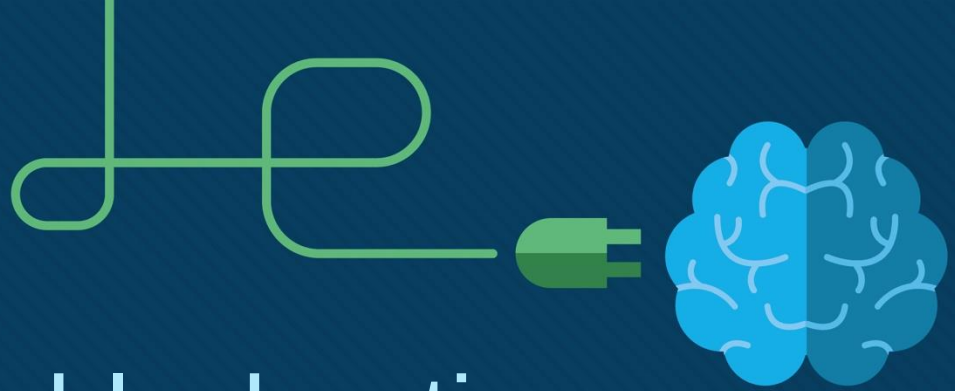


28 Network Troubleshooting

28.1 Network Documentation
网络文档

文档概述

网络管理员要想能够监控网络并排除故障，他们必须拥有一整套准确且最新的网络文档。此类文档包括：

- 配置文件，包括网络配置文件和终端系统配置文件
- 物理和逻辑拓扑图
- 基线性能级别

所有网络文档信息都应保存到一个位置，可保存为硬拷贝形式，或保存到受保护服务器的网络上。备份文档应当在不同位置进行维护和保存。

网络文档

网络拓扑图

物理网络拓扑显示连接到网络的设备的物理布局。

逻辑网络拓扑说明设备如何与网络进行逻辑连接，即设备在与其他设备通信时如何通过网络实际传输数据。

Physical Topology

- 设备类型
- 型号和制造商
- 操作系统版本
- 电缆类型及标识符
- 电缆规格
- 接头类型
- 电缆连接端点

Logical Topology

- 设备标识符
- IP 地址和前缀长度
- 接口标识符
- 连接类型
- 虚电路的帧中继 DLCI（如果适用）
- 站点到站点 VPN
- 路由协议
- 静态路由
- 数据链路协议
- 所采用的 WAN 技术

网络设备文档

- 网络设备文档应包含网络硬件和软件的准确、最新记录。
- 文档应包括有关网络设备的所有相关信息。

Router Device Documentation

Device	Model	Description	Location	IOS	License
Central	ISR 4321	Central Edge Router	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9

Interface	Description	IPv4 Address	IPv6 Address	MAC Address	Routing
G0/0/0	Connects to SVR-1	10.0.0.1/30	2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3

Switch Device Documentation

Device	Model	Description	Mgt. IP Address	IOS	VTP
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 switch	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M	Domain: CCNA Mode: Server

Port	Description	Access	VLAN	Trunk	EtherChannel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1	-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2	-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***	Yes	999	-	-		Shut
Fa0/4	*** Not in use ***	Yes	999	-	-		Shut
Fa0/5	Access port to user	Yes	10	-	-		Yes

End-System Documentation

Device	OS	Services	MAC Address	IPv4 / IPv6 Addresses	Default Gateway	DNS
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

建立网络基线

监控网络的目的是观察网络性能，将其与预先确定的基线进行比较。基线用于确定正常的网络或系统性能。要建立网络性能基线，需要从对于网络运行不可或缺的端口和设备上收集性能数据。

- 网络管理员可以通过度量关键网络设备和链路的初始性能及可用性，在网络扩展时或流量模式变化时辨别网络的异常运行情况和正常运行情况。
- 基线还会提供关于当前网络设计能否满足企业需求的信息。如果没有基线，在度量网络流量最佳状况特征以及拥塞程度时便没有了依据。
- 初始基线建立后进行的分析往往也能揭示一些隐藏的问题。收集的数据会显示网络中拥塞或潜在拥塞的真实情况。还可能会显示网络中利用率不足的区域，而且往往会促使设计人员根据质量和容量观察结果重新设计网络。

