GJS01-H-3X3-C 24芯卧式光缆接头盒 室外三进三出接续盒 哈呋式双端光纤接头包

产品名称	GJS01-H-3X3-C 24芯卧式光缆接头盒 室外三进三出接续盒 哈呋式双端光纤接头包
公司名称	浙江泰平通信技术有限公司
价格	.00/件
规格参数	品牌:PTTP普天泰平 型号:GJS01/GPJ01立式/卧式 产地:浙江.宁波
公司地址	慈溪市观海卫镇工业区
联系电话	0574-63622522 13736014228

产品详情

GJS01-H-3X3-C 24芯卧式光缆接头盒 室外三进三出接续盒 哈呋式双端光纤接头包

「PTTP普天泰平&GJS01系列通信光缆接续盒|接头盒/接续包」光缆接头盒|GJS01型光缆接头盒|GPJ01系列光缆接续盒（opticalcable connect,jointbox）【（哈呋式/卧式）（炮筒式/立式）】光缆接线盒,光缆接续盒,光缆接续包,光缆接头包规格（12芯,24芯,48芯,72芯,96芯,144芯,288芯）光缆接头盒是通俗的叫法,学名叫光缆接续盒,又称光缆接续包,光缆接头包和炮筒,主要是在适用于各种结构光缆的架空,管道,直埋等敷设方式之直通和分支连接。盒体采用进口增强塑料,强度高,耐腐蚀,终端盒适用于结构光缆的终端机房内的接续,结构成熟,密封可靠,施工方便。 广泛用于通信,网络系统,CATV有线电视,光缆网络系统等等。

光缆接头盒是根据通信标准专业设计用以保护光纤接续点的产品,泰平通信提供全规格,多种类的光缆接头盒,旗下产品卧式光缆接头盒与帽式光缆接头盒可用以地埋,架空,管道,人井等多种场合,防护等级达到IP65。

GJS01/GPJ系列卧式光缆接头盒（哈呋式）

光缆接头盒是对光缆的接续提供可靠保护的无源设备。光缆接头盒由接头盒罩、固定组件、接头盒密封组件以及余纤收留盘四部分构成。

产品特点

可提供光缆的直通、分歧、熔接功能

适用于架空、和管道人井壁挂以及直埋安装

内装层叠式熔接盘，开启方便，可以取下操作，便于线路安装及维护

选择熔接盘，适合带状光纤或集成束状光纤，可在大容量内任意配置

走纤规范，确保光纤、光缆在任何位置的弯曲曲率半径大于30mm

订货信息

名称

型号

规格

满配容量

密封方式

光缆进出口数

适用缆径

安装方式

高×宽×深（mm）

束状

带状

GJS01/GPJ01型光缆接头盒（卧式）

GJS-01A

474×222×124

96

144

机械密封

2进2出

φ8-16mm

架空、壁挂、直埋

GJS-01B

388×185×104

96

144

机械密封

3进3出

4孔：φ8-13mm

2孔：φ8-16mm

架空、壁挂

GJS-01C

560×245×180

384

432

机械密封

8进8出

2孔：φ2-23mm

2孔：φ2-20mm

4孔：φ4-16mm

8孔：φ8-14mm

GJS-01D

455×180×120

96

--

机械密封

2进2出

φ10-17.5mm

GPJ-01A

474×201×150

144

432

机械密封

2进2出

φ10-20mm

GPJ-01B

460×180×108

96

--

机械密封

2进2出

φ7-18mm

GJS01/GPJ系列帽式光缆接头盒

光缆接头盒主要适用于架空光缆、直埋光缆、管道井光缆的直通和分歧接头，并对接头起保护作用。

产品特点

可提供光缆的直通、分歧、熔接功能

适用于架空、管道人井壁挂以及抱杆安装

内装层叠式熔接盘，开启方便，可以取下操作，便于线路安装及维护

选择熔接盘，适合带状光纤或集成束状光纤，可在大容量内任意配置

走纤规范，确保光纤、光缆在任何位置的弯曲曲率半径大于30mm

产品特点

可提供光缆的直通、分歧、熔接功能

适用于架空、管道人井壁挂以及抱杆安装

内装层叠式熔接盘，开启方便，可以取下操作，便于线路安装及维护

选择熔接盘，适合带状光纤或集成束状光纤，可在大容量内任意配置

走纤规范，确保光纤、光缆在任何位置的弯曲曲率半径大于30mm

产品特点

可提供光缆的直通、分歧、熔接功能

适用于架空、管道人井壁挂以及抱杆安装

内装层叠式熔接盘，开启方便，可以取下操作，便于线路安装及维护

选择熔接盘，适合带状光纤或集成束状光纤，可在大容量内任意配置

走纤规范，确保光纤、光缆在任何位置的弯曲曲率半径大于30mm

订货信息

名称

型号

规格

满配容量

密封方式

光缆进出口数

适用缆径

安装方式

高×宽×深（mm）

束状

带状

GJS01/GPJ01系列光缆接头盒（帽式）

GJS-M01

435×190

96

--

热缩密封

1直通3分歧

分歧孔：φ8-16mm

直通孔：φ8-25mm

架空、壁挂、抱杆

GJS-M02

598×285

960

--

机械密封

1直通8分歧

分歧孔：φ8-22mm

直通孔：φ8-23mm

GPJ-M01

450×230

144

432

机械密封

1直通4分歧

分歧孔：φ8-18mm

直通孔：φ8-18mm

GPJ-M02

520×245

96

--

机械密封

1直通4分歧

分歧孔：φ5-17.5mm

直通孔：φ8-17.5mm

GPJ-M03

460×230

144

432

热缩密封

1直通4分歧

分歧孔：φ7-22mm

直通孔：φ7-22mm

实际上，所有的WiFi流量都可以在监控模式下使用适配器进行嗅探。大多数Linux发行版都支持将某些WiFi芯片组放入这个监控的模式中，这样就可以处理所有网络流量。

加密的网络也没有你想象的安全，WEP加密甚至WPA2-PSK都是不安全的，攻击者可以通过欺骗一个deauthentication框架来强制一个新的身份验证过程，从而将你的设备与网络断开。

由于嗅探流量是被动进行的，不能被检测到。所以实际上所有开放或关闭的WiFi通信都是公开的，这就要求在更高层次上进行通信加密，比如HTTPs。

暴力访问

和其他密码一样，无线网络的密码也可以被暴力获取。WEP可以通过分析记录的流量在几分钟内被破解，并被渲染成无用的。所以对于WPA安全网络，黑客只需要一个标准的字典攻击即可达到目的。

实际上，目前大多数暴力破解工具都是针对WiFi流量的。

像流量嗅探一样，这种方法也是可以被检测到的。唯一的保护的方法是使用强密码，避免WEP加密。

WiFi网络干扰

在802.11协议标准下，干扰WiFi网络的方法很简单，就是将相关的通信频率填充大量垃圾。具体过程就是：利用Deauthentication和disassociation框架。

因为deauth框架是管理框架，它们是未加密的，即使没有连接到网络，任何人都可以对修改它。通过在框架中设置“发送器”地址，攻击者可以处于攻击范围内，不但可以发送持续的deauth框架，而且还能监听你的设备发送的指令。甚至干扰器脚本能监测出所有接入点和客户机的列表，同时不断的将deauth框架发送给所有的用户。