

Erstellen und Warten von ONS 15454-Schutzgruppen (CTC Software, Version 3.1 und früher)

Inhalt

[Einführung](#)

[Bevor Sie beginnen](#)

[Konventionen](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Schutzgruppen-Typen](#)

[0:1](#)

[1:1](#)

[1:N](#)

[1+1](#)

[Erstellen von Schutzgruppen](#)

[ONG 15454: 1+1 Protection Group-Einrichtung](#)

[ONG 15454 1:N Protection Group Setup](#)

[ONG 15454 1:1 Schutz-Setup](#)

[Löschen einer Schutzgruppe](#)

[Wartungsarbeiten](#)

[1+1 Wartung](#)

[1:N Wartung](#)

[Version 2.x](#)

[Version 3.x](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie verschiedene Typen von Schutzgruppen erstellt, gelöscht und verwaltet werden, die in der Cisco ONS 15454 verfügbar sind. Dieses Dokument umfasst DS1-, DS3-, DS3E-, DS3XM-, EC1- und OCn-Karten sowie Cisco Transport Controller (CTC)-Softwareversionen bis Version 3.1.

[Bevor Sie beginnen](#)

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips](#)

[Conventions.](#)

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco ONS 15454
- Cisco Transport Controller Version 3.1 oder frühere Version

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Schutzgruppen-Typen

Die Cisco ONS 15454 bietet je nach Kartentyp vier Schutzmechanismen:

0:1

Dieses Schutzschema wird auch als "ungeschützt" bezeichnet. Alle ~~15454-Cisco ONS 15454-~~Karten können in Steckplätzen 1-6 oder 12-17 als ungeschützt betrieben werden. Dies ist die Standardkonfiguration für Schutzgruppen.

1:1

Diese Schutzregelung wird auch als "One-for-One-Schutz" bezeichnet. In dieser Konfiguration wird eine Arbeitskarte mit einer Schutzkarte gekoppelt. Dieses Schutzsystem ist für alle elektrischen Karten verfügbar: DS1, DS3, DS3E, DS3XM und EC1. Die Arbeitskarte muss sich in einem gerade nummerierten Steckplatz befinden, und die Schutzkarte muss sich in einem benachbarten, ungeraden Steckplatz befinden. Wenn die funktionierende DS3-Karte beispielsweise in Steckplatz 4 eingesetzt wird, können Sie die DS3-Karte in Steckplatz 3 oder Steckplatz 5 einsetzen.

1:N

Diese Schutzregelung wird auch als "One-for-n-Schutz" bezeichnet. In dieser Konfiguration werden ein bis fünf Arbeitskarten einer Schutzkarte zugewiesen. Die maximale Anzahl der zu schützenden Arbeitskarten beträgt fünf. Dieses Schutzschema ist für DS1-, DS3- und DS3E-Karten verfügbar. Jede 1:N-Schutzgruppe muss eine Schutzkarte (DS1N-14, DS3N-12 oder DS3N-12E) enthalten, die in Steckplatz 3 oder 15 installiert werden muss. Sie müssen die entsprechende Arbeitskarte auf derselben Gehäusehälfte wie die Schutzkarte installieren. Wenn die DS3N-Karte beispielsweise in Steckplatz 3 installiert ist, können Sie die entsprechenden funktionierenden DS3-Karten in den Steckplätzen 1, 2, 4, 5 und 6 platzieren. Wenn die DS3N-Karte in Steckplatz 15 installiert ist, können Sie die entsprechenden Arbeitskarten in den

Steckplätzen 12, 13, 14, 16 und 17 platzieren. Die genaue Anzahl der zu schützenden Arbeitskarten hängt vom Typ der Karte und Rückwandplatine ab.

1+1

Diese Schutzregelung wird auch als "Eins-plus-Eins-Schutz" bezeichnet. In dieser Konfiguration ist ein funktionierender optischer Port durch einen anderen optischen Port auf einer anderen Karte geschützt. Dieses Schutzschema ist für alle OCn-Ports verfügbar. Beachten Sie, dass dieses Schutzschema für Ports gilt, nicht für Karten. Einige Regeln zum Erstellen optischer Schutzgruppen werden am besten in einem Beispiel mit zwei OC3-Karten mit 4 Ports veranschaulicht.

- Arbeits- und Schutzports müssen sich nicht in benachbarten Steckplätzen befinden, um eine Schutzgruppe zu bilden. Befindet sich eine OC3-Karte in Steckplatz 2 und eine andere OC3-Karte in Steckplatz 13, können die Ports dieser Karten Mitglied einer Schutzgruppe sein.
- Es gibt keine designierten Arbeits- und Schutzsteckplätze. In diesem Beispiel kann Port 1 von Steckplatz 2 der funktionierende Port und Port 1 von Steckplatz 13 der geschützte Port sein. Alternativ kann Port 1 von Steckplatz 13 der funktionierende Port und Port 1 von Steckplatz 2 der geschützte Port sein.
- Nur entsprechende Steckplätze auf verschiedenen Karten können einer Schutzgruppe angehören. Wenn Port 1 an Steckplatz 2 der funktionierende Port ist, kann nur Port 1 an Steckplatz 13 als Schutzport dienen. Die Ports 2, 3 und 4 sind nicht für den Schutz von Ports qualifiziert. Wenn Port 1 an Steckplatz 2 der funktionierende Port ist, können auch die Ports 2, 3 und 4 an Steckplatz 2 nicht als Schutzport dienen.
- Sobald ein Port einer Karte als funktionierend oder als schützend gekennzeichnet wurde, müssen die übrigen Ports derselben Karte gleich gekennzeichnet sein oder ungeschützt bleiben. Angenommen, Port 1, Steckplatz 2 ist ein funktionierender Port und Port 1, Steckplatz 13 ist sein Schutzport in einer Schutzgruppe. Port 2 an Steckplatz 1 kann ein funktionierender Port in einer anderen Schutzgruppe sein oder ungeschützt bleiben. Es kann nicht als Schutzport in einer anderen Schutzgruppe verwendet werden. Ebenso kann Port 2 an Steckplatz 13 als Schutzport in einer anderen Schutzgruppe dienen oder ungeschützt bleiben. Es kann nicht als funktionierender Port in einer anderen Schutzgruppe verwendet werden.

Erstellen von Schutzgruppen

Alle Karten und Ports sind standardmäßig ungeschützt. Sie müssen Schutzgruppen bereitstellen. Zwei Beispiele zum Erstellen von Schutzgruppen sind:

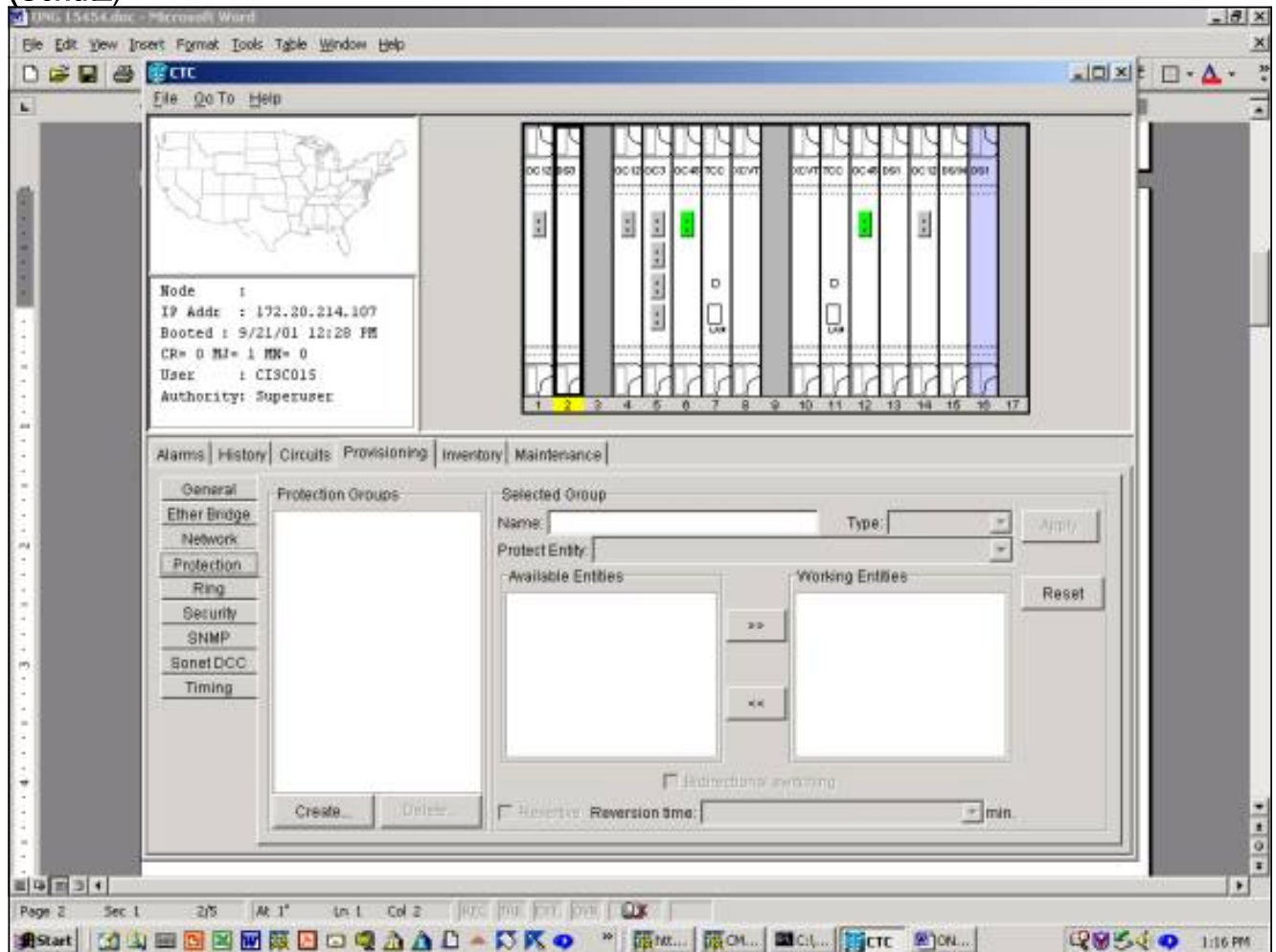
- 1+1
- 1:N

Hinweis: Eine 1:1-Schutzgruppe ist einfach ein Sonderfall der 1:N-Schutzgruppe.

ONG 15454: 1+1 Protection Group-Einrichtung

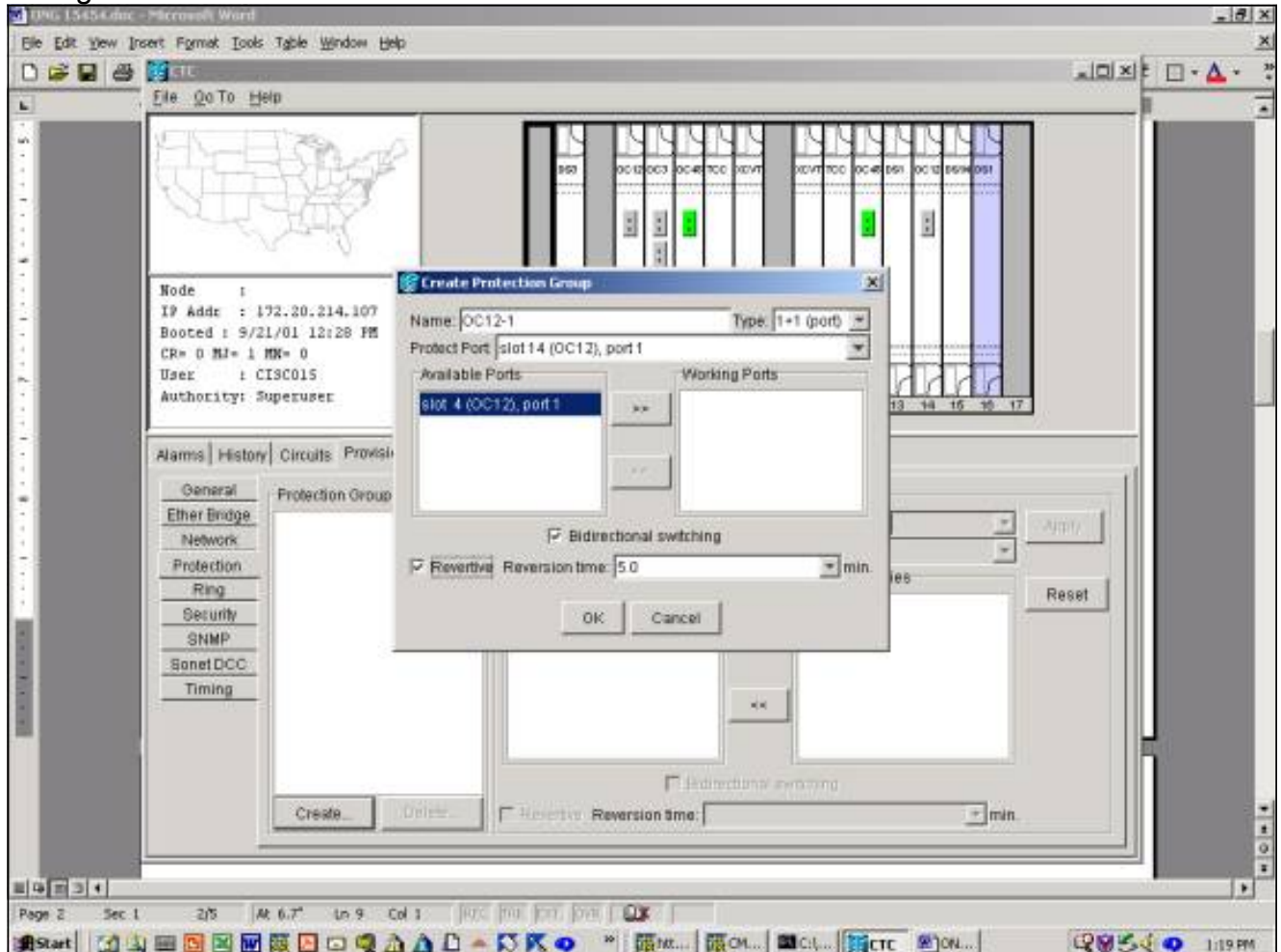
Im folgenden Beispiel wird veranschaulicht, wie eine 1+1-Schutzgruppe mithilfe von zwei OC12-Karten eingerichtet wird. Dieses Beispiel gilt für alle OCn-Karten auf der [15454-Cisco ONS 15454](#).

1. Klicken Sie in der Ansicht auf der Gehäuseebene auf die Registerkarte **Provisioning** (Bereitstellung) und anschließend auf die Registerkarte **Protection** (Schutz).

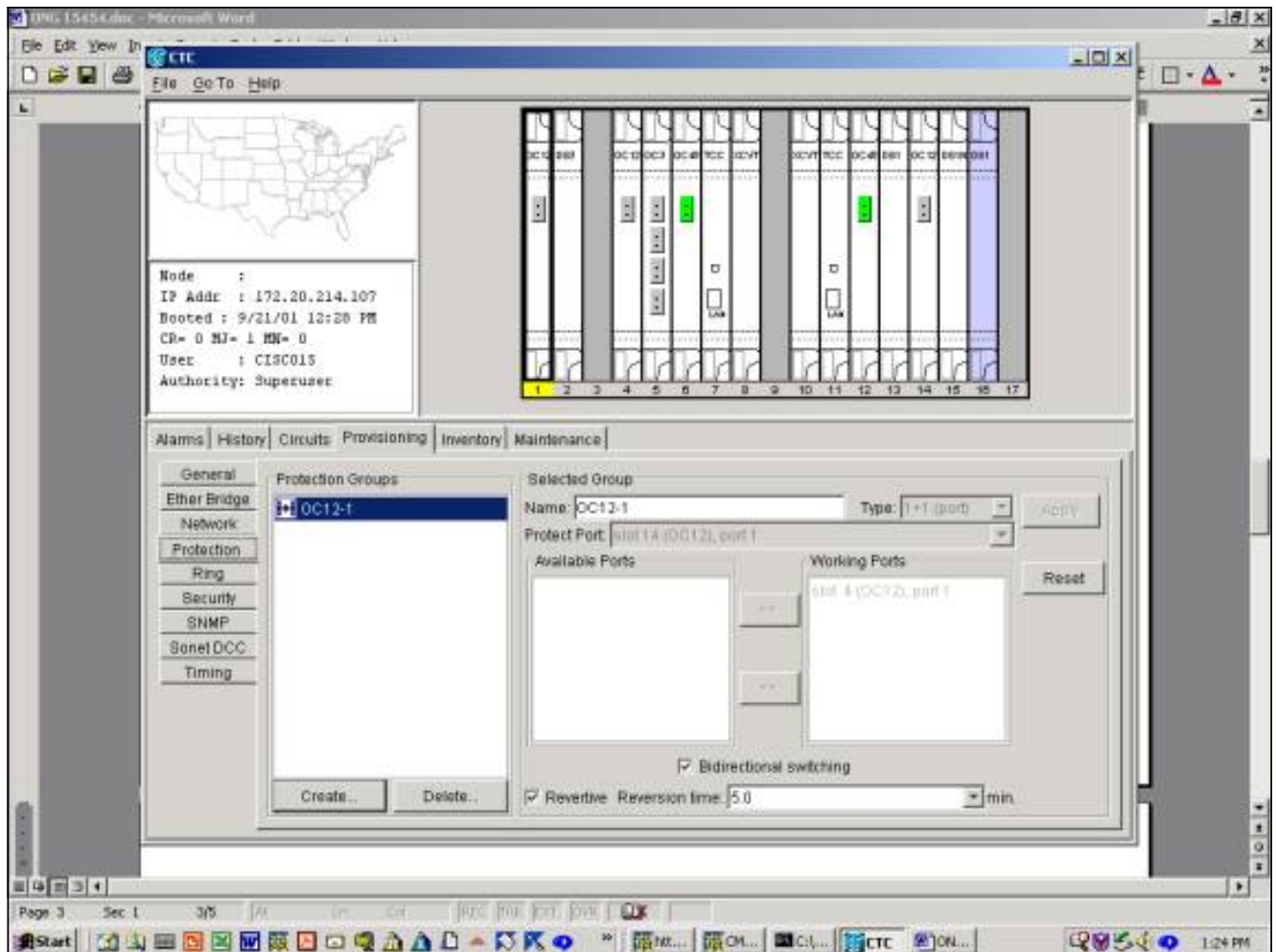


2. **Auswählen**—Klicken Sie auf Erstellen, um das Fenster Schutzgruppe erstellen zu öffnen.
3. Geben Sie im Feld **Name** den Namen dieser Schutzgruppe ein. In diesem Beispiel lautet der Name OC12-1.
4. Wählen Sie im Feld **Typ** im Dropdown-Menü die Option 1+1 (Port) aus.
5. Wählen Sie im Dropdown-Menü im Feld **Protect Port** einen OC-Steckplatz und einen Port aus. Wählen Sie in diesem Beispiel Steckplatz 14 (OC 12), Port 1 als Schutzport aus.
6. Wählen Sie im Feld **Verfügbare Ports** die entsprechende Karte und den entsprechenden Anschluss aus, und markieren Sie diese. Ziehen Sie diesen Steckplatz bzw. Port in das Fenster Working Ports (Arbeitende Ports). Wählen Sie in diesem Beispiel Steckplatz 4 (OC 12) und Port 1 als funktionierenden Port aus.
7. Das Kontrollkästchen **Bidirectional Switching** (Bidirektionales Switching) ermöglicht Ihnen die Wahl zwischen unidirektionalem oder bidirektionalem Switching. Das Überprüfen dieses Kästchens ermöglicht bidirektionales Switching, d. h. bei einem Ausfall werden sowohl die Übertragungs- als auch die Empfangs-Ports aktiviert. ~~werden~~—Switch zu den Schutzanschlüssen wechseln.
8. Das Kontrollkästchen **Revertive** (Umkehrende) oder Non-Revertive-Switching (Umkehrendes Switching). Beim Revertive Switching wechselt der Datenverkehr zurück zur Arbeitskarte, nachdem der ursprüngliche Fehler behoben oder der Software-Switch entfernt wurde. Sie können die Zeitspanne in Minuten zwischen der Behebung des Fehlers und dem Umschalten des Datenverkehrs zur Arbeitsstätte angeben. (Die Umstellungszeit gilt nur für autonome Switches, wie z. B. physische Ausfälle, und nicht für Software- oder vom Benutzer initiierte

Switches. Löschen eines Software-Switches **werden-führt dazu**, dass der Datenverkehr sofort zurück zur Arbeitsstätte umschaltet.) Die Standardumstellungszeit beträgt fünf Minuten. Beim nicht-reversitiven Switching wechselt der Datenverkehr nach der Behebung des ursprünglichen Fehlers oder nach der Bereinigung des Software-Switches nicht wieder zur Arbeitskarte zurück. Der Datenverkehr kann auf unbestimmte Zeit über die zugewiesene Schutzkarte oder den zugewiesenen Port erfolgen, ohne dass die Switching-Funktionalität oder -Funktion beeinträchtigt wird. Wenn Sie die Option Nicht-Revertiv auswählen, ist das Feld **Reversion Time** nicht verfügbar.



