CHAPTER 9

Security in Cisco Unified Border Element (SP Edition) Distributed Model

The Cisco Unified Border Element (SP Edition) distributed model for the Cisco ASR 1000 Series Routers offers high security functions. Enterprise users want to protect their network and service providers want to protect their core or backbone network. Because service providers allow direct users to come into their network to access different services, it is critical to have high security. Customers also want to police the data coming into their networks and require notification if any unwanted user tries to access the network. The data border element (DBE) implementation supports various security features and policing of incoming data.

For example, the DBE supports the ETSI TS 102 333 Gate Management (GM) package to control addressing for the local as well as the remote party. The DBE uses the source address mask and remote source address filtering to specify a range of addresses rather than a specific address and port for the source or remote address of the arriving packet. Data coming from other defined addresses are dropped and reported to the Signaling Border Element (SBE) for security reasons. Local Source Properties (Address and Port) and Remote Source Address Mask Filtering, described in this chapter, are supported features of the GM package.

This chapter describes or cross-references supported security features.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

Contents

This chapter provides information about the following topics:

- Firewall (Media Pinhole Control), page 9-2
- H.248 Address Reporting Package, page 9-2
- H.248 Session Failure Reaction Package, page 9-2
- H.248 Termination State Control Package, page 9-3
- Full Support for Interim Authentication Header, page 9-3
- IP NAPT Traversal Package and Latch and Relatch Support, page 9-9
- Local Source Properties (Address and Port), page 9-11

- NAPT and NAT Traversal, page 9-11
- Remote Source Address Mask Filtering, page 9-12
- Topology Hiding, page 9-12
- Traffic Management Policing, page 9-13
- Two-Rate Three-Color Policing and Marking, page 9-13

Firewall (Media Pinhole Control)

The SBE Call Admission Control (CAC) function inspects the signaling message and instructs the firewall in the DBE to open and close pinholes as needed for the media streams and signaling.

H.248 Address Reporting Package

The data border element (DBE) supports the H.248 Address Reporting (ADR) package, defined in "Draft New H.248.37 Amendment 1", ITU-T document TD-27. The adr package extends the existing IP NAPT Traversal (IPNAPT) package, and adds a new Remote Source Address Change (RSAC) event with two parameters: New Remote Source Address (NRSA), and New Remote Source Port (NRSP).

The rsac event is generated by the media gateway (MG) when the remote source address for the termination changes (that is, when a stream latches), and is used to report the newly detected remote source address and port to which the stream has been latched.

The event is generated in both the LATCH and RELATCH scenarios. The DBE reports the event subscription with the audit response when the media gateway controller (MGC) audits the packages.

For further information on support for the H.248 IP NAPT Traversal package, see the "IP NAPT Traversal Package and Latch and Relatch Support" section on page 9-9.

Restrictions for DBE H.248 Address Reporting Package

The following are restrictions pertaining to ADR package support:

- The MGC must explicitly subscribe for the rsac event.
- The adr package can be used only in conjunction with the IP NAPT Traversal package.

H.248 Session Failure Reaction Package

The data border element (DBE) supports the H.248 Session Failure Reaction (SFR) package. From a security point of view, the media gateway controller (MGC) can put a termination out of service when the H.248 connection between the MGC and media gateway (MG) is lost.

For more information on the SFR package, see the "H.248 Session Failure Reaction Package" section on page 7-4.

H.248 Termination State Control Package

The data border element (DBE) supports the Termination State Control (TSC) package to monitor signaling pinholes.

The "tsc-quiesce" feature of the TSC package helps the media gateway controller (MGC) monitor a signaling pinhole and put the pinhole in "not-in-service" mode when all terminations are subtracted.

For more information on the TSC package, see the "H.248 Termination State Control Package" section on page 7-5.

