

- Cisco IOS, 1/2 af af a, la, sa, ca fca f a, maf IP a Sa, a 3 af ca f a, maf IPv6 a e, ta 1/4 ae S <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip>
- Cisco IOS, 1/2 af af a, la, sa, ca fca f a Secure Copy a a Sa a, ca e TM ae ta 1/4 a e, ta 1/4 ae S <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp>
- Cisco IOS, 1/2 af af a, la, sa, ca fca f a Session Initiation Protocol a a Sa a, Denial of Service (DoS) a e, ta 1/4 ae S <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip>
- Cisco IOS, 1/2 af af a, la, sa, ca fca f a Multiple Features Crafted TCP Sequence Vulnerability <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp>
- Cisco IOS, 1/2 af af a, la, sa, ca fca f a Multiple Features Crafted UDP Packet Vulnerability <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp>
- Cisco IOS, 1/2 af af a, la, sa, ca fca f a WebVPN a Sa, a 3 SSLVPN a e, ta 1/4 ae S <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn>

e 2 a 1/2 e f 1/2 a

e, ta 1/4 ae S a a, a, e f 1/2 a

e 2 a 1/2 a TM a, af af 1/4 a, af sa f a Cisco IOS, 1/2 af af a, a, sa, ca fca f a Sa, a 3 Cisco IOS XE, 1/2 af af a, a, sa, ca fca f a a Y e i e a a a | a, a, af ta f a, ma, 1 a a e Cisco IOS ta ... a sa i a a, a sa, e a a a e Y e f 1/2 a, a 1/2 a TM a, a, a ta e e a sa a, e a

- Airline Product Set (ALPS)
- Serial Tunnel Code (STUN) a Sa, a 3 Block Serial Tunnel Code (BSTUN)
- af a, maf ta a, e af a, af ca, ma, ca fca f a, maf a, a 1/4 af a, sa, ma, 1 a, ca fca f a, af ta, af a f (NCIA) a
- af ta f 1/4 a, a f a f a, a, 1 a, maf fa f a f a (DLSw)
- Remote Source-Route Bridging (RSRB)
- Point to Point Tunneling Protocol (PPTP)
- X.25 for Record Boundary Preservation (RBP)
- X.25 over TCP (XOT)

- X.25

```

#show version
Cisco IOS Software, C2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport

```

<#root>

Router#

show version

```

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

```

<output truncated>

```

#show version
Cisco

```

```

IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport

```

<#root>

Router#

show version

```

Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport

```

<output truncated>

Cisco

IOS, 1/2 f•ãfˆã, lã, šã, çãf•ãfˆãf1/4ã, 1ã®ã'1/2ã è | ã%õã ã®è; 1/2ã Š æf...ã ±ã ¯ã€ <http://www.cisco.com/ref.html> ®ã€ White Paper: Cisco IOS Reference Guideã€ã€šçç°èªã€ã€šã€ã€ã€¾ã€™ã€,

è, †ã1/4±ã€šã, 'ã«ã, "ã€šã, „ãªã, „ã"ã "ã€çç°èªã€ã€ã, €ã€ÿè1/2ã"€
æ¬ã®è£1/2ã"€ã€šã, ^ã³æ©ÿèf1/2ã«ã€è, †ã1/4±ã€šã€€ã~ãœ"ã—ãªã, „ã"ã"ã€çç°èªª

- Cisco IOS XR ã, 1/2 f•ãfˆã, lã, šã, ç
- BGPã€è²ã1/2"ã—ã¾ã>ã,"

Cisco

IOSã, 1/2 f•ãfˆã, lã, šã, çã†...ãšè"ã®šã•ã, €ã | ã, „ã, çã€ã€ã€ã€ã»ã€ã, ã, ã, ã³è£1/2ã"€ã, æ©ÿè

è³ç°

ã"ã®è, †ã1/4±ã€šã€ã, çæ£ã^ç"ã«ã^ãšÿã™ã, çã«ã¯ã€ã»¥ã, çã«æ! , èªã™ã, çæ

Airline Product Set (ALPS)

ALPSç"ã«è"ã®šã•ã, €ã€ÿãf†ãfã, çã, 1ã«ã€è, †ã1/4±ã€šã€€ã~ãœ"ã—ã¾ã™ã€, ALPS

alps local-peer <ip address>

ALPSã®è³ç°ã«ã€çã, „ã | ã¯ã€æ¬ã®ãfããf³ã, ¯ã«ã, ã, çã€ŽCisco IOS
Bridging and IBM Networking Configuration Guide, Release 12.2 - Configuring the Airline
Product

