CBWIPS

宽带无线IP标准工作组标准

CBWIPS/Z XXX—XXXX

无线局域网系统互操作技术要求和测试方法

Technical Requirements and Testing Methods for WLAN System Interoperability

（征求意见稿）

（本稿完成日期：2011 年 12 月）

××××-××-××发布　　××××-××-××实施

工业和信息化部宽带无线 IP 标准工作组　发布

目　　次

前　言

本指导性技术文件由工业和信息化部宽带无线 IP 标准工作组和 WAPI 产业联盟共同提出，由工业和信息化部宽带无线 IP 标准工作组归口。

本指导性技术文件主要起草单位：工业和信息化部宽带无线 IP 标准工作组“无线局域网自动配置与访问技术”标准项目组、WAPI 产业联盟“无线局域网自动配置与访问技术”产品方案组、xxxxxx（以后补充）

本指导性技术文件主要起草人：xxxxxx（以后补充）

CBWIPS/Z ××××.××—××××

无线局域网系统互操作技术要求和测试方法

1 范围

本指导性技术文件确保所有符合 GB15629.11 系列标准的无线局域网产品，可以有效的减少产品之间的不兼容问题，增强产品之间的传输性能。

本指导性技术文件适用于符合 GB15629.11 系列标准的家庭、小型办公应用场景中使用的以及运营商用场景中使用的无线局域网设备。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB15629.11－2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范(ISO/IEC 8802.11:1999，MOD)

GB15629.11－2003/XG1－2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

GB15629.1101－2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：5.8GHz频段高速物理层扩展规范（ISO/IEC8802-11:1999/Amd 1:2000，MOD）

GB15629.1102－2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：2.4GHz频段较高速物理层扩展规范

GB15629.1104－2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：2.4GHz频段更高数据速率扩展规范（ISO/IEC8802-11:2005/Amd 4:2005，MOD）

GB/T 16264.8-2005 信息技术 开放系统互连 目录 公钥和属性证书框架（ISO/IEC9594-8:2005||ITU-T X.509，IDT）

CBWIPS-Z 010-2009 《多信任证书实施技术》指导性技术文件(发布版)

3 定义

GB15629.11系列标准确立的术语和定义及下列术语和定义适用于本指导性技术文件文件。

3.1

服务集标识(SSID) service set identifier (SSID)

ESS的标识，在同一ESS内的所有STA和AP应具有相同的SSID，SSID为0~32个八位位组的字符串。

3.2

无线局域网(WLAN) Wireless Local Area Network (WLAN)

一种通过无线电、红外光信号或其他技术发送和接收数据，不要求在各个结点和集线器之间有物理连接（例如，采用导线或同轴电缆等）的局域网。无线局域网通常用于用户携带可移动终端（例如，便捷式计算机、移动用户终端等）的办公、工厂及公众等环境中。

3.3

GB15629.11 系列标准协议测试平台

一种可以抓取有线以及无线以太网帧，并能够对其结构和格式进行解析的工业计算机，本测试平台可以对所有 WAPI 协议流程和数据格式是否完整和正确进行判别。

3.4

移动终端 Mobile Terminal

可以在移动中使用网络进行通讯的计算机设备（例如，安装有操作系统的智能手机、便携式计算机、移动互联网设备、车载计算机等）。

4 缩略语

下列缩略语适用于本指导性技术文件。

AP	Access Point	接入点
APUT	Access Point Under Test	被测接入点
ASCII	American Standard Code for Information interchange	美国国家信息交换标准代码
ASU	Authentication Service Unit	鉴别服务单元
ASUT	Authentication Server Under Test	被测鉴别服务器
BK	Based Key	基密钥
BSS	Basic Service Set	基本服务集
CTS	Clear to Send	清除待发
CW	Contention Window	竞争窗口
DTIM	Delivery Traffic Indication Map	交付通信量指示消息
ERP	Extended Rate PHY	增强速率物理层
IBSS	Independent Basic Service Set	独立基本服务集
MAC	Medium Access Control	媒体访问控制
MTUT	Mobile Terminal	移动终端
NAV	Network Allocation Vector	网络分配向量
PS	Power Save	节能（模式）
RTS	Request to Send	请求发送
SSID	Service Set Identifier	服务集标识
STA	Station	端站
STAUT	Station Under Test	被测端点
TIM	Traffic Indication Map	通信量指示图
WAI	WLAN Authentication Infrastructure	无线局域网鉴别基础结构
WAPI	WLAN Authentication and Privacy Infrastruction	无线局域网鉴别与保密基础架构
WIE	WAPI Information element	WAPI 信息元素
WLAN	Wireless Local Area Network	无线局域网
WPI	WLAN Privacy Infrastruction	无线局域网保密基础架构

5 设备要求

5.1 被测 STA

厂商应根据第7章中对无线局域网基本功能实体（站点）规定的技术要求来准备被测设备；

STA必须检测7.1节中的所有项。

下文中所有被测STA均用STAUT代替表示。

5.2 被测移动终端

厂商应根据第7章中对无线局域网基本功能实体（移动终端）规定的技术要求来准备被测设备；

移动终端必须检测7.2节中的所有项。还需检测7.1.1.1节的基础协议检测和7.1.1.2节的WAPI协议检测中的所有项。

下文中所有被测移动终端均用MTUT代替表示。

5.3 被测 AP

厂商应根据第7章中对无线局域网基本功能实体（接入点）规定的技术要求来准备被测设备；

AP必须检测7.3节中的所有项。

下文中所有被测AP均用APUT代替表示。

5.4 被测 ASU

厂商应根据第7章中对鉴别服务单元规定的技术要求来准备被测设备；

ASU必须检测7.4节中的所有项。

下文中所有被测ASU均用ASUT代替表示。

6 技术要求

6.1 服务集标识（SSID）元素

无线局域网基本功能实体中的站点、接入点和移动终端需满足此项技术要求。

无线局域网基本功能实体所使用的服务集标识元素应该满足如下要求。

1. SSID应至少支持GB 1988-1989字符集印刷字体，并且不以GB 1988-1989字符集字符NULL为终止；
2. SSID若支持中文，应采用GB2312编码；
3. SSID应为0-32字符（若为中文时应为0-16汉字），SSID长度为0时应被视为广播SSID；
4. SSID应区分大小写；
5. AP必须回应广播的SSID探询请求。

6.2 信道

无线局域网基本功能实体中的站点、接入点和移动终端需满足此项技术要求。

无线局域网基本功能实体的信道应满足如下要求。

1. 在GB 15926.1104或GB 15926.1102模式下，STA、移动终端和AP能够工作在1-13的任意一个信道上；
2. 在GB 15926.1101模式下，STA、移动终端和AP能够工作在149-165的任意一个信道上。

6.3 信标帧间隔

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体的信标帧间隔应满足如下要求。

1. STA应支持100ms-1000ms内的任意信标帧间隔；
2. AP应至少支持100ms-1000ms内的某一信标帧间隔。

6.4 TIM

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体对其产生和解析TIM应满足如下要求。

1. AP必须能产生正确的TIM给处于节电模式的STA；
2. 处于节电模式的STA必须能正确解析TIM。

6.5 报文响应时间

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的报文响应时间应满足如下要求。

1. 若信道空闲，探询响应应在收到探询请求后5ms内发出；STA在发出探询请求后，等待响应的时间应至少为5ms；
2. 若AP空闲，应在100ms内发出链路验证响应、关联或重关联响应；STA在发出链路验证请求、关联或重关联请求后，等待响应的时间至少为100ms。

6.6 数据速率

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的传输数据速率应满足如下要求。

1. STA、移动终端和AP能够工作在1Mbit/s、2Mbit/s、5.5Mbit/s、11Mbit/s、6Mbit/s、9Mbit/s、12Mbit/s、18Mbit/s、24Mbit/s、36Mbit/s、48Mbit/s、54Mbit/s中的任一种数据速率下；
2. STA和AP能够工作在以1Mbit/s、2Mbit/s、5.5Mbit/s、11Mbit/s为基本速率集，以6Mbit/s、
3.
4. 9Mbit/s、12Mbit/s、18Mbit/s、24Mbit/s、36Mbit/s、48Mbit/s、54Mbit/s为可支持速率集的BSS中；
5. STA和AP能够工作在以1Mbit/s、2Mbit/s、5.5Mbit/s、11Mbit/s、6Mbit/s、12Mbit/s、24Mbit/s为基本速率集，以9Mbit/s、18Mbit/s、36Mbit/s、48Mbit/s、54Mbit/s为可支持速率集的BSS中。

6.7 节电模式

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体对其支持的节电模式应满足如下要求。

1. STA不强制要求支持节电模式；
2. AP必须支持处于节电模式的STA；
3. AP必须支持STA在节电模式与非节电模式之间的动态切换；
4. STA如果支持节电模式，当其处于节电模式下，能够正确解析AP信标帧内的DTIM信息，并据此正确接收发往自己的单播业务或广播组播业务；
5. AP必须能生成间隔为1-5的DTIM；
6. AP应该忽略接收到的广播、组播探询请求帧中的“功率管理”位；
7. AP应该忽略接收到的链路验证、关联或重关联帧中的“功率管理”位，且AP能够假定STA处于非节电状态等待接收链路验证响应、关联或重关联响应。

6.8 对 PS-Poll 帧的处理

无线局域网基本功能实体中的接入点需要满足此项技术要求。

无线局域网基本功能实体对PS-Poll帧处理应满足如下要求。

1. 当收到的PS-Poll来自未关联的STA时，应发回确认帧，并跟随以解除链路验证帧或解除关联帧；
2. 当收到的PS-Poll来自已关联的STA时，响应应为下列类型之一：确认帧；数据帧；Null或空数据帧；确认帧+数据帧、或Null数据帧、或空数据帧。

6.9 对错误帧的处理

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体对错误帧的处理应满足如下要求。

1. STA、移动终端和AP能够正确解析所接收MAC帧帧头中的各个字段。
2. 当所接收MAC帧帧头中含有错误或不可识别信息时，STA、移动终端和AP能够丢弃该错误帧；
3. STA、移动终端和AP应忽略未知类型的信息元素。

6.10 对 Null 数据帧的处理

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体对Null数据帧的处理应满足如下要求。

1. STA、移动终端和AP能够在收到Null数据帧后仍能正常工作；
2. 当从一个未通过链路验证或未关联的STA收到Null数据帧的时候，AP能够返回解除链路验证帧或解除关联帧；
3. Null帧中的控制位是有效的（例如，功率管理位。）

6.11 RTS/CTS

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体对其接收RTS并产生CTS应满足如下要求。

1. STA和AP能够正确接收RTS并产生CTS；
2. 不强制要求STA和AP能够产生RTS；
3. 如果符合GB 15629.11-2003或GB 15629.1102-2003的STA关联到AP，则AP必须设置用户保护位；
4. 如果AP设置了用户保护位，则STA必须采用RTS或CTS-to-self保护机制。

6.12 分段

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体对其发送和接收分段报文能力应满足如下要求。

1. STA和AP能够正确接收分段的报文；
2. 不强制要求STA和AP能够发送分段报文。

6.13 关联或重关联

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体对其关联或重关联能力应满足如下要求。

1. STA、移动终端可以关联或重关联到相同SSID的其他AP，并可以与关联或重关联上的新AP正常通信。

6.14 对保留位的处理

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体对其接收和发送帧的保留位应满足如下要求。

1. STA、移动终端和AP能够忽略接收帧中的保留位；
2. STA、移动终端和AP发送帧的保留位应置位0。

6.15 IBSS

无线局域网基本功能实体中的站点需满足此项技术要求。

无线局域网基本功能实体在IBSS模式下应满足如下要求。

1. STA应能创建IBSS，并允许其他STA加入IBSS；
2. 应能以指定SSID和信道创建IBSS；
3. 支持的基本速率集至少包括1Mbit/s，2 Mbit/s，5.5 Mbit/s，11 Mbit/s；
4. IBSS的BSSID应为随即选择；
5. 允许其他STA以主动扫描或被动扫描的方式加入；
6. 在IBSS中，STA应支持分布式信标帧的产生，当创建IBSS的STA离开后，该IBSS内其他STA应仍可以正常通信；
7. 当采用相同信道的两个IBSS具有不同的SSID时，分属于不同SSID的STA之间不能相互通信；
8. IBSS中不采用链路验证；
9. IBSS中不采用电源管理；
10. 必须能够接收以RTS/CTS机制发送的数据包；
11. 必须能够接收分段数据包
12. 必须能够发送和接收广播/组播帧。

6.16 前导码

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的前导码应满足如下要求。

1. 默认条件下STA、移动终端和AP必须允许使用长导码进行通信；
2. STA、移动终端和AP必须支持短前导码；
3. 用户保护机制采用基于ERP信息元素中“巴克前导码模式”指示的短前导码或长前导码。

6.17 NAV

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体使用NAV时应满足如下要求。

1. STA、移动终端和AP必须采用并非发送给自己的有效帧中的持续时间。

6.18 CWmin

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体使用CWmin时应满足如下要求。

1. STA、移动终端和AP必须支持值为15的CWmin。

6.19 短时隙时间

无线局域网基本功能实体中的站点和接入点需满足此项技术要求。

无线局域网基本功能实体的短时隙时间应满足如下要求。

1. STA和AP必须支持短时隙时间选型；
2. IBSS模式下不允许短时隙。

6.20 WAPI 基本要求

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体对其具备的WAPI安全协议功能应满足如下要求。

1. 在GB 15629.11系列标准中定义了无线局域网的两种工作模式：BSS模式和IBSS模式。WAI安全机制分为WAI证书鉴别和密钥管理方式以及WAI预共享密钥鉴别和密钥管理方式。WAI证书鉴别和密钥管理方式中采用证书完成鉴别、密钥协商、组播密钥通告实现接入控制；WAI预共享密钥鉴别和密钥管理方式采用预共享密钥完成单播密钥协商、组播密钥通告实现接入控制；
2. 在BSS模式的WAI证书鉴别和密钥管理方式中，实现WAPI安全机制所需的完整的系统由三部分组成，分别为鉴别请求实体、鉴别器实体和鉴别服务实体；
3. 在BSS模式的WAI预共享密钥鉴别和密钥管理方式中，实现WAPI安全机制所需的完整的系统由两部分组成，分别为鉴别请求实体和鉴别器实体；
4. 在IBSS模式的WAI预共享密钥鉴别和密钥管理方式中，实现WAPI安全机制所需的完整的系统由两部分组成，分别为鉴别请求实体（同时作为鉴别请求实体和鉴别器实体）和鉴别请求实体；
5. 在WAI证书鉴别和密钥管理方式及WAI预共享密钥鉴别和密钥管理方式中，STA和AP都应支持启用或关闭WAPI，当任何一方启用WAPI后，STA若未与AP成功完成WAI过程，STA与AP无法通信；当双方的WAPI设置不一致时，STA与AP无法通信；
6. 移动终端和AP必须支持WAI证书鉴别和密钥管理，支持WAI预共享密钥鉴别和密钥管理；
7. STA必须支持WAI预共享密钥鉴别和密钥管理，IBSS模式下WAI证书鉴别和密钥管理方式可选；

6.21 WAI 证书鉴别和密钥管理中的证书管理

无线局域网基本功能实体中的站点、移动终端、接入点和鉴别服务单元需满足此项技术要求。

无线局域网基本功能实体的证书管理能力应满足如下要求。

1. ASU至少能生成8张证书；
2. ASU生成证书时，可以设置证书的有效期；
3. ASU能够吊销已激活的证书；
4. STA（支持WAI证书鉴别和密钥管理套件）和移动终端能够安装来自不同ASU颁发的多张证书，能够删除所安装的证书；
5. AP能够安装ASU颁发的证书；
6. STA（支持WAI证书鉴别和密钥管理套件）、移动终端、AP和ASU必须支持X.509 v3证书；
7. ASU能够生成P12格式的证书。
8. STA（支持WAI证书鉴别和密钥管理套件）、移动终端和AP能够安装ASU颁发的P12格式的证书。

6.22 WAPI 中的密钥管理

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的密钥管理能力应满足如下要求。

1. WAI预共享密钥应通过手工设置获得，预共享密钥的设置应支持ASCII字符和十六进制数两种输入模式，密钥长度限定为8-64位。

6.23 WAPI 中的动态密钥更新

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的动态密钥更新能力应满足如下要求。

1. STA、移动终端和AP能够正确响应对方发送的动态密钥更新请求（基密钥和单播会话密钥）；
2. 不强制STA和移动终端主动进行动态密钥更新（基密钥和单播会话密钥）。

6.24 WAPI 参数集合

无线局域网基本功能实体中的站点、移动终端和接入点需满足此项技术要求。

无线局域网基本功能实体的WAPI参数集合应满足如下要求。

1. 如果启用WAPI，AP的信标帧和探询帧中必须包含WAPI参数集合；
2. 如果启用WAPI，STA和移动终端的关联或重关联请求帧中必须包含WAPI参数集合。

