TCP/IP Network Security [8]

This section describes how the UNICOS multilevel security (MLS) feature is used to control access over TCP/IP connections. The *UNICOS Multilevel Security (MLS) Feature User's Guide*, publication SG–2111, describes UNICOS security features, including the UNICOS station call processor (USCP) and the Remote Queuing System (RQS). *The Network Queuing System (NQS) User's Guide,* publication SG–2105, discusses security for NQS systems.

This section describes TCP/IP network controls and TCP/IP user commands.

TCP/IP network controls
8.1

On a UNICOS MLS system, mandatory access controls (MACs) are applied for network daemon access to remote workstations or hosts and for UNICOS user processes. These controls check all user process and daemon network connections, based on the classification of the information and the classification of the remote node in the network access list (NAL).

The workstation access list (WAL) provides an additional layer of authorization control over network services. Using the WAL, an administrator can designate who can use the services of a remote host.

The network connection must pass MAC NAL checks and WAL checks. The following subsections explain these controls in more detail:

- TCP/IP NAL and WAL checks
- Network access list
- Login label
- NAL and UDB access procedure
- Workstation access list

TCP/IP NAL and WAL checks 8.1.1

TCP/IP NAL and WAL checks do the following:

- Verify that the connection's MAC label is within the remote node MAC label range, as specified in the NAL.
- Verify that the connection's security label also is bounded by the system's and network interface's security label ranges.
- Verify that the user or group is allowed access by the WAL to the requested service from the given network node.
- Record security violations in the security log.

Network access list 8.1.2

TCP/IP references the NAL for security control information about each network node.

Your security administrator (or `root` on a `PRIV_SU` system) creates a NAL entry for each remote node or network. The entry contains the Internet address, minimum security label, maximum security label, send and receive privileges, the type of security option (`basic`, `cipso`, or `none`), classification, and either the host input and output protection authorities (for `basic`) or the domain of interpretation (for `cipso`).

In Trusted UNICOS, only one label (minimum is the same as maximum) for any remote node can exist when the specified security option is `none`. The `localhost` entry is an exception to this rule.

If a remote node does not have an entry in the NAL, no communication is allowed.

Login label 8.1.3

For a connection that does not send labeled IP packets, the most restrictive security label in the intersection of the NAL, the network interface, and the user database (UDB) is given to you when you log in, as shown in the following example that concerns a user named Mary and her UDB entry.

After the connection label has been identified, the following three things are considered when setting the active MAC label and MAC label range for a session:

- Connection label range

- User's MAC attributes from the UDB, including the following:
  - Minimum level
  - Maximum level
  - Maximum compartments
  - Default level
  - Default compartments
- Login configuration value of `deflbl_as_minlbl`; this configuration value applies to all identification and authentication (I/A) mechanisms. If set, the user's default label is treated as the user's minimum label, allowing a site to define the minimum compartments. See your system administrator for more information.

The second and third considerations (MAC attributes from UDB and login configuration value of `deflbl_as_minlbl`) determine the user's allowed MAC label range. This range is used in conjunction with the connection MAC label range to determine the MAC label range of the session. This does not imply that the session range is made up of the end points of the two ranges, as demonstrated in the following example:

	User label range from the UDB	Connection label range from the NAL
Minimum	1, A, B	0, A, B, C
Maximum	5, A, B, C	2, A, B, C, D E

In the preceding example, the MAC label range for the session is as follows:

minimum 1, A, B, C
maximum 2, A, B, C

The active MAC label for the session is set to the user's default label if it is within the session MAC label range. The session's active MAC label is set to the session minimum label if the user's default is not within the session's label range.

