APPENDIX A

Sample Configurations

These sample configurations are provided as general templates for initial configuration guidance. Each feature and command should be reviewed, tested and possibly revised according to the particular platform, software version and network architecture on which they are being deployed.

Sample TTY Ports Configuration

AUX Port

```
! AUX port access not required and access disabled
line aux 0
login
no password
!
```

Console Port

```
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
aaa authentication login <authen-exec-list> group <adminAAAgroup> local-case
aaa authentication enable default group tacacs-group enable
aaa accounting exec <account-exec-list>  start-stop group <adminAAAgroup>
!
line con 0
 accounting exec <account-exec-list>
 login authentication <authen-exec-list>
!
! Local incoming access only
 transport input none
!
! Incoming access not permitted if the request does not specify the transport protocol
 transport preferred none
!
! No outgoing connections permitted
 transport output none
!
! Idle timeout of 3 minutes
 session-timeout 3
!
! EXEC timeout of 10 minutes
```

```
 exec-timeout 10 0
!
```

Sample VTY Lines Configuration

Sample Telnet Configuration

```
! Prevent hung sessions in case of a remote system crash
service tcp-keepalives-in
!
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
aaa authentication login <authen-exec-list> group <adminAAAgroup> local-case
aaa authentication enable default group tacacs-group enable
aaa authorization exec <author-exec-list> group tacacs-group if-authenticated
aaa accounting exec <account-exec-list>  start-stop group <adminAAAgroup>
!
access-list <xACL#> remark ACL for Telnet
access-list <xACL#> permit tcp <NOCsubnet1> <inverse-mask> any eq 23
access-list <xACL#> permit tcp <NOCsubnet2> <inverse-mask> any eq 23
access-list <xACL#> deny ip any any log-input
!
```

Note that in access-class ACLs, destination should be any, and not a particular IP address of the router. If a specific host IP address is used, packets won't match the ACE.

```
line vty 0 4
! Allow access from trusted hosts
 access-class <xACL#> in
!
! Incoming access via telnet only
 transport input telnet
!
 authorization exec <author-exec-list>
 accounting exec <account-exec-list>
 login authentication <authen-exec-list>
!
! No outgoing connections permitted
 transport output none
!
! Incoming access not permitted if the request does not specify the transport protocol
 transport preferred none
!
! Idle timeout of 3 minutes
 session-timeout 3
!
! EXEC timeout of 10 minutes
 exec-timeout 10 0
!
```

Sample SSH Configuration

```
! Prevent hung sessions in case of a remote system crash
service tcp-keepalives-in
!
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
aaa authentication login <authen-exec-list> group <adminAAAgroup> local-case
aaa authentication enable default group tacacs-group enable
aaa authorization exec <author-exec-list> group tacacs-group if-authenticated
aaa accounting exec <account-exec-list>  start-stop group <adminAAAgroup>
!
access-list <xACL#> remark ACL for SSH
access-list <xACL#> permit tcp <NOCsubnet1> <inverse-mask> any eq 22
access-list <xACL#> permit tcp <NOCsubnet2> <inverse-mask> any eq 22
access-list <xACL#> deny ip any any log-input
!
crypto key generate rsa
! (after entering command, follow the series of prompts)
!
! SSH negotiation timeout of 30 seconds
ip ssh timeout 30
!
! SSH authentication attempts of 2 before an interface reset
ip ssh authentication-retries 2
!
line vty 0 4
 access-class <xACL#> in
!
! Incoming access via SSH only
 transport input ssh
!
 authorization exec <author-exec-list>
 accounting exec <account-exec-list>
 login authentication <authen-exec-list>
!
! No outgoing connections permitted
 transport output none
!
! Incoming access not permitted if the request does not specify the transport protocol
 transport preferred none
!
! Idle timeout of 3 minutes
 session-timeout 3
!
! EXEC timeout of 10 minutes
 exec-timeout 10 0
!
```

Sample Legal Banner Notification Configuration

```
! Present a legal notification banner approved by company legal counsel
banner login #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or
criminal penalties.
All activities performed on this device are logged and monitored.
#
```

```
!
```

