王涛1 2007-01-04 发表

XLog网络流量分析系统配合AR46收集NetStream日志的配置					
 组网需求: XLog网络流量分析系统支持与交换机、路由器等设备联合组网,接收并记录网络日志信息,为用户提供直观、准确的网络流量统计结果,用户可以从其中了解到网络流量的分布情况、历史趋势、网络应用的流量分布以及网络流量的异常信息等。 组网图: 					
<image/>					
XLog服务器操作系统为Windows 2003 Server, XLog版本2.10-R0120 三 配置步骤: 1 登陆XLog配置管理台 打开IE浏览器,在地址栏中输入XLog NTAS登录的URL,如下图: 日本線收管理 区域					
日志被牧配资信息 高未进行日志被牧配资 起版					
图1 XLog配置管理台访问URL XLog配置管理台安装完成时,会提示用户登录XLog的方式,如果配置管理台安装用 的HTTP端口是默认的80端口,那么登录的时候只需要输入IP地址即可,例 如: <u>http://192.168.4.30</u> 。如果选择的端口不是80端口,而是用户自己指定的端口, 比如:8080,那么登录的时候就需要输入IP地址+冒号+端口号的形式,例如: <u>http://</u> 192.168.4.30:8080。打开登录页面,如下图所示:					
Eth0/0/1 Eth0/0/0:192.168.4.2/24 AR46 192.168.4.30 Eth0:192.168.2.1/24					
图2 XLog NTAS登录窗口 输入正确的用户名和密码,单击<登录>按钮进入XLog NTAS。(系统管理员admin的 缺省密码为Admin)。 2 配置管理台窗口介绍					

