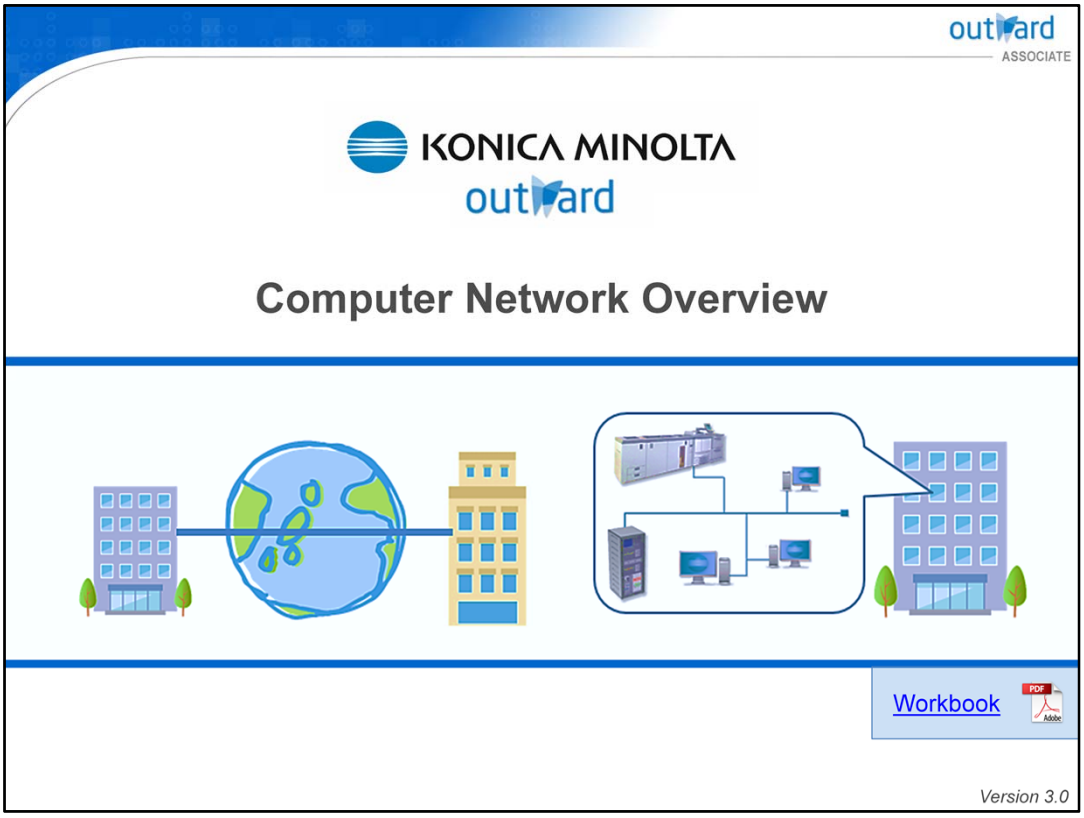
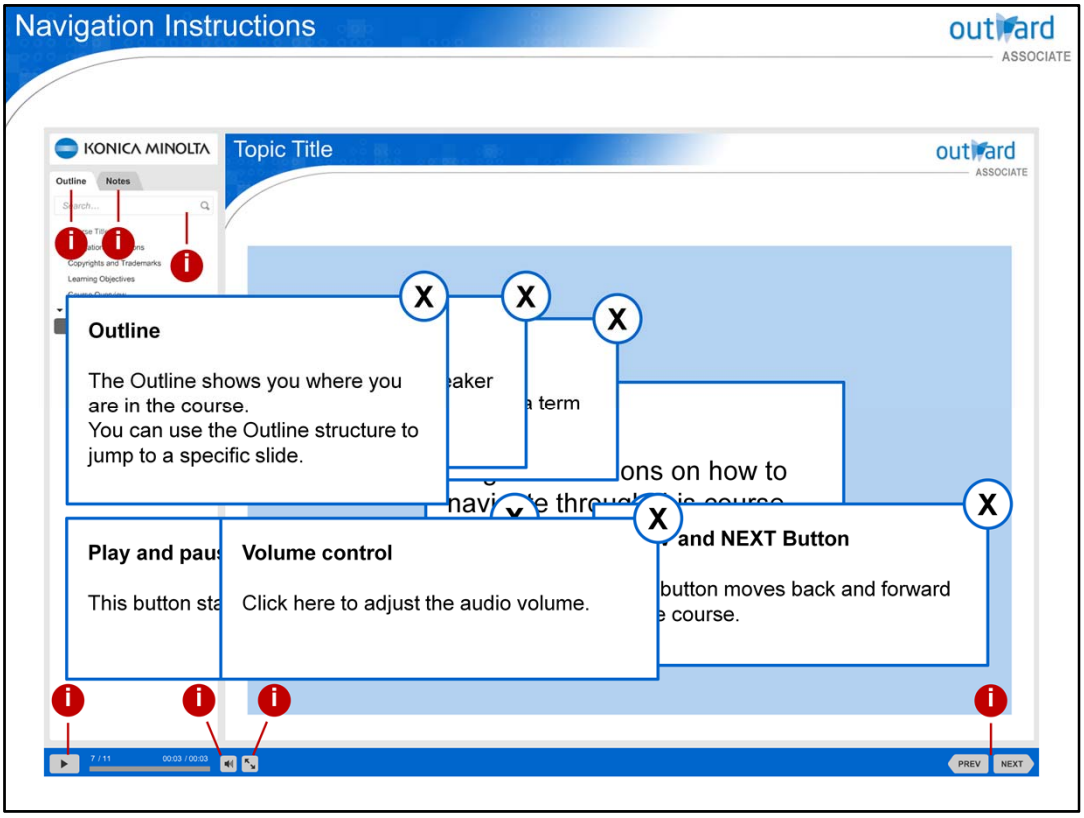
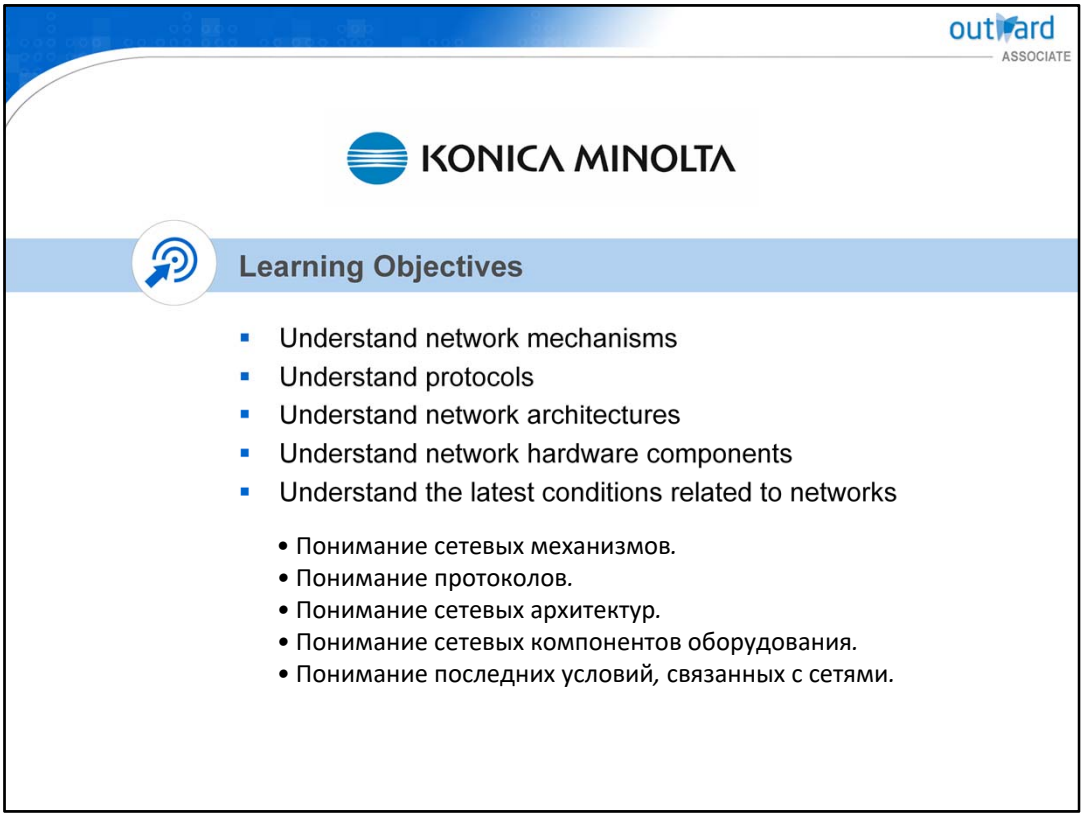


Welcome to the OUTWARD course “Computer Network Overview”! The estimated runtime of this course is 60 minutes.