Sample AAA Services Configuration

```
! Enable AAA
aaa new-model
!
! Define the AAA servers
! If using TACACS+ servers, define the servers, the key to be used for each specific
server
!(rather than a global key) and enable the option to maintain a session to the server for
more
! efficient communication
! Note: The keys must match that entered for this device on the TACACS+ servers and should
follow
! general password policy guidelines (e.g. be at least 16 characters long)
!
tacacs-server host <TAC+server1> key <TAC+key1> single-connection
tacacs-server host <TAC+server2> key <TAC+key2> single-connection
!
! If using RADIUS servers, define the server, non-standard ports and the key to be used
for each ! server (rather than a global key).
! Note: The keys must match that entered for this device on the RADIUS servers and should
follow general password policy guidelines (e.g. be at least 16 characters long)
!
radius-server host <RADserver1> auth-port <port#> acct-port <port#> key <RADkey1>
radius-server host <RADserver2> auth-port <port#> acct-port <port#> key <RADkey1>
!
! Define a AAA group to be used to authenticate device access. Here the servers are
TACACS+
! servers
!
aaa group server tacacs+ <adminAAAgroup>
 server <TAC+server1>
 server <TAC+server2>
!
! This example shows how to define a group of RADIUS servers.
aaa group server radius <adminAAAgroup>
 server <RADIUSserver1>
 server <RADIUSserver2>
!
```

Note Be careful! This should apply to OOB interface. In addition, these ACLs have source and dest inversed.

```
! If using RADIUs, send the attribute 'Service-Type' in authentication requests to enable
the AAA server to only authorize device access to administrative users. This is
particularly important to implement if the same AAA server is being used for both
administrative and service users. The 'Service-Type' attribute is set to '1' for login
access.
radius-server attribute 6 on-for-login-auth
!
! Enable support for RADIUS VSAs for both authentication and accounting
radius-server vsa send authentication
radius-server vsa send accounting
!
! Set the global default setting for the time (in seconds) to wait before re-attempting a
request, e.g. 1 second.
! Note: The timeout may be defined on an individual TACACS+ server basis as part of the
'tacacs-server host' definition. An individual server-defined setting takes priority over
the global setting.
```

```
tacacs-server timeout 5
!
! Note: The timeout may be defined on an individual RADIUS server basis as part of the
'radius-server host' definition. An individual server-defined setting takes priority over
the global setting.
radius-server timeout 5
!
! Set the global default setting for the number of times, e.g. 0, to re-attempt a response
from a particular RADIUS server before attempting communication with an alternative
server, if available. A setting of '0' will cause only one attempt to be made to each
server.
! Note: The retransmit time may be defined on an individual RADIUS server basis as part of
the 'radius-server host' definition. An individual server-defined setting takes priority
over the global setting.
radius-server retransmit 3
!

! Set the time (in minutes) to wait before re-attempting communication with a
non-responsive RADIUS server, e.g. 1 minute. This time only applies if multiple, redundant
RADIUS servers are defined.
radius-server deadtime 1
!
! Define the source interface to be used to communicate with the TACACS+ servers
ip tacacs source-interface <Loopback or OOB interface>
!
! Define the source interface to be used to communicate with the RADIUS servers
ip radius source-interface <Loopback or OOB interface>
!
! Define a AAA method list which enforces login authentication to an administrative server
group, with the local database defined as a fallback method in case of loss of
communication with the remote AAA servers
! Usernames and passwords with exec level access must be configured in the AAA server
and/or defined locally in order to obtain access
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
! Note: Authentication attempts will NOT continue down a method list if a 'fail' response
is received, only if an error is received, e.g. if the server is down.
aaa authentication login <authen-exec-list> group <adminAAAgroup> local-case
!
! Define a AAA authorization method list for exec sessions to a AAA server, with local
fallback in case of loss of communication with the remote AAA servers

aaa authorization exec <author-exec-list> group <adminAAAgroup> if-authenticated
!
! Enable AAA accounting
aaa accounting exec default start-stop group <adminAAAgroup>p
aaa accounting commands 15 default start-stop group <adminAAAgroup>
aaa accounting system default start-stop group <adminAAAgroup>

!
! Ensure the session ID is maintained across all authentication, authorization and
accounting packets in a session
aaa session-id common
!
!
! Apply the authentication method to all active access lines to be secured, such as VTYs,
console, etc.
!
line [type]
 login authentication <authen-exec-list>
!
! Enforce exec session authorization on all active ports, for instance, VTY lines
! Ensure users are defined on the AAA server with the appropriate permissions
```

```
 authorization exec <author-exec-list>
!
!
```

