إستخدام دليل أستكشاف أخطاء الإيثاناليزر وإصلاحها على Nexus 7000

المحتويات

المقدمة

يصف هذا المستند الإيثانالايزر، أداة التقاط الحزم المتكاملة Cisco NX-OS لحزم التحكم المستندة إلى Wireshark.

معلومات أساسية

ويرشارك هو محلل بروتوكولات الشبكات مفتوحة المصدر يستخدم على نطاق واسع في العديد من الصناعات والمؤسسات التعليمية. إنها تفك شفرة الحزم الملتقطة بواسطة libpcap، مكتبة التقاط الحزم. يعمل Cisco NX-OS فوق نواة Linux، والتي تستخدم مكتبة libpcap لدعم التقاط الحزم.

مع الإيثانالايزر، يمكنك:

- التقاط الحزم التي يتم إرسالها أو استقبالها بواسطة المشرف.
- قم بتعيين عدد الحزم التي سيتم التقاطها.
- ثبتت الطول من الربط أن يكون قبض.
- عرض الحزم ذات معلومات البروتوكول التفصيلية أو الملخصة.
- فتح بيانات الحزمة الملتقطة وحفظها.
- تصفية الحزم الملتقطة على العديد من المعايير.
- تصفية الحزم التي سيتم عرضها على العديد من المعايير.
- قم بفك ترميز رأس 7000 الداخلي لحزمة التحكم.

لا يستطيع الإيثانالايزر:

- التخير عندما تواجه الشبكة مشاكل. لكن الإيثانالايزر يمكن ان يساعدكم على تحديد سبب المشكلة.
- التقاط حركة مرور مستوى البيانات التي يتم إعادة توجيهها في الأجهزة.
- دعم التقاط خاص بواجهة.

خيارات المخرجات

هذا عرض ملخص للمخرجات من أمر النطاق الداخلي للواجهة المحلية ethanalyzer. يعرض الخيار '؟' التعليمات.

```
DC# ethanalyzer local interface inband ?
  <CR>
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  autostop              Capture autostop condition
  capture-filter        Filter on ethanalyzer capture
  capture-ring-buffer   Capture ring buffer option
  decode-internal       Include internal system header decoding
  detail                Display detailed protocol information
  display-filter        Display filter on frames captured
  limit-captured-frames Maximum number of frames to be captured (default is
                        10)
  limit-frame-size      Capture only a subset of a frame
  raw                   Hex/Ascii dump the packet with possibly one line
                        summary
  write                 Filename to save capture to
  |                     Pipe command output to filter

DC# ethanalyzer local interface inband
Capturing on inband
2013-02-10 22:58:09.660171 00:23:33:74:47:05 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/1/00:23:33:74:47:00  Cost = 0
    Port = 0x8006
2013-02-10 22:58:09.696505   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:09.697311   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:10.018963   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:10.086445 00:26:99:c7:f0:c3 -> 01:00:0c:cc:cc:cd STP RST. Root = 32768/96/00:23:04:ee:be:01  Cost = 0
    Port = 0x905e
2013-02-10 22:58:10.086608 00:26:99:c7:f0:c3 -> 01:00:0c:cc:cc:cd STP RST. Root = 32768/96/00:23:04:ee:be:01  Cost = 0
    Port = 0x905e
2013-02-10 22:58:10.086667 88:43:e1:c7:4d:b8 -> 01:80:c2:00:00:00 STP RST. Root = 32768/0/00:0d:ec:a3:96:3c  Cost = 3
    Port = 0x9000
```