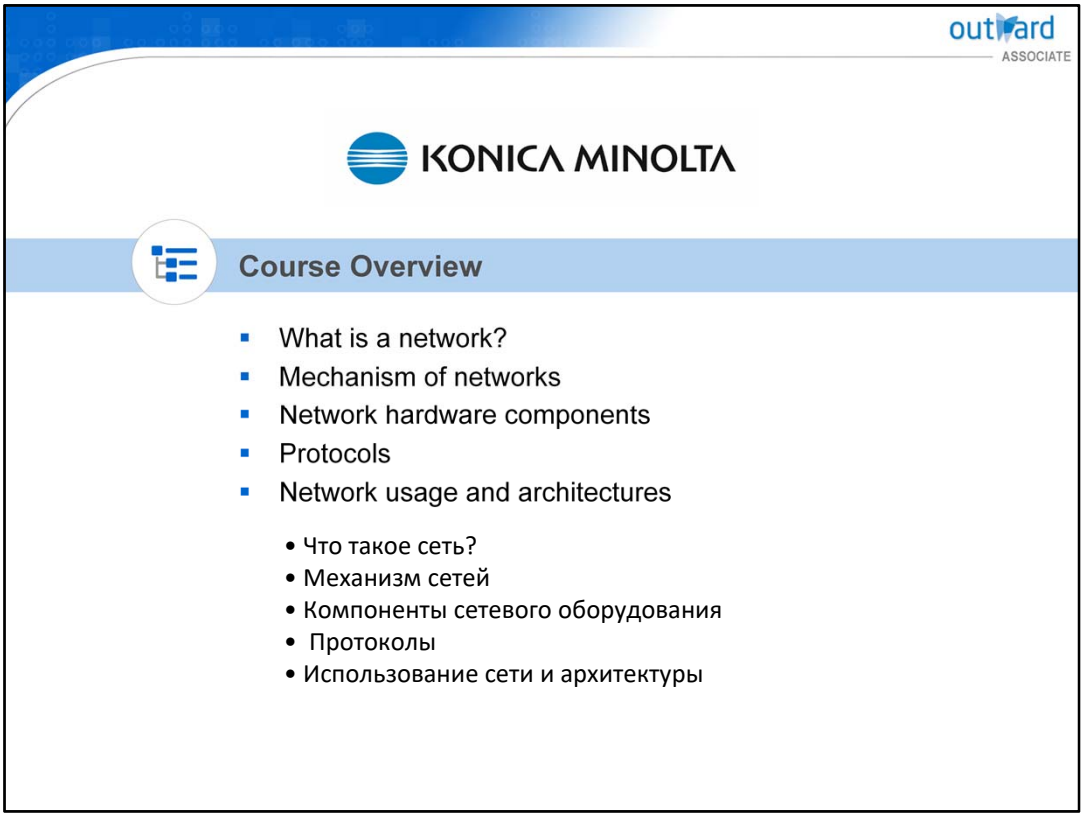
Here you see how to navigate within the course.

Copyrights and Trademarks



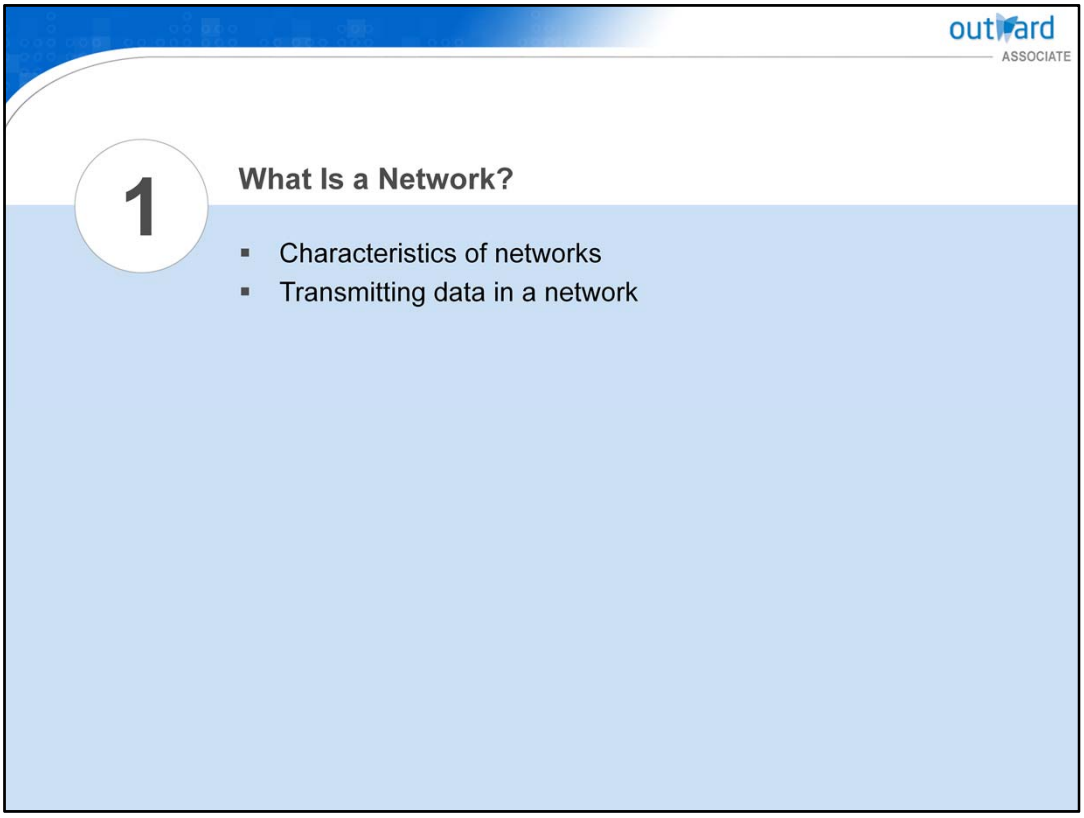
The learning objectives for this course are as shown here. You will learn why networks are connected and how data is transmitted. You will also learn how our enterprise networks are used.
You will learn about the network architecture of companies. You will learn about the main hardware components used to configure networks.
And finally, you will learn about the latest conditions related to constantly evolving networks.
This course helps to develop an understanding of basic network environments.

Цели обучения для этого курса, как показано здесь. Вы узнаете, почему сети подключены и как данные передаются. Вы также узнаете, как используются наши корпоративные сети.
Вы узнаете о сетевой архитектуре компаний. Вы узнаете об основных аппаратных компонентах, используемых для настройки сетей.
И, наконец, вы узнаете о последних условиях, связанных с постоянно развивающимися сетями.
Этот курс помогает развить понимание основных сетевых сред.

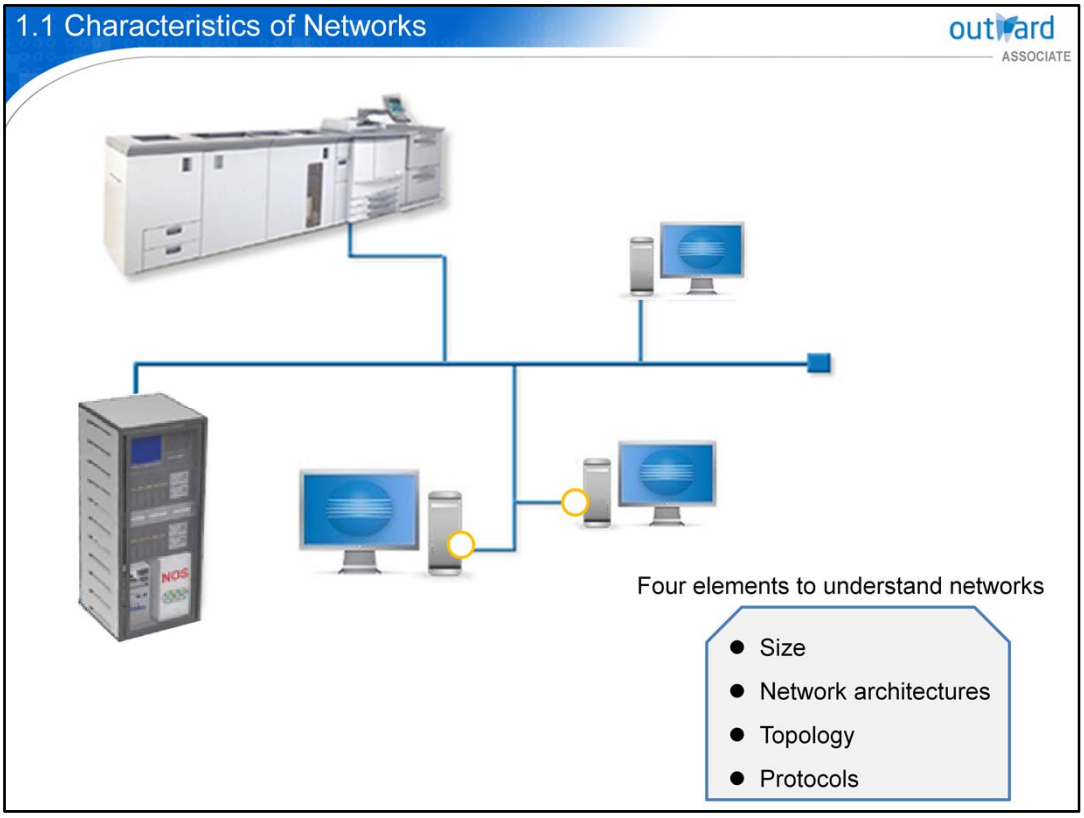


Networks have become an essential part of our day-to-day lives.
Now, anyone can easily connect to a network not only through a wired connection at home or in the office, but also through wireless communication outdoors.
In this course, you will learn about computer networks.
In particular, we will provide an overview of software aspects and hardware aspects to provide an understanding of the mechanism of networks.
Then, you will learn what networks are and how networks communicate.

Сети стали неотъемлемой частью нашей повседневной жизни.
Теперь любой желающий может легко подключиться к сети не только через проводное соединение дома или в офисе, но и через беспроводную связь на улице.
В этом курсе вы узнаете о компьютерных сетях.
В частности, мы предоставим обзор программных аспектов и аппаратных аспектов, чтобы обеспечить понимание механизма сетей.
Затем вы узнаете, что такое сети и как они взаимодействуют.

