Creating and Maintaining ONS 15454 Protection Groups (CTC Software Release 3.1 and Earlier)

Document ID: 20694

Contents

Introduction

This document describes how to create, delete and maintain various types of protection groups available on the Cisco ONS 15454. This document encompasses DS1, DS3, DS3E, DS3XM, EC1, and OCn cards and Cisco Transport Controller (CTC) software releases up to Release 3.1.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco ONS 15454

- Cisco Transport Controller Release 3.1 and earlier

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Protection Group Types

The Cisco ONS 15454 provides four protection schemes, depending on card type:

0:1

This protection scheme is also called "unprotected." Any of the ~~15454~~Cisco ONS 15454 cards may be operated as unprotected in slots 1−6 or slots 12−17. This is the default configuration for protection groups.

1:1

This protection scheme is also referred to as "one−for−one protection". In this configuration, one working card is paired with one protect card. This protection scheme is available for all electrical cards: DS1, DS3, DS3E, DS3XM, and EC1. The working card must be in an even−numbered slot and the protect card must be in an adjacent odd−numbered slot. For example, if the working DS3 card is placed in slot 4, you may place the protect DS3 card in either slot 3 or slot 5.

1:N

This protection scheme is also referred to as "one−for−n protection". In this configuration, one to five working cards are assigned to one protect card. The maximum number of working cards that can be protected is five. This protection scheme is available for DS1, DS3, and DS3E cards. Each 1:N protection group must contain one protect card (DS1N−14, DS3N−12 or DS3N−12E) that must be installed in slot 3 or 15. You must install the corresponding working card on the same chassis half as the protect card. For example, if the DS3N card is installed in slot 3, you can place the corresponding working DS3 cards in slots 1, 2, 4, 5 and 6. If the DS3N card is installed in slot 15, you can place the corresponding working cards in slots 12, 13, 14, 16, and 17. The exact number of working cards that may be protected depends on the card and backplane type.

1+1

This protection scheme is also referred to as "one−plus−one protection". In this configuration, one working optical port is protected by another optical port on a different card. This protection scheme is available for all OCn ports. Note that this protection scheme applies to ports, not cards. Several rules for creating optical protection groups are best illustrated by an example using two 4−port OC3 cards.

- Working and protect ports do not need to be in adjacent slots to form a protection group. If one OC3 card is in slot 2 and another OC3 card is in slot 13, ports on these cards may be members of a protection group.
- There are no designated working and protect slots. In this example, port 1 of slot 2 may be the working port and port 1 of slot 13 may be the protect port. Alternatively, port 1 of slot 13 may be the working port and port 1 of slot 2 may be the protect port.
- Only corresponding slots on different cards may be members of a protection group. If port 1 on slot 2 is the working port, only port 1 on slot 13 may serve as the protect port. Ports 2, 3, and 4 are ineligible to serve as protect ports. Similarly, if port 1 on slot 2 is the working port, ports 2, 3, and 4 on slot 2 cannot serve as the protect port.
- Once a port on a card has been designated as either working or protect, the rest of the ports on the

same card must be designated the same or remain unprotected. Suppose that port 1, slot 2 is a working port and port 1, slot 13 is its protect port in a protection group. Port 2 on slot 1 can be a working port in another protection group or it can remain unprotected; it cannot serve as a protect port in another protection group. Similarly, port 2 on slot 13 can serve as the protect port in another protection group or remain unprotected; it cannot serve as the working port in another protection group.

Creating Protection Groups

All cards and ports are unprotected by default; you must provision protection groups. Two examples of creating protection groups follow:

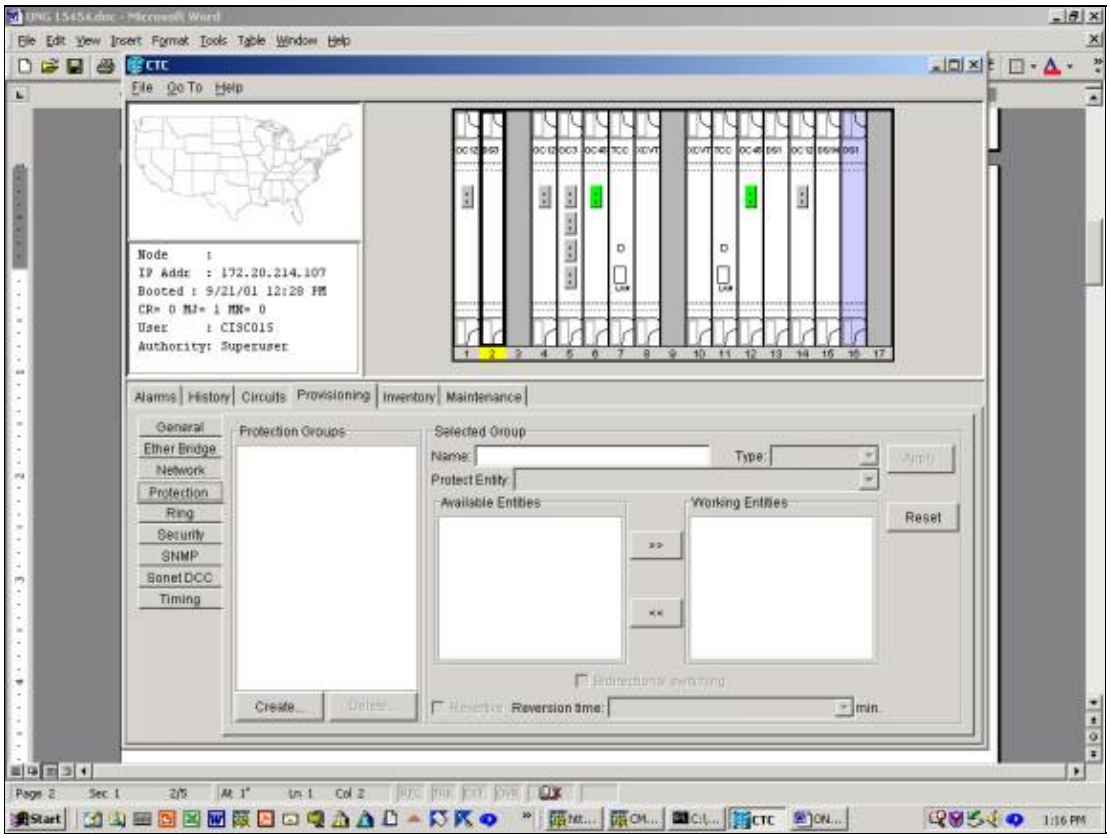
- 1+1
- 1:N

Note: A 1:1 protection group is simply a special case of the 1:N protection group.

ONG 15454: 1+1 Protection Group Setup

The following example illustrates how to set up a 1+1 protection group using two OC12 cards. This example applies to any OCn card on the ~~15454~~Cisco ONS 15454.

1. From the Shelf−level view, click on the **Provisioning** tab and then the **Protection** tab.



2. ~~Select~~Click **Create** to bring up the Create Protection Group window.
3. In the **Name** field, enter the name of this protection group.

   In this example, the name is OC12−1.
4. In the **Type** field, select 1+1 (port) from the drop−down menu.
5. In the **Protect Port** field, select an OCn slot and port from the drop−down menu.

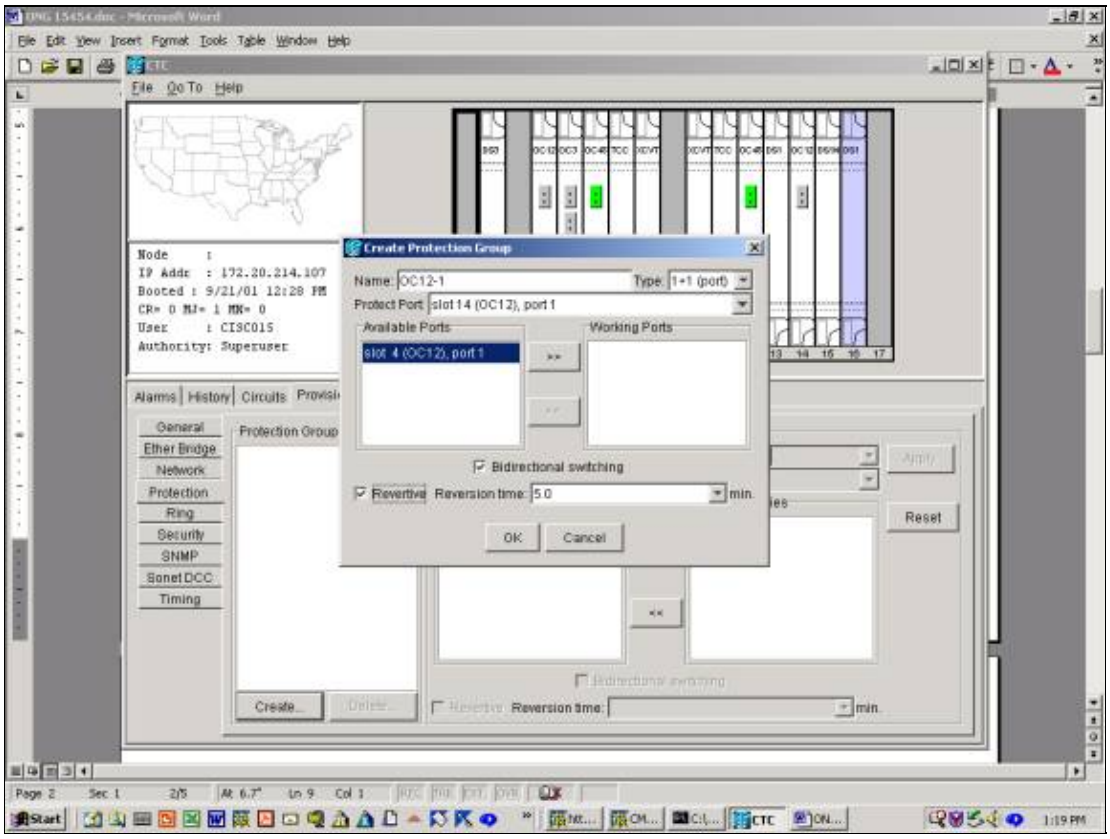
In this example, select slot 14 (OC 12), port 1, as the protection port.

6. In the **Available Ports** field, select the appropriate card and port and highlight it.

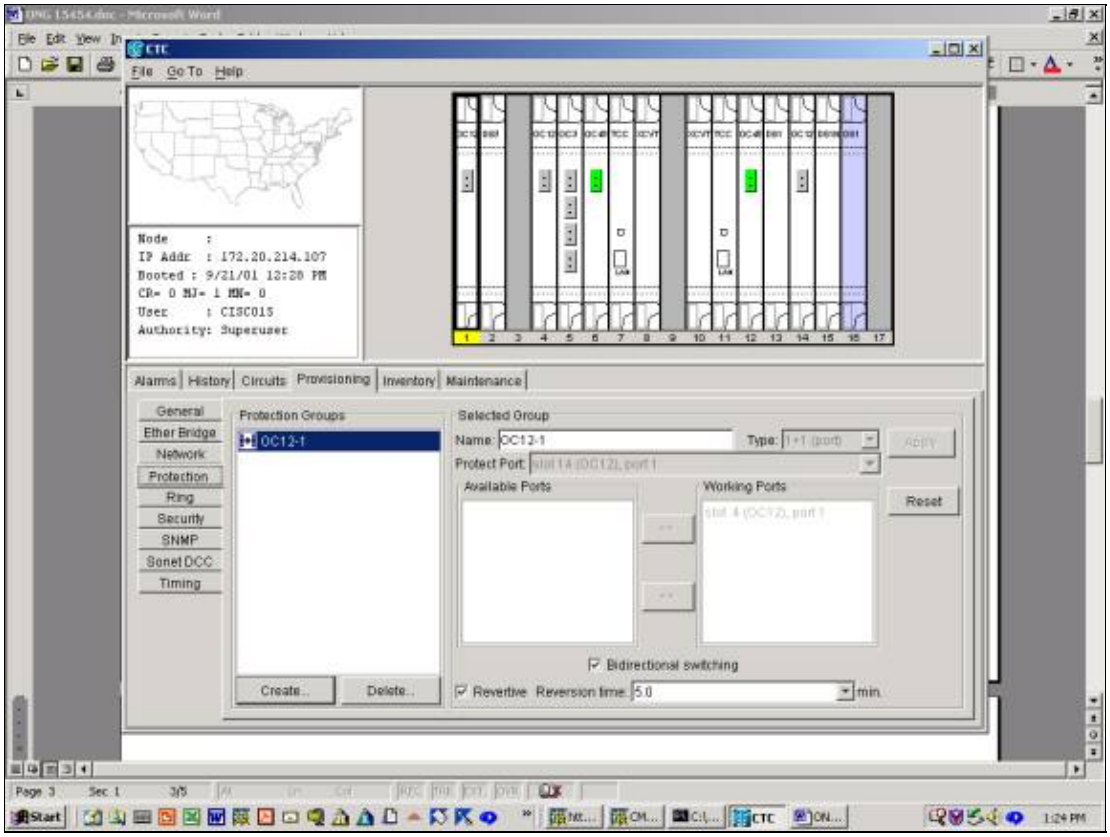
   Drag this slot or port into the Working Ports window. In this example, select slot 4 (OC 12), port 1 as the working port.
7. The **Bidirectional Switching** checkbox allows you to choose unidirectional or bi−directional switching.

   Checking this box provides bi−directional switching, meaning that in the event of a failure, both the Transmit and Receive ports ~~will~~ switch to the protection ports.
8. The **Revertive** checkbox allows you to select revertive or non−revertive switching.

   In revertive switching, traffic switches back to the working card after the original failure is corrected or the software switch has cleared. You can provision the amount of time in minutes between the failure being corrected and the traffic switching back to the working facility. (The reversion time only applies to autonomous switches, such as physical failures, not to software or user−initiated switches. Clearing a software switch ~~will~~ causes the traffic to immediately switch back to the working facility.) The default reversion time is five minutes. In non−revertive switching, traffic does not switch back to the working card after the original failure is corrected or the software switch has cleared. Traffic can operate indefinitely on the designated protection card or port with no loss in switching functionality or capability. When you select non−revertive, the **Reversion Time** field is not available.



9. Clicking **OK** ~~will~~ completes the provisioning and creates the protection group.



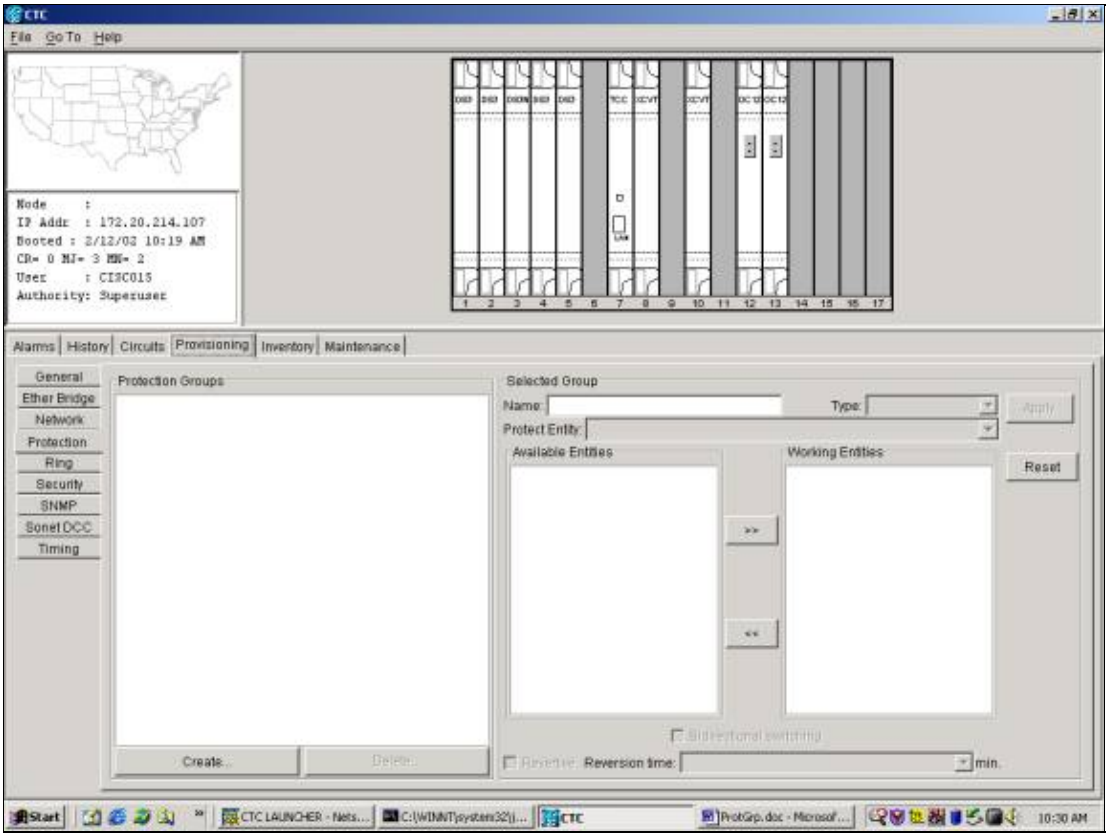
ONG 15454 1:N Protection Group Setup

The following example applies to setting up DS3, DS3E, or DS1 cards in a 1:N protection group. The number of working cards depends on the type of backplane on the side of the chassis where the protection group is being built.