أستخدم الخيار 'detail' للحصول على معلومات البروتوكول التفصيلية. ^C يمكن إستخدامه للإجهاض وإعادة الحصول على مطالبة المحول في وسط عملية الالتقاط إذا لزم الأمر.

```
DC# ethanalyzer local interface inband detail
Capturing on inband
Frame 1 (106 bytes on wire, 74 bytes captured)
    Arrival Time: Feb 10, 2013 23:00:24.253088000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 106 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:eigrp]
Ethernet II, Src: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44), Dst: 01:00:5e:00:00:0a
(01:00:5e:00:00:0a)
    Destination: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)
        Address: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadca
st)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        Address: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.18.6 (10.10.18.6), Dst: 224.0.0.10 (224.0.0.10)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x30)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    ----------------------------------------SNIP----------------------------------------
```

خيارات التصفية

مرشح الالتقاط

أستخدم الخيار "capture-filter" لتحديد الحزم التي سيتم عرضها أو حفظها على القرص أثناء الالتقاط. يجافظ مرشح الالتقاط على معدل عالي من الالتقاط أثناء قيامك بتصفية. لأن التشريح الكامل لم يتم على الحزم، فإن حقول المرشح تكون محددة ومحددة مسبقا.

مرشح العرض

أستخدم الخيار 'display-filter' لتغيير عرض ملف الالتقاط (ملف tmp). يستخدم عامل تصفية العرض الحزم المشفرة بالكامل، لذلك يمكنك إجراء تصفية معقدة ومتقدمة جدا عند تحليل مسار الشبكة. مهما، ال TMP مبرد يستطيع تعبئ بسرعة، بما أن وه أوال على قبض كل ربط وبعد ذلك يعرض فقط الربط المرغوب.

في هذا المثال، يتم تعيين "الإطارات المحدودة" على 5. باستخدام خيار "capture-filter"، يدي لك إيثانالييزر خمس حزم تطابق المرشح "المضيف 10.10.10.2". باستخدام الخيار "display-

filter"، على قبض Ethanalyzer أولا على خمس حزم ثم يعرض الحزم التي تطابق المرشح "ip.addr==10.10.10.2" فقط.

```
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5
Capturing on inband
2013-02-10 12:51:52.150404   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.150480   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.496447   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.497201   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:53.149831   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
5 packets captured

DC# ethanalyzer local interface inband display-filter "ip.addr==10.10.10.2" limit-captured-frames 5
Capturing on inband
2013-02-10 12:53:54.217462   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:53:54.217819   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2 packets captured
```

خيارات الكتابة

كتابة

يتيح لك الخيار "الكتابة" كتابة بيانات الالتقاط إلى ملف في أحد أجهزة التخزين (مثل bootflash أو logflash) على محول سلسلة Cisco Nexus 7000 للتحليل لاحقا. يقتصر حجم ملف الالتقاط على 10 ميغابايت.

مثال على ethanalyzer أمر مع خيار 'write' وه ethanalyzer قارن محلي داخل النطاق write bootflash:capture_file_name. مثال على خيار 'write' مع 'capture-filter' واسم ملف الإخراج 'first-capture' وه:

```
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5 write ?
  bootflash:  Filename
  logflash:   Filename
  slot0:      Filename
  usb1:       Filename
  usb2:       Filename
  volatile:   Filename
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5 write
    bootflash:first-capture
```

عندما يتم حفظ بيانات الالتقاط في ملف، فإن الحزم الملتقطة ال يتم عرضها، بشكل افتراضي، في نافذة المحطة الطرفية. يجبر الخيار 'عرض' Cisco NX-OS على عرض الحزم أثناء حفظ بيانات الالتقاط في ملف.