The following list shows a UDB entry for a user named Mary on a UNICOS MLS system that is not sending labeled IP packets:

- Maximum security label is level 5, compartments A, B, and C
- Minimum security label is level 0, compartment null

- Default security label is level 0, compartment A

The network interface has a security label that consists of the following items:

- Maximum security label is level 5, compartments A, B, and C
- Minimum security label is level 0, compartment null

In addition, the NAL entry establishes the following security label for Mary's workstation:

- Maximum security label is level 3, compartments A and C
- Minimum security label is level 0, compartment null

Based on these entries, access is granted to Mary because her default security label of level 0, compartment A falls within the workstation's minimum security label of level 0, compartment null and maximum of level 3, compartments A, B, and C. The system automatically changes Mary's maximum security level from 5 to 3, because her maximum level (as defined in the UDB) exceeds the maximum level defined in the NAL for the workstation. Also, Mary can add only compartment C to her active set, because the NAL defines only compartments A and C as authorized for the workstation.

If the remote host sends labeled packets, the kernel checks the NAL and sets the specified security label to the socket. In this case, the session has the security label of the incoming packet, assuming that the label is within the security label range of the system, the UDB entry for the user, the NAL, and the network interface. You cannot change your security label while working in the session.

> **Note:** In Trusted UNICOS, the label of a login session is set the same as the label of the connection for the duration of the session. This label is the intersection of the label of the originating host and the NAL entry on the destination host. This label cannot be changed. The user is denied access if the connection label is not within the NAL entry range, the network interface label for the connection, or the user's label range in the UDB. The option `NETW_STRICT_B1` controls the label of a login session, and must be set in a Trusted UNICOS system.
>
> On a UNICOS MLS system, the label of a login session is always the same as the label of the connection if either the `basic` or `cipso` security option is used on the connection.

NAL and UDB access procedure 8.1.4

The NAL and UDB access procedures are as follows:

- For a connection not sending labeled IP packets: If access is granted, and the NAL specifies a security label that is more restrictive than specified in the UDB, your minimum/maximum security levels and compartments are made to match those specified by the NAL. The opposite is also true; if the UDB specifies a more restrictive security label than specified in the NAL, your minimum/maximum security levels and compartments are made to match those specified in the UDB.
- For a system sending labeled packets: Your security label is restricted to the socket connection's security label (that is, you cannot change your security label while connected to the socket). To establish the connection, the socket connection's security label must fall within the range defined for you in the NAL, network interface, and UDB.

Workstation access list 8.1.5

Your security administrator uses the WAL to define the users and groups that are granted access to remote services from a given remote node. The WAL also defines the services that are allowed at that remote node. The services that the WAL allows (by specification string) are `login`, `lpd`, `ftp`, `rsh`, `rexec`, `nfs` (deferred), `mail` (deferred), and `nqs`. The WAL `login` service governs interactive sessions through `rlogin` and `telnet`. The specifications `all` and `none` are also possible in the WAL.

If your workstation is not defined in the WAL, you are granted access to services. If your workstation is defined in the WAL, but your user name and group name is not listed, you are denied access to services.

TCP/IP user commands 8.2

The following subsections describe how the UNICOS MLS and Trusted UNICOS features affect TCP/IP commands:

- Remote nodes and user security ranges
- Generalized connection examples
- The `telnet` command
- The `rlogin` command

- The `remsh` command
- The `ftp` command
- The `rcp` command

For information about interface security labels on your Cray Research system, see your security administrator.

All of the examples in these subsections use the two remote nodes and users specified in subsection 8.2.1.

> **Note:** In a Trusted UNICOS system, the label of a network connection cannot be changed. The following examples apply to UNICOS MLS systems. If an example has an IP security option specified, it applies also to Trusted UNICOS systems.

Remote nodes and user security ranges 8.2.1

In the examples in this subsection, the `snoopy` and `friend` remote nodes and user security ranges are used.

The NAL entry for `snoopy` on the UNICOS MLS system called `cray` is as follows:

- Minimum security level of 0
- Maximum security level of 6
- Minimum compartment of 0
- Maximum compartment of `train`
- Class C2
- IPSO is `none`

> **Note:** This NAL definition is not allowed on a Trusted UNICOS system because hosts that do not have any IPSO security option must use only one label. The `localhost` entry is an exception.