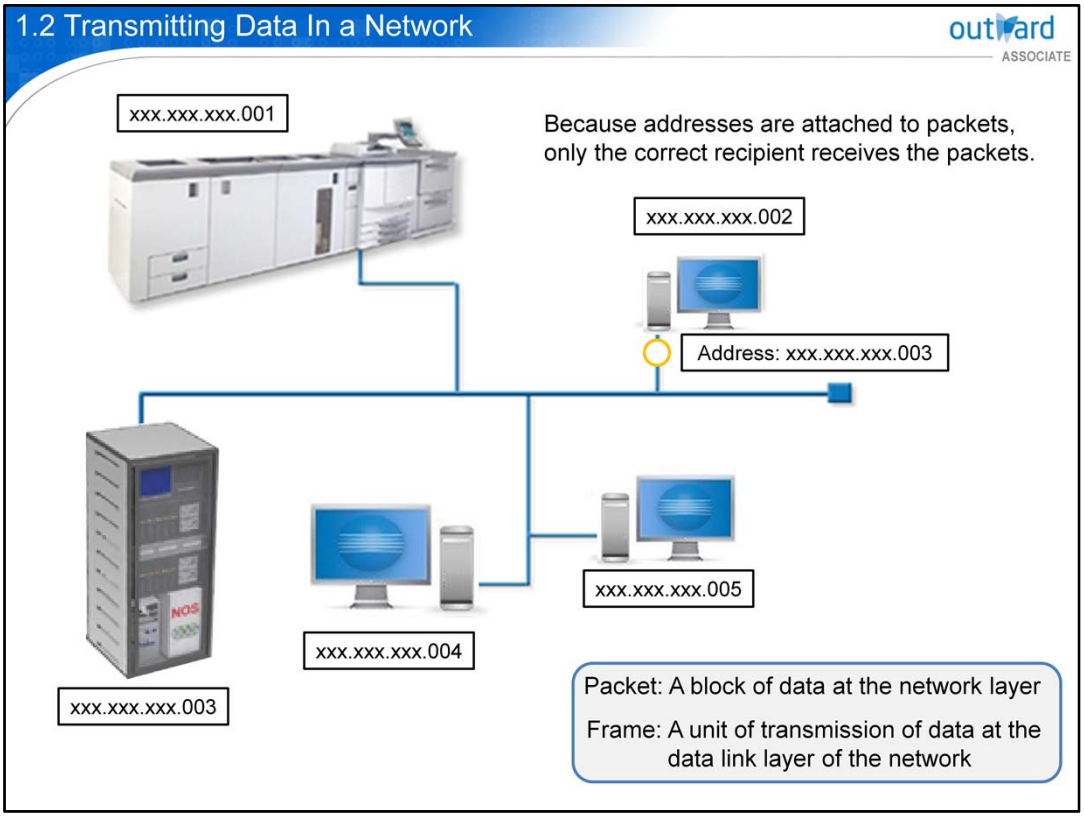


This lesson describes what networks are and how data is transmitted in a network.



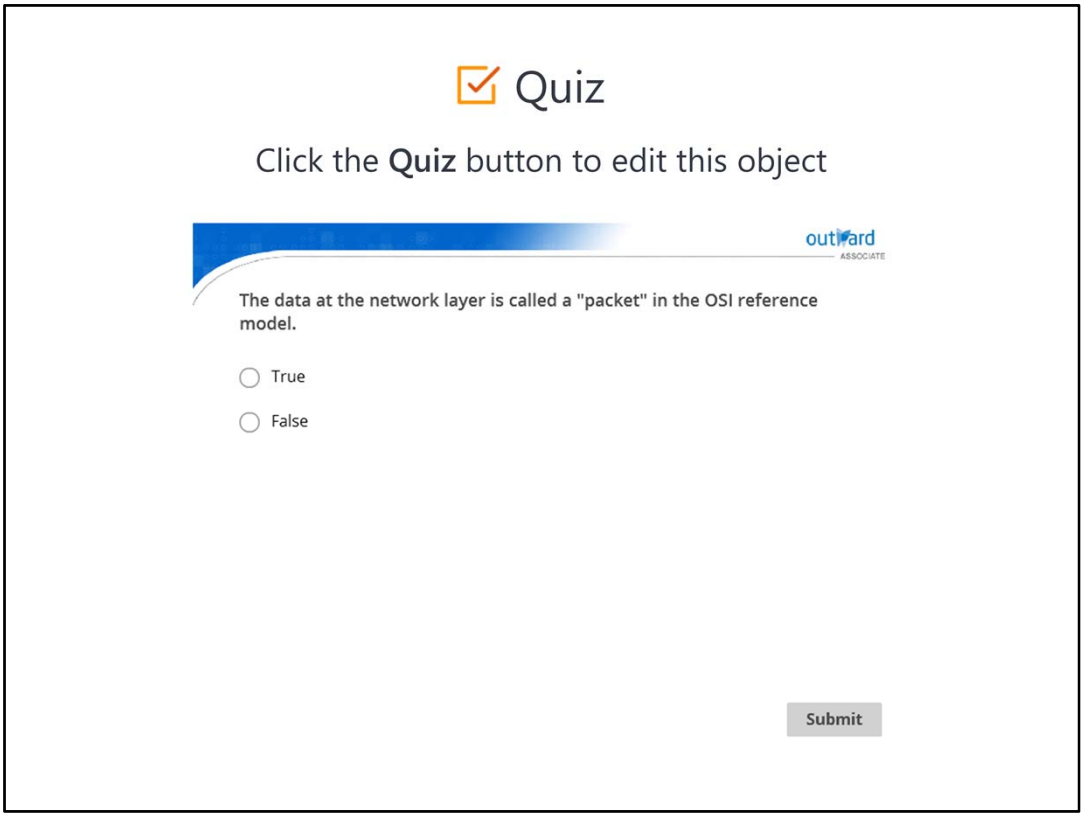
A network is a number of computers and peripherals linked together so that data can be passed between them.
The rise in the popularity of networks has led various approaches to network construction.
To help distinguish between different approaches, engineers categorize networks according to four elements.
The four elements are network size, the model or architecture of how the network functions, the topology, meaning how the networks are arranged, and the protocols used, which are the set of rules they observe when communicating.

Сеть - это несколько компьютеров и периферийных устройств, связанных между собой так, что между ними могут передаваться данные.
Рост популярности сетей привел к различным подходам к построению сетей.
Чтобы помочь отличить разные подходы, инженеры классифицируют сети по четырем элементам.
Четырьмя элементами являются размер сети, модель или архитектура функционирования сети, топология, то есть, как организованы сети, и используемые протоколы, которые представляют собой набор правил, которые они соблюдают при общении.

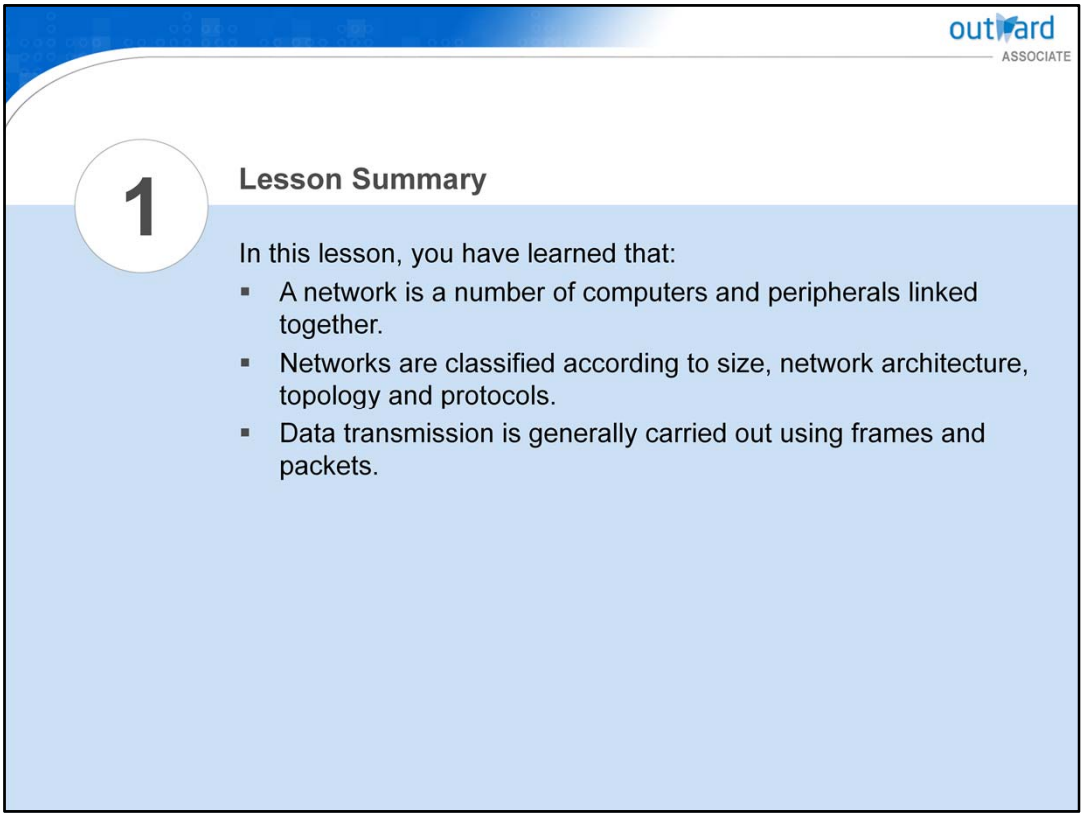


The most common forms of data transmission in a network use frames and packets of data.
A packet is a block of data at the network layer and is destined from one point in the network to another point.
A frame is the unit of transmission of data at the data link layer of the network.
Packets of data are encoded on top of frames, or in other words frames are used to transfer packets of data across the network.
The packets are transmitted via cabling or a wireless communication medium used by the network.
In order to identify the destination of the data packet, an address is attached to it.
The address is a unique identifier of the destination point, whether it is a workstation, printer, or other network hardware component.
In this example, a work station whose address is .002 sends packet data to a workstation whose address is .003.
The destination address attached to the packet ensures that it is directed to the right part of the network.
Only the addressee will be able to receive it.
The structure and addressing of packets is determined by the network protocols the operating system implements.