Setã€ã, ã, ç...šã—ã | ã€ã€ã€ã•ã, „ã, http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration

Serial Tunnel Code(STUN)ãšã, ^ã³Block Serial Tunneling(BSTUN)

STUNã¾ãÿã¯ãBSTUNã«è"ã®šã•ã, €ã€ÿãf†ãfã, çã, 1ã«ã€è, †ã1/4±ã€šã€€ã~ãœ"ã—ã

interface serial 0/0/0

encapsulation stun

æ¬;ã®ã¼ã¬ã€è,,tã¼±æ€šã®ã¬,ã,«BSTUNè¨ã®šã,'ç¬°ã—ã|ã¬,ã¾ã™ã€,

```
interface serial 0/0/0
encapsulation bstun
```

STUNãšã,^ã³BSTUNã®è©³ç°ã«ã¬ã¬,ã¬|ã¬¬ã€æ¬;ã®ãfãf³ã, http://www.cisco.com/en/US/docs/ios/bridging_and_ibm_networking_configuration_guide/configuration/serial_tunnel_and_block_serial_tunnel.html,
IOS Bridging and IBM Networking Configuration Guide, Release 12.2 - Configuring Serial Tunnel and Block Serial Tunnelã€ã,ã,ç...šã—ã|ã¬ã¬ã¬ã¬,ã€,

ãfã,ãftã,£ãf-ã,¬ãf©ã,ã,çãf³ãf^ã,ãf³ã,¿ãf¼ãf•ã,šã,ã,¹ã,çãf¼ã,ãftã,¬ãfãf³ã

NCIAã®è¨ã®šã•ã,CEã¬|ã¬,ã,«ãfãfãfã,ã,¹ã¬ã€ã½¿ç"ã™ã,«ãÿç,ã¬ã,«ãf^ãf©ãf³ã

```
ncia server 1 10.66.91.138 0000.1111.2222 2222.2222.2222 1
```

NCIAã®è©³ç°ã«ã¬ã¬,ã¬|ã¬¬ã€æ¬;ã®ãfãf³ã,¬ã«ã¬,ã,ã€ŽCisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 - Configuring NCIA Client/Serverã€ã,ã,ç...šã—ã|ã¬ã¬ã¬ã¬ã¬,ã€,http://www.cisco.com/en/US/docs/ios/bridging_and_ibm_networking_configuration_guide/configuration/ncia_client_server.html

ãf¼ãf,¿ãfãf³ã,¬ã,¹ã,ããfãfãfãf³ã,°(DLSw)

DLSwç"ã«è¨ã®šã•ã,CEã¬ãfãfãfãfã,ã,¹ã«ã¬¬è,,tã¼±æ€šã®èã~ãœ¨ã—ã¾ã™ã€,DSLW

```
dlsw local-peer peer-id <ip address>
```

FSTã,«ãf—ã,»ãf«ãCE-ã¾ã¬ã¬Directã,«ãf—ã,»ãf«ãCE-ã®è¨ã®šã•ã,CEã¬ãfãfãfãfã,ã,¹ã¬ã

local-peer peer-id ip

addressã€ã,³ãfžãf³ãf%ãšé-ã¬ã,CEã,«ã¬ã¬,ã€ã¾ã¬ç,,¶ã¬ã—ã|è,,tã¼±ãšã™ã€,

DLSwã®è©³ç°ã«ã¬ã¬,ã¬|ã¬¬ã€æ¬;ã®ãfãf³ã,¬ã«ã¬,ã,ã€ŽCisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 - Configuring Data-Link Switching

Plusã€ã,ã,ç...šã—ã|ã¬ã¬ã¬ã¬ã¬,ã€,http://www.cisco.com/en/US/docs/ios/bridging_and_ibm_networking_configuration_guide/configuration/dlsw.html

PPTP Cisco IOS VPDN Configuration Guide, Release 12.4 - Configuring Client-Initiated Dial-In VPDN Tunneling http://www.cisco.com/en/US/docs/ios/vpdn/configuration_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1105140

X.25 Record Boundary Preservation(RBP)

RBP `port`

`port_number` Virtual Circuit

```
interface Serial1/0
  x25 map rbp 1111 local port <port_number>
```