Capture-Ring-buffer

ينشئ الخيار 'capture-ring-buffer' ملفات متعددة بعد عدد معين من الثواني، عدد محدد من الملفات، أو حجم ملف محدد. تعريفات تلك الخيارات موجودة في لقطة الشاشة هذه:

```
DC# ethanalyzer local interface inband capture-ring-buffer ?
  duration  Stop writing to the file or switch to the next file after value
            seconds have elapsed
  files     Stop writing to capture files after value number of files were
            written or begin again with the first file after value number of
            files were written (form a ring buffer)
  filesize  Stop writing to a capture file or switch to the next file after it
            reaches a size of value kilobytes
```

خيارات القراءة

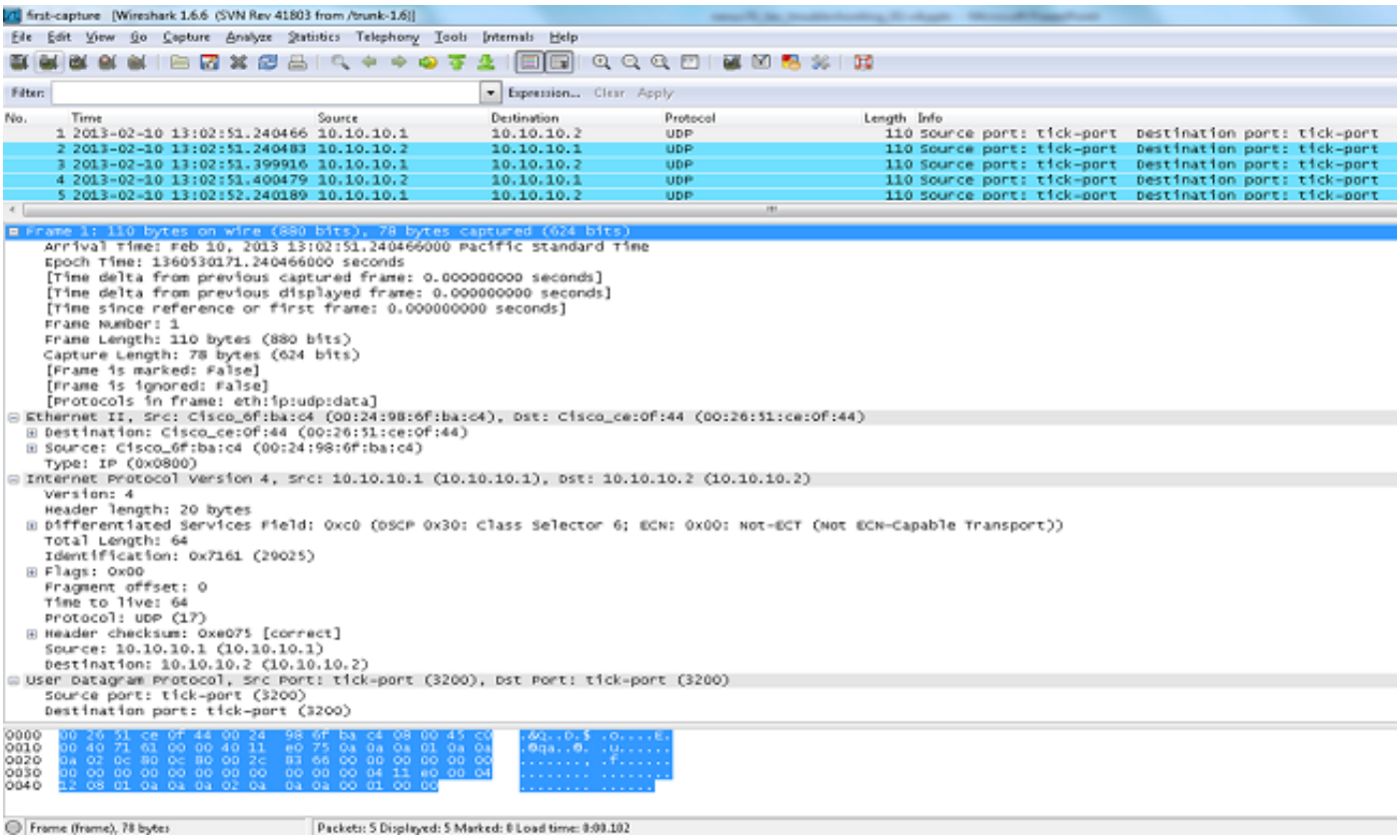
يتيح لك الخيار 'قراءة' قراءة الملف المحفوظ على الجهاز نفسه.

```
DC# ethanalyzer local read bootflash:first-capture
2013-02-10 13:02:51.240466   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.240483   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.399916   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.400479   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:52.240189   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200

DC# ethanalyzer local read bootflash:first-capture detail
Frame 1 (110 bytes on wire, 78 bytes captured)
---------------------------SNIP-------------------------------------------------
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4), Dst: 00:26:51:ce:0f:44
(00:26:51:ce:0f:44)
    Destination: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        Address: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4)
        Address: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
---------------------------------SNIP-------------------------------------
```

