleshoot the port.
- c.) If NES has confirmed a physical port/switch failure, TSPs can obtain any necessary cabinet keys from Public Safety.
- d.) TSPs can move the cable from the failed port to a different port, if available.
- e.) TSPs will document the cable, Jack, and port number in a HEAT ticket for port repair.
- f.) NES will proceed to repair based on HEAT ticket priority.

NES will perform a wiring closet/cabinet audit at least annually to insure procedure adherence and documentation accuracy. NES recommends that two jacks on multiple-jack plates be activated to avoid single port dependency.

21. Service degradation. Reports of service degradation should be verified by a TSP and recorded in Heat with the appropriate priority. However, due to the wide ranging causes of service degradation and the complexity of modern networks, there is no guaranteed time to resolution. Degraded service, in and of itself, does not count as network downtime. However, NES will make every effort to address service degradation because units and users may not be able to distinguish between degradation and outage.

22. Wireless access point failure. Such failures, when verified by a TSP, will be addressed in accordance with the prioritization guidelines (paragraph 27). A call directly to NES will assist in moving this forward, but does not establish the notification time. Unverified wireless access point failures may take longer.

23. Manually managed wireless access points. NES recommends that all wireless access points be left fully functional. However, it is understood that some faculty members prefer to turn off wireless access during class. This gesture will become increasingly futile as more and more services (like email and web browsing) are available from the public wireless network that cannot be switched off. OIT recommends classroom management by policy rather than through toggling the equipment. Access points that TSPs designate as manually managed cannot be monitored by NES.

24. Service priority. OIT is expected to respond to problems within a timeframe appropriate for the severity of the problem reported. In the HEAT database, the severity of the problem determines which priority the problem is assigned (between 1- Mission Critical and 5- Informational). Escalation procedures exist to ensure that calls are both assigned and acknowledged quickly upon initial request, and that management is notified of problems that may have exceeded acceptable acknowledgement times. These procedures are especially intended to ensure that requests by TSPs are quickly acknowledged and resolved. These procedures are designed around HEAT's Business Process Automation Module (BPAM) which sends e-mail notifications based on certain problem criteria. Though BPAM is the primary tool for e-mail notification, OIT technicians and TSPs should regularly check HEAT's Alert Monitor as well as Call Logging for new assignments. Email notification will be made to TSP's originating any HEAT work orders to provide updates of any status changes to those work assignments. Note that failure of OIT and/or NES to contact HEAT requestors due to user inaccessibility will not count as adversely affecting OIT/NES performance. The use of cell phones is highly encouraged. Note that service to Priority Four and Five may

be suspended during critical times of the year (registration periods, fiscal year end, back to school days, etc.)

25. Classes in progress. It is NES's recommendation to not trouble shoot technical problems in a classroom or lab while class is being taught in that facility. However, if the teaching faculty member desires immediate in-class assistance, the procedure below should be followed. Classrooms, labs, AV equipment and equipment brought in by faculty and staff should be checked PRIOR to the start of class to avoid delays and potential embarrassment. Faculty and staff should be reasonably prepared to use alternative facilities equipment (ex. alternate active ports on the plate), access methods (ex. wired or wireless), or manual processes (ex. stored pages) in case of an IT failure during class. There is no guarantee that an in-class networking problem can be solved fast enough to enable the class to continue with on-line operations.

26. Emergency procedure for classes in progress

- a.) Faculty member contacts TSP. Faculty members are not to call NES.
- b.) TSPs will contact NES.
- c.) NES and the TSPs will troubleshoot the connectivity problem.
- e.) TSPs will document the incident in a HEAT ticket, after the fact.
- f.) NES will proceed, if necessary, to permanently repair based on HEAT ticket priority.

27. Priority definitions. The priority definitions below represent goals for monitoring service levels. As previously stated, diverse factors prevent guaranteed service levels. To get faster response, NES, on an incident by incident basis, may request and authorize others, including users and/or TSPs to assist in the resolution of problems. NES has responsibilities under this MoU, but intends to partner with the TSPs wherever possible and appropriate.