Backplane Type	DS3, DS3E Eligible Working Slots	DS1 Eligible Working Slots
SMB−84	1:5 Maximum1, 2, 4, 5, 6 (3 is the protect slot) 12, 13, 14, 16, 17 (15 is the protect slot)	1:5 Maximum1, 2, 4, 5, 6 (3 is the protect slot) 12, 13, 14, 16, 17 (15 is the protect slot)
BNC−24	1:2 Maximum2, 4 (3 is the protect slot)14, 16 (15 is the Protect slot)	Not available
BNC−48	1:4 Maximum1, 2, 4, 5 (3 is the protect slot) 13, 14, 16, 17 (15 is the Protect slot)	Not available

This example uses a combination of DS3 and DS3E cards. In order to take full advantage of the additional DS3E functionality, the protect card must be DS3N−12E.

1. From the Shelf−level view, click on the **Provisioning** tab and then the **Protection** tab.

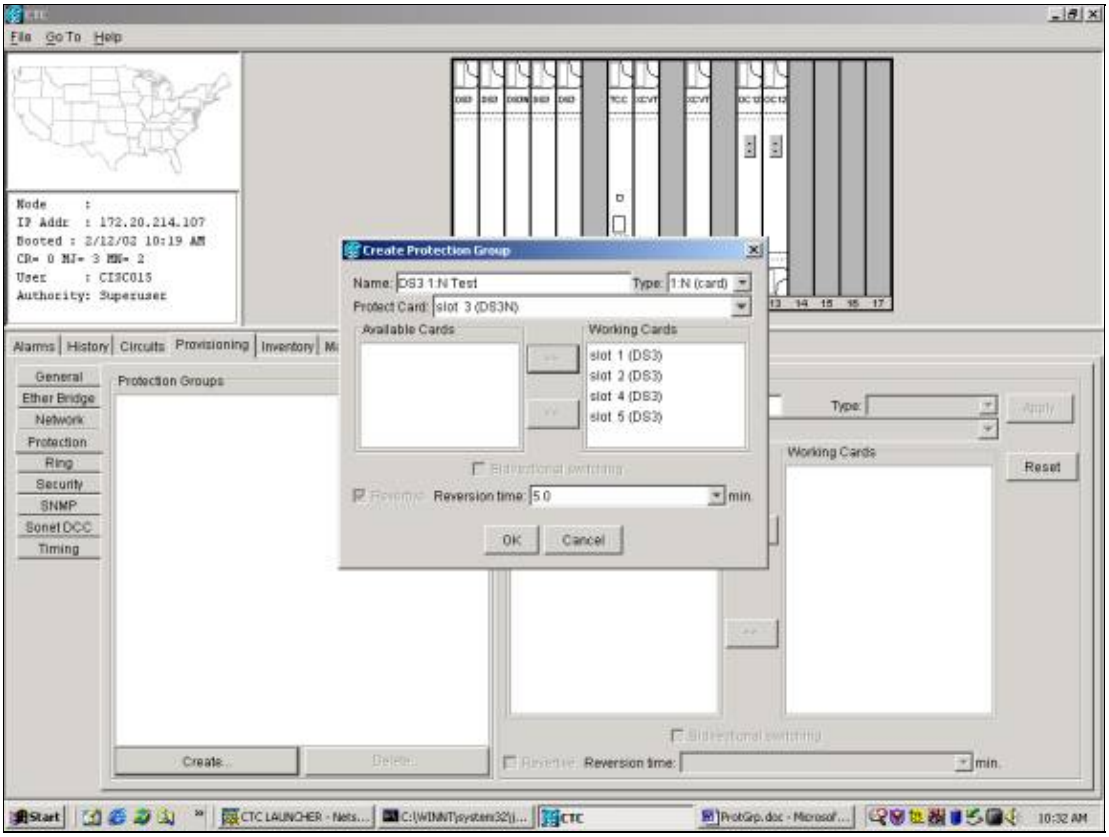


2. ~~Select~~Click **Create** to bring up the Create Protection Group window.
3. In the **Name** field, enter the name of this protection group. In this example, the name is DS3 1:N Test.
4. In the **Type** field, select 1:N (card) from the drop−down menu.
5. In the **Protect Card** field, select the slot that contains the DS3N card, either slot 3 or slot 15, from the drop−down menu.

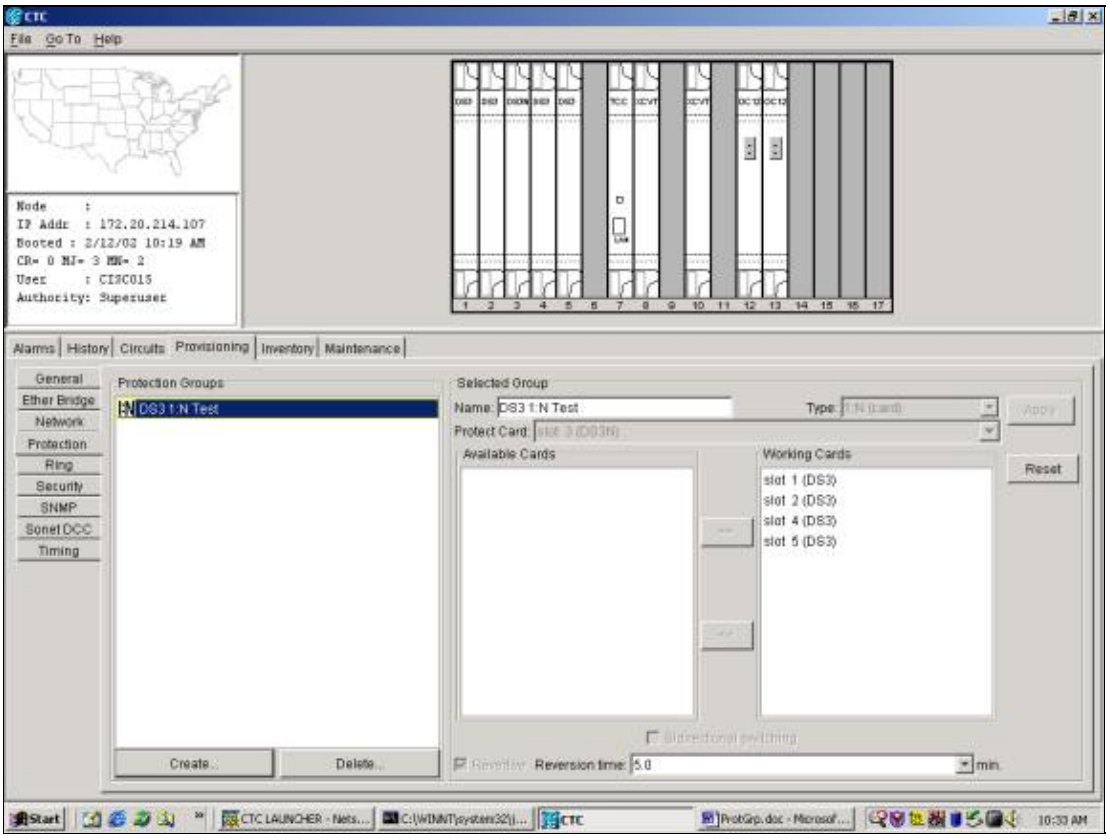
   In this example, select slot 3 (DS3N), as the protection entity.
6. In the **Available Cards** field, all the DS3 cards on that chassis half are displayed, regardless of whether or not the backplane can support connections to all of them.

   Select and highlight one or more of the DS3 cards. Use the double−arrow to move them to the working cards window. In this example, all four of the eligible DS3 cards have been selected as working cards.
7. The **Bidirectional Switching** checkbox is grayed−out and unavailable. DSn cards switch at the card level, not at the individual Tx/Rx port.

   The **Revertive** checkbox is grayed−out and unavailable. By default, the 1:N protection group is revertive, so that traffic switches back to the working card after the original failure is corrected or the software switch has cleared. You can provision the amount of time in minutes that ~~will~~ pass between the failure being corrected and the traffic switching back to the working facility. (The reversion time only applies to autonomous switches, such as physical failures, not to software or user−initiated switches. Clearing a software switch ~~will~~ cause<u>s</u> the traffic to immediately switch back to the working facility.) The default reversion time is five minutes.



8. Clicking **OK** completes the provisioning and creates the protection group.



ONG 15454 1:1 Protection Setup

Setting up DS3, DS3E, or DS1 cards in a 1:1 protection group is a special case of the 1:N case. Any DS3−12 or DS3−12N can serve as a working or protect card. The working and protect cards must be in adjacent slots,

with the working card in the even−numbered slot and the protect card in the odd−numbered slot. Again, the slots available for working traffic depend on the type of chassis backplane.

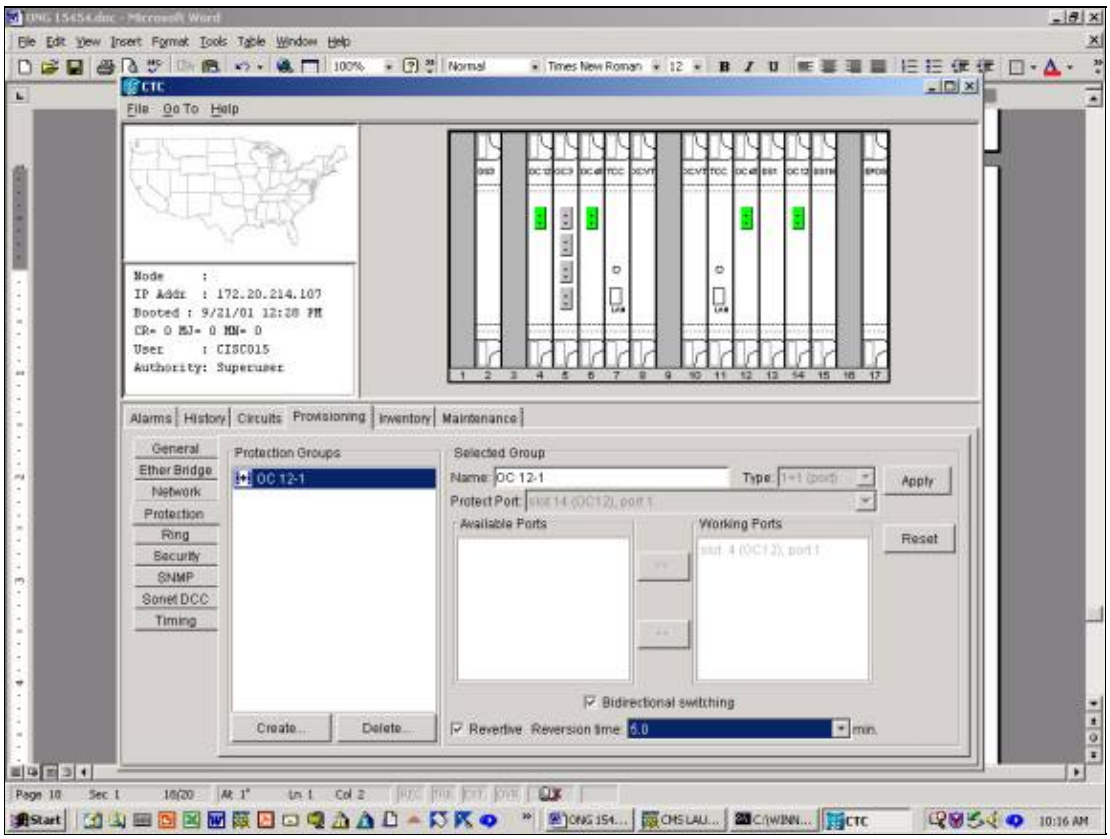
To create a 1:1 protection group, follow the 1:N example above, choosing appropriate cards and slots.

Deleting a Protection Group

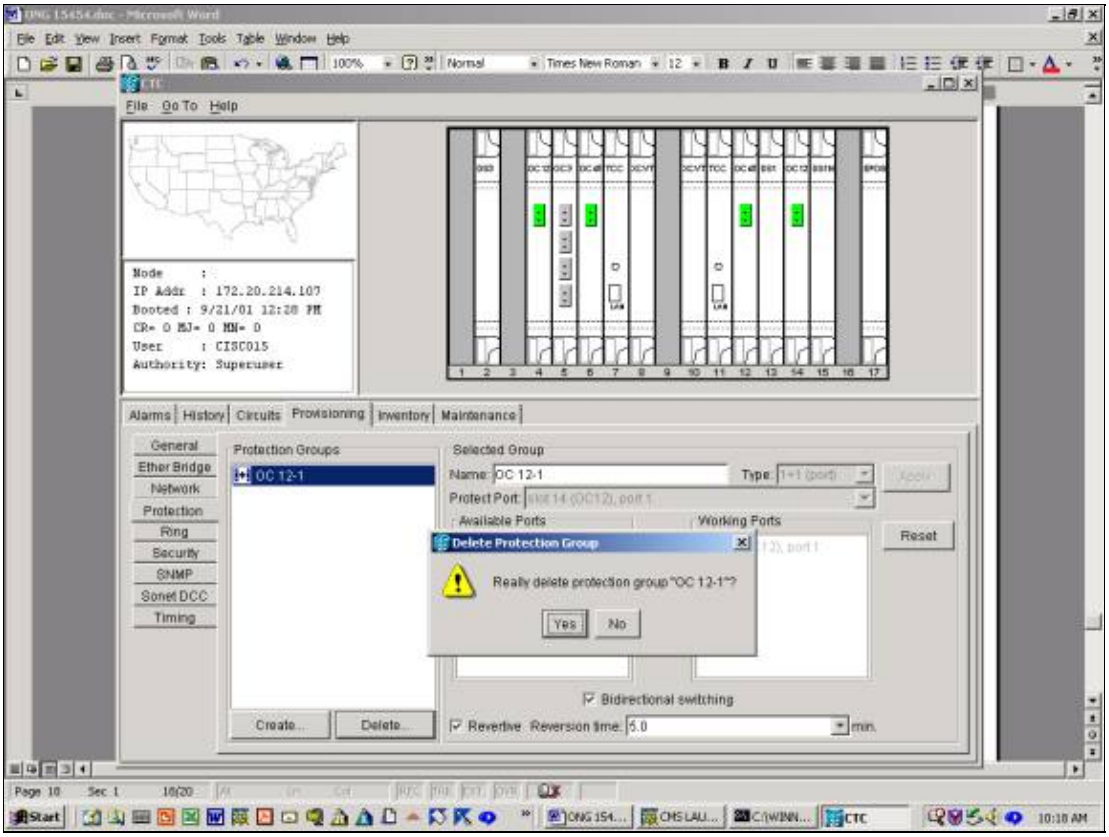
The procedure to delete a protection group is the same regardless of the protection scheme (1+1, 1:1, 1:N).

To delete a protection group, from the Shelf view, click on the **Provisioning** tab and then the **Protection** tab. Select the protection group to be deleted from the Protection Group window. In this example, we are deleting an OC12 protection group.