Permanent Virtual Circuit

```
interface Serial1/0
  x25 map pvc <pvc_number> rbp local port <port_number>
```

RBP Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - X.25 Record Boundary Preservation for Data Communications Networks <http://www.cisco.com/en/US/docs/ios/wan/configuration>

X.25 over TCP(XOT)

XOT

```
xot access-group 1
and a corresponding access-list 1.
```

XOT Cisco IOS Wide-

Profiles, <http://www.cisco.com/en/US/docs/ios/wan/configuration>

X.25 over TCP

X.25 over TCP, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

x25 routing

X.25 over TCP, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and

LAPB, <http://www.cisco.com/en/US/docs/ios/wan/configuration/>

Cisco Bug ID [CSCsr29468](#)

Common Vulnerabilities and Exposures (CVE) ID CVE-2009-

0629, Cisco Bug ID [CSCsr29468](#)

Access Control Lists (ACLs)

IOS, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

Access Control Lists (ACLs), Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

Access Control Lists (ACLs), Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

Access Control Lists (ACLs)

Access Control Lists (ACLs), Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

Access Control Lists (ACLs), Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

Access Control Lists (ACLs), Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB

!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: ALPS

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 350
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 10000
```

!---

*!--- Deny ALPS TCP traffic from all other sources destined
!--- to infrastructure addresses.*

!---

```
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 350
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 10000
```

!---

!--- Feature: STUN

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1994
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1990 1992
```

!---

*!--- Deny STUN TCP traffic from all other sources destined
!--- to infrastructure addresses.*

!---

```
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1994
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1990 1992
```

!---

!--- Feature: BSTUN

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1963
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1976 1979
```

!---

*!--- Deny BSTUN TCP traffic from all other sources destined
!--- to infrastructure addresses.*

!---

```
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1963
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1976 1979
```

```
!---
!--- Feature: NCIA
!---
```

```
!---
!--- Leverage the underlying protocols, DLSw, RSRB, etc.
!---
```

```
!---
!--- Feature: DLSW
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 2065
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 2067
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1981 1983
```

```
!---
!--- Deny DLSW TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 2065
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 2067
access-list 150 deny tcp any
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1981 1983
```

```
!---
!--- Feature: RSRB
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD range 1987 1989
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1996
```

```
!---
!--- Deny RSRB TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
```

```
INFRASTRUCTURE_ADDRESSES WILDCARD range 1987 1989
access-list 150 deny tcp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1996
```

```
!---
!--- Feature: PPTP
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1723
```

```
!---
!--- Deny PPTP TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1723
```

```
!---
!--- Feature: RBP
!---
!--- RBP will listen for TCP connections on the configured port
!--- as per "local port
```

```
    ". The following example
!--- uses port 1055
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1055
```

```
!---
!--- Deny RBP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1055
```

```
!---
!--- Feature: XOT and X.25 Routing
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1998
```

```
!----
!--- Deny XOT and X25 TCP traffic from all other sources
!--- destined to infrastructure addresses.
!----
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1998
```

```
!----
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations Permit all other traffic to transit the
!--- device.
!----
```

```
access-list 150 permit ip any any
```

```
!----
!--- Apply access-list to all interfaces (only one example
!--- shown)
!----
```

```
interface serial 2/0
    ip access-group 150 in
```

Protecting Your Core: Infrastructure Protection Access Control

Lists http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

ACL(rACL)

Cisco 12000

(GSR) Cisco 7500

Cisco 10720 Cisco 120(31)S IOS

Receive ACL

ACL

ACL

ACL

ACL

12000, 7500, 10720 Receive ACL

ACL

IP any

ACL

ACL

ACL

Your Core: Infrastructure Protection Access Control

ACL

ACL

ACL

!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---

!---
!--- Permit ALPS traffic from trusted hosts allowed to the RP.
!---

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 350
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 10000

!---
!--- Deny ALPS traffic from all other sources to the RP.
!---

access-list 150 deny tcp any any eq 350
access-list 150 deny tcp any any eq 10000

!---
!--- Permit STUN traffic from trusted hosts allowed to the RP.
!---

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 1994
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any range 1990 1992

!---
!--- Deny STUN traffic from all other sources to the RP.
!---

```
access-list 150 deny tcp any any eq 1994
access-list 150 deny tcp any any eq range 1990 1992
```

```
!---
!--- Permit BSTUN traffic from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 1963
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1976 1979
```

