Лекция 4. Сетевые характеристики: надёжность

Дисциплина: Сетевые технологии

Цель лекции

Изучить основные характеристики надёжности компьютерных сетей, причины потери пакетов, показатели доступности и отказоустойчивости, принципы использования альтернативных маршрутов, повторной передачи данных и механизма скользящего окна.

1. Понятие надёжности компьютерной сети

Надёжность компьютерной сети представляет собой способность сети сохранять работоспособность и обеспечивать передачу данных с требуемым качеством в течение определённого времени.

Надёжность имеет большое значение для корпоративных сетей, банковских систем, медицинских учреждений, университетов и других организаций, в которых потеря связи может привести к нарушению работы информационных систем.

Надёжность сети зависит от состояния каналов связи, сетевого оборудования, программного обеспечения, источников электропитания и правильности настройки сетевых протоколов.

Основные характеристики надёжности

- Потери пакетов показывают долю пакетов, которые не были доставлены получателю.
- Доступность характеризует долю времени, в течение которого сеть или услуга работоспособна.
- Отказоустойчивость характеризует способность сети сохранять работу при отказе отдельных компонентов.
- Время восстановления показывает, сколько времени требуется для восстановления работы после отказа.
- Среднее время наработки на отказ (MTBF) характеризует средний интервал между отказами ремонтируемого оборудования.
- Среднее время восстановления (MTTR) показывает среднюю продолжительность восстановления после отказа.

Эти показатели дополняют друг друга. Например, сеть может иметь низкий процент потерь пакетов при нормальной работе, но при отказе единственного маршрутизатора полностью потерять связь. Поэтому для оценки надёжности

необходимо учитывать не только качество передачи данных, но и возможность восстановления связи.

2. Характеристики потерь пакетов

Потеря пакета возникает, когда отправленный сетевой пакет не достигает получателя в предусмотренных условиях передачи.

При передаче данных информация разделяется на пакеты. Каждый пакет содержит полезные данные и служебную информацию, необходимую для доставки.

В реальной сети пакеты могут теряться из-за перегрузки каналов, ошибок передачи, отказов оборудования или неправильной конфигурации.

2.1. Основные причины потери пакетов

1. Перегрузка сети. Число поступающих пакетов превышает возможности их обработки и передачи.
2. Переполнение очередей. Маршрутизатор или коммутатор не может сохранить все поступившие пакеты в буфере.
3. Ошибки канала связи. Помехи и повреждение данных могут привести к отбрасыванию кадров или пакетов.
4. Отказ оборудования. Неисправность маршрутизатора, коммутатора или сетевого интерфейса нарушает передачу.
5. Ошибки настройки. Неправильные маршруты, фильтры или правила межсетевого экрана могут блокировать трафик.
6. Перегрузка конечного устройства. Получатель может не успевать обрабатывать поступающие данные.

2.2. Расчёт процента потерь пакетов

Процент потерь определяется по формуле:

$$P_{\text{потерь}} = \frac{N_{\text{отпр}} - N_{\text{получ}}}{N_{\text{отпр}}} \cdot 100\%$$

где:

- $N_{\text{отпр}}$ — число отправленных пакетов;
- $N_{\text{получ}}$ — число полученных пакетов.

Пример.

Устройство отправило 1000 пакетов. Получатель принял 980 пакетов.

$$P_{\text{потерь}} = \frac{1000 - 980}{1000} \cdot 100\% = 2\%$$

Таким образом, потери составили 2%.

2.3. Влияние потерь на работу приложений

Приложение	Последствия потери пакетов
Электронная почта	Возможны повторные передачи или задержка доставки
Передача файлов	Повторная передача потерянных данных увеличивает время загрузки
Видеоконференция	Могут появиться пропуски звука и искажения изображения
Онлайн-игры	Возможны задержки и потеря игровых событий
Веб-сервисы	Может увеличиться время ответа
IP-телефония	Возможны прерывания речи и ухудшение качества разговора

Влияние потерь зависит от протокола и приложения. Например, TCP может обнаружить потерю и повторно передать данные, а UDP сам по себе не обеспечивает повторную передачу.

