juma/forsete-ii series user guide

DKTCOMEGA

introduction

This is the user guide for the DKTCOMEGA 7973x/794xx JUMA/Forsete-II Series CPE.

The series include the following variants:
- 79734 – 1x 10/100/1000Mbps RJ-45
- 79741 – 4x 10/100/1000Mbps RJ-45, SNMP
- 79742 – 4x 10/100/1000Mbps RJ-45, SNMP, CATV

The user guide includes explaination of features supported from firmware revision 05_02.
Syntaxes for the individual features are listed in this document, please notice if the functionality is not implemented in the revision of the firmware yet - it is be marked as

(feature will be supported in a future release)

index

DKTCOMEGA

the boot process of the cpe node

Boot start-up procedure:

- The first time that the device boots, it issues a DHCP Discover with dhcp option 60 set to `DKT_F2_firstboot`. The firmware can be downloaded to the unit.
- Alternatively if firmware is present in the device, the device issues a dhcp request with dhcp option 60 set to `DKT_F2_firmware_vXX_XX` (where XX_XX is the version number of the firmware).

When a new node is unpacked from the factory, it doesn't contain any firmware, and before it can be used in must be updated with the latest revision. This mean that when the node is installed at the customer premise, it will be required to remotely update with firmware, before it will be working. It is highly recommended to visit www.dktcomega.com -> support -> firmware for latest boot loader and firmware revision.
The managed node depends on DHCP negotiation. Through this negotiation the firmware ID of the managed node is exchanged for a configuration file. The DHCP server hands out the configuration file depending on the firmware ID.

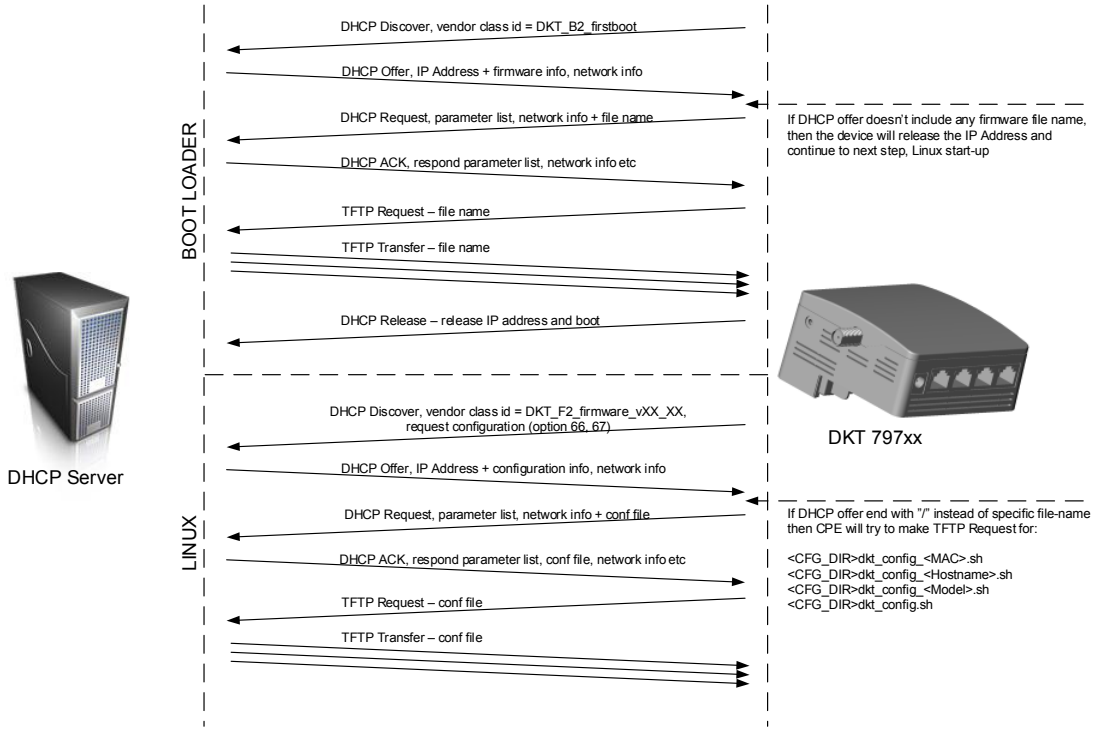
Uboot.

A device power-up it will start the uboot process. The purpose is to validate if the device has the correct firmware image (if any), and bring it onto the network using DHCP.