6.25 移动终端测试要求

无线局域网基本功能实体中的移动终端需满足此项技术要求。

无线局域网移动终端的基本功能和性能应满足如下要求。

1. 与安全协议有关的功能检测应依据STA的功能要求进行检测；
2. 与安全协议有关的其他功能协议依据移动终端的功能要求进行检测；
3. 与移动终端有关的性能测试依据移动终端的性能要求进行检测。

6.26 多信任证书测试要求

无线局域网基本功能实体中的站点、移动终端、接入点和鉴别服务单元需满足此项技术要求。

无线局域网基本功能实体的多信任证书功能应满足如下要求。

1. STA、移动终端、AP和ASU支持多信任证书功能；
2. 多信任证书协议符合CBWIPS-Z 010-2009 《多信任证书实施技术》指导性技术文件。

7 设备检测

7.1 STA 检测

7.1.1 STA 的 BSS 检测

7.1.1.1 基础协议检测

7.1.1.1.1 SSID

测试目的：

验证STAUT支持的SSID长度应为0-32字符或长度为0-16个汉字；当SSID不同时，STAUT应无法关联至基准AP；不同大小写的SSID应被视作不同的SSID。

测试拓扑图：

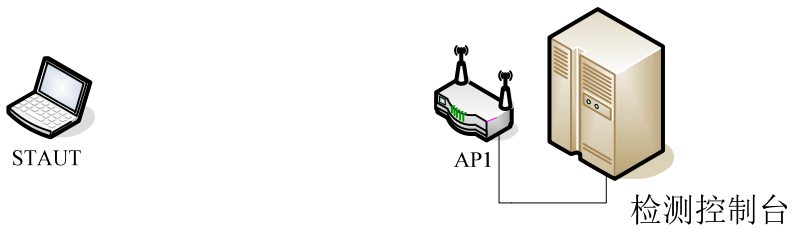


图1 SSID 测试拓扑图

测试步骤：

表1 STAUT 和 AP1 配置信息表

设备	AP1	STAUT
SSID	根据不同测试用例配置	根据不同测试用例配置
信标间隔	默认	默认
信道	1	1
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	开放方式	开放方式

a) 将AP1与检测控制台相连接（见图1）。配置STAUT的IP地址为“192.168.1.100”。
b) 配置AP1和STAUT为开放模式，SSID为“default”，采用信道1，其余配置采用默认值(见表1)。如果STAUT关联至AP1，则须在检测控制台运行“ping 192.168.1.100”命令，观察AP1能否与STAUT通信；
c) 配置AP1的SSID为“abcd”，配置STAUT的SSID为默认不填写，连接AP1，观察STAUT能否关联至AP1；
d) 配置AP1和STAUT的SSID均为“abc”，观察STAUT能否关联至AP1；修改STAUT的SSID为“def”，观察STAUT能否关联至AP1；
e) 配置AP1和STAUT的SSID均为“abcdefghijklmnopqrstuvwxyz012345”，STAUT能否关联至AP1；修改STAUT的SSID为“abcdefghijklmnopqrstuvwxyz0123456”，观察STAUT的SSID设置是否成功；
f) 配置AP1的SSID为“abcdef”，配置STAUT的SSID为“abc”，观察STAUT能否关联至AP1；
g) 配置AP1的SSID为“abc”，配置STAUT的SSID为“abcdef”，观察STAUT能否关联至AP1；
h) 配置AP1的SSID为“abc”，配置STAUT的SSID为“ABC”，观察STAUT能否关联至AP1；
i) 配置AP1的SSID为“ABC”，配置STAUT的SSID为“abc”，观察STAUT能否关联至AP1；
j) 配置AP1的SSID为“abc”，配置STAUT的SSID为“cba”，观察STAUT能否关联至AP1；
k) 配置AP1的SSID为“无线局域网”，配置STAUT的SSID为默认不填写，连接AP1，观察STAUT能否关联至AP1；
l) 配置AP1和STAUT的SSID为“无线局域网”，观察STAUT能否关联至AP1；修改STAUT的SSID为“系统互操作”，观察STAUT能否关联至AP1；
m) 配置AP1和STAUT的SSID为“无线局域网系统互操作站点功能测试”，观察STAUT能否关联至AP1；修改STAUT的SSID为“无线局域网系统互操作站点功能测试一”，观察STAUT能否关联至AP1。

预期结果：

a) 步骤b)中，STAUT能够关联至AP1，并且在检测控制台上能够与AP通信；
b) 步骤c)中，STAUT能够关联至AP1；
c) 步骤d)中，STAUT能够关联至AP1，STAUT修改SSID后不能关联至AP1；
d) 步骤e)中，STAUT能够关联至AP1，STAUT修改SSID时不能成功修改；
e) 步骤f)中，STAUT不能关联至AP1；
f) 步骤g)中，STAUT不能关联至AP1；
g) 步骤h)中，STAUT不能关联至AP1；
h) 步骤i)中，STAUT不能关联至AP1；
i) 步骤j)中，STAUT不能关联至AP1；
j) 步骤k)中，STAUT能够关联至AP1；
k) 步骤l)中，STAUT能够关联至AP1，STAUT修改SSID后不能关联至AP1；
l) 步骤m)中，STAUT能够关联至AP1，STAUT修改SSID时不能成功修改。

7.1.1.1.2 关联或重关联

测试目的：

验证STAUT可以从一个基准AP关联或重关联至采用相同SSID的另外一个基准AP。

测试拓扑图：

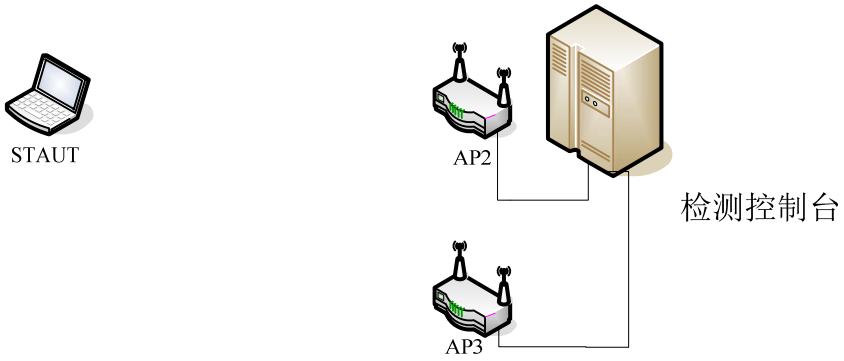


图2　关联或重关联测试拓扑图

测试步骤：

表2　STA 和 AP 配置信息表

设备	AP2	AP3	STAUT
SSID	association	association	association
信标间隔	默认	默认	默认
信道	6	6	6
RTS 门限	默认	默认	默认
分包门限	默认	默认	默认
加密方式	开放方式	开放方式	开放方式

a) 将AP2和AP3与检测控制台相连接（见图2）。配置STAUT的IP地址为“192.168.1.100”。

b) AP2、AP3和STAUT为开放方式，SSID为“association”,采用信道6，其余配置都采用默认值。将AP2加电，关闭AP3，观察STAUT是否能关联至AP2。若STAUT关联至AP2，则在检测控制台上运行“ping 192.168.1.100 －t”，观察AP2是否能与STAUT通信。若AP2可以与STAUT通信，则保持ping命令，将AP3加电，关闭AP2。抓帧并分析，观察STAUT能否关联至AP3，STAUT能否发出关联或重关联请求帧。检测控制台的ping命令在90秒内能够恢复；

c) 若检测控制台的ping命令在90秒内能够恢复,则重新启动AP2,关闭AP3。抓帧并分析,观察STAUT能否关联至AP2，STAUT能否发出关联或重关联请求帧。检测控制台的ping命令在90秒内能够恢复。

预期结果：

d) 步骤b）中的STAUT能够关联至AP3，STAUT能够发出关联或重关联请求帧。并且检测控制台上运行的ping命令能够在90秒内恢复通信；

e) 步骤c）中的STAUT能够关联至AP2，STAUT能够发出关联或重关联请求帧。并且检测控制台上运行的ping命令能够在90秒内恢复通信。

7.1.1.2　WAPI 协议检测

7.1.1.2.1　WAI 证书鉴别和密钥管理方式下证书安装与接入控制

测试目的：

验证STAUT可以安装X.509 v3证书，并能够对所安装的证书进行删除操作；

验证STAUT在启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，能够实现安全接入与保密通信；

验证在STAUT与基准AP都启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，当基准AP采用

非法X.509 v3证书时，STAUT不能与基准AP正常通信；

验证STAUT在启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，基准AP在启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制或不启用WAPI安全机制时，STAUT不能与基准AP正常通信。

测试拓扑图：

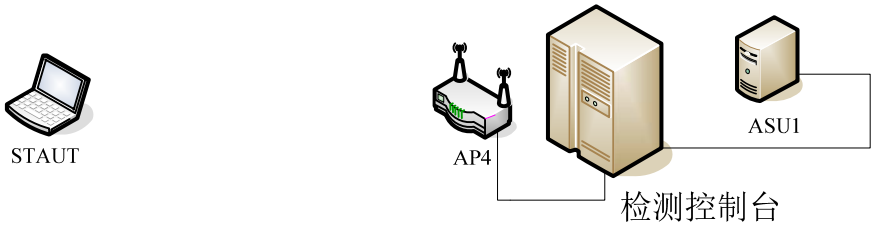


图3　证书鉴别和密钥管理方式下证书安装与接入控制测试拓扑图

测试步骤：

表3　STAUT 和 AP4 配置信息表

设备	AP4	STAUT
SSID	WAPI	WAPI
信标间隔	默认	默认
信道	9	9
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP4与检测控制台相连接（见图3），配置STAUT的IP地址为“192.168.1.100”；

b) 将ASU1与检测控制台相连接（见图3），配置ASU1的IP地址为“192.168.1.1”。ASU1生成颁发者证书、STAUT的证书、AP4的证书、已过期或被吊销的AP4的证书；

c) AP4和STAUT为证书鉴别和密钥管理方式，SSID为“WAPI”，采用信道9，其余配置采用默认值（见表3），在AP4上安装ASU1颁发的X.509 v3证书；

d) 使用ASU1颁发的X.509 v3证书，在STAUT上安装，观察STAUT是否能够正确安装和成功删除该证书；若能成功删除该证书，则重新安装该证书，观察STAUT是否能够正确安装；

e) STAUT启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，AP4不启用任何WAPI安全机制，观察STAUT是否能够接入AP4；STAUT不启用任何WAPI安全机制，AP4启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够接入AP4；STAUT不启用任何WAPI安全机制，AP4启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够接入AP4；

f) STAUT和AP4启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够正确接入AP4，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；

g) 使用ASU1颁发已过期或被吊销的证书，在AP4上安装，STAUT与AP4均开启WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够接入AP4，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；

h) STAUT启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，AP4启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够接入AP4，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功。

预期结果：

a) 步骤d）证书能够在STAUT上被安装和删除；

b) 步骤e）STAUT不能接入AP4；

c） 步骤f）STAUT能够接入AP4，STAUT与AP4能够通信成功；

d） 步骤g）STAUT不能接入AP4，STAUT与AP4不能通信成功；

e） 步骤h）STAUT不能接入AP4，STAUT与AP4不能通信成功。

7.1.1.2.2 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试目的：

验证STAUT在启用证书鉴别和密钥管理方式下的WAPI安全机制时，WAPI协议的处理流程、数据格式是否符合GB15629.11系列标准所规定的内容，以及在此基础上和基准AP的互通性。

测试拓扑图：

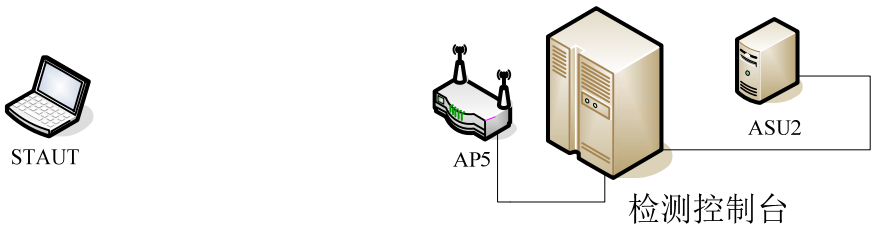


图4 证书鉴别和密钥管理方式下的协议流程与数据格式测试拓扑图

测试步骤：

表4 STAUT 和 AP5 配置信息表

设备	AP5	STAUT
SSID	WAPI	WAPI
信标间隔	默认	默认
信道	4	4
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a） 将AP5和ASU2与检测控制台相连接（见图4），配置ASU2的IP地址为“192.168.1.1”。ASU2生成颁发者证书、STAUT的证书、AP5的证书；

b） 配置STAUT与AP5的SSID均为“WAPI”，采用信道4，在STAUT与AP5上安装ASU2生成的X.509 v3证书，其余配置采用默认值（见表4），观察STAUT是否能够关联至AP5；

c） 开启检测控制台上的WAI证书鉴别和密钥管理方式下的WAPI检测，根据提示开启STAUT和AP5上的WAPI安全机制，检测控制台的WAPI检测程序将对WAPI协议流程进行捕捉分析，并生成检测结果和详细检测纪录。

预期结果：

a） 步骤b）STAUT能够关联至AP5

b） 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

STAUT发送的包含WAPI参数集合的关联请求帧；

STAUT在接收到AP5发送的鉴别激活后，向AP5发送的接入鉴别请求分组；

STAUT处理AP5返回的接入鉴别响应后，能够得到证书鉴别结果；

STAUT在接收到AP5的单播密钥协商请求分组后，向AP5发送的单播密钥协商响应分组；

STAUT发送的单播密钥协商响应分组中的WIE_{asue}字段与STAUT在关联请求帧中发送的WAPI参数集合字段相同；

STAUT在处理AP5返回的单播密钥协商确认分组和AP5发出的组播密钥通告分组，并得到组播密钥后，向AP5发送的组播密钥通告响应分组；

STAUT利用密钥协商所获得的密钥对数据地进行加解密的操作。

7.1.1.2.3 WAI 预共享密钥鉴别和密钥管理方式下的接入控制

测试目的：

验证 STAUT 采用预共享密钥鉴别和密钥管理方式正确进行接入控制的情况。

验证 STAUT 在启用预共享密钥鉴别和密钥管理方式下的 WAPI 安全机制时，能够实现安全接入与保密通信。

测试拓扑图：

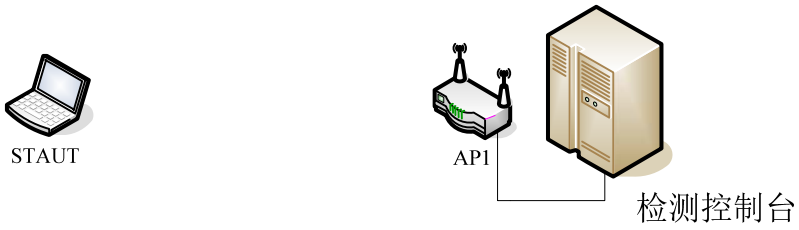


图5 预共享密钥鉴别和密钥管理方式下的接入控制测试拓扑图

测试步骤：

表5 STAUT 和 AP1 配置信息表

设备	AP1	STAUT
SSID	sharedkey	sharedkey
信标间隔	默认	默认
信道	11	11
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

a) 将AP1与检测控制台相连接（见图5），配置STAUT的IP地址为“192.168.1.100”；

b) 配置STAUT与AP1的SSID均为“sharedkey”，采用信道11,其余配置采用默认值（见表5）；

c) 将STAUT的预共享密钥设为字符串“12345678”，将AP1的预共享密钥设为字符串“123456789”，观察STAUT与AP1是否能够通信；

d) 将STAUT的预共享密钥设为字符串“12345678”,将AP1的预共享密钥设为字符串“12345678”，观察STAUT是否能够关联至AP1，如果STAUT成功关联至AP1，则在检测控制台上运行“ping 192.168.1.100”，观察STAUT与AP1是否能够通信；

e) 将STAUT的预共享密钥设为十六进制数“0x1234ABCDEF”，将AP1的预共享密钥设为十六进制数“0x1234ABCD”，观察STAUT与AP1是否能够通信；

f) 将STAUT的预共享密钥设为十六进制数“0x1234ABCD”，将AP1 的预共享密钥设为十六进制数“0x1234ABCD”，观察STAUT是否能够关联至AP1，如果STAUT成功关联至AP1，则在检测控制台上运行“ping 192.168.1.100”，观察STAUT与AP1是否能够通信。