2.4. Способы уменьшения потерь

Для снижения потерь пакетов применяются:

- увеличение пропускной способности каналов;
- настройка очередей и приоритетов трафика;
- модернизация сетевого оборудования;
- устранение неисправностей линий связи;
- резервирование каналов;
- контроль загрузки сети;
- настройка протоколов передачи данных.

3. Доступность и отказоустойчивость

3.1. Доступность сети

Доступность показывает, какую долю времени сеть или услуга находится в рабочем состоянии и доступна пользователям.

Доступность обычно выражается в процентах.

$$A = \frac{T_{\text{работы}}}{T_{\text{общ}}} \cdot 100\%$$

где:

- A— доступность;
- $T_{\text{работы}}$ — время работоспособности;
- $T_{\text{общ}}$— общий период наблюдения.

Если сеть работала 719 часов из 720 часов за условный 30-дневный месяц, то:

$$A = \frac{719}{720} \cdot 100\% \approx 99{,}86\%$$

Следовательно, доступность сети составила около 99,86%.

Пример допустимого простоя

Расчёт для условного месяца продолжительностью 30 суток, или 720 часов.

Доступность	**Примерный простой за месяц**
99%	7 ч 12 мин
99,9%	43 мин 12 с
99,99%	4 мин 19 с
99,999%	26 с

Чем выше показатель доступности, тем меньше допустимое время простоя. Однако фактические условия расчёта зависят от методики измерения и соглашения об уровне обслуживания (SLA).

3.2. Отказоустойчивость

Отказоустойчивость представляет собой способность сети продолжать работу при отказе одного или нескольких компонентов.

Для повышения отказоустойчивости используются:

- резервные маршрутизаторы;
- дополнительные коммутаторы;
- резервные линии связи;
- дублирующие источники электропитания;
- альтернативные пути передачи данных;
- автоматическое переключение на резервные компоненты.

Например, если корпоративная сеть использует только один маршрутизатор для выхода в Интернет, его отказ может полностью нарушить связь. Если предусмотрен второй маршрутизатор и механизм автоматического переключения, связь может быть сохранена.

3.3. Различие между доступностью и отказоустойчивостью

Характеристика	Доступность	Отказоустойчивость
Основной смысл	Доля времени работоспособности	Сохранение работы при отказах
Способ оценки	Процент времени	Поведение сети при отказе компонентов
Основные средства	Мониторинг, обслуживание, восстановление	Резервирование, альтернативные маршруты
Пример	Сеть доступна 99,9% времени	При отказе основного канала включается резервный

Отказоустойчивость способствует повышению доступности, но эти понятия не являются одинаковыми.

4. Альтернативные маршруты передачи данных

Альтернативный маршрут представляет собой дополнительный путь передачи пакетов между отправителем и получателем.

В компьютерных сетях маршрутизаторы определяют, через какие интерфейсы и соседние узлы следует передавать пакеты. Если основной маршрут становится недоступным, сеть может выбрать другой путь, если он заранее предусмотрен или может быть найден протоколом маршрутизации.

4.1. Пример сети с резервным маршрутом



Оба маршрута ведут к узлу назначения. Если основной путь недоступен, резервный может обеспечить передачу данных.

Рисунок 1. Пример основного и резервного маршрутов.

4.2. Как работают альтернативные маршруты

1. Маршрутизатор определяет основной маршрут к сети назначения.
2. Пакеты передаются через выбранный путь.
3. При отказе канала или соседнего узла обнаруживается изменение состояния сети.
4. Протокол маршрутизации или механизм резервирования выбирает доступный альтернативный путь.
5. Передача данных восстанавливается через резервный маршрут.

Время восстановления зависит от протокола маршрутизации, настроек оборудования и способа обнаружения отказа. Поэтому переключение не всегда происходит мгновенно.

4.3. Технологии и протоколы резервирования

Для обеспечения альтернативных маршрутов применяются:

- OSPF и IS-IS для маршрутизации внутри автономной системы;
- BGP для обмена маршрутами между автономными системами;
- VRRP для резервирования шлюза по умолчанию;
- RSTP для предотвращения петель и восстановления связности на канальном уровне в Ethernet-сетях;
- резервные физические линии и независимые каналы связи.