Priority One – Critical

Network failures or outages, including contributing factors, affecting a large group of people, an entire unit, a whole computer lab or the entire University, largely interfering with the mission of teaching, learning, research and administration on a wide scale. This could, for example, be due to one or more attached machines affecting all or large parts of Pacific Net, or a failure of a major network component. It is the goal of NES to investigate and resolve all priority one issues immediately, 24x7.

Priority Two – Urgent

Network failures or outages, including contributing factors, affecting an individual or small number of individuals, largely interfering with their ability to fulfill the mission of teaching, learning, research and administration at an individual level, including instructing a class in a smart classroom. Such failures may result from a failed network port, wireless access point or localized network component. Individual machine compromise due to a Virus/Worm is included. It is the goal to acknowledge the problem within HEAT and contact the User within 15 business minutes. It is the goal of NES to offer a temporary solution within 30 business minutes. It is the goal of NES to resolve the issue permanently within 2 business hours.

Priority Three – Important

Network issues causing a single user application failure or a network printing failure. It is the goal of NES to acknowledge the problem within HEAT in 30 business minutes, and notify the user within 90 business minutes. It is the goal to resolve these problems or provide a temporary solution within 4 business hours, with permanent solution within 2 business days.

Priority Four – Foundational

Port management issues including activation due to installs or office moves. It is the goal of NES to acknowledge these requests in HEAT within 1 business hour and contact the user within 8 business hours. The goal is to resolve the request within 3 business days. Note that service to Priority Four may be suspended during critical times of the year (registration periods, fiscal year end, back to school days, etc.)

Priority Five – Informational

Requests for information, general questions. It is the goal of NES to respond to these requests within 8 business hours, and provide a resolution within 7 business days. Note that service to

Priority Five may be suspended during critical times of the year (registration periods, fiscal year end, back to school days, etc.)

28. Notice of network equipment or configuration changes. Changes that could impact the delivery of services to any unit of the University will be made through written or person-to-person verbal notification between NES and that unit's TSP, where they exist. In cases where emergency actions are necessary, the notification will occur within 12 business hours after the action.

29. Scheduled downtime. This will be arranged 2 weeks in advance for proactive maintenance and will be done between the hours of 3:00 a.m. Friday morning and 6:00 a.m. Friday morning. Longer blocks of time, if necessary, to be arranged with unit TSPs.

30. Notification of planned or unplanned large scale outages. Notification will be done via E-mail to a specified list of users (ptug-a@lists.pacific.edu).

31. Emergency network outages. These will be coordinated via phone and followed by Emergency Service Outage E-mail to ptug-a@lists.pacific.edu. NES will make every effort to restore service, but cannot guarantee when service can be restored. TSP's are responsible for communications within their purview.

32. NES Business Hours are from 7:30 a.m. to 5:30 p.m., Monday through Friday, official Stockton campus holidays excepted. The Stockton campus may observe Summer Hours, from 7:30 to 4:00 p.m. Monday through Thursday and 7:30 a.m. to 1:00 p.m. on Friday. However, OIT's NES, OIT's Systems and OIT's CSC will maintain an appropriate level of readiness such that any designated summer hours or school holidays are transparent to any school not observing them. HEAT tickets may be entered at any time. However, Priority Two through Priority Five requests will be responded to only during NES Business Hours.

33. Reliability goals for Pacific Net as a whole. The nature of current networking does not allow for guarantees of reliability, but reliability must be measured and tracked. During the core hours of each campus (ex. non-summer hours, weekdays between 7:00 AM and 10:00 PM, and weekends between 9:00 AM and 6:00 PM) it is the goal of Pacific Net to have 100% uptime and 0 problem-related (Priority One, Two and Three) HEAT tickets. Outside of core hours, the goal is 99% uptime. Downtime will be measured in approximate port-minutes of inaccessibility/un-usability due to verified network causes. Downtime will not include inaccessibility/un-usability resulting from suspected or actual prohibited activity.

[Rob, Greg and Paul to revise to specify the metrics and to set realistic goals. The intent is to minimize the requirement for incident justification, clarify reasonable expectations and provide verification mechanisms.]

