

无线局域网控制器IDS签名参数

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[背景信息](#)

[控制器IDS参数](#)

[控制器IDS标准签名](#)

[IDS消息](#)

[Related Information](#)

[Introduction](#)

本文描述如何配置在Cisco无线LAN (WLAN)控制器软件版本3.2和以下版本的入侵检测系统(IDS)签名。

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

本文的信息根据WLAN控制器软件版本3.2和以上。

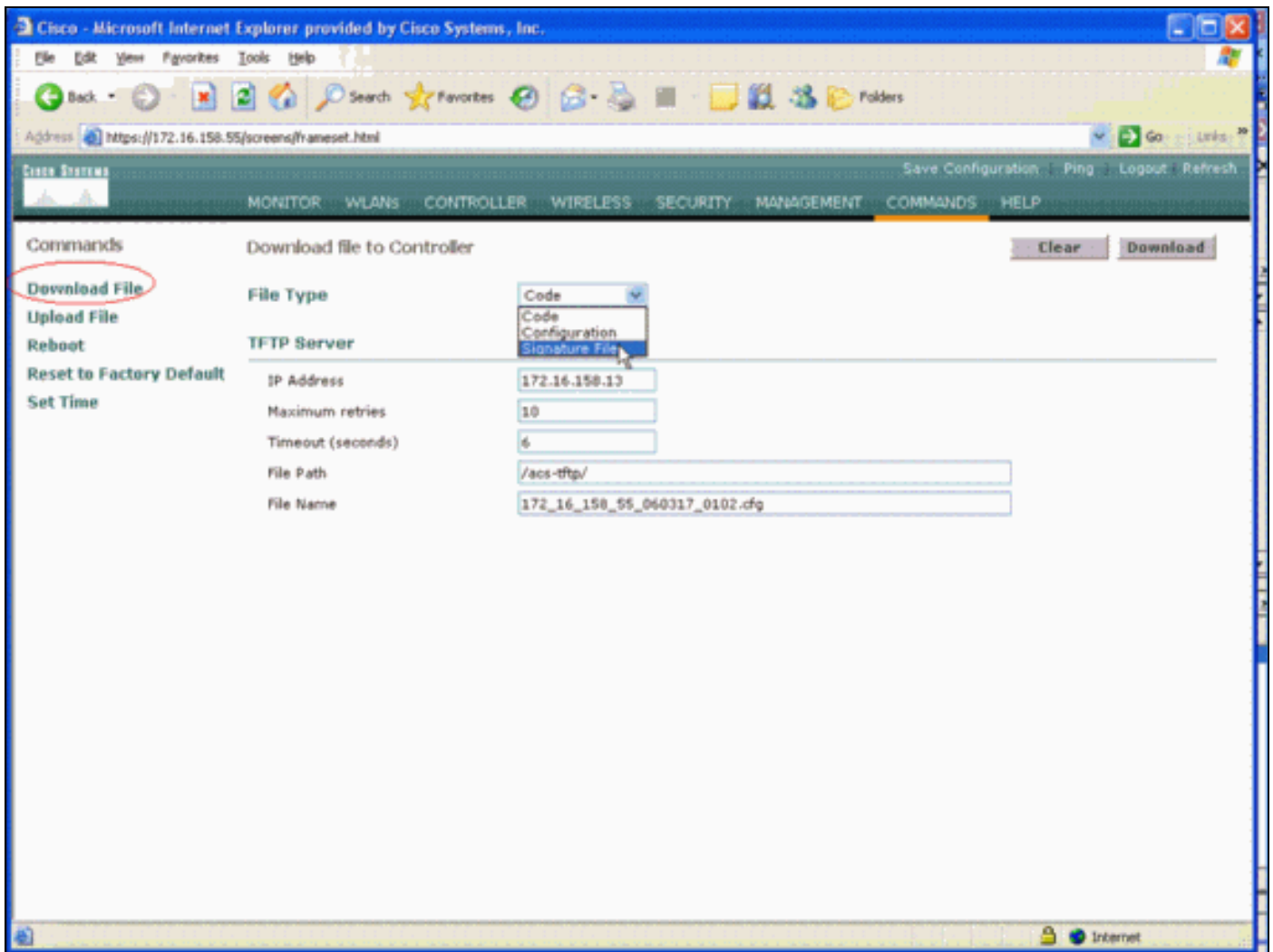
[Conventions](#)

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

[背景信息](#)

您能加载签名的IDS签名文件编辑(或文档检查)。选择**命令>上传文件>签名文件**。为了下载一个被修改的IDS签名文件，请选择**命令>下载File>签名文件**。在您下载一个签名文件到控制器后，所有接入点(APs)被连接到控制器在与新编出签名参数的实时被刷新。

此窗口表示如何下载签名文件：



每个IDS签名的IDS签名文本文件文件九参数。您能修改这些签名参数和写新的自定义签名。请参阅本文[控制器IDS](#)参数部分提供的格式。

控制器IDS参数

所有签名必须有此格式：

```
Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern =  
<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>,  
Desc = <str>
```

线路的最大长度是1000个字符。比1000长的线路没有正确地解析。

请开始#在IDS文本文件的所有线路认为备注和被跳过。并且被跳过所有空行，是与空白或换行符的线路。第一非注释，nonblank线路必须有关键字。如果文件是一个Cisco提供的签名文件，您不能更改值。Cisco使用此值管理签名文件版本。如果文件包含是由终端用户创建了签名，值一定是(=)。

您能修改的九个IDS签名参数是：

- **Name**=签名名字。这是识别签名的唯一字符串。名字的最大长度是20个字符。
- **Preced** =签名优先次序。指示签名优先次序在所有签名中的在签名文件被定义的这是唯一的ID。必须有每个签名一个Preced令牌。
- **FrmType** =帧类型。此参数能占用从<frmType-val>列表的值。必须有每个签名一个FrmType令牌。