9. Klicken Sie auf **OK** **werden-beendet** die Bereitstellung und **erstellt** die Schutzgruppe.



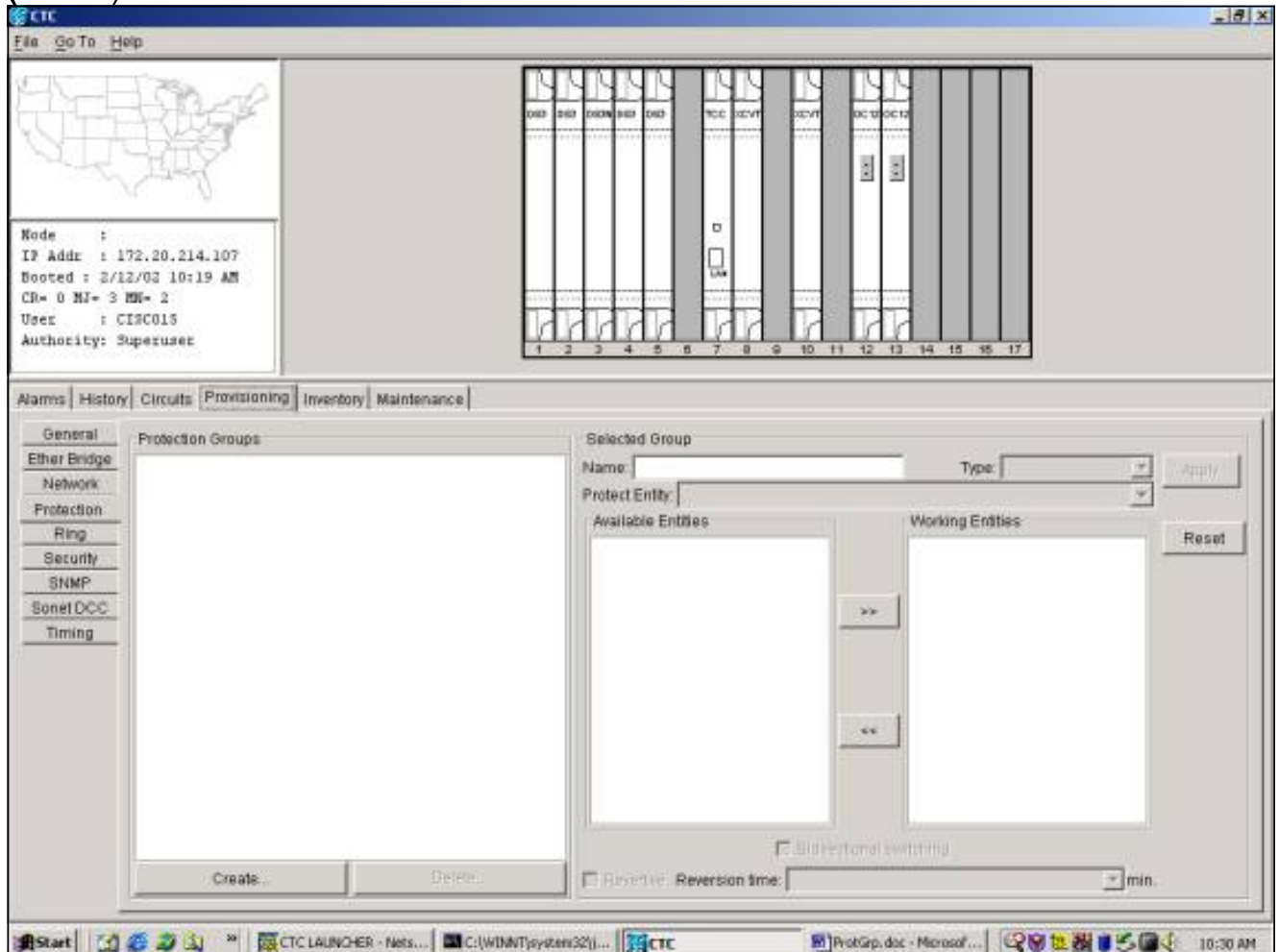
ONG 15454 1:N Protection Group Setup

Das folgende Beispiel gilt für die Einrichtung von DS3-, DS3E- oder DS1-Karten in einer 1:N-Schutzgruppe. Die Anzahl der Arbeitskarten hängt vom Typ der Rückwandplatine auf der Seite des Chassis, in dem die Schutzgruppe erstellt wird.

Backplane-Typ	Für DS3 und DS3E zulässige Arbeitssteckplätze	Für DS1 berechnete Arbeitssteckplätze
SMB-84	1:5 Maximal 1, 2, 4, 5, 6 (3 ist der Sicherungssteckplatz) 12, 13, 14, 16, 17 (15 ist der Sicherungssteckplatz)	1:5 Maximal 1, 2, 4, 5, 6 (3 ist der Sicherungssteckplatz) 12, 13, 14, 16, 17 (15 ist der Sicherungssteckplatz)
BNC-24	1:2 Maximal 2, 4 (3 ist der Sicherungssteckplatz) 14, 16 (15 ist der Sicherungssteckplatz)	Nicht verfügbar
BNC-48	1:4 Maximal 1, 2, 4, 5 (3 ist der Sicherungssteckplatz) 13, 14, 16, 17 (15 ist der Sicherungssteckplatz)	Nicht verfügbar

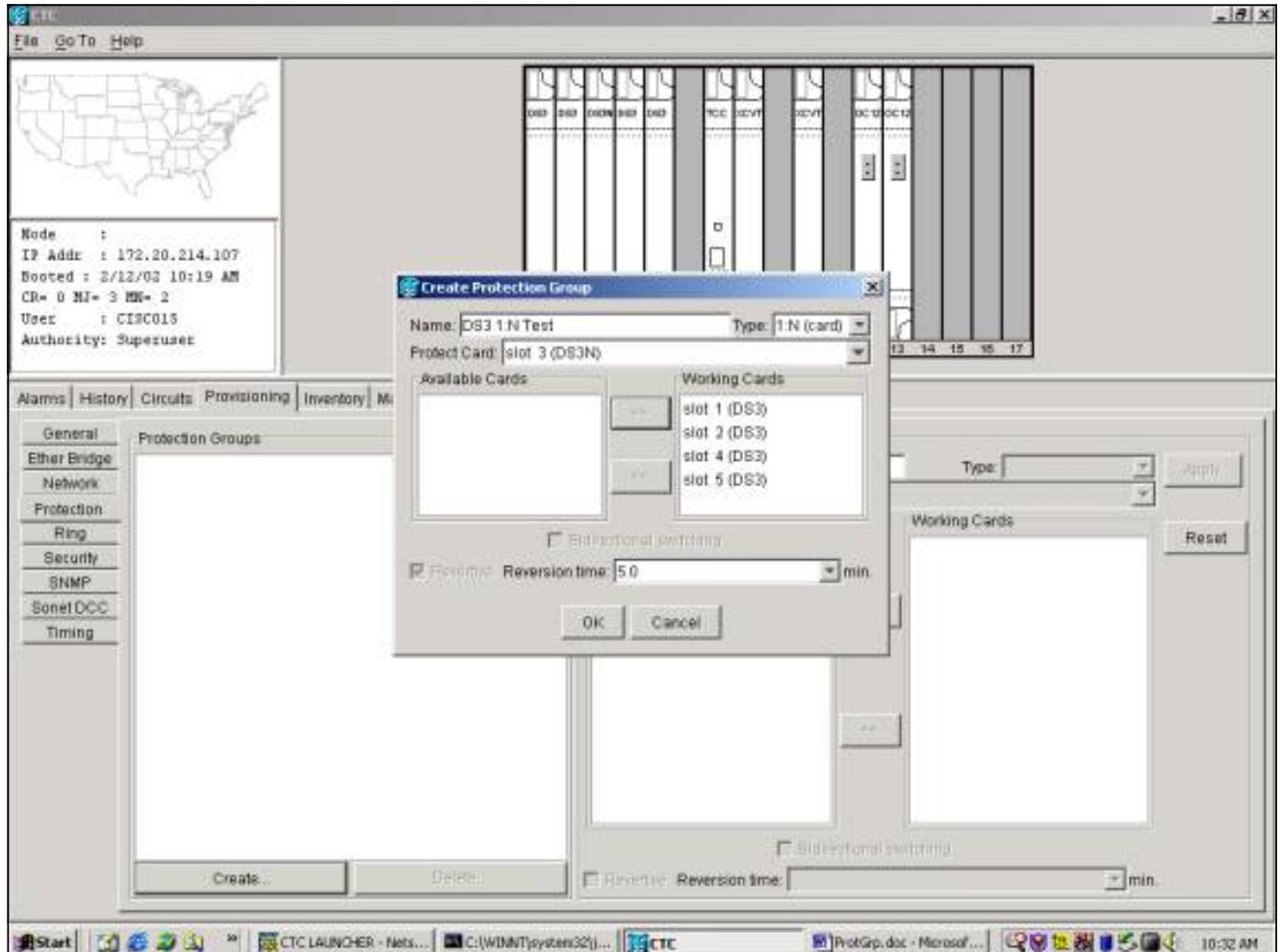
In diesem Beispiel wird eine Kombination aus DS3- und DS3E-Karten verwendet. Damit die zusätzliche DS3E-Funktionalität optimal genutzt werden kann, muss die Schutzkarte DS3N-12E sein.

1. Klicken Sie in der Ansicht auf der Gehäuseebene auf die Registerkarte **Provisioning** (Bereitstellung) und anschließend auf die Registerkarte **Protection** (Schutz).

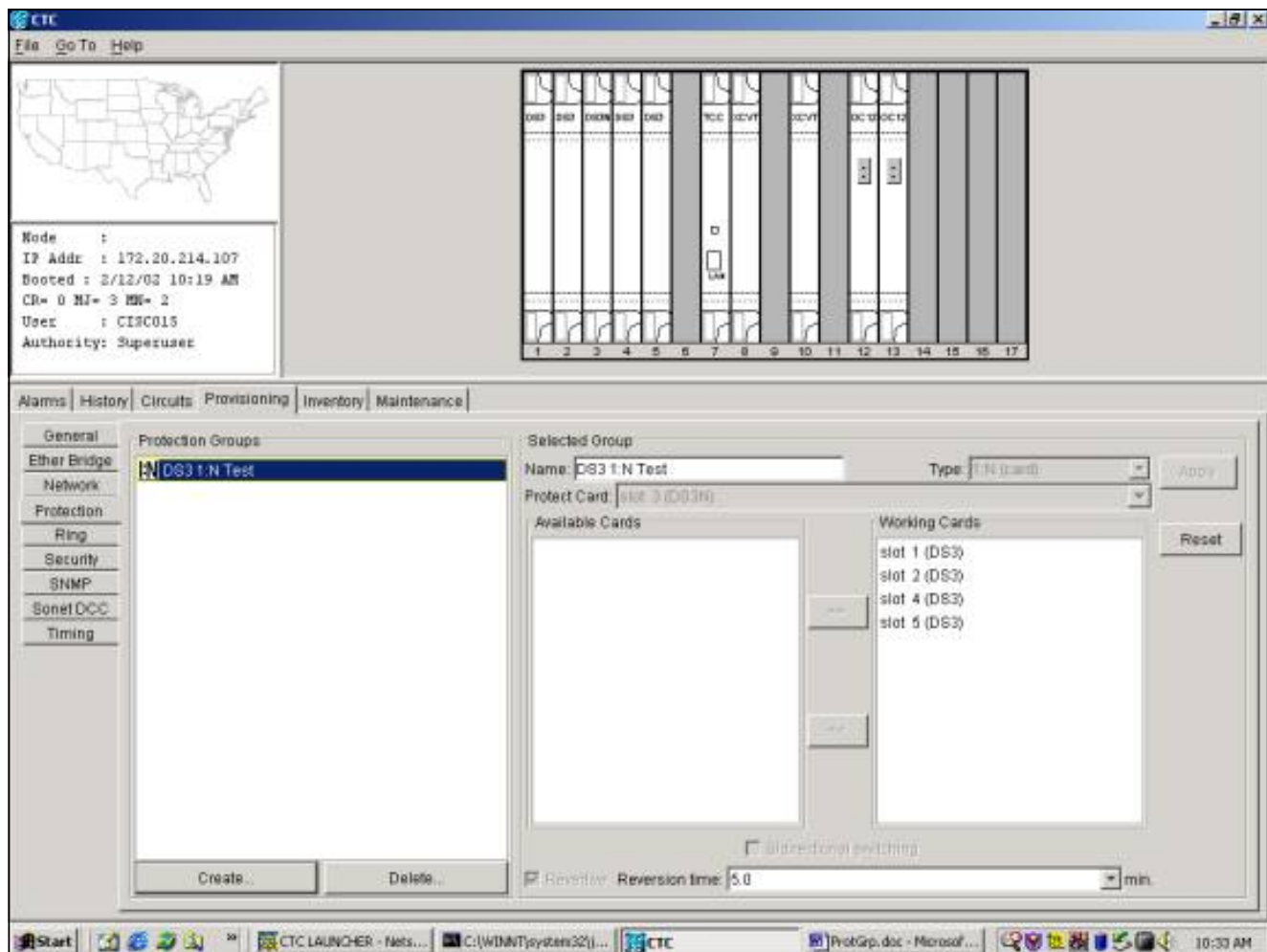


2. Auswählen-Klicken Sie auf Erstellen, um das Fenster Schutzgruppe erstellen zu öffnen.
3. Geben Sie im Feld **Name** den Namen dieser Schutzgruppe ein. In diesem Beispiel lautet der Name DS3 1:N Test.
4. Wählen Sie im Feld **Typ** im Dropdown-Menü die Option 1:N (Karte) aus.
5. Wählen Sie im Feld **Protect Card** den Steckplatz aus, der die DS3N-Karte enthält, entweder Steckplatz 3 oder Steckplatz 15, aus dem Dropdown-Menü. Wählen Sie in diesem Beispiel Steckplatz 3 (DS3N) als Schutzeinheit aus.
6. Im Feld **Available Cards (Verfügbare Karten)** werden alle DS3-Karten in der Chassis-Hälfte angezeigt, unabhängig davon, ob die Backplane Verbindungen zu allen Karten unterstützen kann oder nicht. Wählen Sie eine oder mehrere DS3-Karten aus, und markieren Sie sie. Verwenden Sie den Doppelpfeil, um sie in das Fenster Arbeitskarten zu verschieben. In diesem Beispiel wurden alle vier zur Auswahl stehenden DS3-Karten als Arbeitskarten ausgewählt.
7. Das Kontrollkästchen **Bidirectional Switching** (Bidirektionales Switching) ist ausgegraut und nicht verfügbar. DSn-Karten schalten auf Kartenebene und nicht auf den einzelnen Tx/Rx-Port um. Das Kontrollkästchen **Revertive** ist ausgegraut und nicht verfügbar. Standardmäßig ist die 1:N-Schutzgruppe reversibel, sodass der Datenverkehr nach der Behebung des ursprünglichen Fehlers oder nach der Bereinigung des Software-Switches wieder auf die

Arbeitskarte umschaltet. Sie können die Zeitdauer in Minuten festlegen, die **werden** zwischen dem behobenen Ausfall und dem Umschalten des Verkehrs zur Arbeitsstätte. (Die Umstellungszeit gilt nur für autonome Switches, wie z. B. physische Ausfälle, und nicht für Software- oder vom Benutzer initiierte Switches. Löschen eines Software-Switches **werden führt dazu**, dass der Datenverkehr sofort zurück zur Arbeitsstätte umschaltet.) Die Standardumstellungszeit beträgt fünf Minuten.



8. Durch Klicken auf **OK** wird die Bereitstellung abgeschlossen und die Schutzgruppe erstellt.



ONG 15454 1:1 Schutz-Setup

Das Einrichten von DS3-, DS3E- oder DS1-Karten in einer 1:1-Schutzgruppe ist ein Sonderfall im 1:N-Fall. Jede DS3-12 oder DS3-12N kann als funktionierende oder geschützte Karte dienen. Die Arbeits- und Schutzkarten müssen sich in benachbarten Steckplätzen befinden, wobei sich die Arbeitskarte im geraden Steckplatz und die Schutzkarte im ungeraden Steckplatz befindet. Auch hier hängen die für den Arbeitsverkehr verfügbaren Steckplätze vom Typ der Chassis-Backplane ab.