建立网络基线

如需建立和捕获初始网络基线，请执行以下步骤：

- **第 1 步：确定要收集的数据类型。**
- **第 2 步：确定关键设备和端口。**
- **第 3 步：确定基线期限。**

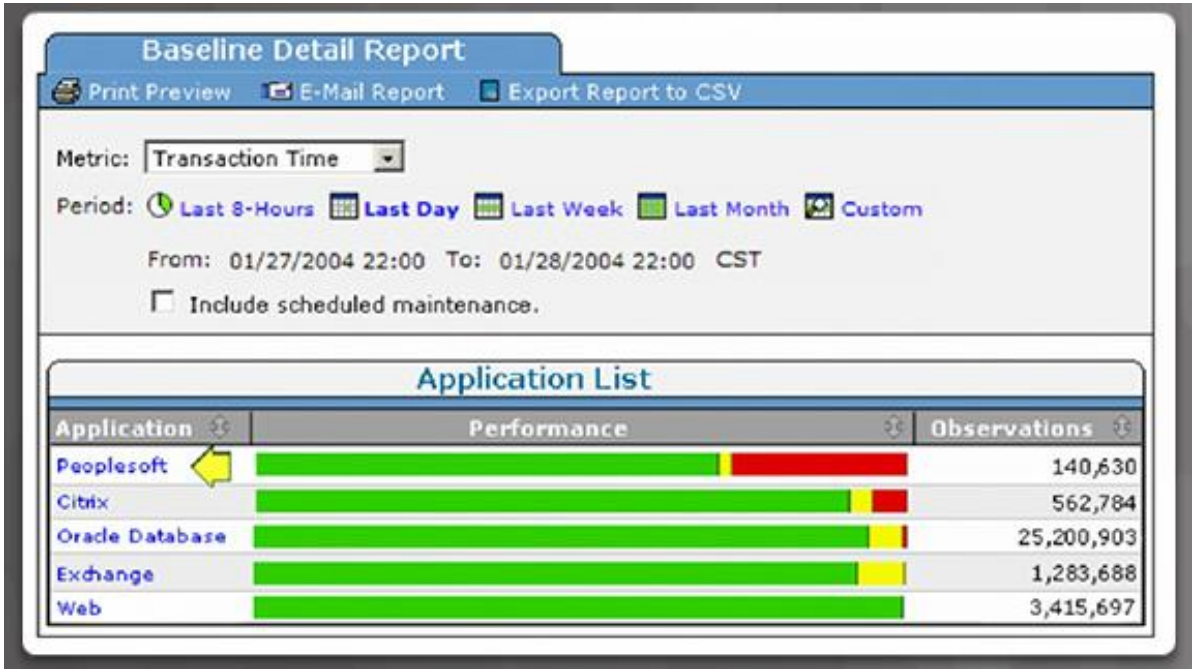
网络文档

测量数据

命令	描述
show version	显示设备软件和硬件的运行时间、版本信息。
show ip interface[brief] show ipv6 interface[brief]	显示接口上设置的所有配置选项。使用 brief关键字可以只显示 IP 接口的开启/关闭状态及每个接口的 IP 地址。
show interfaces [interface_type interface_num]	显示每个接口的详细输出。要仅显示单个接口的详细输出，请在命令中添加接口类型和编号（例如，gigabitethernet 0/0）。
show ip route show ipv6 route	显示路由表的内容。
show arp show ipv6 neighbors	显示 ARP 表 (IPv4) 和邻居表 (IPv6) 的内容。
show running-config	显示当前配置。
show port	显示交换机上的端口状态。
show vlan	显示交换机上 VLAN 的状态。
show tech-support	此命令可以帮助收集大量设备信息，以便进行故障排除。它可以执行多个 show 命令，在报告问题时可将这些命令提供给技术支持代表。
show ip cache flow	显示 NetFlow 记账统计数据汇总。

网络文档

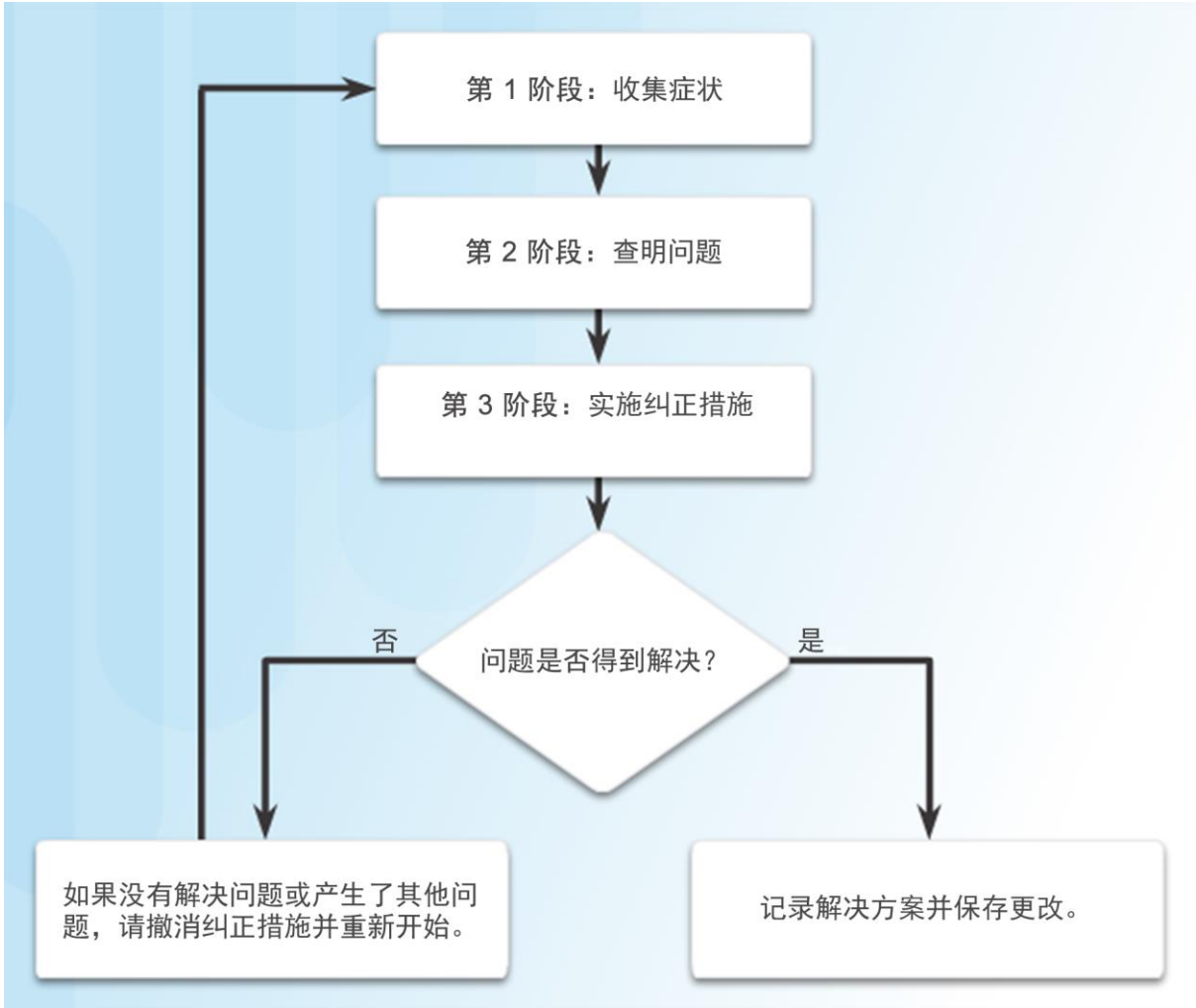
测量数据


Baseline Detail Report
Print Preview
E-Mail Report
Export Report to CSV
Metric: Transaction Time
Period: Last 8-Hours Last Day Last Week Last Month Custom
From: 01/27/2004 22:00 To: 01/28/2004 22:00 CST
Include scheduled maintenance.
Application List
Application
Performance
Observations
Peoplesoft 140,630
Citrix 562,784
Oracle Database 25,200,903
Exchange 1,283,688
Web 3,415,697