<frmType-val>可以只是这两个关键字之一：mgmt<frmType-val>指示此签名是否发现数据或管理帧。

- =签名模式。令牌的值用于发现匹配签名的信息包。必须有每个签名至少一个令牌。可以有每个签名五个这样令牌。如果签名有超过一个这样令牌，信息包必须匹配所有令牌的值为了信息包能匹配签名。当AP收到一个信息包时，AP采取开始在<offset>，ANDs它与<mask>，并且结果与<pattern>字节流。如果AP查找匹配，AP凝视信息包与签名的匹配。<pattern-format>可以在相反的运算符之后“!”。在那种情况下，FAIL匹配操作此部分描述凝视与签名的匹配的所有信息包。
- Freq =在信息包/间隔的数据包匹配频率。此令牌的值指示多少个信息包每个测量间隔必须匹配此签名，在签名被执行前。值为0表明签名每次采取信息包匹配签名。此令牌的最大值是65,535。必须有每个签名一个Freq令牌。
- =测量间隔以秒钟。此令牌的值指示阈值的时间(即Freq)指定。DEFAULT值此令牌的是1秒。此令牌的最大值是3600。
- =平静的时间以秒钟。此令牌的值指示必须通过的时间哪些期间AP不收到匹配签名的信息包，在AP确定前签名指示消退的攻击。如果Freq令牌的值是0，此令牌被忽略。必须有每个签名一个令牌。
- Action=签名动作。这指示什么AP必须执行，如果信息包匹配签名。此参数能占用从<action-val>列表的值。必须有每个签名一个令牌。<action-val>可以只是这两个关键字之一：=不执行。
=报告对交换机的匹配。
- Desc =签名说明。这是描述签名的目的字符串。当签名匹配在简单网络管理协议(SNMP)陷阱时报告，此字符串被提供给陷阱。说明的最大长度是100个字符。必须有每个签名一个Desc令牌。

控制器IDS标准签名

这些IDS签名装备控制器作为“标准的IDS签名”。因为[控制器IDS](#)参数部分描述，您能修改所有这些签名参数。

```
Revision = 1.000
```

```
Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,  
Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast  
Deauthentication Frame"
```

```
Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern =  
0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc =  
"NULL Probe Response - Zero length SSID element"
```

```
Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern =  
0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc =  
"NULL Probe Response - No SSID element"
```

```
Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF,  
Freq=50, Quiet = 600, Action = report, Desc="Association Request flood"
```

```
Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF,  
Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood"
```

```
Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF,  
Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood"
```

```
Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern =  
0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600,  
Action = report, Desc="Broadcast Probe Request flood"
```

Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF, Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood"

Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF, Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood"

Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF, Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7"

Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF, Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D"

Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF, Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F"

Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF, Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood Attack"

Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern = 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern = 36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0"

Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern = 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern = 36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3"

Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern = 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern = 36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0"

Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern = 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler"

Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF, Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569:0xff, Freq = 1, Quiet = 600, Action = report, Desc="Wellenreiter"

[IDS消息](#)

使用无线局域网控制器版本4.0，您也许收到此IDS消息。

Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx, Slot ID 0 and Source MAC 00:00:00:00:00:00

此IDS消息表明在无线802.11帧的802.11网络分配向量(NAV)字段太大，并且无线网络也许受到DOS攻击(或有一个行为不端的客户端)。

在您收到此IDS消息后，下一步是搜寻触犯的客户终端。您必须找出根据其信号强度的客户终端用一个无线嗅探器区域在接入点附近或使用位置服务器精确定位其位置。

NAV字段是用于的虚拟载波侦听机制缓和在隐藏的终端(当前无线客户端不能发现的无线客户端之间的冲突，当传输)时802.11发射的。隐藏的终端制造问题，因为接入点也许从能传达给接入点的两个客户端收到信息包，但是不接受彼此的发射。当这些客户端同时传输，他们的信息包碰撞在接入点，并且这不导致清楚地收到信息包的接入点。

每当无线客户端要发送数据包到接入点，实际上传输称为RTS-CTS-DATA-ACK数据包序列的四个数据包顺序。四个802.11帧中的每一个运载指示微秒的数量信道留给由无线客户端的一个NAV字段

。在无线客户端和接入点之间的RTS/CTS握手期间，无线客户端发送包括足够大一个NAV间隔完成整个顺序的一个小的RTS帧。这包括CTS帧、数据帧和随后的确认帧从接入点。

当无线客户端传输其与设置时的NAV的RTS信息包，被传输的值用于设置在其他无线客户端的NAV计时器被关联对接入点。接入点回复RTS信息包从有在数据包序列期间，包含更新的新的NAV值占时间已经流逝的CTS信息包的客户端。在发送后CTS信息包，能从接入点接受的每个无线客户端更新他们的NAV计时器并且延迟所有发射，直到他们的NAV计时器到达0。这保持信道自由为了无线客户端能完成传达信息包的进程给接入点。

攻击者也许通过主张在NAV字段的大时光利用此虚拟载波侦听机制。这防止其他客户端传送信息包。NAV的最大值是在802.11b网络的32767或者大致32毫秒。因此在理论上攻击者只需要传输大致30个信息包每秒钟阻塞对信道的所有访问。

[Related Information](#)

- [Cisco 4400 系列无线局域网控制器](#)
- [Cisco 4100 系列无线局域网控制器](#)
- [Cisco 2000 系列无线局域网控制器](#)
- [Cisco入侵检测系统签名引擎版本3.1](#)
- [Technical Support & Documentation - Cisco Systems](#)