Sample Web-Based GUI Configuration

Sample HTTP Configuration

```
! Disable HTTP access unless absolutely necessary
no ip http server
!
! Enable HTTP only if absolutely necessary
ip http server
!
! Require all access to be authenticated
! Note: Ensure the AAA server group and server configuration have been configured and at
least one username and password is available prior to applying this command. See the AAA
Configuration Guidelines section for complete details.
!
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
aaa authentication login default group adminAAAgroup local-case
! Require AAA authorization for exec level commands
! Note: Ensure a AAA method list has been configured using 'aaa authorization exec' and at
least
! one username and password is available in order to enable access.
aaa authorization exec default group adminAAAgroup local
!
ip http authentication aaa
!
! Optionally enable accounting
aaa accounting exec default start-stop group adminAAAgroup
!
! Restrict where HTTP access attempts must originate from in order for them to be
processed,
! being as specific as possible, for instance, only permitting access from the NOC
subnets. HTTP
! access-class does not currently support the application of an extended ACL.
! The use of the log keyword enables unauthorized access attempts to be logged, thereby
enabling
! the tracking of abnormal activity. See the Logging Device Access section for more
information.
! Note: Ensure source IP spoofing protection mechanisms are also deployed
access-list <ACL#> remark ACL for HTTP
access-list <ACL#> permit <NOCsubnet1> <inverse-mask>
access-list <ACL#> permit <NOCsubnet2> <inverse-mask>
access-list <ACL#> deny any log
!
ip http access-class <ACL#>
!
! Restrict the maximum number of concurrent HTTP sessions, e.g. to 3.
ip http max-connections 3
!
! HTTP access requires telnet service to be enabled on VTY lines
line vty 0 4
 transport input telnet
```

Sample HTTPS Configuration

```
! Disable HTTP access
no ip http server
!
crypto key generate rsa
! (after entering command, follow the series of prompts)
!
! Enable HTTPS access
ip http secure-server
!
! Require all access to be authenticated
! Note: Ensure the AAA server group and server configuration have been configured and at
least one username and password is available prior to applying this command. See the AAA
Configuration Guidelines section for complete details.
!
! Define local username for fallback access.
username adminuser privilege 15 password <mypassword>
!
aaa authentication login default group adminAAAgroup local-case
! Require AAA authorization for exec level commands
! Note: Ensure a AAA method list has been configured using 'aaa authorization exec' and at
least
! one username and password is available in order to enable access.
aaa authorization exec default group adminAAAgroup local
!
ip http authentication aaa
!
! Optionally enable accounting
aaa accounting exec default start-stop group adminAAAgroup
!
!
! Restrict where HTTP access attempts must originate from in order for them to be
processed,
! being as specific as possible, for instance, only permitting access from the NOC
subnets. HTTP
! access-class does not currently support the application of an extended ACL.
! The use of the log keyword enables unauthorized access attempts to be logged, thereby
enabling
! the tracking of abnormal activity. See the Logging Device Access section for more
information.
! Note: Ensure source IP spoofing protection mechanisms are also deployed
access-list <ACL#> remark ACL for HTTP
access-list <ACL#> permit <NOCsubnet1> <inverse-mask>
access-list <ACL#> permit <NOCsubnet2> <inverse-mask>
access-list <ACL#> deny any log
!
ip http access-class <ACL#>
!
```

Sample SNMP Configuration

```
! Restrict where SNMP access attempts must originate from in order for them to be
processed,
! being as specific as possible, for instance, only permitting access from the SNMP
management
! stations.
access-list 55 remark ACL for SNMP access to device
access-list 55 permit 172.26.150.206
access-list 55 deny   any log
```

```
!
! Define an SNMP view which denies queries to download the full IP routing and ARP tables
snmp-server view myview internet included
snmp-server view myview ipRouteTable excluded
snmp-server view myview ipNetToMediaTable excluded
snmp-server view myview at excluded
!
! In case any of the above keywords are not recognized by a particular IOS release, use
the ones ! below
snmp-server view myview internet included
snmp-server view myview ip.21 excluded
snmp-server view myview ip.22 excluded
snmp-server view myview mib-2.3 excluded
!
! Once the views are defined, associate them to the SNMP community strings. In addition,
restrict ! access to those communities to read-only (RO) and apply the previously defined
ACL.
snmp-server community mycommunity view myview  RO 55
!
! Define the SNMP managers, their supported SNMP version and permitted community string.
snmp-server engineID remote 172.26.150.206 80000009030000B064EFE100
snmp-server host 172.26.150.206 version 3 priv mycommunity
!
!If SNMP v3 is supported, define an SNMP v3 user group with security level 'authPriv' and
enforce ! a restricted view
snmp-server group mygroup v3 priv read myview
!
!Define a user within the SNMP v3 group, along with their authentication password and
encryption
!key
snmp-server user admin mygroup v3 encrypted auth md5 cisco123 priv des56 mykey
!
! Set the source IP address for SNMP traps to the address used on the administrative
loopback
! interface of OOB interface.
snmp-server trap-source GigabitEthernet1/2
!
! Configure the system to send a trap on SNMP authentication failure.
snmp-server enable traps snmp authentication
!
!Configure the System to send a trap for configuration changes.
snmp-server enable traps config
!
!Configure the system to send a trap for environmental monitor threshold exceptions
snmp-server enable traps envmon
!
!Enable any additional required traps. It is recommended that only operationally important
traps
!are enabled, e.g. BGP state changes. Ensure enabled traps are monitored.
snmp-server enable traps bgp
!
!If configuration files are downloaded via SNMP by TFTP servers, restrict which TFTP
servers may
!do so.
snmp-server tftp-server-list 55!
```