Наиболее распространенные формы передачи данных в сети используют кадры и пакеты данных.
Пакет представляет собой блок данных на сетевом уровне и предназначен из одной точки сети в другую точку.
Кадр - это единица передачи данных на канальном уровне сети.
Пакеты данных кодируются поверх кадров, или, другими словами, кадры используются для передачи пакетов данных по сети.
Пакеты передаются по кабелю или беспроводной среде связи, используемой в сети.
Чтобы идентифицировать пункт назначения пакета данных, к нему прикрепляется адрес.
Адрес является уникальным идентификатором точки назначения, будь то рабочая станция, принтер или другой компонент сетевого оборудования.
В этом примере рабочая станция с адресом .002 отправляет пакетные данные на рабочую станцию с адресом .003.
Адрес назначения, прикрепленный к пакету, гарантирует, что он направлен в правую часть сети. Только адресат сможет получить его.
Структура и адресация пакетов определяются сетевыми протоколами, которые реализует операционная система.

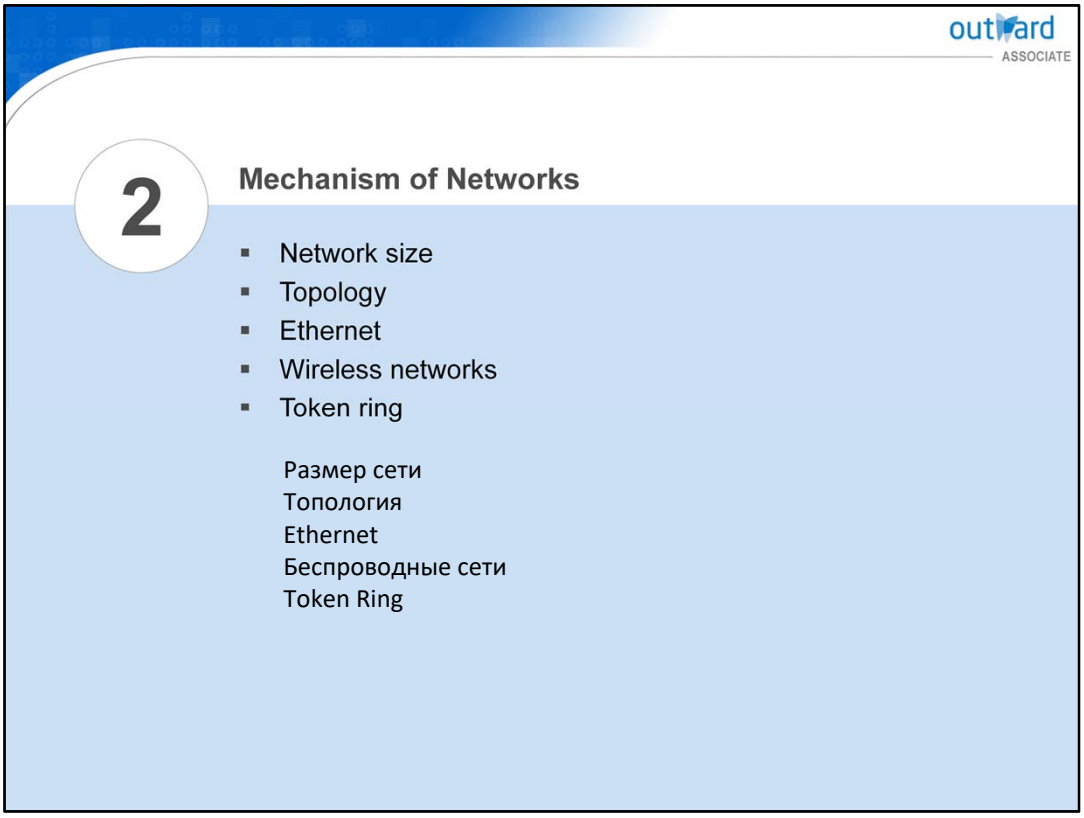


Test your knowledge in a quiz!

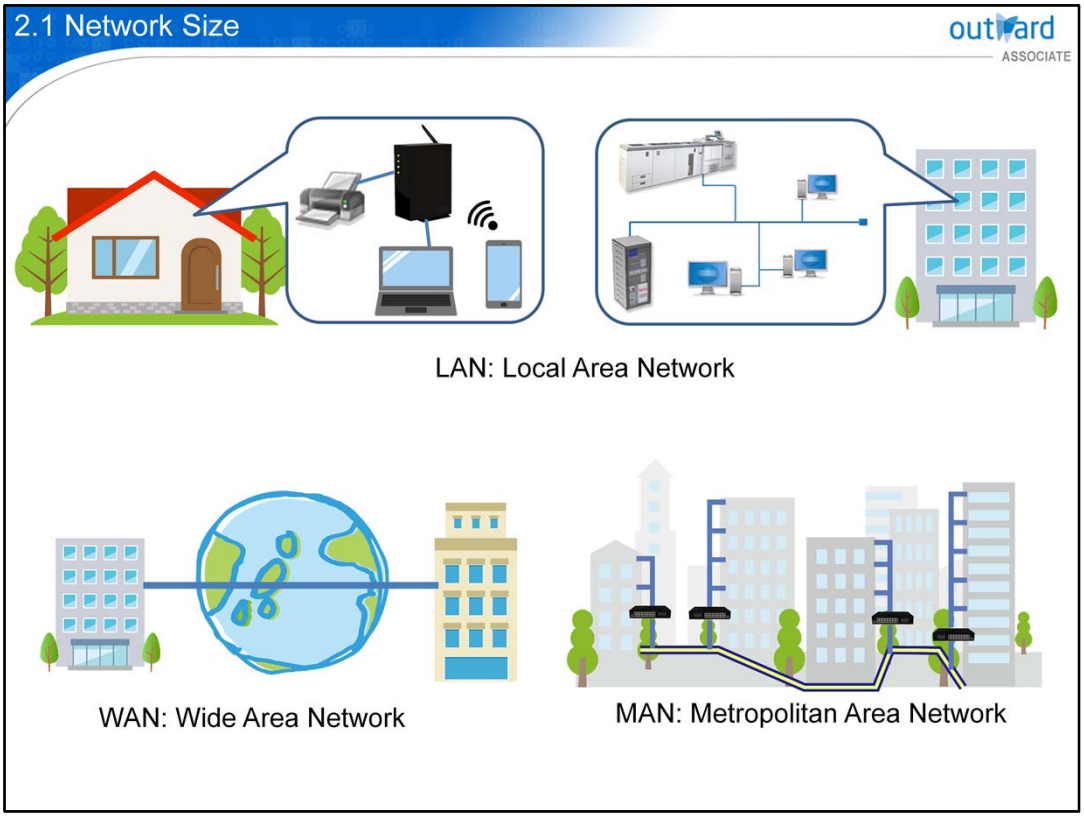


• A network is a number of computers and peripherals linked together so that data can be transferred.
• Because there are various ways to create networks, they are classified based on four items: size, network architecture, topology and protocols.
• Data transmission is generally carried out using frames and packets, and packets contain address information for identifying the destination.

• Сеть - это несколько компьютеров и периферийных устройств, связанных между собой, чтобы можно было передавать данные.
• Поскольку существуют различные способы создания сетей, они классифицируются на основе четырех элементов: размер, архитектура сети, топология и протоколы.
• Передача данных обычно осуществляется с использованием кадров и пакетов, а пакеты содержат адресную информацию для идентификации пункта назначения.

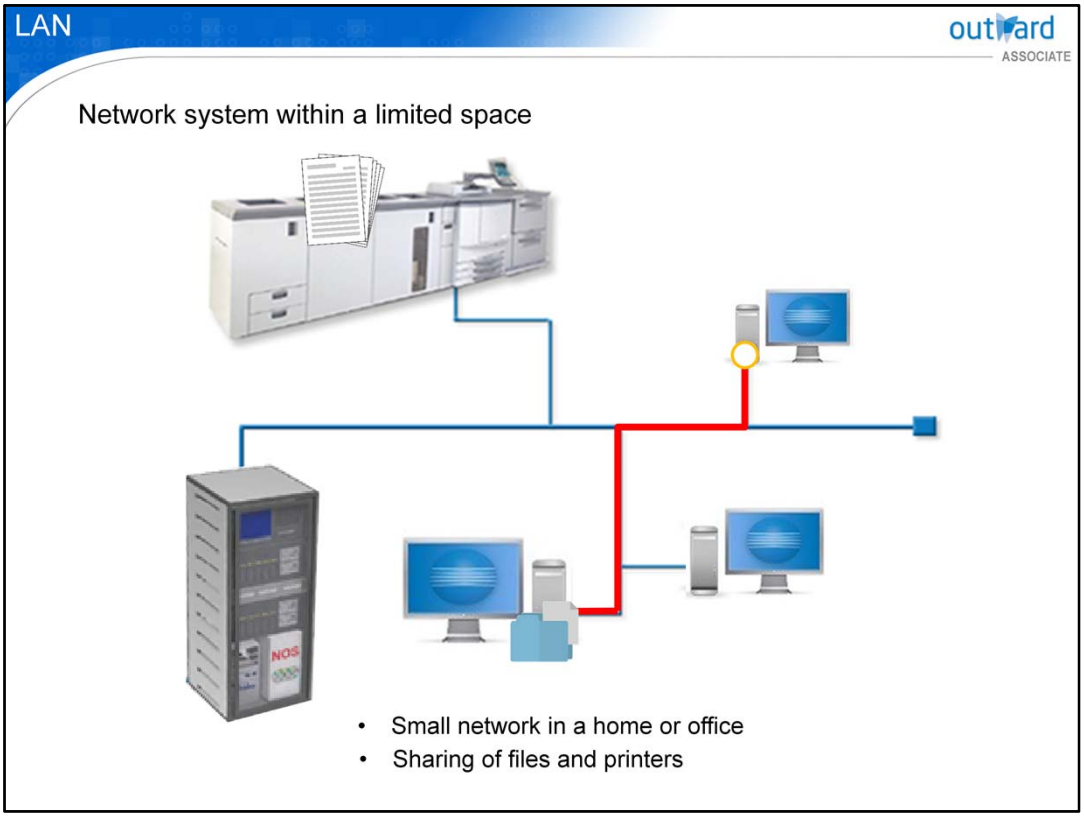


This lesson explains the technology used for network connections.