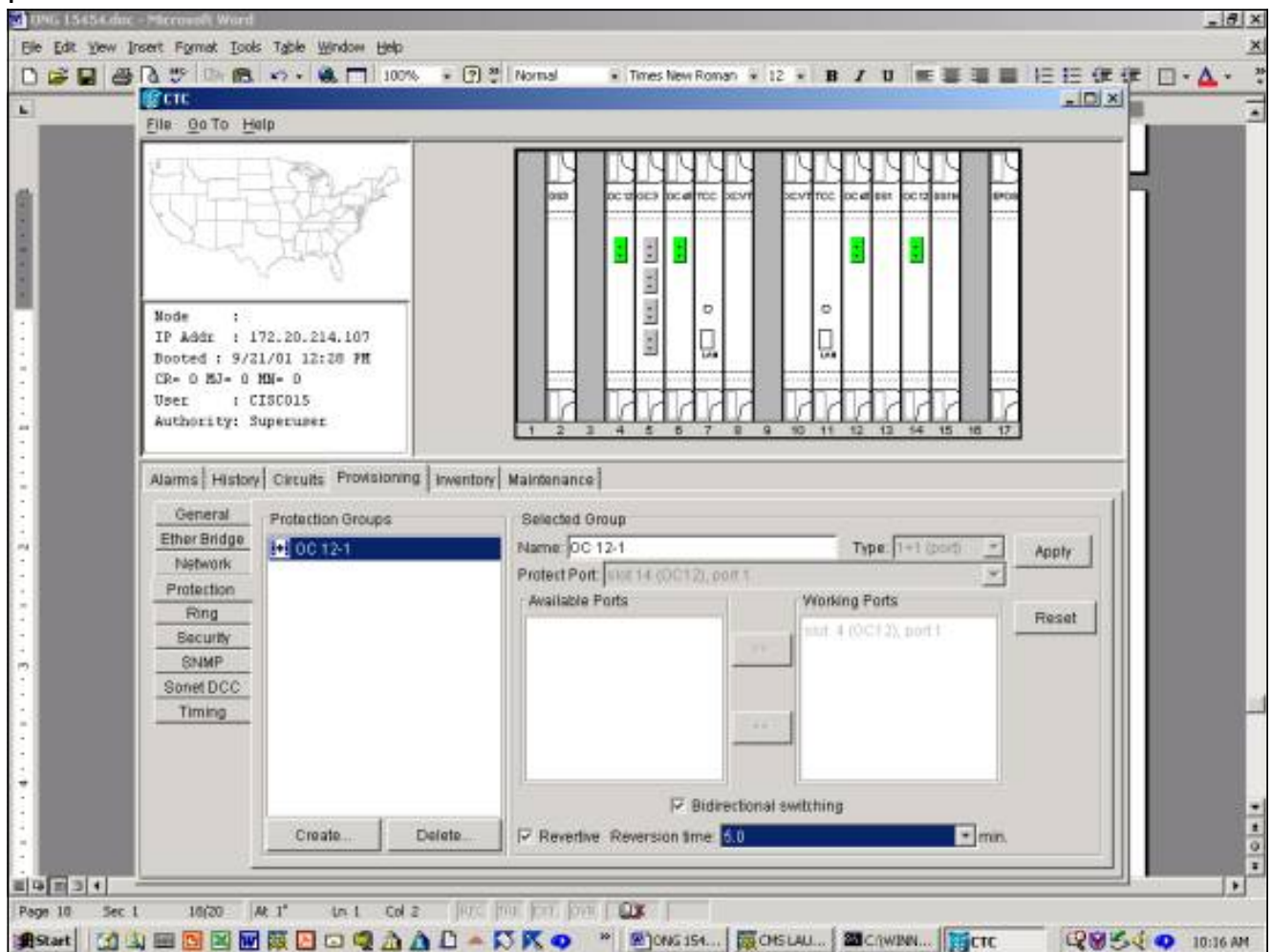
Um eine 1:1-Schutzgruppe zu erstellen, befolgen Sie das obige Beispiel 1:N und wählen Sie die entsprechenden Karten und Steckplätze aus.

Löschen einer Schutzgruppe

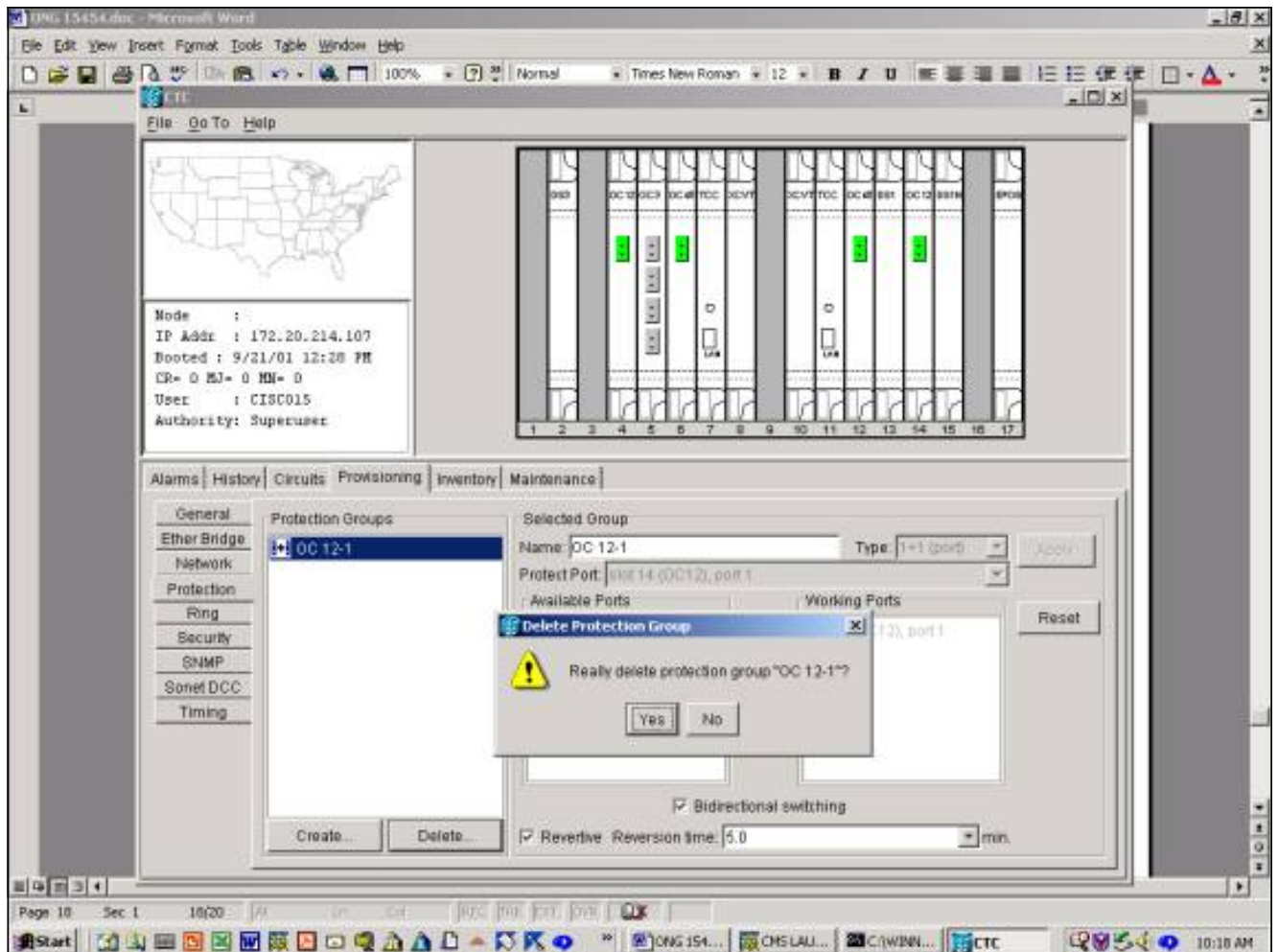
Das Verfahren zum Löschen einer Schutzgruppe ist unabhängig vom Schutzschema (1+1, 1:1, 1:N) identisch.

Um eine Schutzgruppe zu löschen, klicken Sie in der Shelf-Ansicht auf die Registerkarte **Provisioning** und dann auf die Registerkarte **Protection (Schutz)**. Wählen Sie im Fenster Schutzgruppe die Schutzgruppe aus, die gelöscht werden soll. In diesem Beispiel löschen wir eine OC12-Schutzgruppe.

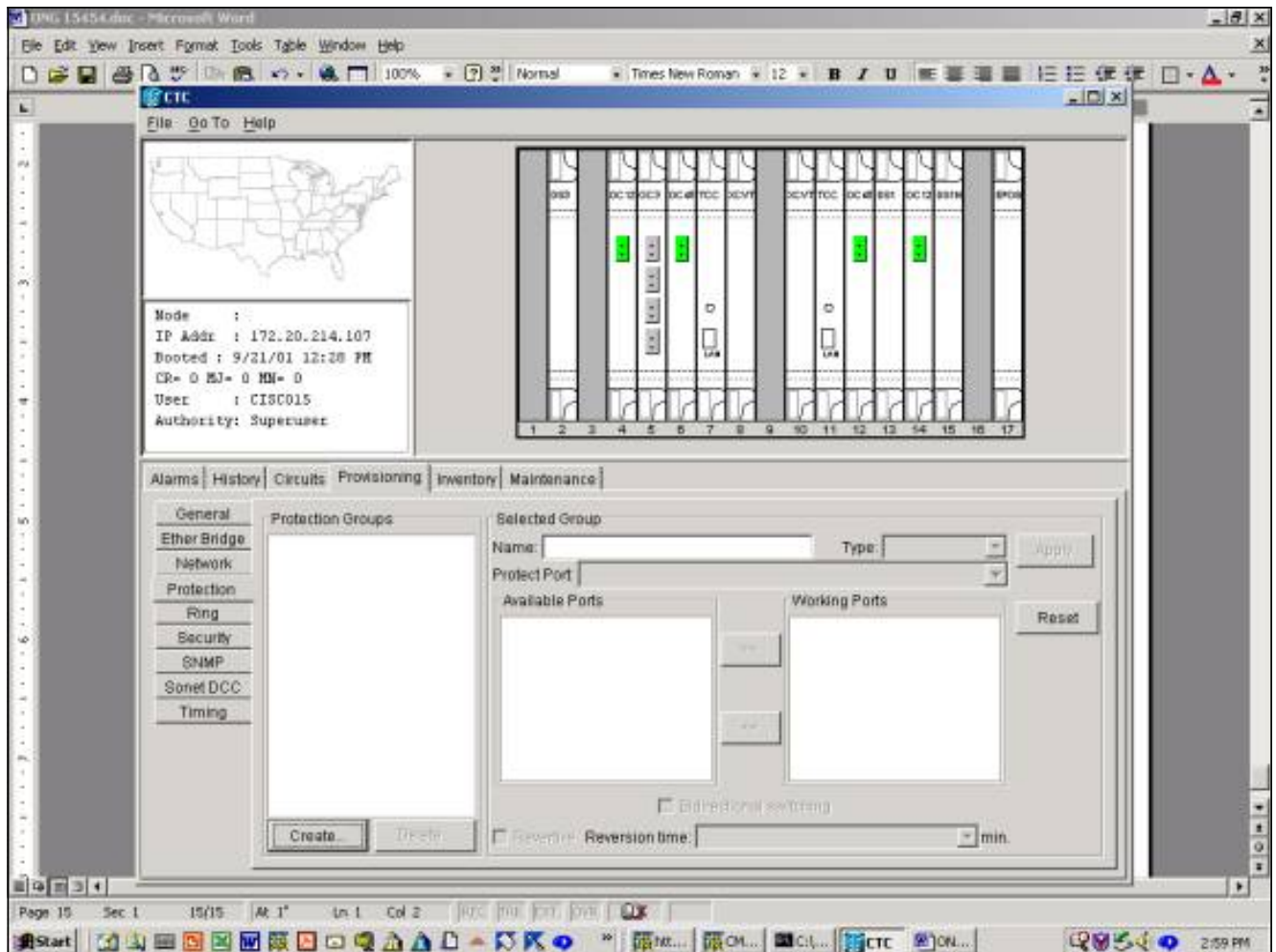
1. Markieren Sie die Schutzgruppe OC12 und anschließend **auswählen-klicken <-Löschen >**



2. Es wird ein Dialogfeld angezeigt, in dem Sie den Löschvorgang der Schutzgruppe bestätigen müssen.



3. So löschen Sie die Schutzgruppe: auswählen-Klicken Sie auf Ja.



Die Schutzgruppe wurde erfolgreich gelöscht.

Wartungsarbeiten

Die verfügbaren Wartungsvorgänge hängen von der Art der von Ihnen erstellten Schutzgruppe ab.

1+1 Wartung

Das 1+1-Schutzschema gilt für optische Ports und folgt der SONET-Switching-Hierarchie, angepasst an GR-253 und unten dargestellt. Einige dieser Funktionen, wie etwa die Ausübung, gelten nicht für das lineare 1+1-Schutzsystem. Die 1+1-Schutzgruppe erkennt derzeit keine hohen oder niedrigen Switching-Prioritäten.

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](#)

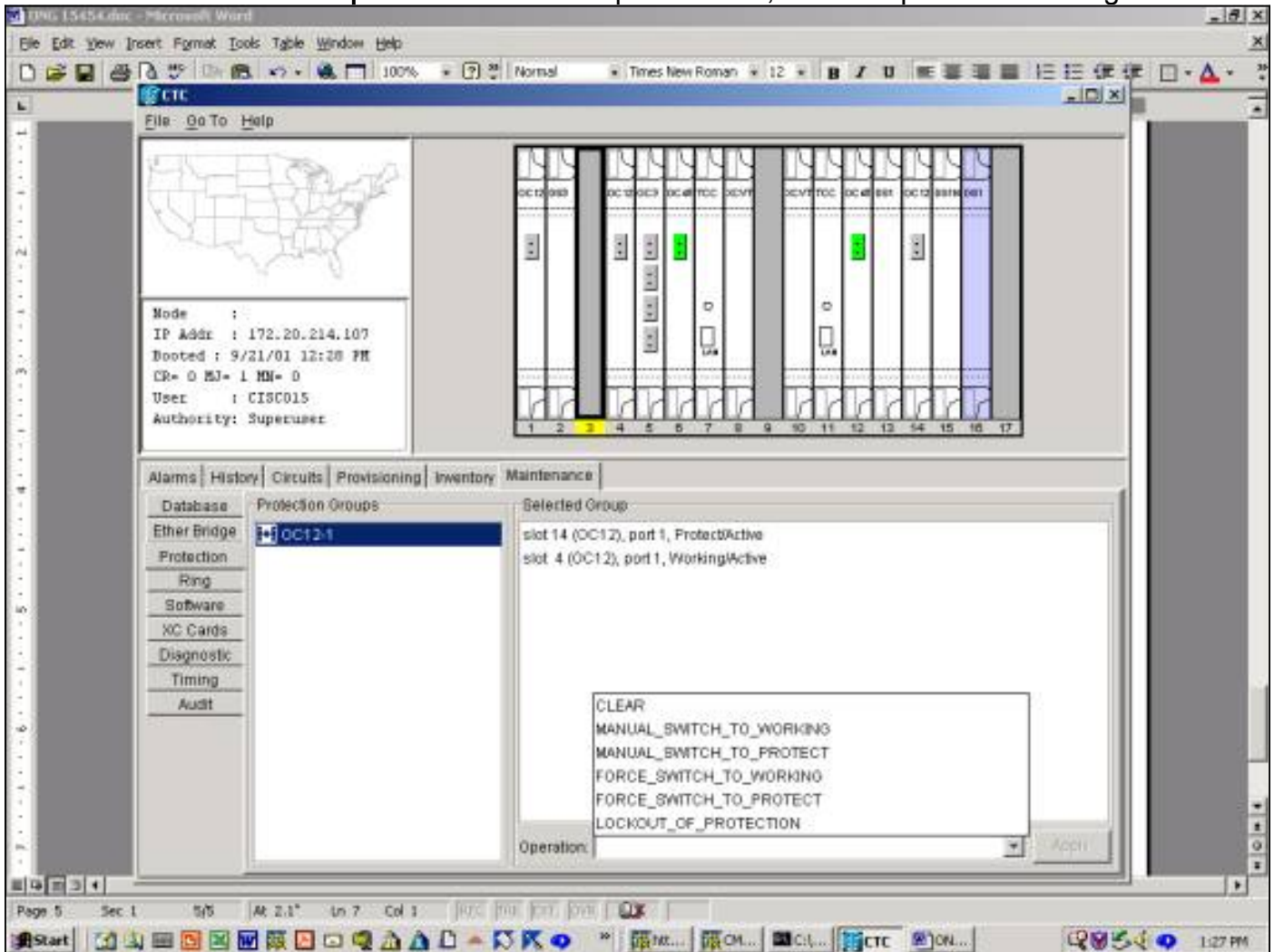
Die [15454-Cisco ONS 15454](#) unterstützt die folgenden Wartungsfunktionen für die Manipulation der Arbeits- und Schutzkarten:

- LOCKOUT_OF_PROTECTION
- FORCED_SWITCH_TO_PROTECT
- FORCED_SWITCH_TO_WORKING
- MANUAL_SWITCH_TO_PROTECT
- MANUAL_SWITCH_TO_WORKING

- KLARSTELLEN

In Version 2.x von **Cisco TC (Cisco Transport Controller)** Software, werden diese wie folgt angezeigt:

1. **Auswählen-Klicken Sie auf** die Registerkarte **Wartung** und die Registerkarte **Schutz**.
2. Wählen Sie im Fenster Schutzgruppen eine der angezeigten Schutzgruppen aus.
3. Klicken Sie im Feld **Operation** auf den Dropdown-Pfeil, um die Optionen anzuzeigen.



LOCKOUT OF PROTECTION

Durch das Auslösen einer Sperre wird der gesamte Datenverkehr zur Arbeitskarte erzwungen. Solange die Sperre eingerichtet ist, wird der Datenverkehr nicht auf die Sicherungskarte umgeschaltet, selbst wenn die funktionierende Karte oder die funktionierende Glasfaser ausfällt. Wenn eine Sperre besteht und ein Fehler auf der Arbeitskarte oder der Glasfaser auftritt, wird der Datenverkehr unterbrochen. Ein Sperrvorgang hat die höchste Priorität und überschreibt alle anderen Switch-Anfragen oder -Ausfälle. Sie können eine Sperrfunktion entfernen, indem Sie **Clear** Befehl.

So starten Sie eine Sperre in Version 2.x:

1. Auf der Registerkarte **Wartung** und **Schutz** können Sie **auswählen-klicken Sie** im Feld **Betrieb auf Sperrung des Schutzes**.
2. **Auswählen-Klicken Sie auf Übernehmen**.
3. Ein Bestätigungsdialegfeld wird angezeigt. **auswählen**-Wenn Sie auf **Ja** klicken, wird die

Sperrung ausgelöst und ~~auswählen~~-Durch Klicken auf **Nein** wird die Sperranforderung aufgehoben.