设备名称 接口名	称 流入途率	所占比例	流出速率	所占比例
R46(192.168.4.2) 2个接口			0.001	
GigabitEthern	<u>et1/0/0</u> 0.00 bps <1 et1/0/0 0.00 bps <1	%	0.00 bps 0.00 bps	<1%
1信息列表(最近一小时	.)			
	目前还未配置任	何接口姐。		
	配置接到	3組		
	图3 配置	管理台窗口	个绍	
便于后续的操作	, 需要说明配置台	的窗口区域的	划分。如	上图所示左面的
」"导航菜单区",	右面的窗口区域为"	主窗口"。在1	以下的配置	置过程中都按照证
述对应窗口区域				
配置设备信息				
□导航采单区的[M 加下航 示 ・	的络流重分析官理/19	之备信息官理	采早坝,	进入设备信息官
作 局:ADMIN (192.168.2.135)	④登录时间:2006年11)	3日 星期五 上午11时035	23秒 22 单改密码	⑦ 帮助 0 关于 🥥 语
18.9488	及备信息列表 (最近一小时)			Ritki
1887		目前还未配置任何	设备	
2X87	C160/070/# / 8/25 - 4.043	EAUN		
12	11001020754C (BEEL - 17637	目前还未配置任何非	ю ш.	
物管理 管理		配置接口组		
2NT2				
当我管理 远班管理		主窗口		
}航菜单区				
右上角的<增加。	图4 设备 •按钮,进入增加设 ***	·信息管理主管 备信息窗口, 森: •	መር해 . 窗口 如下图:	麦湖 重要 增加
;右上角的<增加; 痛息管理 痛息一覧	图4 设备 按钮,进入增加设 _{党备}	·信息管理主管 备信息窗口, 3称: [*	窗口 如下图:	查词 重量 增加
5右上角的<增加> 信息管理 信息管理 1条记录,当前显示第 13 改善名案。	图4 设备 •按钮,进入增加设 ****	:信息管理主管 备信息窗口, 5称: ┣ [15 ■ 条U] ¥#64	部刊。 如下图:	
后右上角的<增加> 信息管理 信息一覧 1.条记录,当前显示第 13 <u>设备名集。</u> 26 192.18	图4 设备 -按钮,进入增加设 设备 3) 1条记录•第 1/1页 <u>各印 设备编述</u> (8.4.2 AR46	:信息管理主覧 备信息窗口, 3条: □ [15] 条辺 済物信息 済物信息	窗口 如下图: 如下图: () () () () () () () () () () () () ()	211 III IIII 211 III IIII 211 IIIII 211 IIIII 211 IIIII 211 IIIIIII 211 IIIII 211 IIIII
5右上角的<増加> 信息管理 備 <u>自一覧</u> 1 余记录,当前显示第 13 <u>登登名集本</u> 受 16 192.18	图4 设备 •按钮,进入增加设 设备: 11余记录•第1/1页 <u>卷印 设多写述</u> 84.42 AR46	:信息管理主 信息管理主 新: ▶ 15 ▼ \$423 予用版具 予用版具	如下图: 如下图: [] () () () () () () () () () () () () ()	
第二百二年前の<増加、 信息管理 第 <u>第一章</u> 1条记录,当前显示单 13 <u>支資名条。</u> 受 6 192.16	图4 设备 •按钮,进入增加设 ^{设备4} 811条记录•第 1/1页 <u>金P 设备集选</u> 84.42 AR46	★ 10 ● 10 ○ 10 ○ 10 ○ 10 ○ 10 ○ 10 ○ 10 ○		
右上角的<増加> 高息管理 高島一覧 1条记录・当商显示第 13 登金名祭・ 型 6 19216 お加设备窗口中,	图4 设备 •按钮,进入增加设 @ 1 条记录• 第 1/1页 @ 1 条记录• 第 1/1页 @ 4.2 AR46 图5 月 正确输入设备IP地	acknows and marked in the field of the	· 如下图: · · · · · · · · · · · · · · · · · · ·	董建 端加 董建 端加 董建 董章 ● 10 0 0 董章 章章 章章 章章
 右上角的<増加> 「加> 「東山市 「東山市 「東山市 「東京大学・13 	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	accentence of the second	·····································	1000000000000000000000000000000000000
后右上角的<增加> 信息管理 篇 <u>8一笔</u> 1条记录,当前显示率 13 <u>登望名集⁶</u> 受 6 19216 前加设备窗口中, 口。 行P地址就是所要	图4 设备 •按钮,进入增加设 *** 8) 1 条记录• 第 1/1页 <u>201</u> 交互延送 84.2 AR46 图5 打 正确输入设备IP地 监控的设备的地址	a. A wind a find a general field a field	如下图: 如下图: 顺 ① ① #2 章 ① ①	 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章
