



МОДУЛЬ 12. ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК В СЕТИ

КАФЕДРА
ТЕЛЕКОММУНИКАЦИЙ

12.1 СЕТЕВАЯ ДОКУМЕНТАЦИЯ

12.1.1 ОБЗОР СЕТЕВОЙ ДОКУМЕНТАЦИИ

Для эффективного мониторинга и устранения неполадок сетей требуется точная и полная сетевая документация.

Общая сетевая документация включает следующее:

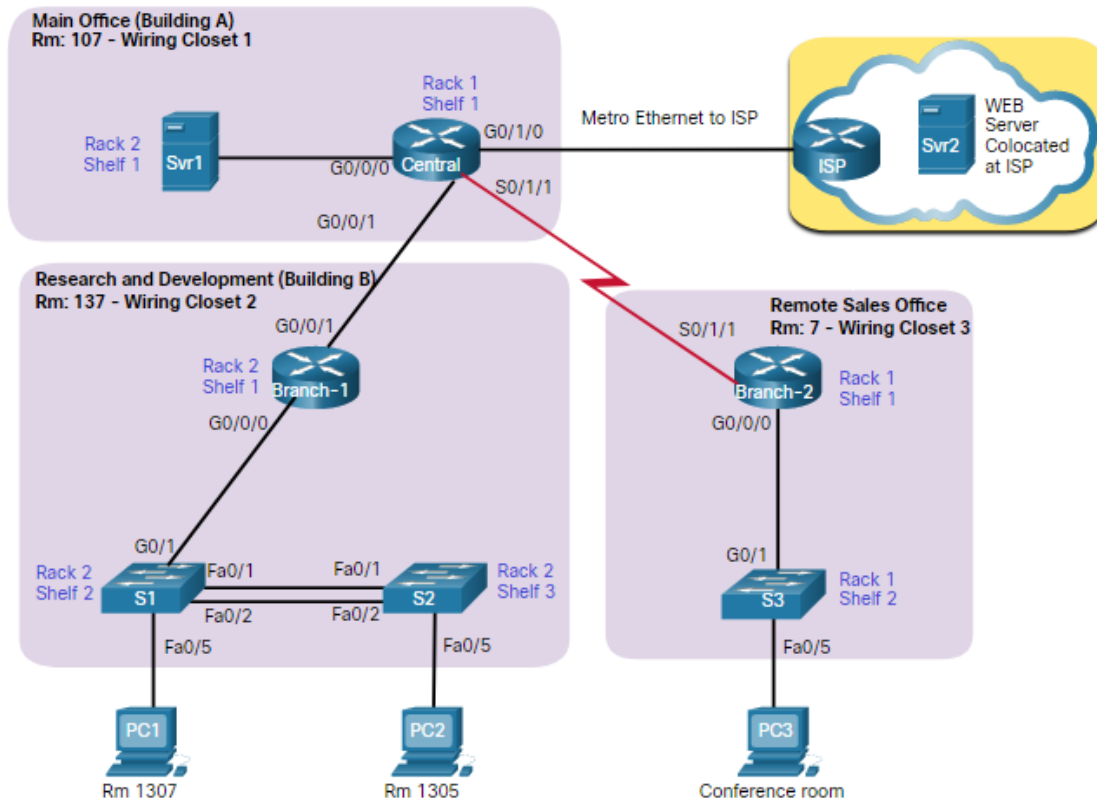
- Схемы физической и логической топологии сети.
- Документация по сетевому устройству, в которой записана вся необходимая информация об устройстве.
- Документация по базовым показателям производительности сети.

Вся сетевая документация должна храниться в одном месте, а резервная документация должна храниться в отдельном месте.

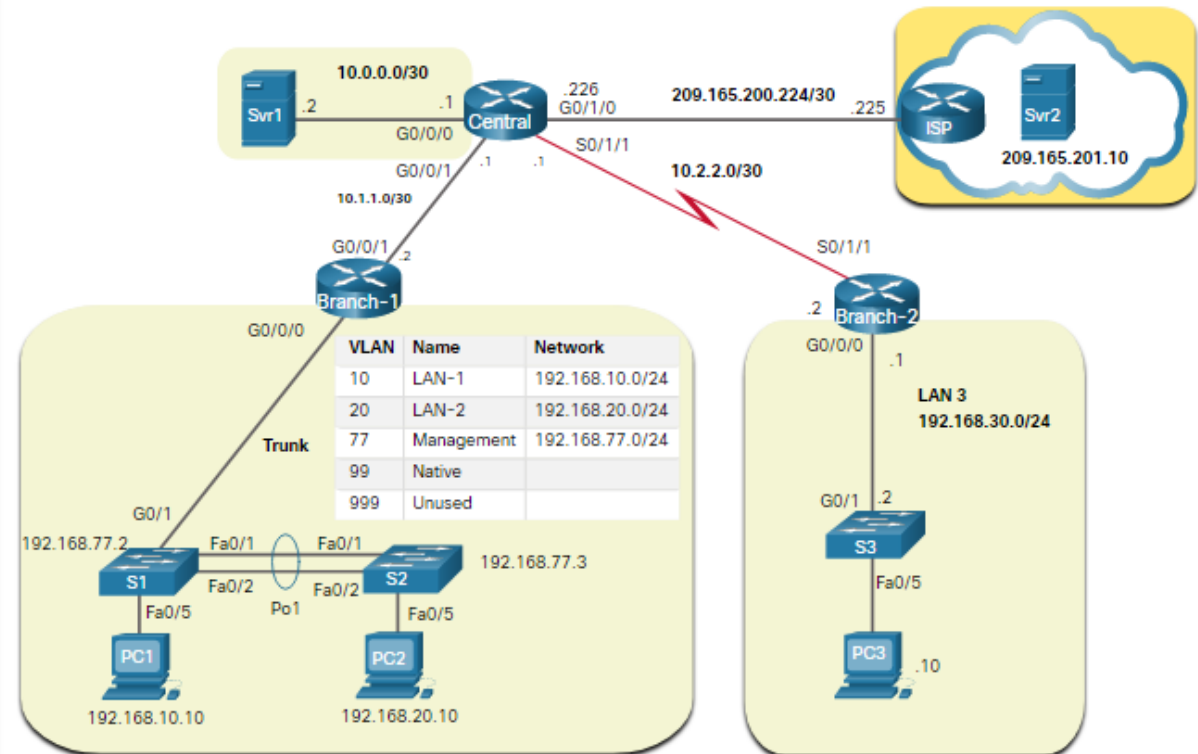
12.1.2 ДИАГРАММЫ СЕТЕВОЙ ТОПОЛОГИИ

Существует два типа топологических диаграмм: физическая и логическая.

Физическая топология



Логическая топология



12.1.3 ДОКУМЕНТАЦИЯ ПО СЕТЕВЫМ УСТРОЙСТВАМ

В файлах настройки сети содержатся точные, актуальные записи об оборудовании и программном обеспечении, применяемом в сети.

Документация должна содержать всю необходимую информацию о сетевых устройствах.

Маршрутизатор Документация

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		Routing
G0/0/0	Connects to SVR-1		10.0.0.1/30	2001:db8:acad:1::1/64		OSPF
G0/0/1	Connects to Branch-1		10.1.1.1/30	2001:db8:acad:a001::1/64		OSPFv3
G0/1/0	Connects to ISP		209.165.200.226/30	2001:db8:feed:1::2/64		Default
S0/1/1	Connects to Branch-2		10.1.1.2/24	2001:db8:acad:2::1/64		OSPFv3

Коммутатор Документация

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

Конечные устройства Документация

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

12.1.4 ОПРЕДЕЛЕНИЕ БАЗОВЫХ ПОКАЗАТЕЛЕЙ СЕТИ

Базовый уровень производительности сети используется для установления нормальной производительности сети для определения «портрета» сети в нормальных условиях. Для формирования базового уровня производительности сети требуется сбор данных о производительности, поступающих из портов и устройств, необходимых для обеспечения работы сети.

Базовыми данными являются те, которые:

- позволяют понять, может ли текущая схема сети удовлетворять требованиям бизнеса;
- могут выявлять области перегрузки или области в сети, которые недостаточно загружены.