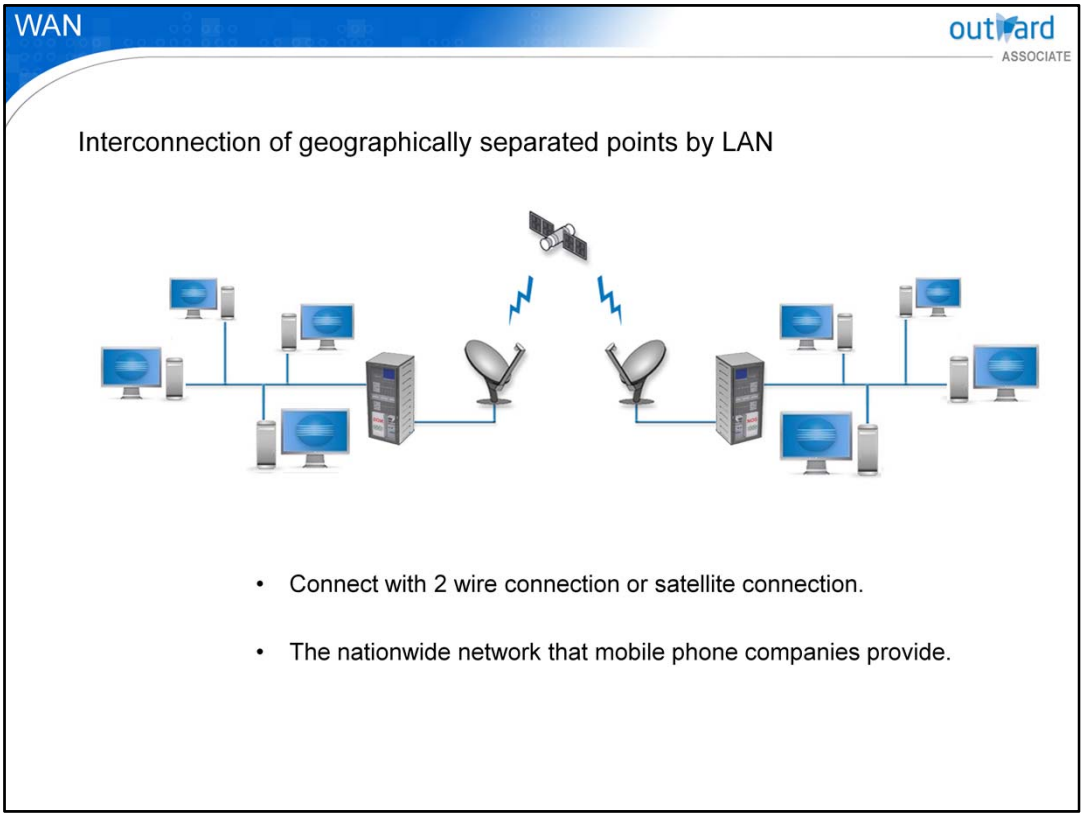
Networks are generally grouped into three categories based on their size: LAN, MAN and WAN.
A LAN is a group of two or more workstations that share a common communications line in a small, defined area such as a home, office or building.
A LAN has the flexibility to connect as few as two workstations in a home or over a thousand workstations in a company's office.
A WAN connects computers that are geographically remote each other to form a broader network, and interactively connect LANs and other WANs.
This enables the creation of remote offices by connecting the head office with the LANs of branch offices.
A 2-wire connection or satellite connection are used to connect services, usually provided by telecommunications carriers.
A MAN is a network positioned somewhere between these networks, and is a network system for interconnecting LANs on a city level.

Сети, как правило, сгруппированы в три категории в зависимости от их размера: LAN, MAN и WAN.
Локальная сеть (LAN) - это группа из двух или более рабочих станций, которые совместно используют общую линию связи в небольшой определенной области, такой как дом, офис или здание.
ЛВС позволяет подключать всего две рабочие станции в доме или более тысячи рабочих станций в офисе компании.
WAN соединяет компьютеры, которые географически удалены друг от друга, чтобы сформировать более широкую сеть, и интерактивно соединяет LAN и другие WAN.
Это позволяет создавать удаленные офисы, соединяя головной офис с локальными сетями филиалов.
Двухпроводное или спутниковое соединение используется для подключения услуг, обычно предоставляемых операторами связи.
MAN - это сеть, расположенная где-то между этими сетями, и сетевая система для соединения локальных сетей на уровне города.



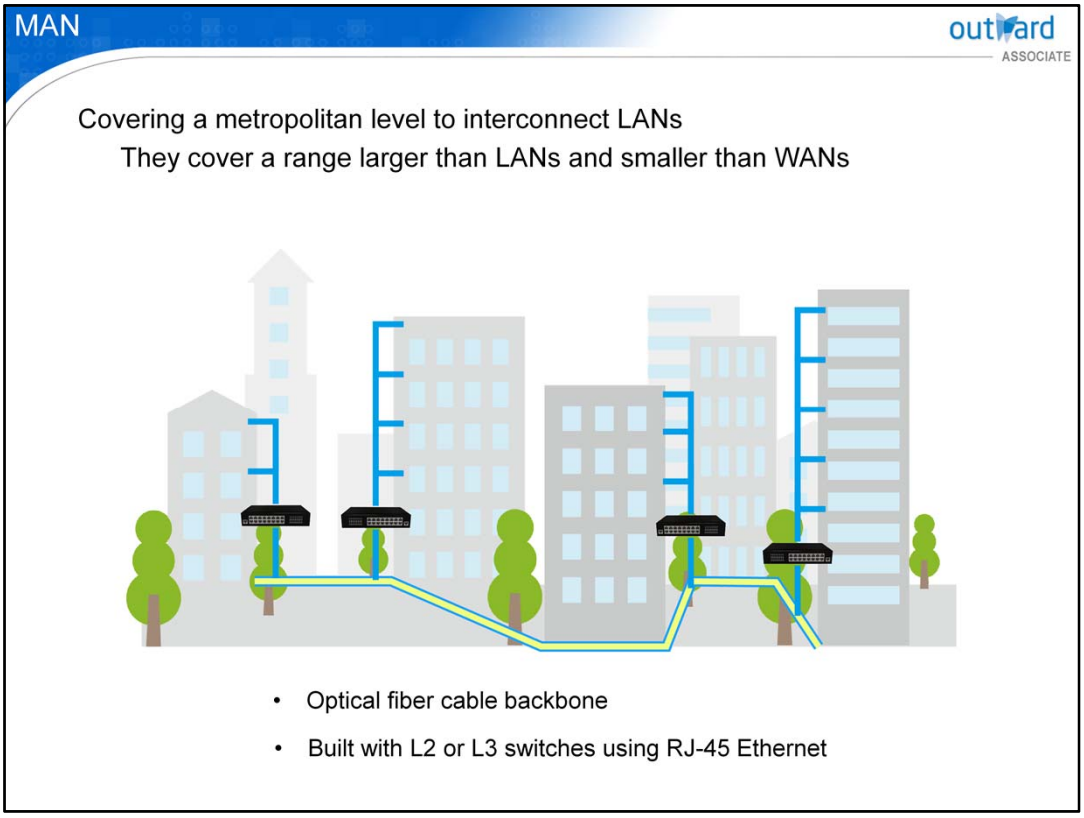
LANs have become extremely popular because of their various applications for business and personal use due to their flexibility.
A LAN can be used to share files, hardware resources and other network resources such as printers or mail servers. There are many different approaches to setting up a LAN, but the principal types you are likely to encounter are explained in 2.2 Topology and Lesson 3: Protocols.

Локальные сети стали чрезвычайно популярными из-за их различных приложений для бизнеса и личного использования благодаря их гибкости.
Локальная сеть может использоваться для обмена файлами, аппаратными ресурсами и другими сетевыми ресурсами, такими как принтеры или почтовые серверы. Существует много разных подходов к настройке ЛВС, но основные типы, с которыми вы, вероятно, столкнетесь, описаны в 2.2 Топология и Урок 3: Протоколы.