Linux (Device OS system).

This is the main software with full network support and features to use the complete hardware platform. The network is configured using DHCP, and the system configuration is downloaded using TFTP.
The first bootp/dhcp request from the device can be used to remote upgrade the firmware. If a bootfile and a bootserver is given in the bootp response then the file is downloaded via tftp and executed by the device.

The device is configured to not pass any traffic per default, so in order to pass traffic through the switch engine, the switch --enable-lan command must be provisioned to the device. Also telnet daemon must be started, with the use of telnetd -l /bin/sh command in the script



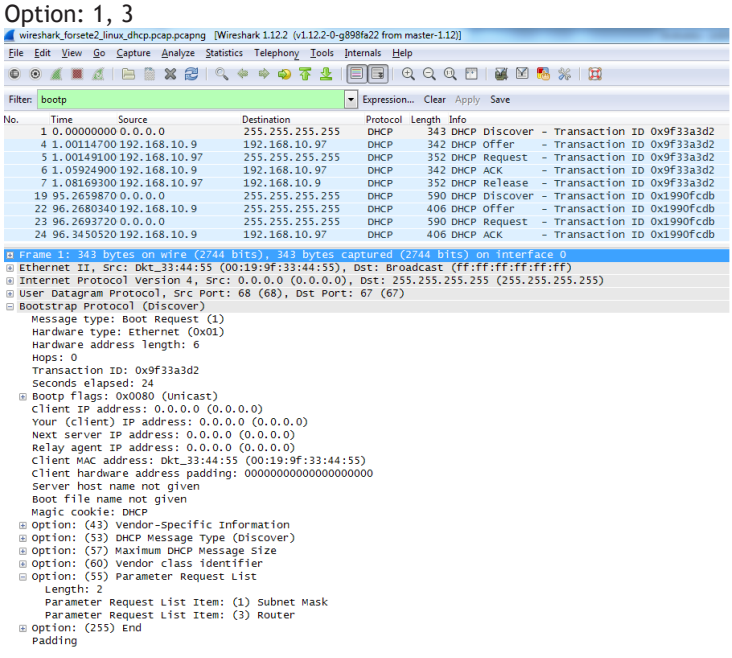
At device start-up configuration is provisioned automatically. Firmware is provisioned by request, either at first boot or when applicable

Ensures correct device settings and automatically firmware upgrade without user interaction
Firmware and configuration are provisioned by the operator

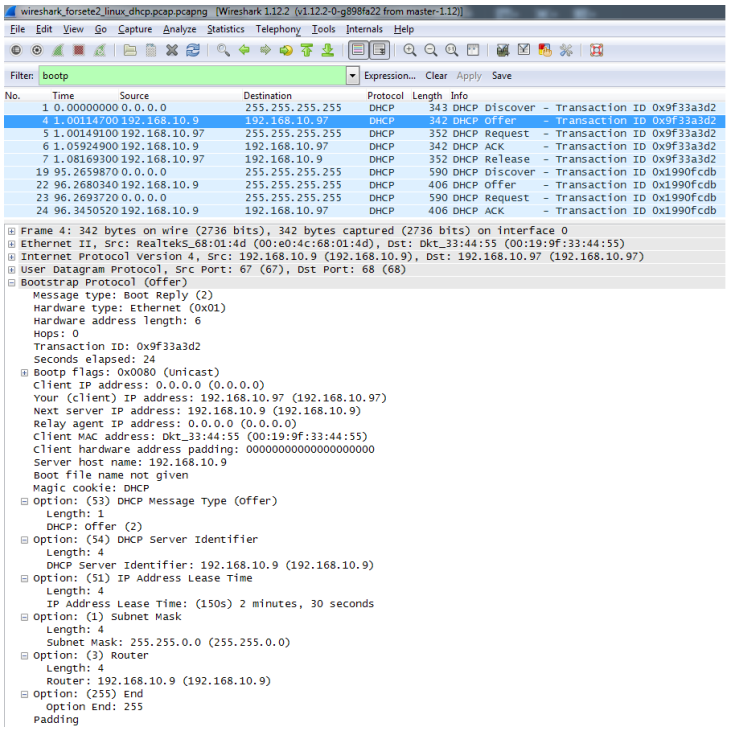
dhcp settings

The CPE requires a dhcp server connected to the fiber WAN port before power on.
Please refer to Appendix 3 – DHCP Settings for example of DHCP settings