```
!---
!--- Deny BSTUN traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1963
access-list 150 deny tcp any any eq range 1976 1979
```

```
!---
!--- Permit DLSw from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2065
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2067
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1981 1983
```

```
!---
!--- Deny DLSw all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 2065
access-list 150 deny tcp any any eq 2067
access-list 150 deny tcp any any range 1981 1983
```

```
!---
!--- Permit RSRB traffic from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 1996
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1987 1989
```

```
!---
!--- Deny RSRB traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1996
access-list 150 deny tcp any any range 1987 1989
```

```
!---
!--- Permit PPTP traffic from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 1723
```

```
!---
!--- Deny PPTP traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1723
```

```
!---
!--- Permit RBP traffic from trusted hosts allowed to the RP.
!--- RBP will listen for TCP connections on the configured port
!--- as per "local port
```

```
        ". The following example
!--- uses port 1055
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 1055
```

```
!---
!--- Deny RBP traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1055
```

```
!---
!--- Permit XOT and X.25 Routing traffic from trusted hosts allowed
!--- to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 1998
```

```
!---
```

```
!--- Deny XOT and X.25 Routing traffic from all other sources to
!--- the RP.
!---
```

```
access-list 150 deny tcp any any eq 1998
```

```
!--- Permit all other traffic to the RP.
!--- according to security policy and configurations.
```

```
access-list 150 permit ip any any
```

```
!--- Apply this access list to the 'receive' path.
```

```
ip receive access-list 150
```

ã,³ãf³ãf^ãfãf¼ãf«ãf—ãf~ãf¼ãf³ãfãfã,ãf³ã,°

ã,³ãf³ãf^ãfãf¼ãf«ãf—ãf~ãf¼ãf³ãfãfã,ãf³ã,°(CoPP)ã,'ã½çç'''ã—ã|ã€ã½±éÿã,'ã—ã'ã,æ©
IOS ã,½ãf•ãf^ã,|ã,šã,çãfãfãf¼ã,¹
12.0Sã€12.2SXã€12.2Sã€12.3Tã€12.4ã€ãŠã,^ã³ 12.4Tã—ã€CoPP
æ©ÿèf½ã,'ã,µãfãf¼ãf^ã—ã|ã,,ã¾ã™ã€,ç®;ç®tãŠã,^ã³ã,³ãf³ãf^ãfãf¼ãf«ãf—ãf~ãf¼ã
CoPP
ã,'æ©ÿã™''ã«è''ã®šã—ã€æ—çã~ã®ã,»ã,ãfãfãfãfã,£ãf¼ãfãfã,ãf¼ã''ã,³ãf³ãf•ã,£ã,®ãf

```
!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: ALPS
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 350
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 10000
```

```
!---
!--- Permit ALPS traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any eq 350
access-list 150 permit tcp any any eq 10000
```



```
!---  
!--- Feature: STUN  
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
    any eq 1994  
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
    any range 1990 1992
```

```
!---  
!--- Permit STUN traffic sent to all IP addresses  
!--- configured on all interfaces of the affected device so  
!--- that it will be policed and dropped by the CoPP feature  
!---
```

```
access-list 150 permit tcp any any eq 1994  
access-list 150 permit tcp any any range 1990 1992
```

```
!---  
!--- Feature: BSTUN  
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
    any eq 1963  
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
    any range 1976 1979
```

```
!---  
!--- Permit BSTUN traffic sent to all IP addresses  
!--- configured on all interfaces of the affected device so  
!--- that it will be policed and dropped by the CoPP feature  
!---
```

```
access-list 150 permit tcp any any eq 1963  
access-list 150 permit tcp any any range 1976 1979
```

```
!---  
!--- Feature: NCIA  
!---  
!--- Leverage the underlying protocols, DLSw, RSRB, etc.  
!---
```

```
!---  
!--- Feature: DLSW  
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
    any eq 2065  
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
```

```
any eq 2067
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
any range 1981 1983
```

```
!---
!--- Permit DLSW traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any eq 2065
access-list 150 permit tcp any any eq 2067
access-list 150 permit tcp any any range 1981 1983
```

```
!---
!--- Feature: RSRB
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
any range 1987 1989
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
any eq 1996
```

```
!---
!--- Permit RSRB traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any range 1987 1989
access-list 150 permit tcp any any eq 1996
```

```
!---
!--- Feature: PPTP
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
any eq 1723
```