Sample Timestamps and NTP Configuration

The following are the configuration fragments for the WAN edge and branch routers used in our validation lab. In this scenario, the WAN edge routers were configured as time servers, and the branch routers as clients. The WAN edge routers are synchronized with an internal time server accessible throughout an Out of Band management network. Communication between branch routers and the WAN edge routers is inband (uses the data network).

NTP Server Configured as Master Stratus 3

```
! Enables timestamp information for debug messages
service timestamps debug datetime localtime show-timezone msec
!
! Enables timestamp information for log messages
service timestamps log datetime localtime show-timezone msec
!
! This router has a hardware calendar that is used as an
! authoritative time source
clock calendar-valid
!
! This allows NTP to update the hardware calendar chip.
ntp update-calendar
!

! Sets the network-wide zone to Eastern Standard Time (UTC -5 hours)
clock timezone EST -5
!
! Defines summertime adjustment for Eastern Daylight Saving Time (UTC -4 hours)
clock summer-time EDT recurring
!
! Sets source of NTP packets to the IP address used on the OOB interface
ntp source GigabitEthernet1/2
!
! Sets the router as a NTP master clock to which peers may synchronize in case
! an external NTP source is not available.
ntp master 3
!
! Defines server and peer
ntp server 172.26.129.252
ntp peer 172.26.159.163
!
! Enables authentication
ntp authentication-key 10 md5 00071A1507545A545C 7
ntp trusted-key 10
ntp authenticate
!
! Enforces a list of allowed NTP servers and peers
access-list 10 permit 127.127.7.1
access-list 10 permit 172.26.129.252
access-list 10 permit 172.26.159.163
access-list 10 deny any log
!
ntp access-group peer 10
!
! Enforces what clients may use this server
access-list 20 permit 10.139.5.11
access-list 20 permit 10.139.5.9
access-list 20 permit 10.139.5.7
```

```
access-list 20 deny any log
!
ntp access-group serve-only 20
```

Example NTP Client (Stratus 4)

```
! Enables timestamp information for debug messages
service timestamps debug datetime localtime show-timezone msec
!
! Enables timestamp information for log messages
service timestamps log datetime localtime show-timezone msec
!
! Sets the network-wide zone to Eastern Standard Time (UTC -5 hours)
clock timezone EST -5
!
! Defines summertime adjustment for Eastern Daylight Saving Time (UTC -4 hours)
clock summer-time EDT recurring
!
! Defines server
ntp server 172.26.158.236
!
! Enables authentication
ntp authentication-key 10 md5 00071A1507545A545C 7
ntp trusted-key 10
ntp authenticate!
```

Sample Syslog Configuration

Note Ensure timestamps and NTP are enabled on a device prior to enabling syslog.

```
! Disable console logging
no logging console
!
! Define the source IP address for syslog messages
logging source-interface Loopback0
!
! Define the syslog servers
logging <syslog-server1>
logging <syslog-server2>
!
! Enable a local history buffer log, e.g. of 64k bytes, for debug level messages
logging buffered 64000 debugging
!
! Define a facility to be used by the syslog server to determine where to store the traps
logging facility <facility>
!
! Enable 'informational' level syslog traps to be sent
logging trap informational
!
! Enable syslog rate-limiting for levels 3 and above
logging rate-limit <#msgs/sec> except 2
!
```

Disabling Unnecessary Services

```
! BOOTP, IP Source Routing, PAD Disable global service on ALL ROUTERS
no ip bootp server
no ip source-route
no service pad


! Global Services disabled by default (all routers)
no service finger
no ip identd
no service tcp-small-servers
no service udp-small-servers

! Disable CDP, MOP, IP Redirects on EXTERNAL facing interfaces
interface <interface-type/number>
 no cdp enable
 no mop enabled
 no ip redirects
 no ip proxy-arp

! Disable MOP, IP Redirects on ACCESS interfaces
interface <interface-type/number>
 no mop enabled
 no ip redirects
 no ip proxy-arp

! Interface services disabled by default
interface <interface-type/number>
 no ip directed-broadcast
```