1) The device requests in its Uboot DHCP discoverer:
Option: 1, 3

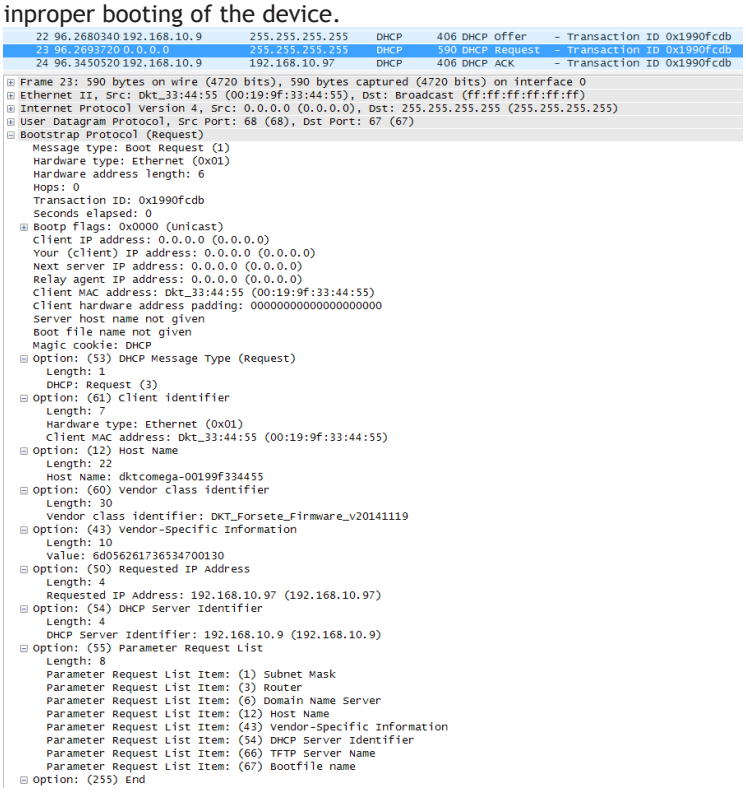


2) DHCP Server offers in its response:
Option: 53, 54, 51, 1, 3



DKTCOMEGA

3) CPE requests in its LINUX Boot-up process, where configuration file is requested:
Option: 1, 3, 6, 12, 43, 54, 66, 67 - Please make sure that DHCP Server responds to these option requests, as it will influence on the booting sequence, if these are not correctly answered, and may cause inproper booting of the device.



custom configuration

When the OS issue a dhcp request a filename of a configuration file can be sent to the device. This configuration file is then downloaded by tftp during the boot process and issued instead of the default configuration. In this way it is possible to persist settings for each customer (by mapping the hardware address of the node and the customer number).

The server and the filename of the configuration file should be sent in respective tftp-server-name (option 66) and bootfile-name (option 67) from the dhcp server. Notice these options are different from the bootfile/bootserver used in the bootp response.

If it is not feasible that the dhcp server distinguish the customer's configurations base on the hardware address an alternative method can be used. The dhcp server sends out the name of a generic configuration. This configuration can then include instruction to the node of fetching a node specific configure by tftp where the requested filename is a combination of the node hardware address.
In the generic configuration script, which is common for all devices and that will provisioned during boot up, the following instructions can be inserted:

```
source /etc/dhcp.vars
export WAN_MACADDR=$(ip addr show dev eth0 | grep "ether" | cut -d " " -f6 | tr -d :)
tftp -g -r my_conf_$WAN_MACADDR -l /tmp/config.sh $TFTP_SERVER
save_configuration
source /tmp/config.sh
```

Alternatively, if DHCP offer in the response instead just end with "/" instead of specific file-name then the device will try to make TFTP Request for:

<CFG_DIR>dkt_config_<MAC>.sh
<CFG_DIR>dkt_config_<Hostname>.sh
<CFG_DIR>dkt_config_<Model>.sh <CFG_DIR>dkt_config.sh