```
!---
!--- Permit PPTP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any eq 1723
```

```
!---
!--- Feature: RBP
```

```
!---
!--- RBP will listen for TCP connections on the configured port
!--- as per "local port
```

```
    ". The following example
!--- uses port 1055
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1055
```

```
!---
!--- Permit RBP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any eq 1055
```

```
!---
!--- Feature: XOT and X.25 Routing
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1998
```

```
!---
!--- Permit XOT and X25 traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature
!---
```

```
access-list 150 permit tcp any any eq 1998
```

```
!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- configurations for traffic that is authorized to be sent
!--- and to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
!---
```

```
class-map match-all drop-tcp-class
    match access-group 150
```

```
!---
```

```
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!---
```

```
policy-map drop-tcp-traffic
class drop-tcp-class
drop
```

```
!---
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
!---
```

```
control-plane
service-policy input drop-tcp-traffic
```

CoPP CoPP "permit"
ACE (ACE)
policy-
map "drop" deny"
policy-
map "drop" deny
Cisco IOS
:

```
policy-map drop-tcp-traffic
class drop-tcp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

CoPP
Plane Policing Implementation Best Practices
Cisco IOS Software Releases
12.2 S - Control Plane

Policing <http://www.cisco.com/web/about/security/intelligence>

Applied Mitigation

Bulletin <https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-tcp-and-ip>

ä;®æ£æ, ^ã;ã, 1/2ãf•ãf^ã, |ã, šã, ç

ã, çäffäf—ã, °äf-äf¼äf%ã, 'æœèèZä™ã, <ã 'ã^ã-ã€<http://www.cisco.com/go/psirt>

ã "ã¼Cç¶šã®ã, çäf%ãäfã, ðã, ¶äfã, „ã, ç...šã—ã | ä€ããé: Cä®èš£æ±ºçš¶äã "ã
ã, ½äfãäf¼ã, .äfšäfã, 'çç°èã—ã | ääãããäã, „ã€,

ã„ãšã, Cä®ã 'ã^ã, „ã€ã, çäffäf—ã, °äf-äf¼äf%ã™ã, <æ©Yä™ã «ããã^täãäfjãfcãfãä
Technical Assistance

Centeri¼^TACi¼%ã¾ãYä-ã¥ç', „ã, çmuã, „ãšãã, „ã, <äfjãfãftãfšãfã,¹
äf—äfäfã, ðäfäf¼ã «ãšããã, „ã^ããããããããããã, „ã€,

Cisco IOS ä, ½äfããfã, lä, šã, çã®è: i¼^ä, <æž²i¼%ã®ã„è:Cä®äã-ã€ Cisco IOS
ã®äfããfãã,¹

äfãf-ã, ðäfããCè~è¼%ãã, Cä®ã | ä, „ã¾ã™ã€, ç%ã¹ã®šã®äfããfãã,¹
äfãf-ã, ðäfãã «è, ðã¼±æ€šãCä®, ä, <ã^ã-ã€ä:®æ£ã, 'ã «ã, €æœ€ã^ã®äfããfãã,¹i¼%
1

ä:®æ£æ, ^ããäfããfãã,¹ã€ã^—ã «è~è¼%ãã, Cä®¾ã™ã€, ä€Cäž"ã¥ãfããfãã,¹ã€ã^
1
ä:®æ£æ, ^ããäfããfãã,¹ã, ^ã, šããã, i¼%ããfãf-ã, ðäfãã «ã «ã¾ã, Cä®, <äfããfãã,¹ã Cç"¼ã

äfã, äfããfãã
äfããfããã,¹

Affected 12.0-Based Releases First Fixed Releasei¼^ä:®æ£ãã, Cä®Yæœ€ã^ãã®äfããfããã,¹i¼%
è©²ã½"ã™ã, < 12.0 äfããfãã,¹ãã®äfããfããã,¹ã-ã, ä, šã¾ããã, „ã€,

Affected 12.1-Based Releases First Fixed Releasei¼^ä:®æ£ãã, Cä®Yæœ€ã^ãã®äfããfããã,¹i¼%
è©²ã½"ã™ã, < 12.1 äfããfãã,¹ãã®äfããfããã,¹ã-ã, ä, šã¾ããã, „ã€,