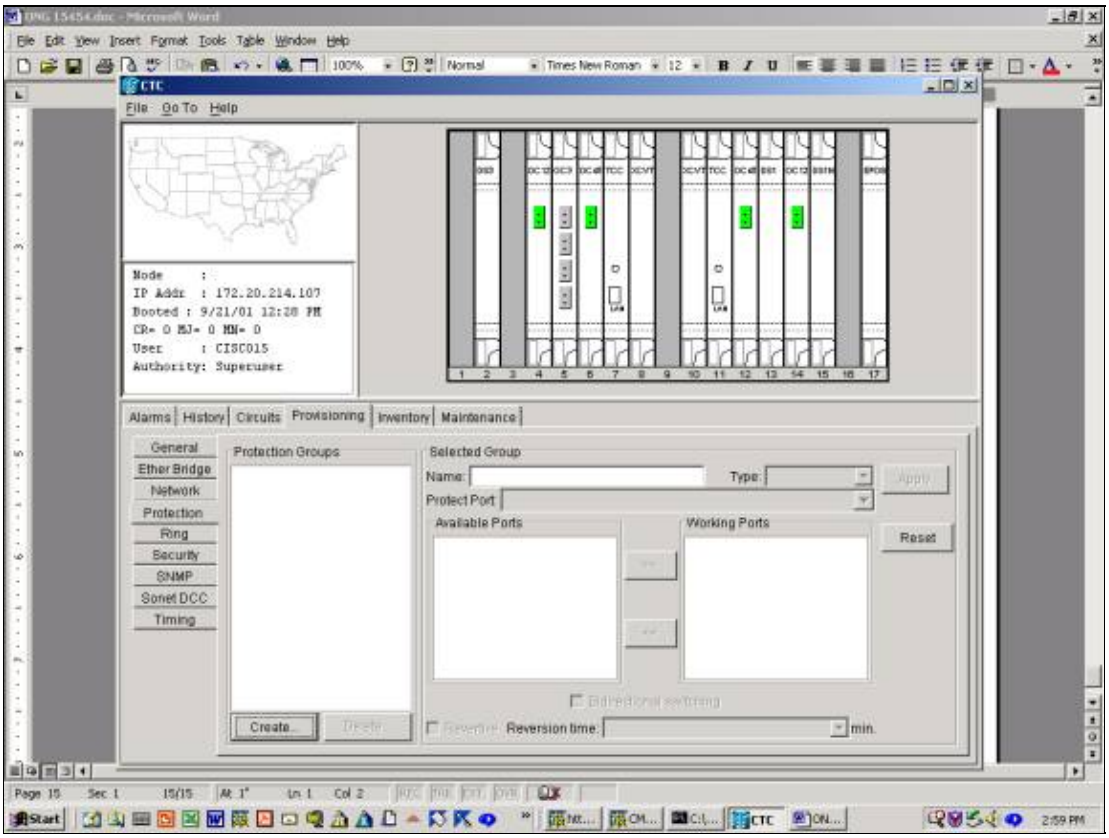
1. Highlight the OC12 protection group and then ~~select~~click ~~**<**~~**Delete** ~~>~~.



2. A dialog box asking you to confirm the deletion of the protection group appears.



3. To delete the protection group, ~~select~~click **Yes**.



The protection group is successfully deleted.

Maintenance Operations

The maintenance operations available depend on the type of protection group you have created.

1+1 Maintenance Operations

The 1+1 protection scheme applies to optical ports and follows the SONET switching hierarchy, adapted from GR−253, and shown below. Some of these functions, such as exercise, do not apply to the 1+1 linear protection scheme. The 1+1 protection group currently does not recognize high or low switching priorities.

Table 5-4. K1 Byte, Bits 1 through 4: Type of Request

Bit 1234	Automatically Initiated, External, or State Request (Note 1)
1111	Lockout of Protection
1110	Forced Switch
1101	SF - High Priority (Note 2)
1100	SF - Low Priority
1011	SD - High Priority (Note 2)
1010	SD - Low Priority
1001	(not used)
1000	Manual Switch
0111	(not used)
0110	Wait-to-Restore (Note 3)
0101	(not used)
0100	Exercise (Note 4)
0011	(not used)
0010	Reverse Request (Note 5)
0001	Do Not Revert (Note 6)
0000	No Request

Notes:

1. Request priority is in descending order, except that an SF request by the null channel (for an SF condition detected on the protection line) has a higher priority than a Forced Switch (i.e., it is between Lockout of Protection and Forced Switch).
2. High Priority codes apply only to the 1:n architecture.
3. 1+1 LTE provisioned for nonrevertive switching does not transmit Wait-to-Restore.
4. Exercise may not be applicable in some linear APS systems.
5. Reverse Request applies only to bidirectional systems.
6. Only 1+1 LTE provisioned for nonrevertive switching transmits Do Not Revert.

Telcordia Technologies GR−253−Core Issue 3 September 2000

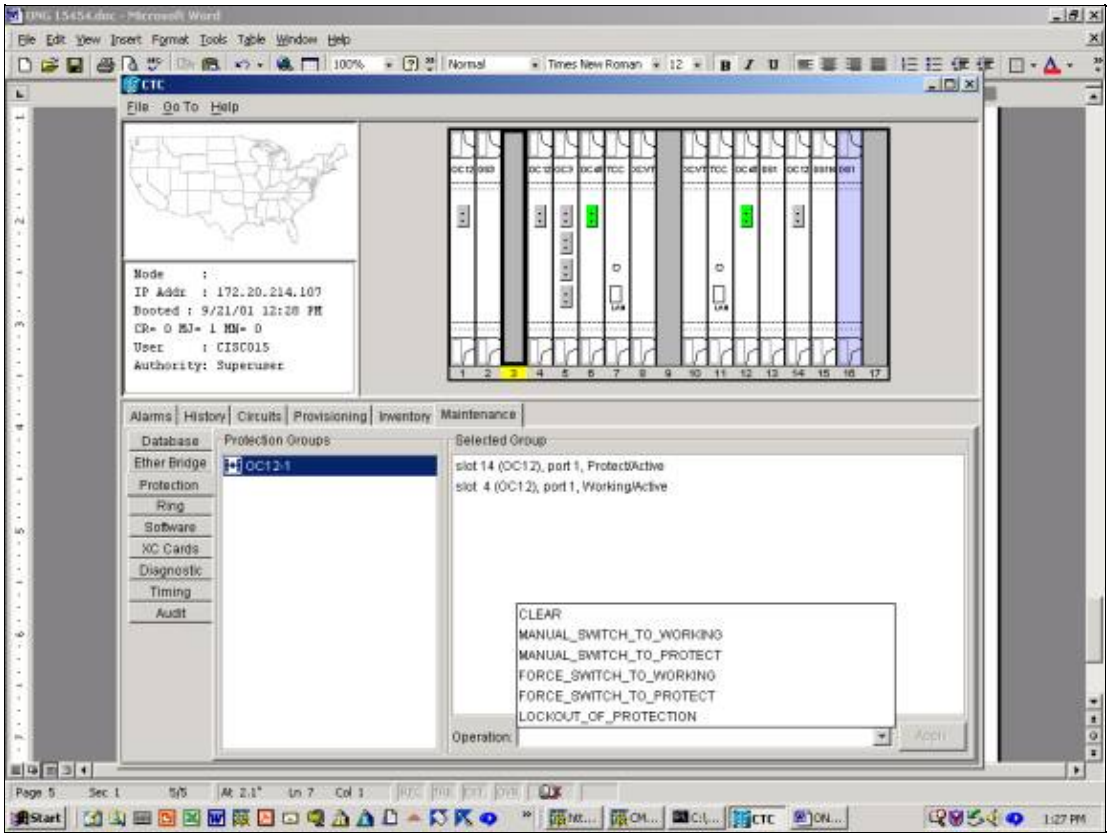
The ~~15454~~Cisco ONS 15454 supports the following maintenance functions for manipulating the working and protect cards:

- LOCKOUT_OF_PROTECTION
- FORCED_SWITCH_TO_PROTECT
- FORCED_SWITCH_TO_WORKING
- MANUAL_SWITCH_TO_PROTECT
- MANUAL_SWITCH_TO_WORKING

- CLEAR

In Release 2.x of Cisco TC ~~(Cisco Transport Controller)~~ software, these are displayed as follows:

1. ~~Select~~Click the **Maintenance** tab and the **Protection** tab.
2. Select one of the displayed protection groups from the Protection Groups window.
3. In the **Operation** field, click the drop−down arrow to display the options.



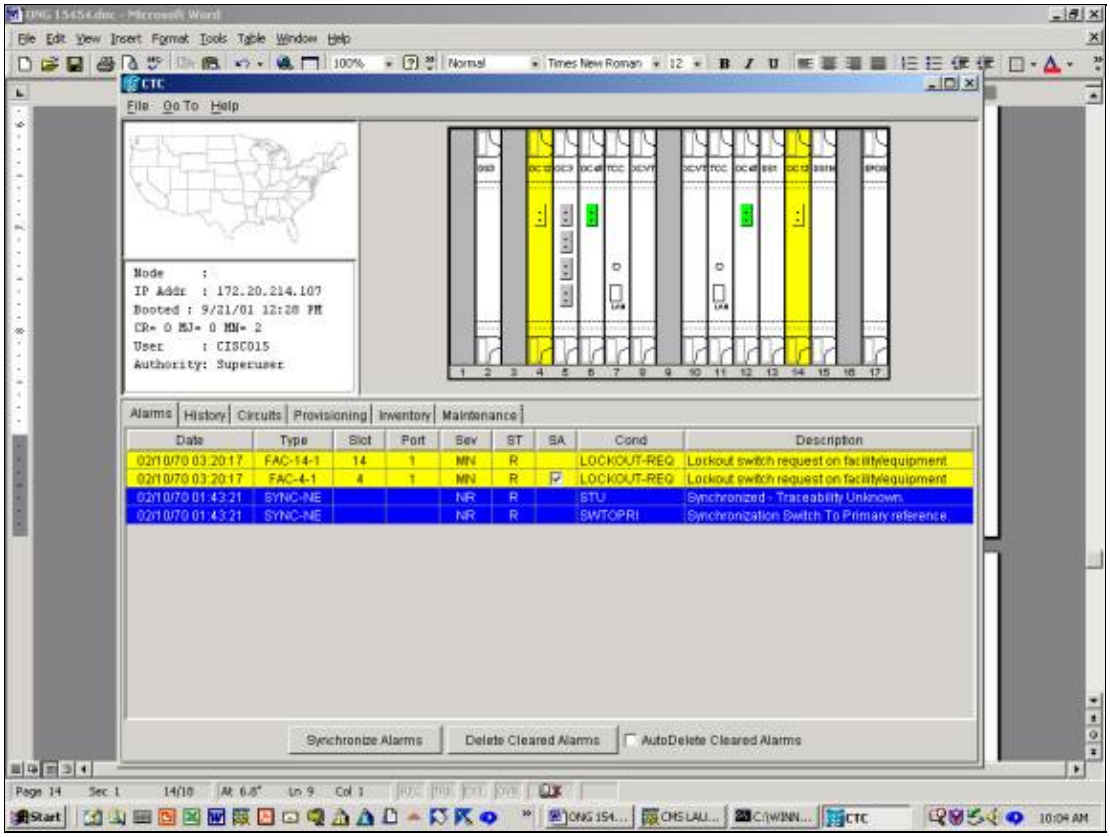
LOCKOUT_OF_PROTECTION

Initiating a lockout of protection forces all traffic to the working card. As long as the lockout is in place, traffic does not switch to the protect card, even in the event of a failure on the working card or working fiber. If a lockout is in place, and a failure occurs on the working card or fiber, traffic goes down. A lockout has the highest priority and overrides all other switch requests or failures. You can remove a lockout by issuing the **~~C~~clear** command.

To initiate a lockout in Release 2.x:

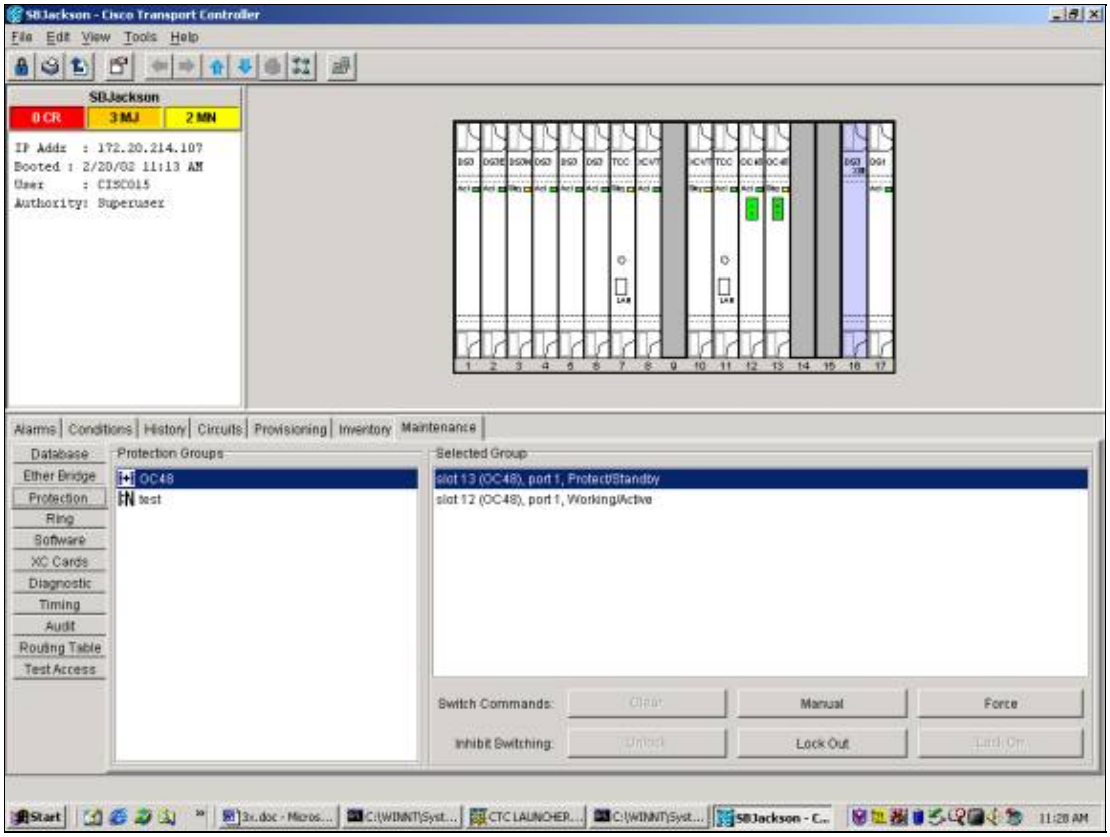
1. From the **Maintenance** tab and **Protection** tab, ~~select~~click **Lockout of Protect** from the Operation field.
2. ~~Select~~Click **Apply**.
3. A confirmation dialog box appears; ~~select~~clicking **Yes** initiates the lockout and ~~select~~clicking **No** cancels the lockout request.

Issuing a lockout of protect results in an alarm on both the working and the protect member of the protection group. The example below shows the alarms for a lockout issued on an OC12 protection group.

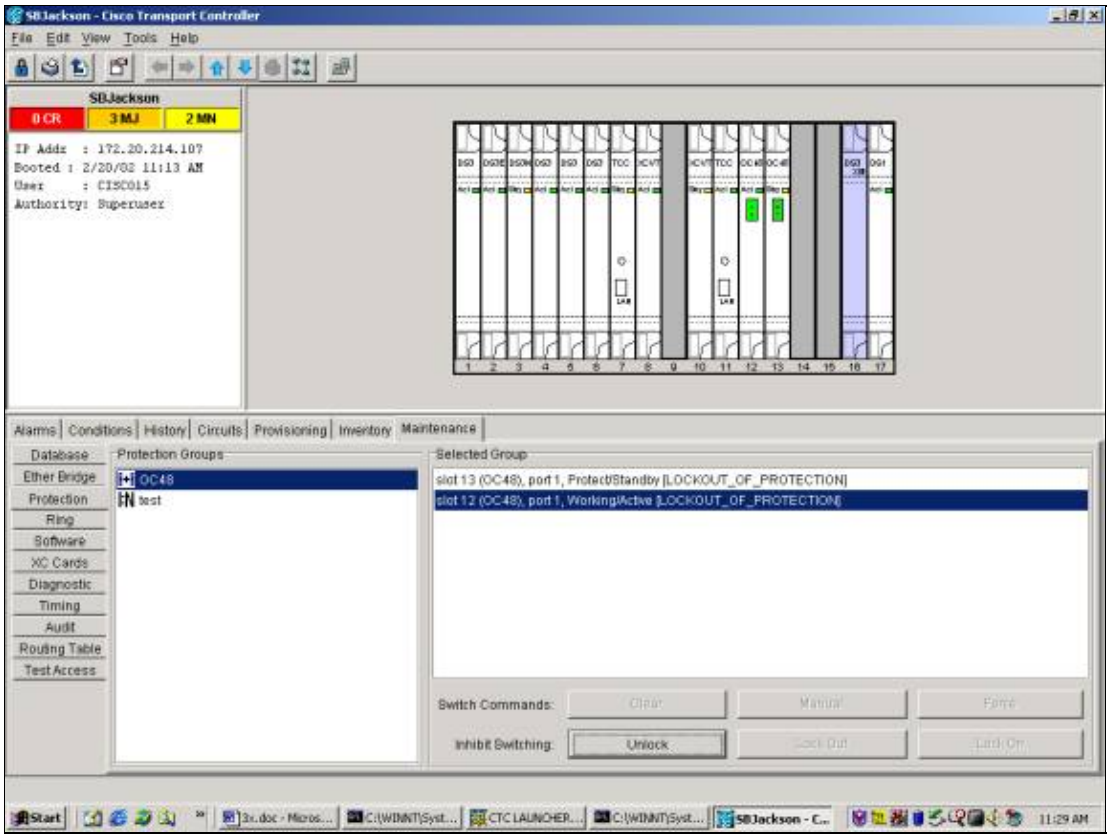


To clear the lockout, go to the **Maintenance** tab and then the **Protection** tab. In the Operation field, ~~select~~click **Clear** as shown below. The associated alarms clear and the lockout is removed.