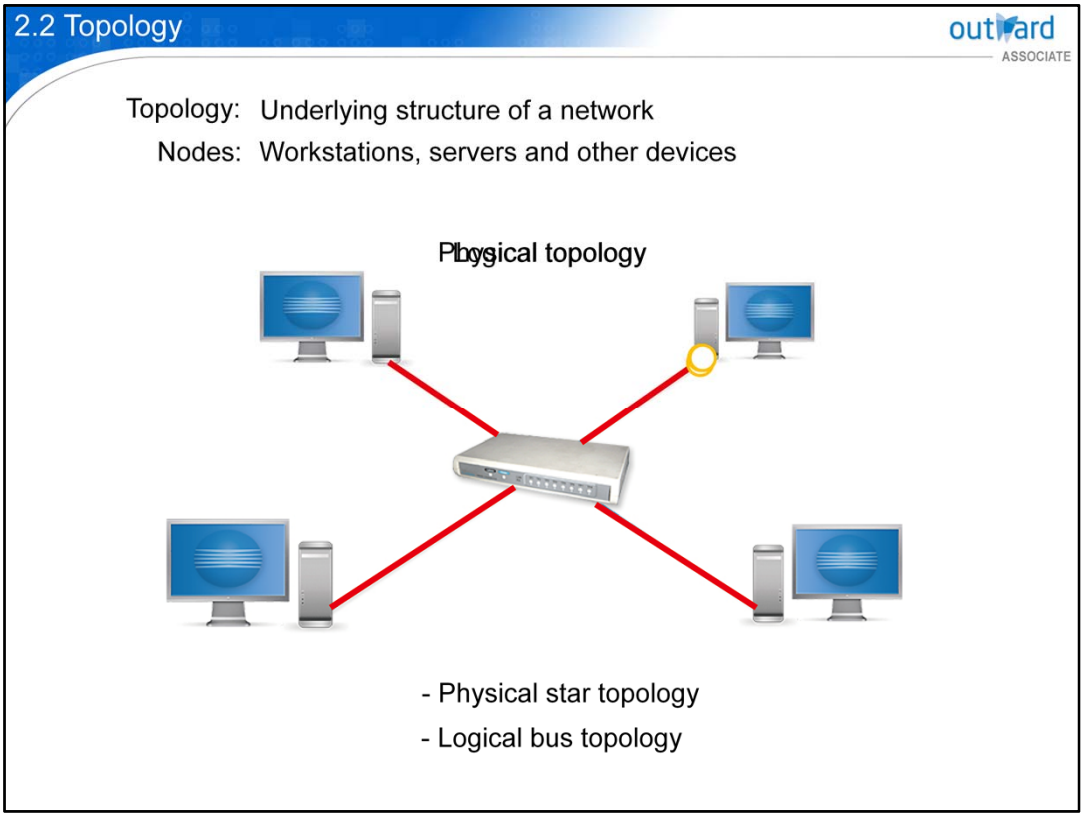
A WAN joins together LANs and other WANs to form a broader network covering large and often remote areas. WANs often use a 2 wire connection or satellite connection to link together smaller, more localized networks.
The network that mobile phone companies provide nationwide can be said to be a WAN.

WAN объединяет локальные и другие глобальные сети для формирования более широкой сети, охватывающей большие и более удаленные районы.
В глобальных сетях часто используется двухпроводное или спутниковое соединение чтобы связать вместе меньшие, более локализованные сети.
Сеть, которую предоставляют компании мобильной связи по всей стране можно сказать, что WAN.



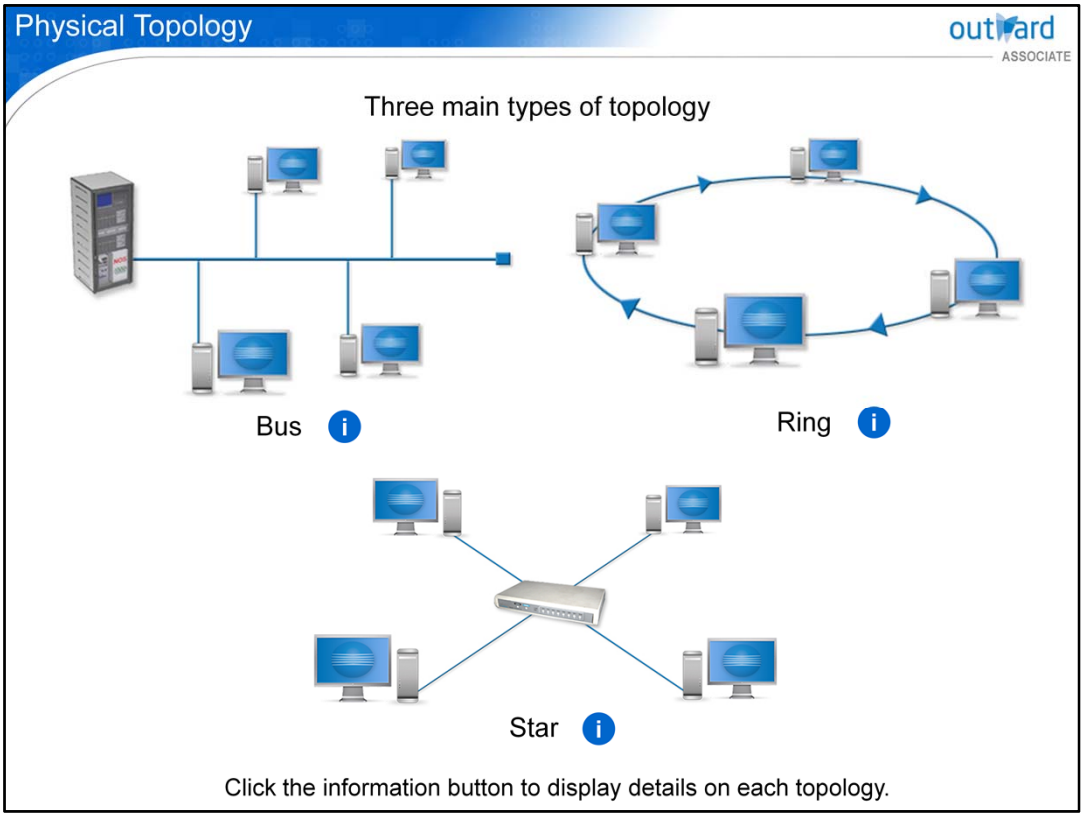
MANs refer the networks that are larger than LANs and smaller than WANs. However, there is no definite boundary that can be used for classification. This network is also used as a campus network nowadays.
Applications include use in the entire area of a single university, the entire area of a single company and the entire area of a single city.
Optical fiber cable is used for the backbone and is constructed with L2 or L3 switches using RJ-45 Ethernet. L2 switches work as a hub which has a bridge function. L3 switches specify the route of data.

MAN - это сети, которые больше, чем LAN, и меньше, чем WAN.
Тем не менее, нет определенной границы, которая может быть использована для классификации. Эта сеть также используется в качестве сети кампуса в настоящее время.
Приложения включают использование на всей территории одного университета, на всей территории одной компании и на всей территории одного города.
Оптоволоконный кабель используется для магистрали и состоит из коммутаторов L2 или L3 с использованием RJ-45 Ethernet. Коммутаторы L2 работают как концентратор, который имеет функцию моста. Коммутаторы L3 определяют маршрут данных.



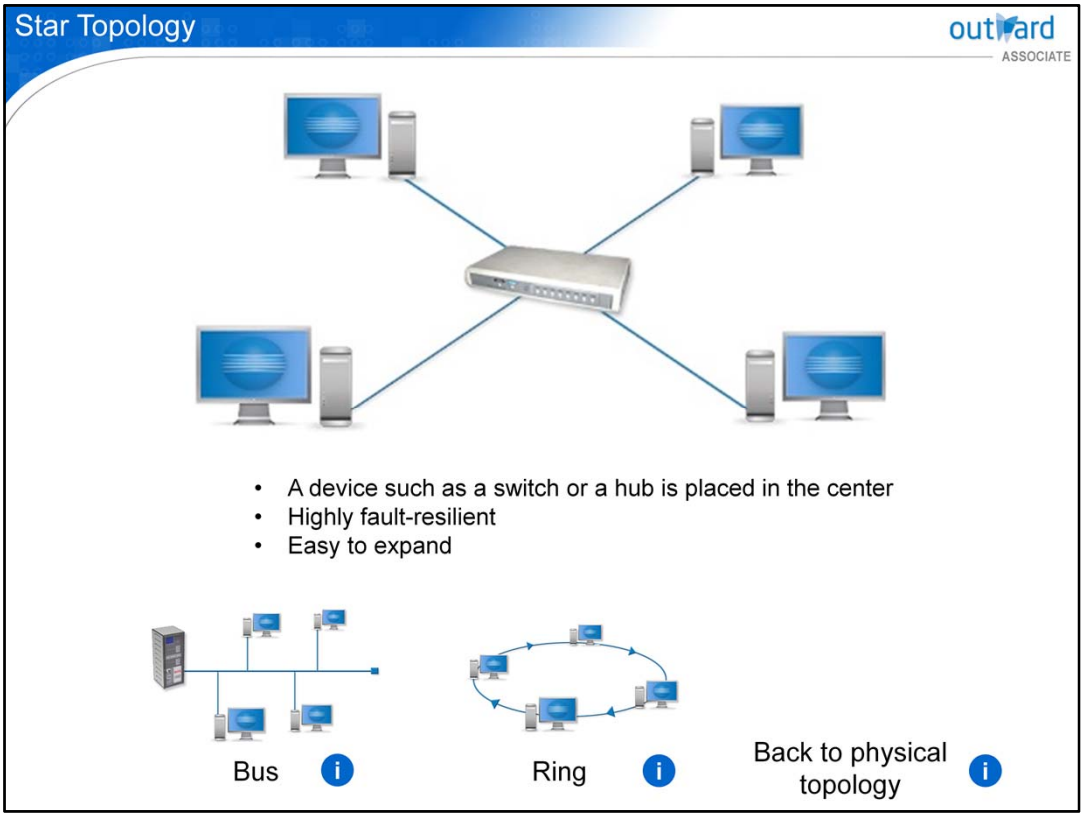
Topology is the underlying structure of a network.
Physical topology refers to how a network is physically connected, and logical topology refers to how data is transmitted around the network.
A network's physical topology may be of one kind, and its logical topology of another kind. For example, a network with a physical star topology may have a logical bus topology. In topology, the workstations, servers and other devices forming the network are called nodes.