The NAL entry for `friend` on the UNICOS MLS system called `cray` is as follows:

- Minimum security level of 0
- Maximum security level of 16
- Minimum compartment of 0
- Maximum compartments of all the compartments in the system

- Class B2
- IPSO is `cipso`

The network interface to the UNICOS MLS system called `cray` has the following limits:

- Minimum security level of 0
- Maximum security level of 16
- Minimum compartment of 0
- Maximum authorized compartments of `test` and `train`

Two users, Jack and Jill, have accounts on the UNICOS MLS system called `cray`.

Jack's UDB entry assigns him the following limits:

- Minimum security level of 0
- Maximum security level of 5
- Default security level of 0
- Authorized compartments are `train` and `test`
- Active compartments of null

Jill's UDB entry assigns her the following limits:

- Minimum security level of 0
- Maximum security level of 5
- Default security level of 0
- Authorized compartments are `train` and `test`
- Active compartments of null

Generalized connection examples 8.2.2

The following examples apply to all connection methods (`telnet`, `rsh`, `rlogin`, and so forth).

They use the previous definitions.

Example 1: Jack attempts to connect to `cray` from `snoopy` at active level 0, and active compartment `admin`.

Jack is denied access to `cray` because the interface device does not allow the compartment `admin`.

Example 2: Jack attempts to connect to `cray` from `snoopy` at active level 0, and active compartment `test`.

Jack is denied access to `cray` because the NAL states that `cray` does not allow a connection from `snoopy` with active compartment `test`.

Example 3: Jill attempts to connect to `cray` from `friend` at active level 6 and active compartment `test`.

Jill is denied access to `cray` because the UDB states that user Jill is not allowed a level higher than 5.

Example 4: Jill attempts to connect to `cray` from `friend` at active level 5 and active compartments `train` and `test`.

Jill is allowed access to `cray`.

The `telnet` *command*
8.2.3

When you use the `telnet` command to connect to a UNICOS MLS system from your remote node, you are assigned the most restrictive set of security levels and compartments from the combination of your UDB entry, the incoming host's NAL entry, and the security label for the network interface.

In example 1, Jack logs into `cray` from `snoopy`. Because his UDB entry is more restrictive for security level than the NAL entry for `snoopy`, and because the NAL is more restrictive for security compartments than his UDB entry, Jack's security environment reflects the intersection of these two entries.

Example 1:

```
snoopy$ telnet cray
Trying...
Connected to cray
Escape character is '^]'.
Cray UNICOS (cray) (ttyp051)
login: jack
Password:

Active label set to : level0,none


Last successful login was : Tue May 22 13:45:04 from snoopy

                Welcome to the UNICOS 9.0 system
cray$ spget

 permits equal 00
                none
 security level is 0
                level0
 maximum level is  5
                level5
 minimum level is  0
                level0
 authorized compartments are 040
                train
 active compartments are 00
                none
 integrity class is 0
                class0
 maximum class is   0
                class0
 active categories are 00
                none
 authorized categories are 00
                 none
cray$ setulvl 1
setulvl: New security label is
Level[1:level1] Compartments[none]
cray$
```

In example 2, Jack logs into `cray` from `friend`. Because `friend` uses the Common IP Security Option (CIPSO) method of labeling network packets, Jack's label range is constrained to a single label value, which is the label of the connection. The label of the connection is the same as the label of the session that Jack is using on `friend`. To operate at a different label, Jack needs to create a different session with the label he wants on `friend`, and initiate a connection from that session.

Example 2:

```
friend$ telnet cray
Trying...
Connected to cray
Escape character is ’^]’.
Cray UNICOS (cray) (ttyp051)
login: jack
Password:

Active label set to : level0,none

Last successful login was : Tue May 22 13:45:04 from friend

                Welcome to the UNICOS 9.0 system
cray$ spget

 permits equal 00
                none
 security level is 0
                level0
 maximum level is  0
                level0
 minimum level is  0
                level0
 authorized compartments are 0
                none
 active compartments are 00
                none
 integrity class is 0
                class0
 maximum class is   0
                class0
 active categories are 00
                none
 authorized categories are 00
                 none
cray$ setulvl 1
sh:  cannot set security label: 1
cray$
```

The label at which you log in (the default) can be modified if the connection does not use Internet Protocol Security Options (IPSO) and if the NETW_STRICT_B1 configuration parameter for the connection is not set. For example, if your default security level is 4 in the UDB but the NAL entry allows only a maximum and minimum security level of 0 for your remote node, you receive security level 0 as your default security level. To be allowed access, the UDB entry must allow the label. One exception exists. If the login configuration option deflbl_as_minlbl is not set, then users can log in at a lower label than the default label, if the default label is higher than 0.