预期结果：

a) 步骤c）中STAUT与AP1不能通信；

b) 步骤d）中STAUT能够成功关联至AP1，STAUT与AP1能够成功通信；

c) 步骤e）中STAUT与AP1不能通信；

d) 步骤f）中STAUT能够成功关联至AP1，STAUT与AP1能够成功通信。

7.1.1.2.4 WAI 预共享密钥鉴别和密钥管理方式下的协议流程与数据格式

测试目的：

验证STAUT在启用预共享密钥鉴别和密钥管理方式下的WAPI安全机制时，WAPI协议的处理流程、数据格式是否符合GB15629.11系列标准所规定的内容，以及在此基础上和基准AP的互通性。

测试拓扑图：

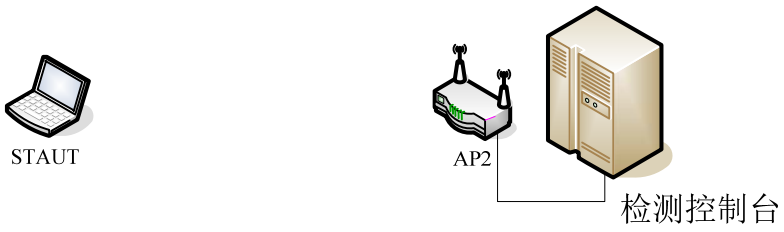


图6　　预共享密钥鉴别和密钥管理方式下的协议流程与数据格式测试拓扑图

测试步骤：

表6　　STAUT 和 AP2 配置信息表

设备	AP2	STAUT
SSID	sharedkey	sharedkey
信标间隔	默认	默认
信道	7	7
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

a) 将AP2与检测控制台相连接（见图6）；

b) 配置STAUT与AP2的SSID均为“sharedkey”，采用信道7，其余配置采用默认值（见表6）；

c) 将STAUT与AP2的预共享密钥均设为字符串“sharedkey”，观察STAUT是否能够关联至AP2；

d) 开启检测控制台上的WAI预共享密钥鉴别和密钥管理方式下的WAPI检测，根据提示开启STAUT和AP2上的WAPI安全机制，检测控制台的WAPI检测程序将对WAPI协议流程进行捕捉分析，并生成检测结果和详细检测纪录。

预期结果：

a) 步骤c）STAUT能够关联至AP2；

b) 步骤d）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

STAUT发送的包含WAPI参数集合的关联请求帧；

STAUT在接收到AP2的单播密钥协商请求分组后，向AP2发送的单播密钥协商响应分组；

STAUT发送的单播密钥协商响应分组中的WIE_{asue}字段与STAUT在关联请求帧中发送的WAPI参数集合字段相同；

STAUT在处理AP2返回的单播密钥协商确认分组和AP2发出的组播密钥通告分组，并得到组播密钥后，向AP2发送的组播密钥通告响应分组；

STAUT利用密钥协商所获得的密钥对数据地进行加解密的操作。

7.1.1.2.5　　基密钥更新功能

测试目的：

验证 STAUT 能够响应基准 AP 发起的基密钥更新过程，STAUT 能够利用新的密钥对数据进行保密通信。

测试拓扑图：

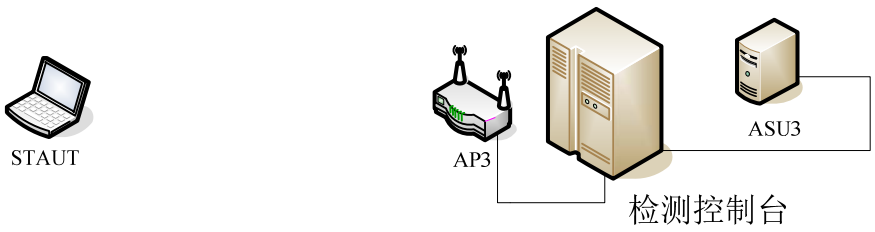


图7　　基密钥更新功能测试拓扑图

测试步骤：

表7　　STAUT 和 AP3 配置信息表

设备	AP3	STAUT
SSID	BK	BK
信标间隔	默认	默认
信道	3	3
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP3和ASU3与检测控制台相连接（见图7），配置ASU3的IP地址为“192.168.1.1”，配置STAUT的IP地址为“192.168.1.100”。ASU3生成颁发者证书、STAUT的证书、AP3的证书；

b) 配置STAUT与AP3的SSID均为“BK”，采用信道3，在STAUT与AP3上安装ASU3生成的X.509 v3证书，其余配置采用默认值（见表7），观察STAUT是否能够关联至AP3；

c) 在AP3上发起对STAUT的基密钥更新，检测控制台的WAPI检测程序对AP3与STAUT之间的基密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 基密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察STAUT与AP3是否能够通信。

预期结果：

a) 步骤b）STAUT和AP3能够安装ASU3的证书，STAUT能够关联至AP3；

b) 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

鉴别激活分组、接入鉴别请求分组、接入鉴别响应分组、单播密钥协商分组、组播密钥协商分组中的BK更新标识位为1；

STAUT处理AP3发送的鉴别激活后，向AP3发送的接入鉴别请求分组；

STAUT处理AP3返回的接入鉴别响应后，能够得到证书鉴别结果；

STAUT处理AP3的单播密钥协商请求分组后，向AP3发送的单播密钥协商响应分组；

STAUT发送的单播密钥协商响应分组中的WIE_{asue}字段与STAUT在关联请求帧中发送的WAPI参数集合字段相同；

STAUT处理AP3返回的单播密钥协商确认分组和AP3发出的组播密钥通告分组，并得到组播密钥后，向AP3发送的组播密钥响应分组；

STAUT利用密钥协商所获得的新密钥对数据地进行加解密的操作。

c) 步骤d）基密钥更新完毕后，检测控制台可以与STAUT通信。

7.1.1.2.6　　单播会话密钥更新功能

测试目的：

验证 STAUT 能够响应基准 AP 发起的密钥更新过程，STAUT 能够利用新的密钥对数据进行保密通信。

测试拓扑图：

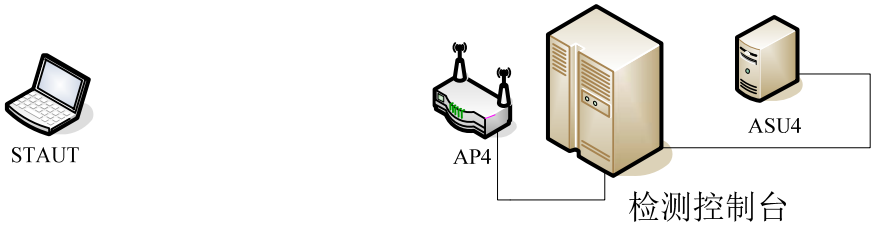


图8　　单播会话密钥更新功能测试拓扑图

测试步骤：

表8　　STAUT 和 AP4 配置信息表

设备	AP4	STAUT
SSID	USK	USK
信标间隔	默认	默认
信道	8	8
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP4和ASU4与检测控制台相连接（见图8），配置ASU4的IP地址为“192.168.1.1”，配置STAUT的IP地址为“192.168.1.100”。ASU4生成颁发者证书、STAUT的证书、AP4的证书；

b) 配置STAUT与AP4的SSID均为“USK”，采用信道8，在STAUT与AP4上安装ASU4生成的X.509 v3证书，其余配置采用默认值（见表8），观察STAUT是否能够关联至AP4；

c) 在AP4上发起对STAUT的单播会话密钥更新，检测控制台的WAPI检测程序对AP4与STAUT之间的单播会话密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 单播会话密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察 STAUT 与 AP4 是否能够通信。

预期结果：

a) 步骤b) STAUT和AP4能够安装ASU4的证书，STAUT能够关联至AP4；

b) 步骤c) 检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

AP4发送的单播密钥协商分组中的USK更新标识位为1；

STAUT处理AP4的单播密钥协商请求分组后，向AP4发送的单播密钥协商响应分组；

STAUT发送的单播密钥协商响应分组中的WIE_{asue}字段与STAUT在关联请求帧中发送的WAPI参数集合字段相同；

c) 步骤d) 单播会话密钥更新完毕后，检测控制台可以与STAUT通信。

7.1.1.2.7　　组播会话密钥更新功能

测试目的：

验证 STAUT 能够响应基准 AP 发起的密钥更新过程，STAUT 能够在组播会话密钥更新完毕后对数据进行保密通信。

测试拓扑图：

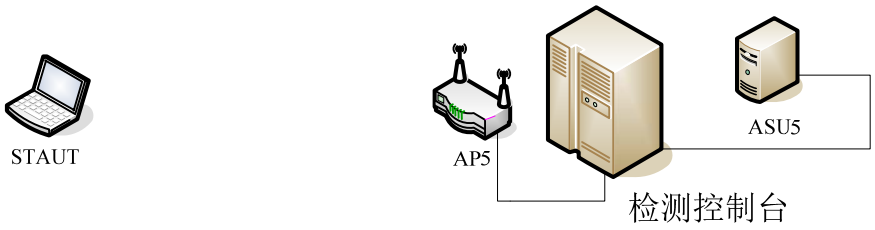


图9　　组播会话密钥更新功能测试拓扑图

测试步骤：

表9　　STAUT 和 AP5 配置信息表

设备	AP5	STAUT
SSID	MSK	MSK
信标间隔	默认	默认
信道	4	4
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP5和ASU5与检测控制台相连接（见图9），配置ASU5的IP地址为“192.168.1.1”，配置STAUT的IP地址为“192.168.1.100”。ASU5生成颁发者证书、STAUT的证书、AP5的证书；

b) 配置STAUT与AP5的SSID均为“MSK”，采用信道4，在STAUT与AP5上安装ASU5生成的X.509 v3证书，其余配置采用默认值（见表9），观察STAUT是否能够关联至AP5；

c) 在AP5上发起组播会话密钥更新，检测控制台的WAPI检测程序对AP5与STAUT之间的组播会话密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 组播会话密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察 STAUT 与 AP5 是否能够通信。

预期结果：

a) 步骤b）STAUT和AP5能够安装ASU5的证书，STAUT能够关联至AP5；

b) 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

AP5发送的组播密钥通告分组；

STAUT发送的组播密钥响应分组。

c) 步骤d）组播会话密钥更新完毕后，检测控制台可以与STAUT通信。

7.1.1.3　性能测试

7.1.1.3.1　　单播性能检测 1（开放方式）

测试目的：

验证STAUT和基准AP均为开放方式，基准AP采用不同的参数配置时，测试STAUT与基准AP之间典型通信的数据吞吐量，从而衡量STAUT与不同基准AP应具有的良好的互通性。

测试拓扑图：

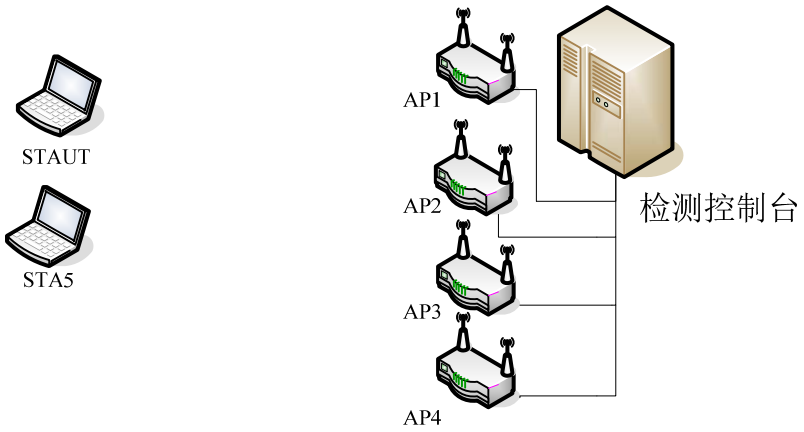


图10　　单播性能检测 1（开放方式）测试拓扑图

测试步骤：

表10　　单播性能检测 1 STAUT、基准 AP 和 STA5 配置信息表

设备	STAUT	AP1	AP2	AP3	AP4
模式	-	1	2	3	4
SSID	a	a	a	a	a
信道	-	149	11	2	3
信标帧间隔	100ms	100ms	100ms	100ms	100ms
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
加密方式	开放方式	开放方式	开放方式	开放方式	开放方式
				设备	STA5
				模式	4
				SSID	A
				信道	-
				信标帧间隔	-
				RTS 门限	256
				分段门限	500
				加密方式	开放方式

a)　将AP1、AP2、AP3和AP4与检测控制台相连接（见图10），配置STAUT的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”。其余配置见表10，其中：

模式1：AP1为符合GB15629.1101的设备；

模式2：AP2为符合GB15629.1104的设备；

模式3：AP3为符合GB15629.1102的设备；

模式4：AP4为符合GB15629.1104的设备，STA5为符合GB15629.1102的设备。

b)　在检测控制台上运行单播性能 检测程序，观察性能检测结果。

预期结果：

表11　　性能检测结果判别标准表

模式	1	2	3	4
T1	≥13.0Mbit/s	≥13.0Mbit/s	≥3.6Mbit/s	≥3.9Mbit/s，BT1≥1.5Mbit/s
T2	≥13.0Mbit/s	≥13.0Mbit/s	≥3.6Mbit/s	≥5.3Mbit/s，BT2≥0.30Mbit/s
T3	≥1.05Mbit/s	≥1.05Mbit/s	≥0.66Mbit/s	≥0.61Mbit/s,BT3≥0.07Mbit/s

T1 表示帧 1[1]下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2[2]下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行吞吐量。

a) 步骤 b）检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2 和 BT3 均能超过表 11 中相对应的数值。

7.1.1.3.2 单播性能检测 2（证书鉴别和密钥管理方式）

测试目的：

验证STAUT和基准AP均为证书鉴别和密钥管理方式，基准AP采用不同的参数配置时，测试STAUT与基准AP之间典型通信的数据吞吐量，从而衡量STAUT与不同基准AP应具有的良好的互通性。

测试拓扑图：

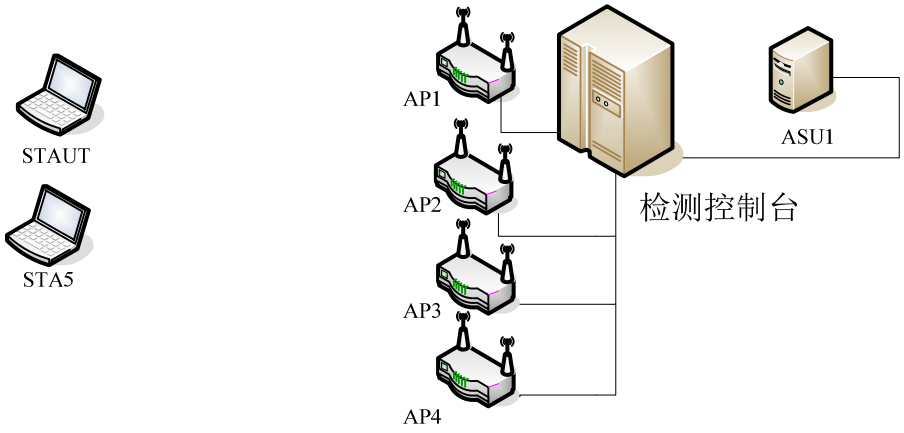


图11 单播性能检测 2（证书鉴别和密钥管理方式）测试拓扑图

测试步骤：

表12 单播性能检测 2 STAUT、基准 AP 和 STA5 配置信息表

设备	STAUT	AP1	AP2	AP3	AP4
模式	-	1	2	3	4
SSID	-	abcdefghijklmnopqrstuvwxyzABCDEF	abcdefghijklmnopqrstuvwxyzABCDEF	12345678901234567890123456789012	abcdefghijklmnopqrstuvwxyzABCDEF
信道	-	157	4	5	6
信标帧间隔	-	200ms	200ms	200ms	200ms
RTS 门限	默认	默认	默认	256	默认
分段门限	默认	500	500	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式
				设备	STA5
				模式	4
				SSID	abcdefghijklmnopqrstuvwxyzABCDEF
				信道	-

[1] 帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

[2] 帧 2:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100 字节。

信标帧间隔	–
RTS 门限	默认
分段门限	500
加密方式	证书鉴别和密钥管理方式

a） 将AP1、AP2、AP3、AP4和ASU1与检测控制台相连接（见图11），配置ASU1的IP地址为“192.168.1.1”，配置STAUT的IP地址为“192.168.1.100”，配置STA5的IP地址为“192.168.1.101”。ASU1生成颁发者证书、STAUT和STA5的证书、AP1、AP2、AP3和AP4的证书，其余配置见表12，其中：