28.2 Troubleshooting Process
故障排除流程

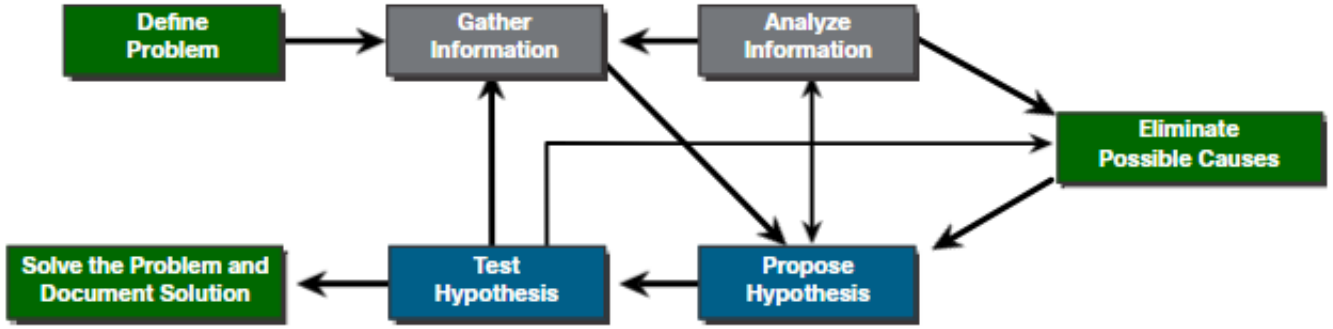
总体故障排除流程

- 由于网络不同，问题不同，故障排除经验也不同，因此故障排除可能很耗时.
- 使用结构化的故障排除方法将缩短整个故障排除时间。



故障排除流程

故障排除7步法



Steps	Description
定义问题	• 确认存在问题，然后正确定义问题
收集信息	• 识别、访问和收集信息的目标（即主机、设备）.
分析信息	• 使用网络文档、网络基线、知识库等确定可能的原因。
评估可能的原因	• 逐步排除可能的原因，最终确定最可能的原因。
提出假设	• 确定最可能的原因后，必须制定解决方案。
测试假设	• 评估问题的紧迫程度，创建回滚计划，实施解决方案，并验证结果。
解决问题	• 解决后，通知所有相关人员，并记录原因和解决方案，以帮助解决未来的问题。

询问终端用户

- 很多情况下问题是由终端用户报告的。信息经常会是模糊的或具有误导性的，例如，“网络中断”或“我无法访问我的邮件”。在这些情况下，必须更清楚地明确问题。这可能需要向终端用户提问。
- 当向终端用户询问他们可能遇到的网络问题时，请使用有效的提问技巧。这将帮助您获得记录问题症状所需的信息。

指南	终端用户问题示例
询问与故障有关的问题。	哪一部分无法正常运行？
将每个问题用作解决或发现潜在问题的方法。	正常运行的部分与无法正常运行的部分是否有关联？
以用户能够理解的技术深度与用户交谈。	无法正常运行的部分之前是否能够正常运行？
询问用户最初注意到问题是什么时候。	最初注意到问题是什么时候？
确定自从设备上次正常运行以来是否发生过什么事情。	上次正常运行之后进行了哪些更改？
如有可能，要求用户重现问题。	您能否重现问题？
确定问题发生之前事件发生的顺序。	问题具体发生在什么时候？

收集信息

命令	描述
`ping {host|ip-address}`	向某个地址发送 echo 请求数据包，然后等待响应。*host* 或*ip-address* 变量是目标系统的 IP 别名或 IP 地址。
`traceroute {destination}`	确定数据包通过网络采用的路径。*destination* 变量是目标系统的主机名或 IP 地址。
`telnet {host|ip-address}`	使用 Telnet 应用连接到某个 IP 地址。
`ssh -l userid ip-address`	使用 SSH 连接到某个 IP 地址。
`show ip interface brief` `show ipv6 interface brief`	显示设备上所有接口状态的汇总。
`show ip route` `show ipv6 route`	显示当前的 IPv4 和 IPv6 路由表，这些路由表包含通往所有已知网络目的地的路由。
`show running-config`	显示当前运行的配置文件的内容。
`[no] debug ?`	显示启用或禁用调试事件的选项列表。
`show protocols`	显示已配置的协议，并显示所有已配置的第 3 层协议的全局状态和接口特定状态。