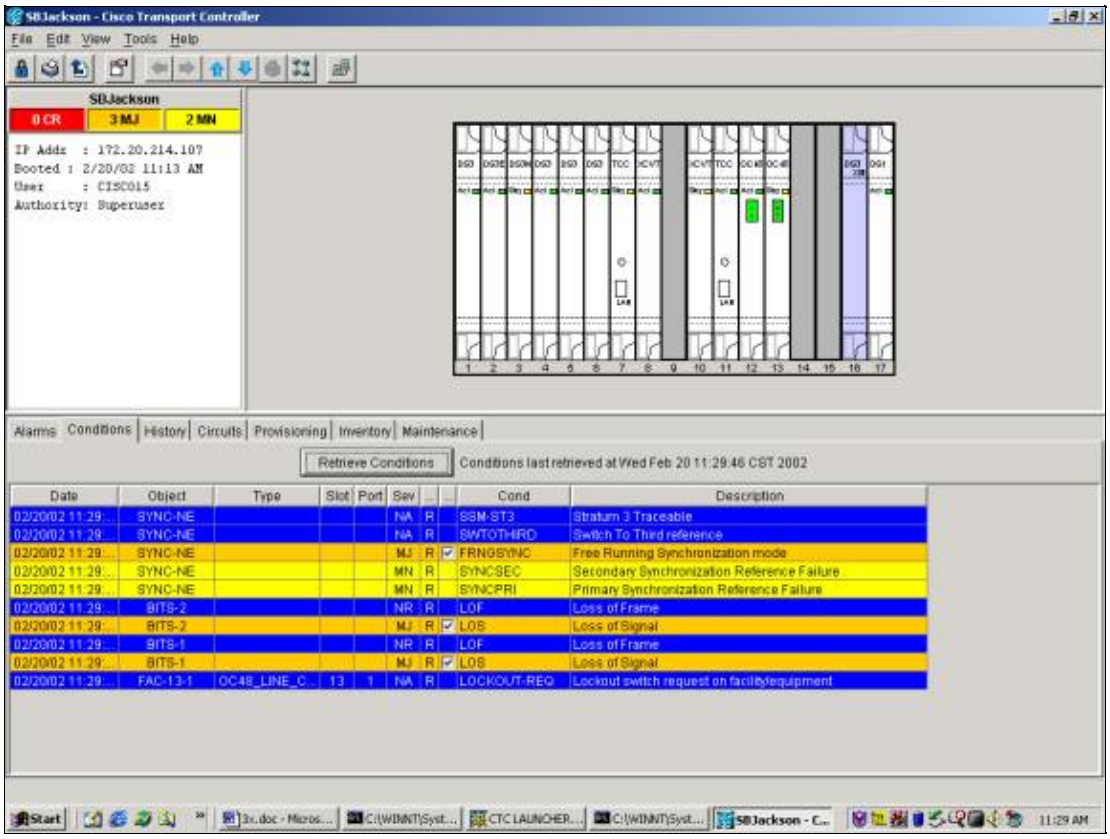
In Release 3.x, there are two options for locking traffic to a card. Applying a lock on to a working card locks traffic to the working card and fiber. Applying a lock out to the protect card switches all traffic to the working card. Traffic remains on the working card until the Unlock Request is issued. If a failure occurs on the working side while the Lock on or lock out is Active, traffic drops. A lock on or a lock out has the highest priority and overrides all other switch requests.



A lock out is issued from the **Maintenance** tab and the **Protection** tab. If the protect card is highlighted, ~~select~~click **Lock Out** and then ~~select~~click **Apply**. A confirmation dialog box appears; ~~select~~clicking **Yes** initiates the lock out and ~~select~~clicking **No** cancels the lockout request.



Issuing a lock out results in a condition raised against the protect member of the protection group. The example below shows the condition for a lock out issued on an OC48 protection group.



To remove the lock out, ~~select~~click **Unlock** from the **Maintenance** ~~**Protection**~~ tab and **Protection** tab. The condition clears and the lock out is removed.

The condition and screens are the same for a lock on applied to the working card.

FORCE SWITCH TO WORKING/PROTECT

Initiating a "Force Switch" forces all traffic to either the working card or the protect card, depending upon which switch type is selected. In a "Force Switch to Protect", all traffic is switched to the protect card and fiber. If there is a failure on the protect side while the Force Switch is in place, traffic switches to the working card and fiber. Once the failure on the protect side is fixed, traffic switches back to the protect side.

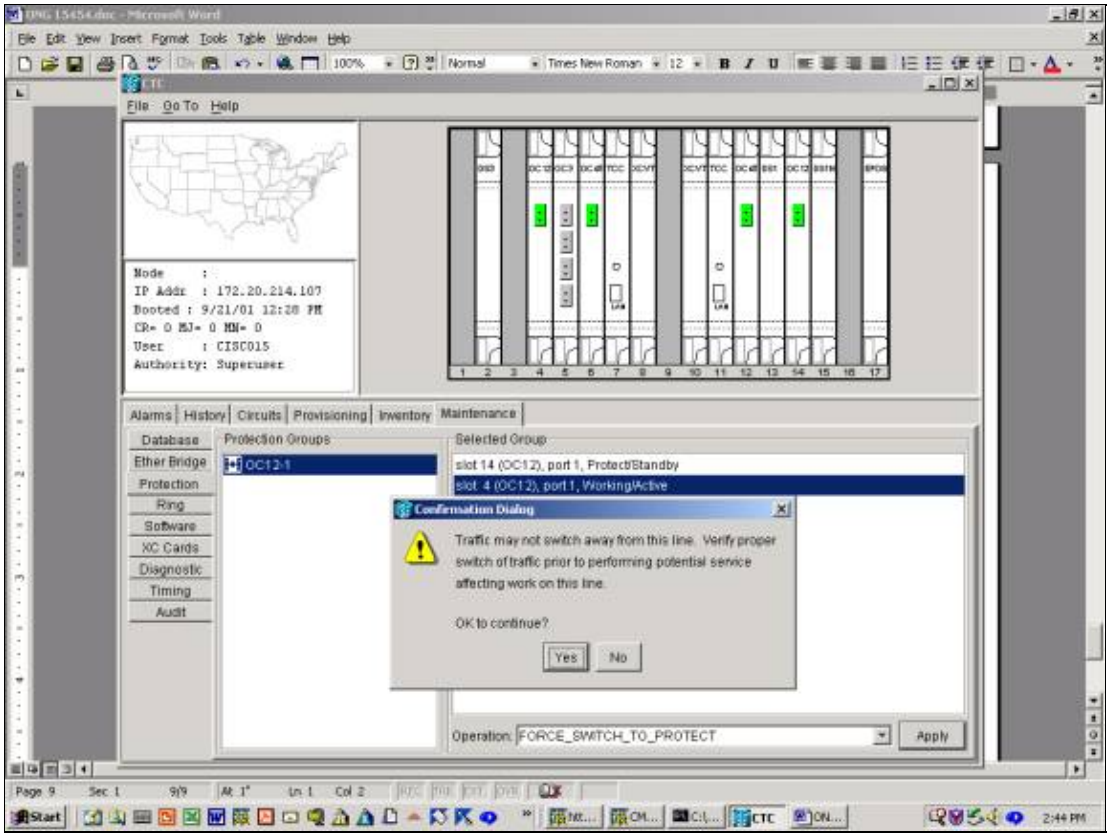
A Force Switch to Protect ~~will~~ fails if the protect card or fiber has a signal fail condition. In this case, the signal fail overrides the Force Switch and traffic remains on the working side. A Force Switch to protect succeeds, however, if the protect side has a signal degrade condition present.

A Force Switch always overrides a manual switch. A lockout always overrides both a Force Switch and a manual switch.

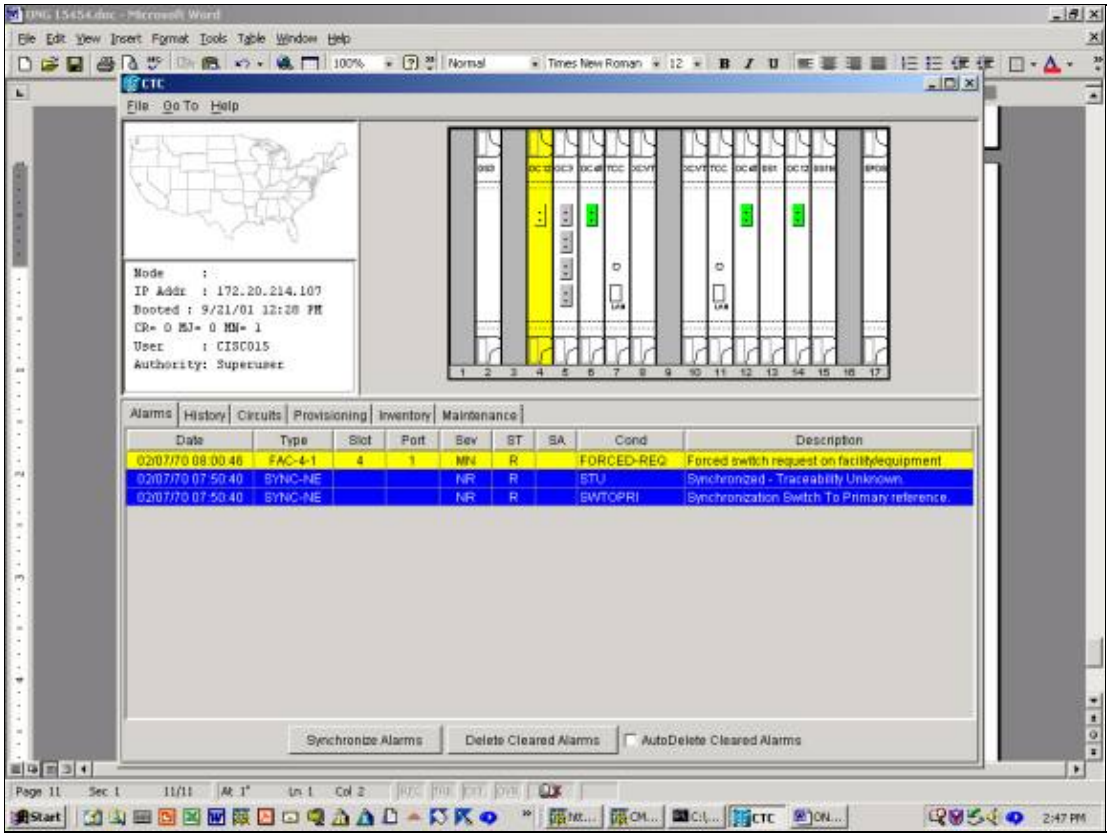
The ~~C~~c**lear** command removes the Force Switch. In non−revertive switching, traffic remains on the protect port indefinitely or until another switch request is issued. In revertive switching, traffic returns to the working port immediately after the switch request is cleared. (The wait−to−restore timer is only activated by autonomous or physical switch conditions, not by software switches.)

Results are analogous for issuing a "Force Switch to Working".

To initiate a Force Switch to Protect in Release 2.x, from the **Maintenance** tab and **Protection** tab, select Force Switch to Protect from the **Operation** field and ~~select~~click **Apply**. A confirmation dialog appears, to inform you that the switch may not occur and to verify that it has before performing service affecting maintenance. ~~Select~~clicking **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.

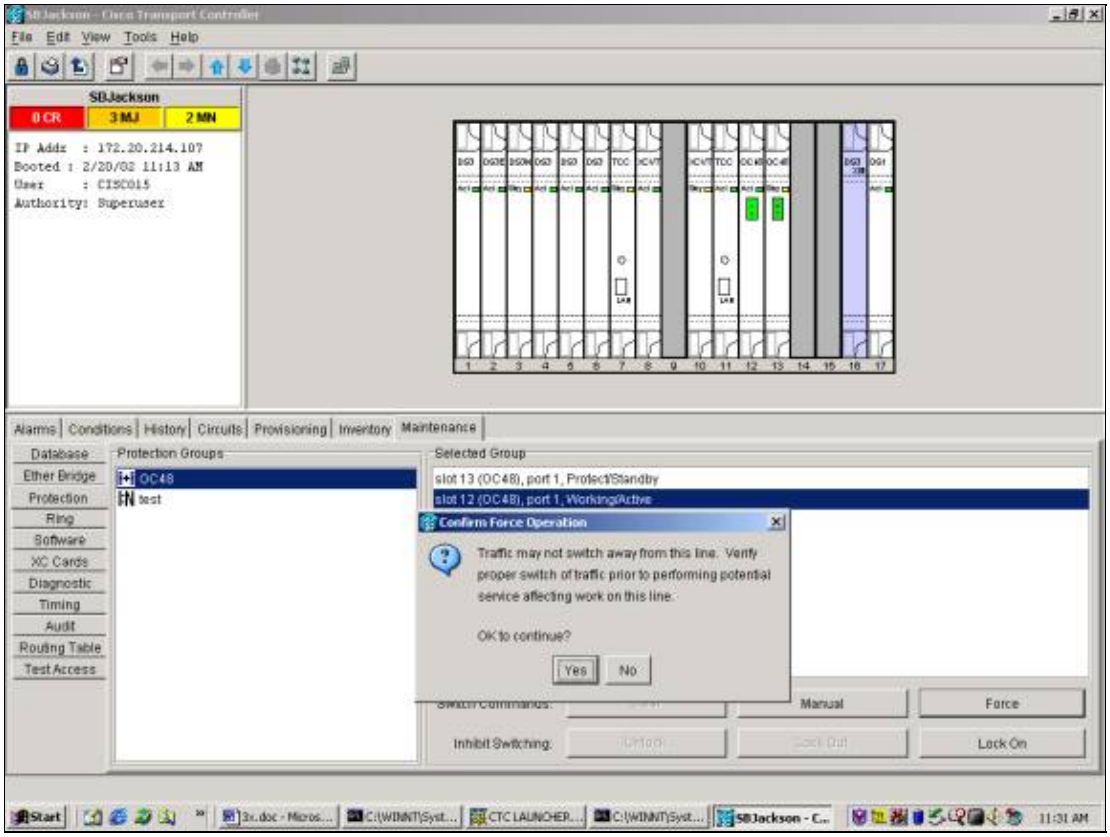


A Force Switch to Protect results in a minor alarm on the designated working member of the protection group, as shown below.

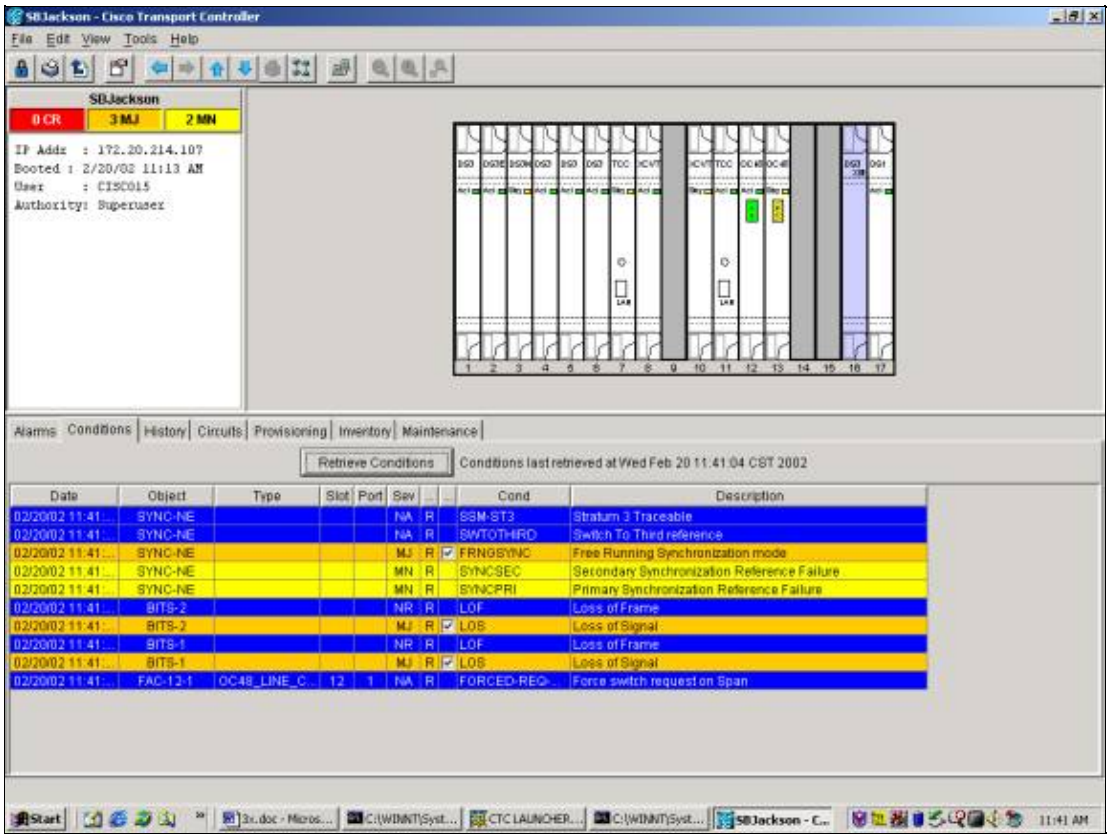


To remove the Force Switch, go to the **Maintenance** tab and **Protection** tab and in the **Operation** field, ~~select~~click **Clear**. The associated alarms clear and the Force Switch is removed.