An example of a configuration file could be the following:

```
#####################################################################
# DKT configuration
# Firmware version: XX_XX
#####################################################################
switch --enable-lan # enable LAN ports
# Example, how to create 4 VLANs, egress tagged on WAN and untagged on all LANs
conf vlan init
conf vlan create vlan-table vid 100
conf vlan create vlan-table vid 200
conf vlan create vlan-table vid 300
conf vlan create vlan-table vid 400
conf vlan set vlan-table vid 100 member 0,4
conf vlan set vlan-table vid 200 member 1,4
conf vlan set vlan-table vid 300 member 2,4
conf vlan set vlan-table vid 400 member 3,4
conf vlan set pvid port 0 100
conf vlan set pvid port 1 200
conf vlan set pvid port 2 300
conf vlan set pvid port 3 400
conf vlan set vlan-table vid 100 untag-member 0
conf vlan set vlan-table vid 200 untag-member 1
conf vlan set vlan-table vid 300 untag-member 2
conf vlan set vlan-table vid 400 untag-member 3

# Example, how to enable double tagging on WAN, define SVID for each origin port
conf svlan init
conf svlan set service-port 4
conf svlan create svlan-table svid 500
conf svlan create svlan-table svid 600
conf svlan create svlan-table svid 700
conf svlan set svlan-table svid 500 member 0,4
conf svlan set svlan-table svid 600 member 1,4
conf svlan set svlan-table svid 700 member 2,4
conf svlan set port 0 svid 500
conf svlan set port 1 svid 600
conf svlan set port 2 svid 700
conf svlan set svlan-table svid 500 untag-member 0
conf svlan set svlan-table svid 600 untag-member 1
conf svlan set svlan-table svid 700 untag-member 2
#
# The following command enables TELNET access from WAN
telnetd -l /bin/sh
# End of DKT configuration
#####################################################################
```

device script commands

The following commands are supported in the script that will be downloaded to the CPE via TFTP during boot-up process.
This command is used to configure the switch in the unit. The command takes one or more of the following parameters, with the syntax switch --nn or conf/diag xx.

The 79741/742 models have 4 LAN ports, whereas 79734 model has 1 LAN port. The port outline and port mapping is as follows, shown from the front:

4 port (79741/742):

LAN1	LAN2	LAN3	LAN4
1	2	3	4

Please refer to syntax guide for Command Line Interface, to configure VLAN, QoS etc. parameters

Notice:
I configuration is made via TELNET or SSH, start switch configuration shell by typing *conf* or *diag*

reboot

The device can be accessed via TELNET, and is rebooted with the use of “reboot” command. TELNET access must however be configured in the configuration file.

```
# The following command enables TELNET access from WAN
telnetd -l /bin/sh
```

save configuration to flash

Per default device configuration is provisioned via DHCP at boot, and it will be stored in device RAM memory, which means that the device would need to have the configuration loaded at every boot.

Concept is if dhcp service is out, the device will restore its latest saved - the latest saved configuration is the incident where there is a difference between saved configuration and provisioned configuration. Also the CPE will get an ad-hoc link-local IP address, which is an auto configuration algorithm described in the IETF Draft “Dynamic Configuration of IPv4link-local addresses”.

Procedure is to
- insert a syntax in the configuration file “save_configuration”

Please note that the syntax “save_configuration” will be filtered by the device, so if you do a “cat /tmp/config.sh” or “cat /mnt/flash/config.sh” this command is not visible.

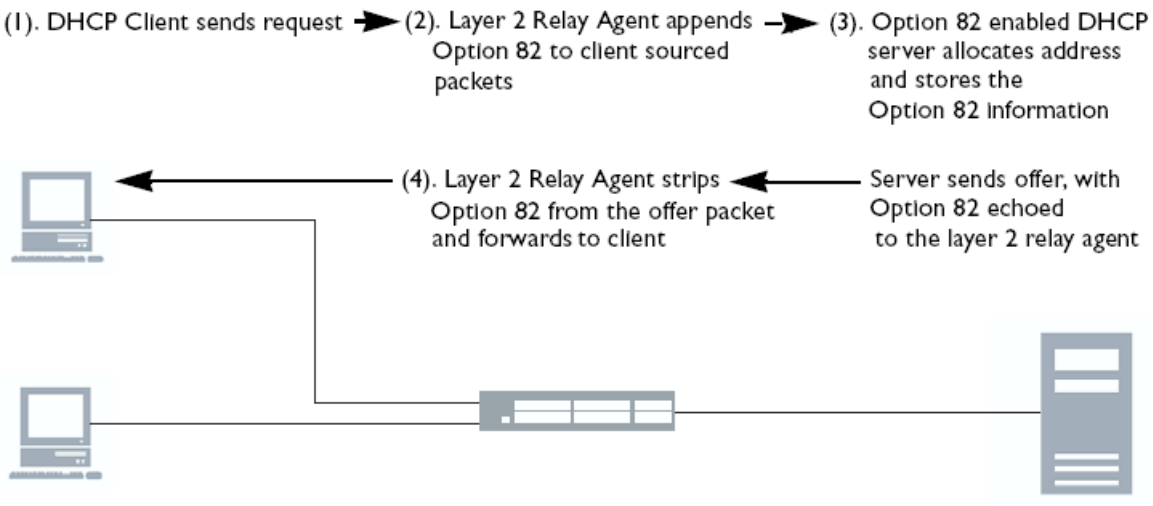
When dhcp service comes back, then the device will lease an IP address again, but not fetch any new configuration, as it will keep its restored configuration until next boot process.

```
# The following command allows the configuration to be saved to flash memory, and this will be restore if dhcp service is out.
save_configuration
```