Важно различать резервирование маршрута и балансировку нагрузки. При резервировании дополнительный путь может использоваться только при отказе основного. При балансировке нагрузка распределяется между несколькими доступными путями.

5. Повторная передача потерянных пакетов

Повторная передача представляет собой механизм, при котором данные отправляются повторно, если их доставка не была подтверждена или обнаружена потеря.

Повторная передача помогает восстановить целостность данных, но может увеличить задержку и нагрузку на сеть.

5.1. Принцип работы повторной передачи

1. Отправитель передаёт пакет или блок данных.
2. Получатель принимает данные и отправляет подтверждение.
3. Отправитель ожидает подтверждение в течение определённого времени.
4. Если подтверждение не поступило, отправитель предполагает потерю данных или подтверждения.

5. Отправитель повторяет передачу в соответствии с правилами используемого протокола.

Пример обмена данными с повторной передачей



5.2. Повторная передача в TCP

Протокол TCP обеспечивает надёжную передачу потока данных. Для этого он использует:

- номера последовательности;
- подтверждения получения (ACK);
- таймеры повторной передачи;
- обнаружение потерь;
- повторную отправку отсутствующих данных.

TCP может обнаружить потерю по истечении таймера или по поступлению нескольких одинаковых подтверждений. В зависимости от ситуации применяются разные механизмы восстановления.

При этом TCP не передаёт каждый IP-пакет повторно автоматически на уровне IP. Повторная передача выполняется транспортным протоколом для восстановления потерянных данных.

5.3. Преимущества и недостатки повторной передачи

Преимущества:

- повышается надёжность передачи данных;
- восстанавливаются потерянные блоки;
- обеспечивается целостность потока данных;
- приложения получают данные в правильной последовательности.

Недостатки:

- увеличивается время передачи;

- возрастает сетевой трафик;
- дополнительная нагрузка может усилить перегрузку;
- при больших задержках подтверждения восстановление занимает больше времени.

В приложениях реального времени, например в голосовой связи, повторная передача может оказаться бесполезной, если данные поступят слишком поздно. Поэтому такие приложения часто используют UDP и механизмы обработки потерь на уровне приложения.

6. Механизм скользящего окна

Скользящее окно представляет собой механизм управления передачей данных, при котором отправитель может передать несколько блоков данных до получения подтверждения на каждый из них.

Этот механизм повышает эффективность канала, поскольку отправителю не требуется ожидать подтверждение после передачи каждого отдельного блока.

Скользящее окно применяется, в частности, в протоколе TCP.

6.1. Принцип работы

В механизме скользящего окна определённое количество данных может находиться в состоянии передачи, но ещё не подтверждено получателем.

После получения подтверждения окно сдвигается вперёд, и отправитель получает возможность передать новые данные.

Основные элементы:

- Размер окна определяет объём данных, который может находиться в передаче без подтверждения.
- Номер последовательности позволяет определить положение данных в потоке.
- Подтверждение ACK сообщает о получении данных.
- Сдвиг окна открывает возможность для отправки следующего блока.

6.2. Пример работы скользящего окна

Предположим, размер окна равен четырём сегментам.

Состояние 1. Передача сегментов



Состояние 2. Получены подтверждения сегментов 1 и 2



Подтверждённые сегменты освобождают место в окне.

Состояние 3. Окно сдвинулось



Отправитель может передать новые сегменты 5 и 6, если другие условия передачи

это позволяют.

Рисунок 3. Упрощённый пример скользящего окна.

6.3. Преимущества скользящего окна

- повышается эффективность использования канала;
- уменьшается время ожидания между передачами;
- поддерживается передача нескольких сегментов до получения подтверждений;
- обеспечивается управление объёмом данных в пути;
- улучшается использование каналов с высокой задержкой.

Размер окна влияет на производительность TCP. Если окно слишком мало, канал может использоваться не полностью, особенно при большой задержке между отправителем и получателем.

6.4. Связь размера окна и производительности

Для эффективной передачи данных размер окна должен соответствовать объёму данных, который можно передать за время кругового обхода (RTT).
Приближённая оценка необходимого объёма данных:

$$W \approx R \cdot RTT$$

где:

- W — объём данных в битах;
- R — целевая скорость передачи в бит/с;
- RTT — время кругового обхода в секундах.

