

General Schedule

The cut-over from the old IPAM system to the new IPAM system is scheduled to begin on Sunday, February 15, 2009 at 10:00am. We have set up a conference bridge at 273-8386 so all testers can communicate with the IPAM Project team during the testing. Please read carefully and make plans for the following activities.

1. Plan to arrive in your office or testing area no later than 10:30am, and plan to stay until 4:30pm.
2. Please check in with the IPAM project team by calling the conference bridge at 273-8386. State your name and your Unit so we know what Units are present and testing and what Units are not. Remain on the conference bridge to hear our instruction to commence testing. Just be sure to MUTE your phone so your local conversations will not interfere with IPAM project team communication with other testers.
3. The conference bridge is not impacted by the new IPAM system cutover. However, your HSC office IP phone is impacted. If you are unable to call the conference bridge due to an outage of your HSC office IP phone, use your cell phone. If you do not have a cell phone and your HSC office IP phone is not working, come to Communicore C3-37 and we will figure out another way to stay in contact with you.
4. Upon instruction from the IPAM project team over the conference bridge, begin executing your test plan. At this point you can leave the conference bridge if you like and return when you have a problem or have completed your testing.
5. If you encounter a device during your testing that does not appear to be getting DHCP service, execute the triage steps provided.
6. When you have successfully completed all of your testing, call the conference bridge back. State your name and your Unit and the results of your testing (completed pass or completed fail.)
7. If significant problems persist with the new IPAM system by 3:00pm, the IPAM project team will meet to discuss the prospects of resolving them on cutover Sunday, versus executing the back-out plan and rescheduling the cutover. An example of a significant problem is one or more subnets unable to get DHCP service.
8. If the new IPAM system remains in production, please plan to have a technical person on-site at 6:00am Monday morning to monitor for and respond to network access issues by your users.

We will have beverages and snacks in the HSC Security Office, Communicore 3rd floor, C3-37. So please be sure to drop by before, during or after testing.

Test Plan

General Guidelines

- Please make up a test plan prior to Sunday.
- The new IPAM DHCP services will either be working for all devices on a subnet or no devices on a subnet. If you have the situation where one DHCP device on a subnet fails to get DHCP service and another DHCP device on the same subnet succeeds, then the problem is not with the new IPAM DHCP service.
- Static devices are not impacted by the new IPAM DHCP system. Further, you won't see your static devices in the IPAM system right away. Engage your normal troubleshooting for failed static devices.
- Plan to test at least two devices in each subnet where you have presence. If two fail, try two more. If all four fail after executing the problem triage steps, inform the IPAM project team on the conference bridge right away (273-8386.) We'll need to know the subnet that is failing. If you occupy space in the same subnet as another HSC Unit ISM, feel free to make plans to leverage each other's testing.

Sample

1. Identify all the subnets where you have presence. Create a small test results table like the ones below for each subnet where you have presence. In our example, the tester has devices on subnets .42 and .45.
2. Identify two DHCP devices from each subnet where you have presence.
3. Enter the subnets, bldg & floor information, and the device names in each test results table. Identify and enter the services/servers to which you will test access. You don't need 5 as in the example, but pick most critical services if at all possible.
4. As you test a connection from the test device to the critical service, only make an entry for successful connections. Leave failures blank. They will ultimately be resolved.
5. Run through the triage steps for every failure. If failure persists with your two devices, select two more and record them in the appropriate test results table. If they fail as well, contact the IPAM Project team for resolution.

Subnet: 262.38.42		Bldg, Floor:			
	Critical Server A	Critical Server B	Dept Email Server (if applicable)	Dept Fileshare (if applicable)	Internet
ITR-BAKCH01					
ITR-BAKCH02					

Subnet: 262.38.45		Bldg, Floor:			
	Critical Server A	Critical Server B	Dept Email Server (if applicable)	Dept Fileshare (if applicable)	Internet
Research-0A					
CTRC-98					

Triage Steps

The HSC Unit technical staff will need to take the following steps to isolate a IPAM problem, differentiating it from another type of network problem, or a computer/software failure prior to escalating to the IPAM project team.

1. From the command line type “ipconfig /all” to verify DHCP ip-address:
 - a. If IP Address is = 169.*.*.* then your device is not getting service from the new DHCP service and does not have a valid IP Address to access the network / internet. Proceed to step 1.c.
 - b. If DHCP Server is not 159.178.61.125 or 159.178.81.50 then your device has not updated its DHCP parameters to reflect the new DHCP server. Proceed to step 1.c.
 - c. Type “ipconfig /renew” to try and obtain a new DHCP lease. This step forces your device to look for a new DHCP address from the new DHCP server. Repeat step 1. If you find yourself here a second time, proceed to step 2.
2. If your device still has a 169.*.*.* address, attempt connectivity from 1 to 3 more DHCP devices on the same subnet.
 - a. If one or more of the additional DHCP devices tested has valid IP and can access the network / Internet, the new IPAM DHCP service is functional for this subnet. Proceed to step 3.
 - b. If none of the additional DHCP devices tested can access the network / Internet, go to step 4.
3. It’s possible the device failing to get DHCP service is not registered in the new IPAM system. Log into IPAM at <https://ipam.shands.ufl.edu>. In the quick search enter the MAC address for the device having issues. If no results come back, register the device. Wait 15 minutes, perform step 1.c again and test again.
4. Escalation
 - a. Have one point of contact within your Unit for escalating. This way, someone in your Unit will have awareness of ALL escalated problems in your Unit and may be able to detect a pattern.
 - b. The Unit point of contact should be prepared with the following:
 - i. The computer is still getting a 169.*.*.* address, and
 - ii. The results of testing 1 to 3 additional DHCP devices on the same subnet
 - iii. The DHCP Server IP address shown upon running “ipconfig/all”
 - iv. The registration record in Proteus showing a valid MAC-pool association
 - c. The Unit point of contact should escalate the problem to the conference bridge at 273-8386.