

Serie VCS o Expressway Xconfig y Xstatus Output Collection con PuTTY

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Conectar por consola](#)

[Conexión mediante SSH](#)

[VCS y Expressway Series x8.2](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo recopilar la salida CLI de los comandos `xconfig` y `xstatus` de la serie Video Communication Server (VCS) y los dispositivos de la serie Expressway como VCS-Control, VCS-Expressway, Expressway-C y Expressway-E, que ocasionalmente necesita recuperar el Cisco Technical Assistance Center (TAC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PuTTY o software de emulación de terminal similar como SecureCRT, Tera Term o similar.
- Nombre de usuario y contraseña de la cuenta de administrador para el dispositivo de la serie VCS/Expressway.
- Cable de consola serie RJ45-D-Sub9pin o Shell seguro (SSH) permitido en la ruta de red.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PuTTY (Visite la [página de descarga de PuTTY](#) para obtener una copia).

- En este ejemplo se utiliza un VCS-C que ejecuta la versión 7.2.1 que se aplica a través de la versión 8.2.2, que es la última versión en el momento actual.

Configurar

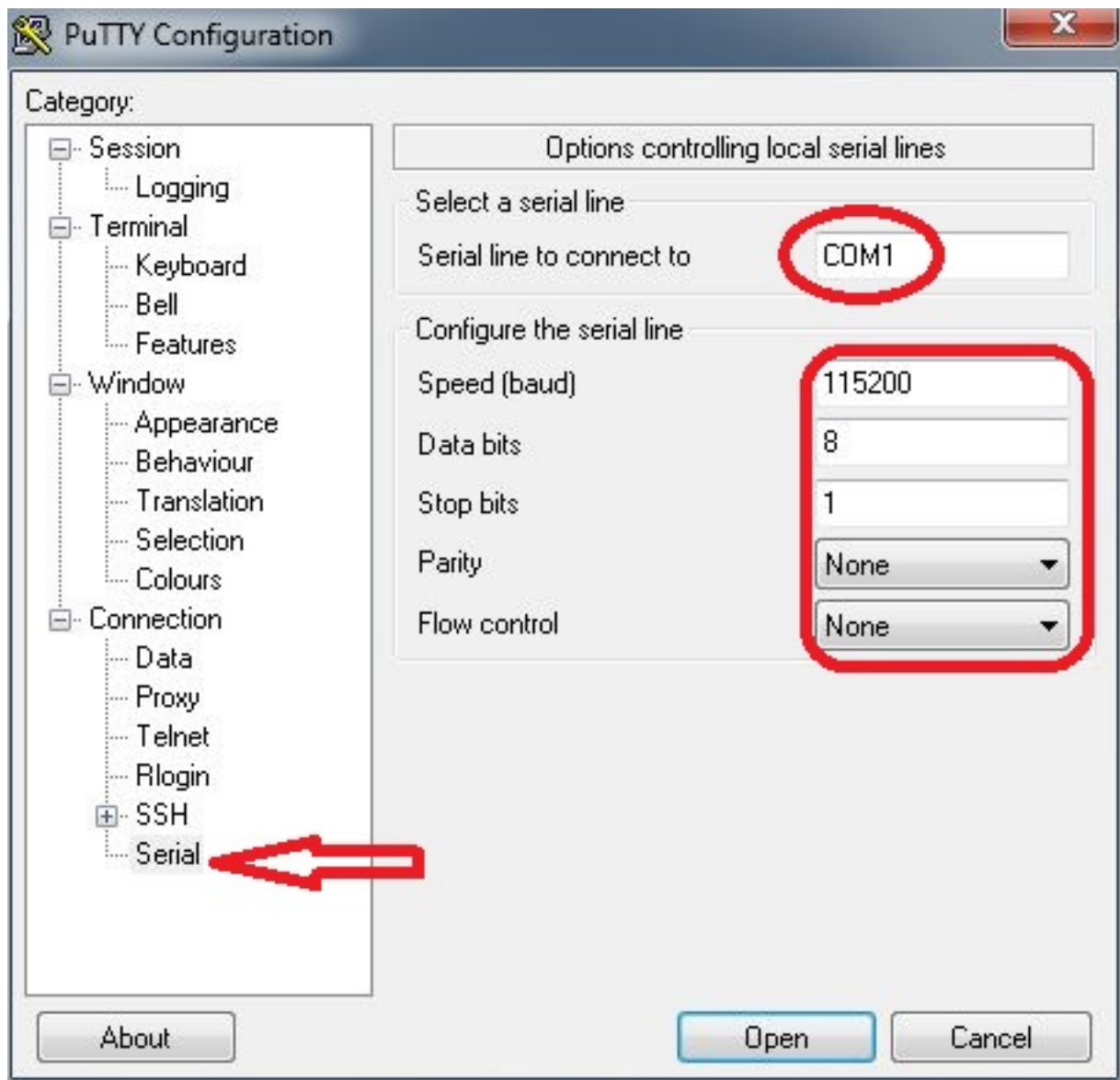
Conectar por consola

Nota: En este artículo se asume que tiene conectado un cable de consola serial físico funcional. Debería haber recibido uno con su dispositivo.

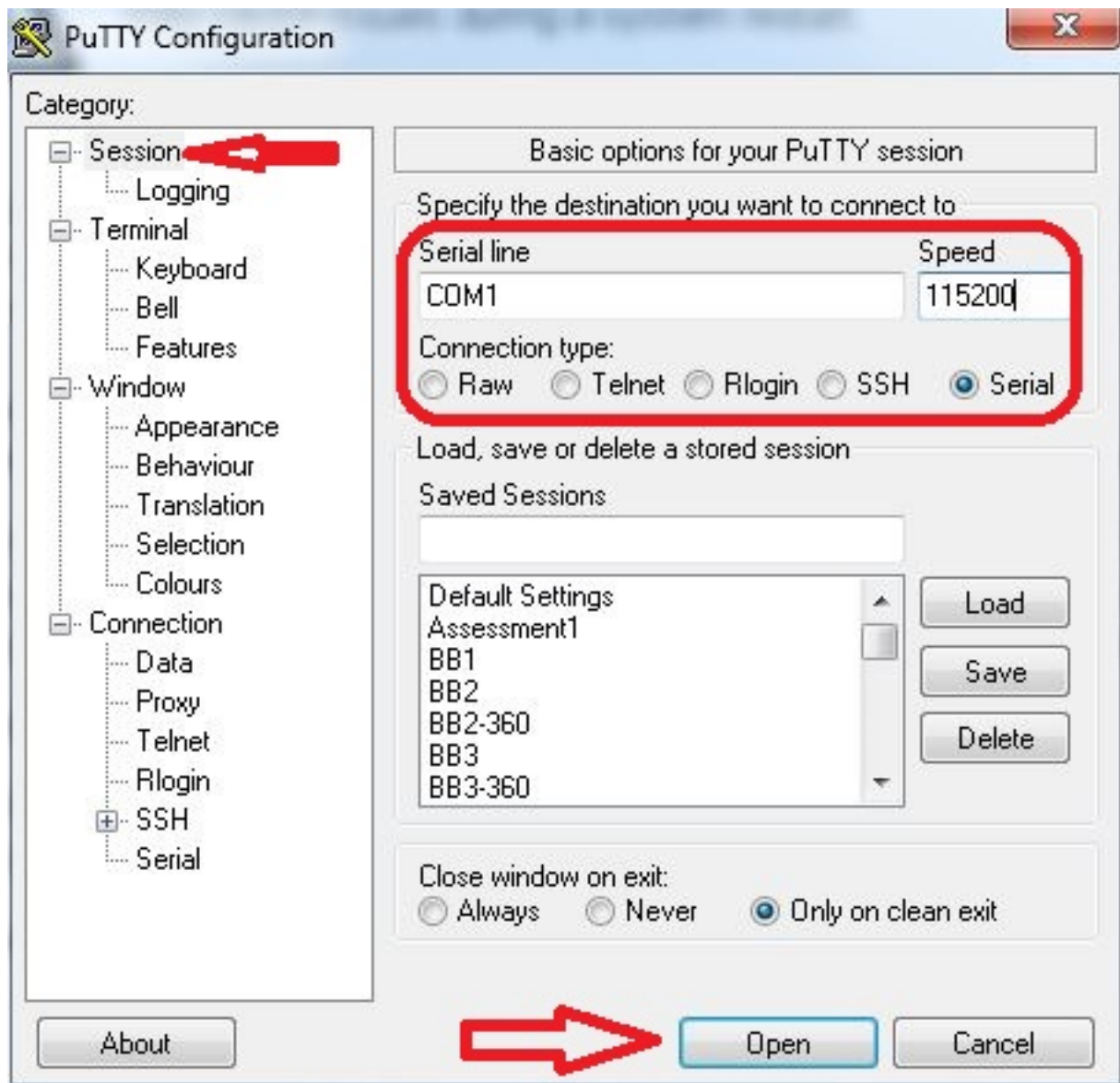
A continuación se muestra un ejemplo de los parámetros que debe configurar para el acceso a la consola serie en PuTTY.