12.1.4 ОПРЕДЕЛЕНИЕ БАЗОВЫХ ПОКАЗАТЕЛЕЙ СЕТИ

Шаг 1. Определите типы данных, которые необходимо собирать.

При определении начальных базовых показателей начните с выбора нескольких переменных, которые представляют определенные политики.

В случае выбора слишком большого количества точек данных объем собираемой информации может оказаться крайне большим, что очень усложнит процесс анализа собранных данных.

Начните с самого простого и постепенно вносите изменения по ходу работы.

На начальном этапе рекомендуется начать с определения коэффициента использования интерфейсов и ЦП.

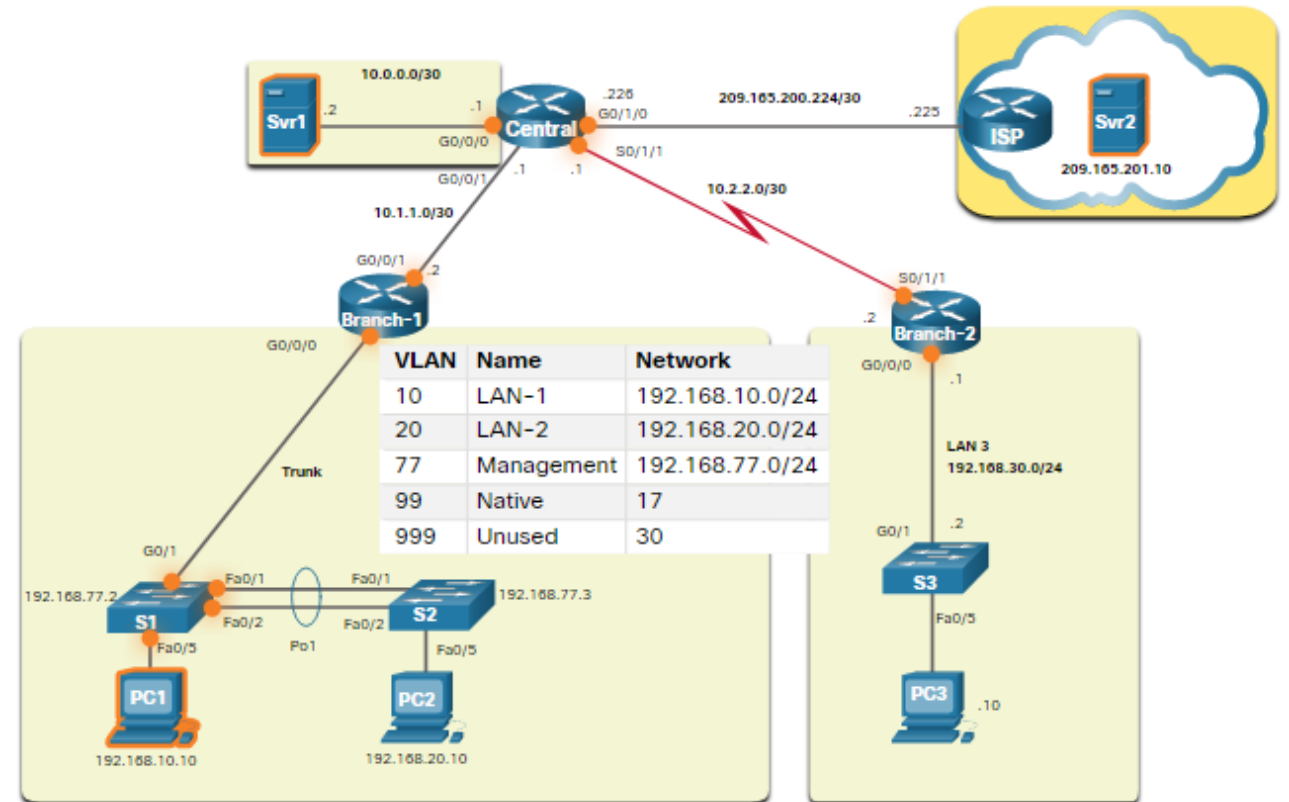
12.1.4 ОПРЕДЕЛЕНИЕ БАЗОВЫХ ПОКАЗАТЕЛЕЙ СЕТИ

Шаг 2. Определите требуемые устройства и порты.

Логическая диаграмма топологии сети может быть полезна при определении основных устройств и портов, подлежащих наблюдению.

Как показано в примере топологии, устройства и порты, представляющие интерес, включают:

- PC1 (терминал администратора)
- Два сервера (т.е. Srv1 и Svr2)
- Интерфейсы маршрутизатора
- Ключевые порты на коммутаторах



12.1.4 ОПРЕДЕЛЕНИЕ БАЗОВЫХ ПОКАЗАТЕЛЕЙ СЕТИ

Шаг 3. Определите длительность сбора базовых показателей.

При захвате данных для анализа указанный период должен быть:

- Как минимум, семь дней.
- Должен продолжаться не более 6 недель (если не потребуется определение специальных долгосрочных тенденций).
- Как правило, для определения базовых показателей достаточным будет период длительностью от 2-х до 4-х недель.

Выполняйте ежегодный анализ всей сети или базовых показателей отдельных ее частей поочередно.

Анализ необходимо выполнять регулярно, чтобы узнать, какое влияние на сеть оказывают ее рост, а также другие изменения.

12.1.5 ИЗМЕРЕНИЕ ДАННЫХ

На рисунке указаны некоторые наиболее часто используемые команды ОС IOS Cisco, применяемые для сбора данных.

Команда	Описание
show version	Позволяет отобразить время безотказной работы, информацию о версиях для оборудования и программного обеспечения устройства
show ip interface [brief] show ipv6 interface [brief]	Позволяет отобразить все параметры настройки, установленные на интерфейсе.
show interfaces	Позволяет отобразить подробные выходные данные для каждого интерфейса.
show ip route [static eigrp ospf bgp] show ipv6 route [static eigrp ospf bgp]	Отображает содержимое таблицы маршрутизации со списком напрямую подключенных сетей и удаленных сетей.
show cdp neighbors detail	Отображает подробные сведения о напрямую подключенных соседних устройствах Cisco.
show arp show ipv6 neighbors	Позволяет отобразить содержимое таблицы ARP (IPv4) и таблицы соседних устройств (IPv6).
show running-config	Отображает текущую конфигурацию.
show vlan	Отображает состояние сетей VLAN в коммутаторе.
show port	Отображает состояние портов на коммутаторе.
show tech-support	Используется для сбора большого объема информации с помощью нескольких команд show для создания отчетов технической поддержки.

12.2 ПРОЦЕДУРА ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

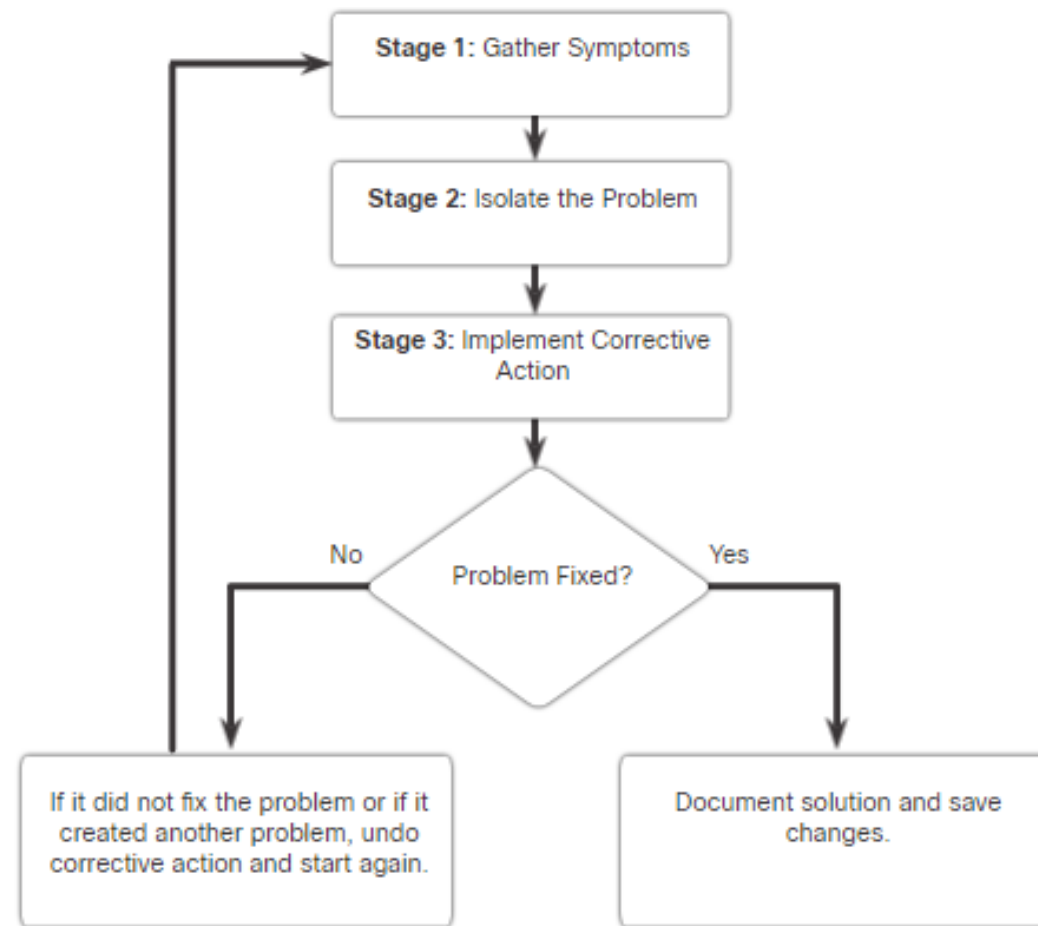
12.2.1 ОБЩИЕ ПРОЦЕДУРЫ ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