Full Support for Interim Authentication Header

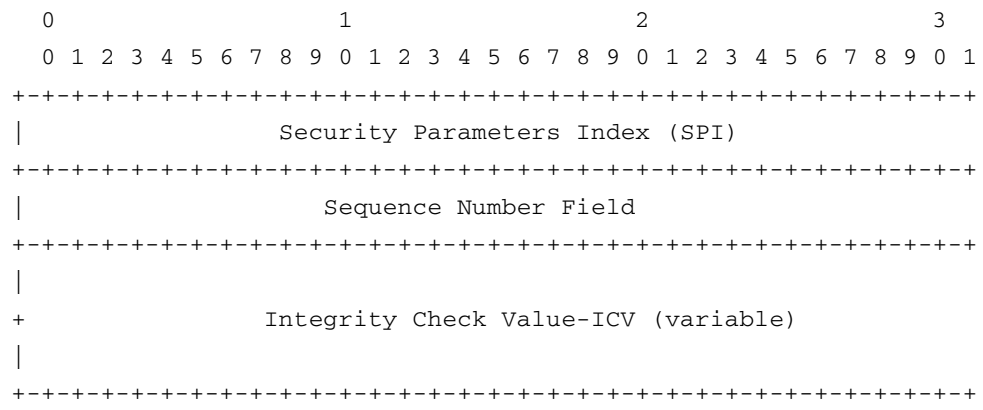
The Cisco Unified Border Element (SP Edition) distributed model offers full support to the Interim Authentication Header (IAH) that conforms to section 10.2, Interim AH Scheme, of the H.248.1v3 Gateway Control Protocol: Version 3. An IAH is part of every H.248 message generated by the data border element (DBE) to the media gateway controller (MGC). Information in the IAH is used to authenticate and check the integrity of packets, thus ensuring packet security.

The DBE generates an IAH for outgoing H.248 messages sent to the MGC. The DBE calculates and then populates an IAH which is sent with the H.248 message. For all incoming H.248 messages received from the MGC, the DBE validates that the IAH received matches its calculation. The IAH scheme inserts the IAH within the H.248.1 protocol header. Note that for IPsec, the IAH is inserted immediately after the IP header for IPsec.

Figure 9-1 shows the IAH format consisting of the Security Parameters Index (SPI), Sequence Number, and Integrity Check Value (ICV):

- Security Parameters Index (SPI)—An arbitrary 32-bit value that the MGC uses to identify the Security Association to which an incoming or outgoing packet is bound, and specifies which hashing key to use.
- Sequence Number—A monotonically increasing number, used to prevent replay attacks.
- Integrity Check Value (ICV)—A variable-length field that contains the Integrity Check Value for the packet. The MGC computes the ICV over the appropriate fields of the packet, using the specified integrity algorithm, and verifies that it is the same as the ICV included in the ICV field of the packet. If the computed and received ICVs match, then the packet is valid.

Figure 9-1 Interim Authentication Header Format



To enable full support of IAH, you must configure the following:

- IAH hashing scheme – Configure one of the following:
  - HMAC-MD5: Hashing for Message Authentication-Message Digest 5 that produces a 128-bit hash value.
  - HMAC-SHA: Hashing for Message Authentication-Secure Hash Algorithm that produces a message digest that is 160 bits long.

  MD5 hashing is faster to calculate, but provides less secure authentication than SHA hashing. The hash calculation includes a synthesized IP header consisting of a 32-bit source IP address, a 32-bit destination address, and a 16-bit UDP or TCP destination port encoded as 20 hexadecimal digits.
- Inbound (local) Security Parameter Index (SPI)
- Outbound (remote) SPI
- Hex-key argument, which is a string of a maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde.

Note IPv6 packets that support IPsec do not use the Interim Authentication Header scheme.

Restrictions for DBE Interim Authentication Header Full Support

In some circumstances, the DBE uses zero authentication where the IAH is inserted in the packet and all fields in the IAH are set to zeroes. The DBE checks the packet syntactically, however, the DBE does not authenticate whether there is an IAH or if it is correct.

The following are restrictions pertaining to the IAH full support, where the DBE reverts back to zero authentication:

- If you enable authentication of call packets by specifying the **interim-auth-header** keyword in the **transport** command, but you do not specify either **ah-md5-hmac** or **ah-sha-hmac**, the authentication reverts back to zero authentication.
- For the MD5 or SHA hashing scheme to work, both the inbound and outbound SPI must be configured. If you configure only the inbound or outbound SPI key or neither inbound or outbound SPI key, the authentication reverts back to zero authentication, and the DBE issues a warning message “Both inbound and outbound keys must be configured to enable authentication”.