To initiate a Force Switch to protect in Release 3.x, ~~select~~click the **Maintenance** tab and the **Protection** tab. You can issue a Force Switch by highlighting the working card and ~~select~~clicking **Force**. A confirmation dialog appears, to inform you that the switch may not occur and to verify that it has before performing service affecting maintenance. ~~Select~~Clicking **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.



A Force Switch to Protect results in a condition, not an alarm, against the designated working member of the protection group, as shown below.



To remove the Force Switch, go to the **Maintenance** tab and **Protection** tab and ~~select~~click **Clear**. The associated condition clears and the Force Switch is removed.

MANUAL SWITCH TO WORKING/PROTECT

Initiating a "Manual Switch" switches all traffic to either the working card or the protect card, depending on which switch type is selected. In a "Manual Switch to Protect", all traffic is switched to the protect card and fiber. If there is a failure on the protect side while the Manual Switch is in place, traffic switches to the working card and fiber. Once the failure on the protect side is fixed, traffic ~~will~~ switchs back to the protect side.

A Manual Switch to protect ~~will~~ fails if the protect card or fiber has a Signal Degrade or Signal Fail condition. In this case, both the Signal Degrade and the Signal Fail override the Force Switch and traffic ~~will~~ remains on the working side.

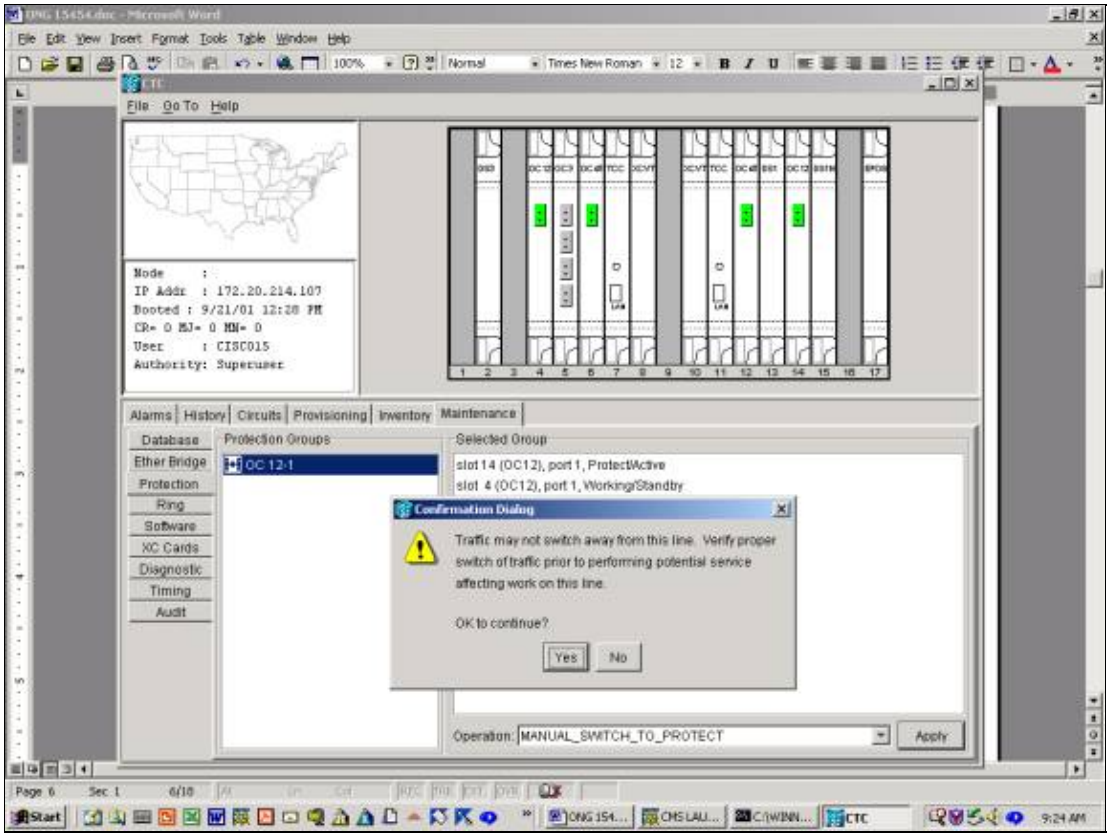
Note: A Force Switch always overrides a Manual Switch. A lockout always overrides both a Force Switch and a Manual Switch.

Issuing the ~~C~~**clear** command removes the Manual Switch. In non−revertive switching, traffic ~~will~~ remains on the protect side indefinitely or until another switch request is issued. In revertive switching, traffic ~~will~~ returns to the working side immediately after the switch request is cleared. (The Wait−to−Restore timer is only activated by autonomous or physical switch conditions, not by software switches.)

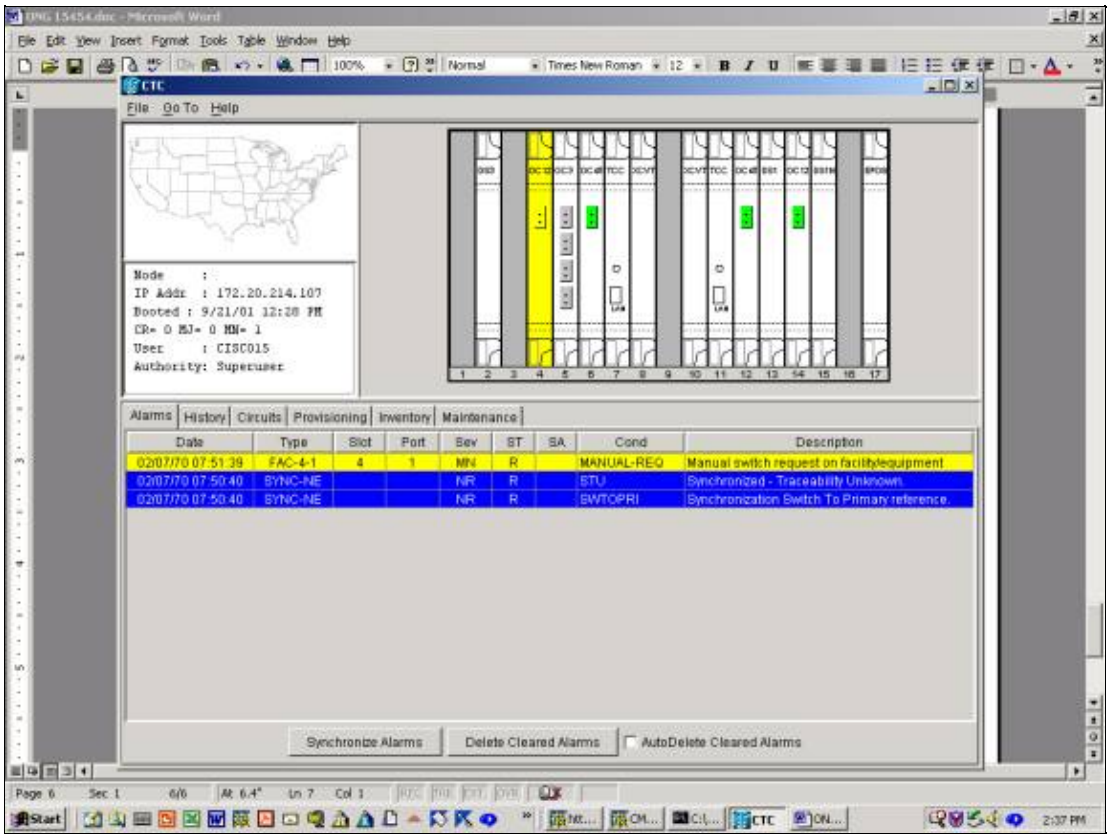
Results are analogous for issuing a Manual Switch to Working.

To initiate a Manual Switch to Protect in Release 2.x:

1. From the **Maintenance** tab and **Protection** tab, ~~select~~click **Manual Switch to Protect** from the **Operation** field.
2. ~~Select~~Click **Apply**. A confirmation dialog appears, to inform you that the switch may not occur and to verify that it has before performing service affecting maintenance.
3. 3. ~~Select~~Click **Yes** to initiate the switch or **No** to cancel the switch request.

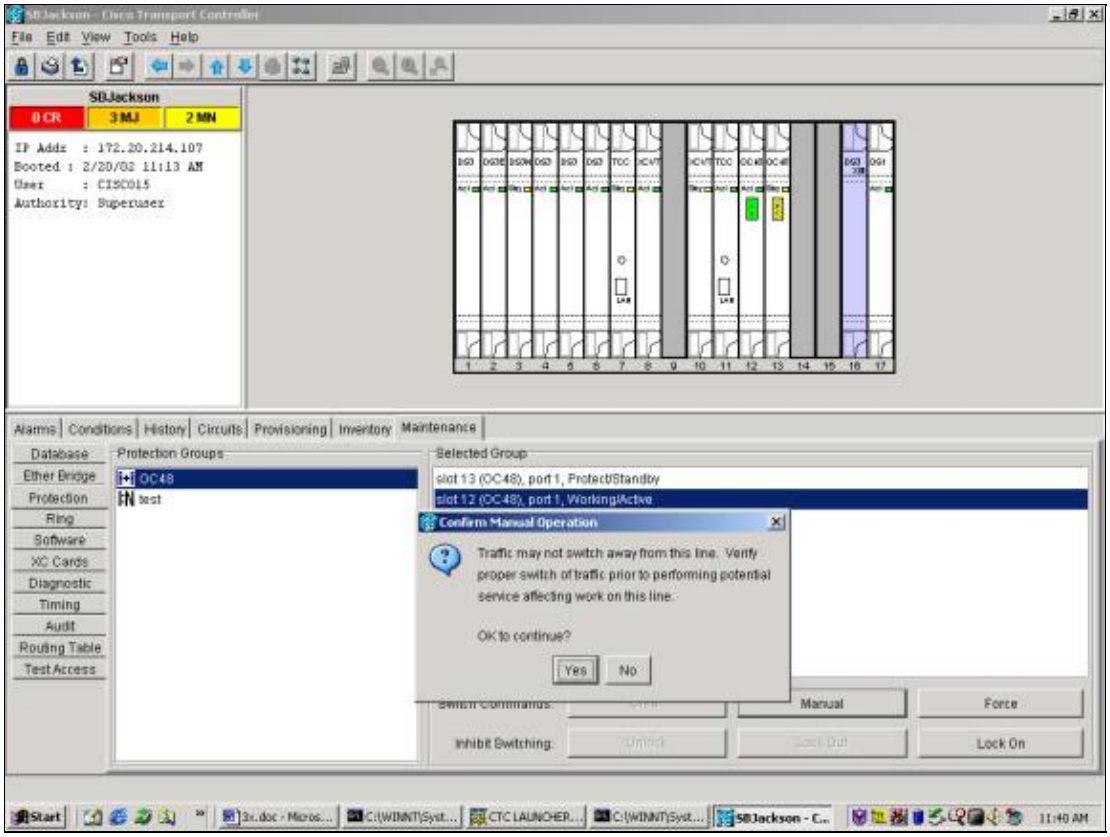


A Manual Switch results in a minor alarm on the designated working member of the protection group, as shown below.

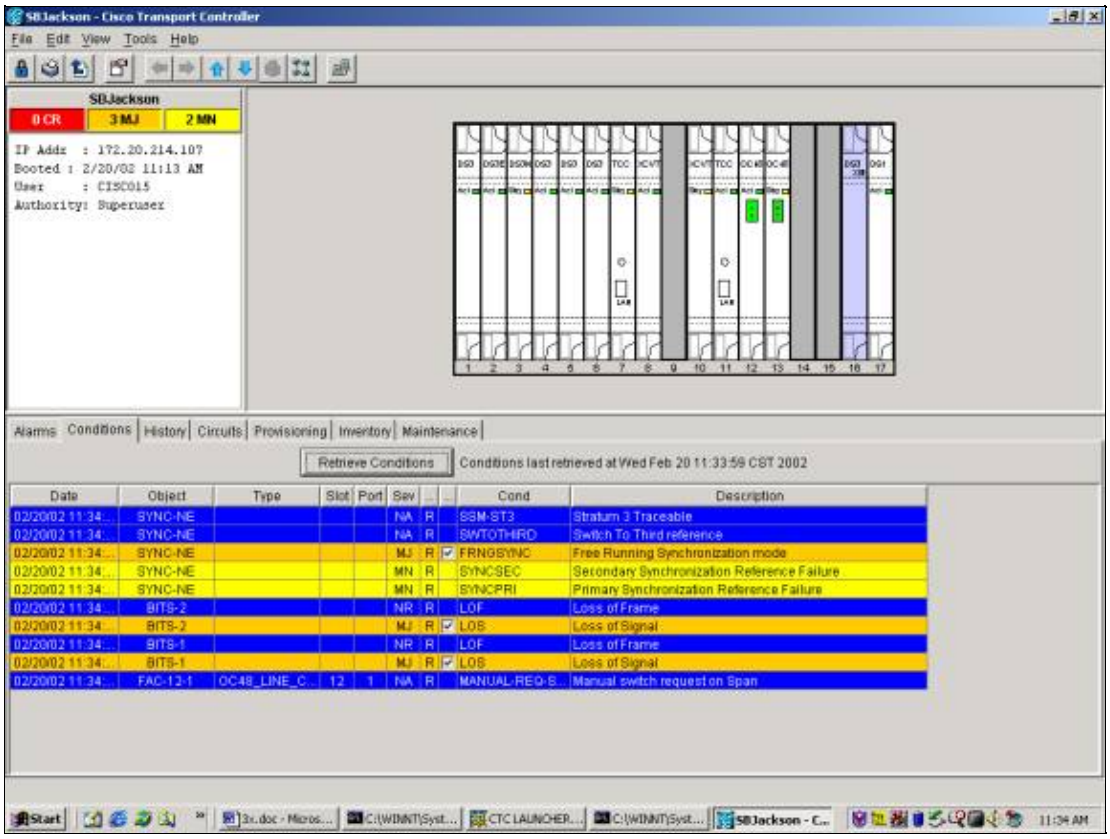


To remove the Manual Switch, go to the **Maintenance** tab and **Protection** tab and in the **Operation** field, ~~select~~click **Clear**. The associated alarms ~~will~~ clear and the Manual Switch is removed.

To initiate a Manual Switch to Protect in Release 3.x, ~~select~~click the **Maintenance** tab and the **Protection** tab. Issue a Manual Switch to Protect by highlighting the working card and ~~select~~clicking **Manual**. A confirmation dialog appears, to inform you that the switch may not occur and to verify that it has before performing service affecting maintenance. Selecting **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.



A Manual Switch to Protect results in a condition, not an alarm, against the designated working member of the protection group, as shown below.



To remove the Manual Switch, go to the **Maintenance** tab and **Protection** tab and ~~select~~click **Clear**. The associated condition clears and the Manual Switch is removed.

1:N Maintenance Operations

The 1:N Protection Scheme applies to DS1 and DS3 cards. 1:N protection switching is always revertive. When a failure or a switch on any working card occurs, traffic is switched to the protect card in either slot 3 or slot 15. Traffic remains on the protect card until the failure is repaired or the software switch is released. Traffic is then restored to the original working card.

1:1 protection is a special case of 1:N. The protect card always resides in an odd−numbered slot. 1:1 protection groups may be provisioned as either revertive or non−revertive. In revertive switching, traffic is restored to the designated working card after the failure or software switch has cleared. In non−revertive switching, traffic remains on the protect card indefinitely or until the next failure or software switch.