Nota: Deberá ajustar el puerto de comunicación (COM) en función de cómo tenga la consola conectada al PC.

1. Vaya a **Configuration > Category > Connection > Serial** y ajuste los parámetros de serie como se muestra aquí:



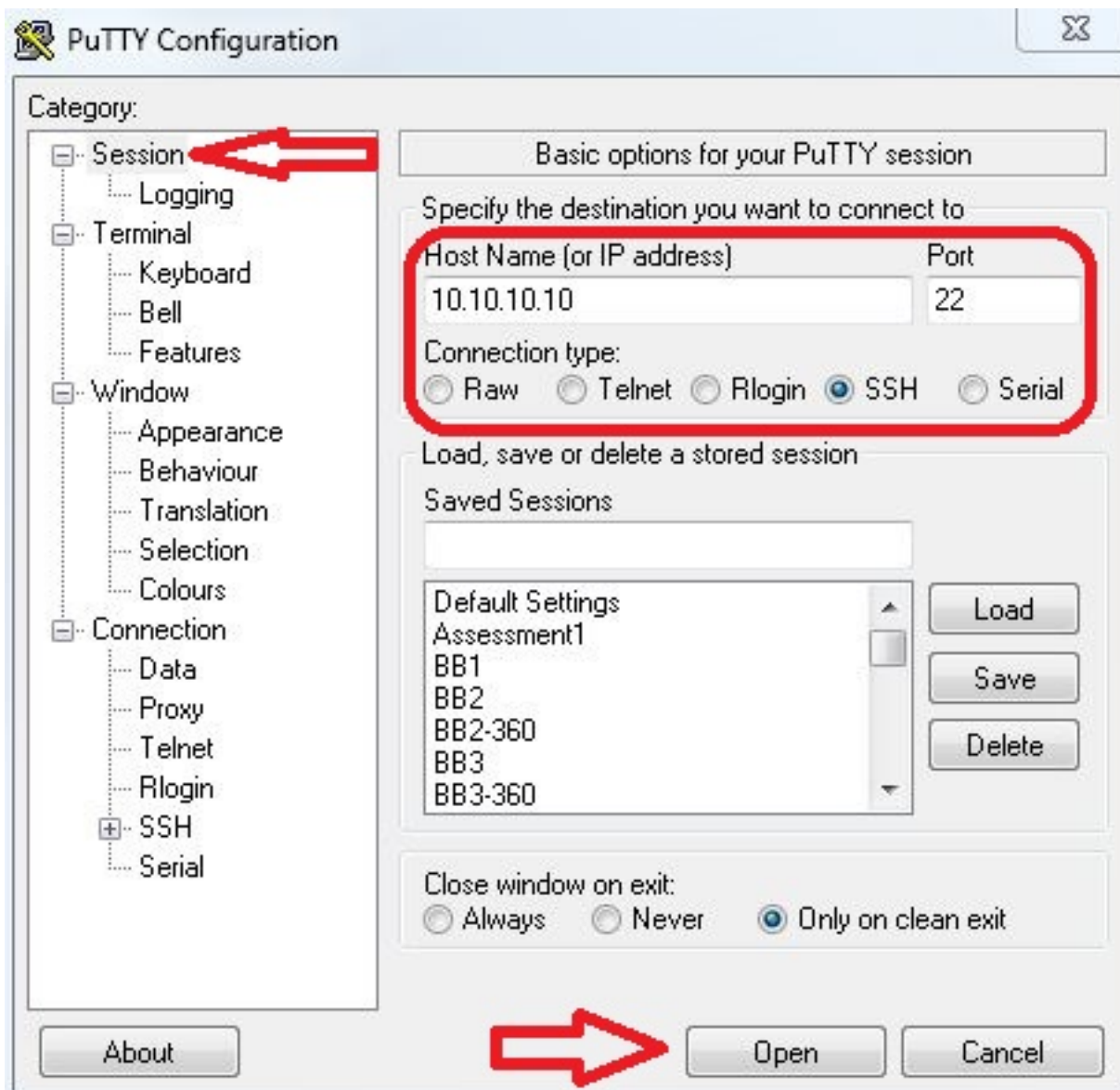
2. Vaya a **Category > Session**, seleccione **Serial** type como tipo de conexión y haga clic en **Open** como se muestra aquí:



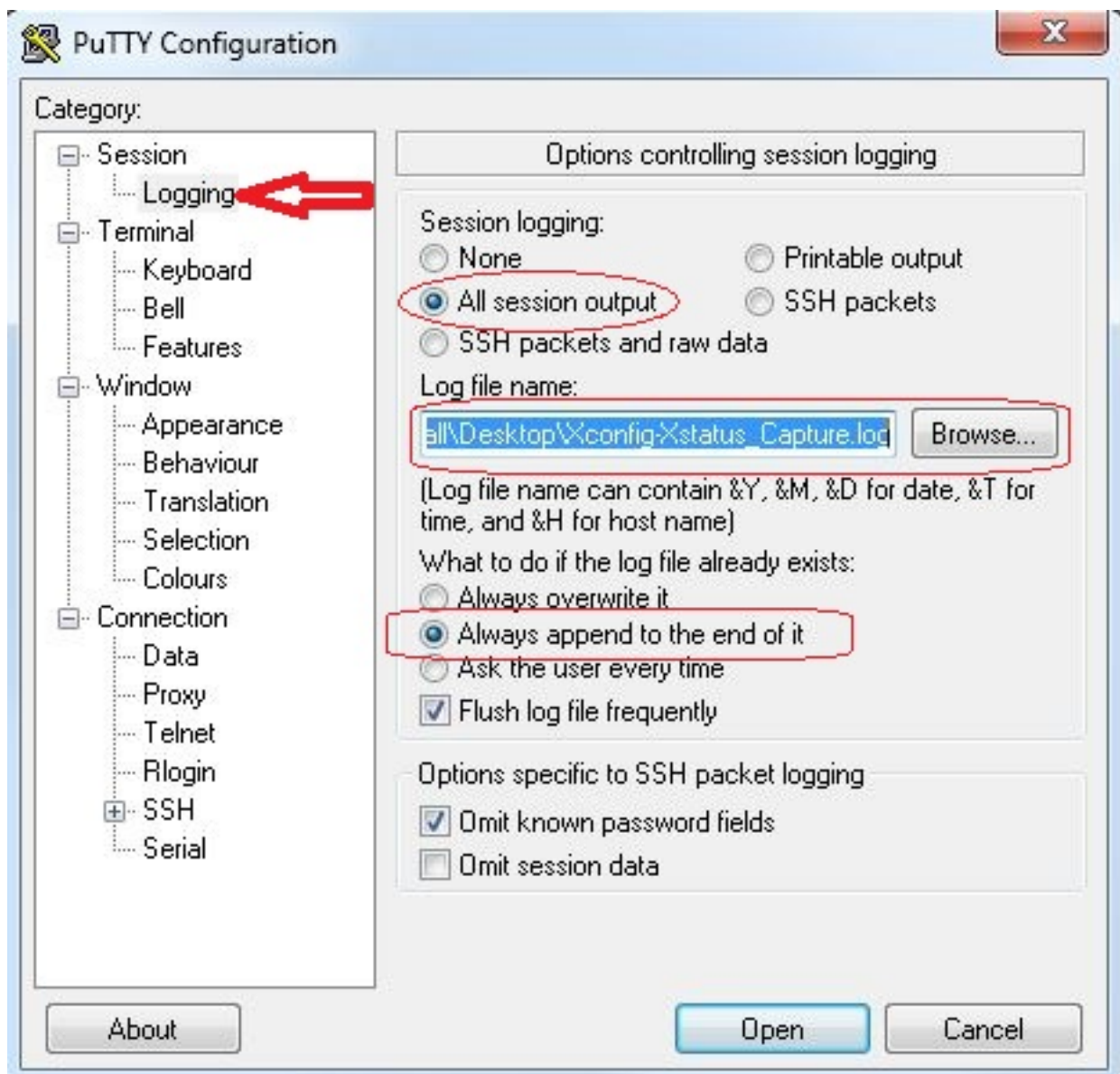
Conexión mediante SSH

Una alternativa más sencilla es el SSH en el dispositivo.

1. Utilice la dirección IP del dispositivo VCS/Expressway para ajustar los parámetros en PuTTY, como se muestra en este ejemplo:



2. Antes o durante la sesión PuTTY en el dispositivo, debe establecer la configuración de registro. Para hacerlo, vaya a **Configuration > Category > Session > Logging** y configure los ajustes para que coincidan con este ejemplo (ajuste la ruta de acceso del archivo y el nombre del archivo para que se adapten a su propio equipo y necesidades):



3. Una vez conectado y conectado, se muestra una pantalla similar a esta. Inicie sesión como admin como se indica aquí.

```
VCSorExpressway - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:

5 alarms:
 * error      Insecure password in use - The admin user has the default password
 set
 * warning    Security alert - The TMS agent database has the default LDAP passw
 ord set
 * warning    Configuration warning - The VCS is running in a legacy TMS Agent m
 ode; you are recommended to switch your system to use a different mode
 * warning    Insecure password in use - The root user has the default password
 set
 * warning    Security alert - The TMS agent database has the default replicatio
 n password set

Last login: Thu Jun 19 08:12:21 EDT 2014
Welcome to VCS1-Control
TANDBERG VCS Release X7.2.1
SW Release Date: 2012-09-25

OK
```

Precaución: Debido a que se trata de un entorno de laboratorio, se pueden ignorar las alarmas. Si se observan alarmas en un entorno de producción, deben abordarse lo antes posible.

4. Escriba el comando `xstatus` y presione **Enter**:

```
VCSorExpressway - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:

5 alarms:
 * error      Insecure password in use - The admin user has the default password
 set
 * warning    Security alert - The TMS agent database has the default LDAP passw
 ord set
 * warning    Configuration warning - The VCS is running in a legacy TMS Agent m
 ode; you are recommended to switch your system to use a different mode
 * warning    Insecure password in use - The root user has the default password
 set
 * warning    Security alert - The TMS agent database has the default replicatio
 n password set

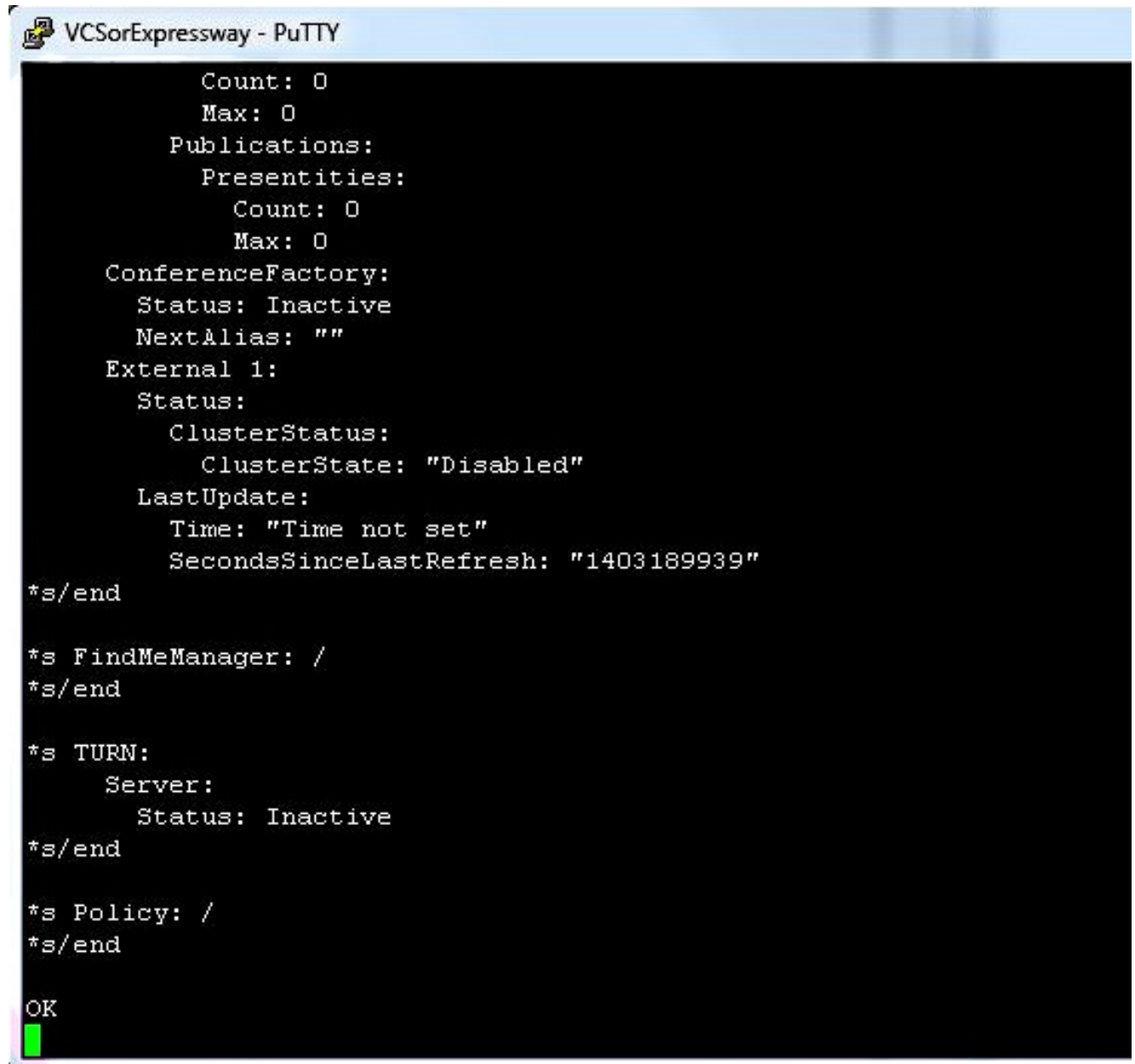
Last login: Thu Jun 19 08:12:21 EDT 2014
Welcome to VCS1-Control
TANDBERG VCS Release X7.2.1
SW Release Date: 2012-09-25

OK

xstatus
```

