网桥安全

Contents

Introduction

当设计以太网段之间时的一条桥接的无线链路安全是重要的考虑因素。本文展示如何获取流过一条桥接的无线链路的数据流使用IPSec隧道。

在本例中，两Cisco Aironet 350系列网桥设立WEP;两路由器设置IPSec隧道。

Prerequisites

Requirements

在尝试此配置前，请保证您对使用满意这些：

- Cisco Aironet网桥配置接口
- Cisco IOS line命令接口

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行IOS版本12.1的Cisco 2600系列路由器
- 运行固件版本11.08T的Cisco Aironet 350系列网桥

本文档中的信息都是基于特定实验室环境中的设备创建的。All of the devices used in this document started with a cleared (default) configuration.如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

背景理论

Cisco Aironet 340， 350和1400系列网桥提供至128-bit WEP加密。这不可能为安全连接由于在WEP算法的著名的问题和开发方便取决于，正如WEP算法的安全所描述 和在Cisco Aironet回应按-在802.11安全的缺点。

强化在一条无线桥接链路间通过的数据流安全一个方法将创建流过链路的一条被加密的路由器IPSEC隧道。因为网桥运行在OSI模型的第2层，这工作。您能运行IPSec路由器到路由器在连接在网桥之间。

如果包含破坏无线链路的安全，数据流依然是加密并且巩固。

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

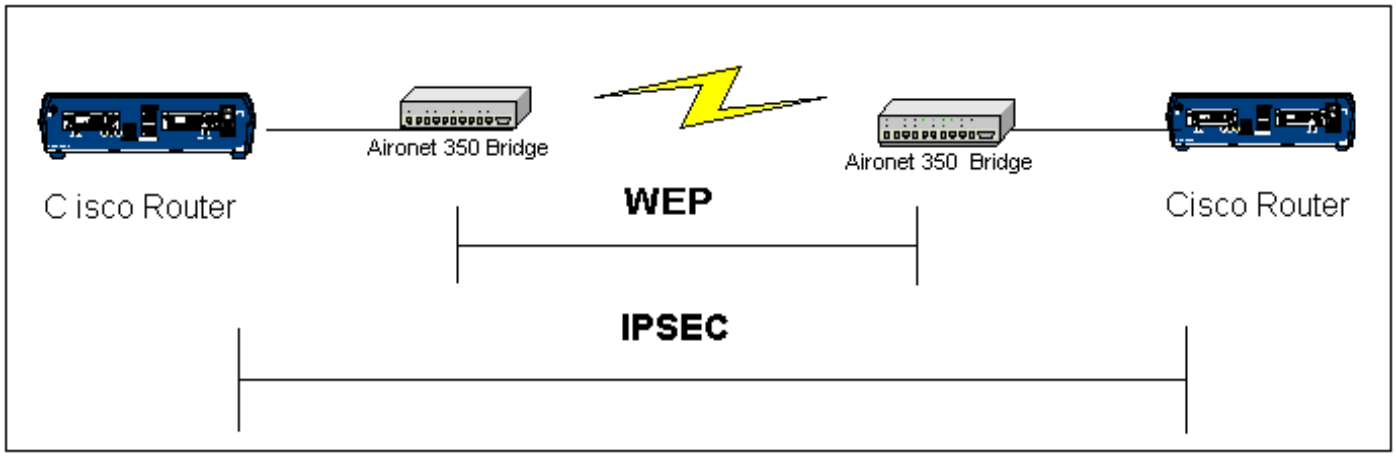
Configure

此部分引见信息配置在本文描述的功能。

Note: 要寻找关于用于本文的命令的其他信息，请使用ios命令查找工具。

Network Diagram

本文档使用此图中所示的网络设置：



配置

本文档使用以下配置：

- RouterA
- RouterB
- 网桥示例

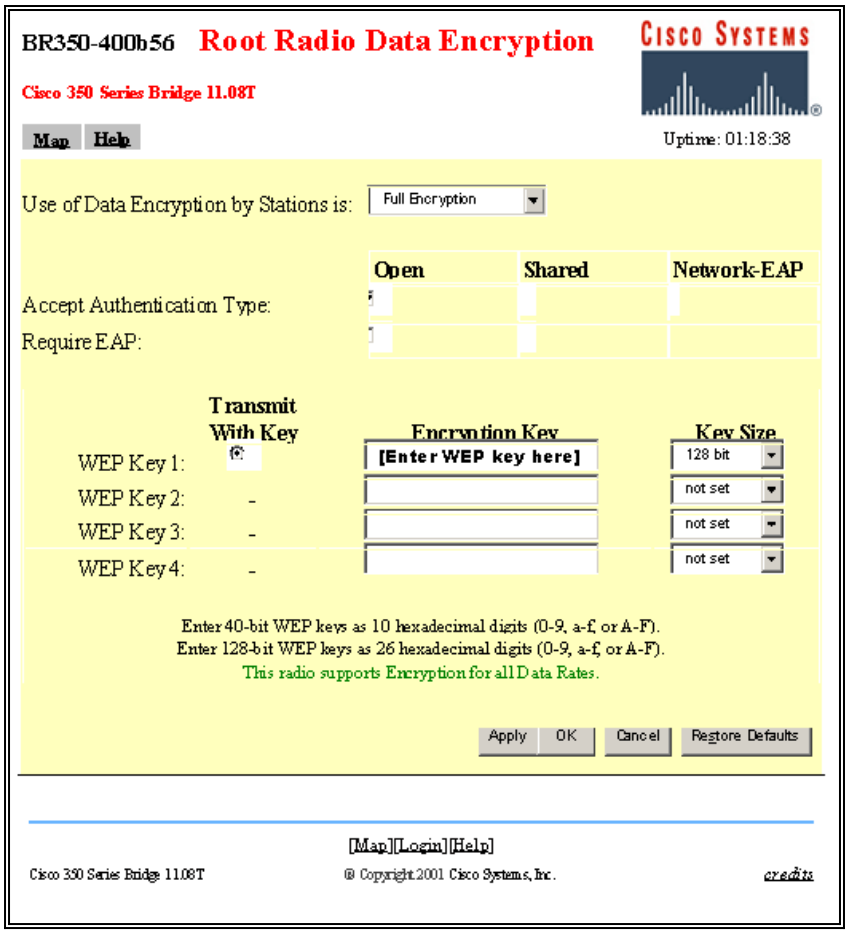
RouterA (Cisco 2600 Router)

```
RouterA#show running-config
Building configuration...

Current configuration : 1258 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
ip dhcp excluded-address 10.1.1.20
ip dhcp excluded-address 10.1.1.30
!
ip dhcp pool wireless
 network 10.1.1.0 255.255.255.0
!
ip audit notify log
ip audit po max-events 100
call rsvp-sync
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco address 10.1.1.30
!
!
crypto ipsec transform-set set esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.30
set transform-set set
match address 120
!
interface Loopback0
ip address 20.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 10.1.1.20 255.255.255.0
crypto map vpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.30
no ip http server
no ip http cable-monitor
!
access-list 120 permit ip 20.1.1.0 0.0.0.255 30.1.1.0
0.0.0.255
!
!
line con 0