dhcp option 82

DHCP Option 82 relay feature will be supported in a future release.
DHCP Relay Agent Information Option 82 is an extension to the Dynamic Host Configuration Protocol (DHCP), and is defined in RFC 3046 and RFC 3993. DHCP Option 82 can be used to send information about DHCP clients to the authenticating DHCP server. DHCP Option 82 can as an example identify the VLAN number, port number as well as a customer ID of a client, during any IP address allocation. When DHCP Option 82 is enabled on the CPE, it inserts the per port defined information into the DHCP packets as they pass through the CPE on their way to the DHCP server. The DHCP server stores the IP allocation record. The CPE will strip off the DHCP reply from the DHCP server, so the clients will never see the DHCP option 82 information.
The DHCP Option 82 information can hold a 32 char string per port.

```
# Syntax is switch --set-port-dhcp-option82=PORT:enable[:Circuit ID[:Remote ID]]
switch --set-port-dhcp-option82=1:1:”DKT 797xx LAN port 1”:”Client XYZ”
switch --set-port-dhcp-option82=2:1:”DKT 797xx LAN port 2”:”Client XYZ”
switch --set-port-dhcp-option82=3:1:”DKT 797xx LAN port 3”:”Client XYZ”
switch --set-port-dhcp-option82=4:1:”DKT 797xx LAN port 4”:”Client XYZ”
```


(1). DHCP Client sends request
(2). Layer 2 Relay Agent appends Option 82 to client sourced packets
(3). Option 82 enabled DHCP server allocates address and stores the Option 82 information
(4). Layer 2 Relay Agent strips Option 82 from the offer packet and forwards to client
Server sends offer, with Option 82 echoed to the layer 2 relay agent

support for ssh

In order to have SSH support, please insert the following command in the configuration script:

```
# SSH daemon is started with the following command
/etc/init.d/sshd start
```

The CPE is preconfigured with a login for SSH, please consult DKTCOMEGA for user name and password.

The first time the SSH daemon is started; two secret key files are generated.

Please note that it takes a while to generate the secret key files. The secret key files are not automatically stored to flash.

Save the SSH secret key files to flash using save_configuration in the configuration file:

```
# Save configuration to flash memory, same SSH key is used at every boot
save_configuration
```

Now it is possible to log into the CPE as the user ”Administrator” (case sensitive) through SSH.

```
ssh Administrator@<IP address>
```

or

```
ssh -l Administrator <IP address>
```

or using e.g. Putty application

When logged in as Administrator, it is not possible to make any changes, as you must switch user to root with this command:

```
su
```

Now it is possible to run all of the configuration commands, and it is possible to change the password of the user with the command

```
passwd <username>
```

Now copy the password files to a tftp server, typing

```
cd /etc
tftp -p -l shadow -r shadow <TFTP Server IP Address>
tftp -p -l passwd -r passwd <TFTP Server IP Address>
```

These two password files have to be pushed to all CPEs. You can edit CPEs configuration files by inserting the following commands:

```
# Get the password files for Administrator from TFTP server and store this in /tmp directory
tftp -g -r shadow -l /tmp/shadow <TFTP Server IP Address>
tftp -g -r passwd -l /tmp/passwd <TFTP Server IP Address>
chmod 600 /tmp/passwd /tmp/shadow
# Move the password files to the RAM-disk version of the files
mv /tmp/passwd /tmp/shadow /var
# save configuration to flash memory
save_configuration
```

The TFTP commands are only needed to be in the configuration file once, and can be deleted before the CPE is rebooted the next time.
The save_configuration command compares the password files with the stored files, and will not over-write the flash copy unless there are any changes.

