# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY GUIDELINE

|  |  |
| --- | --- |
| Name Of Guideline: | Number: |
| **Internetworking Problem Solving** | **GDL-ENSS006** |
| Domain: | Category: |
| **Network** | **Wide, Metropolitan & LAN’s** |
| Date Issued: | Issued By: |
| **10/01/2001** | Dean Schutte, TSO Compute Service Delivery Chief, Health & Human Services Delivery Center |
| Date Revised: |
| **07/28/2020** |

**Abstract:**

The Health and Human Services Delivery Center (HHS DC) supports the Departments of Health (DOH), Human Services (DHS), Aging (PDA), Drug and Alcohol Programs (DDAP) and Military and Veterans Affairs (DMVA).

The purpose of this document is to describe how to define symptoms, identify problems, and implement solutions in generic internetworking environments.

**General:**

When there is a failure in internetworking, certain symptoms appear. These symptoms might be general (such as clients being unable to access specific servers). An internetworking expert uses specific troubleshooting tools and techniques to trace the cause of the problem. He or she then implements a solution to the problem.

**Guideline:**

**General Problem-Solving Model**

Always apply the specific context in which you are troubleshooting to determine how to detect symptoms and diagnose problems for your specific environment.

When troubleshooting a network environment, a systematic approach works best. Define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential cause (from most likely to least likely) until the symptoms disappear.

Step 1

When analyzing a network problem, make a clear problem statement. Define the problem in terms of a set of symptoms and potential causes. To do this, identify the general symptoms and then ascertain what kinds of problems could cause these symptoms.

For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might be a miss-configured host, bad interface cards, or missing routing configuration commands.

Step 2

Gather the more detailed facts you need to help isolate possible causes. Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, or software release notes.

Step 3

Consider possible problems based on the facts you gathered. Using the facts you gathered, you can eliminate potential problems from your list. For example, depending on the data, you might be able to eliminate hardware as a problem, allowing you to focus on software problems. At every opportunity, try to narrow the number of potential problems so that you can create an efficient plan of action.

Step 4

Create an action plan based on the remaining potential problems. Begin with the most likely problem and devise a plan in which only one variable is manipulated. This approach allows you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific cause of the problem will not be possible.

Step 5

Implement the action plan, performing each step carefully while testing to see if the symptom disappears.

Step 6

Whenever you change a variable, you should be sure to gather results. Generally, you should use the same method of gathering facts that you used in Step 2. Analyze the results to determine whether the problem has been solved. If it has, then the process is complete.

Step 7

If the problem has not been solved, you must create an action plan based on the next most likely problem in your list. Return to Step 4 and perform the process again. Do this until the problem is solved.

Make sure to undo any changes you made in implementing your action plan that does not result in a solution to the problem. Remember that you want to change only one variable at a time.

**Preparing for Network Failure**

It is always easier to recover from a network failure if you are prepared ahead of time. To see if you are prepared for a network failure, answer the following questions:

1. Do you have an accurate physical and logical map of your internetwork?
2. Does your organization or department have an up-to-date internetwork map that outlines the physical location of all the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, sub-networks, and so forth?
3. Do you have a list of all network protocols implemented in your network? For each of the protocols implemented, do you have a list of the network numbers, sub-networks, zones, areas, and so on that are associated with them?
4. Do you know all the points of contact to external networks, including any connections to the Internet? For each external network connection, do you know what routing protocol is being used?
5. Do you have an established baseline for your network? Has your organization documented normal network behavior and performance so that you can compare current problems with a baseline?

If you can answer “Yes”to these questions, you will be able to recover from a failure more quickly and more easily than if you are not prepared.

**Refresh Schedule:**

All guidelines and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the HHS Delivery Center Domain Leads.

**Guideline Revision Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 10/01/2001 | 1.0 | Initial Creation | DPW |
| 08/12/2002 | 1.1 | Edited for Style | Beverly Shultz |
| 08/02/2004 | 1.1 | Reviewed content – No changes | Tom Zarb |
| 07/13/2005 | 1.1 | Reviewed content – No changes | Tom Zarb |
| 11/13/2006 | 1.1 | Reviewed content – No changes | Doug Rutter |
| 02/07/2008 | 1.2 | Reviewed content & edit style | Doug Rutter |
| 09/24/2010 | 1.2 | Reviewed content – No changes | Doug Rutter |
| 02/24/2011 | 1.2 | Reviewed content – No changes | Doug Rutter |
| 12/06/2013 | 1.2 | Reviewed content – No changes | Matthew Messinger |
| 04/02/2015 | 1.3 | Changed DPW to DHS | Bob Gordon, BIS-DTE |
| 03/08/2016 | 1.3 | Reviewed content – No changes | Aamir Qureshi, BIS-DTE |
| 04/15/2020 | 1.4 | Organization Name Change | HHS TSO |
| 07/20/2020 | 1.4 | Reviewed content – No changes | Bob Gordon, HHS Network |
| 07/28/2020 | 1.4 | Signature removed | M Koerber, HHS TSO |