transport input none
line vty 0 4
!
end
```

RouterB (Cisco 2600 Router)

```
RouterB#show running-config
Building configuration...

Current configuration : 1177 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
call rsvp-sync
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco address 10.1.1.20
!
!
crypto ipsec transform-set set esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.20
set transform-set set
match address 120
interface Loopback0
ip address 30.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 10.1.1.30 255.255.255.0
no ip mroute-cache
crypto map vpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.20
no ip http server
no ip http cable-monitor
!
access-list 120 permit ip 30.1.1.0 0.0.0.255 20.1.1.0
0.0.0.255
!
!
line con 0
transport input none
line vty 0 4
login
!
end
```

Cisco Aironet网桥



Verify

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto engine connections active** -此命令用于查看当前活动加密的会话连接

```
RouterA#show crypto engine connection active
  ID Interface   IP-Address      State Algorithm            Encrypt Decrypt
   1 Ethernet0   10.1.1.20       set   HMAC_MD5+DES_56_CB         0       0
2002 Ethernet0   10.1.1.20       set   HMAC_MD5+3DES_56_C         0       3
2003 Ethernet0   10.1.1.20       set   HMAC_MD5+3DES_56_C         3       0

RouterB#show crypto engine connection active
  ID Interface    IP-Address     State Algorithm            Encrypt Decrypt
   1  <none>          <none>     set   HMAC_MD5+DES_56_CB         0       0
2000 Ethernet0    10.1.1.30      set   HMAC_MD5+3DES_56_C         0       3
2001 Ethernet0    10.1.1.30      set   HMAC_MD5+3DES_56_C         3       0
```

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

要排除IPSec连通性故障，请参见以下：

- IP安全故障排除-了解和使用debug命令
- Cisco 网络层加密的配置与故障排除：IPSec和ISAKMP、第1部分和第2部分

关于排除无线连接故障，请参见以下：

- TAC案例收集工具-无线局域网
- 无线桥接网络常见问题故障排除
- 排除在无线LAN网络的连接故障

Related Information

- **技术支持-无线局域网**
- **技术支持- IPSec协商/IKE协议**
- Technical Support - Cisco Systems