Related Commands

The **transport (session border controller)** command is used in conjunction with the **inbound** and **outbound** commands. The three commands are used together to enable Interim Authentication Header (IAH) authentication of inbound and outbound call packets. If you specify a hashing scheme (**ah-md5-hmac** or **ah-sha-hmac** keywords) using the **transport (session border controller)** command, you must configure incoming and outgoing call packets using both the **inbound** and **outbound** commands.

- **transport** command—**interim-auth-header** keyword was added to insert the IAH into H.248 messages. The **ah-md5-hmac** and **ah-sha-hmac** keywords are added to specify the type of hashing scheme for authentication.
- **inbound** and **outbound** commands—Configures inbound and outbound packets with the *spi* and *hex-key* arguments to use a specific Security Parameters Index (SPI) and hex key.

For more information on the **transport (session border controller)**, **inbound**, and **outbound** commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

Configuring IAH Full Support

This section contains steps to configure the IAH full support functionality in a typical configuration scenario on the Cisco ASR 1000 Series Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface sbc** {*interface-number*}
4. **ip address** *ip-address*
5. **exit**
6. **sbc** {*sbc-name*} **dbe**
7. **vdbe** [**global**]
8. **h248-version** *version*
9. **h248-napt-package** [**napt** | **ntr**]
10. **local-port** {*port-num*}
11. **control-address h248 ipv4** {*A.B.C.D*}
12. **controller h248** {*controller-index*}
13. **remote-address ipv4** {*A.B.C.D*}
14. **remote-port** {*port-num*}
15. **transport** {**udp** | **tcp**} [**interim-auth-header**] [**ah-md5-hmac** | **ah-sha-hmac**]
16. **inbound** {*spi*} {*hex-key*}
17. **outbound** {*spi*} {*hex-key*}
18. **exit**
19. **exit**
20. **attach-controllers**
21. **exit**
22. **location-id** {*location-id*}
23. **media-address ipv4** {*A.B.C.D*}
24. **activate**
25. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface sbc** {*interface-number*} **Example:** `Router(config)# interface sbc 1`	Creates an SBC virtual interface and enters into interface configuration mode.
Step 4	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 1.1.1.1 255.0.0.0`	Configures an IP address on the SBC virtual interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**sbc** {*sbc-name*} **dbe** **Example:** `Router(config)# sbc global dbe`	Creates the DBE service on the SBC and enters into SBC-DBE configuration mode.
Step 7	**vdbe** [**global**] **Example:** `Router(config-sbc-dbe)# vdbe global`	Enters into VDBE configuration mode with a default DBE named “global”. Only one DBE is supported and its name must be “global”.
Step 8	**h248-version** *version* **Example:** `Router(config-sbc-dbe-vdbe)# h248-version 3`	Specifies that the DBE uses an H.248 version when it forms associations with an H.248 controller. Version 2 is the default.
Step 9	**h248-napt-package** [**napt** | **ntr**] **Example:** `Router(config-sbc-dbe-vdbe)# h248-napt-package napt`	Defines whether the DBE uses the Network Address and Port Translation (NAPT) or NAT Traversal (NTR) H.248 package for signaling NAT features. NTR is the default. The example shows how to configure the DBE to use NAPT.
Step 10	**local-port** {*port-num*} **Example:** `Router(config-sbc-dbe-vdbe)# local-port 2971`	Configures the DBE to use the specific local port number when connecting to the default media gateway controller (MGC).