Die Ausgabe einer Sperrung für den Schutz führt zu einem Alarm sowohl für das funktionierende als auch das schützende Mitglied der Schutzgruppe. Das nachfolgende Beispiel zeigt die Alarmlisten für einen Sperrvorgang, der für eine Schutzgruppe OC12 ausgestellt wurde.

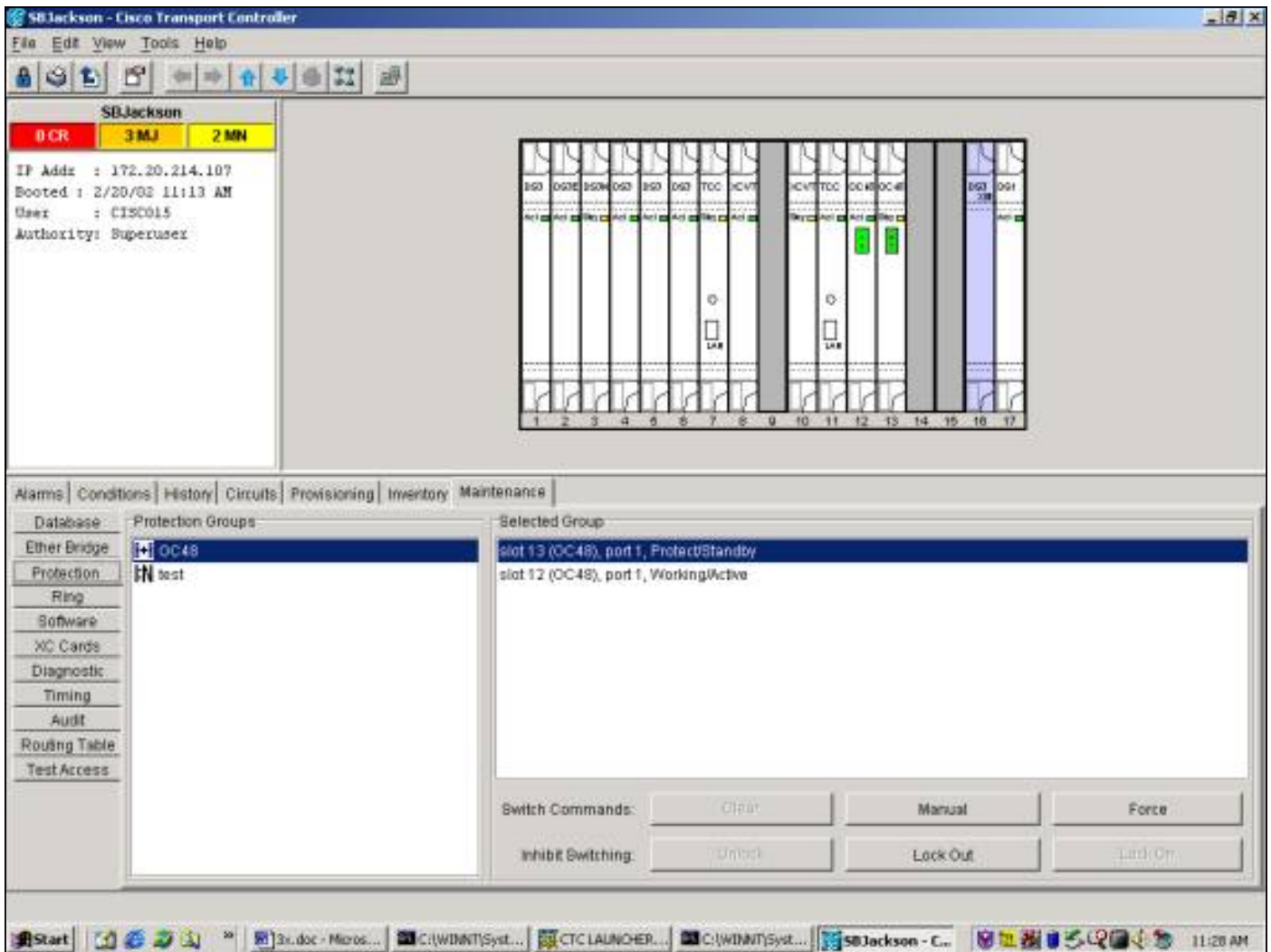
The screenshot shows the CTC interface with a rack configuration and an Alarms table. The rack configuration shows slots 4 and 14 highlighted in yellow. The Alarms table is as follows:

Date	Type	Slot	Port	Sev	BT	SA	Cond	Description
02/10/2017 03:20:17	FAC-14-1	14	1	MR	R		LOCKOUT-REQ	Lockout switch request on facility/equipment
02/10/2017 03:20:17	FAC-4-1	4	1	MR	R	<input checked="" type="checkbox"/>	LOCKOUT-REQ	Lockout switch request on facility/equipment
02/10/2017 01:43:21	SYNC-NE			NR	R		STU	Synchronized - Traceability Unknown
02/10/2017 01:43:21	SYNC-NE			NR	R		SWTOPRI	Synchronization Switch To Primary reference

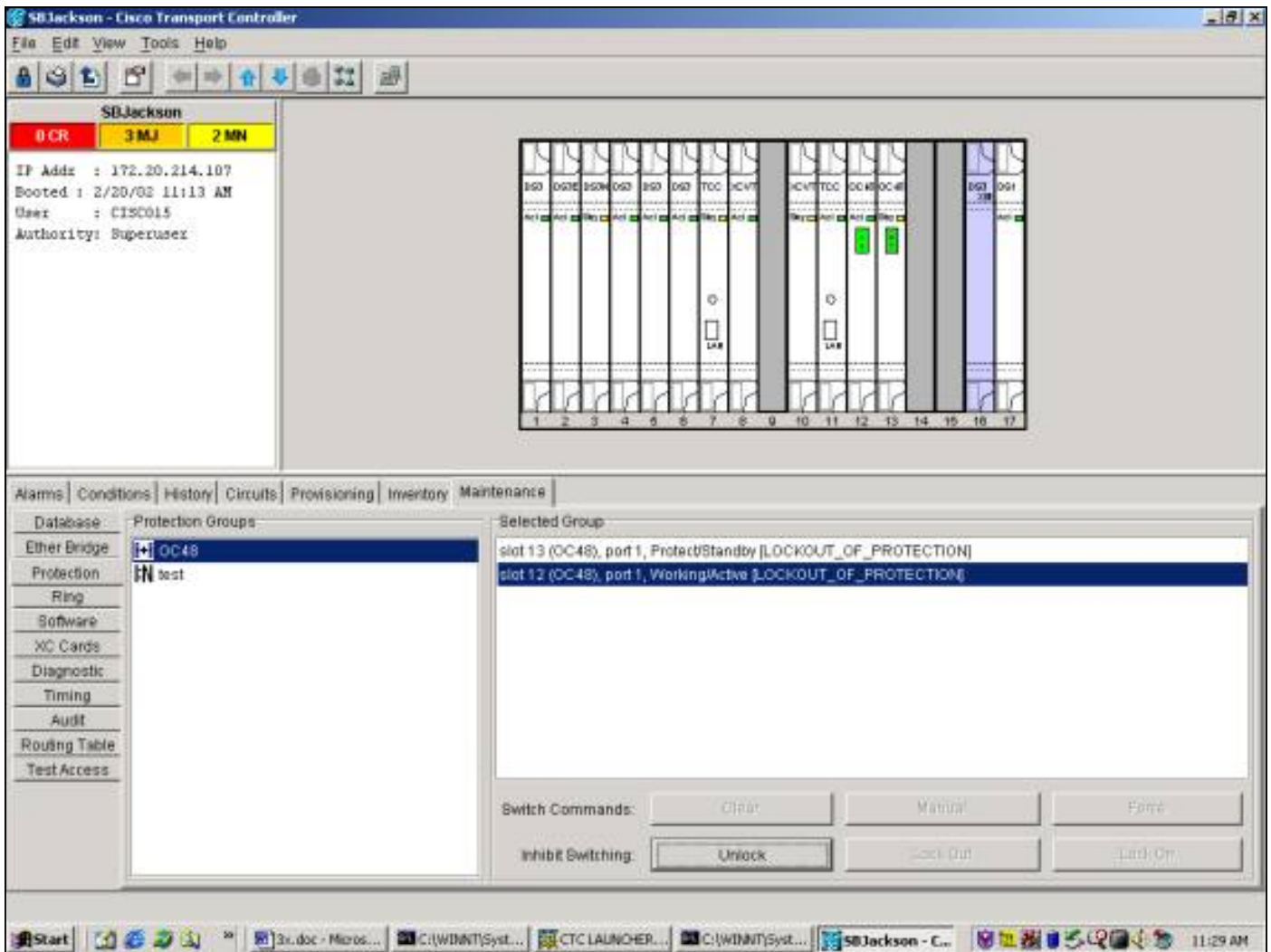
Buttons at the bottom of the Alarms table: Synchronize Alarms, Delete Cleared Alarms, AutoDelete Cleared Alarms.

Um die Sperrfunktion zu deaktivieren, wechseln Sie zur Registerkarte **Maintenance** und dann zur Registerkarte **Protection**. Im Feld Vorgang auswählen-klicken Sie auf Löschen, wie unten gezeigt. Die zugeordneten Alarmlisten werden gelöscht, und die Sperrung wird entfernt.

In Version 3.x gibt es zwei Optionen zum Sperren des Datenverkehrs zu einer Karte. Wenn eine Sperrung auf eine Arbeitskarte angewendet wird, wird der Datenverkehr an die Arbeitskarte und die Glasfaser gesperrt. Wenn eine Sperrung auf die Schutzkarte angewendet wird, wird der gesamte Datenverkehr auf die Arbeitskarte umgeleitet. Der Datenverkehr verbleibt auf der Arbeitskarte, bis die Entsperrungsanfrage ausgestellt wird. Wenn auf der Arbeitsseite ein Ausfall auftritt, während die Sperrung aktiviert ist, wird der Datenverkehr unterbrochen. Eine Sperrung oder ein Sperren hat die höchste Priorität und überschreibt alle anderen Switch-Anforderungen.



Über die Registerkarte **Wartung** und die Registerkarte **Schutz** wird eine Sperre ausgestellt. Wenn die Sicherungskarte markiert ist, **auswählen-klicken Sie auf Sperren** und dann **auswählen-klicken Sie auf Übernehmen**. Ein Bestätigungsfeld wird angezeigt. **auswählen**-Durch Klicken auf **Ja** wird die Sperre ausgelöst und **auswählen**-Durch Klicken auf **Nein** wird die Sperranforderung aufgehoben.



Die Herausgabe einer Sperre führt dazu, dass eine Bedingung gegen das Schutzmitglied der Schutzgruppe gestellt wird. Das nachfolgende Beispiel zeigt die Bedingung für eine Sperrung, die für eine Schutzgruppe OC48 ausgestellt wurde.

Date	Object	Type	Slot	Port	Sev	Cond	Description
02/20/02 11:29	SYNC-NE				NA R	SSM-ST3	Stratum 3 Traceable
02/20/02 11:29	SYNC-NE				NA R	SWTOTHRO	Switch To Third reference
02/20/02 11:29	SYNC-NE				MJ R	FRNGSYNC	Free Running Synchronization mode
02/20/02 11:29	SYNC-NE				MN R	SYNC-SEC	Secondary Synchronization Reference Failure
02/20/02 11:29	SYNC-NE				MN R	SYNCPRI	Primary Synchronization Reference Failure
02/20/02 11:29	BITS-2				NR R	LOF	Loss of Frame
02/20/02 11:29	BITS-2				MJ R	LOS	Loss of Signal
02/20/02 11:29	BITS-1				NR R	LOF	Loss of Frame
02/20/02 11:29	BITS-1				MJ R	LOS	Loss of Signal
02/20/02 11:29	FAC-13-1	OC48_LINE_C...	13	1	NA R	LOCKOUT-REQ	Lockout switch request on facility/equipment

So entfernen Sie die Sperre: **auswählen-Klicken Sie** im Fenster auf **Entsperren. Wartung Schutz und der Registerkarte** Schutz. Der Zustand wird gelöscht, und die Sperre wird entfernt.

Der Zustand und die Bildschirme sind für eine Sperre auf der Arbeitskarte identisch.

FORCE SWITCH TO WORKING/PROTECT

Durch die Initiierung eines "Force Switch" wird der gesamte Datenverkehr entweder zur Arbeitskarte oder zur Schutzkarte gezwungen, je nachdem, welcher Switch-Typ ausgewählt ist. Bei einem "Force Switch to Protect" wird der gesamte Datenverkehr auf die Sicherungskarte und Glasfaser umgeleitet. Bei einem Ausfall auf der Schutzseite, während der Force Switch eingesetzt ist, wechselt der Datenverkehr zur Arbeitskarte und zu Glasfaser. Sobald der Ausfall auf der Schutzseite behoben ist, schaltet der Datenverkehr zurück zur Schutzseite.

Ein erzwungener Switch zum Schutz **werden-schlägt fehl**, wenn die Sicherungskarte oder die Glasfaser einen Signalausfall aufweist. In diesem Fall überschreibt das Signal den Force Switch und der Datenverkehr bleibt auf der Arbeitsseite. Ein Force Switch zum Schutz ist jedoch erfolgreich, wenn auf der Schutzseite eine Signalherabstufung vorliegt.

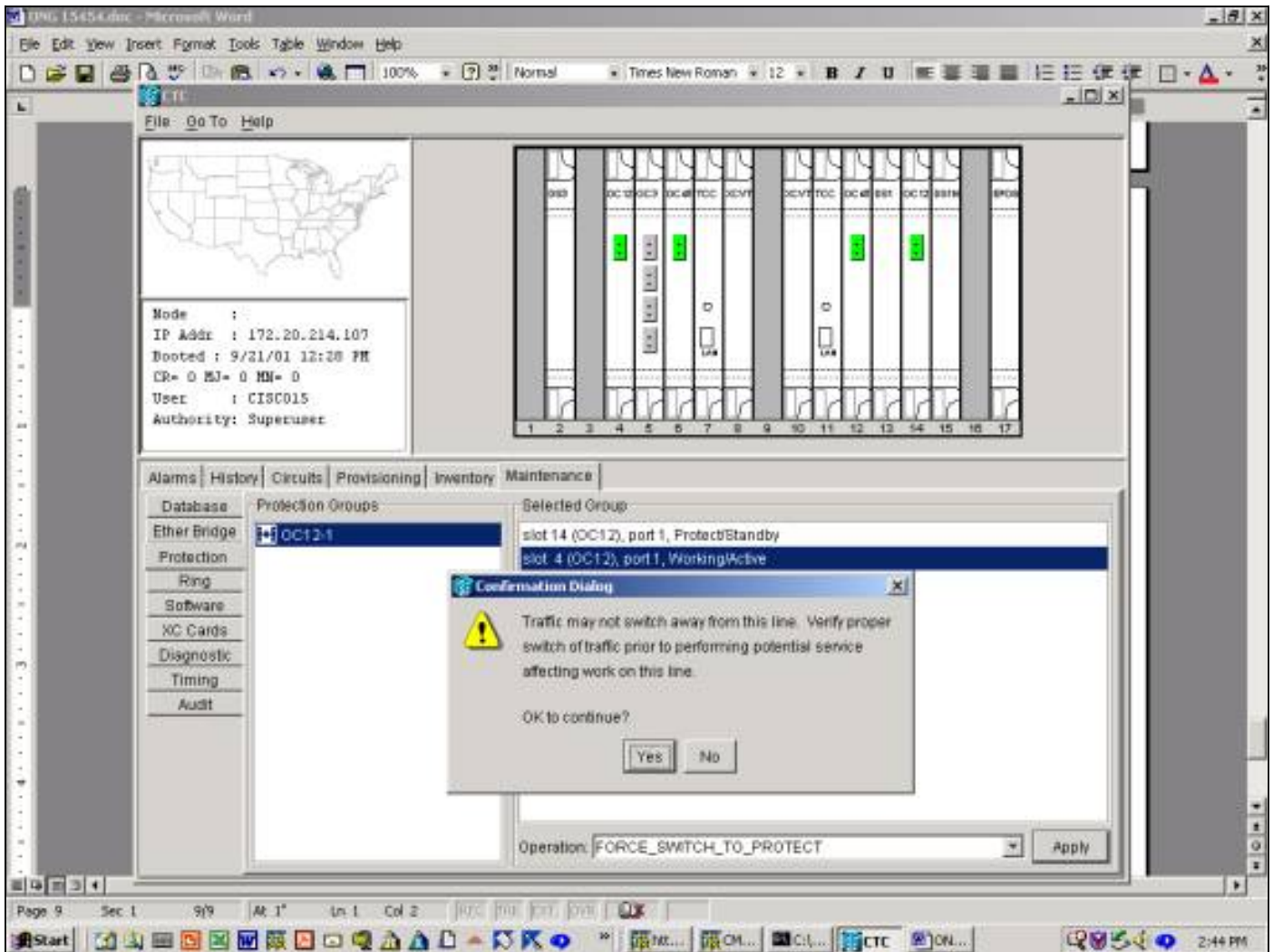
Ein Force Switch überschreibt immer einen manuellen Switch. Ein Lockout überschreibt immer sowohl einen Force Switch als auch einen manuellen Switch.