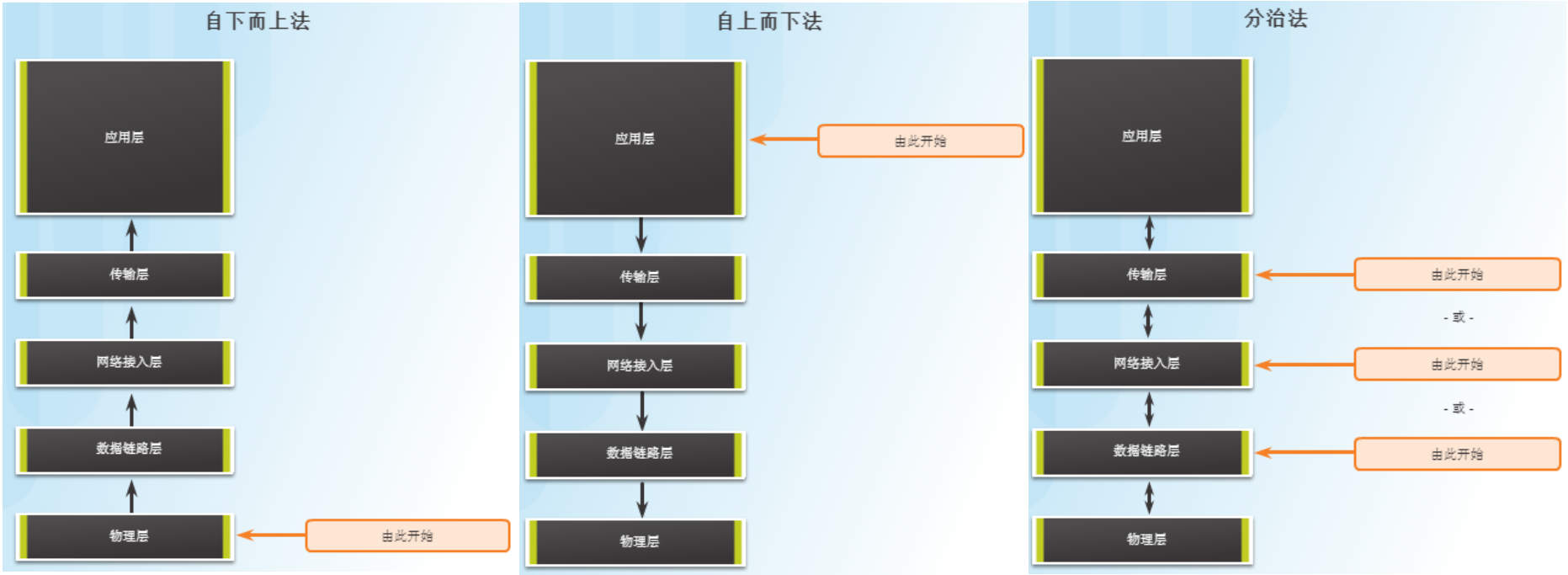
使用分层故障排除模型


7 应用层
6 表示层
5 会话层
4 传输层
3 网络接入层
2 数据链路层
1 物理层
终端系统
路由器
多层交换机
标准
交换机
集线器

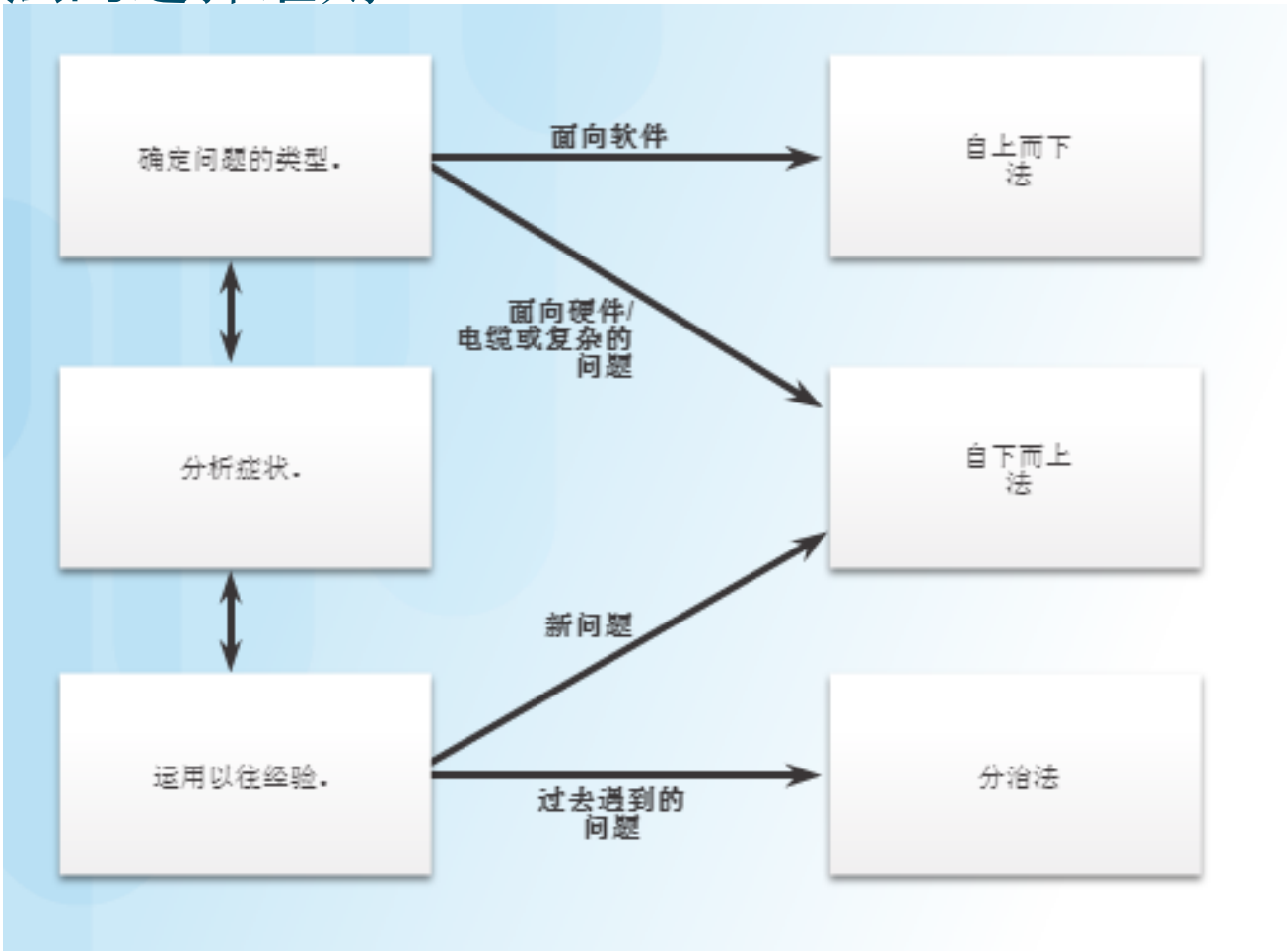

OSI 模型
TCP/IP 模型
7 应用层
6 表示层
5 会话层
4 传输层
3 网络接入层
2 数据链路层
1 物理层
应用层
TCP
传输层
IP
Internet 层
网络接入层