34. Viruses, worms, Trojans, spyware and other malware. TSP's, where they exist, are responsible for keeping their unit's systems clean. The OIT CSC is available to assist, where possible and appropriate, during its normal business hours. Systems found to be threatening the network and/or engaged in illegal activity may be disconnected in accordance with the University Information Technology Policies, especially the Acceptable Use Policy (AUP). Advance notice will be given to the appropriate individual and/or TSP for AUP violations not threatening the operation of Pacific Net. Notice after the fact will be given to the appropriate individual and/or TSP for disconnections requiring emergency or immediate action. It is OIT's direction to automate anti-virus efforts to the extent possible.

35. Patch Levels, personal firewalls, security clients. TSP's, where they exist, are responsible for keeping their units systems patched and software firewalls and/or security clients, including anti-virus software, configured correctly. The OIT CSC is available to assist during normal business hours. OIT may require systems to be at patch level and or have properly configured client software before being granted to full access on Pacific Net.

36. IT Policy as it applies to Pacific Net. In accordance with Pacific's Information Technology Policies: "1) Academic and business information resources are critical assets of the University and must be appropriately protected, 2) Individual accountability must be maintained on all University computing and communications systems, 5) The integrity, confidentiality and availability of the University's information resources will be protected by logical and physical access control mechanisms commensurate with their

value, sensitivity, risk of loss or compromise and ease of recovery of these resources, 7) The University's computing and communications resources shall be used securely, respectfully, cooperatively in support of the University's mission, 10) Remote access to University systems and information will be appropriately provisioned and/or controlled to ensure required security, 11) The University will not implement any dedicated connection between the University's network and the network of an external entity prior to conducting a formal risk assessment and 12) The University will treat all of its individual User information, User activity, and User communications as Confidential Information as defined in its Information Management Policy."

37. Business continuity planning policy. According to the University IT Policies; "9) Each academic department or administrative unit that provides critical services based on information technology will document, develop, implement and periodically test continuity plans." In particular, if Pacific Net is down in whole or in part, it is expected that academic and administrative business units will fall back on their non-network dependant business continuity plans. While NES, working with TSPs and key administrators, will make every effort to ensure that Pacific Net is robust and highly available, it does not and cannot guarantee that outages significantly affecting on-going teaching, learning, research and administration will not occur. Given that in today's world where forces are actively engaged in attacking networks with the intent of denying service to their users, absolute dependence on IT in general or Pacific Net in particular is not advised. OIT and NES cannot be responsible for lack of business continuity planning on the part of the units.

38. Ancillary systems. This MoU has implications for ancillary systems just above the network level (like DNS/DHCP), at the middleware level (like network authentication systems) and at the application layer (like HEAT and e-mail). OIT, working with the TSPs, will continue to address the robustness of ancillary systems. In particular, OIT will continue to work towards centralization of key infrastructure components, architecting them, where possible, to have maximum availability.

39. Employee and Contractor Identification. All OIT personnel will visibly wear their Pacific Cards as identification when they are in any user area of any campus. Contractors and consultants should have locally issued identification so that all staff are reasonably assured that their presence is authorized. Contractors should be encouraged to identify themselves when entering an inhabited area where they intend to perform work and to enter without undue disruption to current activities. Where possible, NES will provide TSPs and/or appropriate administrators a schedule of anticipated contractor visits. NES will inform its contractors of proper security procedures relative to each campus.

40. Holes in, and changes to, the MoU. While this MOU attempts to describe a variety of specific scenarios and procedures, no single document can continuously capture all the detail in such a complex undertaking as Pacific Net. Reasonableness, communication and cooperation will be necessary where issues are not addressed by the MOU. Updates to the MOU should be expected as necessary. Review of this memorandum will be done on a semi-annual basis or as circumstance requires it. This MoU, with input from unit TSPs and appropriate administrators, may be updated by NES and/or the CIO from time to time based on changing institutional requirements and/or resource levels. After reasonable discussion with the IT leadership on the three campuses, notice of proposed modifications and, eventually, the final revision will be posted to ptug-i@lists.pacific.edu.

41. Contact list. A contact list identifying authorized technical staff and their respective areas of responsibility will be maintained by each technical department, and distributed between all technical service providers. Appropriate notification will be made regarding any relevant staffing changes or changes to staff members' responsibilities or level of authorization.