An outgoing telnet request from a UNICOS system requires that your active security level and compartments must be within the range of levels and compartments assigned to the NAL entry for the remote node to which you are trying to connect, and must be within the range of the network interface that is used.

In example 3, Jill tries to log into snoopy. Her current security level is 0 and her active compartment is test. She is denied the connection to snoopy, because snoopy does not have the test compartment listed in the NAL.

In example 4, Jill tries to log into friend. She can connect to friend, because the NAL entry for friend supports compartment test.

Example 3:

```
cray$ id
uid=1234(jill) gid=28(trng)
cray$ setucmp test
setucmp: New security label is
Level[0:level0] Compartments[test]
cray$ telnet snoopy
Trying 128.162.121.3...
telnet: Unable to connect to remote host: Security level outside host range
cray$
```

Example 4:

```
cray$ id
uid=1234(jill) gid=28(trng)
cray$ telnet friend
Trying 234.6.12.4...
Connected to friend.
Escape character is '^]'.

4.2 BSD UNIX (friend)

login:
```

The rlogin *command* 8.2.4

Incoming and outgoing rlogin requests abide by the same rules as telnet requests.

There are two rlogin behaviors, with the configuration parameter NETW_RCMD_COMPAT in the SECURE_NET_OPTIONS configuration entry serving as a toggle between them. When you set NETW_RCMD_COMPAT, .rhosts and /etc/host.equiv provide the normal BSD functionality. If it is not set, .rhosts and /etc/hosts.equiv work in restricted fashion. For the r commands to work without a password, the following must be true:

- The host is listed in the /etc/hosts.equiv and .rhosts files.
- The remote user ID is the same as the local user ID (the -l option does not work).
- The user is not root.

In example 1 (following), Jack has created a .rhosts file on cray that allows an automatic login for Jack from friend, and the system administrator has added friend to the hosts.equiv file. The connection from friend to cray uses CIPSO, so Jack's range is restricted to a single label (level 0, no compartments), which is what Jack had on friend before he started the session on cray. The actual security label values on friend are translated on the cray into UNICOS MLS security label values by taking values from the Domain Of Interpretation (DOI) translate table that are appropriate for friend.

> **Note:** The NAL parameter of class must be C2 or higher to enable automatic login, r commands, remote printing by using lpd, and NFS clients.

In example 2, Jack has created a .rhosts file on snoopy that allows an automatic login for jack from cray. However, Jack's active security compartment (test) is not supported in the NAL entry for snoopy on the cray host.

Example 1:

```
friend$ rlogin cray
Last successful login was : Tue May 22 14:12:38 from snoopy

               Welcome to the UNICOS 9.0 system

cray$ spget

 permits equal 00
                 none
 security level is 0
                 level0
 maximum level is  0
                 level0
 minimum level is  0
                 level0
 authorized compartments are 000
                 none
 active compartments are 00
                 none
 integrity class is 0
                 class0
 maximum class is   0
                 class0
 active categories are 00
                 none
 authorized categories are 00
                 none
```

Example: 2

```
cray$ id
uid=2345 (jack) gid=28(trng)
cray$ setucmp test
setucmp: New security label is
Level[0:level0] Compartments[test]
cray$ rlogin snoopy
snoopy.cray.com: Security level outside host range
cray$
```

The* `remsh` *command

8.2.5

Outgoing `remsh` requests execute the same as outgoing `telnet` or `rlogin` requests. Your security label must be within the boundary of the host's security range, as defined in the NAL and the interface range.

In example 1, Jill tries to execute the `remsh` command to `snoopy`. She is denied access because the NAL entry for `snoopy` does not have the `test` compartment.