5右上角的<增加> 信息管理 備息一覧 11条记录,当前显示美 13 <u>夜音名集</u> 2 16 192.16 前加设备窗口中, 行口。 备IP地址就是所要 音描述可以不填,	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	i信息管理主任 备信息窗口, 3称: ► 15 ● \$UB 15 ● \$UB YHEEL 曾加设备窗口 增加设备窗口 计HEEL 第 15 ● \$UB YHEEL 第 第 YHEEL 第 第 第 第 第 第 第 新;	· 如下图: · · · · · · · · · · · · · · · · · · ·	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	i信息管理主任 备信息窗口, 5条: ▶ 15 ● \$429 第15 ● \$429 详细信息 創加设备窗口 中加设备窗口 第 (15 ● \$429 第 (15 ● \$429 第 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429 (15 ● \$429	如下图: 如下图: (例 ① ① () (例 ② ① () () () () () () () () () () () () () (第 第 第 第 第 第 1 1
5右上角的<增加> 信息管理 偏血一覧 11条记录,当前显示差 13 <u>20全名象</u> 2 66 192.16 当加设备窗口中, 5日P地址就是所要 各描述可以不填, MP相关参数要和 15元设备参数后,	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	antward in a = 1 if 信息管理主情 备信息窗口, 3乘: 「 15 ● 承認 第第: 「 15 ● 承認 評価値 曾加设备窗口 增加设备窗口 時間 第二 第二 <td>窗口 如下图: (可 ① ① (可 ① ① (可 选) 备接口选择</td> <td> (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</td>	窗口 如下图: (可 ① ① (可 ① ① (可 选) 备接口选择	 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
5右上角的<增加> 信息管理 備息一覧 11条记录,当前显示差 13 <u>改善名集</u> 15 19216 前加设备窗口中, 行口。 针P地址就是所要 针描述可以不填, MP相关参数要和 15完设备参数后, 携收管理>>日志接收配	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	i信息管理主任 备信息窗口, 5称: ▶ 15 ● \$409 15 ● \$409 详细简单 详细简单 第四日, 设备描述 ; 称; 微一致。 钮, 进入设备	會中世。 如下图: () () () () () () () () () (2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
5右上角的<增加> 信息管理 備息一覧 1条记录,当前显示差 13 <u>支金名条</u> 20 16 19216 前加设备窗口中, 口。 备旧地址就是所要 各描述可以不填, MP相关参数要和 量完设备参数后, 接收管理>日志接收配置	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	i信息管理主任 备信息窗口, 5条: ▶ 15 ● \$127 38: ▶ 15 ● \$127 计编信息 10 ● \$128 计编信息 第加设备窗口 计编信息 第加设备窗口 计编信息 第加设备窗口 计编信息 第加设备窗口 计通信息 第加设备面面口 第二、设备描述 ; 称; 徵一致。 钮,进入设备	9 如下图: (() () () () () () () () ()	 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
古右上角的<増加> 信息管理 備息一覧 備息一覧 (1条记录,当前星示楽) 1 20全名家 20 46 192.16 当加设备窗口中, 5口。 61P地址就是所要 各描述可以不填, MP相关参数要和 電完设备参数后, 接收管理>日志接收管理 差な配置 生産器PP機址:	图4 设备 •按钮,进入增加设 *** *** *** *** *** *** *** *** *** *	i信息管理主管 i信息管理主管 i信息管理主管 i信息管理主管 i通道 i i	會口 如下图: () () () () () () () () () (① ①
5右上角的<增加> 信息管理 備息一覧 1 集记录,当前显示单 13 <u>或差名条</u> 或 16 192.16 第1D1边备窗口中, 门。 备1D1地址就是所要 备描述可以不填, MP相关参数要和 量完设备参数后, 排收管理>>目志排收配] 繁秋配置 处理器PP地址: FTP生用录:	图4 设备 •按钮,进入增加设 设备 1 象记录• 第 1/1页 <u>金印 设备写述</u> 84.2 AR46 图5 f 正确输入设备IP地 监控的设备的地址 缺省会取设备的名 设备上的snmp的参 单击<增加接口>按	antwind the approximation of the approximation	朝口 如下图: (御 ()) () () () () () () () () () () () () ()) ()) () () () ()) ()) ()) ()) ()) ())) ())) ())) ())) ())) ())) ()))) ()))))) ())))) ())))	 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
右上角的<増加> 信息管理 備島一覧 1 条记录・当前显示率 13 支査名条 2 登る名条 1 多に浸水・当前显示率 13 支査名条 1 多に浸水・当前显示率 13 支査名条 1 多に浸水・当前显示 13 支査名条 1 多に浸水・13 支査名条 1 92.16 1 92.	图4 设备 •按钮,进入增加设 ***** ***** ***** ***** ***** ******	antward in a part of the second	如下图:	 1 1
