# 无线局域网控制器IDS签名参数

## 目录



## 简介

本文档介绍如何在思科无线局域网(WLAN)控制器软件版本3.2及更低版本中配置入侵检测系统(IDS)签名。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于WLAN控制器软件版本3.2及更高版本。

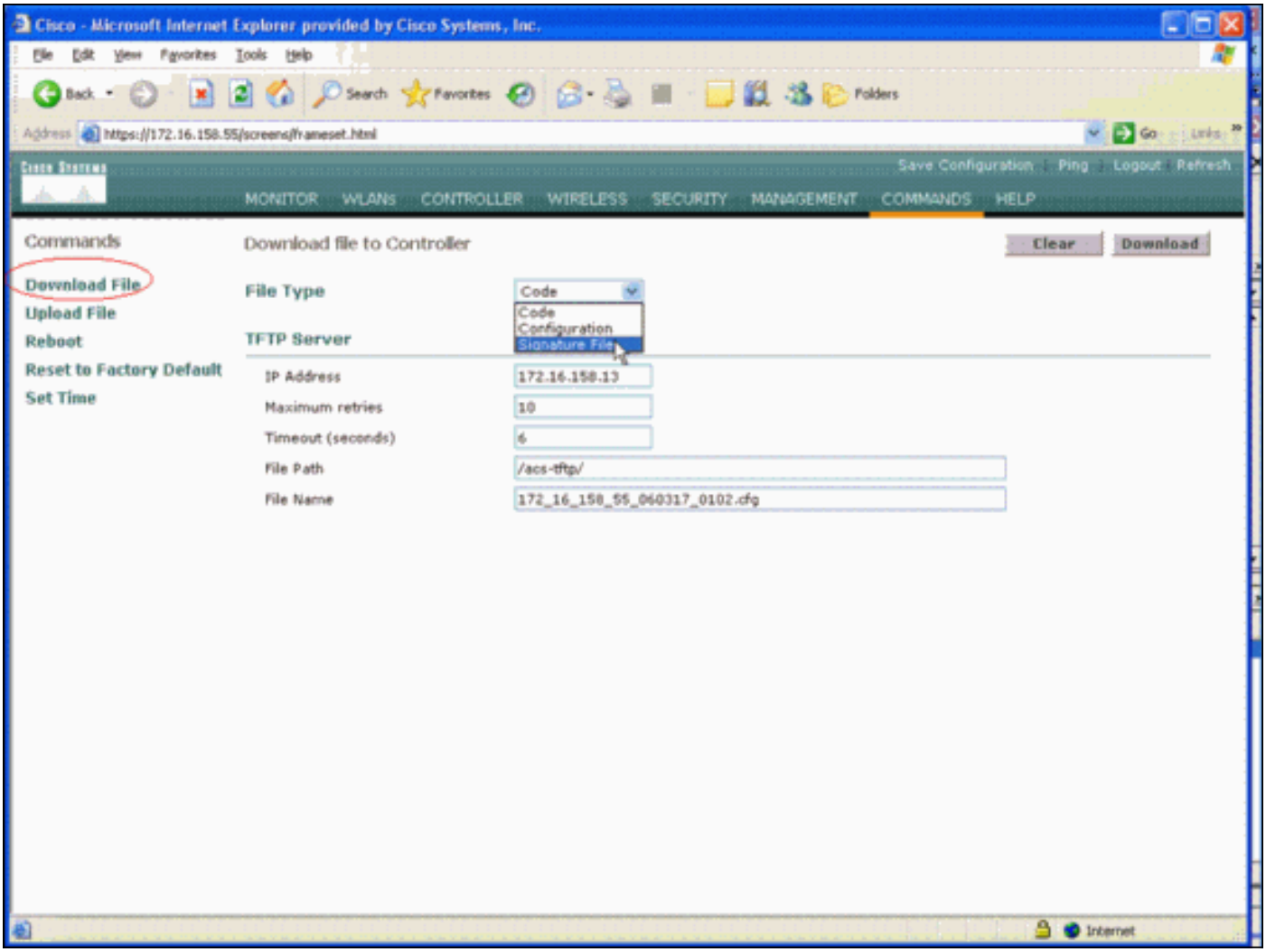
### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## 背景信息

您可以上传IDS签名文件以进行签名编辑（或文档审阅）。 选择**Commands > Upload File > Signature File**。要下载修改的IDS签名文件，请选择**Commands > Download File > Signature File**。将签名文件下载到控制器后，连接到控制器的所有接入点(AP)都会使用新编辑的签名参数实时刷新。

此窗口显示如何下载签名文件：




IDS签名文本文件记录每个IDS签名的九个参数。您可以修改这些签名参数并编写新的自定义签名。请参阅本文档的"控制器IDS参数"部分提供的格式。

## 控制器IDS参数

所有签*名必*须具有以下格式：

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

行的最大长度为1000个字符。长度超过1000的行未正确解析。

IDS文本文件中以#头的所有行均被视为注释并被跳过。还跳过了所有空行，这些行仅包含空格或换行符。第一个非注释非空行*必须*具有关键字Revision。如果文件是思科提供的签名文件，则不能更改修订版。思科使用此值管理签名文件版本。如果文件包含由最终用户创建的签名，则Revision的值*必*是自定义(Revision = custom)。