Affected 12.2-Based Releases First Fixed Releasei¼^ä:®æ£ãã, Cä®Yæœ€ã^ãã®äfããfããã,¹i¼%
è©²ã½"ã™ã, < 12.1 äfããfãã,¹ãã®äfããfããã,¹ã-ã, ä, šã¾ããã, „ã€,

12.2	è,,†å¼±æ€§ãªã—
12.2B	è,,†å¼±æ€§ãªã—
12.2BC	è,,†å¼±æ€§ãªã—
12.2BW	è,,†å¼±æ€§ãªã—
12.2BX	è,,†å¼±æ€§ãªã—
12.2BY	è,,†å¼±æ€§ãªã—
12.2BZ	è,,†å¼±æ€§ãªã—
12.2CX	è,,†å¼±æ€§ãªã—
12.2CY	è,,†å¼±æ€§ãªã—
12.2CZ	è,,†å¼±æ€§ãªã—
12.2DA	è,,†å¼±æ€§ãªã—
12.2DD	è,,†å¼±æ€§ãªã—
12.2DX	è,,†å¼±æ€§ãªã—
12.2EW	è,,†å¼±æ€§ãªã,Š(æœ€å^ªãª®ä¿®æĚã— 12.2SG)
12.2EWA	è,,†å¼±æ€§ãªã,Š(æœ€å^ªãª®ä¿®æĚã— 12.2SG)

12.2EX	12.2(44)EXã, ã, Šã%o ðã ð @ãfããfããfãã, ã ð «ã ð è,, ðã¼±æ€Šã ð Æã ð, ã, Šã€ ð 12.2(44)EXã
12.2EY	12.2(44)EY
12.2EZ	è,, ðã¼±æ€Šã ð, ã, Šã€ ð æœ€ã^ ð ã ð @ã¼@æfã ð 12.2SE
12.2FX	è,, ðã¼±æ€Šã ð ã ð —
12.2FY	è,, ðã¼±æ€Šã ð ã ð —
12.2FZ	è,, ðã¼±æ€Šã ð, ã, Šã€ ð æœ€ã^ ð ã ð @ã¼@æfã ð 12.2SE
12.2IRA	è,, ðã¼±æ€Šã ð, ã, Š(æœ€ã^ ð ã ð @ã¼@æfã ð 12.2SRC
12.2IRB	è,, ðã¼±æ€Šã ð, ã, Š(æœ€ã^ ð ã ð @ã¼@æfã ð 12.2SRC
12.2IXA	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXB	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXC	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXD	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXE	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXF	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ
12.2IXG	è,, ðã¼±æ€Šã ð, ã, Šã€, 12.2IXHã ð @ã»»æ,, ð ã ð @ãfããfããfãã, ã ð «çš»è;Æ

12.2JA	è,,†à¼±æ€§ãªã—
12.2JK	è,,†à¼±æ€§ãªã—
12.2MB	è,,†à¼±æ€§ãªã—
12.2MC	è,,†à¼±æ€§ãªã—
12.2S	è,,†à¼±æ€§ãª,Šã€æœ€å^ãª®ä¿®æfã— 12.2SB
12.2SB	12.2(33)SB3 12.2(28)SB13 12.2(31)SB14
12.2SBC	è,,†à¼±æ€§ãª,Šã€æœ€å^ãª®ä¿®æfã— 12.2SB
12.2SCA	è,,†à¼±æ€§ãª,Š(æœ€å^ãª®ä¿®æfã— 12.2SCB)
12.2SCB	12.2(33)SCB1
12.2SE	12.2(46)SE2 12.2(50)SE 12.2(44)SE5
12.2SEA	è,,†à¼±æ€§ãª,Šã€æœ€å^ãª®ä¿®æfã— 12.2SE
12.2SEB	è,,†à¼±æ€§ãª,Šã€æœ€å^ãª®ä¿®æfã— 12.2SE
12.2SEC	è,,†à¼±æ€§ãª,Šã€æœ€å^ãª®ä¿®æfã— 12.2SE