模式1：AP1为符合GB15629.1101的设备；

模式2：AP2为符合GB15629.1104的设备；

模式3：AP3为符合GB15629.1102的设备；

模式4：AP4为符合GB15629.1104的设备，STA5为符合GB15629.1102的设备。

b） 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表13　　性能检测结果判别标准表

模式	1	2	3	4
T1	≥6.1Mbit/s	≥6.1Mbit/s	≥3.2Mbit/s	≥3.0Mbit/s，BT1≥3.6Mbit/s
T2	≥7.1Mbit/s	≥8.1Mbit/s	≥3.3Mbit/s	≥2.3Mbit/s，BT2≥0.36Mbit/s
T3	≥0.70Mbit/s	≥0.70Mbit/s	≥0.50Mbit/s	≥0.42Mbit/s,BT3≥0.43Mbit/s

T1 表示帧 1[3]下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2[2]下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行吞吐量。

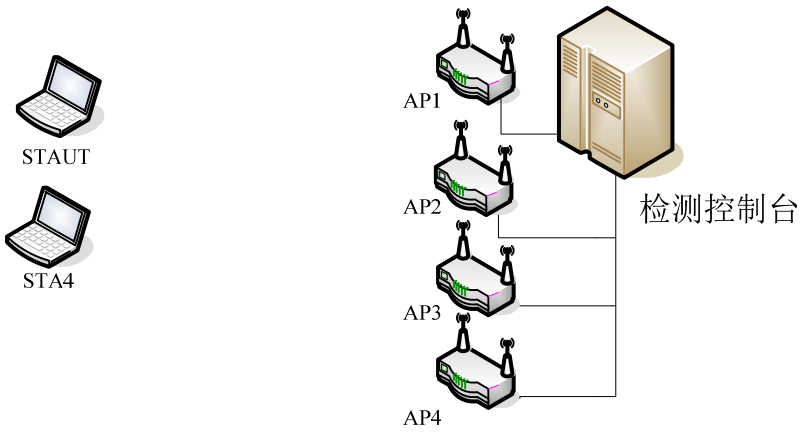
a） 步骤b）检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2和BT3均能超过表13中相对应的数值。

7.1.1.3.3　单播性能检测 3（预共享密钥鉴别和密钥管理方式）

测试目的：

验证STAUT和基准AP均为预共享密钥鉴别和密钥管理方式，基准AP采用不同的参数配置时，测试STAUT与基准AP之间典型通信的数据吞吐量，从而衡量STAUT与不同基准AP应具有的良好的互通性。

测试拓扑图：



[3]帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

[2] 帧 2:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100 字节。

图12　　单播性能检测 3（预共享密钥鉴别和密钥管理方式）测试拓扑图

测试步骤：

表14　　单播性能检测 3 STAUT、基准 AP 和 STA4 配置信息表

参数	STAUT	AP1	AP2	AP3	AP4
模式	-	1	2	3	4
SSID	sharekey	sharekey	sharekey	sharekey	sharekey
信道	-	161	7	8	9
信标帧间隔	默认	300ms	300ms	300ms	300ms
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	500	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

参数	STA4
模式	4
SSID	sharekey
信道	-
信标帧间隔	-
RTS 门限	256
分段门限	默认
加密方式	预共享密钥鉴别和密钥管理方式

测试步骤：

a)　将AP1、AP2、AP3和AP4与检测控制台相连接（见图12），配置STAUT的IP地址为“192.168.1.100”，配置STA4的IP地址为“192.168.1.101”。预共享密钥为“12345678”，其余配置见表14，其中：

模式1：AP1为符合GB15629.1101的设备；

模式2：AP2为符合GB15629.1104的设备；

模式3：AP3为符合GB15629.1102的设备；

模式4：AP4为符合GB15629.1104的设备，STA4为符合GB15629.1102的设备。

b)　在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表15　　性能结果判别标准表

模式	1	2	3	4
T1	≥12.4Mbit/s	≥11.4Mbit/s	≥2.3Mbit/s	≥3.7Mbit/s，BT1≥2.5Mbit/s
T2	≥12.6Mbit/s	≥10.6Mbit/s	≥3.6Mbit/s	≥2.6Mbit/s，BT2≥0.40Mbit/s
T3	≥0.88Mbit/s	≥0.88Mbit/s	≥0.64Mbit/s	≥0.50Mbit/s,BT3≥0.39Mbit/s

T1 表示帧 1^4下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2^2下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行

吞吐量。

a） 步骤b）检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2和BT3均能超过表15中相对应的数值。

7.1.1.4 组播检测

7.1.1.4.1 组播功能测试

测试目的：

验证STAUT在启用WAPI安全方式和不启用WAPI安全方式下的接收组播帧的能力。

每种模式的测试又分为启用WAPI安全的组播性能检测和不启用安全的组播性能检测。

测试拓扑图：

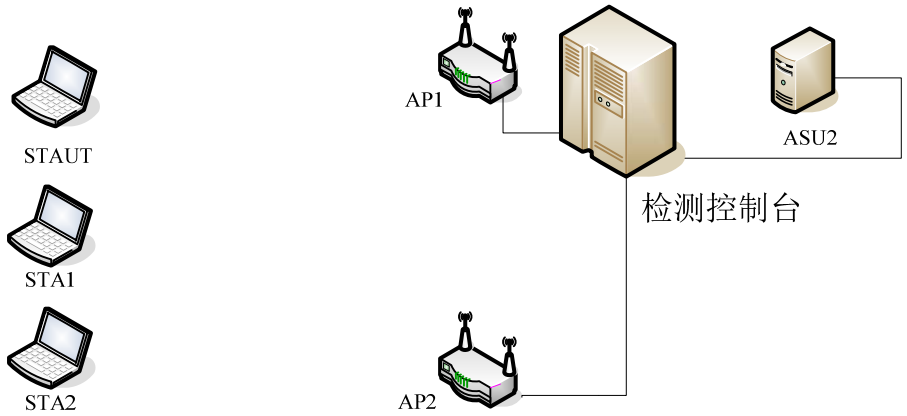


图13 组播功能测试拓扑图

测试步骤：

表16 组播能力检测 STAUT、基准 AP 和基准 STA 配置信息表

设备	AP1	AP2	STA1	STA2	STAUT
模式	1	1	1	1	-
SSID	multicastG	multicastG	multicastG	multicastG	multicastG
信道	10	10	默认	默认	默认
信标帧间隔	100ms	100ms	默认	默认	默认
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
安全方式	证书鉴别和密钥管理方式	开放方式	证书鉴别和密钥管理方式	开放方式	-

a） 将AP1、AP2和ASU2与检测控制台相连接（见图13），配置ASU2的IP地址为“192.168.1.1”，配置STAUT的IP地址为“192.168.1.100”，配置STA1的IP地址为“192.168.1.101”，配置STA2的IP地址为“192.168.1.102”。ASU2生成颁发者证书、STAUT和STA1的证书、AP1的证书，在检测控制台上配置AP1向STA1和STAUT发送组播数据帧，AP2向STA2和STAUT发送组播数据帧；其余配置见表16；

b） STAUT、STA1和AP1启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STAUT是否能够正确接入AP1，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；

c） 运行检测控制台中的启用证书鉴别和密钥管理方式的安全机制下的组播功能检测；

d） STAUT、STA2和AP2启用开放方式，观察STAUT是否能够正确接入AP2，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；

e） 运行检测控制台中的启用开放方式下的组播功能检测；

d） 观察检测控制台上的组播功能检测是否通过。

预期结果：

a） 步骤b）中STAUT能够成功关联至AP1，STAUT与AP1能够成功通信；

b） 步骤c）中STAUT可以接收到AP1向STA1和STAUT发送的组播数据帧，检测控制台的组播功能检测程序必须通过；

c） 步骤d）中STAUT能够成功关联至AP2，STAUT与AP2能够成功通信；

d） 步骤e）中STAUT可以接收到AP2向STA2和STAUT发送的组播数据帧，检测控制台的组播功能检测程序必须通过。

7.1.2 STA 的自组网（IBSS）模式检测

7.1.2.1 基础协议检测

7.1.2.1.1 主动扫描

测试目的：

验证STAUT可以配置SSID和信道建立IBSS并发送探询响应帧或信标帧，允许基准STA加入，验证STAUT支持的基本数据速率集包括1Mbit/s，2Mbit/s，5.5Mbit/s，11Mbit/s。

测试拓扑图：

图14 IBSS 主动扫描测试拓扑图

测试步骤：

表17 主动扫描能力测试 STAUT 配置信息表

设备	STAUT
SSID	IBSSAC
信道	5
RTS 门限	默认
分段门限	默认
安全方式	开放方式

表18 主动扫描能力测试 STA1 配置信息表

设备	STA1
SSID	IBSSAC
信道	-
RTS 门限	500
分段门限	500
安全方式	开放方式

a） 配置STAUT的IP地址为“192.168.1.100”，配置STA1的IP地址为“192.168.1.101”，其余配置见表17、表18；

b） 先启动STAUT，使其作为IBSS的创建者。在检测控制台上启动无线接口捕捉程序，进入监听状态后启动STA1，令其加入STAUT创建的IBSS；

c） 检测控制台对捕捉到的帧进行分析，观察STAUT是否对STA1的探询请求发回了探询响应；

d） 检测控制台能够捕捉到STAUT发出的信标帧，信标帧信息内必须包含基本速率集，包括

1Mbit/s，2Mbit/s，5.5Mbit/s ，11Mbit/s，信道必须为表17中所配置的信道；

e) 在STA2上运行“ping 192.168.1.100 -t”，观察STAUT与STA1是否能够通信。

预期结果：

a) 步骤c）STAUT应对STA1的探询请求发回探询响应；

b) 步骤d）STAUT的信标帧信息包含基本速率集和信道的信息；

c) 步骤e）STAUT应与STA1成功通信。

7.1.2.1.2 被动扫描

测试目的：

验证STAUT可以加入基准STA建立的IBSS，验证STAUT支持的基本数据速率集包括1Mbit/s，2Mbit/s，5.5Mbit/s，11Mbit/s。

测试拓扑图：

图15 IBSS 被动扫描测试拓扑图

测试步骤：

表19 被动扫描能力测试 STA2 配置表

设备	STA2
SSID	IBSSED
信道	7
RTS 门限	默认
分段门限	默认
安全方式	开放方式

表20 被动扫描能力测试 STAUT 配置表

设备	STAUT
SSID	IBSSED
信道	-
RTS 门限	500
分段门限	500
安全方式	开放方式

a) 配置STAUT的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”，其余配置见表19、表20；

b) 先启动STA2，使其作为IBSS的创建者。在检测控制台上启动无线接口捕捉程序，进入监听状态后启动STAUT，令其加入STA2创建的IBSS；

c) 检测控制台对捕捉到的帧进行分析，观察STAUT是否对STA2发出了探询请求帧；

d) 在STA2上运行“ping 192.168.1.100 -t”，观察STAUT与STA2是否能够成功通信。

预期结果：

a) 步骤c）检测控制台的无线接口捕捉程序能够捕捉到STAUT对STA2发出的探寻请求帧；

b) 步骤d）STAUT应与STA2成功通信。

7.1.2.1.3 加入与重加入 IBSS

测试目的：

验证STAUT可以正确加入一个已存在的IBSS，并且当STAUT离开该IBSS，返回后能自动再次加入；

测试拓扑图：

图16 加入与重加入 IBSS 测试拓扑图

测试步骤：

表21 加入 IBSS 能力测试 STAUT 配置表

设备	STAUT
SSID	rejoin
信道	13
RTS 门限	默认
分段门限	默认
安全方式	开放方式

表22 加入 IBSS 能力测试 STA3 配置表

设备	STA3
SSID	rejoin
信道	13
RTS 门限	默认
分段门限	默认
安全方式	开放方式

a) 配置STAUT的IP地址为“192.168.1.100”，配置STA3的IP地址为“192.168.1.101”，其余配置见表21、表22；
b) 先启动STA3，使其作为IBSS的创建者；随后启动STAUT，令其加入STA3创建的IBSS。在STAUT上运行“ping 192.168.1.101 -t”，观察STAUT与STA3是否能够成功通信；
c) 将STAUT移动至足够远处，或者将其置于金属屏蔽盒中，使STAUT上的ping通信命令中断，启动检测控制台的无线抓帧软件，抓帧软件不能抓到STAUT发出的信标帧；
d) 将STAUT移动回初始位置，或者将其移出金属屏蔽盒，STAUT能够重新加入STA3所创建的IBSS，检测控制台的无线抓帧软件能够重新捕捉到STAUT发出的信标帧。

预期结果：

a) 步骤b) STAUT与STA3能够通信成功；
b) 步骤d) STAUT能够重新加入STA3创建的IBSS，并且STAUT上的ping通信命令应能恢复通信。

7.1.2.2 WAPI 协议检测

7.1.2.2.1 密钥设置与接入控制

测试目的：

验证STAUT在自组网模式下可以启用WAI预共享密钥鉴别和密钥管理方式的WAPI安全机制，并支持十六进制数和ASCII字符两种密钥输入方式。

测试拓扑图：

图17　IBSS 下的 WAI 预共享密钥鉴别和密钥管理方式测试拓扑图

测试步骤：

表23　IBSS 密钥设置与接入控制 STAUT 配置表

设备	STAUT
SSID	share-key
信道	1
RTS 门限	默认
分段门限	默认
安全方式	共享密钥鉴别和密钥管理方式

表24　IBSS 密钥设置与接入控制 STA4 配置表

设备	STA4
SSID	share-key
信道	1
RTS 门限	默认
分段门限	默认
安全方式	共享密钥鉴别和密钥管理方式

a) 配置STAUT的IP地址为“192.168.1.100”，配置STA4的IP地址为“192.168.1.101”，其余配置见表23、表24；

b) 先启动STAUT，令其作为IBSS的创建者；启动STA4，令其加入STAUT创建的IBSS。在STAUT上运行“ping 192.168.1.101”，在STA4上运行“ping 192.168.1.100 -t”，观察STAUT与STA4是否能够通信成功；

c) 在STAUT上启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用十六进制数方式输入密钥“0x0123456789ABCDEF”，STA4启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用十六进制数输入密钥“0xFEDCBA9876543210”，观察STAUT与STA4上的ping通信命令是否中断；

d) 在STA4上启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用ASCII方式输入密钥“12345”，观察STAUT与STA4上的ping通信命令是否能够成功通信；

e) 在STA4上启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用十六进制数输入密钥“0x0123456789ABCDEF”，观察STAUT与STA4上的ping通信命令是否能够成功恢复通信；

f) 在STAUT上启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用ASCII方式输入密钥“ABCDEF”，在STA4上启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，采用十六进制数方式输入密钥“0xABCDEF”，观察STAUT与STA4上的ping通信命令是否能够通信成功；

g) 在STA4上采用ASCII方式输入密钥“abcdef”，观察STAUT与STA2上的ping通信命令是否通信成功；

h) 在STA4上采用ASCII方式输入密钥“ABCDEF”，观察STAUT与STA2上的ping通信命令是否通信成功。

预期结果：

a） 步骤b）STAUT与STA4应该能够通信成功；

b） 步骤c）STAUT与STA4上的ping通信命令应该断开；

c） 步骤d）STAUT与STA4上的ping通信命令不能恢复；

d） 步骤e）STAUT与STA4上的ping通信命令能够恢复；

e） 步骤f）STAUT与STA4上的ping通信命令应该断开；

f） 步骤g）STAUT与STA4上的ping通信命令不能恢复；

d） 步骤f）STAUT与STA4上的ping通信命令能够恢复。

7.1.3 WAPI 移动终端检测

7.1.3.1 移动终端漫游功能检测

7.1.3.1.1 WAPI 多信任证书漫游功能测试

测试目的：

验证移动用户终端MTUT能够支持多信任证书功能，可通过漫游功能，实现在不同接入地，安全接入网络。

测试拓扑图：

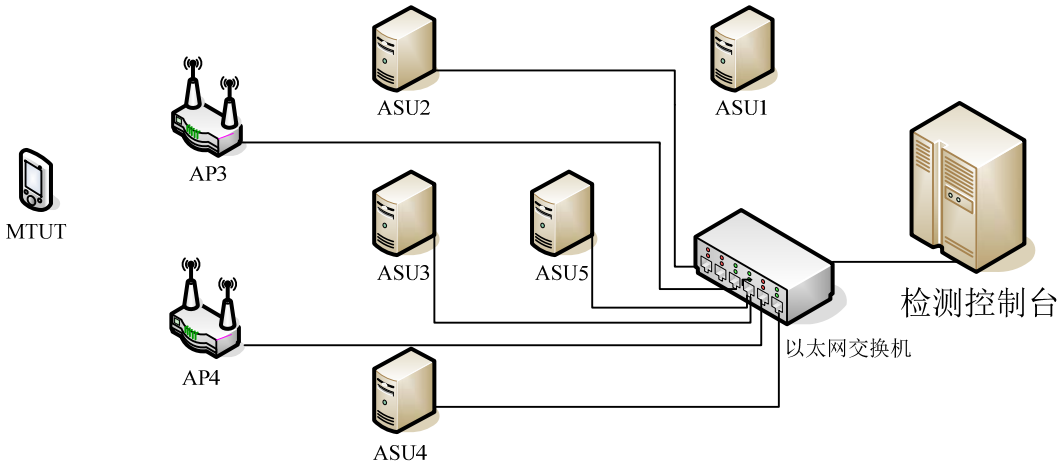


图18 WAPI 多信任证书漫游功能测试拓扑图

测试步骤：

表25 AP 和 MTUT 配置信息表

设备	AP3	AP4	MTUT
SSID	Roaming	roaming	roaming
信标间隔	默认	默认	默认
信道	1	1	1
RTS 门限	默认	默认	默认
分包门限	默认	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a） 按照测试拓扑图连接测试环境（见图27），其中AP3与AP4作为处于不同地域的接入地AP，ASU1作为颁发与管理证书的机构。ASU5作为中心ASU，配置ASU5的IP地址为“192.168.1.1”。ASU2作为归属地ASU，配置ASU2的IP地址为“192.168.1.2”。ASU3与ASU4作为接入地ASU，配置ASU3的IP地址为“192.168.1.3”，ASU4的IP地址为“192.168.1.4”；