故障排除流程

结构化故障排除方法



故障排除法的选择准则


确定问题的类型。
面向软件
自上而下法
面向硬件/电缆或复杂的问题
分析症状。
自下而上法
新问题
运用以往经验。
过去遇到的问题
分治法

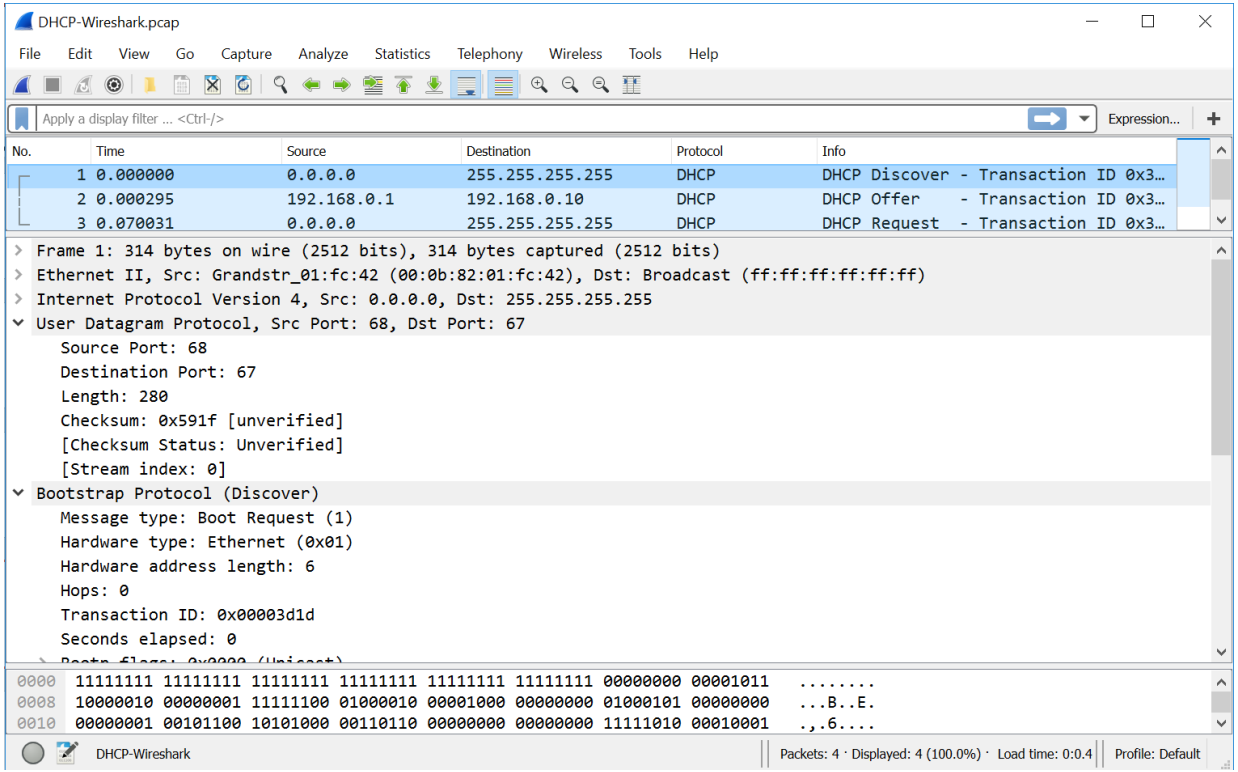
28.3 Troubleshooting Tools
故障排除工具

故障排除工具
软件工具

Software Tool	Description
Network Management System Tools	• 网络管理系统 (NMS) 工具包括设备级的监控、配置及故障管理工具。 • 网络监控软件以图形方式显示网络设备的物理视图，网络管理员可以利用该视图自动连续监控远程设备。 • 设备管理软件提供关键网络设备的动态设备状态、统计信息及配置信息。
Knowledge Bases	• 在线网络设备供应商知识库已成为不可或缺的信息来源。 • 当基于供应商的知识库与互联网搜索引擎相结合时，网络管理员可以访问大量基于经验的信息。
Baselining Tools	• 可以使用许多工具（ SolarWinds）来使网络数据记录及基线建立过程自动化。 • 基线建立工具可帮助您完成一般记录任务。

故障排除工具
协议分析器

- **协议分析器**有助于调查通过网络的数据包内容。



硬件工具

- **数字万用表**是测试仪器，用于直接测量电压、电流和电阻的电气值。
- **电缆测试仪**是专用的手持设备，用于测试各种类型的数据通信电缆。这些设备沿电缆发送信号，并等待信号反射，从发送信号至收到反射信号的时间会转换为距离测量值。
- **电缆分析仪**是多功能的手持设备，用于测试和验证适用于不同服务和标准的铜缆和光缆。
- **便携式网络分析仪器**可插在网络中的任何地方，用于排除故障。
- **网络分析模块**可以捕获并解码数据包，以及跟踪响应时间，以向特定网络或服务器指出应用故障的具体位置。

使用系统日志服务器进行故障排除

实施日志记录设施是网络安全的重要部分，并可用于排除网络故障。思科设备可对有关配置更改、ACL 违规、接口状态和许多其他类型事件的信息进行日志记录。思科设备可将日志消息发送给多个不同设施。

- 日志消息可以发送到控制台、VTY、内存缓冲区或syslog服务器。
- Cisco IOS日志消息分为八个级别。
- 级别数越低，严重性级别越高。
- 默认情况下，控制台显示级别6（调试）消息。
- 在命令输出中，0级（紧急情况）到5级（通知）将发送到位于209.165.200.225的syslog服务器

```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
R1(config)#
```

	级别	关键字	描述	定义
最高级别	0	emergencies	系统不可用	LOG_EMERG
	1	alerts	需要立即采取措施	LOG_ALERT
	2	critical	存在高危情况	LOG_CRIT
	3	errors	存在错误情况	LOG_ERR
	4	warnings	存在警告情况	LOG_WARNING
	5	notifications	正常但比较重要的情况	LOG_NOTICE
	6	informational	仅信息性消息	LOG_INFO
最低级别	7	debugging	调试消息	LOG_DEBUG