In example 2, Jill tries to execute the `remsh` command to `friend`. She is granted access because the NAL entry for `friend` supports the `test` compartment and her `.rhosts` file on `friend` grants her access.

Example 1:

```
cray$ id
uid=1234(jill) gid=28(trng)
cray$ setucmp test
setucmp: New security label is
Level[0:level0] Compartments[test]
cray$ remsh snoopy ls
snoopy: Security level outside host range
$cray
```

Example 2:

```
cray$ id
uid=1234(jill) gid=28(trng)
cray$ remsh friend ls
calendar       letter  pers    read    testfile
file           mbox    ows     roster  work
cray$
```

The `ftp` command
8.2.6

When transferring classified files between a UNICOS MLS system and a remote node, you should use the `ftp` command. If you use the `ftp` command from the remote node and are not running with IPSO, you can transfer files only at the default security label assigned to you at login. No mechanism exists for changing your security label within `ftp`. However, the active label when starting an `ftp` session is the label for the `ftp` session.

When you have logged into your UNICOS MLS system, set your active security label to that of the file you want to transfer, then execute the `ftp` command. If the remote node supports your security label, you can transfer the file. Files that are transferred to the UNICOS MLS system are labeled with the active security label of the `ftp` session. Also, you must be in a directory that can accommodate a file created at that label.

The following three examples illustrate use of the `ftp` command.

In example 1, Jill wants to transfer the file called `testdata` from `cray` to `snoopy`. `testdata` has a security level of 1 and the `test` compartment. Jill adjusts her security level and compartment settings to match the file's security level and compartments. She then executes the `ftp` command, but she is denied access because the NAL entry for `snoopy` does not support the `test` compartment.

Example 1:

```
cray$ spget –f testdata
 Security Values for: testdata
          level:   1
                 level1
 compartments:   010
                 test
          class:   0
                class0
    categories:   0
                none
          flags:   0
                none
cray$ setulvl 1
setulvl: New security label is
Level[1:level1] Compartments[none]
cray$ setucmp test
setucmp: New security label is
Level[1:level1] Compartments[test]
cray$ ftp snoopy
ftp: connect: Security level outside host range
ftp> quit
cray$
```

In example 2, Jill transfers the file to `friend`. The transfer is successful because the NAL entry for `friend` supports her security label.

Example 2:

```
cray$ ftp friend
Connected to friend
220 friend FTP server (Version 4.15 Sat Nov 7 15:24:41 PST 1987)
ready.
Name (friend:jill):
331 Password required for jill.
Password: 230 User jill logged in.
ftp> put testdata
200 PORT command okay.
150 Opening data connection for testdata (234.6.12.4,1035).
226 Transfer complete.
16 bytes sent in 0.022 seconds (0.71 Kbytes/s)
ftp> quit
221 Goodbye.
cray$
```

In example 3, Jill transfers a file to `cray` from `friend`. First, she changes to a directory where she can create a file with a security level of 1 and `test` compartment. The transfer is successful because the NAL entry for `friend` supports her security label and the file can be created in her current directory.

Example 3:

```
cray$ cd lev_1_comp_test-dir
cray$ spget -f .
Security Values for: .
         level:   1
                 level1
  compartments:   010
                 test
         class:   0
                 class0
    categories:   0
                 none
         flags:   0
                 none
cray$ ftp friend
Connected to friend
220 friend FTP server (Version 4.15 Sat Nov 7 15:24:41 PST 1987)
ready.
Name (friend:jill): jill
331 Password required for jill.
Password:
230 User jill logged in.
ftp> get friend.file
200 PORT command okay.
150 ASCII data connection for friend.file(128.162.82.15,1187
226 ASCII Transfer complete.
56821  bytes received in 0.58 seconds (96 Kbytes/s)
ftp> quit
211 Goodbye.
cray$ spget -f friend.file
Security Values for: friend.file
         level:   1
                 level1
  compartments:   010
                 test
         class:   0
                 class0
    categories:   0
                 none
         flags:   0
                 none
cray$
```

The `rcp` *command*
8.2.7

On a UNICOS MLS system, all files sent or received when executing the `rcp` command are accessed at your active security label. Outgoing `rcp` requests can copy files to or from the remote node. The NAL entry for the remote node must accommodate this security label. Any file that is created in this manner is labeled with your active security label.