Esta es la salida `xstatus` que aparece después de presionar Enter. El resultado se desplazó

demasiado rápido para verlo hasta el final. Siempre que el registro se haya configurado anteriormente, esto estará en el archivo de texto.



```
Count: 0
Max: 0
Publications:
Presentities:
Count: 0
Max: 0
ConferenceFactory:
Status: Inactive
NextAlias: ""
External 1:
Status:
ClusterStatus:
ClusterState: "Disabled"
LastUpdate:
Time: "Time not set"
SecondsSinceLastRefresh: "1403189939"
*s/end

*s FindMeManager: /
*s/end

*s TURN:
Server:
Status: Inactive
*s/end

*s Policy: /
*s/end

OK
```

Ahora que ha recolectado el resultado del comando **xstatus**, está listo para recolectar el resultado del **comando xconfig**.

5. Escriba el comando **xconfig** y presione **Enter**.


```
xconfig
```

Este es un ejemplo del resultado **xconfig** después de presionar intro. El resultado se desplazó demasiado rápido para verlo hasta el final. Siempre que el registro se haya configurado anteriormente, esto estará en el archivo de texto.

```
VCsOrExpressway - PuTTY
% xConfiguration Policy AdministratorPolicy Service Server 3 Address: ""
% xConfiguration Policy AdministratorPolicy Service Path: ""
% xConfiguration Policy AdministratorPolicy Service Status Path: "status"
% xConfiguration Policy AdministratorPolicy Service UserName: ""
% xConfiguration Policy AdministratorPolicy Service Password: "(cipher)"
% xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='504' reason='Admin Policy Unavailabl
e' />"
% xConfiguration Policy FindMe Mode: Off
% xConfiguration Policy FindMe CallerId: IncomingID
% xConfiguration Policy FindMe UserDeviceRestriction: Off
% xConfiguration Applications ConferenceFactory Mode: Off
% xConfiguration Applications ConferenceFactory Alias: ""
% xConfiguration Applications ConferenceFactory Template: ""
% xConfiguration Applications ConferenceFactory Range Start: 1
% xConfiguration Applications ConferenceFactory Range End: 65535
% xConfiguration Applications OCS Relay Mode: Off
% xConfiguration Applications OCS Relay OCS Domain: ""
% xConfiguration Applications OCS Relay OCS Routing Prefix: "ocs"
% xConfiguration Applications Presence Server Mode: Off
% xConfiguration Applications Presence Server Publication ExpireDelta: 1800
% xConfiguration Applications Presence Server Subscription ExpireDelta: 3600
% xConfiguration Applications Presence User Agent Mode: Off
% xConfiguration Applications Presence User Agent ExpireDelta: 3600
% xConfiguration Applications Presence User Agent RetryDelta: 1800
% xConfiguration Applications Presence User Agent Presentity Idle Status: Online
% xConfiguration ResourceUsage Warning Activation Level: 90
% xConfiguration Services AdvancedMediaGateway Zone Name: ""
% xConfiguration Services AdvancedMediaGateway Policy Mode: Off
OK
```

VCS y Expressway Series x8.2

En la versión de software de x8.2, la `xconfiguration` y `xstatus` se incluyen ahora cuando se toma un registro de diagnóstico.

1. Vaya a **Mantenimiento > Diagnóstico > Registro de diagnóstico**.
2. Seleccione **Start new log** y luego inmediatamente **Stop logging**.

Nota: Este método también contiene el `loggingSnapshots.txt` que registra los mensajes en respuesta a las actividades que tienen lugar en la serie VCS o Expressway en ese momento.

El archivo de registro de diagnóstico descargado contiene estos archivos:

`loggingsnapshot.txt`: contiene mensajes de registro en respuesta a las actividades realizadas durante el período de registro.

`xconf_dump.txt`: contiene información sobre la configuración del sistema en el momento en que se inició el registro.

`xstat_dump.txt`: contiene información sobre el estado del sistema en el momento en que se inició el registro.

(si procede) `diagnostic_logging_tcpdump.pcap` - Contiene los paquetes capturados durante el período de registro.

Verificación

A continuación se muestra un ejemplo de cómo se ven los resultados `xstatus` y `xconfig` en el archivo de texto guardado con la configuración de registro:

```
xstatus
```

```
*s SystemUnit:
  Product: "TANDBERG VCS"
  Uptime: 24963390
  SystemTime: "2014-06-19 14:58:59"
  TimeZone: "US/Eastern"
  LocalTime: "2014-06-19 10:58:59"
  Software:
    Version: "X7.2.1"
    Build: "296181"
    Name: "s42700"
    ReleaseDate: "2012-09-25"
    ReleaseKey: "*****"
    Configuration:
      NonTraversalCalls: 500
      TraversalCalls: 200
      Registrations: 2500
      Expressway: False
      Encryption: True
      Interworking: True
      FindMe: True
      DeviceProvisioning: True
      DualNetworkInterfaces: False
      AdvancedAccountSecurity: False
      StarterPack: False
      EnhancedOCSCollaboration: True
    Hardware:
      Version: "VMWare"
      SerialNumber: "*****"
*s/end

*s Ethernet 1:
  MacAddress: "00:50:56:A1:70:06"
  Speed: 10000full
  IPv4:
    Address: "10.10.10.10"
    SubnetMask: "255.255.255.0"
*s/end

*s Ethernet 2:
  MacAddress: "00:50:56:A1:70:04"
  Speed: 10000full
  IPv4:
    Address: "192.168.0.100"
    SubnetMask: "255.255.255.0"
*s/end

*s Options:
  Option 1:
    Key: "116341X300-1-!!!!!!!"
    Description: "300 Non-traversal Calls"
  Option 2:
    Key: "116341P00-1-!!!!!!!"
    Description: "Device Provisioning"
  Option 3:
    Key: "116341G00-1-!!!!!!!"
    Description: "H323-SIP Interworking Gateway"
  Option 4:
```

```
Key: "116341U00-1-!!!!!!!"
Description: "FindMe"
Option 5:
Key: "116341C00-1-!!!!!!!"
Description: "Enhanced OCS Collaboration"
Option 8:
Key: "116341Y200-1-!!!!!!!"
Description: "200 Traversal Calls"
Option 9:
Key: "116341X200-1-!!!!!!!"
Description: "200 Non-traversal Calls"
*s/end

*s IP:
Protocol: IPv4
IPv4:
Gateway: "10.10.10.1"
*s/end

*s ExternalManager:
Status: Active
Address: "10.10.10.104"
Protocol: HTTP
URL: "tms/public/external/management/systemmanagementservice.asmx"
*s/end

*s Feedback 1:
Status: Off
*s/end

*s Feedback 2:
Status: Off
*s/end

*s Feedback 3:
Status: On
URL: "http://10.10.10.104/tms/public/feedback/code.aspx"
Expression: "/Event/CallDisconnected"
Expression: "/Event/CallConnected"
Expression: "/Event/CallFailure"
Expression: "/Event/RegistrationAdded"
Expression: "/Event/RegistrationChanged"
Expression: "/Event/ResourceUsage"
Expression: "/Event/AuthenticationFailure"
Expression: "/Status/Warnings"
*s/end

*s ResourceUsage:
Calls:
Traversal:
Current: 0
Max: 0
Total: 0
NonTraversal:
Current: 0
Max: 1
Total: 2
Registrations:
Current: 0
Max: 3
Total: 42
*s/end

*s Calls: /
```