Sample iACL Configurations

iACL at Internet Edge

The example below shows an iACL protecting an enterprise Internet Edge, and involving the following:

- The enterprise is assigned the 198.133.219.0/24 address block
- The enterprise edge router (198.133.219.6) has a BGP peering session with 198.133.219.10

The iACL shown below was developed based on this information. The ACL permits external BGP peering to the external peer, provides anti-spoof filters, and protects the infrastructure from all external access.

```
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Module 1: Anti-spoofing Denies
!--- These ACEs deny fragments, RFC 1918 space,
!--- invalid source addresses, and spoofs of
!--- internal space (space as an external source).
!
!--- Deny fragments.
access-list 110 deny tcp any 198.133.219.0 0.0.0.255 fragments
access-list 110 deny udp any 198.133.219.0 0.0.0.255 fragments
access-list 110 deny icmp any 198.133.219.0 0.0.0.255 fragments
!--- Deny special-use address sources.
!--- See RFC 3330 for additional special-use addresses.
```

```
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
!--- Filter RFC 1918 space.
access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Module 2:  Explicit Permit
!--- Permit only applications/protocols whose destination
!--- address is part of the infrastructure IP block.
!--- The source of the traffic should be known and authorized.
!
!--- Note: This template must be tuned to the network's
!--- specific source address environment. Variables in
!--- the template need to be changed.
!--- Permit external BGP.
access-list 110 permit tcp host 198.133.219.10 host 198.133.219.6 eq bgp
access-list 110 permit tcp host 198.133.219.10 eq bgp host 198.133.219.6
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Module 3:  Explicit Deny to Protect Infrastructure
access-list 110 deny ip any 198.133.219.0 0.0.0.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Module 4:  Explicit Permit for Transit Traffic
access-list 110 permit ip any any
```

iACL at WAN Edge

This example corresponds to an enterprise WAN edge. The objective of the iACL is to protect the core infrastructure from threats rising from the branches. This scenario involves the following:

172.16.0.0/16 is reserved to OBB network. No packets in this range should come from the branches.

10.122.0.0/16 is allocated to the core infrastructure devices. No packets in this range should come from the branches.

10.139.5.0/24 is allocated to the WAN links. Branch routers are the only systems expected to send packets from this network range, and for the following purposes:

- -EIGRP routing
- ICMP
- SSH (client and server)
- TACACS+
- NTP
- Syslog

```
!--- Module 1: Anti-spoofing, deny special use addresses
! Deny your OOB address space as a source in packets
access-list 101 deny ip 172.26.0.0 0.0.255.255 any
! Deny src addresses of 0.0.0.0 and 127/8 (special use IPv4 addresses RFC3330)
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.0.2.0 0.0.0.255 any
```

```
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
!
!--- Module 2:  Explicit Permit
! Permit traffic from routing peer
access-list 101 permit eigrp host 10.139.5.11 host 224.0.0.10
access-list 101 permit icmp host 10.139.5.11 172.26.0.0 0.0.255.255
access-list 101 permit tcp host 10.139.5.11 eq 22 172.26.0.0 0.0.255.255
access-list 101 permit tcp host 10.139.5.11 172.26.0.0 0.0.255.255 eq 22
access-list 101 permit tcp host 10.139.5.11 host 172.26.150.206 eq 49
access-list 101 permit udp host 10.139.5.11 eq ntp host 172.26.158.236 eq ntp
access-list 101 permit udp host 10.139.5.11 host 172.26.150.206 eq syslog
!
!--- Module 3:  Explicit Deny to Protect Infrastructure
! Deny all other access to infrastructure
access-list 101 deny ip any 10.139.5.0 0.0.0.255
access-list 101 deny ip any 10.122.0.0 0.0.255.255
access-list 101 deny ip any 172.26.0.0 0.0.255.255
!
!--- Module 4:  Explicit Permit/Deny for Transit Traffic
! Permit transit traffic enterprise inner iACL
access-list 101 permit ip any any
```

Sample rACL Configurations

The following is an example rACL protecting an enterprise edge router in a scenario involving the following addresses:

- Public address block is 198.133.219.0/24
- Public infrastructure block is 198.133.219.0/28
- External routing IP address is 198.133.219.5/32
- Out of band management segment is 172.26.0.0/16, router address is 172.26.159.164
- Private address space is 10.135.5.0/24 (directly connected to router)