Effect of security labels on electronic mail
8.3

The following subsections describe the effect of security labels on sending and receiving electronic mail.

To become familiar with security concepts in this subsection, see the *UNICOS Multilevel Security (MLS) Feature User's Guide*, publication SG–2111. For information about how to use the `mail` and `mailx` utilities, see subsection 5.1, page 65.

Mail is sent both locally and across the network. From a user perspective, mail sent across the network is the same as mail sent locally. In the examples in this subsection, no differentiation is made between the two. Subsection 8.3.2.3 on page 116 describes what happens to security labels on mail delivered over a network.

To illustrate how electronic mail works with systems having security labels, this subsection begins with the simplest example of using `mail`(1) and `mailx`(1). Subsequent examples become more complex, and describe how labeling and delivery of messages is affected when the security label on the mail sent to you is different from your active security label.

Sending and receiving labels are the same
8.3.1

In the simplest example, all users on the system and all network connections to the system have the same security label. Therefore, all mail is sent at that label. On this system, you can always read mail; you can always forward mail; and you can always receive forwarded mail. Editing, saving, and deleting mail follows the mandatory access control (MAC) rules for security labels and discretionary access control (DAC) considerations.

Sent mail label differs from the label of the receiver 8.3.2

The next example describes sending and receiving mail when all security labels are not the same. In this example, all users on the system can have one of two security labels, label A or label B. Label A has a level of 0 and a null compartment set. Label B has a level of 1 and a null compartment set. (All examples have the null compartment set to simplify understanding. The same rules apply to labels having compartment sets that are not null.)

Receiving mail at both label A and label B 8.3.2.1

When someone logs in to a UNICOS MLS system at label A and sends mail, the mail is delivered to your mailbox at label A. Likewise, when a sender logs in to a UNICOS MLS system at label B and sends mail, the mail is delivered at label B. Suppose that mail messages at each label were sent to you.

In this case, when you log in at label A, the following message is displayed:

```
You have unreadable mail at label 1/0.
```

This means that mail with a level of 1 and a null compartment set, that is, mail at label B, was delivered to you.

If you execute `mail`(1) or `mailx`(1), a similar message appears, and you can read the mail sent at label A. If your saved mail directory is at label A, you can save, edit, delete, and forward the mail at label A as usual.

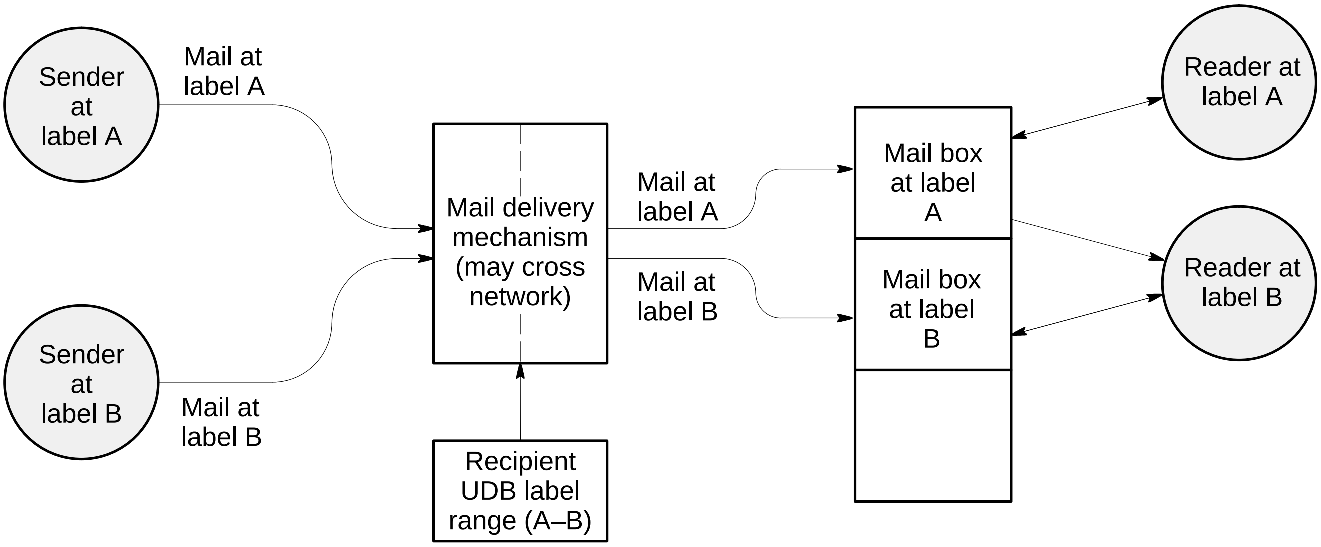
To read the mail sent at label B, you must change your security label to label B. Note that the `unreadable mail` message will no longer be displayed, since your label now dominates all mail labels.