5右上角的<增加> 信息管理 備血一覧 (1条记录,当前显示素) <u>改全名条</u> 2 3 3 3 3 3 3 3 3 4 6 192.16 3 193.16 3 192.16 3 193.193.16 3 193.16 193.10	图4 设备 •按钮,进入增加设 读者 3) 1 条记录• 第 1/1页 <u>3) 1 条记录• 第 1/1页</u> <u>3) 1 条记录• 第 1/1</u> 页 <u>3) 1 条记录• 1 /1</u> <u>3) 1 条记录• 1 /1</u> <u>3) 1 条记录• 1 /1</u> <u>3) 1 条记录• 1 /1</u> <u>1 年</u> <u>4 年</u> <u>4 年</u> <u>4 年</u> <u>4 年</u> <u>5 月</u> <u>1 年</u> <u>4 年</u> <u>5 月</u> <u>1 年</u> <u>5 月</u> <u>1 年</u> <u>5 月</u> <u>5 月</u> <u></u>	i信息管理主旨 备信息窗口, 5本: □ 15 ● \$103 3本: □ 15 ● \$103 3本: □ ?##61 ?##65 曾加设备窗口 计量量量 常加设备窗口 ?##65 第四, 设备描述 ; 称; 微一致。 钮, 进入设备	9 如下图: (可强) (可选)	 ① ① ① ① ① ① ①
古右上角的<増加> 信息管理 備息一覧 第二日 新田 (1) 新田 (1	图4 设备 •按钮,进入增加设 读者 ¹¹ #记录• 第 1/1页 21 <u>23</u> <u>23</u> <u>23</u> (84.2 AR46 图5 引 正确输入设备IP地 监控的设备的地址 缺省会取设备的名 设备上的snmp的参 单击<增加接口>按	antwind the approximation of the approximation	朝口 如下图: (()) () () () () () () () () () () ())) ())) ())) ())) ())) ())) ())) ()))) ())))) ())))))) ()))))))))))))	 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
5右上角的<增加> 信息管理 備息一覧 1条记录,当前显示第13 <u>2毫名条</u> 2 2 16 192.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16 第12.16	图4 设备 •按钮,进入增加设 ** ** **	ife 管理主管 ife 管理主管 ife 會信息窗口, ife ●	望口 如下图: (()) () () () () () () () () () ()) ()) ()) () ())) ()) ())) ())) ())) ())) ()))) ()))) ()))) ()))) ()))) ()))) ())))) ())))))) ())))) ()))))))) ()))))))))))))	 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
	图4 设备 •按钮,进入增加设 读者: 30 1 象记录• 第 1/1页 <u>30 2 3 3 3 5 1</u> 2 4 4 6 1 1 3 1 3 1 3 1 3 1 3 1 3 1 3 1 3 1 3	11 11 11 11 12 4 11 13 4 115 15 4 115 15 4 115 15 4 12 4 12 14 15 4 15 16 4 15 17 4 15 16 4 16 17 4 17 16 4 17 10 10 18 1 10 10 19 10 10 10 10 10 10 10 11 10 10 10 12 10 10 10 13 10 10 10 14 10 10 10 15 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 1	如下图:	 新聞 新聞
 右上角的<増加> 高急管理 第急一覧 第急一覧 1条记录,当前显示差,13 3登金2条 3252条 3252% 3252%<td>图4 设备 •按钮,进入增加设 读者 ¹¹ #记录·兼 1/1页 21 <u>设备</u>是达 ¹¹ 建记录·兼 1/1页 21 <u>设备</u>是达 ¹¹ 正确输入设备IP地 监控的设备的地址 缺省会取设备的名 设备上的snmp的参 单击<增加接口>按 ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹</td><td>21 21 21 21</td><td>望口 如下图: (())) () ())) ())) ()))))))))))))</td><td> 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</td>	图4 设备 •按钮,进入增加设 读者 ¹¹ #记录·兼 1/1页 21 <u>设备</u> 是达 ¹¹ 建记录·兼 1/1页 21 <u>设备</u> 是达 ¹¹ 正确输入设备IP地 监控的设备的地址 缺省会取设备的名 设备上的snmp的参 单击<增加接口>按 ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹ ¹¹	21 21 21 21	望口 如下图: (())) () ())) ())) ()))))))))))))	 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