Топология является базовой структурой сети.
Физическая топология определяет, как физически связана сеть, а логическая топология опеределяет, как данные передаются по сети.
Физическая топология сети может быть одного типа, а ее логическая топология - другим. Например, сеть с физической топологией звезда может иметь топологию логической шины. В топологии рабочие станции, серверы и другие устройства, образующие сеть, называются узлами.



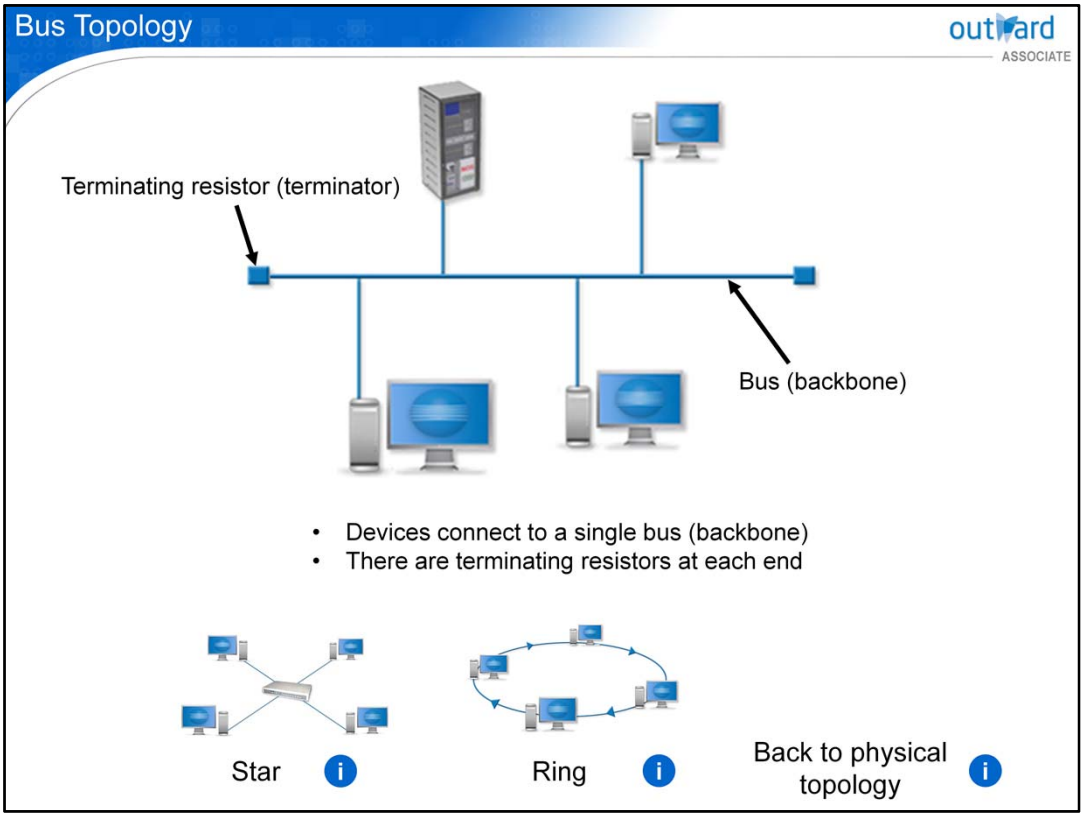
The physical topology refers to the way networks are physically interconnected at the hardware level.
This affects how robust the network is and determines how it reacts if, for example, a workstation fails.
Three typical topologies are the star, bus and ring types. These are not always used alone and there are also hybrid topologies and mixed topologies that combine several network structures.
A WAN is a very common example of a hybrid network because it is connected to a combination of different types of networks.
Click the information button to display details on each topology.

Физическая топология определяет, как сети физически взаимосвязаны на аппаратном уровне.
Это влияет на надежность сети и определяет, как она реагирует, например, на сбой рабочей станции.
Три типичные топологии - это звезды, шины и кольца. Они не всегда используются отдельно, а также существуют гибридные топологии и смешанные топологии, которые объединяют несколько сетевых структур.
WAN является очень распространенным примером гибридной сети, потому что он связан с комбинацией различных типов сетей.
Нажмите кнопку информации, чтобы отобразить детали по каждой топологии.



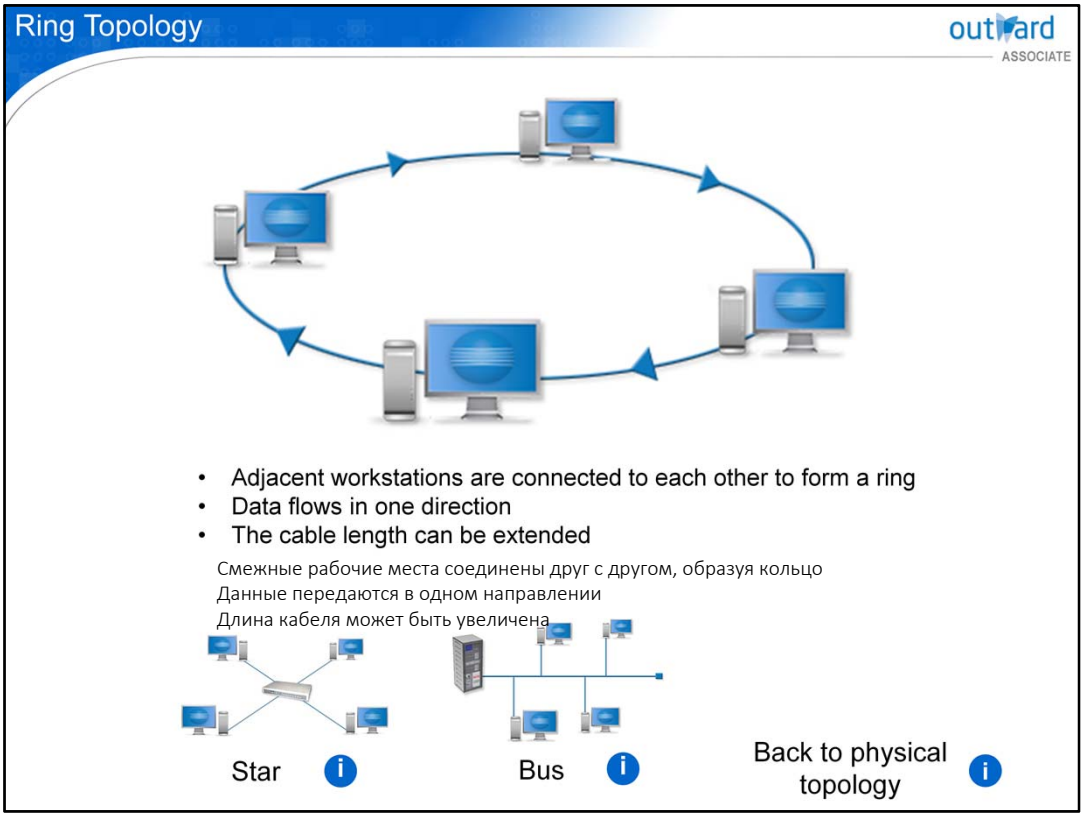
In a star topology, workstations are connected together via a central distribution point. In most LANs a specific device, called a network switch, serves as the central distribution point.
Physical star topologies allow the network to be more robust against cabling failures or workstations going offline.
Also, it is easier to extend a star network than other topologies. Because of these factors, most networks run with physical star topologies.
The drawback is that the entire network is affected when the central switch or hub fails.

В топологии «звезда» рабочие станции соединены вместе через центральную точку распространения.
В большинстве локальных сетей конкретное устройство, называемое сетевым коммутатором, служит центральной точкой распространения.
Физические звездные топологии позволяют сети быть более устойчивой к отказам кабельной системы или отключению рабочих станций.
Кроме того, расширить звездную сеть проще, чем другие топологии. Из-за этих факторов большинство сетей работают с физическими звездными топологиями.
Недостаток заключается в том, что вся сеть подвержена влиянию сбоя центрального коммутатора или концентратора.