يمكنك أيضا نقل الملف إلى خادم أو كمبيوتر شخصي وقراءته باستخدام Wireshark أو أي تطبيق آخر يمكنه قراءة ملفات cap أو pcap.

```
DC# copy bootflash:first-capture tftp:
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the tftp server: 192.168.21.22
Trying to connect to tftp server......
Connection to Server Established.
TFTP put operation was successful
Copy complete.
```



فك ترميز داخلي مع خيار التفاصيل

يقوم خيار "فك الترميز الداخلي" بتقديم معلومات داخلية حول كيفية إعادة توجيه Nexus 7000 للحزمة. تساعدك هذه المعلومات على فهم تدفق الحزم عبر وحدة المعالجة المركزية (CPU) واستكشاف أخطائه وإصلاحها.

```
DC# ethanalyzer local interface inband decode-internal capture-filter "host 10.10.10.2" limit-captured-frames 5
detail
Capturing on inband
NXOS Protocol
    NXOS VLAN: 0==================>VLAN in decimal=0=L3 interface
    NXOS SOURCE INDEX: 1024 ======================>PIXM LTL source index in decimal=400=SUP inband
    NXOS DEST INDEX: 2569=======================>PIXM LTL destination index in decimal=0xa09=e1/25
Frame 1 (78 bytes on wire, 78 bytes captured)
    Arrival Time: Feb 10, 2013 22:40:02.216492000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 78 bytes
    Capture Length: 78 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:26:51:ce:0f:43 (00:26:51:ce:0f:43), Dst: 00:24:98:6f:ba:c3
(00:24:98:6f:ba:c3)
    Destination: 00:24:98:6f:ba:c3 (00:24:98:6f:ba:c3)
        Address: 00:24:98:6f:ba:c3 (00:24:98:6f:ba:c3)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:26:51:ce:0f:43 (00:26:51:ce:0f:43)
----------------------------------------------SNIP-----------------------------------------
```

قم بتحويل فهرس NX-OS إلى قاعدة سداسية عشرية، ثم أستخدم الأمر show system internal pixm info ltl x لتعيين فهرس المنطق الهدف المحلي (LTL) إلى واجهة مادية أو منطقية.

أمثلة على قيم Capture-Filter

التقاط حركة مرور البيانات من أو إلى مضيف IP

```
host 10.1.1.1
```

التقاط حركة المرور من أو إلى نطاق من عناوين IP

```
net 172.16.7.0/24
net 172.16.7.0 mask 255.255.255.0
```

التقاط حركة المرور من نطاق عناوين IP

```
src net 172.16.7.0/24
src net 172.16.7.0 mask 255.255.255.0
```

التقاط حركة المرور إلى مجموعة من عناوين IP

```
dst net 172.16.7.0/24
dst net 172.16.7.0 mask 255.255.255.0
```

التقاط حركة مرور البيانات فقط على بروتوكول معين - التقاط حركة مرور فقط DNS

DNS هو بروتوكول نظام اسم المجال.

```
port 53
```

التقط حركة مرور البيانات فقط على بروتوكول معين - على قبض حركة مرور

DHCP طقف

DHCP وه بروتوكول تكوين المضيف الديناميكي.

```
port 67 or port 68
```

التقاط حركة مرور البيانات غير الموجودة على بروتوكول معين - إستثناء حركة مرور HTTP وأ SMTP