Die **G-klar** entfernt den Force Switch. Beim nicht-reversitiven Switching verbleibt der Datenverkehr unbegrenzt oder bis eine weitere Switch-Anfrage ausgegeben wird. Beim Revertive Switching

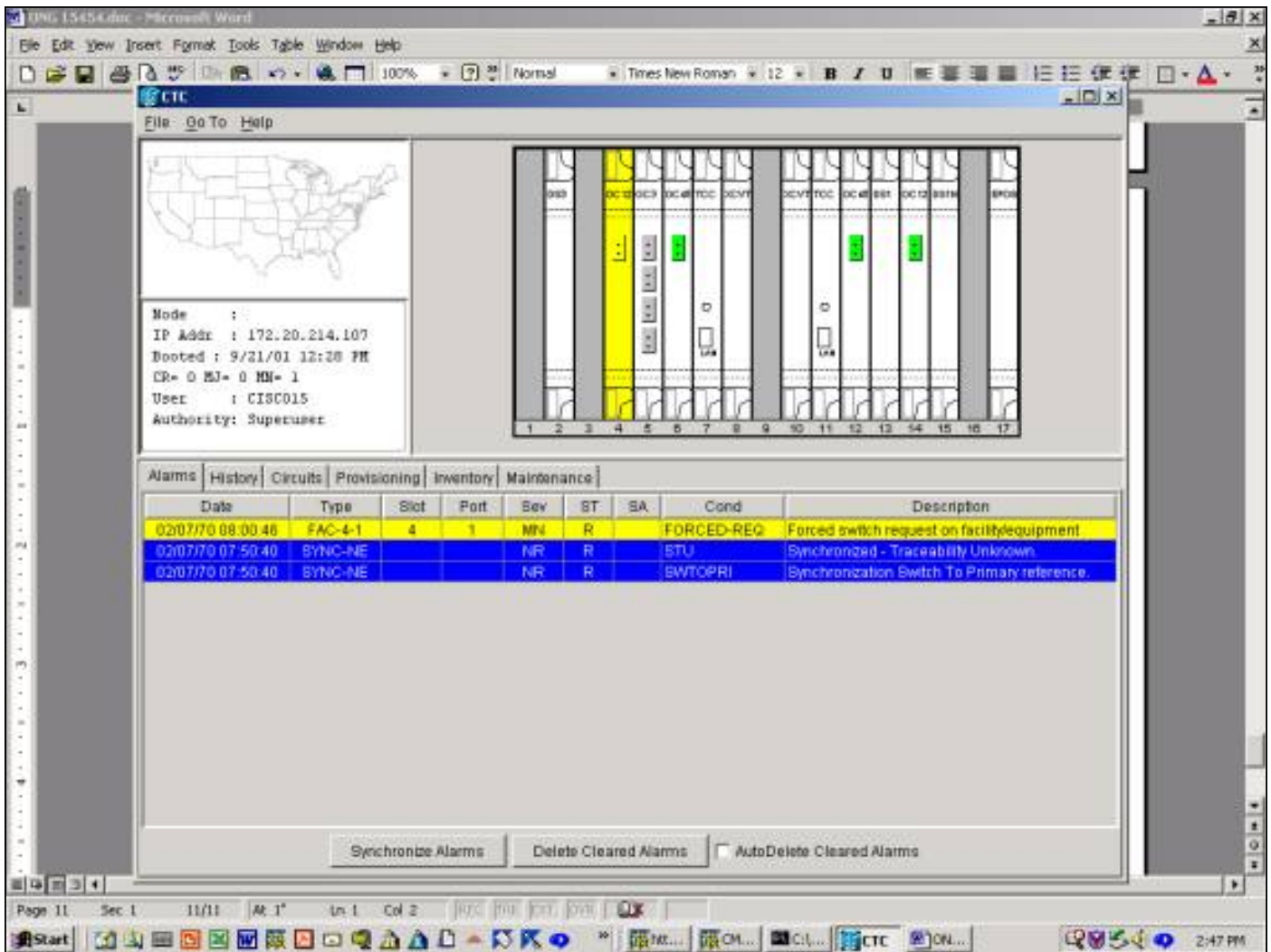
kehrt der Datenverkehr unmittelbar nach dem Löschen der Switch-Anfrage zum funktionierenden Port zurück. (Der Wiederherstellungs-Timer wird nur unter autonomen oder physischen Switch-Bedingungen aktiviert, nicht über Software-Switches.)

Die Ergebnisse entsprechen der Ausgabe eines "Force Switch to Working".

Um einen Force Switch to Protect in Version 2.x über die Registerkarte **Maintenance** und **Protection** zu initiieren, wählen Sie im Feld **Operation** die Option Switch zum Schutz erzwingen und **auswählen-klicken Sie auf Übernehmen**. Es wird ein Bestätigungsfeld angezeigt, das Sie darüber informiert, dass der Switch möglicherweise nicht vorhanden ist, und das bestätigt, bevor der Service die Wartung beeinträchtigt. **Auswählen**-Durch Klicken auf **Ja** wird der Switch initiiert. **auswählen**-Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.

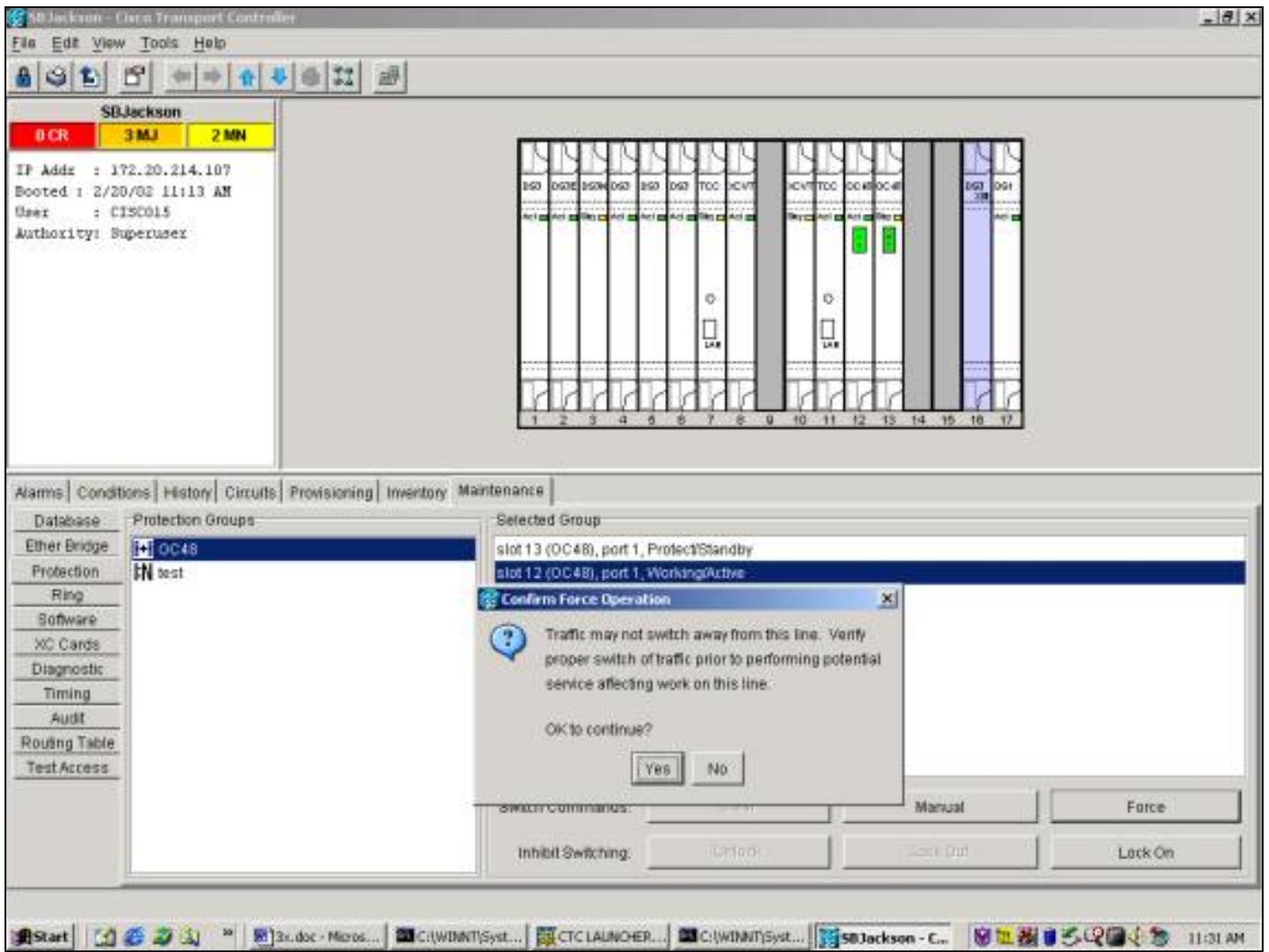


Ein Force Switch to Protect führt zu einem geringfügigen Alarm für das designierte Arbeitsmitglied der Schutzgruppe, wie unten gezeigt.



Um den Force Switch zu entfernen, gehen Sie zur Registerkarte **Maintenance** und **Protection** sowie zum Feld **Operation**. **auswählen-klicken Sie auf Löschen**. Die zugeordneten Alarme werden gelöscht, und der Force Switch wird entfernt.

So starten Sie einen Force Switch zum Schutz in Version 3.x: **auswählen-klicken Sie auf** die Registerkarte **Wartung** und die Registerkarte **Schutz**. Sie können einen Force Switch ausstellen, indem Sie die Arbeitskarte markieren und **auswählen**-Klicken Sie auf **Force**. Es wird ein Bestätigungsdialegfeld angezeigt, das Sie darüber informiert, dass der Switch möglicherweise nicht vorhanden ist, und das bestätigt, bevor der Service die Wartung beeinträchtigt. **Auswählen** Durch Klicken auf **Ja** wird der Switch initiiert. **auswählen**-Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.



Ein Force Switch to Protect führt, wie unten gezeigt, zu einem Zustand, nicht zu einem Alarm gegen das designierte Arbeitsmitglied der Schutzgruppe.

The screenshot shows the Cisco Transport Controller interface for 'SBJackson'. The top left panel displays system information: IP Addr: 172.20.214.107, Booted: 2/20/02 11:13 AM, User: CISCO15, Authority: Superuserx. The main area shows a rack diagram with 17 slots. Below the rack is a 'Conditions' table with the following data:

Date	Object	Type	Slot	Port	Sev	...	Cond	Description
02/20/02 11:41...	SYNC-NE				NA	R	SSM-ST3	Stratum 3 Traceable
02/20/02 11:41...	SYNC-NE				NA	R	SWTO-TRD	Switch To Third reference
02/20/02 11:41...	SYNC-NE				MJ	R	FRNGSYNC	Free Running Synchronization mode
02/20/02 11:41...	SYNC-NE				MN	R	SYNC-SEC	Secondary Synchronization Reference Failure
02/20/02 11:41...	SYNC-NE				MN	R	SYNCPRI	Primary Synchronization Reference Failure
02/20/02 11:41...	BITS-2				NR	R	LOF	Loss of Frame
02/20/02 11:41...	BITS-2				MJ	R	LOS	Loss of Signal
02/20/02 11:41...	BITS-1				NR	R	LOF	Loss of Frame
02/20/02 11:41...	BITS-1				MJ	R	LOS	Loss of Signal
02/20/02 11:41...	FAC-12-1	OC48_LINE_C...	12	1	NA	R	FORCED-REQ...	Force switch request on Span

Um den Force Switch zu entfernen, gehen Sie zur Registerkarte **Maintenance** und **Protection** und **auswählen-klicken Sie auf Löschen**. Die zugeordnete Bedingung wird gelöscht, und der Force Switch wird entfernt.

MANUELLER SWITCH ZUR ARBEIT/ZUM SCHUTZ

Bei der Initiierung eines "manuellen Switches" wird der gesamte Datenverkehr entweder an die Arbeitskarte oder an die Sicherungskarte weitergeleitet, je nachdem, welcher Switch-Typ ausgewählt ist. Bei einem "Manual Switch to Protect" wird der gesamte Datenverkehr auf die Sicherungskarte und Glasfaser umgeschaltet. Wenn beim Einsetzen des manuellen Switches auf der Schutzseite ein Fehler auftritt, wechselt der Datenverkehr zur Arbeitskarte und zu Glasfaser. Sobald der Ausfall auf der Schutzseite behoben ist, wird der Datenverkehr **werden-Schaltet** zurück zur Schutzseite.

Ein manueller Switch zum Schutz **werden-schlägt fehl**, wenn die Sicherungskarte oder Glasfaser einen Zustand von Signal Degrade oder Signal Fail aufweist. In diesem Fall überschreiben sowohl das Signal Degrade als auch das Signal Fail den Force Switch und den Datenverkehr **werden bleibt** am Arbeitsplatz.

Hinweis: Ein Force Switch überschreibt immer einen manuellen Switch. Ein Lockout überschreibt immer sowohl einen Force Switch als auch einen Manual Switch.

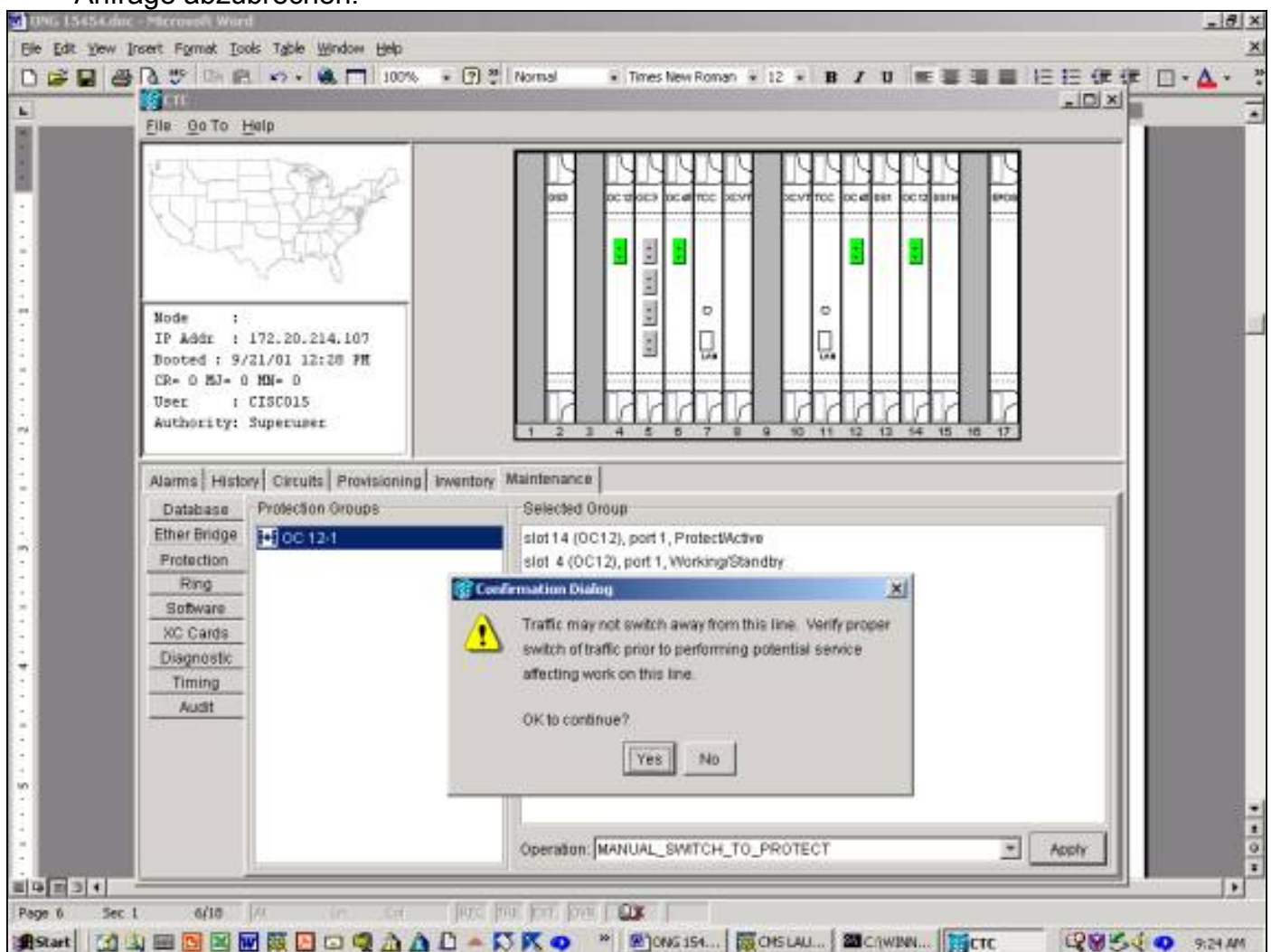
Ausgabe der **G-klar** entfernt den manuellen Switch. Bei nicht-revertivem Switching wird Datenverkehr **werden-bleibt** auf unbestimmte Zeit oder bis eine weitere Switch-Anfrage

ausgegeben wird, auf der Schutzseite. Bei Reverse-Switching wird Datenverkehr werden-kehrt unmittelbar nach dem Löschen der Switch-Anforderung zur Arbeitsseite zurück. (Der Wait-to-Restore-Timer wird nur unter autonomen oder physischen Switch-Bedingungen aktiviert, nicht über Software-Switches.)

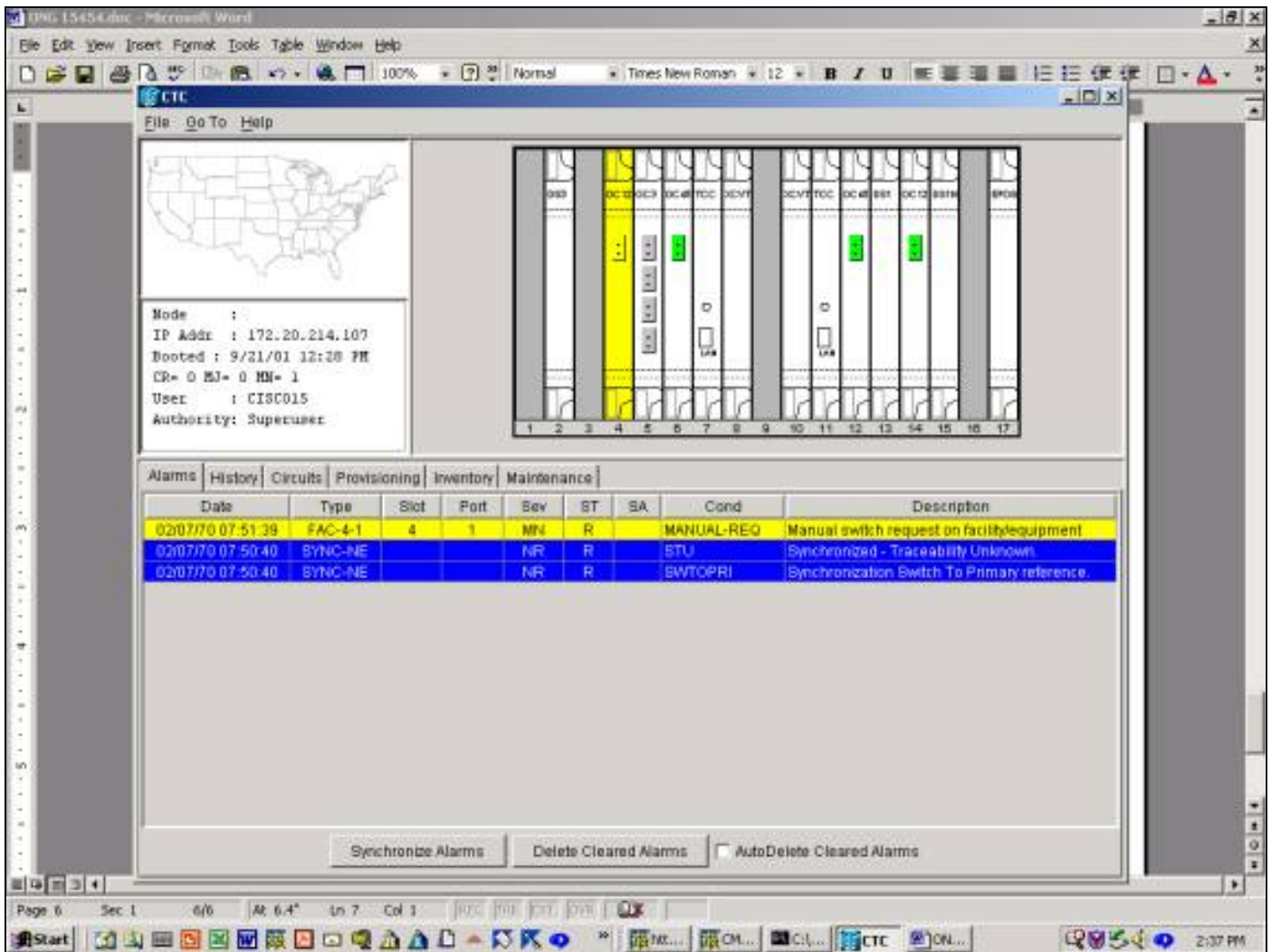
Die Ergebnisse sind für die Ausgabe eines manuellen Switches zum Arbeiten identisch.