Устранение неполадок может занять много времени, поскольку сети отличаются друг от друга, проблемы различаются и опыт устранения неполадок различается.

Использование структурированного метода устранения неполадок сократит общее время устранения неполадок.

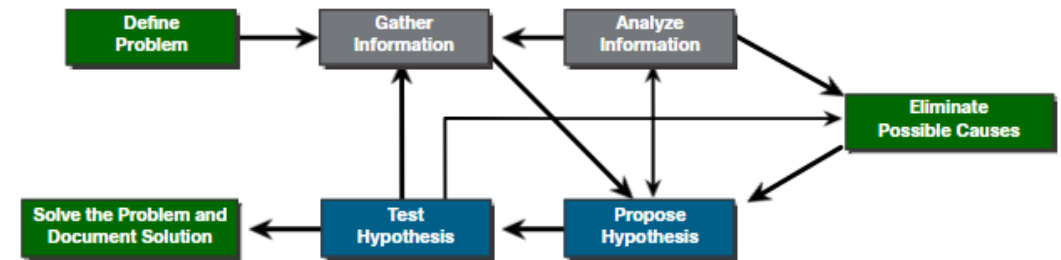
Существует несколько процессов устранения неполадок, которые можно использовать для решения проблемы.

На рисунке показана логическая схема упрощенного трехэтапного процесса устранения неполадок.



12.2.2 ЭТАПЫ ПРОЦЕДУРЫ ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

На рисунке показан более подробный семиэтапный процесс устранения неполадок.



Этапы	Описание
Определить проблему	Убедиться, что есть проблема, а затем правильно определить, что за проблема.
Сбор информации	Целевые объекты (например, хосты, устройства) идентифицируются, обеспечивается доступ к ним и проводится сбор информации.
Анализ информации	Определение возможных причин с помощью сетевой документации, базовой модели сети, баз знаний.
Устранение возможных причин	Постепенно устранять возможные причины, чтобы в конечном итоге определить наиболее вероятную причину.
Предложить гипотезу	Когда выявлена наиболее вероятная причина, необходимо сформулировать решение.
Проверка гипотезы	Оцените срочность проблемы, создайте план отката, внедрите решение и проверьте результат.
Решение проблемы	После решения, сообщите всем участвующим и задокументируйте причину и решение, чтобы помочь решить будущие проблемы.

12.2.3 ОПРОС КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

В таблице на рисунке приведены несколько рекомендаций, а также примеры вопросов для конечных пользователей.

Рекомендации	Примеры вопросов конечному пользователю
Задайте соответствующие вопросы.	Что не работает? В чем именно проблема? Чего ты пытаешься добиться?
Определите масштаб проблемы.	На кого влияет эта проблема? Это только вы или другие? Какое устройство имеет проблемы?
Определите, когда возникла проблема.	Когда именно возникает проблема? Когда впервые была обнаружена проблема? Были ли выведены сообщения об ошибках?
Определите, является ли проблема постоянной.	Можете ли вы воспроизвести проблему? Можете ли вы отправить мне скриншот или видео проблемы?
Определите, менялось ли что-то.	Что изменилось с тех пор, когда все еще нормально работало?
Используйте каждый вопрос в качестве средства исключения или обнаружения возможных проблем.	Что работает? Что не работает?

12.2.4 СБОР ИНФОРМАЦИИ

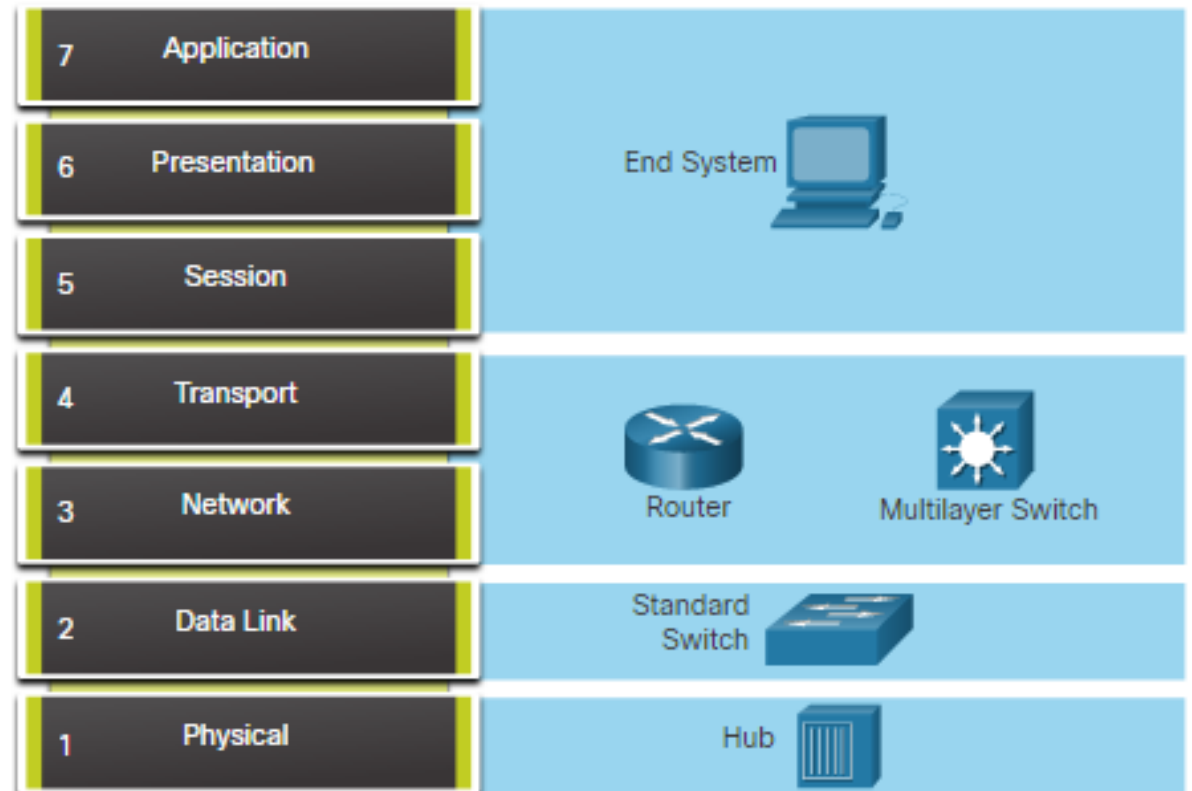
Стандартные команды Cisco IOS для сбора данных о сетевых проблемах.