28.4 Symptoms and Causes of Network Problems

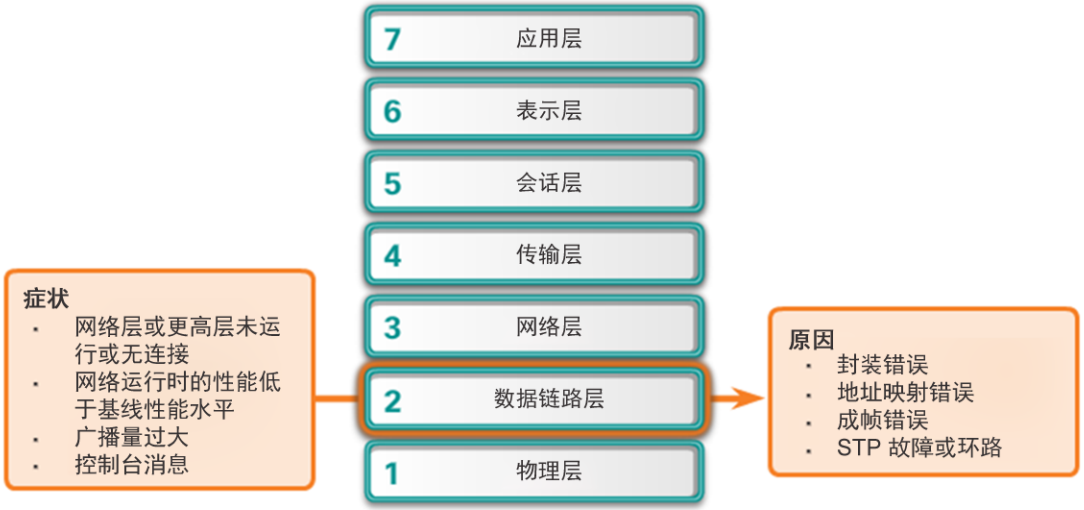
网络故障的症状和原因

网络故障排除的症状和原因

物理层故障排除

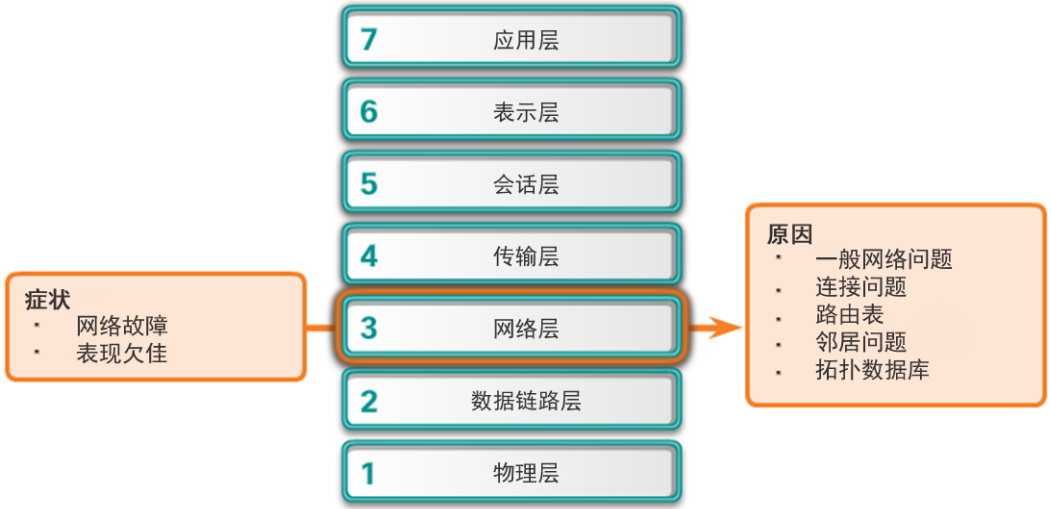
网络故障排除的症状和原因

数据链路层故障排除



网络故障排除的症状和原因

网络层故障排除

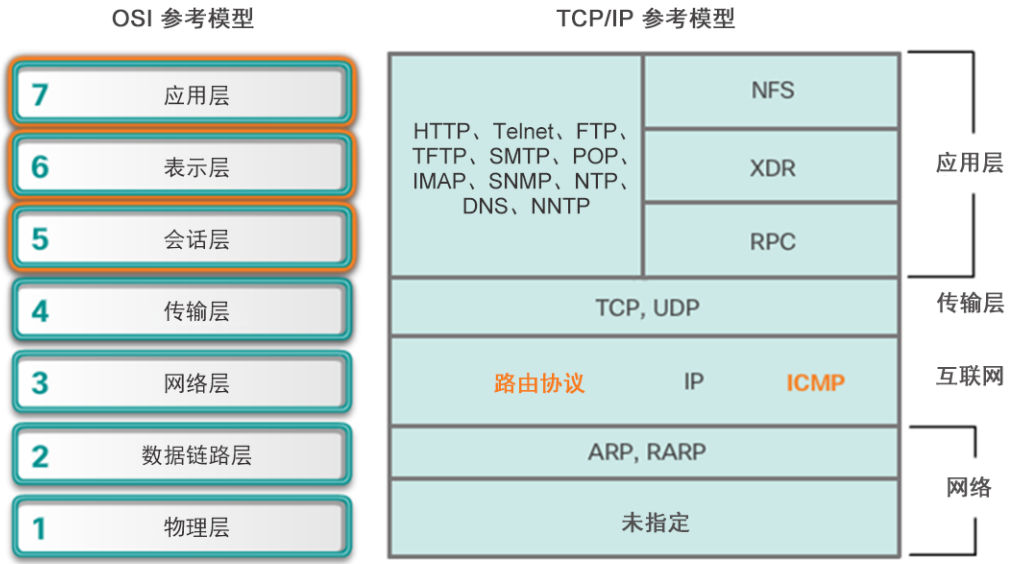


网络故障排除的症状和原因

传输层故障排除

网络故障排除的症状和原因

应用层故障排除

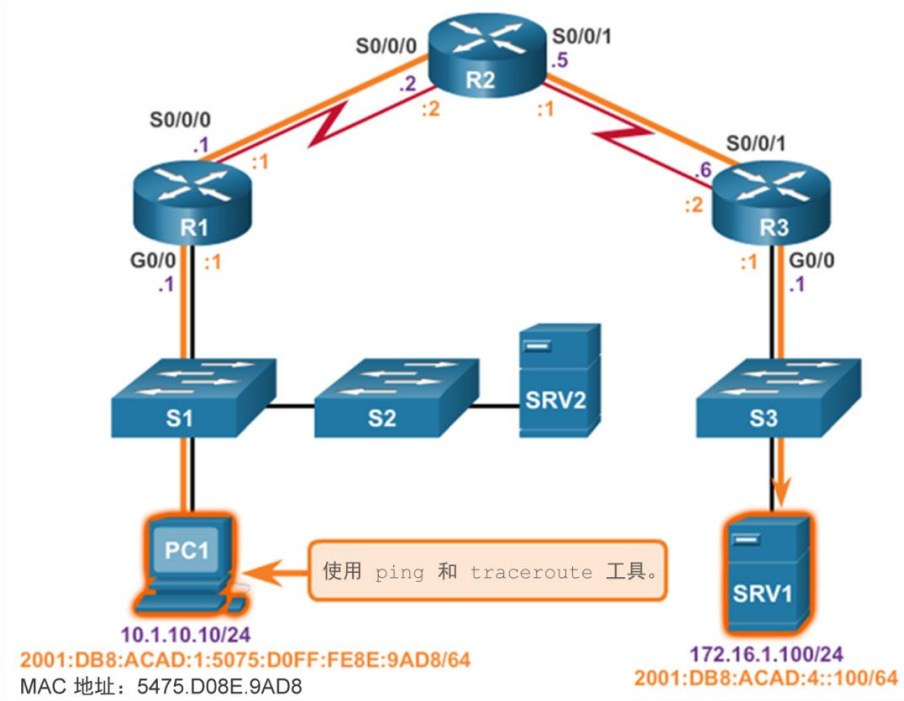


28.5 Troubleshooting IP Connectivity
IP 连接故障排除

端到端连接问题引发故障排除

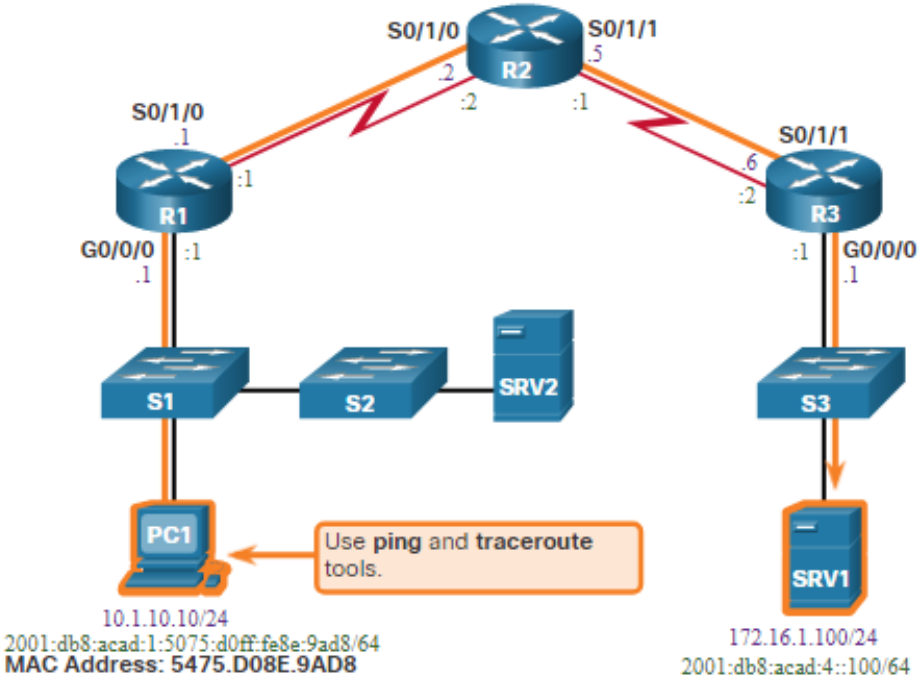
适用于端到端连接的常见自下而上故障排除步骤：

- **第 1 步：**检查物理连接
- **第 2 步：**检查双工不匹配情况。
- **第 3 步：**检查数据链路层和网络层地址。
- **第 4 步：**验证默认网关是否正确。
- **第 5 步：**确保设备正在确定从源到目的地的正确路径。
- **第 6 步：**确认传输层正常运行。
- **第 7 步：**确认没有 ACL 阻止流量。
- **第 8 步：**确保 DNS 设置正确。