So starten Sie einen manuellen Switch zum Schutz in Version 2.x:

1. Auf der Registerkarte **Wartung** und **Schutz** können Sie auswählen-Klicken Sie im Feld **Betrieb** auf **Manueller Switch zum Schutz**.
2. Auswählen-Klicken Sie auf Übernehmen. Es wird ein Bestätigungsdialogfeld angezeigt, das Sie darüber informiert, dass der Switch möglicherweise nicht vorhanden ist, und das bestätigt, bevor der Service die Wartung beeinträchtigt.
3. Auswählen-Klicken Sie auf Ja, um den Switch zu initiieren, oder **Nein**, um die Switch-Anfrage abzubrechen.

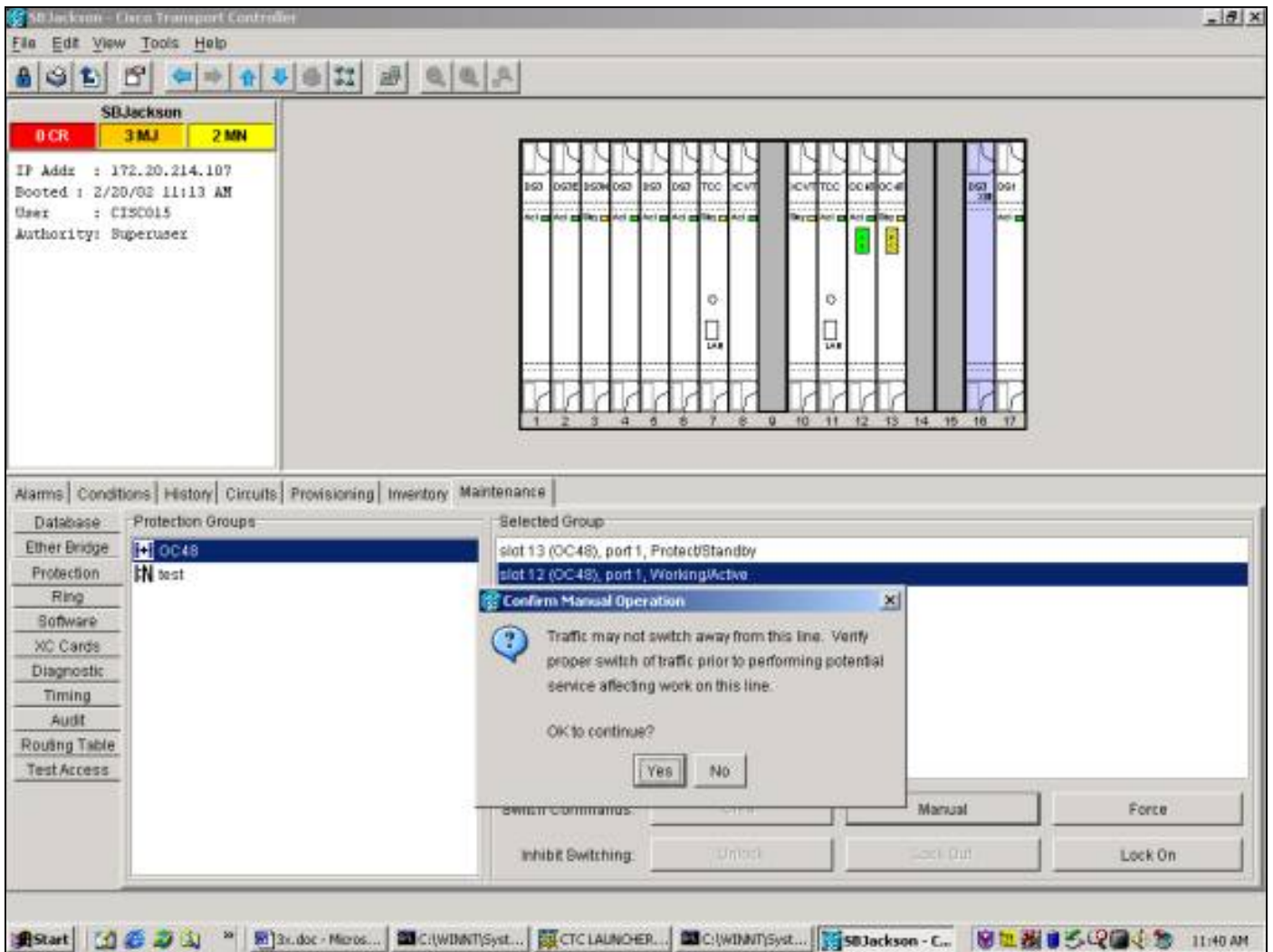


Ein manueller Switch löst einen geringfügigen Alarm für das designierte Arbeitsmitglied der Schutzgruppe aus, wie unten gezeigt.



Um den manuellen Switch zu entfernen, wechseln Sie zur Registerkarte **Wartung** und **Schutz** sowie zum Feld **Betrieb**. **auswählen-klicken Sie auf Löschen**. Die zugehörigen Alarme **werden** löschn und der manuelle Switch wird entfernt.

So starten Sie einen manuellen Switch zum Schutz in Version 3.x: **auswählen-klicken Sie auf** die Registerkarte **Wartung** und die Registerkarte **Schutz**. Stellen Sie einen manuellen Switch zum Schutz aus, indem Sie die funktionierende Karte markieren und **auswählen**-Klicken Sie auf **Manuell**. Es wird ein Bestätigungsdiaologfeld angezeigt, das Sie darüber informiert, dass der Switch möglicherweise nicht vorhanden ist, und das bestätigt, bevor der Service die Wartung beeinträchtigt. Durch die Auswahl von **Ja** wird der Switch initiiert. **auswählen**-Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.



Ein manueller Switch zum Schutz führt, wie unten gezeigt, zu einem Zustand, nicht zu einem Alarm gegen das designierte Mitglied der Schutzgruppe.

Date	Object	Type	Slot	Port	Sev	Cond	Description
02/20/02 11:34...	SYNC-NE				NA R	SSM-ST3	Stratum 3 Traceable
02/20/02 11:34...	SYNC-NE				NA R	SWTO-TRD	Switch To Third reference
02/20/02 11:34...	SYNC-NE				MJ R	FRNGSYNC	Free Running Synchronization mode
02/20/02 11:34...	SYNC-NE				MN R	SYNC-SEC	Secondary Synchronization Reference Failure
02/20/02 11:34...	SYNC-NE				MN R	SYNCPRI	Primary Synchronization Reference Failure
02/20/02 11:34...	BITS-2				NR R	LOF	Loss of Frame
02/20/02 11:34...	BITS-2				MJ R	LOS	Loss of Signal
02/20/02 11:34...	BITS-1				NR R	LOF	Loss of Frame
02/20/02 11:34...	BITS-1				MJ R	LOS	Loss of Signal
02/20/02 11:34...	FAC-12-1	OC48_LINE_C...	12	1	NA R	MANUAL-REQ-S...	Manual switch request on Span

Um den manuellen Switch zu entfernen, gehen Sie zur Registerkarte **Wartung** und **Schutz** und **auswählen-klicken Sie auf Löschen**. Der zugehörige Zustand wird gelöscht, und der manuelle Switch wird entfernt.

1:N Wartung

Das 1:N-Schutzschema gilt für DS1- und DS3-Karten. 1:N Schutz-Switching ist immer reversibel. Bei einem Ausfall oder einem Switch einer Arbeitskarte wird der Datenverkehr entweder in Steckplatz 3 oder Steckplatz 15 auf die Sicherungskarte umgeschaltet. Der Datenverkehr bleibt auf der Sicherungskarte, bis der Fehler behoben oder der Software-Switch freigegeben wird. Der Datenverkehr wird dann auf die ursprüngliche Arbeitskarte zurückgesetzt.

1:1 Schutz ist ein Sonderfall von 1:N. Die Sicherungskarte befindet sich immer in einem ungeraden Steckplatz. 1:1 Schutzgruppen können entweder als Revertive oder als Nicht-Revertive bereitgestellt werden. Beim Revertive Switching wird der Datenverkehr auf die designierte Arbeitskarte wiederhergestellt, nachdem der Fehler oder Software-Switch behoben wurde. Beim nicht-reversitiven Switching verbleibt der Datenverkehr unbegrenzt oder bis zum nächsten Ausfall oder Software-Switch auf der Sicherungskarte.

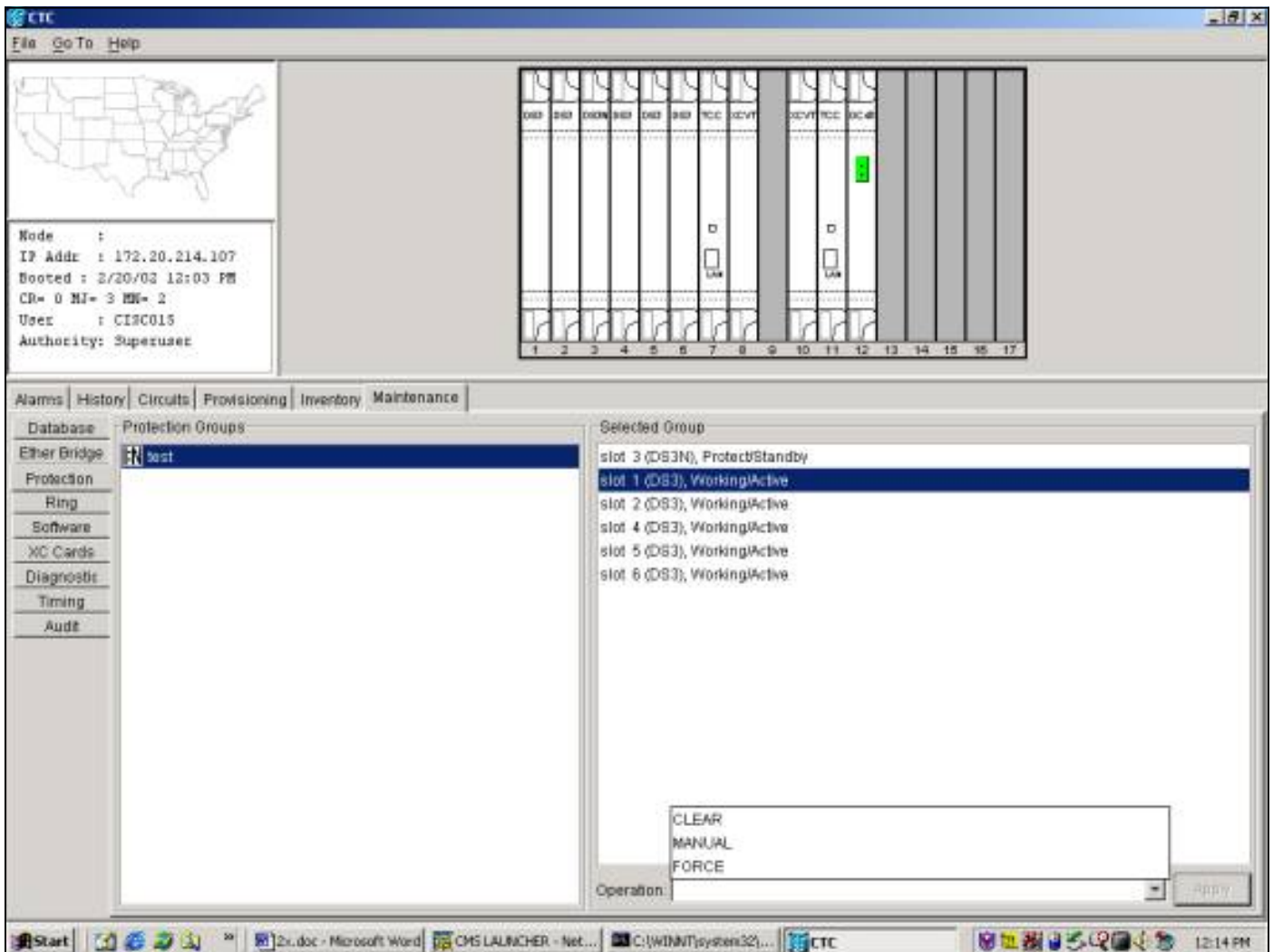
In diesem Abschnitt wird der Betrieb der Wartungsfunktionen für die 1:1- und 1:N-Fälle beschrieben.

Version 2.x

In Version 2.x [15454-Cisco ONS 15454](#) unterstützt die folgenden Wartungsfunktionen für die Manipulation der Arbeits- und Schutzkarten:

- FORM
- MANUELL
- KLARSTELLEN

Sie können auf diese zugreifen, indem Sie **auswählen**-Klicken Sie auf die Registerkarte **Wartung** und die Registerkarte **Schutz**. Wählen Sie im Fenster Schutzgruppen eine der angezeigten Schutzgruppen aus. Klicken Sie im Feld **Operation** auf den Dropdown-Pfeil, um die Optionen anzuzeigen.



Force-Switch

Durch die Initiierung eines Force Switch wird der gesamte Datenverkehr an die festgelegte Schutzkarte umgeleitet. Wenn bei der Sicherheitskarte ein Fehler auftritt, während der Force Switch eingesetzt ist, wechselt der Datenverkehr zurück zur Arbeitskarte. Sobald der Fehler auf der Sicherungskarte behoben ist, wechselt der Datenverkehr zurück zur Schutzkarte.

Ausgabe der **C klar** entfernt den Force Switch. Im Fall von 1:N und im Fall 1:1 Revertive Datenverkehr **werden-kehrt** unmittelbar nach dem Löschen der Switch-Anfrage zur Arbeitskarte zurück. (Der Wait-to-Restore-Timer wird nur unter autonomen oder physischen Switch-Bedingungen aktiviert, nicht über Software-Switches.)

- Im nicht umkehrbaren Fall von 1:1 bleibt der Datenverkehr auf der Sicherungskarte

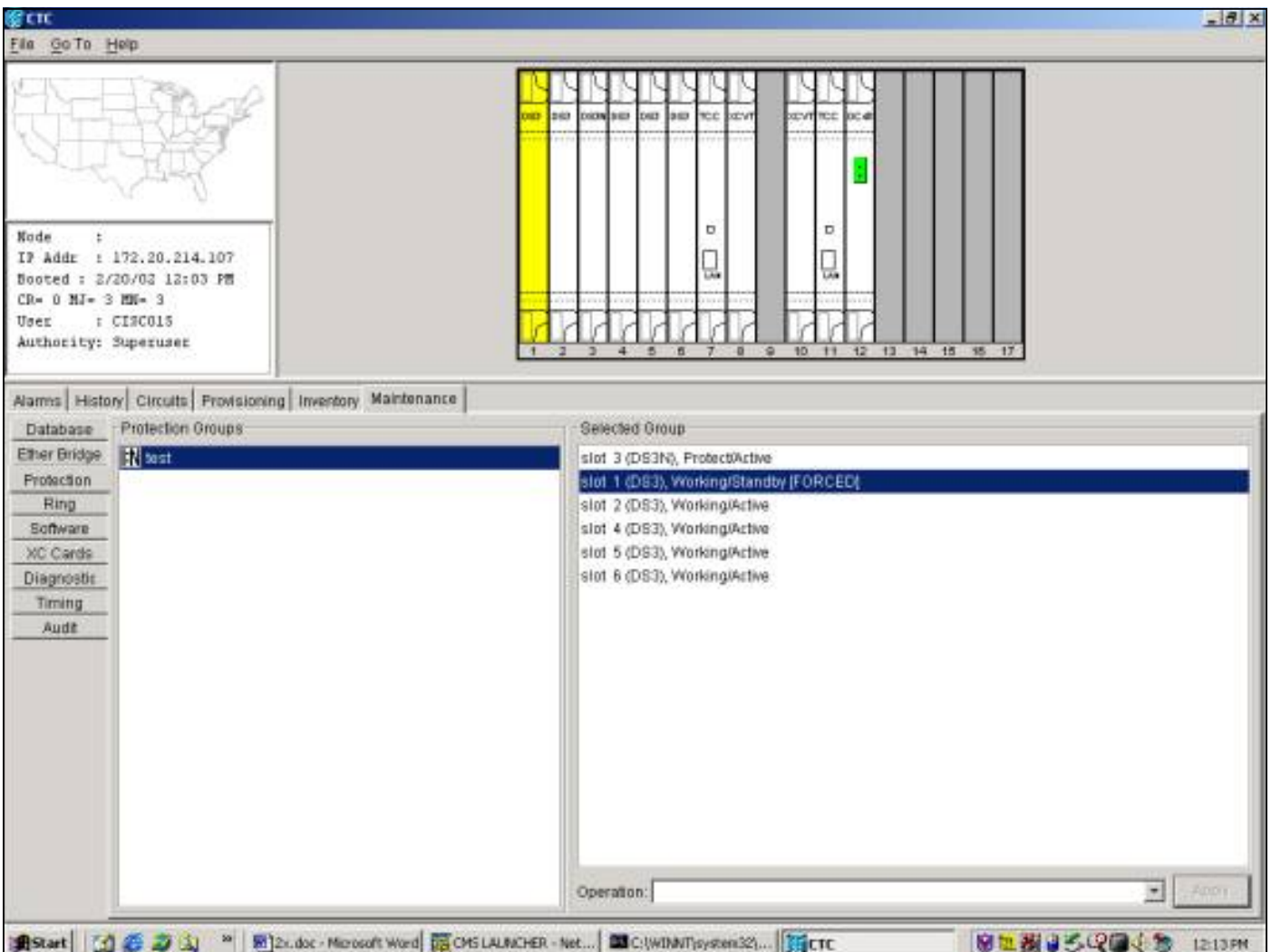
unbegrenzt oder bis eine weitere Ausfall- oder Switch-Anfrage auftritt.

- Wenn im nicht umkehrbaren Fall 1:1 der Datenverkehr ursprünglich auf der Schutzkarte lag, wird der Datenverkehr bei einer Force Switch-Anforderung an die Arbeitskarte umgeleitet. Die Ergebnisse entsprechen den oben beschriebenen Ergebnissen.