Another way is to issue this one-line command from a Linux host PC without modifying the configuration file:

```
ssh Administrator@<CPE IP> “tftp -g -r shadow -l /tmp/shadow <TFTP Server IP>; tftp -g -r passwd -l /tmp/passwd <TFTP Server IP>;chmod 600 /tmp/passwd /tmp/shadow;mv /tmp/passwd /tmp/shadow /var;save_configuration”
```

The files can also be transferred with http or https using wget:

```
ssh Administrator@<CPE IP> “cd /tmp; wget https://<Web server IP>/passwd; wget https://<Web server IP>/shadow;chmod 600 /tmp/passwd /tmp/shadow;mv /tmp/passwd /tmp/shadow /var;save_configuration”
```

configuration of snmp values

SNMP feature will be supported in a future release.
The following SNMP values can be set by the configuration file:

SysContact the administrate contact for the network
echo “syscontact techsupport@example.com” >> /etc/snmp/snmpd.local.conf

SysLocation for the location of the system
echo “syslocation somewhere” >> /etc/snmp/snmpd.local.conf

SysName the name of the system e.g the customer identification
echo “sysname customerXYZ” >> /etc/snmp/snmpd.local.conf

syslog

Syslog feature will be supported in a future release.
Support for remote logging via syslog (RFC 3164)
To start syslog, enter the following line in your configuration file

```
syslogd [-l <log level>] -R <Remote server IP>
```

The syslog daemon sends logging information in UDP packets - port 514.

If all IP addresses are handled by the DHCP server, then there is also a way that the syslog daemon may be started by the DHCP client:

```
echo “-O logsrv” > /tmp/dhcp_requests.txt
/etc/init.d/udhcpc restart
```

The daemon will be started by the DHCP client if the log server parameter (DHCP option 7) is received in the DHCP response.

You may control which extra DHCP options that are requested in DHCP option 55. It is done by creating a file /tmp/dhcp_requests.txt containing just one line with a list of request commands to the DHCP client.

The format of the line is:
-O <option name> [-O <option name>] ...

The following values for <option name> are currently supported:

Name	DHCP Option	Description
dns	6	Domain name server IP
logsrv	7	Log server IP address
hostname	12	Hostname of the box
domain	15	Domain name
serverid	54	DHCP server identifier

Laser eye safety warning statement

Warning:
Risk of eye injury by laser
Fiber optic equipment can emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to a light source.

AVERTISSEMENT
Risques de blessure oculaire par lumière laser
L'équipement de fibres optiques peut émettre une lumière laser ou infrarouge nuisible à vos yeux. Ne regardez jamais en direction de fibres optiques ou d'un port connecteur. Supposez toujours que les câbles de fibres optiques sont connectés à une source de lumière.

WARNUNG
Risiko einer Augenverletzung durch Laser
Risiko einer Augenverletzung durch Laser Glasfasergeräte können Laserstrahlen oder ultraviolettes Licht aussenden, das Ihre Augen verletzen kann. Schauen Sie nie direkt in
Laser eye safety warning statement

einen Glasfaserleiter oder Verbindungsanschluss. Gehen Sie immer davon aus, dass Glasfaserkabel mit einer Lichtquelle verbunden sind.

ADVERTENCIA
Riesgo de lesión en los ojos por láser
El equipo de fibra óptica puede emitir una luz láser o infrarroja que dañe sus ojos. Nunca mire un puerto de fibra óptica o conector. Siempre asuma que los cables de fibra óptica están conectados a una fuente de luz.

AVISO
O laser pode causar ferimentos no olho
O equipamento de fibra ótica pode emitir laser ou luz infravermelha que pode causar danos a sua vista. Nunca olhe para dentro da fibra ótica ou da porta do conector. Tenha sempre em mente que os cabos de fibra ótica estão ligados a uma fonte de luz.

AVVISO
Rischio di ustioni agli occhi dovute al laser
Le apparecchiature con fibre ottiche possono emettere raggi laser o infrarossi in grado di provocare ferite agli occhi. Non guardare mai all'interno di una porta di connessione o una fibra ottica. Tenere sempre presente che i cavi a fibra ottica sono collegati a una sorgente luminosa.

Laser eye safety connector inspection warning statement

Warning:
Risk of eye injury
When inspecting a connector, ensure that light sources are off. The light source used in fiber optic cables can damage your eyes.