End-to-End Connectivity Problem Initiates Troubleshooting

- 通常引发故障排除工作的原因是发现存在端到端连接问题。
- 用于核实端到端连接问题的两种最常见的实用工具是 `ping` 和 `traceroute`。
- 当 ping 命令失败时，通常会执行 traceroute 命令。如果 ping 成功，通常无需再执行 traceroute 命令，因为技术人员已经确信连接存在。



IP 连接故障排除

Step 1 -检验物理层

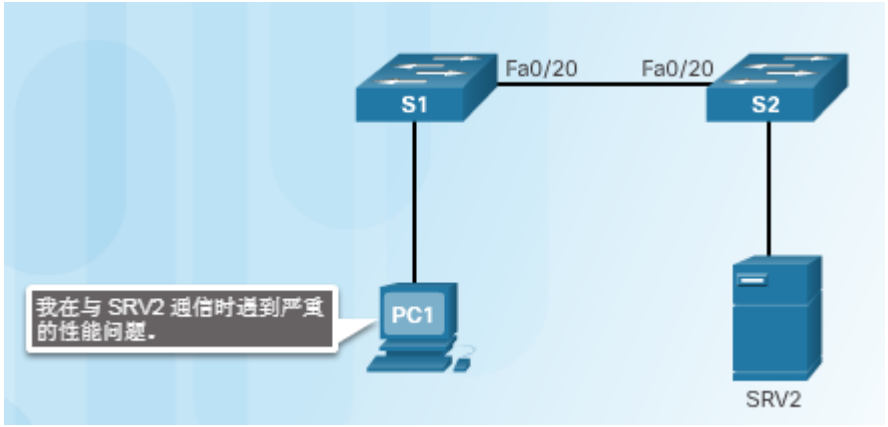
- 最常用的IOS命令是 show processes cpu、show memory 和 show interfaces.
- 在排除与性能相关的问题且怀疑硬件是故障所在时，可使用 show interfaces 命令检验流量通过的接口。
- show interfaces命令的输出列出了许多可以检查的重要统计信息：

```
R1# show interfaces GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0(bia d48c.b5ce.a0c0)
Internet address is 10.1.10.1/24
(Output omitted)
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
 Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
85 packets input, 7711 bytes, 0 no buffer
Received 25 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 5 multicast, 0 pause input
10112 packets output, 922864 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
11 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R1#
```

- 接口状态：UP UP
- 输入队列丢包：输入队列丢包在某一点上传输到路由器的流量超出了路由器的处理能力。这并不一定表明存在问题。
- 输出队列丢包:输出队列丢包表示数据包因接口出现拥塞而被丢弃。在总输入流量高于输出流量的任何点上，看到输出丢包是正常的。
- 输入错误:输入错误表明在接收帧的过程中出现错误，例如 CRC 错误。
- 输出错误:输出错误表示帧传输过程中出现的错误，比如冲突。

Step 2 -检查双工不匹配

- 接口错误的另一个常见原因就是以太网链路两端之间的双工模式不匹配。
- IEEE 802.3ab 千兆以太网标准推荐
- 如果自动协商失败，请在互联端手动设置速度和双工。
- 点对点以太网链路应当始终在全双工模式下运行。使用速度和双工的自动协商。




```
S1# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Full-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S1#
```

```
S2# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96d2.4001 (bia 0cd9.96d2.4001)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Half-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S2(config)# interface fa 0/20
S2(config-if)# duplex auto
S2(config-if)#
```

Step 3 -检验本地网络上的第 2 层和第 3 层地址

在IPv4中，此功能由ARP提供。

在IPv6中，ARP 功能由邻居发现协议和ICMPv6取代。邻居表缓存了 IPv6 地址及其解析的以太网物理 (MAC) 地址。

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  10.1.10.1             d4-8c-b5-ce-a0-c0     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

```
PC1> netsh interface ipv6 show neighbor
Interface 13: LAB
Internet Address                Physical Address   Type
------------------------------  -----------------  -------
fe80::9c5a:e957:a865:bde9       00-0c-29-36-fd-f7  Stale
fe80::1                         d4-8c-b5-ce-a0-c0  Reachable (Router)
ff02::2                         33-33-00-00-00-02  Permanent
ff02::16                        33-33-00-00-00-16  Permanent
ff02::1:2                       33-33-00-01-00-02  Permanent
ff02::1:3                       33-33-00-01-00-03  Permanent
ff02::1:ff05:f9fb               33-33-ff-05-f9-fb  Permanent
ff02::1:ffce:a0c0               33-33-ff-ce-a0-c0  Permanent
ff02::1:ff65:bde9               33-33-ff-65-bd-e9  Permanent
ff02::1:ff67:bae4               33-33-ff-67-ba-e4  Permanent
```

检查VLAN故障

在排除端到端连接故障时需要考虑的另一个问题是VLAN分配。

For example, the MAC address on Fa0/1 should be in VLAN 10 instead of VLAN 1.

```
S1# show mac address-table
              Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type     Ports
All       0100.0ccc.cccc      STATIC   CPU
All       0100.0ccc.cccd      STATIC   CPU
 1        d48c.b5ce.a0c0      DYNAMIC  Fa0/1
10        000f.34f9.9201      DYNAMIC  Fa0/5
10        5475.d08e.9ad8      DYNAMIC  Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

The following configuration changes Fa0/1 to VLAN 10 and verifies the change.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1#
S1# show mac address-table
              Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type     Ports
All       0100.0ccc.cccc      STATIC   CPU
All       0100.0ccc.cccd      STATIC   CPU
10        d48c.b5ce.a0c0      DYNAMIC  Fa0/1
10        000f.34f9.9201      DYNAMIC  Fa0/5
10        5475.d08e.9ad8      DYNAMIC  Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

Step 4 -检验默认网关

如果路由器上没有详细路由，或者主机配置了错误的默认网关，那么不同网络中两个终端之间的通信将无法进行。

```
R1# show ip route
<省略部分输出>
Gateway of last resort is 192.168.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.2
```

```
C:\Windows\system32> route print
<省略部分输出>
Network Destination  Netmask    Gateway     Interface    Metric
          0.0.0.0    0.0.0.0    10.1.10.2   10.1.10.100      11
```

排除 IPv6 Default Gateway 举例

可手动配置或使用无状态自动配置（SLAAC）或 DHCPv6 配置默认网关。

For example, a PC is unable to acquire its IPv6 configuration using SLAAC. The command output is missing the all IPv6-router multicast group (FF02::2).