Hinweis: Ein Force Switch **werden überschreibt** einen manuellen Switch. Dies ist jedoch kein SONET APS-Schutz und sollte nicht als solcher verwechselt werden.

So starten Sie einen Force Switch zum Schutz in Version 2.x: **auswählen-klicken Sie auf** die Registerkarte **Wartung** und die Registerkarte **Schutz**.

Stellen Sie einen "Force Switch to Protect" aus, indem Sie die Arbeitskarte markieren und **auswählen**-Klicken Sie auf **Force**. Ein Bestätigungsdialogfeld wird angezeigt. **Auswählen**-Durch Klicken auf **Ja** wird der Switch initiiert. **auswählen**-Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.



Ein Force Switch to Protect führt zu einem geringfügigen Alarm für das designierte Arbeitsmitglied der Schutzgruppe, wie unten gezeigt.

The screenshot shows the CTC interface with a rack of equipment and an Alarms table. The Alarms table is as follows:

Date	Type	Slot	Port	Dev	ST	SA	Cond	Description
01/01/70 18:54:53	SLOT-1	1		MN	R		FORCED-REQ	Forced switch request on facility equipment
01/01/70 18:51:37	SYNC-NE			NR	R		ST3	Stratum 3 Traceable
01/01/70 18:51:37	SYNC-NE			NR	R		SWTOTHIRD	Synchronization Switch To Third reference.
01/01/70 18:51:37	SYNC-NE			MJ	R	<input checked="" type="checkbox"/>	FRNGSYNC	Free Running Synchronization mode.
01/01/70 18:51:37	SYNC-NE			MN	R		SYNCSEC	Loss of timing on secondary synchronization link.
01/01/70 18:51:37	SYNC-NE			MN	R		SYNCPRI	Loss of timing on primary synchronization link.
01/01/70 18:51:37	BITS-2			MJ	R	<input checked="" type="checkbox"/>	LOS	Loss of Signal.
01/01/70 18:51:37	BITS-1			MJ	R	<input checked="" type="checkbox"/>	LOS	Loss of Signal.

Um den Force Switch zu entfernen, gehen Sie zur Registerkarte **Maintenance** und **Protection** sowie zum Feld **Operation**. **auswählen-klicken Sie auf Löschen**. Die zugeordneten Alarme werden gelöscht, und der Force Switch wird entfernt.

Manueller Switch

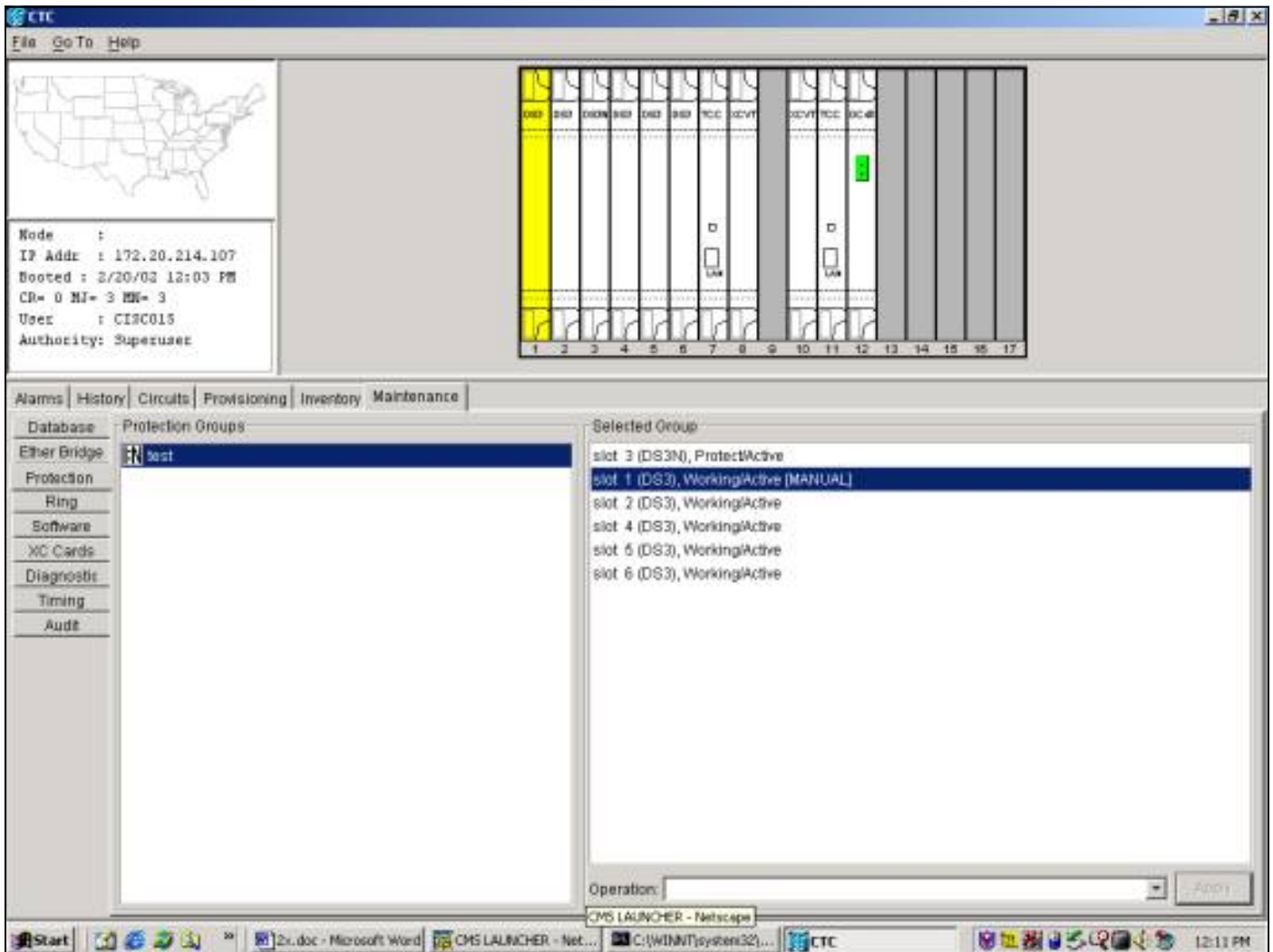
Bei der Initiierung eines manuellen Switches wird der gesamte Datenverkehr auf die designierte Schutzkarte umgeschaltet. Wenn auf der Sicherungskarte ein Fehler auftritt, während der manuelle Switch eingesetzt ist, wird der Datenverkehr zurück zur funktionierenden Karte umgeleitet. Sobald der Fehler auf der Schutzkarte behoben ist, schaltet der Datenverkehr zurück zur Schutzkarte.

Ausgabe der **G-klar** entfernt den manuellen Switch. Im Fall von 1:N und im Fall 1:1 Revertive kehrt der Datenverkehr unmittelbar nach dem Löschen der Switch-Anfrage zur Arbeitskarte zurück. (Der Wiederherstellungs-Timer wird nur unter autonomen oder physischen Switch-Bedingungen aktiviert, nicht über Software-Switches.)

- Im nicht umkehrbaren Fall von 1:1 bleibt der Datenverkehr auf der Sicherungskarte unbegrenzt oder bis eine weitere Ausfall- oder Switch-Anfrage auftritt.
- Wenn im nicht umkehrbaren Fall 1:1 der Datenverkehr ursprünglich auf der Schutzkarte lag, wurde der Datenverkehr bei einer manuellen Switch-Anfrage an die Arbeitskarte umgeleitet. Die Bedingungen entsprechen denen, die oben beschrieben wurden.

Hinweis: Ein Force Switch überschreibt einen manuellen Switch. Dies ist jedoch kein SONET APS-Schutz und sollte nicht als solcher verwechselt werden.

Um einen manuellen Switch zum Schutz in Version 2.x zu aktivieren, gehen Sie zur Registerkarte **Wartung** und **Schutz**. **Auswählen-Klicken Sie** im Feld **Betrieb** auf **Manuell** und **auswählen-klicken Sie auf Übernehmen**. Ein Bestätigungsdialogfeld wird angezeigt. **Auswählen-**Durch Klicken auf **Ja** wird der Switch initiiert. **auswählen-**Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.



Ein manueller Switch löst einen geringfügigen Alarm für das designierte Arbeitsmitglied der Schutzgruppe aus, wie unten gezeigt.

The screenshot shows the CTC interface with a rack diagram at the top and an Alarms table below. The rack diagram shows slots 1 through 17, with slot 1 highlighted in yellow. The Alarms table is as follows:

Date	Type	Slot	Port	Sev	ST	SA	Cond	Description
01/01/70 18:56:04	SLOT-1	1		MN	R		MANUAL-REQ	Manual switch request on facility equipment
01/01/70 18:51:37	SYNC-NE			NR	R		ST3	Stratum 3 Traceable
01/01/70 18:51:37	SYNC-NE			NR	R		SWTOTHRD	Synchronization Switch To Third reference
01/01/70 18:51:37	SYNC-NE			MJ	R	<input checked="" type="checkbox"/>	FRNGSYNC	Free Running Synchronization mode
01/01/70 18:51:37	SYNC-NE			MN	R		SYNCSEC	Loss of timing on secondary synchronization link
01/01/70 18:51:37	SYNC-NE			MN	R		SYNCPRI	Loss of timing on primary synchronization link
01/01/70 18:51:37	BITS-2			MJ	R	<input checked="" type="checkbox"/>	LOS	Loss of Signal
01/01/70 18:51:37	BITS-1			MJ	R	<input checked="" type="checkbox"/>	LOS	Loss of Signal

At the bottom of the Alarms table, there are buttons for "Synchronize Alarms", "Delete Cleared Alarms", and a checkbox for "AutoDelete Cleared Alarms".

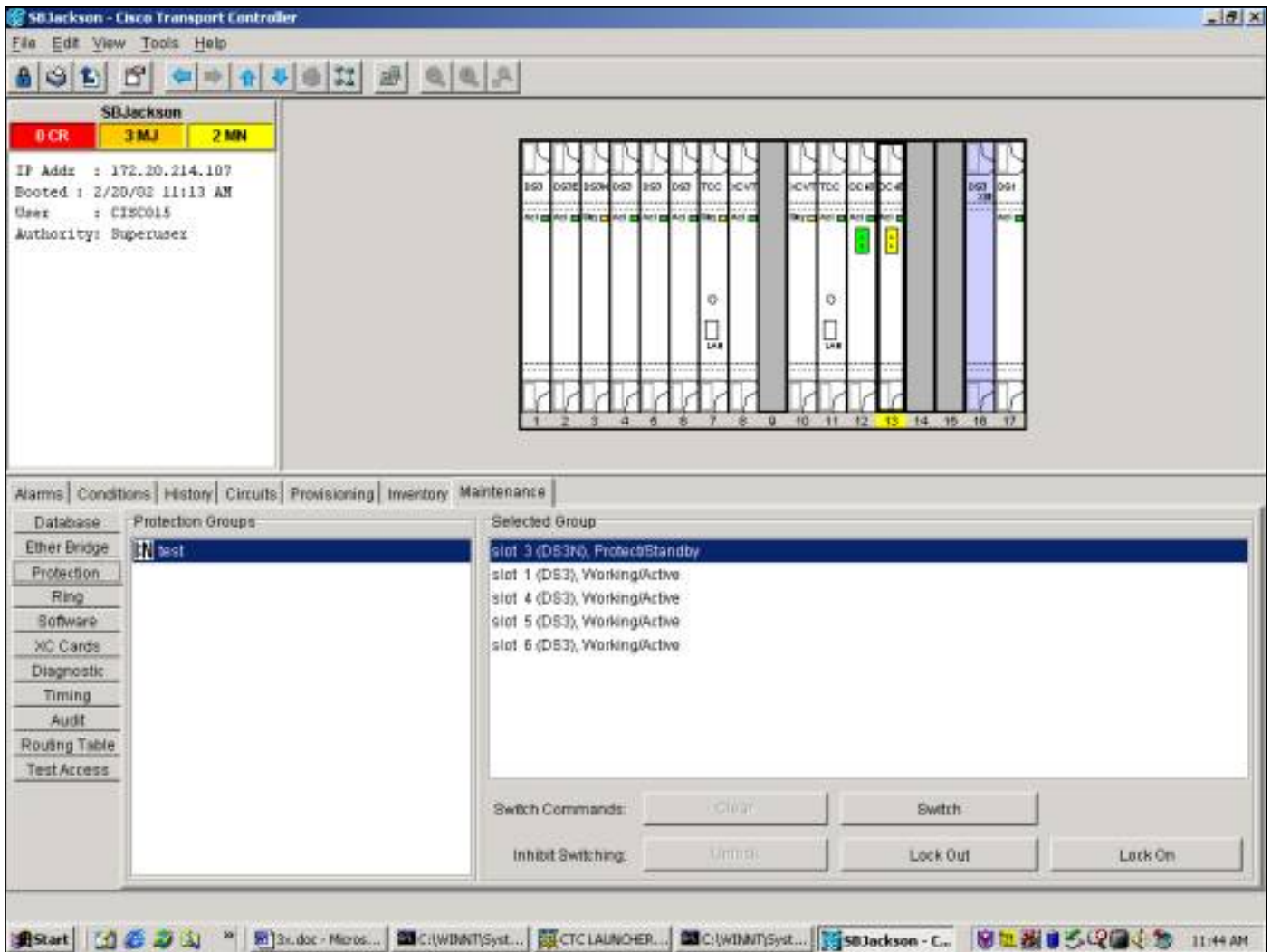
Um den manuellen Switch zu entfernen, gehen Sie zur Registerkarte **Maintenance** und **Protection**. Im Feld "**Operation**" **auswählen-klicken Sie auf Löschen**. Die zugeordneten Alarmer werden gelöscht, und der Force Switch wird entfernt.

Version 3.x

In Version 3.x wurde die SONET APS-Terminologie entfernt. Die [15454-Cisco ONS 15454](#) unterstützt die folgenden Wartungsfunktionen zum Bearbeiten der Arbeits- und Schutzkarten:

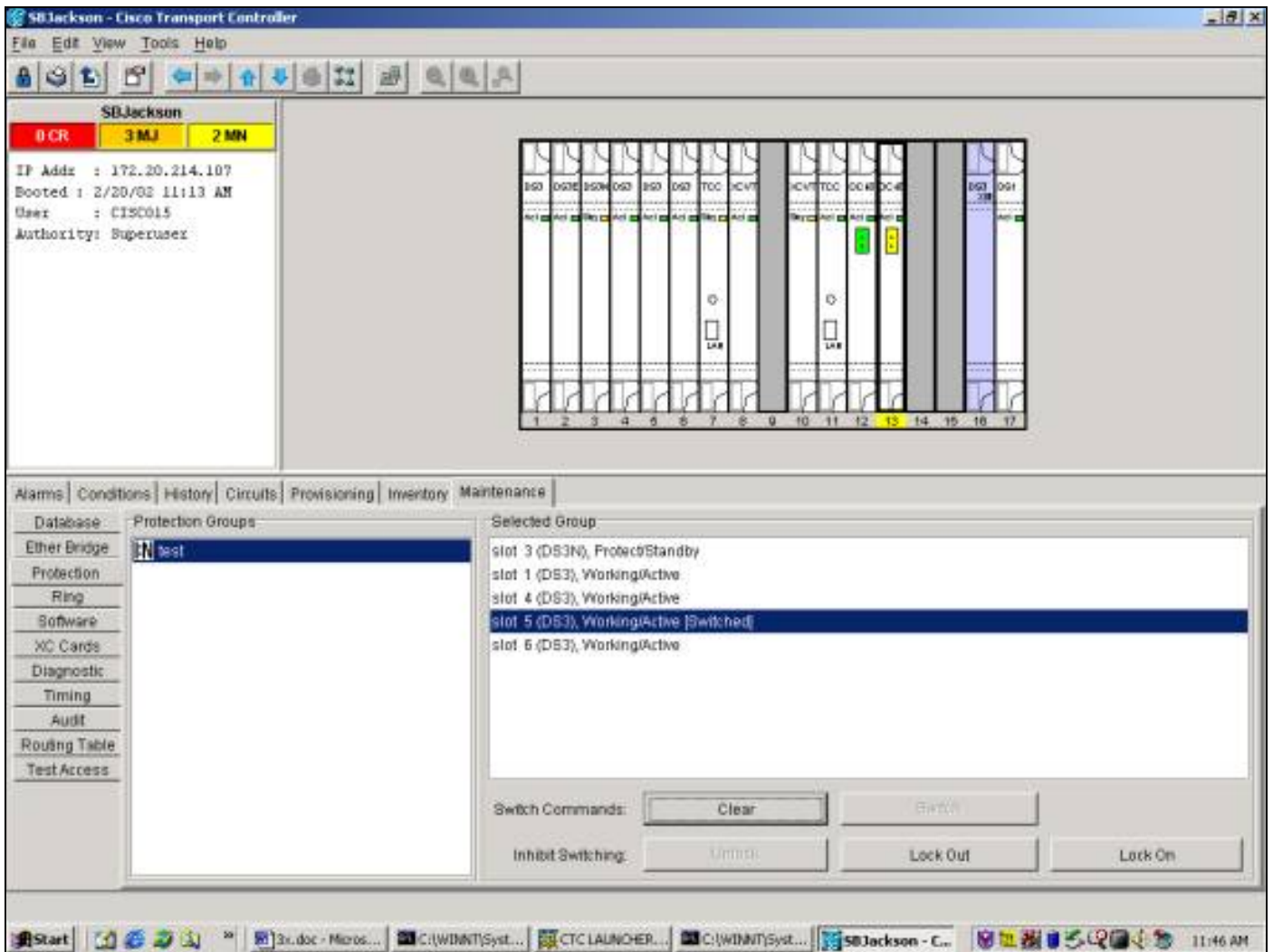
- SWITCH
- EINSCHALTEN
- AUSSCHLIESSEN
- ENTSPERREN
- KLARSTELLEN

Diese anzeigen nach **auswählen**-Klicken Sie auf die Registerkarte **Wartung** und die Registerkarte **Schutz**. Wählen Sie im Fenster Schutzgruppen eine der angezeigten Schutzgruppen aus. Die Optionen **werden**-Änderung, je nachdem, welches Mitglied der Schutzgruppe hervorgehoben ist.

