



CHAPTER 25

Configuring Template ACLs

When user profiles are configured using RADIUS Attribute 242, similar per-user access control lists (ACLs) may be replaced by a single Template ACL. That is, one ACL represents many similar ACLs. In Cisco IOS Release 12.2(28)SB, by using Template ACLs, you can increase the total number of ACLs used in the Cisco 10000 series routers but minimize the memory and CPU consumption in processing the ACLs.

The Template ACL feature is useful for customers in a broadband environment with tens of thousands of subscribers. Network implementations that use a unique ACL for each subscriber can easily exceed the maximum available resources on the Cisco 10000 series routers. In networks where each subscriber has its own ACL, it is common for the ACL to be the same for each user except for the user's IP address. Template ACLs alleviate this problem by grouping ACLs with many common access control elements (ACEs) into a single ACL that compiles faster and saves system resources. By using the Template ACL feature, service providers can provision unique ACLs for up to 60,000 subscribers using RADIUS Attribute 242. Configuration of ACLs remains the same as in previous Cisco IOS versions.

For example, the following example shows two ACLs that can be sent using Attribute 242, for two separate users:

```
ip access-list extended Virtual-Access1.1#1
permit igmp any host 1.1.1.1
permit icmp host 1.1.1.1 any
deny ip host 44.33.66.36 host 1.1.1.1
deny tcp host 1.1.1.1 44.33.66.36
permit udp any host 1.1.1.1
permit udp host 1.1.1.1 any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1
```

```
ip access-list extended Virtual-Access1.1#2
permit igmp any host 13.1.1.2
permit icmp host 13.1.1.2 any
deny ip host 44.33.66.36 host 13.1.1.2
deny tcp host 13.1.1.2 44.33.66.36
permit udp any host 13.1.1.2
permit udp host 13.1.1.2 any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
```

```

permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1

```

With the Template ACL feature enabled, these two ACLs can be recognized as similar, and a new Template ACL is created as follows:

```

ip access-list extended 4_Temp_<random-number>
permit igmp any host <PeerIP>
permit icmp host <PeerIP> any
deny ip host 44.33.66.36 host <PeerIP>
deny tcp host <PeerIP> 44.33.66.36
permit udp any host <PeerIP>
permit udp host <PeerIP> any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1

```

In this example, therefore, an IP address would be associated as follows:

- Virtual-Access1.1#1 1.1.1.1
- Virtual-Access1.1#2 13.1.1.2

The PXF engine knows which user a packet is coming from or going to, so it can get the user IP for comparison from the IP address table.

Template ACLs are activated only for per-user ACLs configured through RADIUS Attribute 242. Any other ACL type is not subject to Template ACL processing. The Template ACL feature is enabled by default, and all Attribute 242 ACLs are considered for template status.

Using the **access-list template number** command, you can limit Template ACL status to only ACLs with *number* or fewer rules. The default setting is 100 rules; this value is larger than most Attribute 242 ACLs.

The Template ACLs feature is described in the following topics:

- [Feature History for Template ACLs, page 25-2](#)
- [Configuration Tasks for Template ACLs, page 25-3](#)
- [Monitoring and Maintaining the Template ACL Configuration, page 25-5](#)
- [Configuration Examples for Template ACLs, page 25-5](#)

Feature History for Template ACLs

Cisco IOS Release	Description	Required PRE
12.2(28)SB	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(31)SB2	Supported was added for the PRE3.	PRE3

Configuration Tasks for Template ACLs

If ACLs are configured using RADIUS Attribute 242, Template ACLs are enabled by default. Configuration tasks for Template ACLs include the following:

- [Configuring the Maximum Size of Template ACLs \(Optional\)](#)
- [Configuring ACLs Using RADIUS Attribute 242](#)

Configuring the Maximum Size of Template ACLs (Optional)

By default, Template ACL status is limited to ACLs with 100 or fewer rules. You can set this number lower.

To configure the maximum number of rules in Template ACLs, enter the following command in global configuration mode:

```
Router(config)# access-list template number
```

The range for *number* is from 1 to 100.

[Example 25-1](#) shows the configuration of Template ACL processing for individual user ACLs with 50 or fewer rules.