*s/end

*s Zones:

DefaultZone:

Name: "DefaultZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

LocalZone:

DefaultSubZone:

Name: "DefaultSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

TraversalSubZone:

Name: "TraversalSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

ClusterSubZone:

Name: "ClusterSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Searches:

Current: 0

CurrentDirected: 0

Total: 64081

Dropped: 0

MaxSubSearchExceeded: 0

MaxTargetsExceeded: 0

Zone 1:

Name: "TraversalZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Status: Active

Type: TraversalClient

TraversalClient:

Peer 1:

H323:

Status: Active

Address: "10.10.10.102"

Port: 6001

LastStatusChange: "2014-04-03 09:50:35"

SIP:

Status: Active

Address: "10.10.10.102"

Port: 7001

LastStatusChange: "2014-04-03 09:49:13"

Server: "TANDBERG/4102 (X7.0)"

*s/end

*s Alternates: /

*s/end

*s Links:

Link 1:

Name: "DefaultSZtoTraversalSZ"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Link 2:

Name: "DefaultSZtoDefaultZ"

```
Bandwidth:
  LocalUsage: 0
  ClusterUsage: 0
Link 3:
  Name: "DefaultSZtoClusterSZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
Link 4:
  Name: "TraversalSZtoDefaultZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
Link 5:
  Name: "Zone001ToTraversalSZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
*s/end

*s Pipes: /
*s/end

*s Registrations: /
*s/end

*s SIP:
  Ethernet 1:
    IPv4:
      UDP:
        Status: Inactive
      TCP:
        Status: Active
        Address: "10.10.10.10:5060"
      TLS:
        Status: Active
        Address: "10.10.10.10:5061"
    IPv6:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
  Ethernet 2:
    IPv4:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
    IPv6:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
  Transport:
    Server 19857:
      Socket:
        Type: "SERV_UDP"
        State: "INUSE"
```

ID:
 Local: 85393
 Global: 0
Buffer:
 Input:
 Length: 20000
 Output:
 Length: 20000
Local:
 Address: "127.0.0.1:5060"
Remote:
 Address: ""
Network:
 Number: 1
Certificate:
 Subject:
 Name: ""
TLS:
 Cipher:
 Name: ""
Last:
 Packet:
 Received: 0
Close:
 In: 20
Secure: False
X509:
 Certificate:
 Verified: False
Queue:
 Max:
 Size: 0
 Add:
 Failures: 0
Flow:
 Token: ""
Server 19856:
Socket:
 Type: "SERV_TCP"
 State: "INUSE"
 ID:
 Local: 150928
 Global: 1
 Buffer:
 Input:
 Length: 0
 Output:
 Length: 0
Local:
 Address: "127.0.0.1:5060"
Remote:
 Address: ""
Network:
 Number: 1
Certificate:
 Subject:
 Name: ""
TLS:
 Cipher:
 Name: ""
Last:
 Packet:
 Received: 0
Close:

In: 20
Secure: False
X509:
 Certificate:
 Verified: False
Queue:
 Max:
 Size: 0
 Add:
 Failures: 0
Flow:
 Token: ""
Server 19855:
Socket:
 Type: "SERV_TLS"
 State: "INUSE"
 ID:
 Local: 216463
 Global: 2
 Buffer:
 Input:
 Length: 0
 Output:
 Length: 0
Local:
 Address: "127.0.0.1:5061"
Remote:
 Address: ""
Network:
 Number: 1
Certificate:
 Subject:
 Name: ""
TLS:
 Cipher:
 Name: ""
Last:
 Packet:
 Received: 0
Close:
 In: 20
Secure: True
X509:
 Certificate:
 Verified: False
Queue:
 Max:
 Size: 0
 Add:
 Failures: 0
Flow:
 Token: ""
Server 19854:
Socket:
 Type: "SERV_UDP"
 State: "INUSE"
 ID:
 Local: 281998
 Global: 3
 Buffer:
 Input:
 Length: 20000
 Output:
 Length: 20000

Local:
Address: "[::1]:5060"
Remote:
Address: ""
Network:
Number: 1
Certificate:
Subject:
Name: ""
TLS:
Cipher:
Name: ""
Last:
Packet:
Received: 0
Close:
In: 20
Secure: False
X509:
Certificate:
Verified: False
Queue:
Max:
Size: 0
Add:
Failures: 0
Flow:
Token: ""
Server 19853:
Socket:
Type: "SERV_TCP"
State: "INUSE"
ID:
Local: 347533
Global: 4
Buffer:
Input:
Length: 0
Output:
Length: 0
Local:
Address: "[::1]:5060"
Remote:
Address: ""
Network:
Number: 1
Certificate:
Subject:
Name: ""
TLS:
Cipher:
Name: ""
Last:
Packet:
Received: 0
Close:
In: 20
Secure: False
X509:
Certificate:
Verified: False
Queue:
Max:
Size: 0

Add:
Failures: 0
Flow:
Token: ""
Server 19852:
Socket:
Type: "SERV_TLS"
State: "INUSE"
ID:
Local: 413068
Global: 5
Buffer:
Input:
Length: 0
Output:
Length: 0
Local:
Address: "[::1]:5061"
Remote:
Address: ""
Network:
Number: 1
Certificate:
Subject:
Name: ""
TLS:
Cipher:
Name: ""
Last:
Packet:
Received: 0
Close:
In: 20
Secure: True
X509:
Certificate:
Verified: False
Queue:
Max:
Size: 0
Add:
Failures: 0
Flow:
Token: ""
Server 19851:
Socket:
Type: "SERV_TCP"
State: "INUSE"
ID:
Local: 478603
Global: 6
Buffer:
Input:
Length: 0
Output:
Length: 0
Local:
Address: "10.10.10.10:5060"
Remote:
Address: ""
Network:
Number: 2
Certificate:
Subject:

Name: ""
TLS:
 Cipher:
 Name: ""
Last:
 Packet:
 Received: 0
Close:
 In: 20
Secure: False
X509:
 Certificate:
 Verified: False
Queue:
 Max:
 Size: 0
 Add:
 Failures: 0
Flow:
 Token: ""
Server 19850:
 Socket:
 Type: "SERV_TLS"
 State: "INUSE"
 ID:
 Local: 544138
 Global: 7
 Buffer:
 Input:
 Length: 0
 Output:
 Length: 0
 Local:
 Address: "10.10.10.10:5061"
 Remote:
 Address: ""
 Network:
 Number: 2
 Certificate:
 Subject:
 Name: ""
 TLS:
 Cipher:
 Name: ""
 Last:
 Packet:
 Received: 0
 Close:
 In: 20
 Secure: True
 X509:
 Certificate:
 Verified: False
 Queue:
 Max:
 Size: 0
 Add:
 Failures: 0
 Flow:
 Token: ""
Client 7747:
 Socket:
 Type: "TLS_OUTG"
 State: "INUSE"