选择要进行监控的设备接口,本文中监控和局域网连接的GigabitEthernet0/0/0 以及和 Internet相连的Ethernet0/0/1。

选择接口后,点击<确定>,返回到增加设备窗口,再次单击<确定>按钮,完成增加设备操作,页面返回到设备信息管理页面,如下图:

自动获	R 手工配置		
选择	接口錯述	接口索引	最大速率
Г	Atm 5/0/0	16	0 bps
	Aux0	5	0 bps
	Cpos4/0/0	15	155,000,000 bps
	Encrypt8/0/0	17	0 bps
	Ethernet0/0/0	3	100,000,000 bps
	Ethernet0/0/1	4	10,000,000 bps
2	GigabitEthernet1/0/0	6	100,000,000 bps
	InLeopBack0	1	0 bps
Г	LoopBack0	29	0 bps
	NULLO	2	0 bps
	Pos2/0/0	12	0 bps
	Serial3/0/0	13	0 bps
	Serial3/0/1	14	0 bps

图7 设备信息管理 (增加设备后)

4 配置日志接收管理

点击导航菜单栏中[系统管理/日志接收管理]菜单项,进入日志接收管理页面。

下发		
处理器配置下发结果		
处理器印 192168430	下发详细信息	_
192.100.4.30	MUSELMU-10	
接收器配置下发结果		
接收器印	下发详细信息	
192.168.4.30	配置成功	
	後定	
	图8 日志接收管理	
トナトタ . 町 卑. 1かな		1.10
「白上用< 能直> 按钮	1(以从古 配直 链按),进行日芯按收配直。外	
An et Alsall		
10.8515.45		mission
	设备名称: " 查询 重查	均衡力口
信息一覧		
剩任何记录	15 💽 条记录/页 🚺 🚺 🚺 🚺	0
<u>设备名称</u> ▲ <u>改</u>	<u>谷印 设备描述</u> 详细信息 修改 图	RR .
	00000	0
吏用默认的9020,902 面返回到日志接收管	21, 单击<增加>, 然后单击右上角<下发>按钮, 下发日志接U 理。然后单击右上角<下发>按钮, 下发日志接U	【器IP,监则 3志接收配: 收配置,显
吏用默认的9020,902 面返回到日志接收管 言息时,表示下发配	21,单击<增加>,然后单击<牵定>按钮,完成 理。然后单击右上角<下发>按钮,下发日志接 置成功,日志接收配置完成。	【器IP, 监吗] 日志接收配: 收配置,显
吏用默认的9020,902 面返回到日志接收管 言息时,表示下发配 <mark>6息管理>>增加设备</mark>	21,单击<增加>,然后单击<确定>按钮,完成 理。然后单击右上角<下发>按钮,下发日志接向 置成功,日志接收配置完成。	【器IP,监则 日志接收配: 收配置,显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 +信息管理>>增加设备	21,单击<增加>,然后单击<确定>按钮,完成[理。然后单击右上角<下发>按钮,下发日志接 置成功,日志接收配置完成。	【器IP, 监则 日志接收配: 收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>>增加设备	21,单击<增加>,然后单击<确定>按钮,完成[理。然后单击右上角<下发>按钮,下发日志接 置成功,日志接收配置完成。	(器IP, 區) 日志接收配: 收配置, 显
走用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理≫增加设备 確备 * 设备P:	21,单击<增加>,然后单击<确定>按钮,完成 理。然后单击右上角<下发>按钮,下发日志接 置成功,日志接收配置完成。	(器IP, 區) 日志接收配: 上版配置, 显
走用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理≫増加设备 	21,单击<增加>,然后单击<确定>按钮,完成 理。然后单击右上角<下发>按钮,下发日志接 置成功,日志接收配置完成。	(器IP, 监) 日志接收配: 位配置,显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理≫増加设备	21, 单击<增加>, 然后单击<确定>按钮, 完成F 理。然后单击右上角<下发>按钮, 下发日志接 置成功, 日志接收配置完成。	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 可返回到日志接收管 信息时,表示下发配 信息管理≫増加设备 "役备 "役备P: 役备用法: * SNMP团件字: * SNMP团件字: * SNMP面件字:	1.1007 , 边中歌目的日志录日来唱。相对 (文代 21, 单击<增加>, 然后单击~确定>按钮, 完成日 理。然后单击右上角<下发>按钮, 下发日志接问 置成功, 日志接收配置完成。 192.168.4.2	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>>增加设备 "设备P: 设备展述: "SNMP团件字: "SNMP团件字: "SNMP面件字: "SNMP面件字:	1.1007 , 边中政目的日志录台来唱。书约 (300 21,单击<增加>,然后单击<条件。	(器IP, 监) 日志接收配置, 显