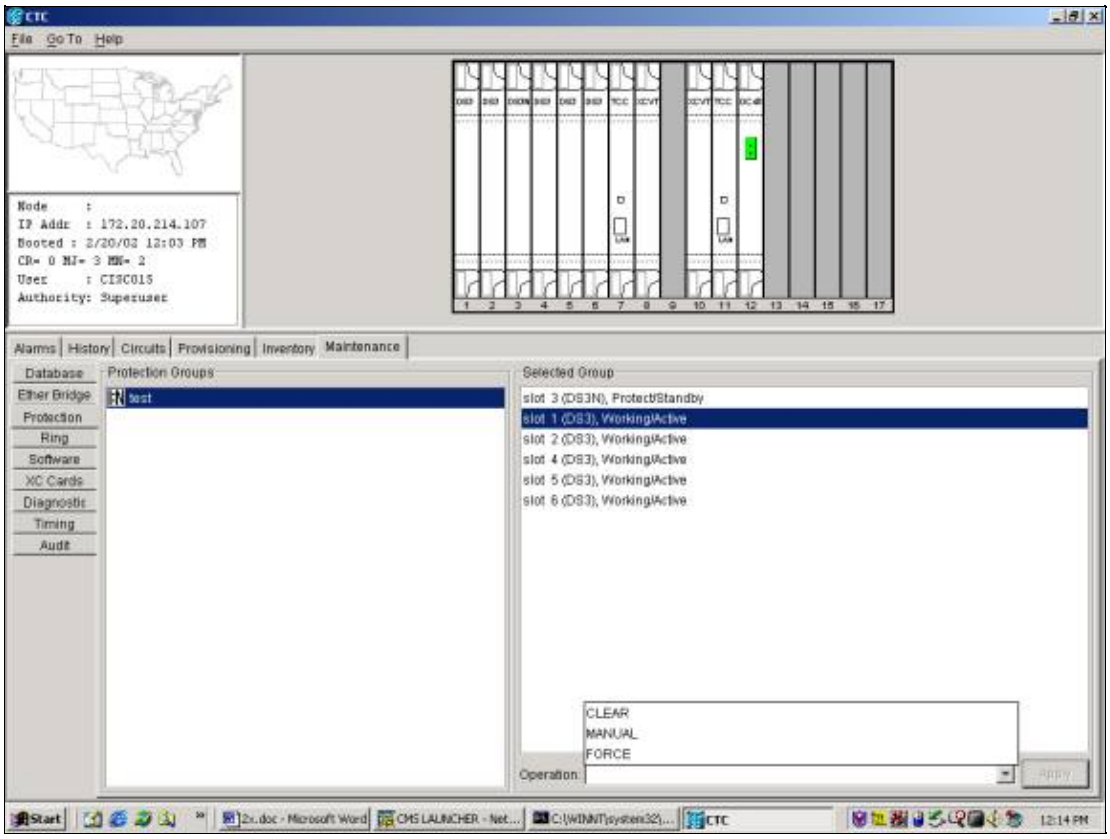
This section describes the operation of the maintenance functions for both the 1:1 and 1:N cases.

Release 2.x

In Release 2.x, the ~~15454~~Cisco ONS 15454 supports the following maintenance functions for manipulating the working and protect cards:

- FORCE
- MANUAL
- CLEAR

You can access these by ~~select~~clicking the **Maintenance** tab and the **Protection** tab. Select one of the displayed protection groups from the Protection Groups window. In the **Operation** field, click the drop−down arrow to display the options.



Force Switch

Initiating a Force Switch switches all traffic to the designated protect card. If there is a failure on the protect card while the Force Switch is in place, traffic switches back to the working card. Once the failure on the protect card is cleared, traffic switches back to the protect card.

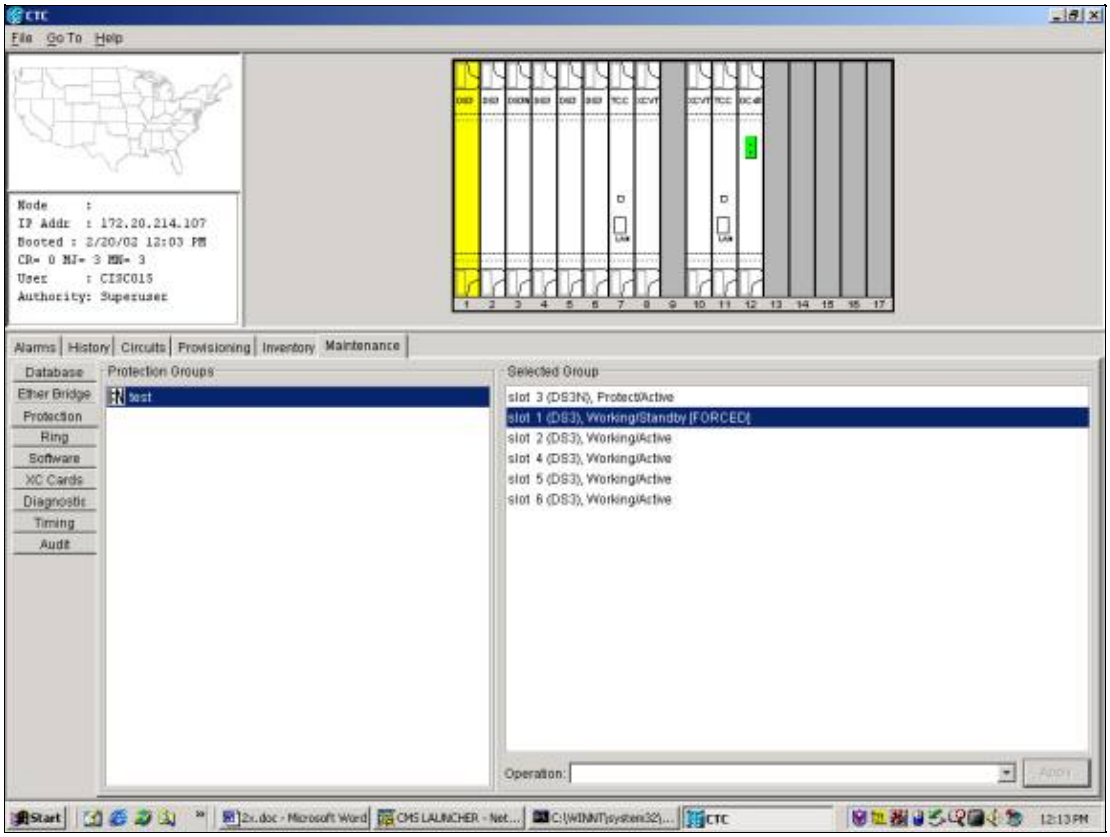
Issuing the ~~C~~c**lear** command removes the Force Switch. In the 1:N case and the 1:1 revertive case, traffic ~~will~~ returns to the working card immediately after the switch request is cleared. (The Wait−to−Restore timer is only activated by autonomous or physical switch conditions, not by software switches.)

- In the 1:1 non−revertive case, traffic remains on the protect card indefinitely or until another failure or switch request occurs.
- In the 1:1 non−revertive case, if traffic was originally on the protect card, a Force Switch request switches the traffic to the working card with results analogous to those outlined above.

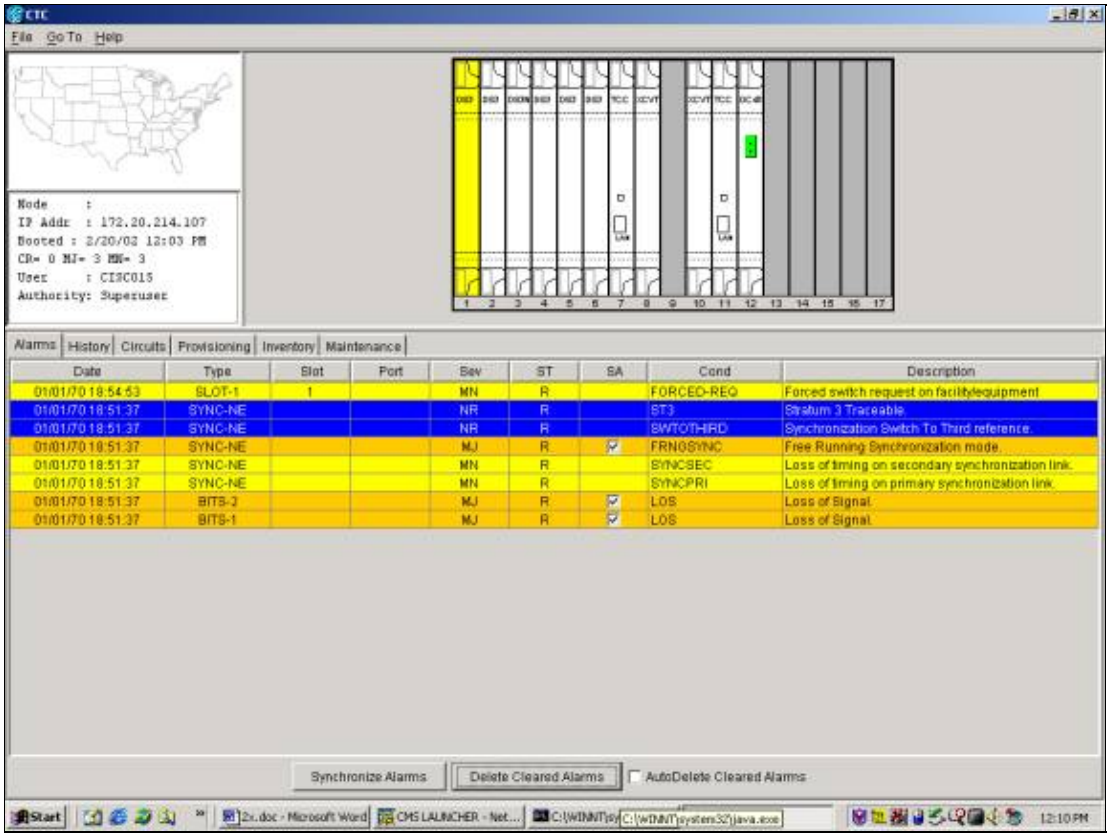
Note: A Force Switch ~~will~~ overrides a manual switch. However, this is not SONET APS protection and should not be mistaken as such.

To initiate a Force Switch to protect in Release 2.x, ~~select~~click the **Maintenance** tab and the **Protection** tab.

Issue a Force Switch to Protect by highlighting the working card and ~~select~~clicking **Force**. A confirmation dialog appears. ~~Select~~Clicking **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.



A Force Switch to Protect results in a minor alarm on the designated working member of the protection group, as shown below.



To remove the Force Switch, go to the **Maintenance** tab and **Protection** tab and in the **Operation** field, ~~select~~click **Clear**. The associated alarms clear and the Force Switch is removed.

Manual Switch

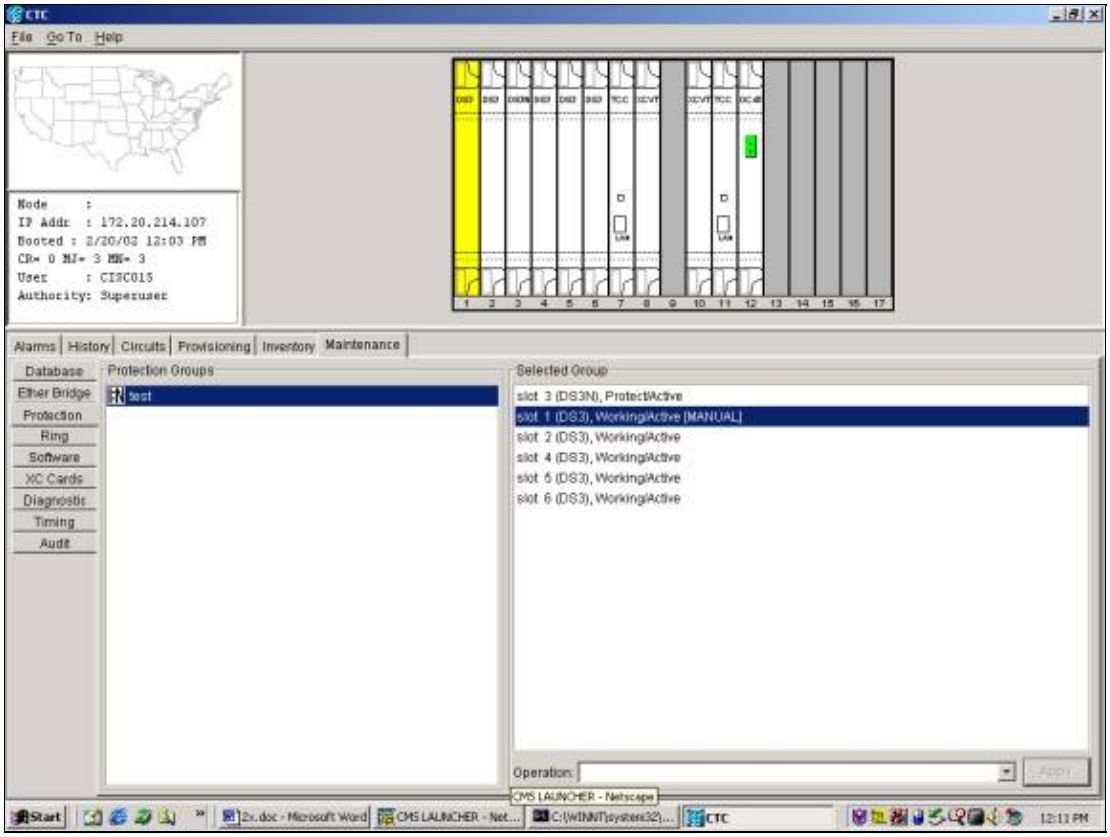
Initiating a Manual Switch switches all traffic to the designated protect card. If there is a failure on the protect card while the Manual Switch is in place, traffic switches back to the working card. Once the failure on the protect card is fixed, traffic switches back to the protect card.

Issuing the ~~C~~**clear** command removes the Manual Switch. In the 1:N case and the 1:1 revertive case, traffic returns to the working card immediately after the switch request is cleared. (The wait−to−restore timer is only activated by autonomous or physical switch conditions, not by software switches.)

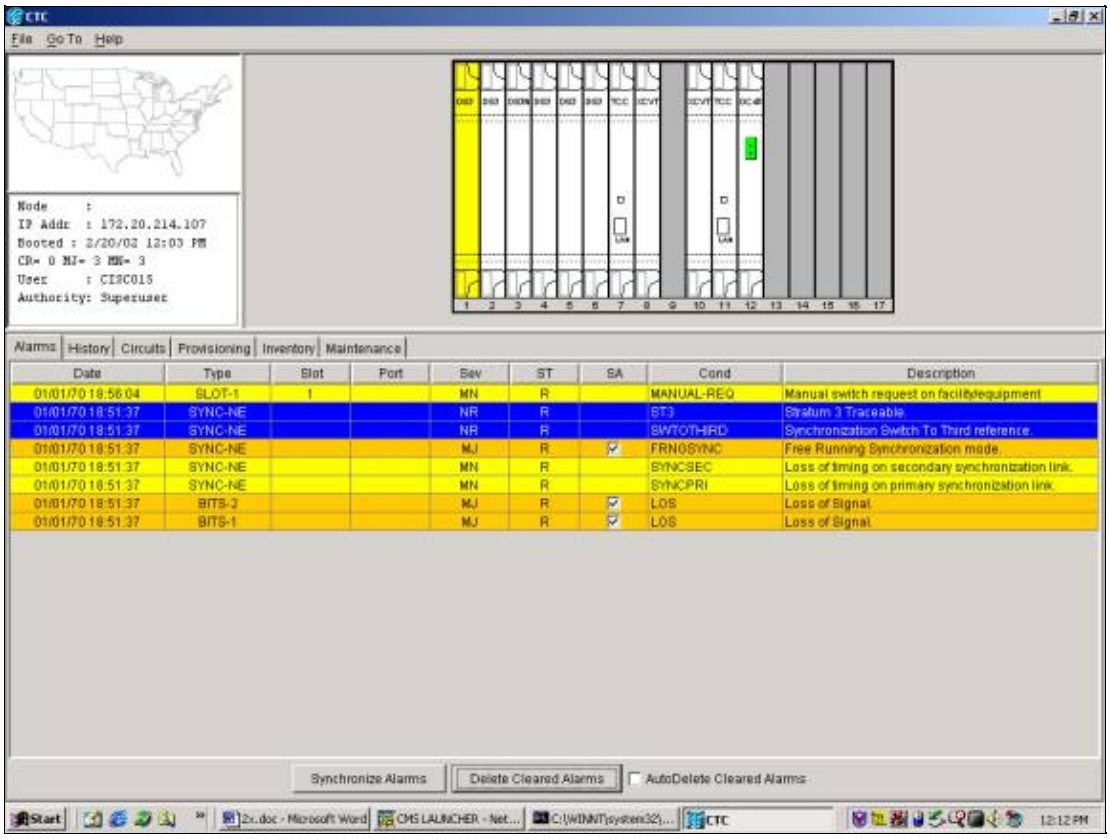
- In the 1:1 non−revertive case, traffic remains on the protect card indefinitely or until another failure or switch request occurs.
- In the 1:1 non−revertive case, if traffic was originally on the protect card, a Manual Switch request would switch the traffic to the working card with conditions analogous to those outlined above.