ID:
 Local: 825433667
 Global: 654
Buffer:
 Input:
 Length: 5120
 Output:
 Length: 20000
Local:
 Address: "10.10.10.10:27573"
Remote:
 Address: "10.10.10.102:7001"
Network:
 Number: 2
Certificate:
 Subject:
 Name: ""
TLS:
 Cipher:
 Name: "DHE-RSA-AES256-SHA"
Last:
 Packet:
 Received: -1798628722
Close:
 In: 900
Secure: True
X509:
 Certificate:
 Verified: False
Queue:
 Max:
 Size: 1
 Add:
 Failures: 0
Flow:
 Token: ""

*s/end

*s H323:

 Registration:
 Status: Active
 IPv4:
 Address: "10.10.10.10:1719"
 CallSignaling:
 Status: Active
 IPv4:
 Address: "10.10.10.10:1720"
 Assent:
 CallSignaling:
 Status: Inactive
 H46018:
 CallSignaling:
 Status: Inactive

*s/end

*s Applications:

 Presence:
 UserAgent:
 Status: Inactive
 Presentity:
 Count: 0
 Server:
 Subscriptions:
 Count: 0

Max: 0
Expired: 0
Subscribers:
 Count: 0
 Max: 0
Status: Inactive
Presentities:
 Count: 0
 Max: 0
Publications:
 Presentities:
 Count: 0
 Max: 0
ConferenceFactory:
 Status: Inactive
 NextAlias: ""
External 1:
 Status:
 ClusterStatus:
 ClusterState: "Disabled"
 LastUpdate:
 Time: "Time not set"
 SecondsSinceLastRefresh: "1403189939"

*s/end

*s FindMeManager: /

*s/end

*s TURN:

 Server:

 Status: Inactive

*s/end

*s Policy: /

*s/end

OK

```
xcommand xconfig
*c xConfiguration Login Remote Protocol: LDAP
*c xConfiguration Login Remote LDAP Server Address: ""
*c xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord
*c xConfiguration Login Remote LDAP Server Port: 389
*c xConfiguration Login Remote LDAP VCS BindUsername: ""
*c xConfiguration Login Remote LDAP VCS BindPassword: "{cipher}XXXXXXXXXX
XXXXXXXXXXXX"
*c xConfiguration Login Remote LDAP VCS BindDN: ""
*c xConfiguration Login Remote LDAP BaseDN Accounts: ""
*c xConfiguration Login Remote LDAP BaseDN Groups: ""
*c xConfiguration Login Remote LDAP Encryption: Off
*c xConfiguration Login Remote LDAP SASL: DIGEST-MD5
*c xConfiguration Login Remote LDAP CRLCheck: None
*c xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory
*c xConfiguration SystemUnit Name: "VCS1-Control"
*c xConfiguration SystemUnit Maintenance Mode: Off
*c xConfiguration Option 1 Key: "116341X300-1-!!!!!!!"
*c xConfiguration Option 2 Key: "116341P00-1-!!!!!!!"
*c xConfiguration Option 3 Key: "116341G00-1-!!!!!!!"
*c xConfiguration Option 4 Key: "116341U00-1-!!!!!!!"
*c xConfiguration Option 5 Key: "116341C00-1-!!!!!!!"
*c xConfiguration Option 8 Key: "116341Y200-1-!!!!!!!"
*c xConfiguration Option 9 Key: "116341X200-1-!!!!!!!"
*c xConfiguration Ethernet 1 Speed: Auto
*c xConfiguration Ethernet 1 IP V4 Address: "10.10.10.10"
*c xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"
*c xConfiguration Ethernet 1 IP V6 Address: ""
*c xConfiguration Ethernet 2 Speed: Auto
*c xConfiguration Ethernet 2 IP V4 Address: "192.168.0.100"
*c xConfiguration Ethernet 2 IP V4 SubnetMask: "255.255.255.0"
*c xConfiguration Ethernet 2 IP V6 Address: ""
*c xConfiguration IPProtocol: IPv4
*c xConfiguration IP Gateway: "10.10.10.1"
*c xConfiguration IP QoS Mode: None
*c xConfiguration IP QoS Value: 0
*c xConfiguration IP V6 Gateway: ""
*c xConfiguration IP DNS Domain Name: "#####.local"
*c xConfiguration IP DNS Hostname: "VCS1-Control"
*c xConfiguration IP Ephemeral PortRange Start: 40000
*c xConfiguration IP Ephemeral PortRange End: 49999
*c xConfiguration IP RFC4821 Mode: Disabled
*c xConfiguration Administration Telnet Mode: Off
*c xConfiguration Administration SSH Mode: On
*c xConfiguration Administration HTTP Mode: On
*c xConfiguration Administration HTTPS Mode: On
*c xConfiguration Administration LCDPanel Mode: On
*c xConfiguration ExternalManager Address: "10.10.10.104"
*c xConfiguration ExternalManager Path: "tms/public/external/management/system
managementservice.asmx"
*c xConfiguration ExternalManager Protocol: HTTP
*c xConfiguration ExternalManager Server Certificate Verification Mode: On
*c xConfiguration Registration RestrictionPolicy Mode: None
*c xConfiguration Registration RestrictionPolicy Service Protocol: HTTP
*c xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On
*c xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off
*c xConfiguration Registration RestrictionPolicy Service Server 1 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Server 2 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Server 3 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Path: ""
*c xConfiguration Registration RestrictionPolicy Service Status Path: "status"
```

```
*c xConfiguration Registration RestrictionPolicy Service UserName: ""
*c xConfiguration Registration RestrictionPolicy Service Password: "{cipher}
XXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject
status='504' reason='Registration Policy Unavailable'/>"
*c xConfiguration Alternates ConfigurationMaster: 1
*c xConfiguration Alternates Cluster Name: ""
*c xConfiguration Alternates Peer 1 Address: ""
*c xConfiguration Alternates Peer 2 Address: ""
*c xConfiguration Alternates Peer 3 Address: ""
*c xConfiguration Alternates Peer 4 Address: ""
*c xConfiguration Alternates Peer 5 Address: ""
*c xConfiguration Alternates Peer 6 Address: ""
*c xConfiguration Transform 1 Description: "Transform destination aliases to
URI format"
*c xConfiguration Transform 1 State: Enabled
*c xConfiguration Transform 1 Priority: 1
*c xConfiguration Transform 1 Pattern String: "([^\@]*)"
*c xConfiguration Transform 1 Pattern Type: Regex
*c xConfiguration Transform 1 Pattern Behavior: Replace
*c xConfiguration Transform 1 Pattern Replace: "\1@#####.local"
*c xConfiguration Call Loop Detection Mode: On
*c xConfiguration Call Routed Mode: Always
*c xConfiguration Call Services CallsToUnknownIPAddresses: Indirect
*c xConfiguration Call Services Fallback Alias: ""
*c xConfiguration H323 Mode: On
*c xConfiguration H323 Gatekeeper Registration UDP Port: 1719
*c xConfiguration H323 Gatekeeper Registration ConflictMode: Reject
*c xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720
*c xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000
*c xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999
*c xConfiguration H323 Gatekeeper TimeToLive: 1800
*c xConfiguration H323 Gatekeeper CallTimeToLive: 120
*c xConfiguration H323 Gatekeeper AutoDiscovery Mode: On
*c xConfiguration H323 Gateway CallerId: ExcludePrefix
*c xConfiguration SIP Mode: On
*c xConfiguration SIP Domains Domain 1 Name: "#####.com"
*c xConfiguration SIP Domains Domain 2 Name: "#####.local"
*c xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"
*c xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains%|
%ip%)"
*c xConfiguration SIP Routes Route 1 Header Name: "Event"
*c xConfiguration SIP Routes Route 1 Header Pattern: "(ua-profile|phonebook).*"
*c xConfiguration SIP Routes Route 1 Authenticated: Off
*c xConfiguration SIP Routes Route 1 Address: "127.0.0.1"
*c xConfiguration SIP Routes Route 1 Port: 22400
*c xConfiguration SIP Routes Route 1 Transport: TCP
*c xConfiguration SIP Routes Route 1 Tag: "Provisioning"
*c xConfiguration SIP Routes Route 2 Method: "INFO"
*c xConfiguration SIP Routes Route 2 Request Line Pattern: ".*@(%localdomains%|
%ip%)"
*c xConfiguration SIP Routes Route 2 Header Name: "Content-Type"
*c xConfiguration SIP Routes Route 2 Header Pattern: "application/tandberg-
phonebook\+xml"
*c xConfiguration SIP Routes Route 2 Authenticated: Off
*c xConfiguration SIP Routes Route 2 Address: "127.0.0.1"
*c xConfiguration SIP Routes Route 2 Port: 22400
*c xConfiguration SIP Routes Route 2 Transport: TCP
*c xConfiguration SIP Routes Route 2 Tag: "Phonebook"
*c xConfiguration SIP Registration Standard Refresh Strategy: Maximum
*c xConfiguration SIP Registration Standard Refresh Minimum: 45
*c xConfiguration SIP Registration Standard Refresh Maximum: 60
*c xConfiguration SIP Registration Outbound Refresh Strategy: Variable
*c xConfiguration SIP Registration Outbound Refresh Minimum: 300
```