Given this information, the required rACL could be something like the example shown below. This sample rACL starts with the necessary deny statements to block fragments, then continues with a list of explicit permit statements that allow the expected management and controls protocols, such as BGP, OSPF, SNMP, and NTP. Finally, the rACL ends with a explicit deny entry to block any unexpected traffic sent to the RP.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Module 1 – Deny fragments Section
! Denies any non-initial fragments directed to the RP
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Module 2 – Explicit Permit Section
!
! Explicit Permit Phase. Permit only applications whose
! destination address are the router's valid infrastructure
! addresses and that come from an valid host.
!
! Permit BGP session (outside)
access-list 110 permit tcp 198.133.219.0 0.0.0.15 host 198.133.219.5 eq bgp
access-list 110 permit tcp 198.133.219.0 0.0.0.15 eq bgp host 198.133.219.5
!
```

```
! Permit OSPF (inside)
access-list 110 permit ospf 10.135.5.0 0.0.0.255 host 224.0.0.5
!
! DR multicast address, if needed (inside)
access-list 110 permit ospf 10.135.5.0 0.0.0.255 host 224.0.0.6
access-list 110 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.13
access-list 110 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.15
access-list 110 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.19
!
! permit EIGRP (inside)
access-list 110 permit eigrp 10.135.5.0 0.0.0.255 host 224.0.0.10
access-list 110 permit eigrp 10.135.5.0 0.0.0.255 host 169.223.253.13
access-list 110 permit eigrp 10.135.5.0 0.0.0.255 host 169.223.253.15
access-list 110 permit eigrp 10.135.5.0 0.0.0.255 host 169.223.253.19
!
! Remote access: ssh (out of band)
access-list 110 permit tcp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq 22
!
! SNMP(out of band)
access-list 110 permit udp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq snmp
!
! NTP (out of band)
access-list 110 permit udp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq ntp
!
! Router originated traceroute
! Each hop returns a ttl exceeded (type 11, code 3) message
! and the final destination returns an ICMP port unreachable
! (type 3, code 0)
access-list 110 permit icmp any host 198.133.219.5 ttl-exceeded
access-list 110 permit icmp any host 198.133.219.5 port-unreachable
access-list 110 permit icmp any host 169.223.253.13 ttl-exceeded
access-list 110 permit icmp any host 169.223.253.13 port-unreachable
access-list 110 permit icmp any host 169.223.253.15 ttl-exceeded
access-list 110 permit icmp any host 169.223.253.15 port-unreachable
access-list 110 permit icmp any host 169.223.253.19 ttl-exceeded
access-list 110 permit icmp any host 169.223.253.19 port-unreachable
!
! TACACS+ for router authentication (out of band)
access-list 110 permit tcp 172.26.0.0 0.0.255.255 host 172.26.159.164 established
!
! RADIUS (out of band)
access-list 110 permit udp 172.26.0.0 0.0.255.255 host 172.26.159.164
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Module 2 – Explicit denies all other traffic
!
! Deny all other traffic
access-list 110 deny ip any any
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!Activation of rACL
!
 ip receive access-list 110
```

CoPP Sample Configuration

The following example shows how to develop a CoPP policy and how to apply it in order to protect the control plane of an Internet Edge router.

The following assumption are made:

- Public address block is 198.133.219.0/24
- The public infrastructure block is 198.133.219.0/28
- The external routing IP address is 198.133.219.5/32
- Out of band management segment is 172.26.0.0/16, router IP is 172.26.159.164
- Private address space is 10.135.5.0/24 (directly connected to router)

In this example, the control plane traffic is classified based on relative importance and traffic type. Nine classes are defined, each of which is associated with a separate extended ACL:

- BGP (coppacl-bgp): BGP traffic
- IGP (coppacl-igp): OSPF traffic
- Interactive Management (coppacl-interactivemanagement): remote access and management traffic such as TACACS, SSH, SNMP, and NTP.
- File Management (coppacl-filemanagement): remote file transfer traffic such as TFTP and FTP.
- Reporting (coppacl-reporting): SAA generated ICMP requests from SAA source routers
- Monitoring (coppacl-monitoring): ICMP and traceroute traffic
- Critical Applications (coppacl-critical-app): HSRP traffic
- Undesirable Traffic (coppacl-undesirable): explicitly denies unwanted traffic (for example, Slammer worm packets)