b) 配置ASU1为ASU2，ASU3，ASU4，ASU5，AP3，AP4和MTUT颁发证书；

c) 在ASU2，ASU3，ASU4上建立与ASU5的互信，并安装ASU1颁发的证书。在ASU5上建立与ASU2，ASU3，ASU4的互信，并安装ASU1颁发的证书；

d) 在AP3和AP4上安装ASU1颁发的证书，其余配置按照上表所述进行配置（见表34），ASU3作为AP3的接入地ASU，ASU4作为AP4的接入地ASU；

e) 在MTUT上安装ASU1颁发的证书，其余配置按照上表所述进行配置（见表34），ASU2作为MTUT的归属地ASU，配置MTUT的IP地址为“192.168.1.100”；

f) 将AP3加电，关闭AP4，使MTUT连接AP3，观察MTUT是否能关联至AP3。若MTUT关联至AP3，则在检测控制台上运行“ping 192.168.1.100 －t”，观察AP3是否能与MTUT通信。若AP3可以与MTUT通信，则保持ping命令，将AP4加电，关闭AP3。抓帧并分析，观察MTUT能否发出证书鉴别和密钥管理方式下的完整的WAI鉴别流程，观察检测控制台是否能够捕捉到漫游证书鉴别请求帧。检测控制台的ping命令能够自动恢复通信；

g) 等待检测控制台的ping通信命令自动恢复通信后，重新启动AP3，关闭AP4。抓帧并分析，观察MTUT能否关联至AP3，观察MTUT能否发出证书鉴别和密钥管理方式下的完整的WAI鉴别流程，观察检测控制台是否能够捕捉到漫游证书鉴别请求帧。检测控制台的ping命令能够自动恢复通信；

预期结果：

a) 步骤f)：MTUT能够关联至AP3，检测控制台能够捕获到完整的WAI证书鉴别和密钥管理方式下的协议流程及加解密处理过程，检测控制台能够捕捉到ASU3向ASU5发送的漫游证书鉴别请求帧，其中漫游证书鉴别请求帧中必须包含：

接入地ASU的证书字段，字段中的ASU证书必须与AP3安装的ASU证书相同；

终端信任的ASU证书持有者名称，字段中的名称必须与归属地ASU2的证书持有者身份一致。

b) 步骤g)：MTUT能够关联至AP4，检测控制台能够捕获到完整的WAI证书鉴别和密钥管理方式下的协议流程及加解密处理过程，检测控制台能够捕捉到ASU4向ASU5发送的漫游证书鉴别请求帧，其中漫游证书鉴别请求帧中必须包含：

接入地ASU的证书字段，字段中的ASU证书必须与AP4安装的ASU证书相同；

终端信任的ASU证书持有者名称，字段中的名称必须与归属地ASU2的证书持有者身份一致。

7.1.3.2 移动终端性能测试

7.1.3.2.1 单播性能检测 1（开放方式）

测试目的：

验证MTUT和基准AP均为开放方式，基准AP采用不同的参数配置时，测试MTUT与基准AP之间典型通信的数据吞吐量，从而衡量MTUT与不同基准AP应具有的良好的互通性。

测试拓扑图：

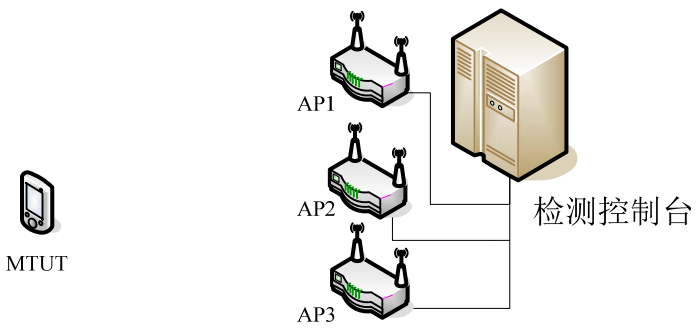


图19　　单播性能检测 1（开放方式）测试拓扑图

测试步骤：

表26　　单播性能检测 1 MTUT 和基准 AP 配置信息表

设备	MTUT	AP1	AP2	AP3
模式	-	1	2	3
SSID	A	a	a	a
信道	-	149	11	2
信标帧间隔	100ms	100ms	100ms	100ms
RTS 门限	默认	默认	默认	默认
分段门限	默认	默认	默认	默认
加密方式	开放方式	开放方式	开放方式	开放方式

a)　将AP1、AP2和AP3与检测控制台相连接（见图28），配置MTUT的IP地址为“192.168.1.100”。其余配置按照上表所述进行配置（见表35），其中：

模式1：AP1为符合GB15629.1101的设备；

模式2：AP2为符合GB15629.1104的设备；

模式3：AP3为符合GB15629.1102的设备；

b)　在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表27　　性能检测结果判别标准表

模式	1	2	3
T1	≥1.0Mbit/s	≥1.0Mbit/s	≥1.0Mbit/s
T2	≥1.0Mbit/s	≥1.0Mbit/s	≥1.0Mbit/s

T1 表示帧 1[5]下行吞吐量，T2 表示帧 1 上行吞吐量。

a)　步骤 b）检测控制台的性能检测结果中，T1、T2、T3 均能超过表 36 中相对应的数值。

[5] 帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

7.1.3.2.2 单播性能检测 2（证书鉴别和密钥管理方式）

测试目的：

验证MTUT和基准AP均为证书鉴别和密钥管理方式，基准AP采用不同的参数配置时，测试MTUT与基准AP之间典型通信的数据吞吐量，从而衡量MTUT与不同基准AP应具有的良好的互通性。

测试拓扑图：

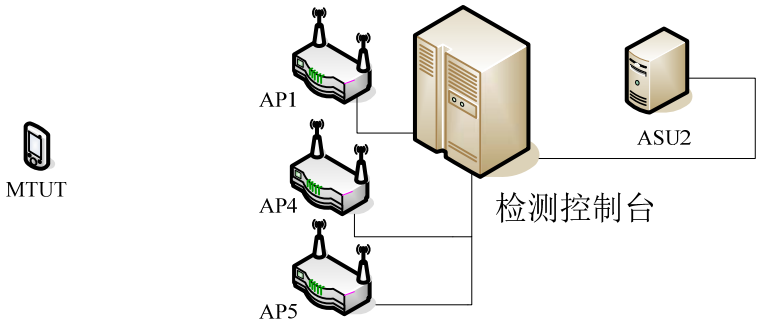


图20 单播性能检测 2（证书鉴别和密钥管理方式）测试拓扑图

测试步骤：

表28 单播性能检测 2 MTUT 和基准 AP 配置信息表

设备	MTUT	AP1	AP4	AP5
模式	-	1	2	3
SSID	-	abcdefghijklmnopqrstuvwxyzABCDEF	abcdefghijklmnopqrstuvwxyzABCDEF	12345678901234567890123456789012
信道	-	157	4	5
信标帧间隔	-	200ms	200ms	200ms
RTS 门限	默认	默认	默认	256
分段门限	默认	500	500	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP1、AP4、AP5和ASU2与检测控制台相连接（见图29），配置ASU2的IP地址为“192.168.1.1”，配置MTUT的IP地址为“192.168.1.100”。ASU2生成颁发者证书、MTUT、AP1、AP2和AP3的证书，其他配置按照上表所述进行配置（见表37），其中：

模式1：AP1为符合GB15629.1101的设备；

模式2：AP4为符合GB15629.1104的设备；

模式3：AP5为符合GB15629.1102的设备；

b) 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表29 性能检测结果判别标准表

模式	1	2	3
T1	≥1.0Mbit/s	≥1.0Mbit/s	≥1.0Mbit/s
T2	≥1.0Mbit/s	≥1.0Mbit/s	≥1.0Mbit/s

T1 表示帧 1[6]下行吞吐量，T2 表示帧 1 上行吞吐量。

a) 步骤b）检测控制台的性能检测结果中，T1、T2均能超过表38 中相对应的数值。

[6]帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

7.1.3.2.3 单播性能检测 3（预共享密钥鉴别和密钥管理方式）

测试目的：

验证MTUT和基准AP均为预共享密钥鉴别和密钥管理方式，基准AP采用不同的参数配置时，测试MTUT与基准AP之间典型通信的数据吞吐量，从而衡量MTUT与不同基准AP应具有的良好的互通性。

测试拓扑图：

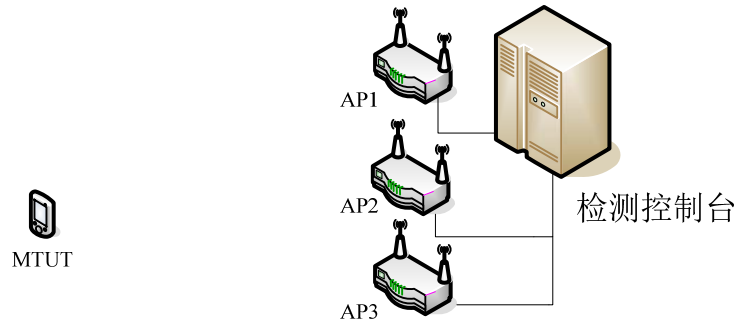


图21 单播性能检测 3（预共享密钥鉴别和密钥管理方式）测试拓扑图

测试步骤：

表30 单播性能检测 3 MTUT 和基准 AP 配置信息表

参数	MTUT	AP1	AP2	AP3
模式	-	1	2	3
SSID	sharekey	sharekey	sharekey	sharekey
信道	-	161	7	8
信标帧间隔	默认	300ms	300ms	300ms
RTS 门限	默认	默认	默认	默认
分段门限	默认	默认	默认	500
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

测试步骤：

a) 将AP1、AP2和AP3与检测控制台相连接（见图30），配置MTUT的IP地址为“192.168.1.100”。预共享密钥为“12345678”，其他配置按照上表所述进行配置（见表39），其中：
模式1：AP1为符合GB15629.1101的设备；
模式2：AP2为符合GB15629.1104的设备；
模式3：AP3为符合GB15629.1102的设备；

b) 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表31 性能结果判别标准表

模式	1	2	3
T1	≥12.4Mbit/s	≥11.4Mbit/s	≥2.3Mbit/s
T2	≥12.6Mbit/s	≥10.6Mbit/s	≥3.6Mbit/s

T1 表示帧 1[7]下行吞吐量，T2 表示帧 1 上行吞吐量。

a） 步骤b）检测控制台的性能检测结果中，T1、T2均能超过表40 中相对应的数值。

7.1.3.3 组播检测

7.1.3.3.1 移动终端组播功能检测

测试目的：

验证STAUT在启用WAPI安全方式和不启用WAPI安全方式下的接收组播帧的能力。

每种模式的测试又分为启用WAPI安全的组播性能检测和不启用安全的组播性能检测。

测试拓扑图：

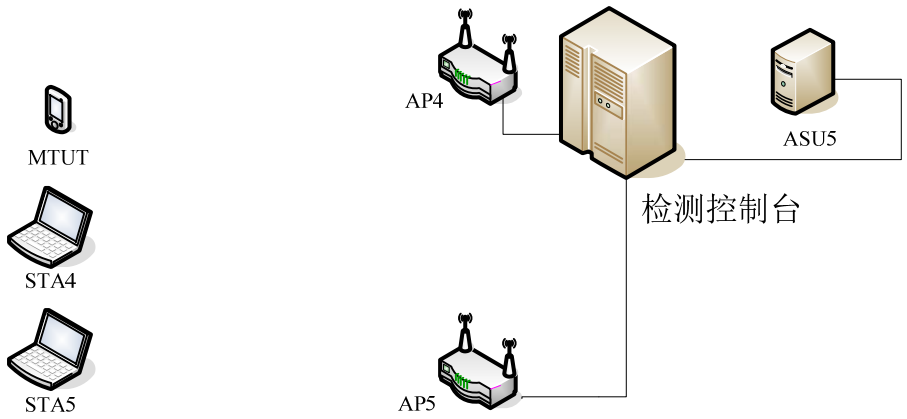


图22 组播功能测试拓扑图

测试步骤：

表32 组播能力检测 MTUT、基准 AP 和基准 STA 配置信息表

设备	AP4	AP5	STA4	STA5	MTUT
模式	1	1	1	1	-
SSID	multicastG	multicastG	multicastG	multicastG	multicastG
信道	10	10	默认	默认	默认
信标帧间隔	100ms	100ms	默认	默认	默认
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
安全方式	证书鉴别和密钥管理方式	开放方式	证书鉴别和密钥管理方式	开放方式	-

a） 将AP4、AP5和ASU5与检测控制台相连接（见图31），配置ASU5的IP地址为“192.168.1.1”，配置MTUT的IP地址为“192.168.1.100”，配置STA4的IP地址为“192.168.1.101”，配置STA5的IP地址为“192.168.1.102”。ASU5生成颁发者证书、MTUT和STA4的证书、AP4的证书，在检测控制台上配置AP4向STA4和MTUT发送组播数据帧，AP5向STA5和MTUT发送组播数据帧；其他配置按照上表所述进行配置（见表41）；

b） MTUT、STA4和AP4启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察MTUT是否能够正确接入AP4，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；

c） 运行检测控制台中的启用证书鉴别和密钥管理方式的安全机制下的组播功能检测；

d） MTUT、STA5和AP5启用开放方式，观察MTUT是否能够正确接入AP5，在检测控制台上运行

[7]帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

“ping 192.168.1.100”，观察是否能够通信成功；

e） 运行检测控制台中的启用开放方式下的组播功能检测；

d） 观察检测控制台上的组播功能检测是否通过。

预期结果：

a） 步骤b）中MTUT能够成功关联至AP4，MTUT与AP4能够成功通信；

b） 步骤c）中MTUT可以接收到AP4向STA4和MTUT发送的组播数据帧，检测控制台的组播功能检测程序必须通过；

c） 步骤d）中MTUT能够成功关联至AP5，MTUT与AP5能够成功通信；

d） 步骤e）中MTUT可以接收到AP5向STA5和MTUT发送的组播数据帧，检测控制台的组播功能检测程序必须通过。

7.2 AP 检测

7.2.1 基础协议检测

7.2.1.1 SSID

测试目的：

验证APUT支持的SSID长度应为0-32字符或长度为0-16个汉字；当SSID不同时，基准STA应无法关联至APUT；不同大小写的SSID应被视作不同的SSID。