Note: A Force Switch overrides a Manual Switch. However, this is not SONET APS protection and should not be mistaken as such.

To initiate a Manual Switch to protect in Release 2.x, go to the **Maintenance** tab and **Protection** tab. ~~Select~~Click **Manual** from the **Operation** field and ~~select~~click **Apply**. A confirmation dialog appears. ~~Select~~Clicking **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.



A Manual Switch results in a minor alarm on the designated working member of the protection group, as shown below.



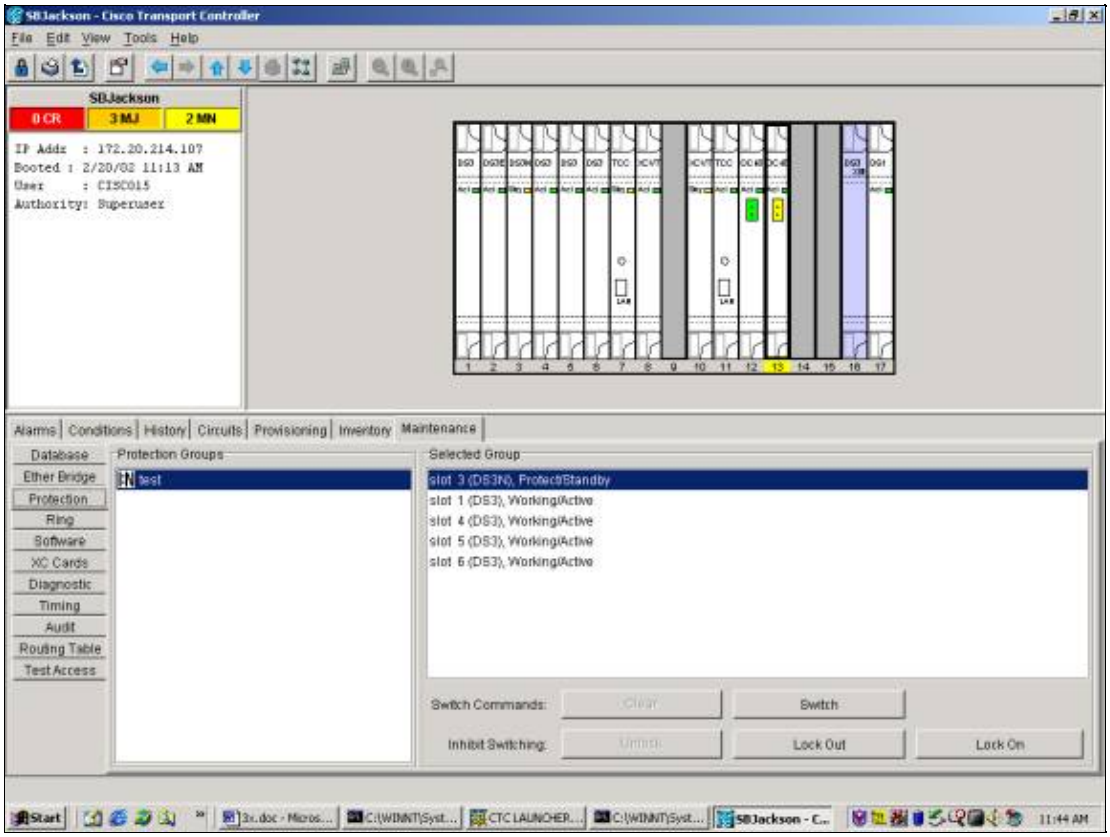
To remove the Manual Switch, go to the **Maintenance** tab and **Protection** tab. In the **Operation** field, ~~select~~click **Clear**. The associated alarms clear and the Force Switch is removed.

Release 3.x

In Release 3.x, the SONET APS terminology has been removed. The ~~15454~~Cisco ONS 15454 supports the following Maintenance functions for manipulating the working and protect cards:

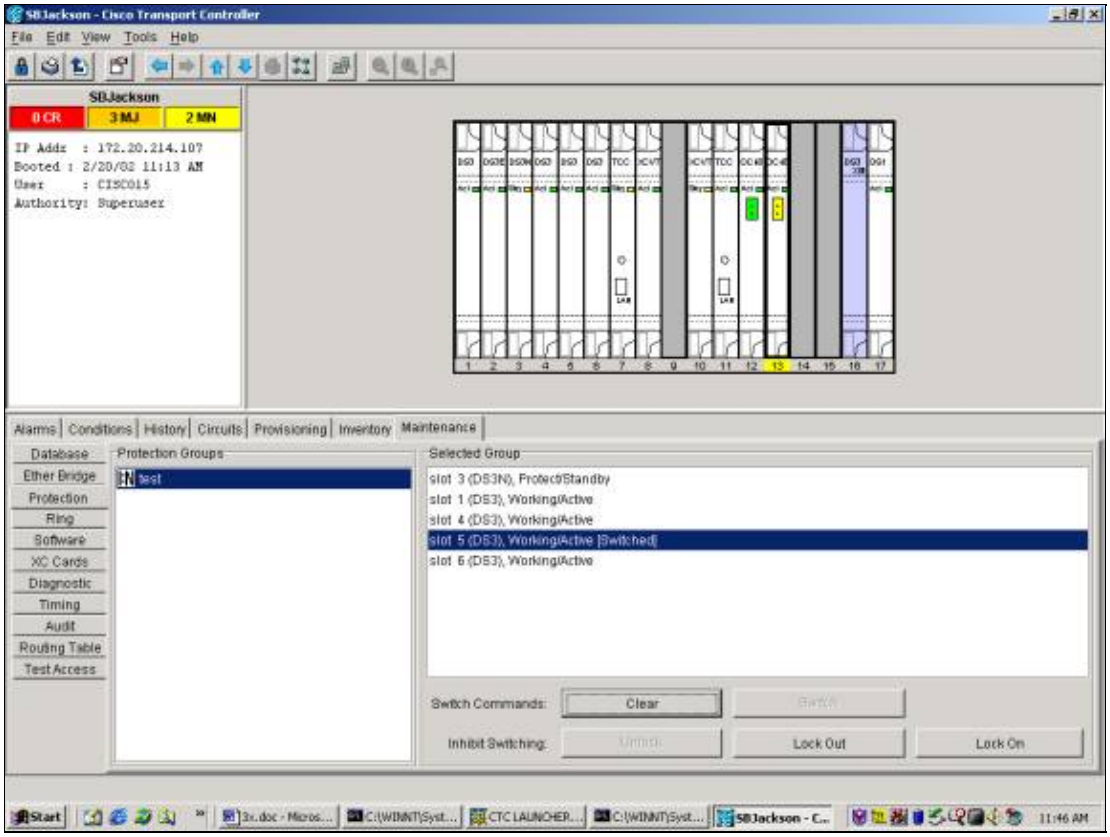
- SWITCH
- LOCK IN
- LOCK OUT
- UNLOCK
- CLEAR

Display these by ~~select~~clicking the **Maintenance** tab and the **Protection** tab. Select one of the displayed protection groups from the Protection Groups window. The options ~~will~~ change based on which member of the protection group is highlighted.

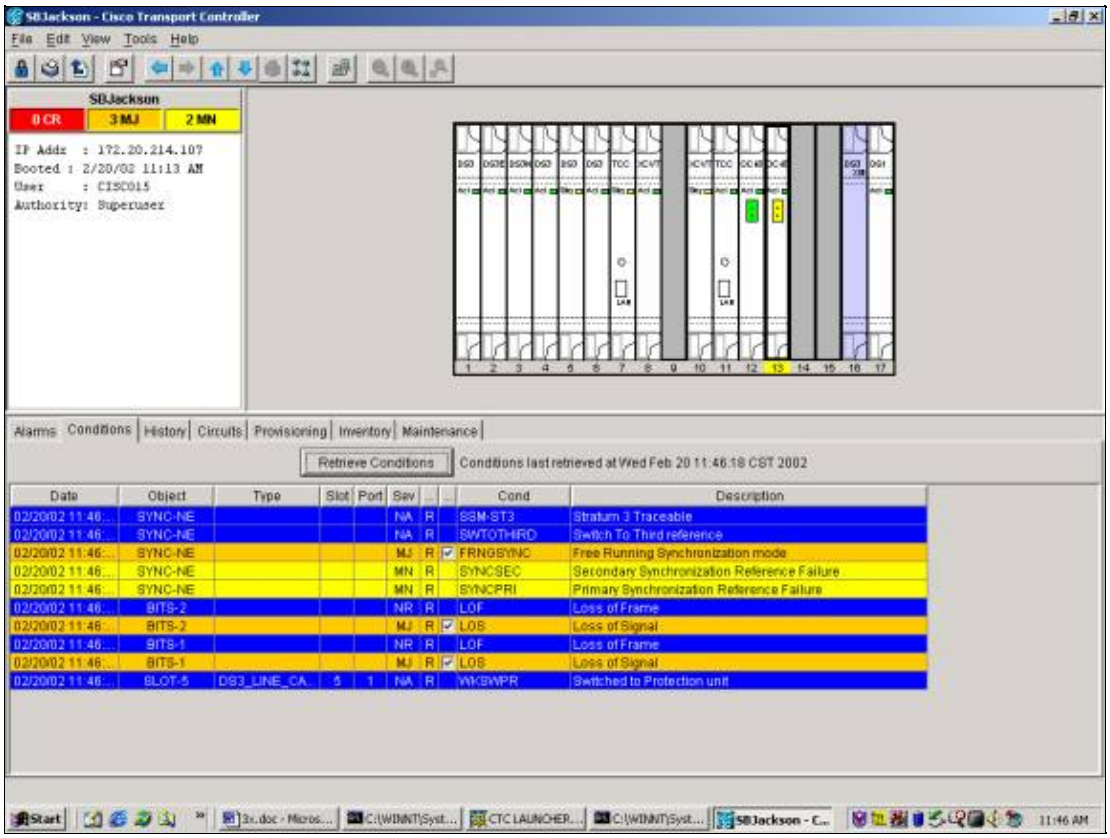


Switch

The ~~S~~**switch** command switches all traffic from the working card that it is issued against to the protect card. To initiate a Switch to Protect, highlight the working card and ~~select~~click **Switch**. A confirmation dialog appears. ~~Select~~Clicking **Yes** initiates the switch; ~~select~~clicking **No** cancels the switch request.



A Switch to Protect results in a condition, not an alarm, against the designated working member of the protection group, as shown below.



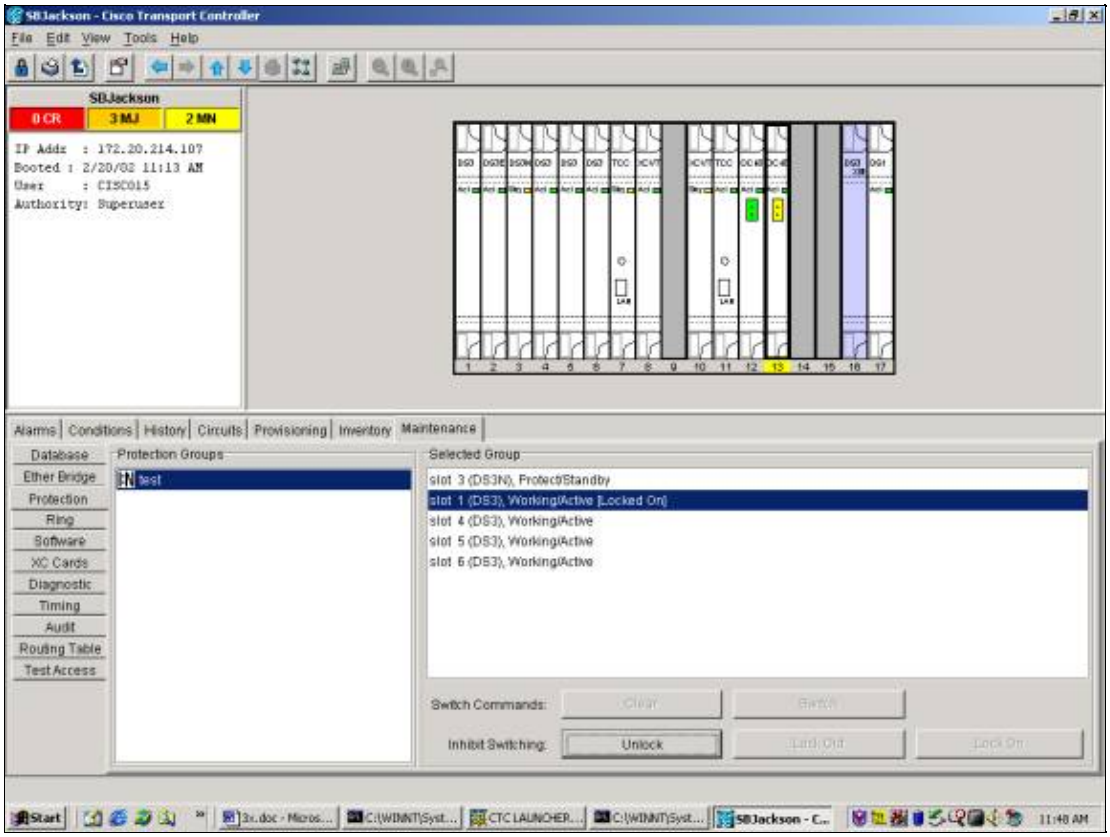
To remove the Switch, go to the **Maintenance** tab and **Protection** tab. In the **Operation** field, ~~select~~click **Clear**. The associated condition clears and the switch is removed.

Lock On/Lock Out

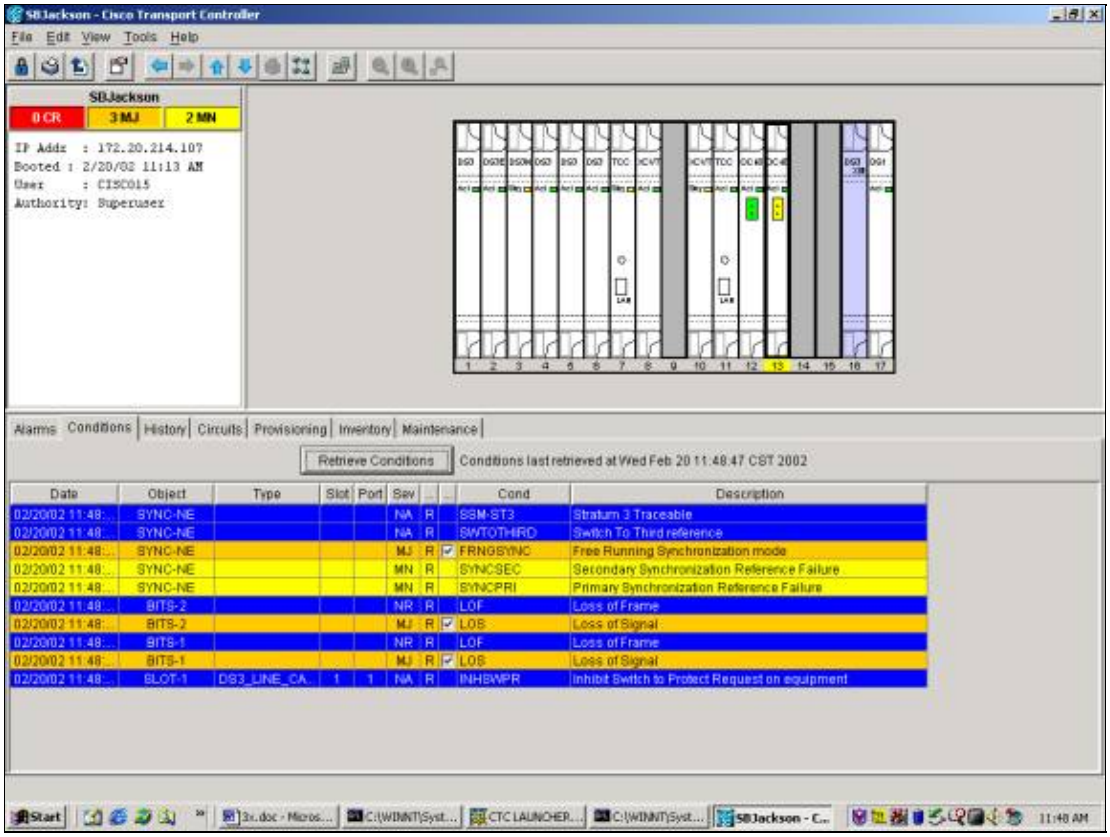
Protection switching in a 1:N or a 1:1 protection group can be inhibited by applying a lock on or lock out to a working or protect card. When traffic is on the working card, applying a lock on prevents traffic from switching from the working card to the protect card. To perform maintenance on a protect card, it is necessary to apply a lock on to each working member of the protection group to prevent switching.