- Default (no ACL needed): all traffic received by the control plane that has not been otherwise identified.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Sample ACLs for CoPP classification
!
! Class for BGP traffic
ip access-list extended coppacl-bgp
 remark BGP traffic class
! allow BGP from routers in the infrastructure block to this router's BGP TCP port
 permit tcp 198.133.219.0 0.0.0.15 host 198.133.219.5 eq bgp
 permit tcp 198.133.219.0 0.0.0.15 eq bgp host 198.133.219.5
!
! Permit OSPF sessions to peers on the local 10.135.5.0/24 network
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.135.5.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.135.5.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.13
 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.15
 permit ospf 10.135.5.0 0.0.0.255 host 169.223.253.19
!
! The Interactive Management class is for traffic that is required for accessing
! and managing the router, in this example, TACACS, ssh,
! snmp, and ntp is classified in this class. Interactive traffic is expected
! to be originated from the Out of band network (172.26.0.0/16)
```

```
ip access-list extended coppacl-interactivemanagement
 remark CoPP interactive management traffic class
! permit return traffic from TACACS+ Servers
 permit tcp 172.26.0.0 0.0.255.255 host 172.26.159.164 established
! SSH access to the router from a subnet
 permit tcp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq 22
! SNMP access from the management segment to the router
 permit udp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq snmp
! Allow the router to receive NTP packets from a known clock sources
 permit udp 172.26.0.0 0.0.255.255 host 172.26.159.164 eq ntp
!
! The File Management class is for file transfer traffic required for software
! and configuration maintenance, in this example, TFTP and FTP is classified in this class
ip access-list extended coppacl-filemanagement
 remark CoPP file management traffic class
! Allow router initiated FTP (active and passive)
 permit tcp 172.26.0.0 0.0.255.255 eq 21 host 172.26.159.164 gt 1023 established
 permit tcp 172.26.0.0 0.0.255.255 eq 20 host 172.26.159.164 gt 1023
 permit tcp 172.26.0.0 0.0.255.255 gt 1023 host 172.26.159.164 gt 1023 established
! Allow router initiated TFTP
 permit udp 172.26.0.0 0.0.255.255 gt 1023 host 172.26.159.164 gt 1023
!
! The reporting class is for traffic used for generating network
! performance statistics. In this example, we are using SAA to
! generate ICMP Pings with different DSCP bits in order to determine
! response times for classes of traffic.  i.e. COS1 will use an ICMP
! with DSCP set to EF, COS2=AF31, COS3=AF21 and COS4=BE.  We will
! create an ACL to classify ICMP pings from specific source routers
! using SAA to generate the ICMPs. We will then use this ACL and the
! 'match ip dscp' classification criteria in the service policy to
! create the reporting class.
ip access-list extended coppacl-reporting
 remark CoPP reporting traffic class
! permit SAA generated ICMP requests from SAA source routers
 permit icmp 172.26.0.0 0.0.255.255 host 172.26.159.164 echo
!
! The monitoring class is used for traffic that is required for
! monitoring the router. Monitoring traffic is traffic that we expect
! to see destined to the router and want to track and limit
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
! permit router originated traceroute
 permit icmp any host 198.133.219.5 ttl-exceeded
 permit icmp any host 198.133.219.5 port-unreachable
 permit icmp any host 169.223.253.13 ttl-exceeded
 permit icmp any host 169.223.253.13 port-unreachable
 permit icmp any host 169.223.253.15 ttl-exceeded
 permit icmp any host 169.223.253.15 port-unreachable
 permit icmp any host 169.223.253.19 ttl-exceeded
 permit icmp any host 169.223.253.19 port-unreachable
! permit receipt of responses to router originated pings
 permit icmp any any echo-reply
! allow pings to router
 permit icmp any any echo
!
! The critical-app class is used for traffic that is crucial to
! particular customer's environment. In this example, HSRP.
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
! permit HSRP
 permit ip any host 224.0.0.2
```

```
!
! This ACL identifies traffic that should always be blocked from
! accessing the Route Processor.! Once undesirable traffic flow is
! identified, an access list entry classifying it can be added and mapped to the
! undesirable traffic class. This can be used as a reaction tool.
ip access-list extended coppacl-undesirable
 remark explicitly defined "undesirable" traffic
! permit, for policing, all traffic destined to UDP 1434
 permit udp any any eq 1434
```