测试拓扑图：

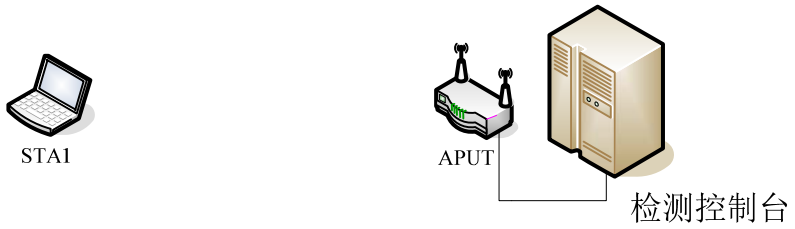


图23 SSID 测试拓扑图

测试步骤：

表33 APUT 和 STA1 配置信息表

设备	APUT	STA1
SSID	根据不同测试用例配置	根据不同测试用例配置
信标间隔	默认	默认
信道	1	1
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	开放方式	开放方式

a） 将APUT与检测控制台相连接（见图32）。配置STA1的IP地址为“192.168.1.100”。

b） 配置APUT和STA1为开放模式，SSID为“default”，采用信道1，其余配置采用默认值(见表42)。如果STA1关联至APUT，则须在检测控制台运行“ping 192.168.1.100”命令，观察APUT能否与STA1通信；

c） 配置APUT的SSID为“abcd”，配置STA1的SSID为默认不填写，连接APUT，观察STA1能否关联至APUT；

d） 配置APUT和STA1的SSID均为“abc”，观察STA1能否关联至APUT；修改APUT的SSID为“def”，观察STA1能否关联至APUT；

e） 配置APUT和STA1的SSID均为“abcdefghijklmnopqrstuvwxyz012345”，STA1能否关联至APUT；

修改APUT的SSID为“abcdefghijklmnopqrstuvwxyz0123456”，观察APUT的SSID设置是否成功；

f) 配置APUT的SSID为“abcdef”，配置STA1的SSID为“abc”，观察STA1能否关联至APUT；

g) 配置APUT的SSID为“abc”，配置STA1的SSID为“abcdef”，观察STA1能否关联至APUT；

h) 配置APUT的SSID为“abc”，配置STA1的SSID为“ABC”，观察STA1能否关联至APUT；

i) 配置APUT的SSID为“ABC”，配置STA1的SSID为“abc”，观察STA1能否关联至APUT；

j) 配置APUT的SSID为“abc”，配置STA1的SSID为“cba”，观察STA1能否关联至APUT；

k) 配置APUT的SSID为“无线局域网”，配置STA1的SSID为默认不填写，连接APUT，观察STA1能否关联至APUT；

l) 配置APUT和STA1的SSID为“无线局域网”，观察STA1能否关联至APUT；修改APUT的SSID为“系统互操作”，观察STA1能否关联至APUT；

m) 配置APUT和STA1的SSID为“无线局域网系统互操作站点功能测试”，观察STA1能否关联至APUT；修改APUT的SSID为“无线局域网系统互操作站点功能测试一”，观察STA1能否关联至APUT。

预期结果：

a） 步骤b)中，STA1能够关联至APUT，并且在检测控制台上能够与APUT通信；

b) 步骤c)中，STA1能够关联至APUT；

c) 步骤d)中，STA1能够关联至APUT，APUT修改SSID后不能与STA1关联；

d) 步骤e)中，STA1能够关联至APUT，APUT修改SSID时不能成功修改；

e) 步骤f)中，STA1不能关联至APUT；

f) 步骤g)中，STA1不能关联至APUT；

g) 步骤h)中，STA1不能关联至APUT；

h) 步骤i)中，STA1不能关联至APUT；

i) 步骤j)中，STA1不能关联至APUT；

j) 步骤k)中，STA1能够关联至APUT；

k) 步骤l)中，STA1能够关联至APUT，APUT修改SSID后不能与STA1关联；

l) 步骤m)中，STA1能够关联至APUT，APUT修改SSID时不能成功修改。

7.2.1.2 关联或重关联

测试目的：

验证基准STA可以从一个基准AP关联或重关联至采用相同SSID的APUT。

测试拓扑图：

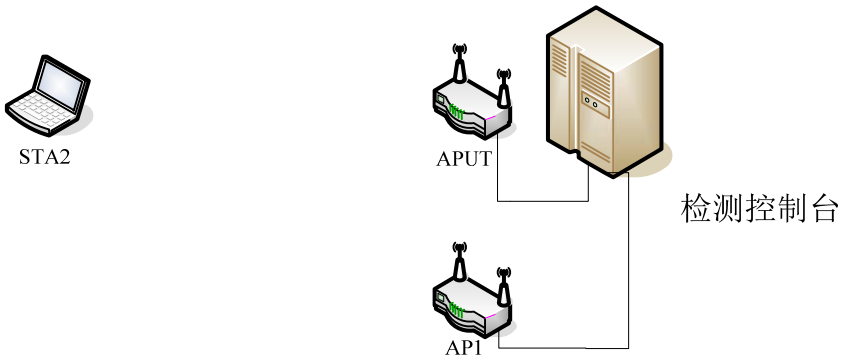


图24 关联或重关联测试拓扑图

测试步骤：

表34　　APUT、AP1 和 STA2 配置信息表

设备	APUT	AP1	STA2
SSID	association	association	association
信标间隔	默认	默认	默认
信道	6	6	6
RTS 门限	默认	默认	默认
分包门限	默认	默认	默认
加密方式	开放方式	开放方式	开放方式

a) 将APUT和AP1与检测控制台相连接（见图33）。配置STAUT的IP地址为“192.168.1.100”。

b) APUT、AP1和STA2为开放方式，SSID为“association”,采用信道6，其他配置按照上表所述进行配置（见表43）。将AP1加电，关闭APUT，观察STA2是否能关联至AP1。若STA2关联至AP1，则在检测控制台上运行“ping 192.168.1.100 -t”，观察AP1是否能与STA2通信。若AP1可以与STA2通信，则保持ping命令，将APUT加电，关闭AP1。抓帧并分析，观察APUT能否响应STA2发出关联或重关联请求帧。检测控制台的ping命令在90秒内能够恢复；

预期结果：

a) 步骤b）中的STA2能够关联至APUT，APUT能够响应STA2发出的关联或重关联请求帧。并且检测控制台上运行的ping命令能够在90秒内恢复通信；

7.2.2　WAPI 协议检测

7.2.2.1　WAI 证书鉴别和密钥管理方式下证书安装与接入控制

测试目的：

验证APUT可以安装X.509 v3证书，并能够对所安装的证书进行删除操作；

验证APUT在启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，能够实现安全接入与保密通信；

验证在APUT与基准STA都启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，当基准STA采用非法X.509 v3证书时，基准STA不能与APUT正常通信；

验证APUT在启用WAI证书鉴别和密钥管理方式下的WAPI安全机制时，基准STA在启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制或不启用WAPI安全机制时，基准STA不能与APUT正常通信。

测试拓扑图：

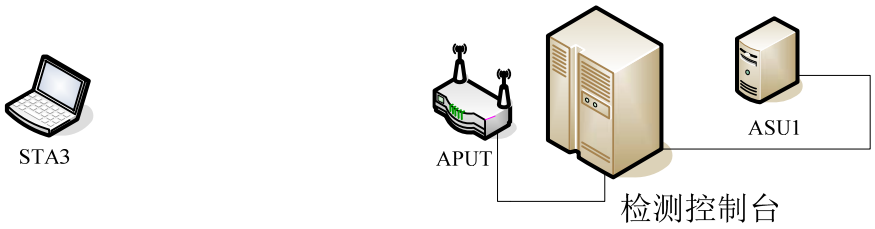


图25　　证书鉴别和密钥管理方式下证书安装与接入控制测试拓扑图

测试步骤：

表35　　APUT 和 STA3 配置信息表

设备	APUT	STA3
SSID	WAPI	WAPI
信标间隔	默认	默认

信道	9	9
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将APUT与检测控制台相连接（见图34），配置STA3的IP地址为“192.168.1.100”；
b) 将ASU1与检测控制台相连接（见图34），配置ASU1的IP地址为“192.168.1.1”。ASU1生成颁发者证书、STA3的证书、APUT的证书、已过期或被吊销的STA的证书；
c) APUT和STA3启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，SSID为“WAPI”，采用信道9，其余配置采用默认值（见表44），在STA3上安装ASU1颁发的X.509 v3证书；
d) 使用ASU1颁发的X.509 v3证书，在APUT上安装，观察APUT是否能够正确安装和成功删除该证书；若能成功删除该证书，则重新安装该证书，观察APUT是否能够正确安装；
e) APUT启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，STA3不启用任何WAPI安全机制，观察STA3是否能够接入APUT；APUT不启用任何WAPI安全机制，STA3启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STA3是否能够接入APUT；APUT不启用任何WAPI安全机制，STA3启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，观察STA3是否能够接入APUT；
f) APUT和STA3启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STA3是否能够正确接入APUT，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；
g) 使用ASU1颁发已过期或被吊销的证书，在STA3上安装，APUT与STA3均开启WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STA3是否能够接入APUT，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功；
h) APUT启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，STA3启用WAI预共享密钥鉴别和密钥管理方式下的WAPI安全机制，观察STA3是否能够接入APUT，在检测控制台上运行“ping 192.168.1.100”，观察是否能够通信成功。

预期结果：

a) 步骤d）证书能够在APUT上被安装和删除；
b) 步骤e）STA3不能接入APUT；
c) 步骤f）STA3能够接入APUT，STA3与APUT能够通信成功；
d) 步骤g）STA3不能接入APUT，STA3与APUT不能通信成功；
e) 步骤h）STA3不能接入APUT，STA3与APUT不能通信成功。

7.2.2.2 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试目的：

验证APUT在启用证书鉴别和密钥管理方式下的WAPI安全机制时，WAPI协议的处理流程、数据格式是否符合GB15629.11系列标准所规定的内容，以及在此基础上和基准STA的互通性。

测试拓扑图：

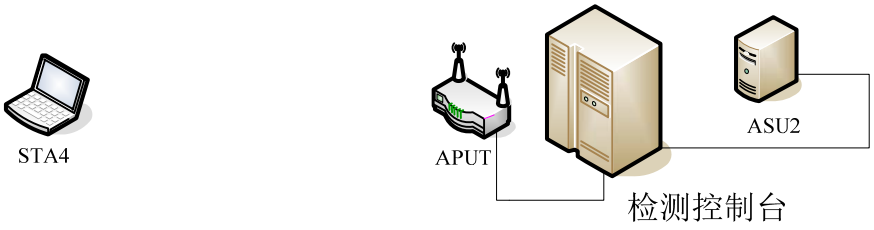


图26 证书鉴别和密钥管理方式下的协议流程与数据格式测试拓扑图

测试步骤：

表36　　APUT 和 STA4 配置信息表

设备	APUT	STA4
SSID	WAPI	WAPI
信标间隔	默认	默认
信道	4	4
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将APUT和ASU2与检测控制台相连接（见图35），配置ASU2的IP地址为“192.168.1.1”。ASU2生成颁发者证书、STA4的证书、APUT的证书；

b) 配置APUT与STA4的SSID均为“WAPI”，采用信道4，在APUT与STA4上安装ASU2生成的X.509 v3证书，其余配置采用默认值（见表45），观察STA4是否能够关联至APUT；

c) 开启检测控制台上的WAI证书鉴别和密钥管理方式下的WAPI检测，根据提示开启APUT和STA4上的WAPI安全机制，检测控制台的WAPI检测程序将对WAPI协议流程进行捕捉分析，并生成检测结果和详细检测纪录。

预期结果：

a) 步骤b）STA4能够关联至APUT

b) 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

APUT发送的包含WAPI参数集合的信标以及发送包含WAPI参数集合的探询响应帧；

STA4关联至APUT时，APUT发出的鉴别激活分组

APUT处理STA4发出的接入鉴别请求后，根据证书验证要求向ASU2发送的证书鉴别请求；

APUT处理ASU2发送的证书鉴别响应后，根据证书的验证结果向STA4发送的接入鉴别响应；

STA4与APUT完成证书鉴别后，APUT向STA4发送的单播密钥协商请求；

APUT处理STA4回应的单播密钥协商响应后，APUT发送的单播密钥协商确认；

APUT发送的单播密钥协商确认中的WIE_{ae}字段应与自身所保存的WAPI参数集合字段必须相同；

APUT完成单播密钥协商后，向STA4发送的组播密钥通告分组；

APUT对数据地进行加解密的操作。

7.2.2.3　WAI 预共享密钥鉴别和密钥管理方式下接入控制

测试目的：

验证 APUT 采用预共享密钥鉴别和密钥管理方式正确进行接入控制的情况。

验证 APUT 在启用预共享密钥鉴别和密钥管理方式下的 WAPI 安全机制时，能够实现安全接入与保密通信。

测试拓扑图：

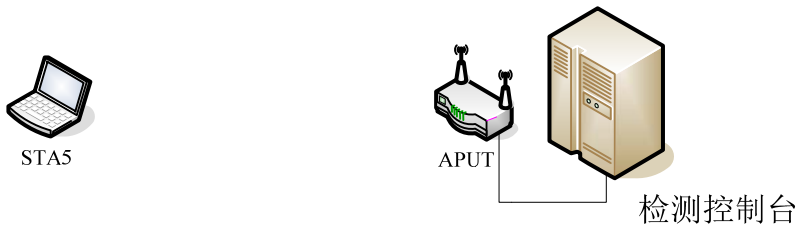


图27　　预共享密钥鉴别和密钥管理方式下的接入控制测试拓扑图

表37　APUT 和 STA5 配置信息表

设备	APUT	STA5
SSID	Sharedkey	sharedkey
信标间隔	默认	默认
信道	11	11
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

a) 将APUT与检测控制台相连接（见图36），配置STA5的IP地址为“192.168.1.100”；
b) 配置STA5与APUT的SSID均为“sharedkey”，采用信道11,其余配置采用默认值（见表46）；
c) 将APUT的预共享密钥设为字符串“12345678”，将STA5的预共享密钥设为字符串“123456789”，观察STA5与APUT是否能够通信；
d) 将APUT的预共享密钥设为字符串“12345678”,将STA5的预共享密钥设为字符串“12345678”，观察STA5是否能够关联至APUT，如果STA5成功关联至APUT，则在检测控制台上运行“ping 192.168.1.100”，观察STA5与APUT是否能够通信；
e) 将APUT的预共享密钥设为十六进制数“0x1234ABCDEF”，将STA5的预共享密钥设为十六进制数“0x1234ABCD”，观察STA5与APUT是否能够通信；
f) 将APUT的预共享密钥设为十六进制数“0x1234ABCD”，将STA5的预共享密钥设为十六进制数“0x1234ABCD”，观察STA5是否能够关联至APUT，如果STA5成功关联至APUT，则在检测控制台上运行“ping 192.168.1.100”，观察STA5与APUT是否能够通信。

预期结果：

a) 步骤c）中STA5与APUT不能通信；
b) 步骤d）中STA5能够成功关联至APUT，STA5与APUT能够成功通信；
c) 步骤e）中STA5与APUT不能通信；
d) 步骤f）中STA5能够成功关联至APUT，STA5与APUT能够成功通信。

7.2.2.4　WAI 预共享密钥鉴别和密钥管理方式下协议流程与数据格式

测试目的：

验证APUT在启用预共享密钥鉴别和密钥管理方式下的WAPI安全机制时，WAPI协议的处理流程、数据格式是否符合GB15629.11系列标准所规定的内容，以及在此基础上和基准AP的互通性。

测试拓扑图：

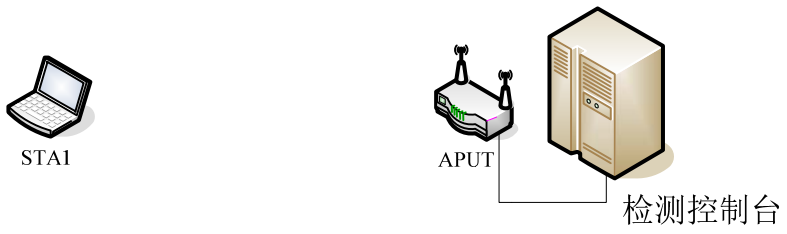


图28　　预共享密钥鉴别和密钥管理方式下的协议流程与数据格式测试拓扑图

测试步骤：

表38　　APUT 和 STA1 配置信息表

设备	APUT	STA1

SSID	Sharedkey	sharedkey
信标间隔	默认	默认
信道	7	7
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

a) 将APUT与检测控制台相连接（见图37）；

b) 配置STA1与APUT的SSID均为“sharedkey”，采用信道7，其余配置采用默认值（见表47）；

c) 将STA1与APUT的预共享密钥均设为字符串“sharedkey”，观察STA1是否能够关联至APUT；

d) 开启检测控制台上的WAI预共享密钥鉴别和密钥管理方式下的WAPI检测，根据提示开启STA1和APUT上的WAPI安全机制，检测控制台的WAPI检测程序将对WAPI协议流程进行捕捉分析，并生成检测结果和详细检测纪录。