Because you are at label B, you cannot delete the mail at label A. If you are using `mail`(1) and try to delete the mail, the mail simply stays. If you are using `mailx`(1), a message is displayed stating that the mail you are trying to delete is read-only. You must log out and log back in at label A in order to delete the mail.

If you are logged on at label B, but your saved mail directory is at label A, you cannot save either message in that directory. In order to write to that directory, you must be at label A. You can save either message in a file or a directory having label B. UNICOS MLS does allow mail to be saved in a single directory at more than one label if the directory to which you save is a multilevel directory (MLD).

If you forward a message or reply to one, the message is sent at your currently active label, which in this example is label B. Even though you receive a forwarded mail message at label A, the message is delivered at label B. To keep the message at label A, you must log out and then log in at label A. However, the opposite is not possible. If you are at label A, and receive a message with label B, you must log out and log back in at label B in order to read it.

See Figure 3 for an illustration of this example.



		Read	Edit/ delete	Reply/ forward	Save	Unreadable message
Reader at label A	Stored mail A	Y	Y	Label A	Label A	N
	Stored mail B	N	N	N/A	N/A	Y

		Read	Edit/ delete	Reply/ forward	Save	Unreadable message
Reader at label B	Stored mail A	Y	N	Label B	Label B	N
	Stored mail B	Y	Y	Label B	Label B	N

Figure 3. Functions of mail at different security labels

Mail label and your label are at several different labels 8.3.2.2

The next example involves four labels: labels A, B, C, and D. Label A is at level 0 with a null compartment set; label B is at level 1 with a null compartment set; label C is at level 3 with a null compartment set; and label D is at level 4 with a null compartment set.

The sender can log in at any of the four labels. You can log in only at labels B and C.

The sender logs in at labels A, B, and D, and sends mail at each label to you. Each mail message is treated differently, depending on its label and your active security label.