Example 25-1 Configuring a Template ACL

```
Router(config)# access-list template 50
Router(config)#
```

Configuring ACLs Using RADIUS Attribute 242

Template ACL processing occurs only for ACLs that are configured using RADIUS Attribute 242. Attribute 242 has the following format for an IP data filter:

Ascend-Data-Filter = “ip <dir> <action> [dstip <dest_ipaddr\subnet_mask>] [srcp <src_ipaddr\subnet_mask>] [<proto> [dstport <cmp> <value>] [srcport <cmp> <value>] [<est>]]”

[Table 25-1](#) describes the elements in an Attribute 242 entry for an IP data filter.

Table 25-1 IP Data Filter Syntax Elements

Element	Description
ip	Specifies an IP filter.
<dir>	Specifies the filter direction. Possible values are in (filtering packets coming into the router) or out (filtering packets going out of the router).
action	Specifies the action the router should take with a packet that matches the filter. Possible values are forward or drop .

Table 25-1 *IP Data Filter Syntax Elements (continued)*

Element	Description
dstip <dest_ipaddr\subnet_mask>	Enables destination-IP-address filtering. Applies to packets whose destination address matches the value of <dest_ipaddr> . If a subnet mask portion of the address is present, the router compares only the masked bits. If you set <dest_ipaddr> to 0.0.0.0, or if this keyword is not present, the filter matches all IP packets.
srcp<src_ipaddr\subnet_mask>	Enables source-IP-address filtering. Applies to packets whose source address matches the value of <src_ipaddr> . If a subnet mask portion of the address is present, the router compares only the masked bits. If you set <src_ipaddr> to 0.0.0.0, or if this keyword is not present, the filter matches all IP packets.
<proto>	Specifies a protocol specified as a name or a number. Applies to packets whose protocol field matches this value. Possible names and numbers are icmp (1) , tcp (6) , udp (17) , and ospf (89) . If you set this value to zero (0), the filter matches any protocol.
dstport <cmp> <value>	Enables destination-port filtering. This keyword is valid only when <proto> is set to tcp (6) or udp (17) . If you do not specify a destination port, the filter matches any port. <cmp> defines how to compare the specified <value> to the actual destination port. This value can be < , = , > , or ! . <value> can be a name or a number. Possible names and numbers are ftp-data (20) , ftp (21) , telnet (23) , nameserver (42) , domain (53) , tftp (69) , gopher (70) , finger (79) , www (80) , kerberos (88) , hostname (101) , nntp (119) , ntp (123) , exec (512) , login (513) , cmd (514) , and talk (517) .
srcportcmp <cmp> <value>	Enables source-port filtering. This keyword is valid only when <proto> is set to tcp (6) or udp (17) . If you do not specify a source port, the filter matches any port. <cmp> defines how to compare the specified <value> to the actual destination port. This value can be < , = , > , or ! . <value> can be a name or a number. Possible names and numbers are ftp-data (20) , ftp (21) , telnet (23) , nameserver (42) , domain (53) , tftp (69) , gopher (70) , finger (79) , www (80) , kerberos (88) , hostname (101) , nntp (119) , ntp (123) , exec (512) , login (513) , cmd (514) , and talk (517) .
<est>	When set to 1, specifies that the filter matches a packet only if a TCP session is already established. This argument is valid only when <proto> is set to tcp (6) .

Example 25-2 shows four Attribute 242 IP data filter entries.

Example 25-2 RADIUS Attribute 242 IP Data Filter Entries

```
Ascend-Data-Filter="ip in drop"
Ascend-Data-Filter="ip out forward tcp"
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16
dstport!=telnet"
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16 icmp"
```

Monitoring and Maintaining the Template ACL Configuration

To monitor and maintain the configuration of the Template ACL feature, enter any of the following commands in EXEC mode:

Command	Purpose
Router# show access-list template summary	Displays information about all Template ACLs.
Router# show access-list template <i>acl-name</i>	Displays information about the named Template ACL.
Router# show access-list template exceed <i>number</i>	Displays the name of all Template ACLs serving as the parent for more than <i>number</i> child ACLs.
Router# show access-list template tree	Displays information about the entries in the Red-Black data tree.
Router# show pxf cpu access security	Displays PXF security ACL statistics. This command does not display statistics for individual child ACLs that are associated with a Template ACL. This command displays the Template ACL parent, with the total statistics for all the associated children ACLs.

Configuration Examples for Template ACLs

Template ACLs are activated only for per-user ACLs configured through RADIUS Attribute 242. For more examples of configuring RADIUS attributes, see [Chapter 16, “Configuring RADIUS Features.”](#)

access-list template Command

To enable Template ACL processing, use the **access-list template** command in global configuration mode. To disable Template ACL processing, use the **no** form of the command.