	Command or Action	Purpose
Step 11	**control-address h248 ipv4** {*A.B.C.D*} **Example:** `Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.41`	Configures the DBE to use a specific IPv4 H.248 control address, which is the local IP address the DBE uses as its own address when connecting to the SBE.
Step 12	**controller h248** {*controller-index*} **Example:** `Router(config-sbc-dbe-vdbe)# controller h248 2`	Configures the H.248 controller for the DBE and enters into Controller H.248 configuration mode. In the example, the configured number 2 identifies the H.248 controller for the DBE.
Step 13	**remote-address ipv4** {*A.B.C.D*} **Example:** `Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254`	Configures the IPv4 remote address of the H.248 controller for the SBE. In the example, 200.50.1.254 is configured as the remote SBE IP address.
Step 14	**remote-port** {*port-num*} **Example:** `Router(config-sbc-dbe-vdbe-h248)# remote-port 2971`	Configures the port number of the H.248 controller that is used to connect to the SBE.
Step 15	**transport** {**udp** | **tcp**} [**interim-auth-header**] [**ah-md5-hmac** | **ah-sha-hmac**] **Example:** `Router(config-sbc-dbe-vdbe-h248)# transport udp interim-auth-header ah-sha-hmac`	Configures the DBE to use either UDP or TCP for H.248 control signaling, and configures the Interim Authentication Header (IAH) to authenticate and check the integrity of call packets by specifying either the MD5 or SHA hashing scheme. Enters into IAH Key configuration mode. **ah-md5-hmac**—Hashing for Message Authentication-Message Digest 5, produces a 128-bit hash value. **ah-sha-hmac**—Hashing for Message Authentication-Secure Hash Algorithm, produces a message digest that is 160-bits long.
Step 16	**inbound** {*spi*} {*hex-key*} **Example:** `Router(config-sbc-dbe-vdbe-h248-iah)# inbound 300 abcdef01234456`	Configures inbound call packets to use a specific Security Parameters Index (SPI) and hex key. spi (Security Parameters Index)—An arbitrary 32-bit value that the MGC uses to identify the Security Association to which an incoming packet is bound, that is, which hashing key to use. Accepts a range of 256 through 2147483647. hex-key—Maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde.

	Command or Action	Purpose
Step 17	**outbound** {*spi*} {*hex-key*} **Example:** `Router(config-sbc-dbe-vdbe-h248-iah)# outbound 400 012345678abcde`	Configures outbound call packets to use a specific Security Parameters Index (SPI) and hex key. spi (Security Parameters Index)—An arbitrary 32-bit value that the MGC uses to identify the Security Association to which an outgoing packet is bound, that is, which hashing key to use. Accepts a range of 256 through 2147483647. hex-key—Maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde.
Step 18	**exit** **Example:** `Router(config-sbc-dbe-vdbe-h248-iah)# exit`	Exits IAH Key configuration mode and enters Controller H.248 configuration mode.
Step 19	**exit** **Example:** `Router(config-sbc-dbe-vdbe-h248)# exit`	Exits Controller H.248 configuration mode and enters VDBE configuration mode.
Step 20	**attach-controllers** **Example:** `Router(config-sbc-dbe-vdbe)# attach-controllers`	Attaches the DBE to an H.248 controller.
Step 21	**exit** **Example:** `Router(config-sbc-dbe-vdbe)# exit`	Exits VDBE configuration mode.
Step 22	**location-id** {*location-id*} **Example:** `Router(config-sbc-dbe)# location-id 1`	Configures a location ID for the DBE. The location ID is used by the network to route calls.
Step 23	**media-address ipv4** {*A.B.C.D*} **Example:** `Router(config-sbc-dbe)# media-address ipv4 1.1.1.1 255.0.0.0`	Adds the IPv4 address to the set of addresses, which can be used by the DBE as a local media address. This address is the SBC virtual interface address. Configure this command for each IP address that you specified under the SBC virtual interface in Step 4.
Step 24	**activate** **Example:** `Router(config-sbc-dbe)# activate`	Initiates the DBE service of the SBC.
Step 25	**end** **Example:** `Router(config-sbc-dbe)# end`	Exits SBC-DBE configuration mode and returns to privileged EXEC mode.

IAH Full Support Examples

The following configuration example shows how to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound SPI to 300 and outbound SPI to 400, and the inbound and outbound hash keys to abcdef01234456 and 012345678abcde, respectively:

```
sbc global dbe
 vdbe global
  h248-version 3
  h248-napt-package napt
  local-port 2970
  control-address h248 ipv4 200.50.1.40
  controller h248 2
   remote-address ipv4 200.50.1.254
   remote-port 2970
   transport tcp interim-auth-header ah-sha-hmac
     inbound 300 abcdef01234456
     outbound 400 012345678abcde
 attach-controllers
```

The following example shows an H.248 message with the IAH:

```
AU=0x00000190:0x00000002:0x6E60A7DC58ECD631A5E13DCFC6E94DEB
!/3 [200.60.255.200]:2944
P=6{
C=1{
A=xyzcompany/sip/gn/0/1/0/1/ac/1,
A=xyzcompany/sip/gn/0/2/0/1/bb/2}}
```

Debugging Tips

The debugging tips for IAH Full Support are as follows:

- If the MGC is rejecting the H.248 messages from the DBE, or the DBE is rejecting H.248 messages from the MGC, compare the IAH configuration on the DBE with that on the MGC. The inbound SPI key on the DBE should match the outbound SPI key on the MGC, and vice-versa.
- If the IAH header on H.248 messages from the DBE looks like all zeros, then it is likely that the IAH configuration is incomplete, for example, only the inbound or the outbound IAH configuration is specified. See also the "Restrictions for DBE Interim Authentication Header Full Support" section on page 9-4.