If the working card fails while the lock on is Active, traffic ~~will~~ drops.

To initiate a lock on, ~~select~~click the **Maintenance** tab and the **Protection** tab with the working card highlighted. ~~Select~~Click **Lock On**. A confirmation dialog appears. ~~Selecting~~Clicking **Yes** initiates the lock on; ~~select~~clicking **No** cancels the lock on request.



A LOCK ON results in a condition, not an alarm, against the designated working member of the protection group, as shown below.

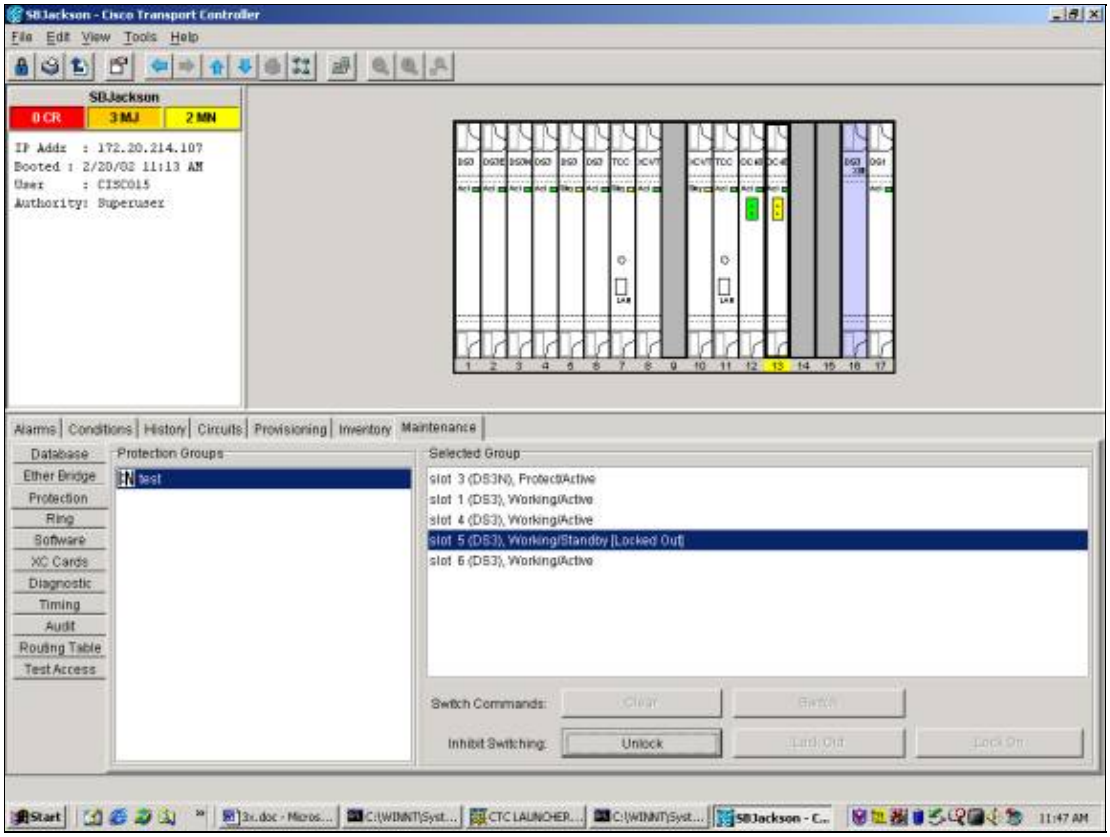


To remove the lock on, go to the **Maintenance** tab and **Protection** tab and in the **Operation** field, ~~select~~click **Unlock**. The associated condition clear and the lock on is removed.

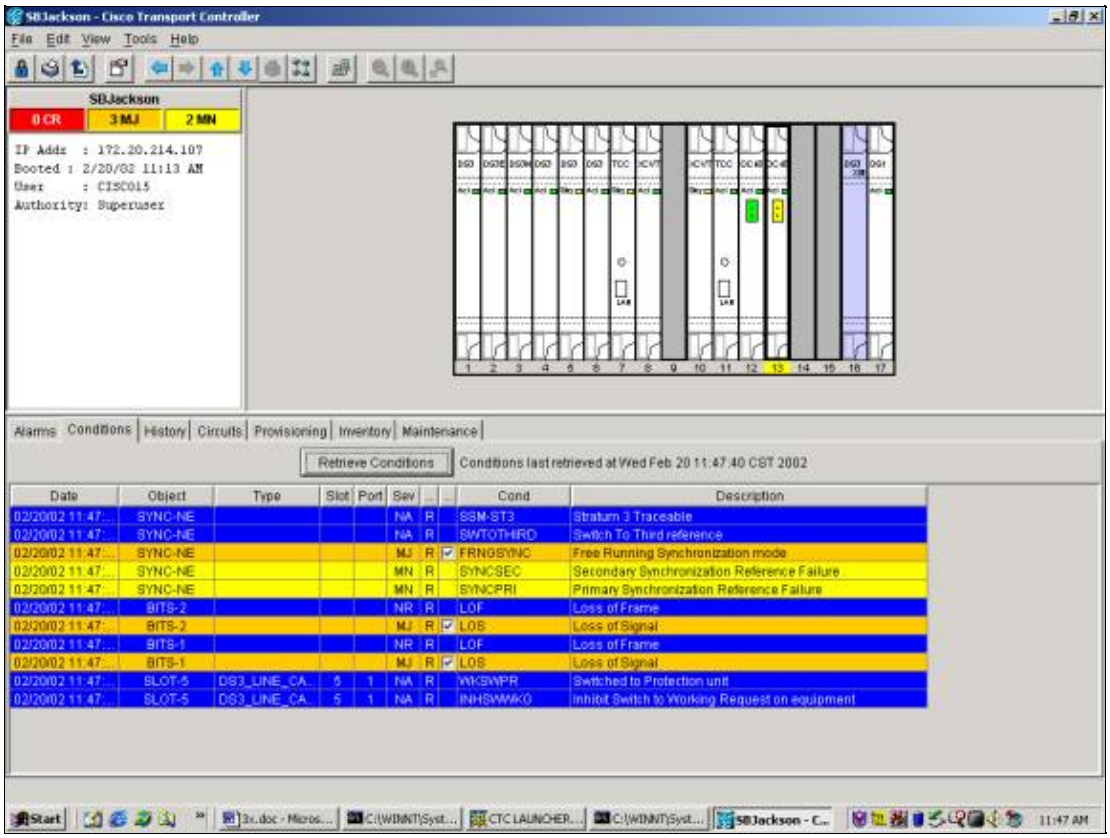
When traffic is on the working card, applying a lock out prevents traffic from switching from the protect card to the working card. To perform maintenance on a working card, it is necessary to apply a lock out to the working card after traffic has been switched to the protect card.

If the protect card fails while the lock on is Active, traffic drops.

To initiate a lock out, ~~select~~click the **Maintenance** tab and the **Protection** tab with the working card highlighted. ~~Select~~Click **Lock Out**. A confirmation dialog ~~will~~ appears. ~~Select~~Clicking **Yes** ~~will~~ initiates the lock out; ~~select~~clicking **No** ~~will~~ cancels the lock out request.



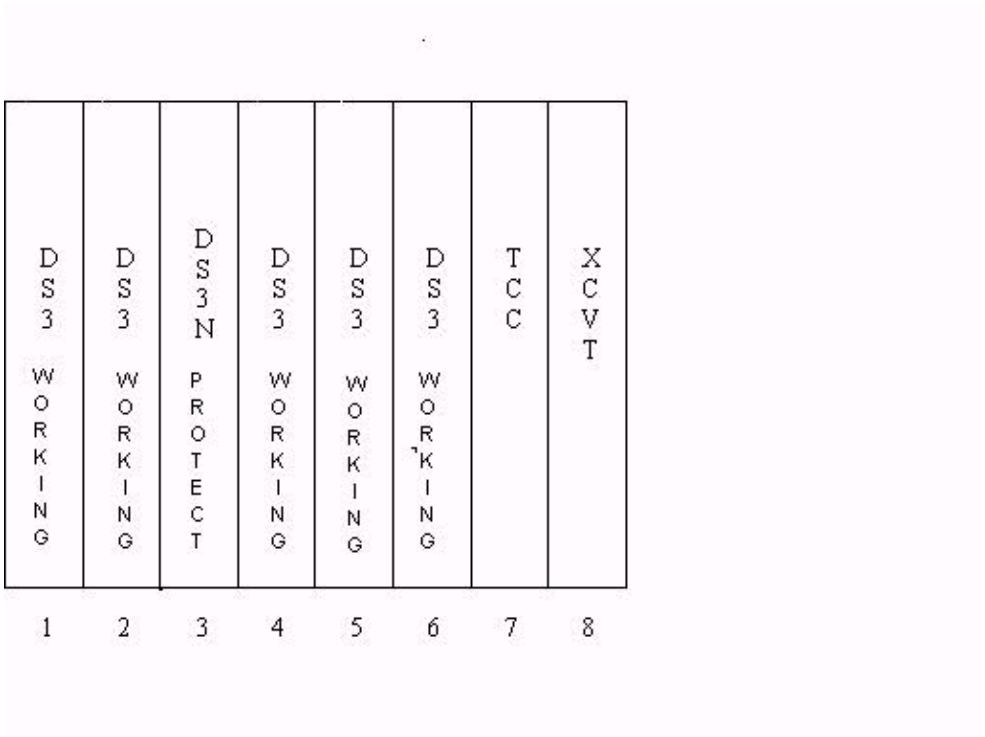
A LOCK OUT results in a condition, not an alarm, against the designated working member of the protection group, as shown below.



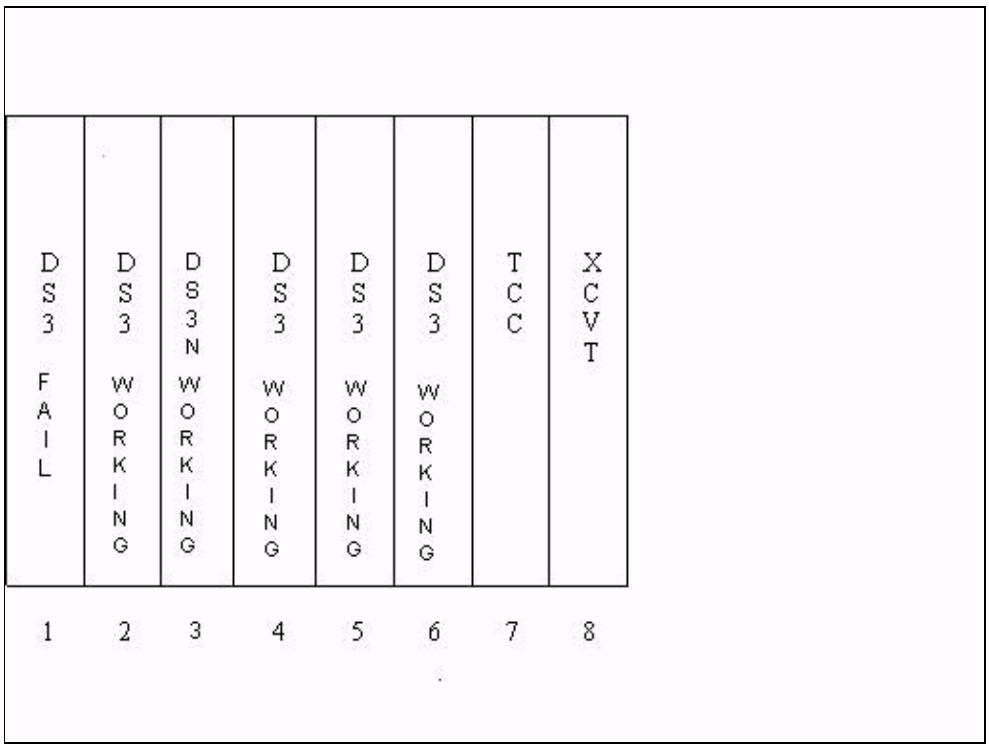
To remove the lock out, go to the **Maintenance** tab and **Protection** tab and in the **Operation** field, ~~select~~click **Unlock**. The associated condition ~~will~~ clears and the lock out ~~will be~~is removed.

Additional 1:N Operation

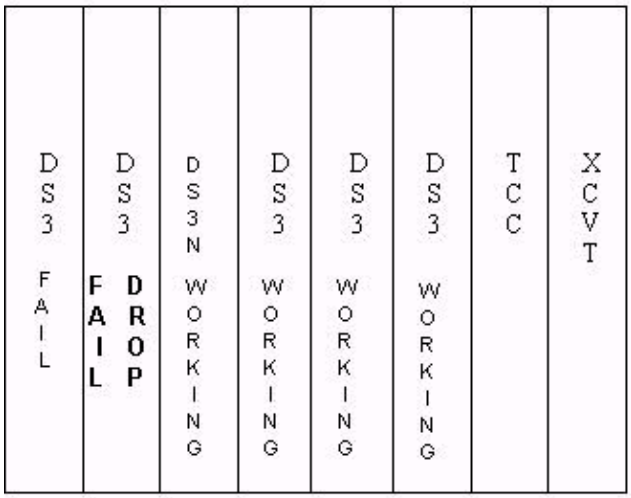
The 1:N protection scenario allows 1 protect card (in slot 3 or 15) to serve as protection for up to five working cards. In the example below, there is working traffic on cards 1, 2, 4, 5, and 6.



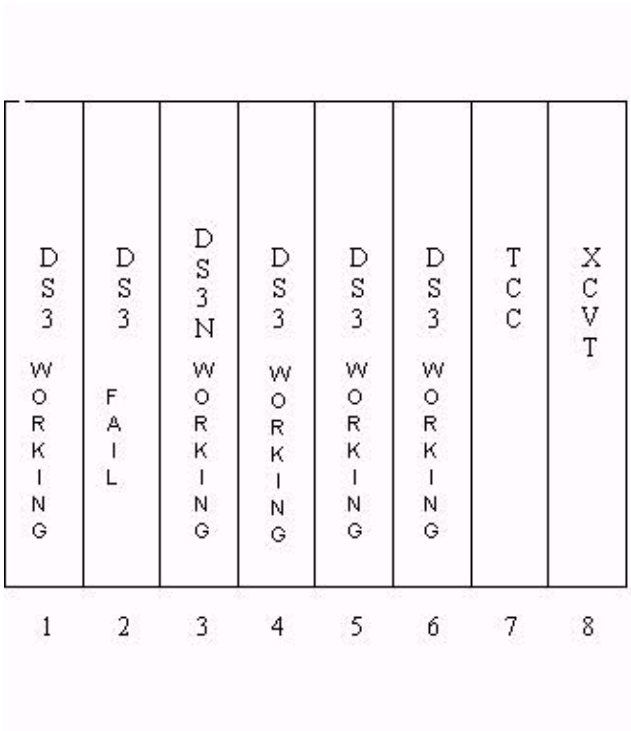
If working card #1 fails or a switch request is initiated on it, the traffic from working card #1 is switched to the protect card in slot 3.



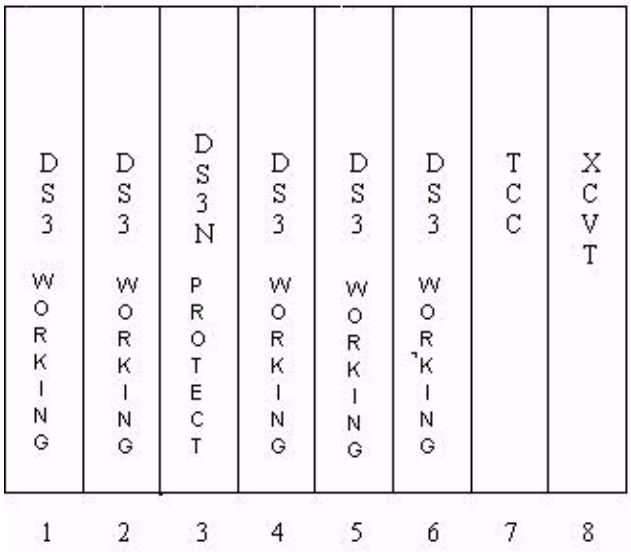
If working card #2 fails while this is occurring, the traffic on working card #2 drops. The traffic from working card #1 that now resides on the protect card in slot 3 is not affected.



If working card #1 is fixed or the switch request on that card is removed, traffic switches back to working card #1. The traffic from working card #2 is then switched to the protect card in slot 3, restoring that traffic.



When working card #2 is fixed or the switch request is removed, traffic switches back to working card #2, leaving the protect card in slot 3 available again.



Related Information

- **Technical Support − Cisco Systems**

Updated: Sep 15, 2005 Document ID: 20694