The Template ACL feature is enabled by default. The default number of rules for Template ACL status is 100, which is larger than most ACLs configured using Attribute 242.

Command	Purpose
Router(config)# access-list template <i>number</i>	Enables Template ACL processing. <i>number</i> specifies the maximum length of ACL that should be considered for template status. Only ACLs with <i>number</i> or fewer rules will be considered for template status. If the <i>number</i> variable is omitted, the default of 100 will be used, and only ACLs with 100 or fewer rules will be considered for template status. Default is 100 rules.

access-list template Command History

Cisco IOS Release	Description
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

access-list template Command Modes

Use this command in global configuration mode.

Usage Guidelines for the access-list template Command

Reducing the number of rules for Template ACL status can lower CPU utilization. The process of checking each ACL against other known ACLs in the system is easier if the matching task can be aborted earlier. However, if you set the number too low (smaller than the largest “similar” Attribute 242 ACL), CPU utilization can go very high, because ACLs that previously would be considered as Template ACL duplicates are now sent to the PXF without regard to other ACLs already in the router.

Setting the number of rules higher can increase CPU utilization, because the comparison task takes some CPU.



Note

Changes in CPU utilization occur only during session initiation. Steady-state CPU utilization is unaffected by these changes in ACL processing.

Examples

The following example specifies that ACLs with more than 50 rules will be considered for Template ACL status:

```
Router# access-list template 50
```

show access-list template Command

To display information about Template ACLs, use the **show access-list template** command in EXEC mode.

Command	Purpose
Router# show access-list template { summary <i>aclname</i> exceed number tree }	Displays information about ACLs. summary displays summary information. <i>aclname</i> displays information about the specified ACL. exceed number identifies Template ACLs that replace more than <i>number</i> individual ACLs. tree provides an easily readable summary of the frequency of use of each of the ACL types that the Template ACL function sees Output from this command includes the following information for each entry on the Red-Black tree: • CRC32 value • For each ACL associated with a particular CRC32: – Primary ACL name – Number of users of that ACL

show access-list template Command Modes

Use the **show access-list template** command in EXEC mode.

show access-list template Command History

Cisco IOS Release	Description
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Examples

This section provides examples of the different forms of the **show access-list template** command.

show access-list template summary

The following example shows output from the **show access-list template summary** command:

```
Router# show access-list template summary
Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

Output from this command includes:

- Maximum number of rules per Template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates

show access-list template *aclname*

The following examples show output from the **show access-list template *aclname*** command.

```
Router# show access-list template 4Temp_1073741891108
```

```
Showing data for 4Temp_1073741891108
4Temp_1073741891108 peer_ip used is 172.17.2.62,
is a parent, attached acl count = 98
currentCRC = 59DAB725
```

```
Router# show access-list template 4Temp_1342177340101
```

```
Showing data for 4Temp_1342177340101
4Temp_1342177340101 idb's ip peer = 172.17.2.55,
parent is 4Temp_1073741891108, user account attached to parent = 98
currentCRC = 59DAB725
```

Output from this display includes:

- Peer IP of the interface associated with the named Template ACL
- Name of the ACL serving as the primary user of the named Template ACL
- Number of ACLs matching the template of the named Template ACL
- Current cyclic redundancy check 32-bit (CRC32) value

show access-list template exceed *number*

The following example shows output from the **show access-list template exceed *number*** command:

```
Router# show access-list template exceed 49
```

```
ACL name          OrigCRC    Count    CalcCRC
4Temp_#120795960097 104FB543   50      104FB543
```

Table 2 describes the significant fields shown in the display.

Table 2 *show access-list template exceed Field Descriptions*

Field	Description
ACL Name	Name of the ACL that serves as the primary ACL for each template that exceeds <i>number</i> ACLs
OrigCRC	Original CRC32 value
Count	Count of ACLs that match the Template ACL
CalcCRC	Calculated CRC32 value

show access-list template tree

The following example shows output from the **show access-list template tree** command:

```
Router# show access-list template tree
```

```
ACL name          OrigCRC    Count    CalcCRC
4Temp_1073741891108 59DAB725   98      59DAB725
```

Table 3 describes the significant fields shown in the display.

Table 3 *show access-list template tree Field Descriptions*

Field	Description
ACL name	Name of an ACL on the Red-Black tree
OrigCRC	Original CRC32 value
Count	Number of users of the ACL
CalcCRC	Calculated CRC32 value