预期结果：

a) 步骤c）STA1能够关联至APUT；

b) 步骤d）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

APUT发送的包含WAPI参数集合的信标帧以及发送的包含WAPI参数集合的探询响应帧；

STA1关联至APUT时，APUT向STA1发送的单播密钥协商请求；

APUT处理STA1回应的单播密钥协商响应，向STA1发送的单播密钥协商确认；

APUT发送的单播密钥协商确认中的WIE_{ae}字段与自身所保存的WAPI参数集合字段必须相同；

APUT在单播密钥协商完成后向STA1发送的组播密钥通告分组；

APUT对数据进行加解密的操作。

7.2.2.5 基密钥更新功能

测试目的：

验证 APUT 能够向基准 STA 发起基密钥更新过程，APUT 能够利用新的密钥对数据进行保密通信。

测试拓扑图：

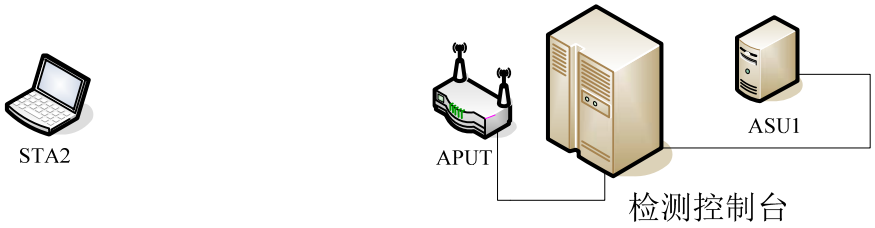


图29 基密钥更新功能测试拓扑图

测试步骤：

表39 APUT 和 STA2 配置信息表

设备	APUT	STA2
SSID	BK	BK
信标间隔	默认	默认
信道	3	3

RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将APUT和ASU1与检测控制台相连接（见图38），配置ASU1的IP地址为“192.168.1.1”，配置STA2的IP地址为“192.168.1.100”。ASU1生成颁发者证书、STA2的证书、APUT的证书；

b) 配置STA2与APUT的SSID均为“BK”，采用信道3，在STA2与APUT上安装ASU1生成的X.509 v3证书，其余配置采用默认值（见表48），观察STA2是否能够关联至APUT；

c) 在APUT上发起对STA2的基密钥更新，检测控制台的WAPI检测程序对APUT与STA2之间的基密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 基密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察APUT与STA2是否能够通信。

预期结果：

a) 步骤b）APUT和STA2能够安装ASU1的证书，STA2能够关联至APUT；

b) 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

鉴别激活分组、接入鉴别请求分组、接入鉴别响应分组、单播密钥协商分组、组播密钥协商分组中的BK更新标识位为1；

STA2关联至APUT时，APUT发出的鉴别激活分组

APUT处理STA2发出的接入鉴别请求后，根据证书验证要求向ASU1发送的证书鉴别请求；

APUT处理ASU1发送的证书鉴别响应后，根据证书的验证结果向STA2发送的接入鉴别响应；

STA2与APUT完成证书鉴别后，APUT向STA2发送的单播密钥协商请求；

APUT处理STA2回应的单播密钥协商响应后，APUT发送的单播密钥协商确认；

APUT发送的单播密钥协商确认中的WIE_{ae}字段应与自身所保存的WAPI参数集合字段必须相同；

APUT完成单播密钥协商后，向STA2发送的组播密钥通告分组；

APUT对数据地进行加解密的操作。

c) 步骤d）基密钥更新完毕后，检测控制台可以与STA2通信。

7.2.2.6 单播会话密钥更新功能

测试目的：

验证 APUT 能够向基准 STA 发起基密钥更新过程，APUT 能够利用新的密钥对数据进行保密通信。

测试拓扑图：

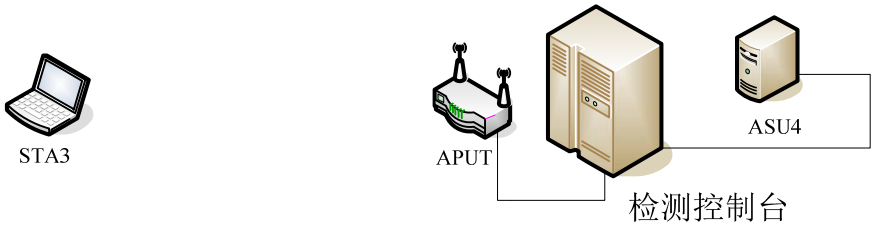


图30 单播会话密钥更新功能测试拓扑图

测试步骤：

表40　　APUT 和 STA3 配置信息表

设备	APUT	STA3
SSID	USK	USK
信标间隔	默认	默认
信道	8	8
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将APUT和ASU4与检测控制台相连接（见图39），配置ASU4的IP地址为“192.168.1.1”，配置STA3的IP地址为“192.168.1.100”。ASU4生成颁发者证书、STA3的证书、APUT的证书；

b) 配置STA3与APUT的SSID均为“USK”，采用信道8，在STA3与APUT上安装ASU4生成的X.509 v3证书，其余配置采用默认值（见表49），观察STA3是否能够关联至APUT；

c) 在APUT上发起对STA3的单播会话密钥更新，检测控制台的WAPI检测程序对APUT与STA3之间的单播会话密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 单播会话密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察 STA3 与 APUT 是否能够通信。

预期结果：

a) 步骤b）STA3和APUT能够安装ASU4的证书，STA3能够关联至APUT；

b) 步骤c）检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

APUT发送的单播密钥协商分组中的USK更新标识位为1；

APUT处理STA3回应的单播密钥协商响应后，APUT发送的单播密钥协商确认；

APUT发送的单播密钥协商确认中的WIE_{ae}字段应与自身所保存的WAPI参数集合字段必须相同；

APUT完成单播密钥协商后，向STA3发送的组播密钥通告分组；

APUT对数据地进行加解密的操作。

c) 步骤d）单播会话密钥更新完毕后，检测控制台可以与STA3通信。

7.2.2.7　组播会话密钥更新功能

测试目的：

验证 APUT 能够向基准 STA 发起基密钥更新过程，APUT 能够利用新的密钥对数据进行保密通信。

测试拓扑图：

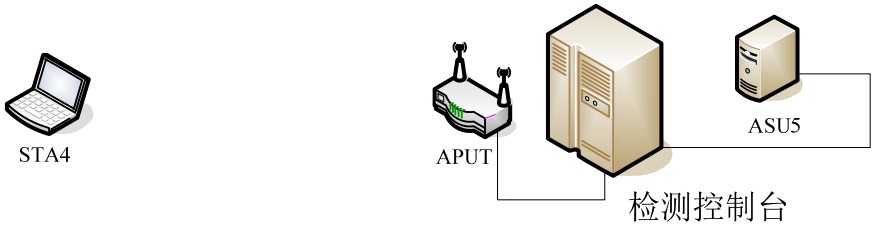


图31　　组播会话密钥更新功能测试拓扑图

测试步骤：

表41　　APUT 和 STA4 配置信息表

设备	APUT	STA4
SSID	MSK	MSK
信标间隔	默认	默认
信道	4	4
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将APUT和ASU5与检测控制台相连接（见图40），配置ASU5的IP地址为“192.168.1.1”，配置STA4的IP地址为“192.168.1.100”。ASU5生成颁发者证书、STA4的证书、APUT的证书；

b) 配置STA4与APUT的SSID均为“MSK”，采用信道4，在STA4与APUT上安装ASU5生成的X.509 v3证书，其余配置采用默认值（见表50），观察STA4是否能够关联至APUT；

c) 在APUT上发起组播会话密钥更新，检测控制台的WAPI检测程序对APUT与STA4之间的组播会话密钥更新流程进行抓取和分析，并生成检测结果和详细检测纪录。

d) 组播会话密钥更新完毕后，在检测控制台上运行“ping 192.168.1.100”，观察 STA4 与 APUT 是否能够通信。

预期结果：

a) 步骤b) STA4和APUT能够安装ASU5的证书，STA4能够关联至APUT；

b) 步骤c) 检测控制台的WAPI检测程序的检测结果必须为通过，详细检测记录必须包括以下内容：

APUT发送的组播密钥通告分组；

STA5发送的组播密钥响应分组。

c) 步骤d) 组播会话密钥更新完毕后，检测控制台可以与STA4通信。

7.2.3 BSS 内 STA 间通信

7.2.3.1 同一 BSS 内 STA 间的通信功能测试

测试目的：

验证 APUT 能够转发其建立的 BSS 内的所有 STA 的报文，使不同基准 STA 之间能够相互通信。

测试拓扑图：

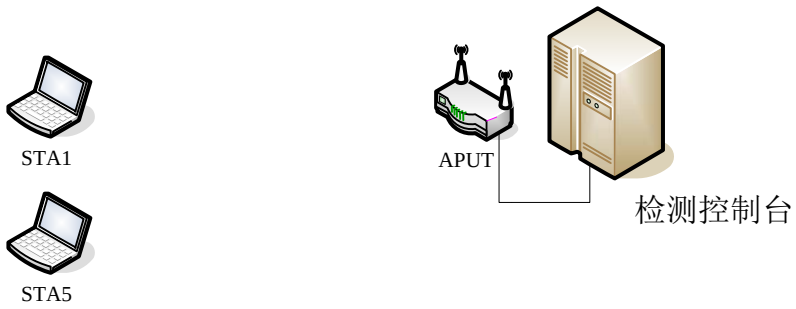


图32 同一 BSS 内 STA 间的通信功能测试拓扑图

测试步骤：

表42 APUT 和 STA1、STA5 配置信息表

设备	APUT	STA1	STA5
SSID	intrabss	intrabss	intrabss
信标间隔	默认	默认	默认

信道	12	12	12
RTS 门限	默认	默认	默认
分包门限	默认	默认	默认
加密方式	开放方式	开放方式	开放方式

a) 将APUT与检测控制台相连接（见图41）。配置STA1的IP地址为“192.168.1.100” STA5的IP地址设置为：“192.168.1.101”。

b) APUT、STA1和STA5为开放方式，SSID为“intrabss”,采用信道12，其他配置按照上表所述进行配置（见表51）。

c) STA1和STA5都关联至APUT,在STA1上运行“ping 192.168.1.101”命令,在STA5上运行“ping 192.168.1.100”命令，观察STA1和STA5上的ping通信命令是否能够成功通信。

预期结果：

a) 步骤c）在STA1和STA5上的ping通信命令能够成功通信。

7.2.4 性能测试.

7.2.4.1 单播性能检测 1（开放方式）

测试目的：

APUT和基准STA均开启开放方式，测试当基准STA采用不同的参数配置时，APUT与基准STA之间典型通信的数据吞吐量，从而衡量APUT与不同基准STA间具有的良好的互通性。

测试拓扑图：

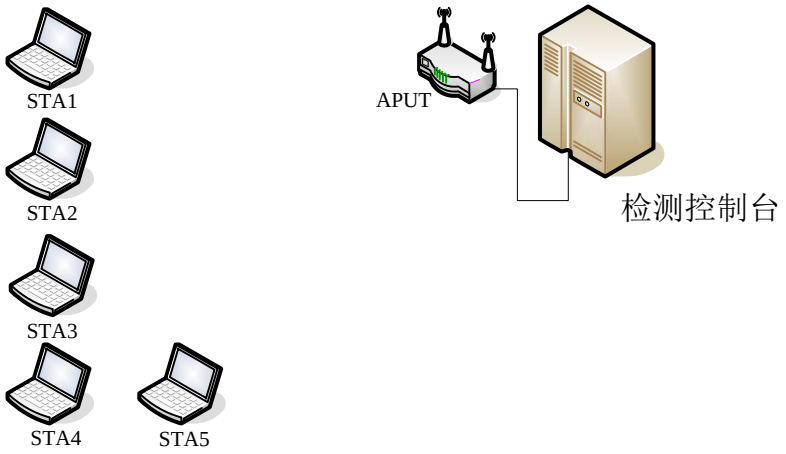


图33 单播性能检测 1（开放方式）测试拓扑图

测试步骤：

表43 单播性能检测 1 APUT 和基准 STA 配置信息表

设备	APUT	STA1	STA2	STA3	STA4
模式	-	1	2	3	4
SSID	-	a	g	b	mix
信道	-	149	11	2	3
信标帧间隔	100ms	100ms	100ms	100ms	100ms
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
加密方式	开放方式	开放方式	开放方式	开放方式	开放方式
				设备	STA5

模式	4
SSID	a
信道	3
信标帧间隔	-
RTS 门限	256
分段门限	500
加密方式	开放方式

a) 将APUT与检测控制台相连接（见图42），配置STA1的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”，配置STA3的IP地址为“192.168.1.102”，配置STA4的IP地址为“192.168.1.103” 配置STA5的IP地址为“192.168.1.104”。APUT根据检测模式配置SSID，保证和模式中的基准STA的SSID相同，其余配置见表52，其中：
模式1：STA1为符合GB15629.1101的设备；
模式2：STA2为符合GB15629.1104的设备；
模式3：STA3为符合GB15629.1102的设备；
模式4：STA4为符合GB15629.1104的设备，STA5为符合GB15629.1102的设备。

b) APUT 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表44 性能检测结果判别标准表

模式	1	2	3	4
T1	≥12.5Mbit/s	≥12.5Mbit/s	≥3.7Mbit/s	≥3.06Mbit/s,BT1≥2.47Mbit/s
T2	≥14.2Mbit/s	≥14.2Mbit/s	≥3.7Mbit/s	≥3.09Mbit/s,BT2≥1.17Mbit/s
T3	≥1.22Mbit/s	≥1.22Mbit/s	≥0.54Mbit/s	≥0.58Mbit/s,BT3≥0.39Mbit/s

T1 表示帧 1[8]下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2[9]下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行吞吐量。

a) 步骤 b) 检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2 和 BT3 均能超过表 11 中相对应的数值。

[8] 帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。
[9] 帧 2:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100 字节。

7.2.4.2 单播性能检测 2（证书鉴别和密钥管理方式）

测试目的：

APUT和基准STA均开启开放方式，测试当基准STA采用不同的参数配置时，APUT与基准STA之间典型通信的数据吞吐量，从而衡量APUT与不同基准STA间具有的良好的互通性。

测试拓扑图：

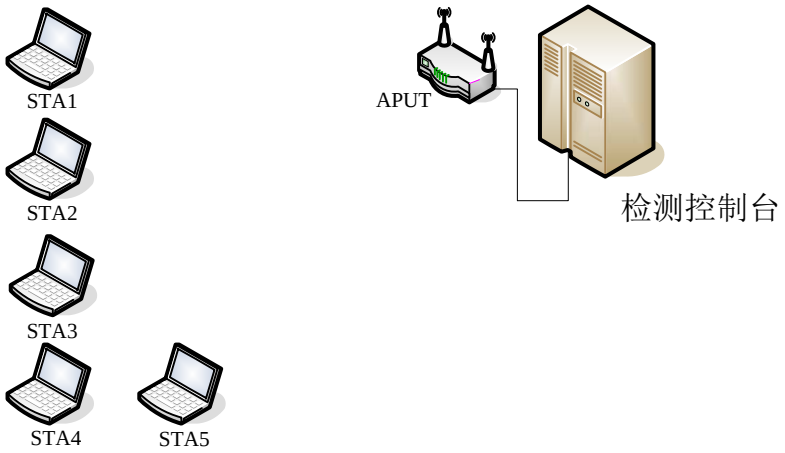


图34 单播性能检测 2（证书鉴别和密钥管理方式）测试拓扑图

测试步骤：

表45 单播性能检测 2 APUT 和基准 STA 配置信息表

设备	APUT	STA1	STA4	STA5	STA2
模式	-	1	2	3	4
SSID	-	a	g	b	mix
信道	-	149	11	2	3
信标帧间隔	100ms	100ms	100ms	100ms	100ms
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
加密方式	开放方式	开放方式	开放方式	开放方式	开放方式

设备	STA3
模式	4
SSID	a
信道	3
信标帧间隔	-
RTS 门限	256
分段门限	500
加密方式	开放方式

a) 将APUT与检测控制台相连接（见图42），配置STA1的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”，配置STA3的IP地址为“192.168.1.102”，配置STA4的IP地址为“192.168.1.103” 配置STA5的IP地址为“192.168.1.104”。APUT根据检测模式配置SSID，保证和模式中的基准STA的SSID相同，其余配置见表52，其中：
模式1：STA1为符合GB15629.1101的设备；

模式2：STA4为符合GB15629.1104的设备；

模式3：STA5为符合GB15629.1102的设备；

模式4：STA2为符合GB15629.1104的设备，STA3为符合GB15629.1102的设备。

b) APUT 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表46 性能检测结果判别标准表

模式	1	2	3	4
T1	≥12.5Mbit/s	≥12.5Mbit/s	≥3.7Mbit/s	≥3.06Mbit/s,BT1≥2.47Mbit/s
T2	≥14.2Mbit/s	≥14.2Mbit/s	≥3.7Mbit/s	≥3.09Mbit/s,BT2≥1.17Mbit/s
T3	≥1.22Mbit/s	≥1.22Mbit/s	≥0.54Mbit/s	≥0.58Mbit/s,BT3≥0.39Mbit/s