 使用默认的9020,902 面返回到日志接收管 高息时,表示下发配 信息管理>增加设备 信息管理>增加设备 "改善P: · 改善P: · 改善即: · SNMP团件字: · SNMP团件字: · SNMP工: 使口信息 第口名 	192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2 192.168.4.2	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>增加设备 。 で登録: ・ で登録: ・ SNMP団件字: ・ SNMP団件字: ・ SNMP端口: 接口信息 推口名案 其口目	1.00.7.00) 7.201年444目10日10-384日9年44日。4100100 21, 单击<增加>,然后单击<402.7523	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>增加设备 で後番単: で後番単: ・SNMP団件字: ・SNMP団件字: ・SNMP端口: 接口信息 接口名案 其口目	102-1603(1), 位于404目10日/2038(1), 年間, 103(1) 21, 单击<增加>, 然后单击<确定>按钮, 完成F 1理。然后单击右上角<下发>按钮, 下发日志接收 2回成功, 日志接收配置完成。 192:168.4.2 public 161 161 翻譯 最大速率 推加讓口	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>>增加设备 で设备理>>增加设备 で设备理≥: 。SNMP团件字: 。SNMP团件字: 。SNMP面件字: 。SNMP面件字: 。SNMP面中字: 者口信息 者口信和 者口名案 者口目	102-1603(1), 位于本政目的日本總計, 百大市 21, 单击<增加>, 然后单击<确定>按钮, 完成目 1理。然后单击右上角<下发>按钮, 下发日志接收 2回成功, 日志接收配置完成。 192:168.4.2 public 161 182 並減 最大速率 撤定 美回	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 面返回到日志接收管 信息时,表示下发配 信息管理>>增加设备 。 でである 。 でである 。 ででは まいが用意に まい の の の の の の の の の の の の の の の の の の	21, 单击<增加>,然后单击<确定>按钮,完成E 1理。然后单击右上角<下发>按钮,下发日志接收 1置成功,日志接收配置完成。 192.168.4.2 public 161 鐵定 差回	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 可返回到日志接收管 信息時,表示下发配 信息管理≫増加设备 で後番述: ・SNMP団件字: ・SNMP団件字: ・SNMP端□: 使可信息 変口名案 変正 変正 変正 変正 変正 変正 変正 変正 変正 変正	21, 单击<增加>, 然后单击<确定>按钮, 完成日 理。然后单击右上角<下发>按钮, 下发日志接い 置成功, 日志接收配置完成。 192.168.4.2 public 192.168.4.2 public 161 161 161 161 161 161 161 10	(器IP, 监) 日志接收配置, 显
使用默认的9020,902 罰返回到日志接收管 急助时,表示下发配 信息管理>>增加设备 。 でである 。 でである 。 SNMP団件字: 。 SNMP団件字: 。 SNMP調口: 度口信息 度口信息 度口信息	102-1603	
使用默认的9020,902 词返回到日志接收管 信息时,表示下发配 信息管理>增加设备 "设备序: 设备题述: SNMP团件字: SNMP面件字: SNMP端口: 按口信息 度口信息 度口信息	10.1.100) , 201年44日10日10-38日7年4日。 450 (300) 21, 単击<増加>, 然后単击右上角<下发>按钮, 完成日 理。然后単击右上角<下发>按钮, 下发日志接い 置成功, 日志接收配置完成。 192.168.4.2 192.168.4 192.168.	
使用默认的9020,902 面返回到日志接收管 急助,表示下发配 信息管理>增加设备 。 设备账: 。SNMP团件字: 。SNMP面件字: 。SNMP端口: 使口信息 重口信息 面包志接收配 音信息和日志接收配	10.1.00) , 201年44日10日10-38日7年4日。487 (304) 21, 単击<増加>, 然后単击右上角<下发>按钮, 完成日 理。然后単击右上角<下发>按钮, 下发日志接い 2度成功, 日志接收配置完成。 192.168.4.2 192.168.4	
使用默认的9020,902 面返回到日志接收管 急助时,表示下发配 信息管理>>增加设备 。设备P: 设备局线: SNMP团件字: SNMP面件字: SNMP面件字: SNMP面件字: SNMP面件字: 者目信息和日志接收配 音伝表,如下图所示	21, 单击<增加>, 然后单击<确定>按钮, 完成日 理。然后单击右上角<下发>按钮, 下发日志接 置成功, 日志接收配置完成。 192.168.4.2 public 161 161 161 101 161 101 161 101	
使用默认的9020,902 面返回到日志接收管 言息时,表示下发配 「信息管理>>增加设备 ■设备 ■设备 ■ 设备IP: - 设备IP: - 没备IP: - 没备IP: 	102-168-42 192-168-42	
使用默认的9020,902 面返回到日志接收管 言息时,表示下发配 。 意識 。 改善即 。 或 。 或 。 或 。 。 或 》 》 。 。 SNMP団件手: 。 SNMP団件手: 。 SNMP団件手: 。 SNMP団件手: 。 SNMP団件手: 。 SNMP団件手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体手: 。 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP団体子: 》 SNMP SNMP団体子: 》 SNMP SNMP SNMP SNMP SNMP SNMP SNMP SNMP	21,单击<增加>,然后单击<确定>按钮,完成日 1理。然后单击右上角<下发>按钮,下发日志接收 1置成功,日志接收配置完成。 1192.168.4.2 public 161 酸症 差回 图10<日志接收配置下发成功	