12.2SED	è,,†å¼±æ€ššã,ã,Šã€æœ€å^ã®ä¿®æ£ã 12.2SE
12.2SEE	è,,†å¼±æ€ššã,ã,Šã€æœ€å^ã®ä¿®æ£ã 12.2SE
12.2SEF	è,,†å¼±æ€ššãã—
12.2SEG	12.2(25)SEG4ã,^ã,Šã%ã®ãf^ãf^ãf^ã,1ã«ãè,,†å¼±æ€ššã€ã,ã,Šã€12.2(25)S
12.2SG	12.2(50)SG
12.2SGA	12.2(31)SGA9
12.2SL	è,,†å¼±æ€ššãã—
12.2SM	è,,†å¼±æ€ššã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããã•ã„
12.2SO	è,,†å¼±æ€ššã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããããã•ã„
12.2SQ	è,,†å¼±æ€ššãã—
12.2SRA	è,,†å¼±æ€ššã,ã,Š(æœ€å^ã®ä¿®æ£ã 12.2SRC
12.2SRB	è,,†å¼±æ€ššã,ã,Š(æœ€å^ã®ä¿®æ£ã 12.2SRC
12.2SRC	12.2(33)SRC3

12.2SRD	12.2(33)SRD1
12.2STE	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããã•ã„
12.2SU	è,†â¼±æ€§ãã—
12.2SV	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ãããããã•ã„
12.2SVA	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããããã•ã„
12.2SVC	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããããã•ã„
12.2SVD	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããããã•ã„
12.2SVE	è,†â¼±æ€§ã,ã,Šã€,TACã«ãŠã•ã„ã^ã,ã>ããããããã•ã„
12.2SW	è,†â¼±æ€§ã,ã,Šã€,12.4SWã®ä»æ„ã®ãfãfãf¼ã,1ã«çš»è¡E
12.2SX	è,†â¼±æ€§ãã—
12.2SXA	è,†â¼±æ€§ãã—
12.2SXB	è,†â¼±æ€§ãã—
12.2SXD	è,†â¼±æ€§ã,ã,Š(æœƒã^ã®ä¿®æfã 12.2SXF)
12.2SXE	è,†â¼±æ€§ã,ã,Š(æœƒã^ã®ä¿®æfã 12.2SXF)
12.2SXF	12.2(18)SXF16

12.2SXH	12.2(33)SXH5
12.2SXI	12.2(33)SXI1
12.2SY	è,,†â¼±æ€§ãª—
12.2SZ	è,,†â¼±æ€§ãª,Šã€æœ€â^ªãª®ä¿®æfãª 12.2SB
12.2T	è,,†â¼±æ€§ãªª—
12.2TPC	è,,†â¼±æ€§ãªª—
12.2XA	è,,†â¼±æ€§ãªª—
12.2XB	è,,†â¼±æ€§ãªª—
12.2XC	è,,†â¼±æ€§ãªª—
12.2XD	è,,†â¼±æ€§ãªª—
12.2XE	è,,†â¼±æ€§ãªª—
12.2XF	è,,†â¼±æ€§ãªª—
12.2XG	è,,†â¼±æ€§ãªª—
12.2XH	è,,†â¼±æ€§ãªª—
12.2XI	è,,†â¼±æ€§ãªª—

12.2XJ	è,,†â¼±æ€§ãªã—
12.2XK	è,,†â¼±æ€§ãªã—
12.2XL	è,,†â¼±æ€§ãªã—
12.2XM	è,,†â¼±æ€§ãªã—
12.2XN	è,,†â¼±æ€§ãª,Š(æœƒâ^ªª®ä¿®æƒã— 12.2SRC
12.2XNA	è,,†â¼±æ€§ãª,Šã€æœƒâ^ªª®ä¿®æƒã— 12.2SRD
12.2XNB	12.2(33)XNB1
12.2XNC	è,,†â¼±æ€§ãªªã—
12.2XO	12.2(46)XO
12.2XQ	è,,†â¼±æ€§ãªªã—
12.2XR	è,,†â¼±æ€§ãªªã—
12.2XS	è,,†â¼±æ€§ãªªã—
12.2XT	è,,†â¼±æ€§ãªªã—
12.2XU	è,,†â¼±æ€§ãªªã—

12.2XV	è,,†å¼±æ€§ãªãª—
12.2XW	è,,†å¼±æ€§ãªãª—
12.2YA	è,,†å¼±æ€§ãªãª—
12.2YB	è,,†å¼±æ€§ãªãª—
12.2YC	è,,†å¼±æ€§ãªãª—
12.2YD	è,,†å¼±æ€§ãªãª—
12.2YE	è,,†å¼±æ€§ãªãª—
12.2YF	è,,†å¼±æ€§ãªãª—
12.2YG	è,,†å¼±æ€§ãªãª—
12.2YH	è,,†å¼±æ€§ãªãª—
12.2YJ	è,,†å¼±æ€§ãªãª—
12.2YK	è,,†å¼±æ€§ãªãª—
12.2YL	è,,†å¼±æ€§ãªãª—
12.2YM	è,,†å¼±æ€§ãªãª—
12.2YN	è,,†å¼±æ€§ãªãª—