可修改的九个IDS签名参数是：

- =签名名称。这是标识签名的唯一字符串。名称的最大长度为20个字符。
- =签名优先级。这是唯一ID，指示签名在签名文件中定义的所有签名中的优先级。每个签名必一个Preced令牌。
- **FrmType** =帧类型。此参数可以从<frmType-val>值。每个签名必须一个FrmType令牌。

<frmType-val>只能是以下两个关键字之一：mg<frmType-val>此签名是否检测到数据或管理帧。

- =签名模式。令牌值用于检测与签名匹配的数据包。每个签名必须至一个模式令牌。每个签名最多可以有五个此类令牌。如果签名有多个此类令牌，则数据包必须匹配所有令牌的值才能使数据包匹配签名。当AP收到数据包时，AP会获取以<offset>，并将其与<mask>进行AND运算，并将结果与<pattern>。如果AP发现匹配项，则AP认为数据包与签名匹配。<pattern-format>前面可以有否定运算符"!"。 在这种情况下，本部分描述的匹配操作失败的所有数据包都被视为与签名匹配。
- =数据包/间隔中的数据包匹配频率。此令牌的值指示在执行签名操作之前，每个测量间隔必须匹配此签名的数量。值0表示每次数据包与签名匹配时执行签名操作。此令牌的最大值为65,535。每个签*名必*须有Freq令牌。
- =测量间隔（秒）。此令牌的值指示阈值（即，Freq）指定的时段。此令牌的默认值为1秒。此令牌的最大值为3600。
- =安静时间（秒）。此令牌的值表示在AP确定签名所指示的攻击已消退之前，AP必须经过的时间量，在此期间AP不会接收与签名匹配的数据包。如果Freq令牌的为0，则忽略此令牌。每个签名必须一个Quiet令牌。
- =签名操作。这表示如果数据包与签名匹配，AP必须执行什么操作。此参数可以从<action-val>值。每个签名必须一个操作令牌。<action-val>只能是以下两个关键字之一：=无所事事。report =向交换机报告匹配项。
- **Desc** =签名说明。这是描述签名用途的字符串。当在简单网络管理协议(SNMP)陷阱中报告签名匹配时，此字符串将提供给陷阱。说明的最大长度为100个字符。每个签名必须一个Desc令牌。

# 控制器IDS标准签名

这些IDS签名随控制器一起提供，作为“标准IDS签名”。您可以修改所有这些签名参数，如控制器IDS参数部分所述。

```
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:0xFFFFFF, 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:0xFFFFFF, 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:0xFFFFFF, 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:0xFFFFFF, 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:
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
Action = report, Desc="Wellenreiter"
```

## IDS消息

使用无线LAN控制器版本4.0时，您可能会收到此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消息表示无线802.11帧中的802.11网络分配矢量(NAV)字段太大，无线网络可能受到DOS攻击（或存在行为不正的客户端）。

收到此IDS消息后，下一步是跟踪违规的客户端。您必须根据客户端的信号强度在接入点周围的区域使用无线嗅探器来定位客户端，或使用定位服务器来定位其位置。

NAV字段是虚拟载波侦听机制，用于缓解802.11传输中隐藏终端（当前无线客户端在传输时无法检测到的无线客户端）之间的冲突。隐藏的终端会产生问题，因为接入点可能会从两个客户端接收数据包，这些数据包可以传输到接入点，但不会相互接收传输。当这些客户端同时传输时，其数据包在接入点发生冲突，这会导致接入点不清楚地接收任何数据包。

无线客户端每当想要向接入点发送数据包时，就会实际发送一个四数据包序列，称为RTS-CTS-

DATA-ACK数据包序列。四个802.11帧中的每个帧都带有一个NAV字段，该字段指示无线客户端为信道保留的微秒数。在无线客户端和接入点之间的RTS/CTS握手期间，无线客户端发送一个小的RTS帧，该帧包含足够大的NAV间隔，以完成整个序列。这包括来自接入点的CTS帧、数据帧和后续确认帧。

当无线客户端使用NAV集传输其RTS分组时，所传输的值用于在与接入点相关联的所有其他无线客户端上设置NAV计时器。接入点用包含更新的新NAV值的CTS数据包回复来自客户端的RTS数据包，该新NAV值用于说明在数据包序列期间已经经过的时间。发送CTS数据包后，可以从接入点接收的每个无线客户端都更新了其NAV计时器，并将所有传输都延迟到其NAV计时器达到0。这使无线客户端可以保持信道空闲，以完成向接入点传输数据包的过程。

攻击者可能会通过在NAV字段中断言大量时间来利用此虚拟载波侦听机制。这会阻止其他客户端传输数据包。NAV的最大值为32767，或802.11b网络上大约32毫秒。因此，理论上，攻击者只需每秒传输大约30个数据包，即可阻塞对信道的所有访问。

## 相关信息

- 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
- 思科入侵检测系统签名引擎版本3.1
- 技术支持和文档 - Cisco Systems