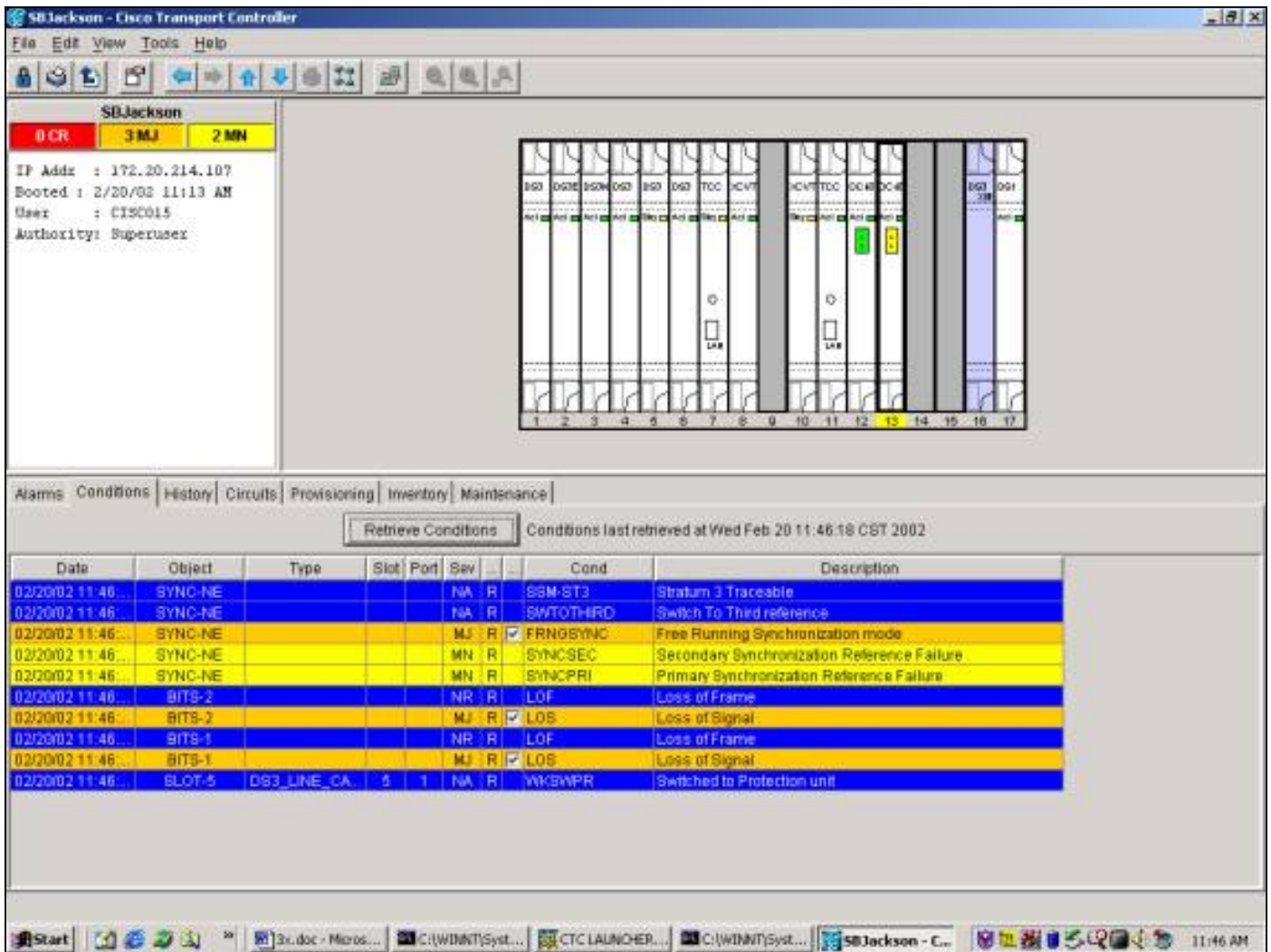


Switch

Die **S-Switch** schaltet den gesamten Datenverkehr von der Arbeitskarte, gegen die er ausgegeben wird, auf die Schutzkarte um. Um einen Switch to Protect zu initiieren, markieren Sie die funktionierende Karte und **auswählen-klicken Sie auf Switch**. Ein Bestätigungsdiaologfeld wird angezeigt. **Auswählen**-Durch Klicken auf **Ja** wird der Switch initiiert. **auswählen**-Wenn Sie auf **Nein** klicken, wird die Switch-Anfrage abgebrochen.



Ein Switch to Protect führt, wie unten gezeigt, zu einem Zustand, nicht zu einem Alarm gegen das designierte Arbeitsmitglied der Schutzgruppe.



Um den Switch zu entfernen, gehen Sie zur Registerkarte **Wartung** und **Schutz**. Im Feld "Operation" auswählen-klicken Sie auf Löschen. Der zugehörige Zustand wird gelöscht, und der Switch wird entfernt.

Ein-/Aussperren

Schutz-Switching in einer 1:N- oder einer 1:1-Schutzgruppe kann verhindert werden, indem eine Sperre oder Sperre auf eine funktionierende oder geschützte Karte angewendet wird. Wenn sich der Datenverkehr auf der Arbeitskarte befindet, verhindert das Anwenden einer Sperre, dass der Datenverkehr von der Arbeitskarte zur Schutzkarte umschaltet. Um Wartungsarbeiten an einer Schutzkarte durchzuführen, ist es notwendig, ein Sperren auf jedes funktionierende Mitglied der Schutzgruppe anzuwenden, um ein Umschalten zu verhindern.

Wenn die Arbeitskarte ausfällt, während die Sperre aktiviert ist, wird der Datenverkehr werden sinkt.

So starten Sie eine Sperre: auswählen-Klicken Sie auf die Registerkarte **Wartung** und die Registerkarte **Schutz**, wobei die Arbeitskarte hervorgehoben ist. Auswählen-Klicken Sie auf Sperren. Ein Bestätigungsdialegfeld wird angezeigt. Auswählen-Durch Klicken auf Ja wird die Sperre aktiviert. auswählen-Durch Klicken auf Nein wird die Sperre auf Anfrage aufgehoben.

The screenshot displays the SB Jackson - Cisco Transport Controller interface. The top-left panel shows system information for SB Jackson, including IP address (172.20.214.107), boot time (2/20/02 11:13 AM), user (CISCO15), and authority (Superuser). The main area shows a rack diagram with slots 1 through 17. Slot 1 is highlighted in blue and labeled 'DS3, WorkingActive [Locked On]'. Below the rack diagram, the 'Protection Groups' section shows a list of groups, with 'test' selected. The 'Selected Group' section lists the slots in the group: slot 3 (DS3N, ProtectStandby), slot 1 (DS3, WorkingActive [Locked On]), slot 4 (DS3, WorkingActive), slot 5 (DS3, WorkingActive), and slot 6 (DS3, WorkingActive). The 'Switch Commands' section includes buttons for 'Clear' and 'Switch', and the 'Inhibit Switching' section includes buttons for 'Unlock', 'Lock Off', and 'Lock On'.

Eine SPERRUNG ("LOCK ON") führt zu einem Zustand, nicht zu einem Alarm gegen das designierte Arbeitsmitglied der Schutzgruppe, wie unten gezeigt.

The screenshot shows the SB Jackson - Cisco Transport Controller interface. At the top, there is a menu bar (File, Edit, View, Tools, Help) and a toolbar. Below the menu, the system status is displayed: SB Jackson, 0 CR, 3 MJ, 2 MN. The IP address is 172.20.214.107, booted on 2/20/02 at 11:13 AM, user is CISCO15, and authority is Superuser.

The main area shows a rack of equipment with slots 1 through 17. Slot 13 is highlighted in yellow, indicating a condition. Below the rack, there is a 'Retrieve Conditions' button and a timestamp: 'Conditions last retrieved at Wed Feb 20 11:48:47 CST 2002'.

Date	Object	Type	Slot	Port	Sev	Cond	Description
02/20/02 11:48...	SYNC-NE				NA R	SSM-ST3	Stratum 3 Traceable
02/20/02 11:48...	SYNC-NE				NA R	SWTOTHRO	Switch To Third reference
02/20/02 11:48...	SYNC-NE				MJ R	FRNGSYNC	Free Running Synchronization mode
02/20/02 11:48...	SYNC-NE				MN R	SYNC-SEC	Secondary Synchronization Reference Failure
02/20/02 11:48...	SYNC-NE				MN R	SYNCPRI	Primary Synchronization Reference Failure
02/20/02 11:48...	BITS-2				NR R	LOF	Loss of Frame
02/20/02 11:48...	BITS-2				MJ R	LOS	Loss of Signal
02/20/02 11:48...	BITS-1				NR R	LOF	Loss of Frame
02/20/02 11:48...	BITS-1				MJ R	LOS	Loss of Signal
02/20/02 11:48...	SLOT-1	DS3_LINE_CA...	1	1	NA R	INHWPWR	Inhibit Switch to Protect Request on equipment

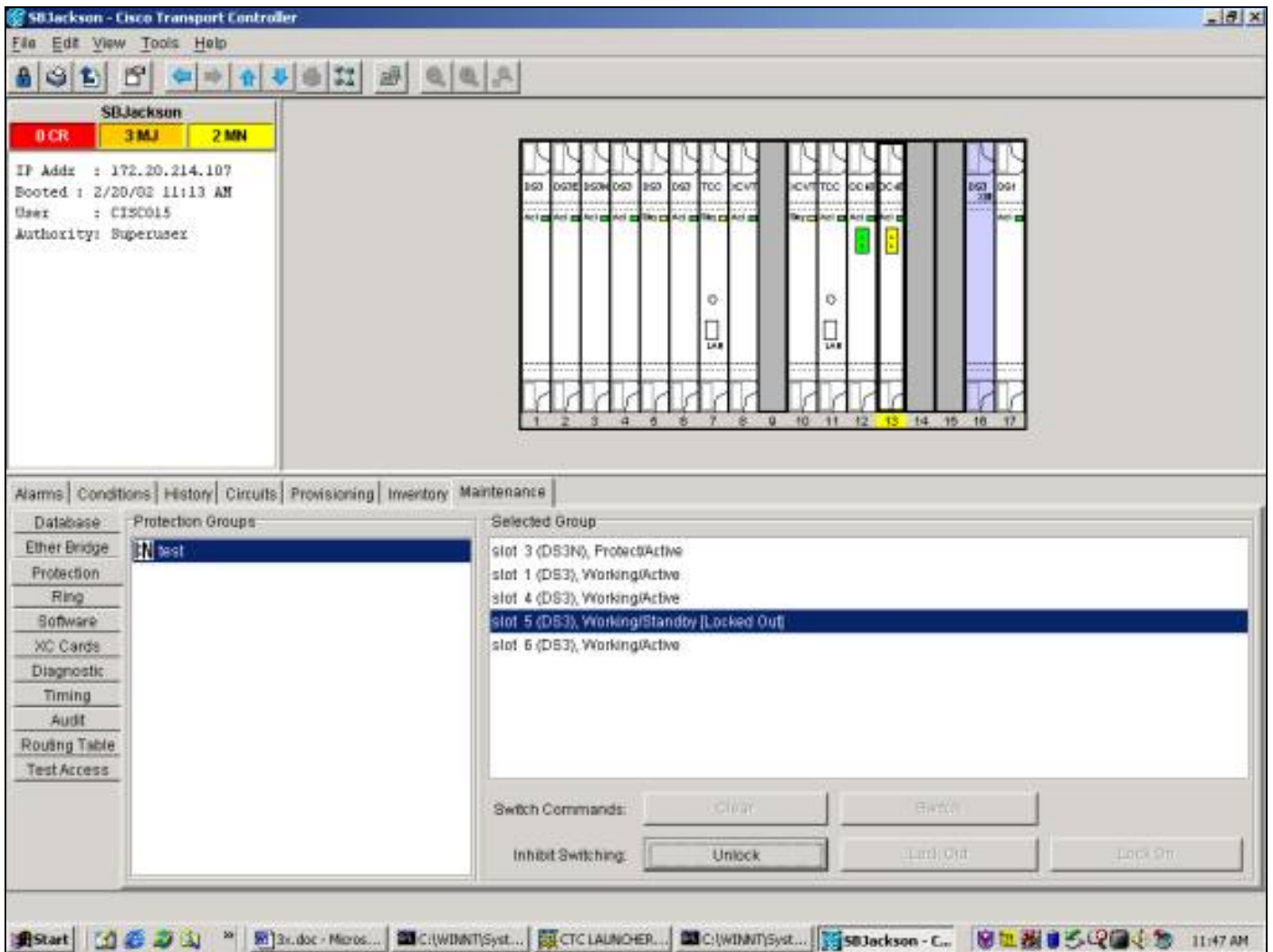
The Windows taskbar at the bottom shows the Start button, several open applications (3x.doc - Micros..., C:\WINNT\System..., CTC LAUNCHER..., C:\WINNT\System..., SB Jackson - C...), and the system clock showing 11:48 AM on 2/20/02.

Um die Sperre zu entfernen, wechseln Sie zur Registerkarte **Wartung** und **Schutz** sowie zum Feld **Betrieb**. auswählen-Klicken Sie auf Entsperren. Die zugeordnete Bedingung wird gelöscht, und die Sperre wird entfernt.

Wenn sich der Datenverkehr auf der Arbeitskarte befindet, verhindert das Anwenden einer Sperre, dass der Datenverkehr von der Schutzkarte zur Arbeitskarte umgeschaltet wird. Um Wartungsarbeiten an einer Arbeitskarte durchführen zu können, ist es erforderlich, eine Sperre auf die Arbeitskarte anzuwenden, nachdem der Datenverkehr auf die Schutzkarte umgeschaltet wurde.

Wenn die Sicherungskarte ausfällt, während die Sperre aktiviert ist, wird der Datenverkehr unterbrochen.

Um eine Sperre auszulösen, auswählen-Klicken Sie auf die Registerkarte **Wartung** und die Registerkarte **Schutz**, wobei die Arbeitskarte hervorgehoben ist. Auswählen-Klicken Sie auf Sperren. Ein Bestätigungsdialogfeld werden wird angezeigt. Auswählen-Klicken Sie auf Ja. werden-Initiiert die Sperrung; auswählen-Klicken auf Nein werden-Storniert die Sperranforderung.



Ein LOCK OUT führt, wie unten gezeigt, zu einem Zustand, nicht zu einem Alarm gegen das designierte Arbeitsmitglied der Schutzgruppe.

The screenshot shows the Cisco Transport Controller (CTC) interface for a device named 'SBJackson'. The top left panel displays system information: IP Addr: 172.20.214.107, Booted: 2/20/02 11:13 AM, User: CISCO15, Authority: Superuser. The main area shows a rack diagram with 17 slots. Slots 1, 2, 4, 5, and 6 are occupied by 'D93' cards, while slot 15 is occupied by a 'D91' card. The bottom panel shows a 'Conditions' table with the following data:

Date	Object	Type	Slot	Port	Sev	...	Cond	Description
02/20/02 11:47...	SYNC-NE				NA	R	SSM-ST3	Stratum 3 Traceable
02/20/02 11:47...	SYNC-NE				NA	R	SWTOTHRO	Switch To Third reference
02/20/02 11:47...	SYNC-NE				MJ	R	FRNGSYNC	Free Running Synchronization mode
02/20/02 11:47...	SYNC-NE				MN	R	SYNCSEC	Secondary Synchronization Reference Failure
02/20/02 11:47...	SYNC-NE				MN	R	SYNCPRI	Primary Synchronization Reference Failure
02/20/02 11:47...	BITS-2				NR	R	LOF	Loss of Frame
02/20/02 11:47...	BITS-2				MJ	R	LOS	Loss of Signal
02/20/02 11:47...	BITS-1				NR	R	LOF	Loss of Frame
02/20/02 11:47...	BITS-1				MJ	R	LOS	Loss of Signal
02/20/02 11:47...	SLOT-5	D93_LINE_CA...	5	1	NA	R	WKSWPR	Switched to Protection unit
02/20/02 11:47...	SLOT-5	D93_LINE_CA...	5	1	NA	R	INH5WVK0	Inhibit Switch to Working Request on equipment

Um die Sperre zu entfernen, wechseln Sie zur Registerkarte **Wartung** und **Schutz** sowie zum Feld **Betrieb**. auswählen-Klicken Sie auf Entsperren. Die zugehörige Bedingung werden löscht und sperrt werden wird entfernt.

Zusätzlicher 1:N-Betrieb

Das 1:N-Schutzszenario ermöglicht 1 Schutzkarte (in Steckplatz 3 oder 15) als Schutz für bis zu fünf Arbeitskarten. Im folgenden Beispiel wird Datenverkehr auf den Karten 1, 2, 4, 5 und 6 verarbeitet.

D S 3	D S 3	D S 3 N	D S 3	D S 3	D S 3	T C C	X C V T
W O R K I N G	W O R K I N G	P R O T E C T	W O R K I N G	W O R K I N G	W O R K I N G		
1	2	3	4	5	6	7	8

Wenn die Arbeitskarte Nr. 1 ausfällt oder eine Switch-Anfrage initiiert wird, wird der Datenverkehr von der Arbeitskarte Nr. 1 in Steckplatz 3 auf die Schutzkarte umgeschaltet.

D S 3	D S 3	D S 3 N	D S 3	D S 3	D S 3	T C C	X C V T
F A I L	W O R K I N G	W O R K I N G	W O R K I N G	W O R K I N G	W O R K I N G		
1	2	3	4	5	6	7	8

Wenn die Arbeitskarte Nr. 2 ausfällt, während dies geschieht, wird der Datenverkehr auf der Arbeitskarte Nr. 2 unterbrochen. Der Datenverkehr von der Arbeitskarte Nr. 1, der sich nun auf der Sicherungskarte in Steckplatz 3 befindet, ist davon nicht betroffen.

D S 3	D S 3	D S 3 N	D S 3	D S 3	D S 3	T C C	X C V T
F A I L	F A I L D R O P	W O R K I N G	W O R K I N G	W O R K I N G	W O R K I N G		
1	2	3	4	5	6	7	8

Wenn die Arbeitskarte Nr. 1 repariert ist oder die Switch-Anfrage auf dieser Karte entfernt wird, wechselt der Datenverkehr zurück zur Arbeitskarte Nr. 1. Der Datenverkehr von der Arbeitskarte Nr. 2 wird dann auf die Schutzkarte in Steckplatz 3 umgeschaltet, um den Datenverkehr wiederherzustellen.

D S 3	D S 3	D S 3 N	D S 3	D S 3	D S 3	T C C	X C V T
W O R K I N G	F A I L	W O R K I N G	W O R K I N G	W O R K I N G	W O R K I N G		
1	2	3	4	5	6	7	8

Wenn die Arbeitskarte Nr. 2 fest installiert oder die Switch-Anfrage entfernt wurde, wechselt der Datenverkehr zurück zur Arbeitskarte Nr. 2, und die Schutzkarte in Steckplatz 3 bleibt wieder verfügbar.

D S 3	D S 3	D S 3 N	D S 3	D S 3	D S 3	T C C	X C V T
W O R K I N G	W O R K I N G	P R O T E C T	W O R K I N G	W O R K I N G	W O R K I N G		
1	2	3	4	5	6	7	8

Zugehörige Informationen

- [Technischer Support - Cisco Systems](#)