Команда	Описание
ping { <i>host</i> <i>ip-address</i> }	Позволяет послать пакет ping-запроса по адресу и ожидать ответ.
traceroute <i>destination</i>	Позволяет определить путь передачи пакета по сетям.
telnet { <i>host</i> <i>ip-address</i> }	Позволяет подключиться к IP-адресу с помощью приложения Telnet (Примечание: по возможности используйте SSH).
ssh -l <i>user-id ip-address</i>	Подключение к IP-адресу по протоколу SSH.
show ip interface brief show ipv6 interface brief	Отображает сводный статус всех интерфейсов на устройстве
show ip route show ipv6 route	Отображает текущие таблицы маршрутизации IPv4 и IPv6.
show protocols	Отображает глобальное состояние и состояние любого настроенного протокола уровня 3.
debug	Отображение списка параметров для включения или отключения событий отладки.

12.2.5 УСТРАНЕНИЕ НЕПОЛАДОК С ИСПОЛЬЗОВАНИЕМ МНОГОУРОВНЕВОЙ МОДЕЛИ

Такие многоуровневые модели можно применять к физической сети для изоляции сетевых проблем при поиске и устранении неполадок.

На рисунке показаны некоторые общие устройства и уровни модели OSI, которые необходимо анализировать в процессе поиска и устранения неполадок для данного устройства.



12.2.6 СТРУКТУРИРОВАННЫЕ МЕТОДЫ УСТРАНЕНИЯ НЕПОЛАДОК

Различные подходы к устранению неполадок, которые могут быть использованы:

Подход к поиску и устранению неполадок	Описание
Снизу вверх	Этот метод хорошо подходит в тех случаях, когда предполагается, что проблема находится на физическом уровне.
Сверху вниз	Этот метод можно использовать для устранения простых проблем или когда предполагается, что проблема связана с некоторым элементом программного обеспечения.
Принцип «разделяй и властвуй»	Начните со среднего слоя (т.е. уровня 3) и сделайте проверку в обоих направлениях от этого слоя.
Последовательный путь (Follow-the-Path)	Используется для обнаружения фактического пути трафика от источника к месту назначения для уменьшения масштабов устранения неполадок.
Замена	Вы физически заменяете подозрительное проблемное устройство на проверенное, работающее.
Сравнение	Попытка решить проблему путем сравнения неработающего элемента с рабочим.
Образованное предположение	Успех этого метода зависит от опыта и возможностей устранения неполадок.

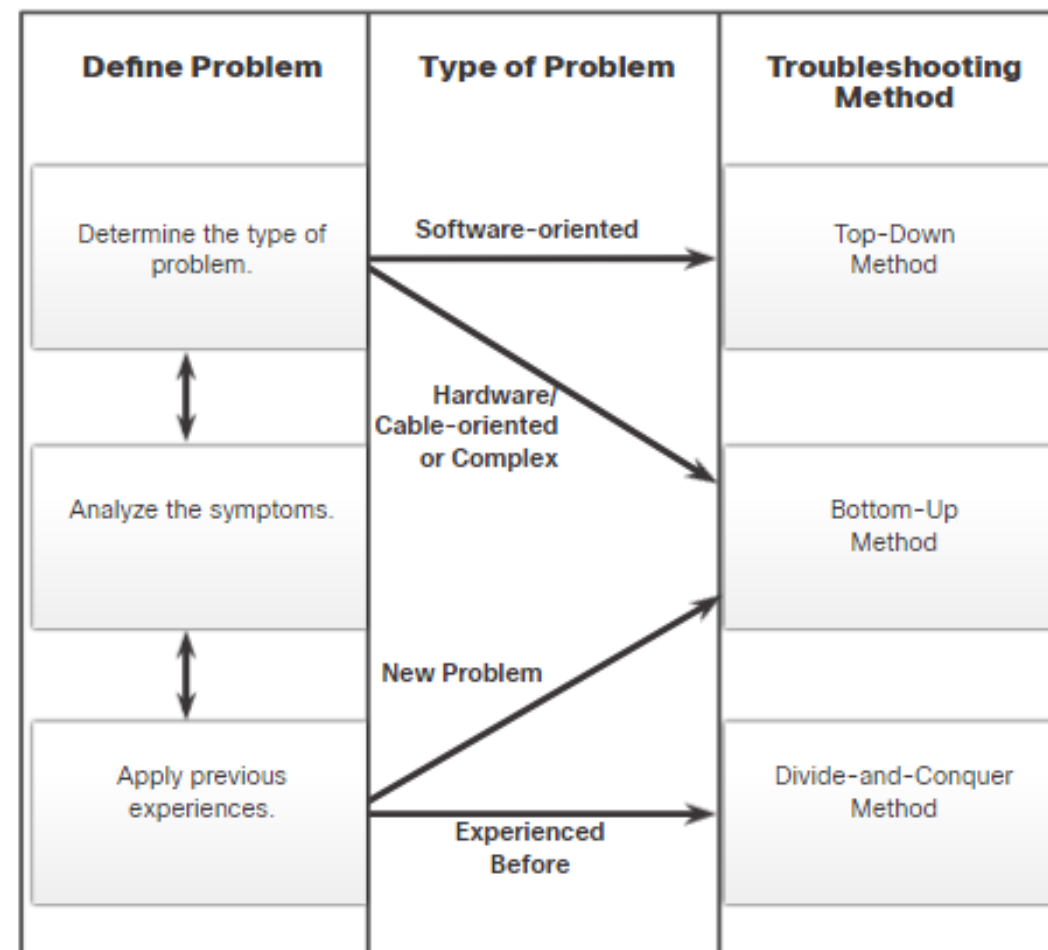
12.2.7 РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕТОДА ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

Для быстрого устранения сетевых проблем найдите время, чтобы выбрать наиболее эффективный метод отладки сети.

На рисунке показано, какой метод может быть использован при обнаружении определенного типа проблемы.

Устранение неполадок - это навык, который развивается в результате этого.

Каждая сетевая проблема, которую вы идентифицируете и решаете, добавляется в ваш набор навыков.



12.2.8 ПРОГРАММНЫЕ СРЕДСТВА ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

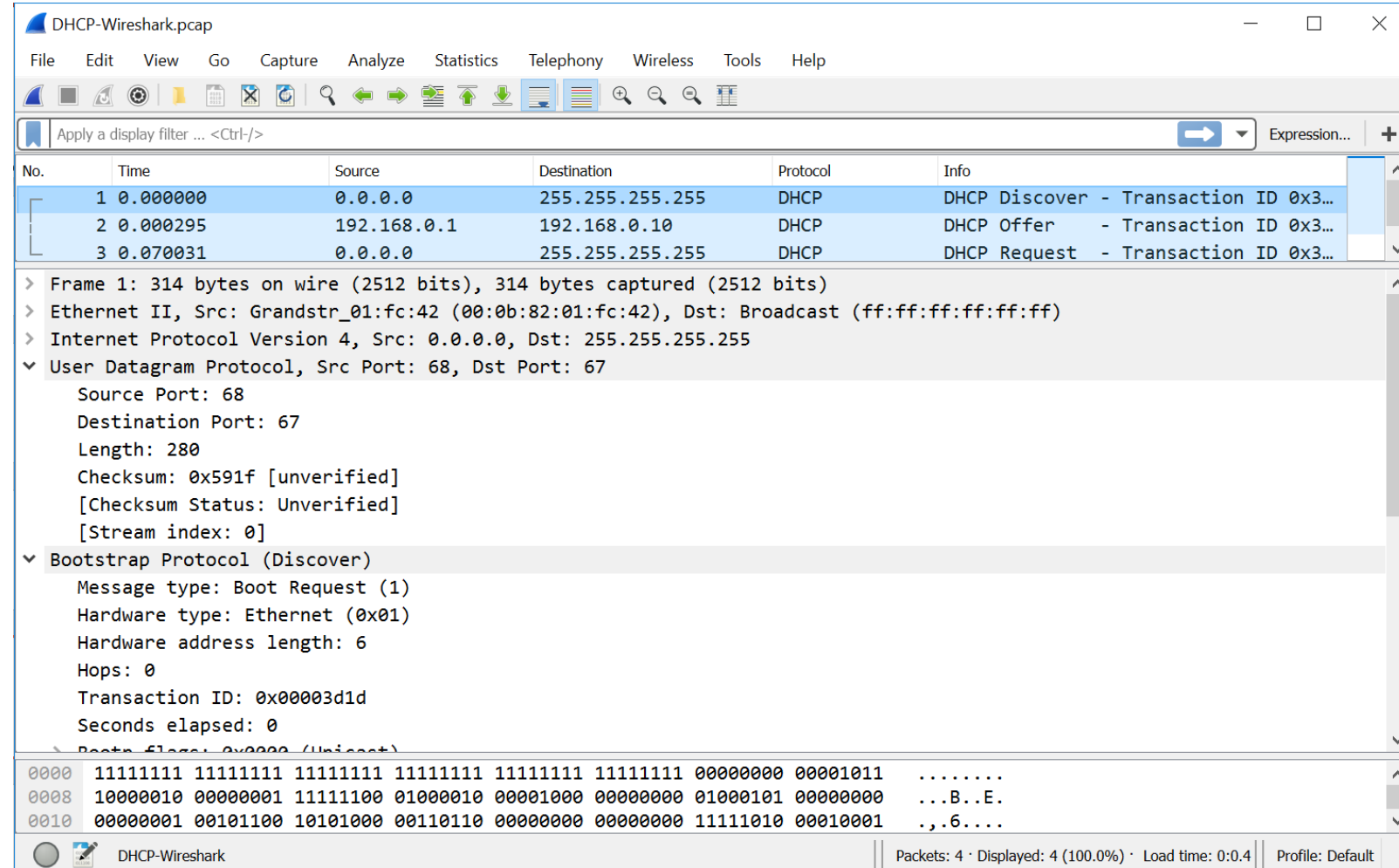
К общим программным средствам для поиска и устранения неполадок относятся:

Программное средство	Описание
Инструментарий системы управления сетью	Сетевое программное обеспечение включает в себя инструменты мониторинга, настройки и устранения неисправностей на уровне устройств. Эти средства можно использовать для анализа и устранения сетевых проблем.
Базы знаний	Базы знаний поставщиков сетевых устройств, доступные в оперативном режиме, стали незаменимыми источниками информации. Объединив возможности баз знаний поставщиков с поисковыми системами Интернета, сетевой администратор получает доступ ко множеству ресурсов с описанием практического опыта.
Средства формирования базовых показателей	Существует много средств для автоматизации процесса документирования сети и формирования базовых показателей Средства формирования базовых показателей помогают выполнять общие задачи по документированию, такие как сетевые диаграммы, обновления сетевого программного и аппаратного обеспечения, а также экономически эффективно измерять базовую пропускную способность сети.

12.2.9 АНАЛИЗАТОРЫ ПРОТОКОЛОВ

Анализатор протокола может захватывать и отображать информацию от физического уровня до уровня приложений, содержащейся в пакете.

Такие анализаторы протоколов, как Wireshark, позволяют упрощать процессы отладки, связанные с производительностью сети.



DHCP-Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x3...
2	0.000295	192.168.0.1	192.168.0.10	DHCP	DHCP Offer - Transaction ID 0x3...
3	0.070031	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3...

> Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)

> Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

▼ User Datagram Protocol, Src Port: 68, Dst Port: 67

- Source Port: 68
- Destination Port: 67
- Length: 280
- Checksum: 0x591f [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]

▼ Bootstrap Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x00003d1d
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)

0000 11111111 11111111 11111111 11111111 11111111 11111111 00000000 00001011

0008 10000010 00000001 11111100 01000010 00001000 00000000 01000101 00000000 ...B..E.

0010 00000001 00101100 10101000 00110110 00000000 00000000 11111010 00010001 ...6....

DHCP-Wireshark

Packets: 4 · Displayed: 4 (100.0%) · Load time: 0:0.4 · Profile: Default

12.2.10 АППАРАТНЫЕ СРЕДСТВА ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

Существует несколько типов средств поиска и устранения неполадок с аппаратным обеспечением.

Аппаратный инструментарий	Описание
Цифровой мультиметр	Позволяет измерять электрические значения напряжения, тока и сопротивления.
Кабельные тестеры	Портативные устройства предназначены для тестирования различных типов кабелей передачи данных.
Анализатор кабельных линий	Многофункциональные портативные устройства, используемые для тестирования и сертификации медных и волоконных кабелей.
Портативный сетевой анализатор	Специализированное устройство, используемое для устранения неполадок коммутируемых сетей и сетей VLAN.
Модуль Cisco Prime NAM	Интерфейс на основе браузера, который отображает анализ производительности устройства в коммутируемой и маршрутизируемой среде.

12.2.11 SYSLOG SERVER КАК СРЕДСТВО УСТРАНЕНИЯ НЕПОЛАДОК

Syslog используется клиентами syslog для отправки текстовых сообщений журнала на сервер syslog.

Сообщения журнала могут отправляться на консоль, линии VTY, буфер памяти или сервер syslog.

Журнальные сообщения Cisco IOS могут быть отнесены к одному из 8 уровней.

Чем меньше номер уровня, тем выше уровень серьезности.

По умолчанию в консоль выводятся сообщения уровня 6.

В выходных данных команды с уровня 0 (чрезвычайные ситуации) до 5 (уведомления) отправляются на сервер системного журнала по адресу 209.165.200.225.

Уровень	Ключевое слово
0	Чрезвычайные
1	Предупреждения
2	Критический
3	Ошибки
4	Предупреждения
5	Уведомления
6	Информационный
7	Отладка

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

12.3 ПРИЗНАКИ И ПРИЧИНЫ ПРОБЛЕМ С СЕТЬЮ

12.3.1 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА ФИЗИЧЕСКОМ УРОВНЕ

В таблице перечислены распространенные симптомы проблем с сетью на физическом уровне.

Признак	Описание
Производительность не достигает ожидаемого базового уровня	Требуются предыдущие исходные условия для сравнения. Наиболее распространенные причины включают перегруженные или недостаточно мощные серверы, неподходящие конфигурации коммутатора или маршрутизатора, перегрузку трафика на канале с низкой пропускной способностью и хроническую потерю кадров.
Потеря соединения с сетью	Потеря подключения может быть вызвана неисправностью или отключением кабеля. Может быть проверено с помощью простого теста ping . Неустойчивая связь может указывать на плохой электрический контакт или окислившиеся контактные поверхности.
Ограниченная пропускная способность или перегрузка сети	В случае сбоя маршрута протоколы маршрутизации могут перенаправить трафик на неоптимальные маршруты. Это может привести к затору или появлению «узких мест» в таких зонах сети.
Высокий уровень загрузки ЦП	Высокие показатели загрузки ЦП указывают на то, что устройство работает с предельными значениями или превышает их. Если данную проблему быстро не устранить, то перегрузка ЦП может привести к выключению или отказу устройства.
Сообщения об ошибках на консоли	Сообщения об ошибках, выводимые на консоли устройства, указывают на проблему на физическом уровне. Сообщения консоли должны регистрироваться на центральном сервере системного журнала.

12.3.1 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА ФИЗИЧЕСКОМ УРОВНЕ

К общим сетевым проблемам на физическом уровне относятся следующие:

Причина проблемы	Описание
Связанные с электропитанием	Также необходимо проверить режим работы вентиляторов и убедиться, что впускные и вытяжные вентиляционные каналы шасси не загрязнены.
Отказы оборудования	Неисправные или поврежденные файлы драйвера сетевого адаптера, неправильные кабели или проблемы заземления могут привести к ошибкам сетевой передачи, таким как поздние коллизии и карликовые кадры.
Проблемы с кабелями	Ищите поврежденные кабели, неправильный кабель и плохо обжатые разъемы. Предположительно неисправные кабели следует проверить и заменить исправными.
Затухание	Если длина кабеля превышает расчетный предел, или при наличии некачественного подключения из-за некачественного кабеля, загрязненных или окисленных контактов.
Помехи	Локальные электромагнитные помехи (EMI) могут быть сгенерированы многими источниками, такими как перекрестными помехами, близлежащие электрические кабели, большие электродвигатели, FM-радиостанции, полицейское радио и многое другое.
Ошибки в настройке интерфейса	Неправильная тактовая частота, неправильный источник синхронизации или интерфейс не включен. Это приводит к потере связи с подключенными сегментами сети.
Превышение расчетных предельных значений	Компонент может работать неоптимально, если он используется за пределами спецификаций.
Перегрузка ЦП	Симптомы включают процессы с высоким процентом использования ЦП, отбрасыванием входящей очереди, низкой производительностью, тайм-аутами SNMP, отсутствием удаленного доступа, отсутствием служб DHCP, Telnet, и эхо-запросы медленные или не отвечают.