IP NAPT Traversal Package and Latch and Relatch Support

The data border element (DBE) supports the IP NAPT Traversal (IP NAPT) package that is defined in H.248.37. IP NAPT traversal is an alternative method to the existing support of the NAT Traversal (NTR) package, defined in ETSI TS 102 333. IP Network Address and Port Translation (IP NAPT) defines two signals, Latch and Relatch, to control how the DBE learns remote addresses for endpoints behind a Network Address Translation (NAT).

The NAPT package is defined through a new field, napt_variant, in the bcaGalEntTable MIB table. If this field is set to "H.248.37," then NAPT support can be requested by the media gateway controller (MGC) using the H.248.37 IP NAPT Traversal package. In other words, the MGC can request that the DBE wait for the first inbound media packet and "latch" onto it. The DBE learns the remote address and port for the flow from that packet. The MGC can request latching or relatching using the H.248 signal.

Latch and Relatch Support

The DBE supports Latch and full Relatch support. The Latch and Relatch signals control how the DBE learns remote addresses. Latch and Relatch are commands from the media gateway controller (MGC). Latch is an event that occurs on a flow when certain packets arrive and are matched to that flow. This event changes the admission criteria for a flow.

The ITU-T H.248.37 standard describes the ipnapt/latch signal with the napt parameter. The napt parameter has the values OFF, LATCH, and RELATCH.

When the LATCH value is set, the DBE ignores the addresses received in the RemoteDescriptor. Instead, the DBE uses the source address and source port from the incoming media streams to be the destination address and destination port of the outgoing streams.

The RELATCH value is similar to the LATCH value except that when the DBE detects a change of source IP address and port on the incoming media stream, then the new source IP address and port are used as the destination address and port for outgoing packets. After relatching, any packets received with the old source address and port are discarded.

When latching, the DBE uses the remote address and port of a source endpoint as the destination endpoint address and port if the source IP address is within a specified Gate Management/remote source address mask (gm/rsam). This means that within a subnet any packet can be latched within a gm/rsam. The Relatch event waits until a packet arrives that fails the latched admission criteria, but which meets the relatch criteria. The relatch may require stricter admission criteria than the original latching, such as packets may have to come from a specific remote address rather than from within the subnet. Or the relatch criteria might identify a different subnet. In relatching, one reason for the change in the source IP address and port could be a subscriber requiring a different service.

When the ntr package is in use, the DBE continues to attempt to relearn remote addresses and ports following any H.248 operation that modifies a termination whose endpoint is behind a NAT. Relearning continues to be timed out if no packets from a new remote source address and port are received within a suitable period.

When the ipnapt package is in use, the DBE does not attempt to relearn remote addresses and ports unless a Relatch is explicitly signaled by the MGC. Relatching is not timed out.

Restrictions for DBE Latch and Relatch Support

The following are restrictions pertaining to DBE support for the IP NAPT Traversal (ipnapt) package and Latch and Relatch:

- The DBE only supports either the NTR package or the IP NAPT Traversal package for a termination. You can configure either package with the **h248-napt-package** command.
- The DBE does not generate the notifyComplete signal when the Latch or Relatch signal completes.
- With the IP NAPT Traversal package, the DBE does not automatically relatch on receipt of an H.248/Megaco request that modifies the gm/sam. If a Relatch is required, it must be explicitly signaled by the MGC. In addition, you cannot update the remote source address mask so that it no longer contains the previously latched remote address without signaling a Relatch.

Related Command

The **h248-napt-package** command defines which H.248 package (either ipnapt or ntr) the DBE uses for signaling NAT features.

Local Source Properties (Address and Port)

The data border element (DBE) is enhanced to support multiple terminations that share a single local address and port. The Gate Management/remote source address mask (gm/rsam) defines a remote subnet. The mask length is a property of the local address and port combination. Only multiple terminations that share the same local address and port are required to have the same gm/rsam length. Terminations with different local addresses or ports can have different gm/rsam lengths.