*c xConfiguration SIP Registration Outbound Refresh Maximum: 3600
*c xConfiguration SIP Registration Outbound Flow Timer: 0
*c xConfiguration SIP Registration Proxy Mode: Off
*c xConfiguration SIP Registration Call Remove: No
*c xConfiguration SIP Session Refresh Value: 1800
*c xConfiguration SIP Session Refresh Minimum: 500
*c xConfiguration SIP UDP Mode: Off
*c xConfiguration SIP UDP Port: 5060
*c xConfiguration SIP TCP Mode: On
*c xConfiguration SIP TCP Port: 5060
*c xConfiguration SIP TCP Outbound Port Start: 25000
*c xConfiguration SIP TCP Outbound Port End: 29999
*c xConfiguration SIP TLS Mode: On
*c xConfiguration SIP TLS Port: 5061
*c xConfiguration SIP TLS Certificate Revocation Checking Mode: Off
*c xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On
*c xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On
*c xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch
Mode: On
*c xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility
Behavior: Fail
*c xConfiguration SIP Require UDP BFCP Mode: On
*c xConfiguration SIP Require Duo Video Mode: On
*c xConfiguration SIP Authentication Retry Limit: 3
*c xConfiguration SIP Authentication NTLM Mode: Auto
*c xConfiguration SIP Authentication NTLM SA Lifetime: 28800
*c xConfiguration SIP Authentication NTLM SA Limit: 10000
*c xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300
*c xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128
*c xConfiguration SIP Authentication Digest Nonce Limit: 10000
*c xConfiguration SIP Authentication Digest Nonce Length: 60
*c xConfiguration SIP GRUU Mode: On
*c xConfiguration SIP MediaRouting ICE Mode: Off
*c xConfiguration Interworking Mode: RegisteredOnly
*c xConfiguration Interworking Encryption Mode: Auto
*c xConfiguration Interworking Encryption Replay Protection Mode: Off
*c xConfiguration Interworking BFCP Compatibility Mode: Auto
*c xConfiguration Interworking Require Invite Header Mode: On
*c xConfiguration Traversal Media Port Start: 50000
*c xConfiguration Traversal Media Port End: 52399
*c xConfiguration Authentication UserName: ""
*c xConfiguration Authentication Password: "{cipher}XXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Authentication LDAP AliasOrigin: LDAP
*c xConfiguration Authentication ADS ADDomain: ""
*c xConfiguration Authentication ADS Workgroup: ""
*c xConfiguration Authentication ADS MachinePassword Refresh: On
*c xConfiguration Authentication ADS SPNEGO: Enabled
*c xConfiguration Authentication ADS SecureChannel: Auto
*c xConfiguration Authentication ADS Encryption: TLS
*c xConfiguration Authentication ADS Mode: Off
*c xConfiguration Authentication ADS Clockskew: 300
*c xConfiguration Zones Policy Mode: SearchRules
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "Local zone ? no domain"
*c xConfiguration Zones Policy SearchRules Rule 1 Description: "Search local
zone for H.323 devices (strip domain)"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: 48
*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 1 Mode: AliasPatternMatch
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Regex
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(.+
@#####.local.*"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Replace


```

*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "\1"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 1 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 2 Name: "Local zone ? full URI"
*c xConfiguration Zones Policy SearchRules Rule 2 Description: "Search local
zone for SIP and H.323 devices with a domain"
*c xConfiguration Zones Policy SearchRules Rule 2 Priority: 51
*c xConfiguration Zones Policy SearchRules Rule 2 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 2 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 2 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 2 Mode: AliasPatternMatch
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Type: Regex
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern String: "(.+
@#####.local.*"
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Behavior: Leave
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Replace: ""
*c xConfiguration Zones Policy SearchRules Rule 2 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 2 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 2 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 2 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Traversal zone search rule"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Search traversal
zone (Cisco VCS Expressway)"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: 100
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: AnyAlias
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "TraversalZone"
*c xConfiguration Zones Policy SearchRules Rule 3 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 4 Name: "External IP address
search rule"
*c xConfiguration Zones Policy SearchRules Rule 4 Description: "Route external
IP address"
*c xConfiguration Zones Policy SearchRules Rule 4 Priority: 100
*c xConfiguration Zones Policy SearchRules Rule 4 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 4 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 4 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 4 Mode: AnyIPAddress
*c xConfiguration Zones Policy SearchRules Rule 4 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 4 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 4 Target Name: "TraversalZone"
*c xConfiguration Zones Policy SearchRules Rule 4 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 5 Name: "LocalZoneMatch"
*c xConfiguration Zones Policy SearchRules Rule 5 Description: "Default rule:
queries the Local Zone for any alias"
*c xConfiguration Zones Policy SearchRules Rule 5 Priority: 50
*c xConfiguration Zones Policy SearchRules Rule 5 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 5 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 5 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 5 Mode: AnyAlias
*c xConfiguration Zones Policy SearchRules Rule 5 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 5 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 5 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 5 State: Enabled
*c xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials
*c xConfiguration Zones DefaultZone SIP Record Route Address Type: IP
*c xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off
*c xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto
*c xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto

```

```
*c xConfiguration Zones LocalZone DefaultSubZone Authentication Mode:
DoNotCheckCredentials
*c xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Unlimited
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode:
Unlimited
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode:
Unlimited
*c xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Unlimited
*c xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode:
Unlimited
*c xConfiguration Zones LocalZone SIP Record Route Address Type: IP
*c xConfiguration Zones Zone 1 Name: "TraversalZone"
*c xConfiguration Zones Zone 1 HopCount: 15
*c xConfiguration Zones Zone 1 H323 Mode: On
*c xConfiguration Zones Zone 1 SIP Mode: On
*c xConfiguration Zones Zone 1 Type: TraversalClient
*c xConfiguration Zones Zone 1 TraversalClient Authentication Mode: DoNot
CheckCredentials
*c xConfiguration Zones Zone 1 TraversalClient Authentication UserName:
"#####auth"
*c xConfiguration Zones Zone 1 TraversalClient Authentication Password:
"{cipher}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Zones Zone 1 TraversalClient Registrations: Allow
*c xConfiguration Zones Zone 1 TraversalClient H323 Protocol: Assent
*c xConfiguration Zones Zone 1 TraversalClient H323 Port: 6001
*c xConfiguration Zones Zone 1 TraversalClient SIP Protocol: Assent
*c xConfiguration Zones Zone 1 TraversalClient SIP Port: 7001
*c xConfiguration Zones Zone 1 TraversalClient SIP Transport: TLS
*c xConfiguration Zones Zone 1 TraversalClient SIP TLS Verify Mode: Off
*c xConfiguration Zones Zone 1 TraversalClient SIP Poison Mode: Off
*c xConfiguration Zones Zone 1 TraversalClient SIP Media Encryption Mode: Auto
*c xConfiguration Zones Zone 1 TraversalClient RetryInterval: 120
*c xConfiguration Zones Zone 1 TraversalClient Peer 1 Address: "10.10.10.102"
*c xConfiguration Zones Zone 1 TraversalClient Peer 2 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 3 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 4 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 5 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 6 Address: ""
*c xConfiguration Bandwidth Default: 384
*c xConfiguration Bandwidth Downspeed PerCall Mode: On
*c xConfiguration Bandwidth Downspeed Total Mode: On
*c xConfiguration Bandwidth Link 1 Name: "DefaultSZtoTraversalSZ"
*c xConfiguration Bandwidth Link 1 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 1 Node2 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 1 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 1 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 2 Name: "DefaultSZtoDefaultZ"
*c xConfiguration Bandwidth Link 2 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 2 Node2 Name: "DefaultZone"
*c xConfiguration Bandwidth Link 2 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 2 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 3 Name: "DefaultSZtoClusterSZ"
*c xConfiguration Bandwidth Link 3 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 3 Node2 Name: "ClusterSubZone"
*c xConfiguration Bandwidth Link 3 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 3 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 4 Name: "TraversalSZtoDefaultZ"
*c xConfiguration Bandwidth Link 4 Node1 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 4 Node2 Name: "DefaultZone"
*c xConfiguration Bandwidth Link 4 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 4 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 5 Name: "Zone001ToTraversalSZ"
*c xConfiguration Bandwidth Link 5 Node1 Name: "TraversalZone"
```

```

*c xConfiguration Bandwidth Link 5 Node2 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 5 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 5 Pipe2 Name: ""
*c xConfiguration Policy AdministratorPolicy Mode: Off
*c xConfiguration Policy AdministratorPolicy Service Protocol: HTTP
*c xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On
*c xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off
*c xConfiguration Policy AdministratorPolicy Service Server 1 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Server 2 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Server 3 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Path: ""
*c xConfiguration Policy AdministratorPolicy Service Status Path: "status"
*c xConfiguration Policy AdministratorPolicy Service UserName: ""
*c xConfiguration Policy AdministratorPolicy Service Password: "{cipher}
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject
status='504' reason='Admin Policy Unavailable'/>"
*c xConfiguration Policy FindMe Mode: Off
*c xConfiguration Policy FindMe CallerId: IncomingID
*c xConfiguration Policy FindMe UserDeviceRestriction: Off
*c xConfiguration Applications ConferenceFactory Mode: Off
*c xConfiguration Applications ConferenceFactory Alias: ""
*c xConfiguration Applications ConferenceFactory Template: ""
*c xConfiguration Applications ConferenceFactory Range Start: 1
*c xConfiguration Applications ConferenceFactory Range End: 65535
*c xConfiguration Applications OCS Relay Mode: Off
*c xConfiguration Applications OCS Relay OCS Domain: ""
*c xConfiguration Applications OCS Relay OCS Routing Prefix: "ocs"
*c xConfiguration Applications Presence Server Mode: Off
*c xConfiguration Applications Presence Server Publication ExpireDelta: 1800
*c xConfiguration Applications Presence Server Subscription ExpireDelta: 3600
*c xConfiguration Applications Presence User Agent Mode: Off
*c xConfiguration Applications Presence User Agent ExpireDelta: 3600
*c xConfiguration Applications Presence User Agent RetryDelta: 1800
*c xConfiguration Applications Presence User Agent Presentity Idle Status: Online
*c xConfiguration ResourceUsage Warning Activation Level: 90
*c xConfiguration Services AdvancedMediaGateway Zone Name: ""
*c xConfiguration Services AdvancedMediaGateway Policy Mode: Off

```

```

OK
exit
Bye!

```

Troubleshoot

Estos son los tres problemas más comunes que podría encontrar:

- **Se utiliza un cable serial incorrecto o defectuoso.** Asegúrese de utilizar el cable que viene con el dispositivo.
- **Se muestran caracteres irreconocibles en la pantalla de la consola.** Esto indica que la velocidad en baudios está configurada incorrectamente. Las velocidades en baudios se basan en múltiplos de dos, por lo que puede duplicar o reducir a la mitad el valor según sea necesario hasta que encuentre la configuración correcta. En este caso, la configuración correcta debe ser **115.200**.
- **No puede conectarse al software de emulación de terminal.** Además de los problemas de cableado, este problema suele deberse a uno de estos problemas:

Intenta conectarse a través de Telnet o SSH y debe cambiar el tipo de conexión a serial cuando utiliza una conexión serial.

Está en el puerto COM incorrecto. Para descubrir el puerto COM que utiliza su PC con conexiones seriales basadas en USB, navegue hasta **Panel de control > Administrador de dispositivos** y haga clic en **Puertos**. Desde esta ventana, puede verificar el puerto COM asignado a su dispositivo serial USB.

No tiene instalados los controladores para el dispositivo serial. Si este es el caso, debe localizarlos e instalarlos.

- **No puede ingresar SSH en el dispositivo.** Además de los problemas de cableado, este problema suele deberse a uno de estos problemas:

Intenta conectarse a través de SSH y no puede alcanzar el dispositivo debido a problemas de conectividad de red. Corrija el problema de conectividad de red. De manera alternativa, es posible que SSH no esté habilitado para el dispositivo. Web/HTTP/HTTPS en el dispositivo y asegúrese de que el acceso SSH esté habilitado en:

Configuration>SystemConfiguration>Network Services.

No tiene una clave Rivest-Shamir-Addleman (RSA) almacenada en caché desde el dispositivo. Normalmente se le solicita que acepte la clave RSA. Asegúrese de aceptar la clave.

El inicio de sesión no se ha realizado correctamente debido a que el nombre de usuario y la contraseña son incorrectos. Asegúrese de utilizar el nombre de usuario y la contraseña correctos para el dispositivo.