```
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
      FF02:: 1
      FF02::1:FF00:1

(Output omit
R1#
```

```
PC1> ipconfig
Windows IP Configuration
 Connection-specific DNS Suffix :
 IPv6 Address. . . . . . . . . . : 2001:db8:acad:1:5075:d0ff:fe8e:9ad8
 Link-local IPv6 Address . . . . : fe80::5075:d0ff:fe8e:9ad8%13
 IPv4 Address. . . . . . . . . . : 10.1.1.100
 Subnet Mask . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . : fe80::1
                                   10.1.10.1
```

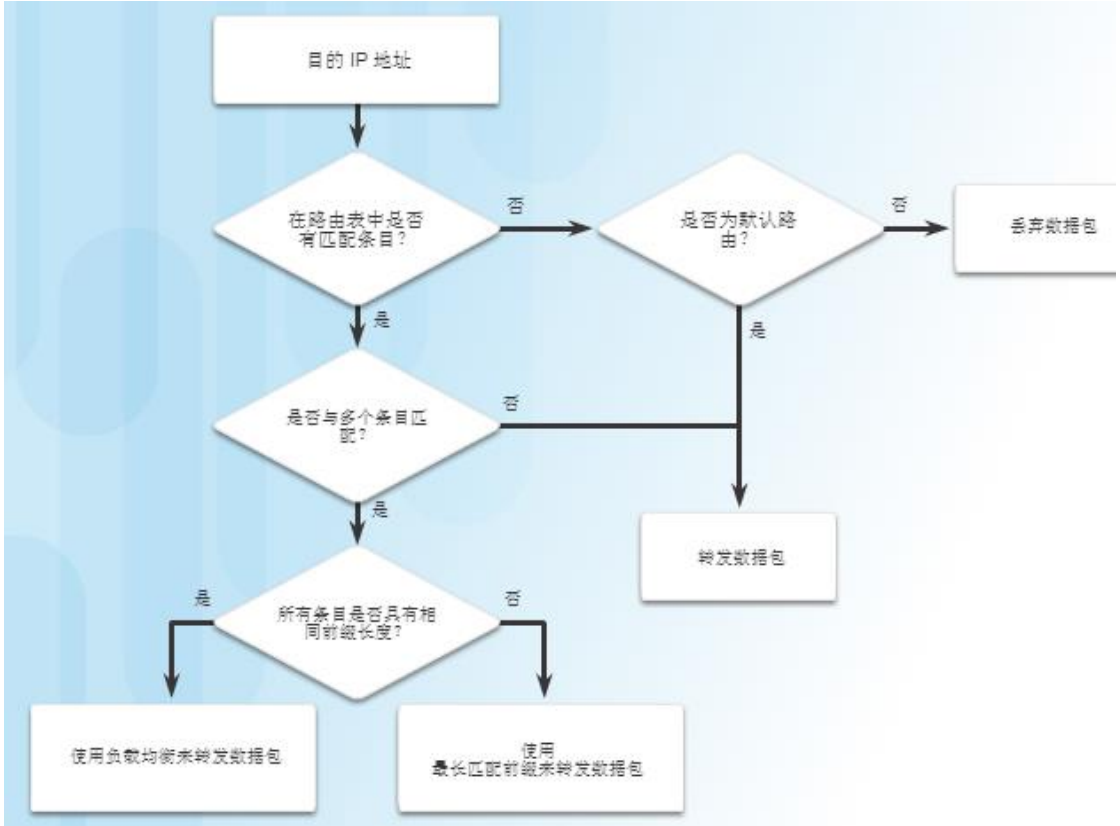
R1 is enabled as an IPv6 router and now the output verifies that R1 is a member of ff02::2, the All-IPv6-Routers multicast group.

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
      FF02:: 1
      FF02:: 2
      FF02::1:FF00:1
```

Step 5 -验证路径是否正确

排除故障时，通常需要检验通向目的地网络的路径。

- IPv4和IPv6路由表可通过以下方法进行填充：直连网络，本地主机或本地路由，静态路由，动态路由，默认路由。
- 转发IPv4和IPv6数据包的过程基于最长位匹配或最长前缀匹配。



Step 6 -检验传输层

影响传输层连接的两个最常见的问题包括ACL配置和NAT配置。 用于测试传输层功能的常见工具是Telnet实用程序。

虽然Telnet服务器应用在自己的公认端口号 23 上运行且Telnet客户端默认连接到此端口，但可以在客户端上指定另一个端口号，以连接到任何必须接受测试的TCP端口。

```
PC1> telnet 2001:DB8:172:16::100
HQ#
```

```
R1# telnet 2001:db8:acad:2::2 80
Trying 2001:DB8:ACAD:2::2, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Mon, 04 Nov 2019 12:34:23 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

```
R1# telnet 2001:db8:acad:3::2
Trying 2001:DB8:ACAD:3::2 ... Open

User Access Verification

Password:
R3>
```

```
R1# telnet 2001:db8:acad:3::2 80
Trying 2001:DB8:ACAD:3::2, 80 ...
% Connection refused by remote host

R1#
```

Step 7 -检验 ACL

在路由器上，可能配置了ACL，禁止协议通过入站或出站方向上的接口。

In this example, ACL 100 has been incorrectly configured inbound on the G0/0/0 instead of inbound on S0/1/1.

```
R3# show ip interface serial 0/1/1 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
R3#
R3# show ip interface gig 0/0/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is 100
R3#
```

The ACL is removed from G0/0/0 and configured inbound on S0/1/1.

```
R3(config)# interface GigabitEthernet 0/0/0
R3(config-if)# no ip access-group 100 in
R3(config-if)# exit
R3(config)#
R3(config)# interface serial 0/1/1
R3(config-if)# ip access-group 100 in
R3(config-if)# end
R3#
```

Step 8 -检验 DNS

DNS 协议用于控制DNS，这是一个可将主机名映射到IP地址的分布式数据库。在设备上配置 DNS 时，对于所有IP命令（如ping 或telnet），您可以用主机名替代IP地址。

- 使用 ip host 命令将名称到IPv4的映射输入到交换机或路由器中。ipv6 host命令可供使用IPv6的相同映射使用。

- 要在基于Windows 的PC上显示名称到IP地址的映射信息，请使用nslookup命令。

```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
R1#

R1# ping ipv4-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R1#
```

```
PC1> nslookup Server
*** Request to 10.1.1.1 timed-out
```


CISCO