A gm/rsam having the same mask length allows multiple terminations to share a single local address and port combination, with the requirement that the terminations are configured with gm/rsams that are distinct. This enables the media gateway controller (MGC) to identify and match the terminations to the correct flow. For more information about Local Source Address and Local Source Port properties, see the ETSI TS 102 333 V1.1.2 Gate Management Package.

Note A termination can be described as a point of entry or exit of media flows relative to the DBE.

Terminations may share a single local address and port under one or the other of the following conditions:

- Terminations have an MGC-managed local address, in which case they must be specified with a proper gm/sam.
- Terminations are specified with a gm/sam and the address is “non-local”; that is, the pinhole is No NAPT or the termination is the one that is the unwritten flow of a Single NAPT pinhole.

This enhancement supports the following functionality:

- Call signaling can be routed to the MGC through the DBE.
- Call signaling from different subscribers can be routed through different pinholes on the DBE.

  These different pinholes can share the same IP address and port on the subscriber side on the DBE. This is a typical scenario on the User-Network Interface, where it is simpler to publish a single IP and port to many subscribers.

Restrictions for DBE Local Source Properties (Address and Port)

The following is a restriction pertaining to DBE support for this feature:

Only three different lengths of network masks can be in use at the same time on a given local address and port combination. Otherwise, the DBE issues error 510 “Insufficient Resources”.

NAPT and NAT Traversal

The data border element (DBE) performs translation of IP addresses and port numbers via Network Address and Port Translation (NAPT) and Network Address Translation (NAT) Traversal functions in both directions.

NAT converts an IP address from a private address to a public address in real time. It allows multiple users to share a single public IP address. The DBE can learn the NAT’s public address and latch onto it for that flow.

Remote Source Address Mask Filtering

This feature adds support for the Remote Source Address Filtering (saf) and Remote Source Address Mask (rsam) properties of the ETSI TS 102 333 Gate Management (GM) package.[1]

The media gateway controller (MGC) can specify the gm/saf and gm/rsam properties of terminations in Add and Modify requests. Cisco Unified Border Element (SP Edition) reports them in Audit responses.

This feature allows the MGC to program multiple terminations with the same local address and port, VPN ID, and transport protocol, as long as the multiple terminations are distinguished by their remote source address mask, and the local address is taken from an MGC-managed address range.

This feature supports a single local address for each phone where each phone transmits media using a single pinhole. This means several signaling flows or pinholes can have the same address and port.

Packets arriving at the SBC are classified into flows using the following data: VPN ID, destination address, destination port, protocol type, and source address. The source address is only required to match a remote source address mask rather than a specific remote address.

Restrictions for DBE Remote Source Address Mask Filtering

The following are restrictions pertaining to data border element (DBE) support for this feature:

- If the remote source address mask is specified for a termination, then it must contain the address in the remote descriptor, unless NAT latching techniques are used. However if you want more than one flow on the same local address or port, then the local address must be MGC-managed.
- A prefix length of 0 for the remote source address mask is invalid.
- The MGC is only allowed to specify local addresses and ports that lie within configured address and port ranges.

Related Commands

The related commands for Remote Source Address Mask Filtering feature include:

- The **media-address ipv4** command has **dbe** and **mgc** options that indicate whether an address pool is provided from which the DBE or MGC can allocate addresses.
- The new **media-address pool ipv4** command creates a pool of sequential IPv4 media addresses that can be used by the DBE as local media addresses; the command also has **dbe** and **mgc** options.

Topology Hiding

Topology hiding is an important function of security because it protects the identity of the users and their network addresses. See Chapter 13, “Topology Hiding” for more information.

1. ETSI TS 102 333 version 1.1.2 Gate Management Package

Traffic Management Policing

The data border element (DBE) supports the H.248 Traffic Management (Tman) package to police signaling and media streams. The DBE can also monitor packets coming from the access (customer) side and from the backbone (network core) side.

For more information on the Tman package, see the "H.248 Traffic Management Package Support" section on page 7-7.

Two-Rate Three-Color Policing and Marking

The data border element (DBE) supports Two-Rate Three-Color Policing and Marking to control the traffic coming from the user.

For more information on the Two-Rate Three-Color Policing and Marking feature, see the "Two-Rate Three-Color Policing and Marking" section on page 5-7.