6.1	根据2.1的组网需求,	配置各接口IP地址和及路由

6 配置路由器AR46

图11 网络流量分析

6.2 配置设备时间 clock datetime 08:00:00 2006/11/03 在用户视图下,配置正确的标准时间,不要配置时区。目前XLog和设备配套时存在时 区问题,具体请参见2.3故障排除举例。 6.3 配置SNMP # snmp-agent snmp-agent community read public snmp-agent sys-info version all 进入系统视图,配置SNMP相关命令。在设备信息管理,增加设备时,SNMP参数要 和设备上配置的一致,否则无法获取到设备的接口列表。 6.4 配置NetStream日志导出 # ip netstream export source interface Ethernet0/0/0 //设备IP ip netstream export host 192.168.4.30 9020 //接收器IP 端口 进入系统视图, 配置上述NetStream日志导出命令。其中source interface的IP地址要 和XLog中设备IP一致,日志导出host 和监听端口要和XLog的接收器IP和监听端口一 致。 6.5 使能NetStream统计 # interface GigabitEthernet1/0/0 ip address 192.168.2.2 255.255.255.0 ip netstream inbound ip netstream outbound 进入接口视图,在该接口下使能NetStream日志统计功能。 6.6 查看NetStream日志导出信息 display ip netstream export Version 5 export information Stream destination IP(UDP) : 192.168.4.30(9020) Stream source interface : Ethernet0/0/0 Exported stream number : 83577 Exported UDP datagram number(failed number): 71281(0) 在用户视图或系统视图都可以使用该命令查看NetStream日志导出的情况。 四 配置关键点: 4.1 接收器和处理器在同一台服务器上时,不需要配置FTP相关参数。XLog支持接收 器和处理器的分布式安装,如果二者不再同一台服务器上时,需要在处理器所在的服 务器上开启FTP服务,同时在日志接收管理配置相应的FTP配置信息。 接收器的监听端口,缺省为9020和9021,用户可以进行修改,但是要保证和设备上配 置的日志导出端口一致。 4.2 设备IP地址就是所要监控的设备的地址,对于路由器 (如AR46)可能存在多个IP ,XLog中配置的设备IP要和设备上 配置的NetStream 日志导出的Source 接口IP相同 ,即和设备上配置的下面命令中的接口IP相同,本文中使用以太网接口Ethernet 0/0/0 , IP为192.168.4.2。

[AR46]ip netstream export source interface Ethernet 0/0/0

XLog中的设备IP要和Eth0/0/0的IP一致。