Table A-1 Sample CoPP Policy

Traffic class	Rate (bps)	Conform action	Exceed action
BGP	80,000	Transmit	Drop
IGP	N/A	Transmit	Transmit
Interactive Management	10,000,000	Transmit	Drop
File Management	N/A	Transmit	Transmit
Reporting	500,000	Transmit	Drop
Monitoring	500,000	Transmit	Drop
Critical Apps	500,000	Transmit	Drop
Undesirable	50,000	Drop	Drop
Default	10,000,000	Transmit	Drop

Once the control plane traffic has been classified, the next step is to define the policy action for each traffic class. In this example the limits set per each class represent the boundary after which the system becomes unresponsive and starts dropping packets. Our intention is to deploy a policy that protects the router while reducing the risk of dropping critical traffic. To that end, CoPP policies are configured to permit each traffic class with an appropriate rate limit. Table A-1 shows the parameters used in the CoPP policies.

Note The rates defined in Table A-1 were successfully tested on a Cisco 7200 VXR Series Router with NPE-G1. It is important to note that the values here presented are solely for illustration purposes; every environment will have different baselines.

The following is the policy for the configuration described inTable A-1:

```
! Define a class for each "type" of traffic and associate it with an ACL
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-interactivemanagement
  match access-group name coppacl-interactivemanagement
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-reporting
  match access-group name coppacl-reporting
  match ip dscp ef af31 af21 default
class-map match-all coppclass-monitoring
```

```
  match access-group name coppacl-monitoring
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-undesirable
  match access-group name coppacl-undesirable
!
! This is the actual policy. Depending on class of traffic, rates and associated actions
! are defined
policy-map copp-policy
!
! BGP traffic is limited to a rate of 80,000 bps, if traffic exceeds
! that rate it is dropped. NOTE: In this example BGP traffic is rate-limited
! to control attacks based on BGP packets. Once the normal rates are determined,
! and depending on the hardware platform used, it's recommended you consider
! readjusting the rate-limiting parameters.
  class coppclass-bgp
     police 80000 8000 8000 conform-action transmit exceed-action drop
!
! IGP traffic will not be limited in this example either therefore no
! operation needs to be specified in this class. NOTE: As with the BGP
! class, once normal rates are determined for your IGP traffic, you may
! consider setting a rate-limit to further protect your router.
  class coppclass-igp
!
! Interactive Management traffic is limited to a rate of 10,000,000 bps,
! if traffic exceeds that rate it is dropped.
  class coppclass-interactivemanagement
     police 10000000 100000 100000 conform-action transmit exceed-action drop
!
! File Management traffic will not be limited in this example either therefore no
! operation needs to be specified in this class. NOTE: As with the IGP
! class, once normal rates are determined for your file management traffic,
! you may consider setting a rate-limit to further protect your router.
  class coppclass-filemanagement
!
! Reporting traffic is limited to a rate of 500,000 bps, if traffic exceeds
! that rate it is dropped
  class coppclass-reporting
     police 500000 5000 5000 conform-action transmit exceed-action drop
!
! Monitoring traffic is limited to a rate of 500,000 bps, if traffic exceeds
! that rate it is dropped
  class coppclass-monitoring
     police 500000 5000 5000 conform-action transmit exceed-action drop
!
! critical-app traffic is limited to a rate of 500,000 bps, if traffic
! exceeds that rate it is dropped
  class coppclass-critical-app
     police 500000 5000 5000 conform-action transmit exceed-action drop
!
! This policy drops all traffic categorized as undesirable, regardless
! of rate.
  class coppclass-undesirable
     police 50000 1500 1500 conform-action drop exceed-action drop
! or if on the T train you can use the drop command
!  drop
!
! The default class applies to all traffic received by the control
! plane that has not been otherwise identified. In this example, all
! default traffic is limited to 10,000,000 bps and violations of that limit
! are dropped.
```

```
  class class-default
     police 10000000 100000 100000 conform-action transmit exceed-action drop
….
! Applies the defined CoPP policy to the control plane
Router(config)# control-plane
Router(config-cp)# service-policy input copp-policy
```

Control Plane Protection Sample Configuration

Assuming that a control plane protection has been configured previously using MQC CLI, the following example shows how the policy is applied to the control-plane host subinterface:

```
Router(config)# control-plane host
Router(config-cp)# service-policy input copp-policy
```

The following example shows how to configure a port-filter policy to drop all traffic destined to closed or "nonlistened" TCP/UDP ports:

```
Router(config)# class-map type port-filter pf-class
Router(config-cmap)# match closed-ports
Router(config-cmap)# exit
Router(config)# policy-map type port-filter pf-policy
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# end
Router#
```

The following example shows how to configure a queue-threshold policy to set the queue limit for SNMP protocol traffic to 50, Telnet traffic to 50, and all other protocols to 150:

```
Router(config)# class-map type queue-threshold qt-snmp-class
Router(config-cmap)# match protocol snmp
Router(config-cmap)# class-map type queue-threshold qt-telnet-class
Router(config-cmap)# match protocol telnet
Router(config-cmap)# class-map type queue-threshold qt-other-class
Router(config-cmap)# match host-protocols
Router(config-cmap)# exit
Router(config)# policy-map type queue-threshold qt-policy
Router(config-pmap)# class qt-snmp-class
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class qt-telnet-class
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class qt-other-class
Router(config-pmap-c)# queue-limit 150
Router(config-pmap-c)# end
Router#
```