AVERTISSEMENT
Risques de blessure oculaire
Assurez-vous que toutes les sources de lumière ont été désactivées avant de procéder au contrôle d'un connecteur. La source de lumière utilisée dans les câbles de fibres optiques risque de provoquer des lésions oculaires.
Translations of Safety Messages

WARNUNG
Verletzungsrisiko der Augen
Achten Sie bei der Kontrolle der Anschlüsse darauf, dass die Lichtquellen abgeschaltet sind. Die für die Glasfaserkabel verwendeten Lichtquellen können Augenschäden hervorrufen.

ADVERTENCIA
Riesgo de lesiones oculares
Cuando inspeccione un conector, controle que las fuentes de luz estén apagadas. La fuente de luz que utilizan los cables de fibra óptica puede ocasionar daños en la vista.

AVISO
Risco de ferimento nos olhos
Ao inspecionar um conector, verifique se as fontes luminosas estão desligadas. A fonte luminosa usada nos cabos de fibra ótica pode causar danos a seus olhos.

AVVISO
Rischio di lesioni agli occhi
Quando si esamina un connettore, assicurarsi che le sorgenti di luce siano spente. La sorgente di luce utilizzata nei cavi a fibre ottiche potrebbero danneggiare gli occhi.

Connector cleaning safety warning statement

Warning:
Risk of eye injury
When inspecting a connector, ensure that light sources are off. The light source used in fiber optic cables can damage your eyes. To avoid getting debris in your eyes, wear safety glasses when working with the canned air duster. To avoid eye irritation on contact, wear safety glasses when working with isopropyl alcohol.

AVERTISSEMENT
Risques de blessure oculaire
Connector cleaning safety warning statement
Installation — SFP, SFP+, XFP, and OADM Hardware Components September 2012 103
Assurez-vous que toutes les sources de lumière ont été désactivées avant de procéder au contrôle d'un connecteur. La source de lumière utilisée dans les câbles de fibres optiques risque de provoquer des lésions oculaires. Pour éviter tout risque de projection vers les yeux, portez des lunettes de protection lorsque vous utilisez la bombe dépoussiérante à air comprimé. Pour éviter tout risque d'irritation oculaire, portez des lunettes de protection lorsque vous utilisez de l'alcool à 90°.

WARNUNG
Verletzungsrisiko der Augen
Achten Sie bei der Kontrolle der Anschlüsse darauf, dass die Lichtquellen abgeschaltet sind. Die für die Glasfaserkabel verwendeten Lichtquellen können Augenschäden hervorrufen. Zum Schutz vor Schmutzteilchen tragen Sie eine Schutzbrille, wenn Sie mit einem Pressluft-Spray arbeiten. Zum Schutz vor Augenirritationen tragen Sie eine Schutzbrille, wenn Sie mit Isopropanol arbeiten.

ADVERTENCIA
Riesgo de lesiones
Cuando inspeccione un conector, controle que las fuentes de luz estén apagadas. La fuente de luz que utilizan los cables de fibra óptica puede ocasionar daños en la vista. Cuando trabaje con el pulverizador de aire envasado, utilice gafas de seguridad para evitar el ingreso de residuos en los ojos. Utilice gafas de seguridad cuando trabaje con alcohol isopropilo para evitar irritación en los ojos.

AVISO
Risco de ferimento nos olhos
Ao inspecionar um conector, verifique se as fontes luminosas estão desligadas. A fonte luminosa usada nos cabos de fibra ótica pode causar danos a seus olhos. Para evitar que seus olhos sejam atingidos por resíduos, use óculos de segurança ao trabalhar com lata de ar comprimido. Para evitar irritação dos olhos, use óculos de segurança ao trabalhar com álcool isopropílico.

AVVISO
Rischio di lesioni agli occhi
Quando si esamina un connettore, assicurarsi che le sorgenti di luce siano spente. La sorgente di luce utilizzata nei cavi a fibre ottiche potrebbero danneggiare gli occhi. Per evitare l'accidentale introduzione di detriti negli occhi, indossare gli occhiali di sicurezza quando si lavora con un'impolveratrice ad aria compressa. Per evitare irritazioni oculari da contatto, indossare gli occhiali di sicurezza quando si lavora con alcool isopropilico.

PRODUCT SAFETY: Please refer to:
http://dkt.dk/safety