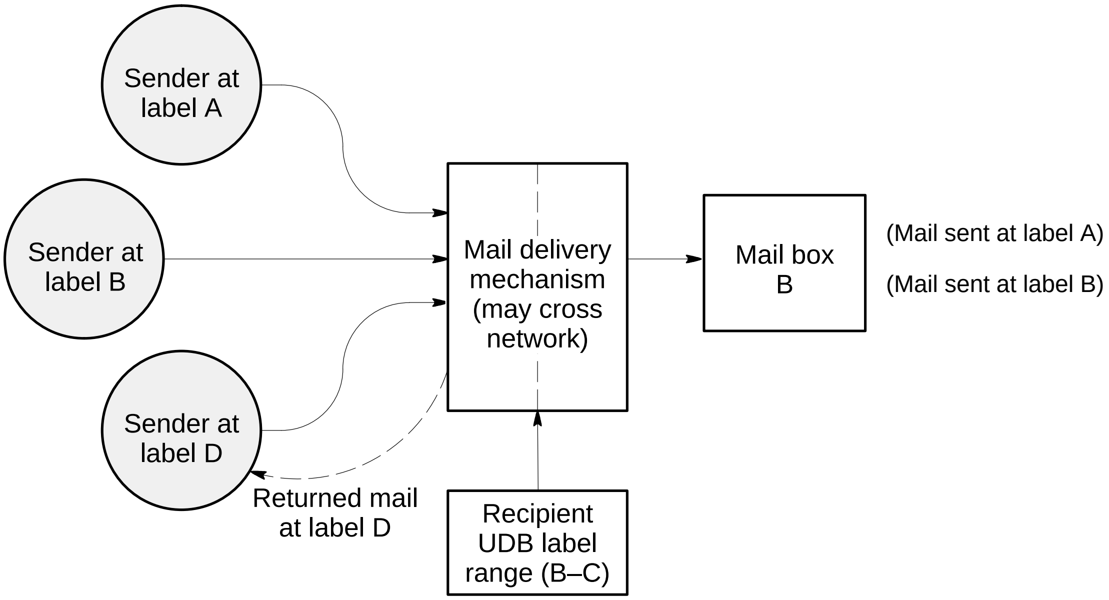
The mail at label A is outside your allowed range of labels. However, the message is dominated by label B, which is the lowest label at which you can log in. The `sendmail`(1) command, which manages mail delivery, automatically changes the label from A to B, your lowest level, which is more restrictive than the mail's label A. The mail is delivered at label B. Thus, you are assured of receiving the mail.

This label change to label B also prevents user-specified mail programs (specified in your `.forward` file or the system `alias` file) from executing on your behalf outside your label range.

The mail at label B is within your range, and is delivered at label B.

The mail at label D is also outside your label range, but in this case, your label range does not dominate the mail label. You will never be able to read or delete the message as a result. The mail is returned to the sender with the error message `User unknown`. Returning the mail also ensures that the program mailer will run only within your label range.

Figure 4 illustrates delivery of mail at different labels to you when you are logged in at different labels.



	Mail delivered	Label at which mail is delivered
Mail sent at label A	Y	B
Mail sent at label B	Y	B
Mail sent at label D	N	N/A

Figure 4. Delivery of mail at different labels to recipients at different labels

Delivering mail across the network
8.3.2.3

When delivering across the network, the security label of the incoming mail is checked against the security label ranges of the network interface and the network node (as specified in the NAL).

A connection is established across the network at the label of the mail being sent. This connection fails if the label is outside the label range of the NAL or the interface. In this case, the response to the sender indicates that the remote host could not be reached.

Figure 5 illustrates how different security labels affect mail delivery across a network.

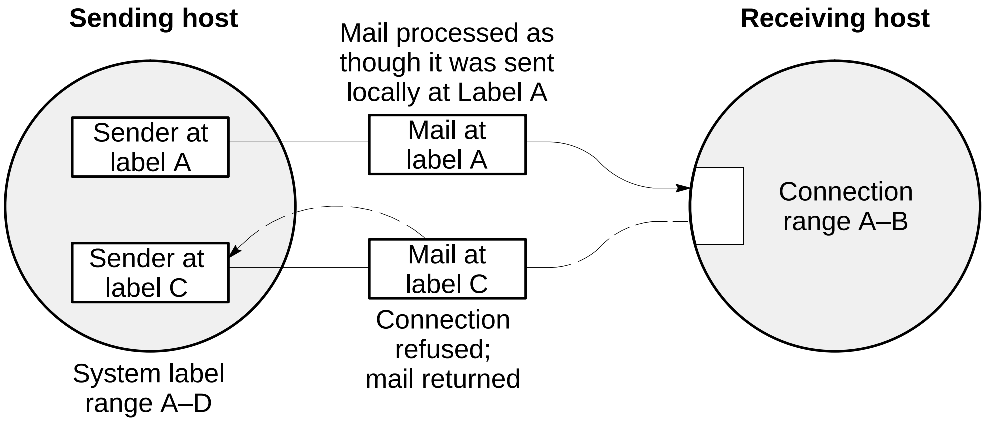


Figure 5. Mail delivery to a system with a different label range at the connection