12.2YO	è,,†â¼±æ€§ãªã—
12.2YP	è,,†â¼±æ€§ãªã—
12.2YQ	è,,†â¼±æ€§ãªã—
12.2YR	è,,†â¼±æ€§ãªã—
12.2YS	è,,†â¼±æ€§ãªã—
12.2YT	è,,†â¼±æ€§ãªã—
12.2YU	è,,†â¼±æ€§ãªã—
12.2YV	è,,†â¼±æ€§ãªã—
12.2YW	è,,†â¼±æ€§ãªã—
12.2YX	è,,†â¼±æ€§ãªã—
12.2YY	è,,†â¼±æ€§ãªã—
12.2YZ	è,,†â¼±æ€§ãªã—
12.2ZA	è,,†â¼±æ€§ãªã—
12.2ZB	è,,†â¼±æ€§ãªã—
12.2ZC	è,,†â¼±æ€§ãªã—

Affected 12.4-Based Releases	First Fixed Release
12.4	12.4(15)MD2
12.4JA	12.4(11)MD6a, ^ã, Šã% @ãfãfãfãfã, 1ã «ã è,,tã¼±æ€šãĀãã12.4(1
12.4JDA	12.4(19)MR1
12.4JK	12.4(16)MR2ã, ^ã, Šã% @ãfãfãfãfã, 1ã «ã è,,tã¼±æ€šãĀããã12.4(1
12.4JL	12.4(22)T
12.4JMA	
12.4JMB	
12.4JX	
12.4MD	12.4(15)MD2 12.4(11)MD6a, ^ã, Šã% @ãfãfãfãfã, 1ã «ã è,,tã¼±æ€šãĀããã12.4(1
12.4MR	12.4(19)MR1 12.4(16)MR2ã, ^ã, Šã% @ãfãfãfãfã, 1ã «ã è,,tã¼±æ€šãĀããã12.4(1
12.4SW	
12.4T	12.4(22)T

æ”1è”à±¥æ´

ãf³ãf“ã,ãfšãf³ 1.2	2009å¹7æœ^6æ—¥	ã,½ãf•ãf^ã,lã,šã,çãⓂæⓂä³⁄é-ãš<æ—¥ã«é-çã™ã,«è”~è¿°ã
ãf³ãf“ã,ãfšãf³ 1.1	2009å¹6æœ^26æ—¥	2009å¹3æœ^ãⓂä¿Ⓜæ£æ,^ã¿ã,½ãf•ãf^ã, ã,šã,çã†ãf¼ãf-ãf«ã
ãf³ãf“ã,ãfšãf³ 1.0	2009å¹3æœ^25æ—¥	ã¿ç%ã^ãf³ãf³ãf¼ã,¹

ã^©ç””è!ç´,,

æœ-ã,çãf%ãfã,ã,ã,ãf³ãç,,jã¿è”¼ãⓂã,,ãⓂã”ã—ã|ã”æⓂⓂä³⁄ã—ã|ãšã,šã
æœ-ã,çãf%ãfã,ã,ã,ãf³ãⓂæf...ã±ãšã,^ã³ãf³ãf³ã,ãⓂã½¿ç””ã«é-çã™ã,«è²-ã»ãⓂã,€
ã³⁄ãÿã€ã,ã,¹ã,³ãæœ-ãf%ãã,ãfãfjãf³ãf^ãⓂã†...ã¹ã,'ã^ãšããã—ã«ã%æ’ã—ã
æœ-ã,çãf%ãfã,ã,ã,ãf³ãⓂè”~è¿°ã†...ã¹ã«é-çã—ã|æf...ã±é...ã¿jãⓂ URL
ã,'çœçç•¥ã—ã€ãã¿ç<-ãⓂè»çè¼%ã,,æ,,è”³ã,'æ-½ã—ãÿã'ã^ã€ã½”ç³⁄ã€çç|çç
ã”ãⓂãf%ãã,ãfãfjãf³ãf^ãⓂæf...ã±ãæœ-ã,ã,¹ã,³è£½ã”ãⓂã,ãf³ãf%ããf!ãf¼ã,ã,ã³⁄è±j

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。