SMTP وه بروتوكول نقل البريد البسيط.

```
host 172.16.7.3 and not port 80 and not port 25
```

التقاط حركة المرور غير الموجودة على بروتوكول معين - إستثناء حركة مرور DNS و ARP

ARP وه بروتوكول تحليل العنوان.

```
port not 53 and not arp
```

التقاط حركة مرور IP طقف - إستثناء بروتوكولات الطبقة السفلى مثل ARP و STP

STP وه بروتوكول الشجرة الممتدة.

```
ip
```

التقاط حركة مرور البث الأحادي طقف - إستثناء إعلانات البث والبث المتعدد

```
not broadcast and not multicast
```

التقاط حركة مرور البيانات ضمن نطاق منافذ الطبقة 4

```
tcp portrange 1501-1549
```

التقاط حركة مرور البيانات استنادا إلى نوع الإيثرنت - التقاط حركة مرور EAPOL

EAPOL هو بروتوكول المصادقة المتوسع عبر شبكة LAN.

```
ether proto 0x888e
```

حل التقاط IPv6

```
ether proto 0x86dd
```

التقاط حركة المرور استنادا إلى نوع بروتوكول IP

```
ip proto 89
```

رفض إطارات الإيثرنت استنادا إلى عنوان MAC - إستثناء حركة مرور البيانات التي تنتمي إلى مجموعة البث المتعدد LLDP

LLDP هو بروتوكول اكتشاف طبقة الارتباط.

```
not ether dst 01:80:c2:00:00:0e
```

عدم قبض UDLD، VTP، أو CDP حركة مرور

UDLD أحادي إتجاه كشف، VTP ال VLAN trunking بروتوكول، و CDP ال cisco إكتشاف بروتوكول.

```
ether host 01:00:0c:cc:cc:cc
```

التقاط حركة مرور البيانات من وأ إلى عنوان MAC

```
ether host 00:01:02:03:04:05
```

ملاحظة:
و = &&
وأ = ||
ال = !
تنسيق عنوان MAC: xx:xx:xx:xx:xx:xx

بروتوكولات مستوى التحكم الشائعة

- UDLD: وحدة التحكم في الوصول إلى الوسائط الوجهة (DMAC) = 01-00-0C-CC-CC و EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 و EthType = 0x8809. LACP يماثل بروتوكول التحكم في تجميع الارتباطات.
- بروتوكول الشجرة المتفرعة (STP): DMAC = 01:80:C2:00:00:00 و ETHtype = 0x4242 - وأ - DMAC = 01:00:0C:cc:CC:CD و ETHtype = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC و EthType = 0x2000
- بروتوكول LLDP: DMAC = 01:80:C2:00:00:0E وأ 01:80:C2:00:03 وأ 01:80:C2:00:00 و EthType = 0x88Cc
- dot1x: DMAC = 01:80:C2:00:00:03 و EthType = 0x888E. DOT1X ترمز إلى IEEE 802. 1x.
- IPv6: EthType = 0x86DD
- [قائمة أرقام منافذ TCP و UDP]

مشكلات معروفة

معرف تصحيح الأخطاء من Cisco CSCue48854: ال يلتقط EtherAlyzer capture-filter حركة مرور البيانات من وحدة المعالجة المركزية على SUP2.

معرف تصحيح الأخطاء من Cisco CSCtx79409: ال يمكن إستخدام عامل تصفية الالتقاط باستخدام ميزة فك التشفير الداخلي.

معرف تصحيح الأخطاء من Cisco CSCvi02546: يمكن أن تحتوي الحزمة التي تم إنشاؤها SUP3 على FCS، وهذا سلوك متوقع.

معلومات ذات صلة

- Wireshark: CaptureFilters
- Wireshark: DisplayFilters
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).