12.3.2 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА КАНАЛЬНОМ УРОВНЕ

В таблице перечислены распространенные симптомы сетевых проблем на канальном уровне.

Признак	Описание
Потеря подключения или работоспособности сети на сетевом и вышестоящих уровнях	Некоторые проблемы, возникающие на уровне 2, могут приводить к невозможности обмена кадрами по каналу, тогда как другие проблемы будут вызывать только ухудшение уровня производительности сети.
Сеть не достигает базового показателя производительности	Кадры могут передаются по неоптимальному пути к месту назначения, но все же прибывают, что приводит к неожиданной высокой загрузке каналов. Расширенный или непрерывный пинг может помочь определить, удаляются ли кадры.
Чрезмерный объем широковещательного трафика	Операционные системы широко используют широковещательные и многоадресные рассылки. Как правило, чрезмерная широковещательная рассылка является результатом плохо запрограммированных или сконфигурированных приложений, больших широковещательных доменов уровня 2 или проблем с основной сетью.
Консольные сообщения	Маршрутизаторы выводят сообщения об ошибках при интерпретации входящих кадров (проблемы с инкапсуляцией или формированием кадров) или при отсутствии сообщений keepalive, которые должны поступать. Самое распространенное сообщение об ошибке на консоли — отключение протокола, свидетельствующее о проблеме на 2-м уровне сети.

12.3.2 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА КАНАЛЬНОМ УРОВНЕ

В таблице перечислены проблемы, которые обычно вызывают проблемы с сетью на канальном уровне.

Причина проблемы	Описание
Ошибки инкапсуляции	Происходит, когда биты, помещенные в кадр отправителем, не то, что ожидает получатель.
Ошибки сопоставления адресов	Происходит, когда адресация уровня 2 и уровня 3 недоступна.
Ошибки формирования кадров	Ошибки формирования кадров могут быть вызваны высоким уровнем помех на последовательной линии, неправильно спроектированным кабелем, неисправной сетевой интерфейсной платой, несоответствием дуплексных режимов или некорректно настроенными тактовыми сигналами на устройствах обслуживания канала.
Сбои или петли STP	Большинство проблем STP связаны с возникновением петель передачи данных, которые возникают, если в топологии с резервными путями не заблокированы порты, вследствие чего происходит циклическое перенаправление трафика, а также чрезмерная лавинная рассылка вследствие очень частого изменения топологии STP.

12.3.3 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА СЕТЕВОМ УРОВНЕ

В таблице перечислены распространенные симптомы сетевых проблем на сетевом уровне.

Признак	Описание
Сбой в сети	<p>Сбой в сети происходит в тех случаях, когда сеть полностью или частично неработоспособна, что сказывается на всех пользователях и приложениях в сети.</p> <p>Обычно о таких сбоях быстро сообщают пользователи и сетевые администраторы, и они отрицательно влияют на уровень производительности компании.</p>
Недостаточная производительность	<p>Недостаточная производительность у группы пользователей, приложений, пунктов назначения или типа трафика. Проблемы оптимизации бывает трудно обнаружить, а также довольно сложно изолировать и диагностировать. Это связано с тем, что обычно они затрагивают несколько уровней или даже сам хост целиком.</p> <p>Чтобы определить, относится ли проблема к сетевому уровню, может потребоваться некоторое время.</p>

12.3.3 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА СЕТЕВОМ УРОВНЕ

В таблице перечислены распространенные симптомы сетевых проблем на сетевом уровне.

Причина проблемы	Описание
Общие сетевые проблемы	Часто изменение топологии может неосознанно повлиять на другие области сети. Выясните, вносились ли недавно какие-либо изменения в сети, и работает ли в настоящее время кто-то над инфраструктурой сети.
Проблемы со связью	Проверьте наличие любых проблем с оборудованием и подключением, включая проблемы с питанием, проблемами окружающей среды и проблемами уровня 1, например проблемы с кабелями, неисправными портами и проблемами поставщика услуг Интернета.
Таблица маршрутизации	Проверьте, нет ли в таблице маршрутизации чего-то необычного, например, отсутствующих или неожиданных маршрутов.
Проблемы соседних устройств	Проверьте, есть ли какие-либо проблемы с соседними маршрутизаторами.
База данных топологии	Проверьте таблицу на наличие чего-то необычного, например, пропущенные записи или неожиданные записи.

12.3.4 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА ТРАНСПОРТНОМ УРОВНЕ. СПИСКИ КОНТРОЛЯ ДОСТУПА

В таблице перечислены области, в которых часто возникают неправильные конфигурации ACL.

Некорректная настройка	Описание
Выбор потока трафика	ACL должен быть применен к правильному интерфейсу в правильном направлении трафика.
Порядок контроля доступа	Записи в ACL должны строго следовать в порядке от конкретных к общим.
Неявная инструкция <code>deny any</code> ;	Неявное ACE может быть причиной неправильной конфигурации ACL.
Адреса IPv4 и шаблонные маски	Шаблонные маски IPv4 более эффективны, но в большей степени подвержены ошибкам конфигурации.
Выбор протокола транспортного уровня	Важно, чтобы в ACE был указан только правильный протокол транспортного уровня.
Порты источника и назначения	Убедитесь, что правильные входящие и исходящие порты указаны в ACE.
Используйте ключевое слово <code>established</code>	Ключевое слово established , примененное неправильно, может обеспечить неожиданные результаты.
Менее распространенные протоколы	Неправильно настроенные ACL создают проблемы для протоколов, отличных от TCP и UDP.

12.3.4 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА ТРАНСПОРТНОМ УРОВНЕ. СПИСКИ КОНТРОЛЯ ДОСТУПА

В таблице приведены общие области взаимодействия с NAT.

Признак	Описание
BOOTP и DHCP	<p>Пакет DHCP-Request имеет IPv4-адрес источника 0.0.0.0.</p> <p>Так как для NAT требуются действительные IPv4-адреса источника и назначения, то протоколы BOOTP и DHCP могут испытывать трудности при взаимодействии с маршрутизатором, на котором выполняется статическое или динамическое преобразование NAT.</p> <p>Настройка помощника (helper) для IPv4 может помочь решить эту проблему.</p>
DNS	<p>DNS-сервер не имеет точного представления о сети за NAT.</p> <p>Настройка помощника (helper) для IPv4 может помочь решить эту проблему.</p>
SNMP	<p>Станция управления SNMP на одной стороне маршрутизатора NAT может быть неспособна связываться с агентами SNMP на другой стороне маршрутизатора NAT.</p> <p>Настройка помощника (helper) для IPv4 может помочь решить эту проблему.</p>
Протоколы туннелирования и шифрования	<p>Протоколам шифрования и туннелирования часто требуется, чтобы источником трафика был конкретный порт UDP или TCP, или же они используют протокол на транспортном уровне, который не может быть обработан таблицей NAT.</p>

12.3.5 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА УРОВНЕ ПРИЛОЖЕНИЙ

В таблице приводится краткое описание этих протоколов уровня приложений.

Приложения	Описание
SSH/Telnet	Позволяет пользователям устанавливать подключения в виде сеансов терминала с удаленными хостами.
HTTP	Поддерживает обмен текстом, графическими изображениями, звуком, видео и другими мультимедийными файлами по Интернету.
FTP	Реализует интерактивный обмен файлами между компьютерами.
TFTP	Реализует базовые возможности интерактивного обмена файлами, обычно между компьютерами и сетевыми устройствами.
SMTP	Поддерживает базовые услуги доставки сообщений электронной почты.
POP	Позволяет подключаться к почтовым серверам и загружать электронную почту.
SNMP	Позволяет собирать управляющую информацию от сетевых устройств.
DNS	Сопоставляет IP-адреса с именами, назначенными сетевым устройствам.
NFS	Сетевая файловая система (NFS) позволяет компьютерам монтировать и использовать диски на удаленных хостах.