Например, для канала со скоростью 100 Мбит/с и RTT, равным 40 мс:

$$W \approx 100 \cdot 10^6 \cdot 0{,}04 = 4 \cdot 10^6 \text{ бит}$$

Это соответствует приблизительно 500 Кбайт данных.

Следовательно, для поддержания такой скорости в идеализированном случае требуется около 500 Кбайт данных в пути. Реальная производительность также зависит от потерь, алгоритма управления перегрузкой TCP, полученного окна и других ограничений.

7. Способы повышения надёжности сети

Для обеспечения надёжной передачи данных применяется комплекс технических и программных решений.

Основные методы

1. Резервирование оборудования. Использование дополнительных маршрутизаторов, коммутаторов и источников питания позволяет снизить зависимость от одного устройства.

2. Резервирование каналов связи. Дополнительные линии обеспечивают альтернативные пути передачи данных.

3. Использование динамической маршрутизации. Протоколы маршрутизации могут выбирать доступные маршруты после изменения состояния сети.

4. Повторная передача. Транспортные протоколы восстанавливают потерянные данные, если механизм надёжной доставки предусмотрен.

5. Управление очередями. Настройка буферов и приоритетов помогает снизить потери при перегрузке.

6. Мониторинг сети. Контроль задержки, доступности, потерь и загрузки позволяет обнаруживать неисправности.

7. Регулярное обслуживание. Проверка оборудования, обновление программного обеспечения и устранение неисправностей снижают риск отказов.

8. Резервное копирование конфигураций. Сохранение настроек упрощает восстановление оборудования после сбоя.

Важно учитывать, что отдельные меры не гарантируют полной надёжности. Например, два канала связи не обеспечат реальное резервирование, если оба проходят через один и тот же кабельный колодец или зависят от одного источника электропитания.

Заключение

В ходе лекции были рассмотрены основные характеристики надёжности компьютерных сетей: потери пакетов, доступность, отказоустойчивость и время восстановления.

Было установлено, что потери пакетов могут возникать из-за перегрузки, ошибок каналов и отказов оборудования. Для повышения доступности применяются резервные устройства и альтернативные маршруты. Повторная передача помогает восстановить потерянные данные, а механизм скользящего окна повышает эффективность использования канала.

Надёжность сети зависит от совместного применения резервирования, управления трафиком, протоколов передачи данных и постоянного контроля состояния инфраструктуры.

Контрольные вопросы

1. Что такое надёжность компьютерной сети?
2. Какие основные причины потери пакетов существуют?
3. Как рассчитывается процент потерь пакетов?
4. Что такое доступность сети?
5. Чем доступность отличается от отказоустойчивости?
6. Для чего используются альтернативные маршруты?
7. Какие протоколы помогают обеспечить резервирование и восстановление маршрутов?
8. Как работает механизм повторной передачи в TCP?
9. Какие преимущества и недостатки имеет повторная передача?
10. Что такое скользящее окно?
11. Как подтверждения ACK влияют на работу скользящего окна?
12. Как размер окна связан с пропускной способностью и RTT?

13. Какие меры повышают надёжность корпоративной сети?

Практическое задание

Тема: Анализ надёжности компьютерной сети.

Выполните следующие задания.

1. Рассчитайте процент потерь, если из 2500 отправленных пакетов получено 2475.
2. Определите доступность сети за месяц продолжительностью 720 часов, если суммарный простой составил 36 минут.
3. Нарисуйте схему сети с основным и резервным маршрутами между двумя офисами.
4. Объясните, как изменится работа сети при отказе основного маршрутизатора, если резервный маршрутизатор настроен правильно.
5. Нарисуйте временную схему повторной передачи потерянного сегмента TCP.
6. Покажите на рисунке, как скользящее окно сдвигается после получения подтверждений.

Дополнительное задание: предложите структуру корпоративной сети университета, которая сохранит доступ к серверу и Интернету при отказе одного канала связи. Укажите, какие компоненты необходимо зарезервировать и как можно обнаружить отказ.