T1 表示帧 1[10]下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2[11]下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行吞吐量。

a) 步骤 b）检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2 和 BT3 均能超过表 55 中相对应的数值。

[10] 帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

[11] 帧 2:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100 字节。

7.2.4.3 单播性能检测 3（预共享密钥鉴别和密钥管理方式）

测试目的：

APUT和基准STA均开启开放方式，测试当基准STA采用不同的参数配置时，APUT与基准STA之间典型通信的数据吞吐量，从而衡量APUT与不同基准STA间具有的良好的互通性。

测试拓扑图：

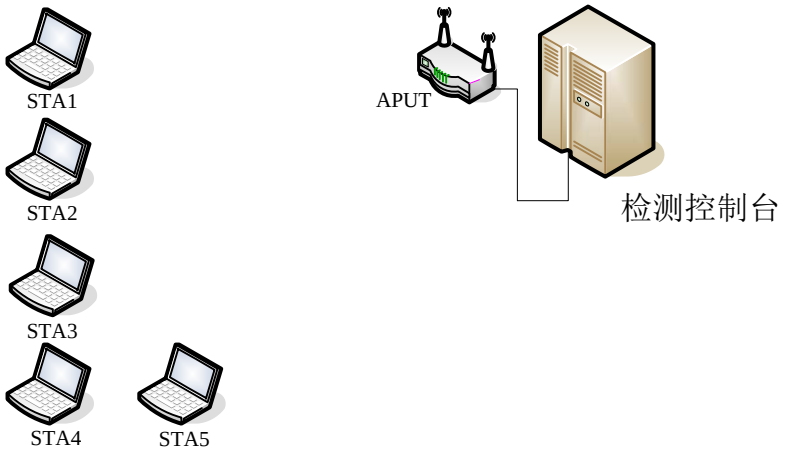


图35 单播性能检测 3（预共享密钥鉴别和密钥管理方式）测试拓扑图

测试步骤：

表47 单播性能检测 3 APUT 和基准 STA 配置信息表

参数	APUT	STA1	STA2	STA3	STA4
模式	-	1	2	3	4
SSID	sharekey	sharekey	sharekey	sharekey	sharekey
信道	-	161	7	8	9
信标帧间隔	默认	300ms	300ms	300ms	300ms
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	500	默认
加密方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式	预共享密钥鉴别和密钥管理方式

参数	STA5
模式	4
SSID	sharekey
信道	-
信标帧间隔	-
RTS 门限	256
分段门限	默认
加密方式	预共享密钥鉴别和密钥管理方式

a) 将APUT与检测控制台相连接（见图44），配置STA1的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”，配置STA3的IP地址为“192.168.1.102”，配置STA4的IP地址为“192.168.1.103” 配置STA5的IP地址为“192.168.1.104”。APUT根据检测模式配置SSID，保证和模式中的基准STA的SSID相同，预共享密钥为“12345678”，其余配置见表56，其中：

模式1：STA1为符合GB15629.1101的设备；

模式2：STA2为符合GB15629.1104的设备；

模式3：STA3为符合GB15629.1102的设备；

模式4：STA4为符合GB15629.1104的设备，STA5为符合GB15629.1102的设备。

b) APUT 在检测控制台上运行单播性能检测程序，观察性能检测结果。

预期结果：

表48 性能检测结果判别标准表

模式	1	2	3	4
T1	≥1.4Mbit/s	≥1.4Mbit/s	≥1.4Mbit/s	≥1.80Mbit/s，BT1≥2.5Mbit/s
T2	≥0.27Mbit/s	≥0.27Mbit/s	≥0.27Mbit/s	≥1.50Mbit/s，BT2≥0.44Mbit/s
T3	≥0.003Mbit/s	≥0.003Mbit/s	≥0.003Mbit/s	≥0.007Mbit/s，BT3≥0.37Mbit/s

T1 表示帧 1[12]下行吞吐量，T2 表示帧 1 上行吞吐量，T3 表示帧 2[13]下行吞吐量。BT1 表示混合模式下的帧 1 下行吞吐量，BT2 表示混合模式下的帧 1 上行吞吐量，BT3 表示混合模式下的帧 2 下行吞吐量。

a) 步骤 b）检测控制台的性能检测结果中，T1、T2、T3 、BT1、BT2 和 BT3 均能超过表 57 中相对应的数值。

7.2.5 组播检测

7.2.5.1 组播功能测试

测试目的：

检测APUT在启用WAPI安全方式和不启用WAPI安全方式下的发送组播帧的能力；

APUT组播功能测试分为启用WAPI安全的组播性能检测和不启用安全的组播性能检测。

测试拓扑图：

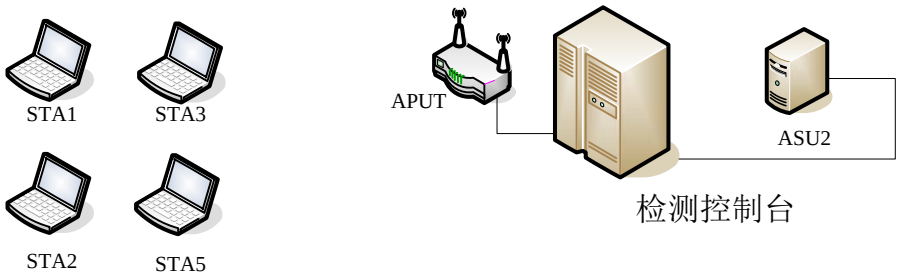


图36 组播功能测试拓扑图

测试步骤：

表49 组播能力检测 APUT 和基准 STA 配置信息表

设备	APUT	STA1	STA2	STA3	STA5
模式	1	1	1	-	-

[12] 帧 1:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100000 字节。

[13] 帧 2:在检测吞吐量时用到的特别规定的以太网数据帧,此帧的帧长度默认为 100 字节。

SSID	multicastG	multicastG	multicastG	multicastG	multicastG
信道	10	默认	默认	默认	默认
信标帧间隔	100ms	默认	默认	默认	默认
RTS 门限	默认	默认	默认	默认	默认
分段门限	默认	默认	默认	默认	默认
安全方式	证书鉴别和密钥管理方式/开放方式	证书鉴别和密钥管理方式	开放方式	证书鉴别和密钥管理方式	开放方式

a) 将APUT和ASU2与检测控制台相连接（见图45），配置ASU2的IP地址为“192.168.1.1”，配置STA1的IP地址为“192.168.1.100”，配置STA2的IP地址为“192.168.1.101”，配置STA3的IP地址为“192.168.1.102”，配置STA5的IP地址为“192.168.1.103”。ASU2生成颁发者证书、STA1、STA2、STA3和STA5的证书、APUT的证书，在检测控制台上配置APUT向STA1和STA3发送一次组播数据帧，APUT向STA2和STA5发送一次组播数据帧；其他配置见表58；

b) STA1、STA3启用WAI证书鉴别和密钥管理方式下的WAPI安全机制，观察STA1、STA3是否能够正确接入APUT，在检测控制台上运行“ping 192.168.1.100”和“ping 192.168.1.102”，观察是否能够通信成功；

c) 运行检测控制台中的启用证书鉴别和密钥管理方式的安全机制下的组播功能检测；

d) STA2、STA5和APUT启用开放方式，观察STA2、STA5是否能够正确接入APUT，在检测控制台上运行“ping 192.168.1.101” 和“ping 192.168.1.103”，观察是否能够通信成功；

e) 运行检测控制台中的启用开放方式下的组播功能检测；

d) 观察检测控制台上的组播功能检测是否通过。

预期结果：

a) 步骤b）中STA1、STA3能够成功关联至APUT，STA1、STA3与APUT能够成功通信；

b) 步骤c）中STA1、STA3可以接收到APUT向STA1和STA3发送的组播数据帧，检测控制台的组播功能检测程序必须通过；

c) 步骤d）中STA2、STA5能够成功关联至APUT，STA2、STA5与APUT能够成功通信；

d) 步骤e）中STA2、STA5可以接收到APUT向STA2和STA5发送的组播数据帧，检测控制台的组播功能检测程序必须通过。

7.3 AS 检测

7.3.1 X.509 v3 证书

7.3.1.1 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试目的：

验证ASUT能够响应基准AP的发送的证书鉴别请求，能够在作出鉴别结果后向基准AP发送的证书鉴别响应。

测试拓扑图：

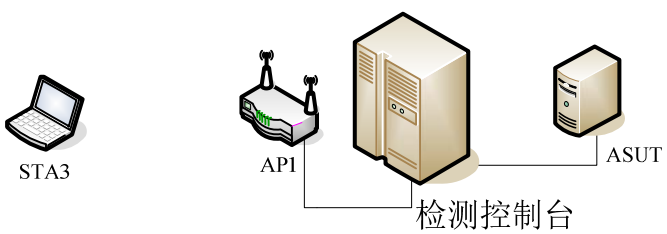


图37 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试步骤：

表50 STA3 和 AP1 配置信息表

设备	AP1	STA3
SSID	WAPI	WAPI
信标间隔	默认	默认
信道	9	9
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP1和ASUT与检测控制台相连接（见图46），配置ASUT的IP地址为“192.168.1.1”，配置STA3的IP地址为“192.168.1.100”，ASUT生成颁发者证书、STA3的证书、AP1的证书、已过期或被吊销的AP1和STA3的证书；在AP1证书安装中安装合法的X.509 v3证书，已吊销的X.509 v3证书。在STA3的证书安装中安装合法的X.509 v3证书，已吊销的X.509 v3证书；
b) 用AP1的合法X.509v3证书和STA3的合法的X.509v3证书组合模拟证书鉴别请求发送给ASUT；
c) 运行检测控制台中的基于ASUT的WAI检测，程序将模拟AP1与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕捉分析，判别ASUT是否采用正确的协议流程和数据封装；
d) 用APUT的合法的X.509v3证书和STA3的已吊销的X.509v3证书组合模拟证书鉴别请求发送给ASUT；
e) 程序将模拟AP1与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装；
f) 用AP1的已吊销的X.509v3证书和STA3的合法的X.509v3证书组合模拟证书鉴别请求分组发送给ASUT；
g) 程序将模拟AP1与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装；
h) 用AP1的已吊销的X.509v3证书和STA3的已吊销的X.509v3证书组合模拟证书鉴别请求分组发给ASUT；
i) 程序将模拟AP1与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装。

预期结果：

a) 步骤c）能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识；
b) 步骤e）能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识；
c) 步骤g）能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识；
d) 步骤i）能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识。

7.3.2 P12 证书

7.3.2.1 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试目的：

验证ASUT能够生成P12格式的证书，能够通过P12证书对基准AP和基准STA进行鉴别。

测试拓扑图：

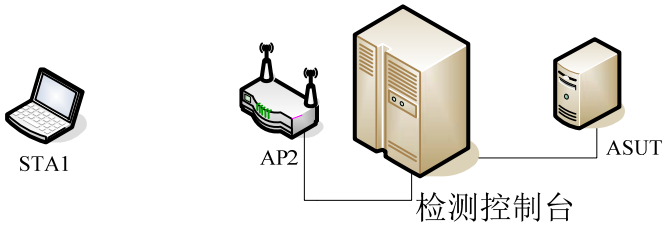


图38 WAI 证书鉴别和密钥管理方式下协议流程与数据格式

测试步骤：

表51　　STA1 和 AP2 配置信息表

设备	AP2	STA1
SSID	WAPI	WAPI
信标间隔	默认	默认
信道	1	1
RTS 门限	默认	默认
分包门限	默认	默认
加密方式	证书鉴别和密钥管理方式	证书鉴别和密钥管理方式

a) 将AP2和ASUT与检测控制台相连接（见图47），配置ASUT的IP地址为“192.168.1.1”，配置STA1的IP地址为“192.168.1.100”，ASUT生成颁发者证书、STA1的P12格式证书、AP2的P12格式证书、已过期或被吊销的AP2和STA1的P12格式证书；在AP2证书安装中安装合法的X.509 v3证书，已吊销的X.509 v3证书。在STA1的证书安装中安装合法的X.509 v3证书，已吊销的X.509 v3证书，P12格式证书的密码设置为“12345678”；

b) 用AP2的合法X.509v3证书和STA1的合法的X.509v3证书组合模拟证书鉴别请求发送给ASUT；

c) 运行检测控制台中的基于ASUT的WAI检测，程序将模拟AP2与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕捉分析，判别ASUT是否采用正确的协议流程和数据封装；

d) 用APUT的合法的X.509v3证书和STA1的已吊销的X.509v3证书组合模拟证书鉴别请求发送给ASUT；

e) 程序将模拟AP2与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装；

f) 用AP2的已吊销的X.509v3证书和STA1的合法的X.509v3证书组合模拟证书鉴别请求分组发送给ASUT；

g) 程序将模拟AP2与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装；

h) 用AP2的已吊销的X.509v3证书和STA1的已吊销的X.509v3证书组合模拟证书鉴别请求分组发给ASUT；

i) 程序将模拟AP2与ASUT之间发送的证书鉴别请求分组，通过对证书鉴别过程中的分组进行捕获分析，判断ASUT是否采用正确的协议流程和数据封装。

预期结果：

a) 步骤c)能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识；

b) 步骤e)能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别

响应报文对认证结果进行标识；

c) 步骤g)能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识；

d) 步骤i)能对模拟的证书鉴别请求发回正确的证书鉴别响应，报文格式正确完整，并在证书鉴别响应报文对认证结果进行标识。

附录

测试项目一览表

一、说明

附录给出了本规范规定的全部测试项目的列表。

二、测试项目一览表

表1　STA测试项目一览表

测试项目	引用条号	支持
SSID	7.1.1.1.1	是□　否□
关联或重关联	7.1.1.1.2	是□　否□
WAI 证书鉴别和密钥管理方式下证书安装与接入控制	7.1.1.2.1	是□　否□
WAI证书鉴别和密钥管理方式下协议流程与数据格式	7.1.1.2.2	是□　否□
WAI预共享密钥鉴别和密钥管理方式下的接入控制	7.1.1.2.3	是□　否□
WAI预共享密钥鉴别和密钥管理方式下的协议流程与数据格式	7.1.1.2.4	是□　否□
基密钥更新功能	7.1.1.2.5	是□　否□
单播会话密钥更新功能	7.1.1.2.6	是□　否□
组播会话密钥更新功能	7.1.1.2.7	是□　否□
单播性能检测1	7.1.1.3.1	是□　否□
单播性能检测2	7.1.1.3.2	是□　否□
单播性能检测3	7.1.1.3.3	是□　否□
组播功能测试	7.1.1.4.1	是□　否□
主动扫描	7.1.2.1.1	是□　否□
被动扫描	7.1.2.1.2	是□　否□
加入与重加入IBSS	7.1.2.1.3	是□　否□
密钥设置与接入控制	7.1.2.2.1	是□　否□

移动终端漫游功能检测	7.1.3.1	是□ 否□
移动终端性能测试	7.1.3.2	是□ 否□
移动终端组播功能检测	7.1.3.3	是□ 否□

表2 AP测试项目一览表

测试项目	引用条号	支持
SSID	7.3.1.1	是□ 否□
关联或重关联	7.3.1.2	是□ 否□
WAI证书鉴别和密钥管理方式下证书安装与接入控制	7.3.2.1	是□ 否□
WAI证书鉴别和密钥管理方式下协议流程与数据格式	7.3.2.2	是□ 否□
WAI预共享密钥鉴别和密钥管理方式下的接入控制	7.3.2.3	是□ 否□
WAI预共享密钥鉴别和密钥管理方式下的协议流程与数据格式	7.3.2.4	是□ 否□
基密钥更新功能	7.3.2.5	是□ 否□
单播会话密钥更新功能	7.3.2.6	是□ 否□
组播会话密钥更新功能	7.3.2.7	是□ 否□
同一BSS内STA间的通信功能测试	7.3.3.1	是□ 否□
单播性能检测1	7.3.4.1	是□ 否□
单播性能检测2	7.3.4.2	是□ 否□
单播性能检测3	7.3.4.3	是□ 否□
组播功能检测	7.3.5.1	是□ 否□

表3　　AS测试项目一览表

测试项目	引用条号	支持
X509v3证书　WAI证书鉴别和密钥管理方式下协议流程与数据格式	7.4.1.1	是□　　否□
P12证书　　WAI证书鉴别和密钥管理方式下协议流程与数据格式	7.4.2.1	是□　　否□