12.4 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК С IP-ПОДКЛЮЧЕНИЯМИ

12.4.1 КОМПОНЕНТЫ ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК СКВОЗНЫХ ПОДКЛЮЧЕНИЙ

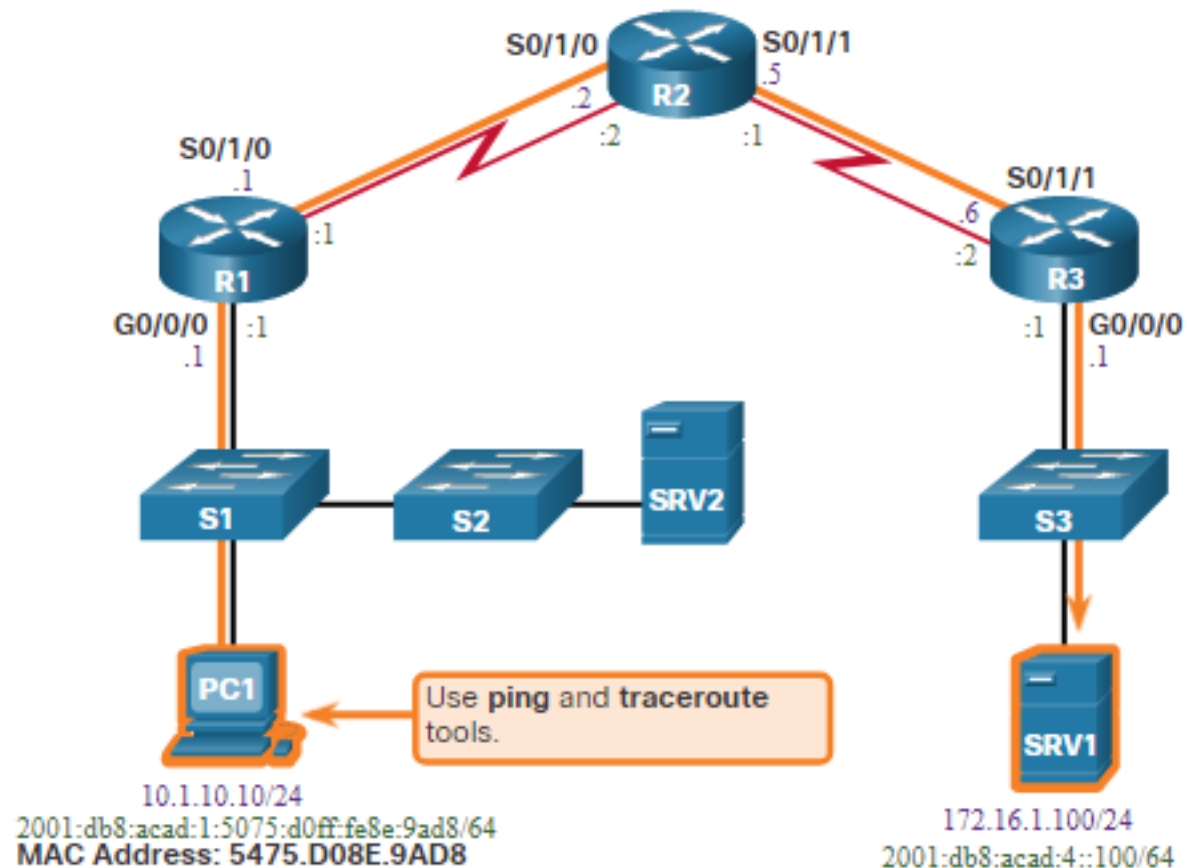
Этапы подхода «снизу вверх» при отсутствии сквозного подключения являются следующими:

- Проверить физическую связь в точке, где прекращается обмен данными в сети.
- Проверить наличие несогласованных параметров дуплексной связи.
- Проверить адресацию на канальном и сетевом уровне в локальной сети.
- Убедиться, что выбран правильный шлюз по умолчанию.
- Убедиться, что устройства определяют правильный путь от источника к пункту назначения.
- Убедиться, что транспортный уровень работает правильно.
- Убедиться, что ни один из списков ACL не блокирует трафик.
- Убедиться, что параметры DNS правильны.

12.4.2 ПРОБЛЕМА СО СВЯЗЬЮ МЕЖДУ КОНЕЧНЫМИ УСТРОЙСТВАМИ ЗАПУСКАЕТ ПРОЦЕСС ПОИСКА И УСТРАНЕНИЯ НЕПОЛАДОК

Обычно работа по поиску и устранению неполадок инициируется фактом обнаружения проблемы со связью между конечными устройствами.

Двумя наиболее распространенными служебными программами, применяемыми для проверки наличия проблемы со связью между конечными устройствами, являются ping и traceroute.



12.4.3 ШАГ 1. ПРОВЕРКА ФИЗИЧЕСКОГО УРОВНЯ

При поиске и устранении неполадок, связанных с производительностью, если предполагается неисправность аппаратного обеспечения, используйте команду `show interfaces`.

Интерес в выводе представляют:

- состояние интерфейса;
- пакеты, удаленные из входной очереди;
- пакеты, удаленные из выходной очереди;
- ошибки ввода;
- ошибки вывода.

```
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#
```


12.4.4 ШАГ 2. ПРОВЕРКА НЕСООТВЕТСТВИЯ ДУПЛЕКСНЫХ РЕЖИМОВ

В стандарте IEEE 802.3ab Gigabit Ethernet говорится об обязательном применении автоматического согласования скорости передачи данных и режима дуплекса и практически все сетевые адаптеры Fast Ethernet также используют автосогласование по умолчанию.

Проблемы могут возникнуть при несовпадении дуплекса.

```
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)#
```

12.4.5 ШАГ 3. ПРОВЕРКА АДРЕСАЦИИ В ЛОКАЛЬНОЙ СЕТИ

Команда `arp` в Windows позволяет отображать и изменять записи в кэше ARP, используемые для хранения IPv4-адресов и их разрешенных физических адресов Ethernet (MAC).

```
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:\>
```

12.4.6 ПРИМЕР УСТРАНЕНИЯ НЕПОЛАДОК, СВЯЗАННЫХ С НАЗНАЧЕНИЕМ VLAN

Другой проблемой, которую следует учитывать при диагностике связи между конечными узлами, является назначение сети VLAN.

Например, MAC-адрес на Fa0/1 должен находиться в VLAN 10 вместо 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#
```

Следующая конфигурация изменяет Fa0/1 на VLAN 10 и проверяет изменения.

```
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#
```

12.4.7 ШАГ 4. ПРОВЕРКА ШЛЮЗА ПО УМОЛЧАНИЮ

Неправильно настроенные или отсутствующие шлюзы по умолчанию могут вызвать проблемы с подключением.

На рисунке, например, шлюзы по умолчанию для:

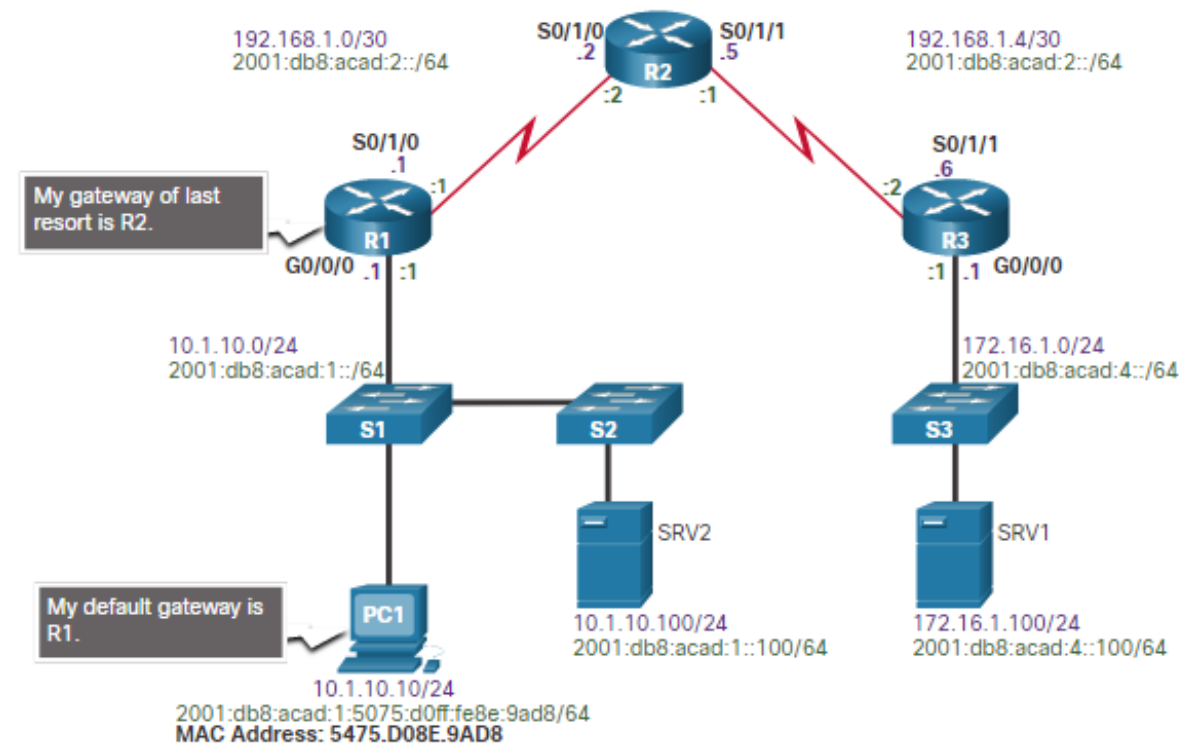
R1 - 192.168.1.2 (R2)

PC1 - 10.1.10.1 (R1 G0/0/0)

Полезные команды для проверки шлюза по умолчанию:

R1: show ip route

PC1: route print (or netstat -r)



12.4.8 ПРИМЕР УСТРАНЕНИЯ НЕПОЛАДОК ШЛЮЗА ПО УМОЛЧАНИЮ IPv6

Шлюз по умолчанию можно настроить вручную с помощью SLAAC или с помощью DHCPv6.

Например, ПК не может получить конфигурацию IPv6 с помощью SLAAC. В выходных данных команды отсутствует вся группа многоадресной рассылки IPv6-router (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 omitted)
R1#
```

R1 включен как маршрутизатор IPv6, и теперь выходные данные проверяют, является ли R1 членом ff02::2, многоадресной группы All-IPv6-Routers.

```
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
(Output omitted)
R1#
```

12.4.9 ШАГ 5. ПРОВЕРКА ПРАВИЛЬНОГО ПУТИ

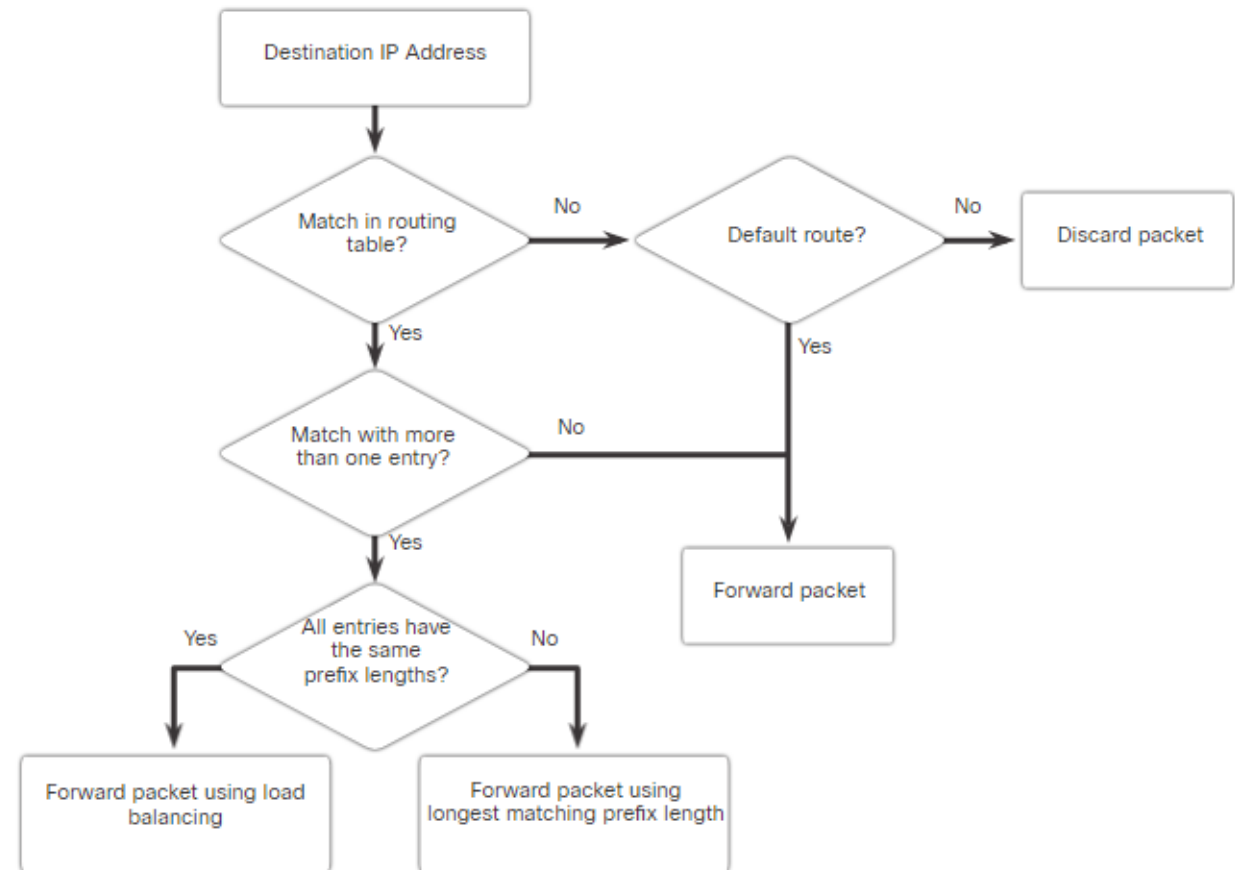
При диагностике неполадок часто приходится проверять путь до сети назначения.

В следующем списке и на рисунке описывается процедура для таблиц маршрутизации IPv4 и IPv6.

Процесс перенаправления пакетов IPv4 и IPv6 основан на наибольшем совпадении битов или наибольшем совпадении префиксов.

Процесс в таблице маршрутизации будет пытаться перенаправить пакет с помощью записи в таблице маршрутизации с максимально большим числом битов, совпавших слева.

Число совпадающих битов указывается длиной префикса маршрута.



12.4.10 ШАГ 6. ПРОВЕРКА ТРАНСПОРТНОГО УРОВНЯ

Двумя самыми распространенными проблемами, влияющими на связь на транспортном уровне, являются настройки списков ACL и настройки NAT.

Общим средством для тестирования функций транспортного уровня является служебная программа Telnet.

Например, администратор пытается установить соединение по протоколу Telnet с R2 используя порт 80.

```
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#
```

12.4.11 ПРОВЕРКА СПИСКОВ КОНТРОЛЯ ДОСТУПА

На маршрутизаторах могут быть настроены ACL, не позволяющие протоколам передавать информацию через интерфейс во входящем или исходящем направлении.

В этом примере ACL 100 настроен неправильно. Входящий на G0/0/0 вместо входящего на 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#
```

ACL удаляется из G0/0 и настраивается входящий на 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#
```


12.4.12 ШАГ 8. ПРОВЕРКА DNS

Протокол DNS позволяет управлять системой DNS, представляющей собой распределенную базу данных, с помощью которой можно сопоставлять имена компьютеров с IP-адресами.

После настройки DNS на устройстве IP-адрес можно заменить на имя компьютера для всех команд IP, например ping или telnet.

Используйте команду глобальной конфигурации `ip host`, чтобы ввести имя, которое будет использоваться вместо адреса IPv4 коммутатора или маршрутизатора, как показано в выходных данных команды.

Используйте команду Windows `nslookup` для отображения информации о сопоставлении имени с IP-адресом.

```
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#
```