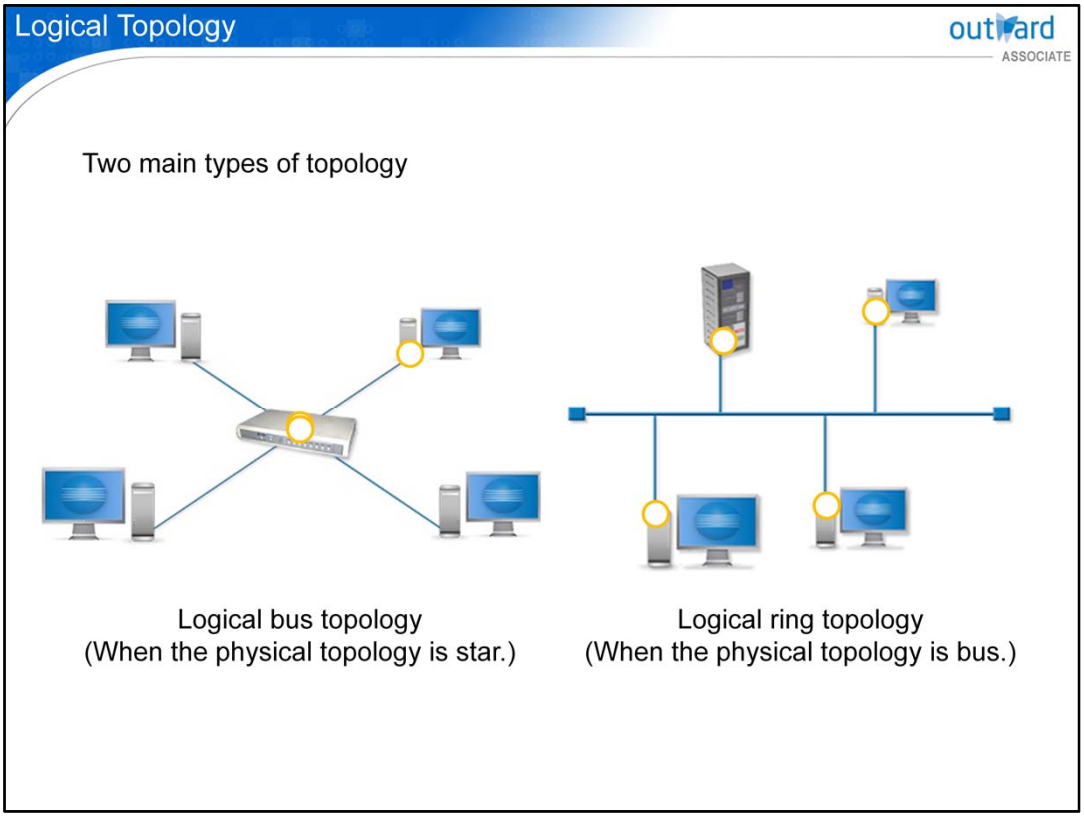
A physical bus topology is a system in which devices are connected to a single cable called a bus or backbone.
The backbone is usually terminated by a special device called a terminator. Terminators are necessary to prevent signals bouncing back into the bus after they have reached either end of the bus. When a bus fails, all communication on the network is lost. The physical bus topology is now hardly used in general networks.

Топология физической шины - это система, в которой устройства подключены к одному кабелю, который называется шиной или магистралью.
Магистраль обычно заканчивается специальным устройством, называемым терминатором.
Терминаторы необходимы для предотвращения отскока сигналов обратно в шину после того, как они достигли любого конца шины. При сбое шины вся связь в сети теряется. Топология физической шины в настоящее время практически не используется в общих сетях.



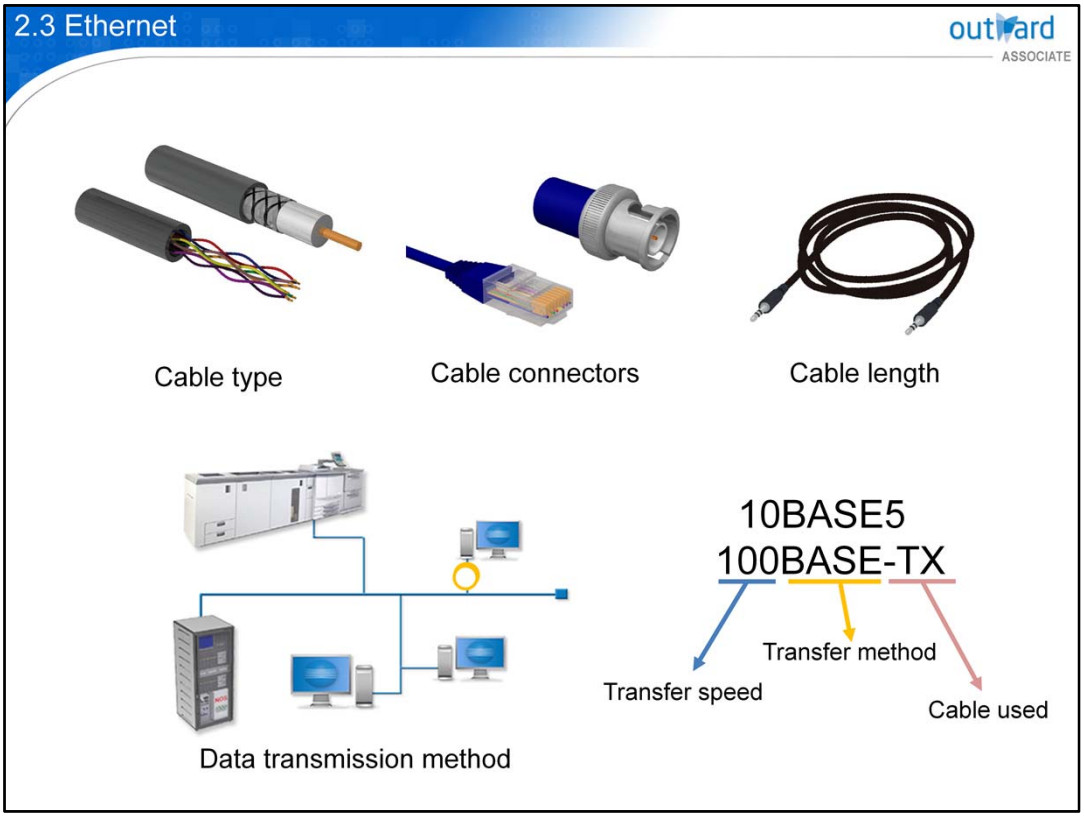
In a physical ring topology, each workstation is connected to two other workstations.
A workstation can only receive data packets from one direction and pass it on in the other direction.
A ring topology allows each workstation to boost the signal, thus increasing normal cable distance restrictions.
The drawback is that when any of workstations fail, all communication is lost. The physical ring topology is now hardly used in general networks.

В топологии физического кольца каждая рабочая станция подключена к двум другим рабочим станциям.
Рабочая станция может принимать пакеты данных только из одного направления и передавать их в другом направлении.
Кольцевая топология позволяет каждой рабочей станции усиливать сигнал, тем самым увеличивая обычные ограничения на расстояние между кабелями.
Недостатком является то, что при сбое любой из рабочих станций вся связь теряется. Топология физического кольца в настоящее время практически не используется в общих сетях.



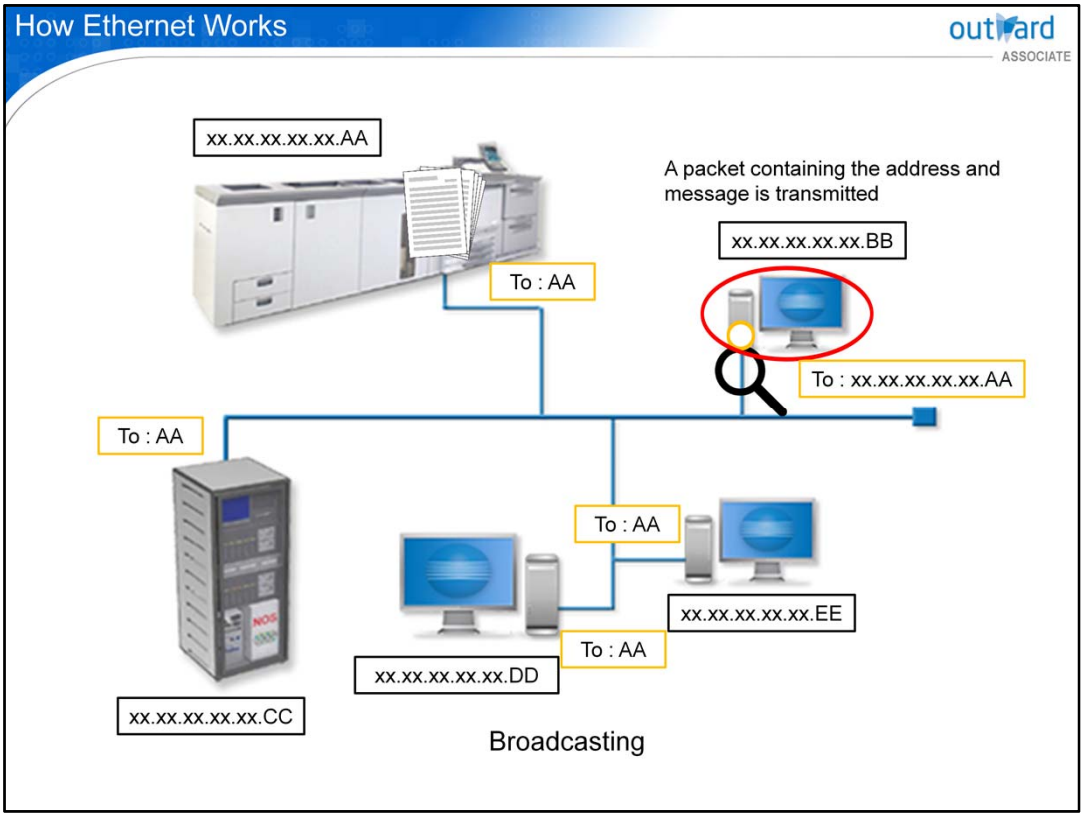
The logical topology determines how workstations communicate with each other and is defined on a software or functional level.
The two dominant configurations are bus and ring.
A logical bus topology can operate in either a bus or star physical configuration, and messages are simultaneously sent to all workstations.
Modern networks use network switches that only route packets to the recipient workstations. This improved behavior, however, does not affect the logical bus topology.
In a logical ring topology, packets are transmitted sequentially around the network in a given order.
Physical ring topologies suffer the disadvantage that every node is essential to the network functioning well.
Failure of any node results in the failure of the network.

Логическая топология определяет, как рабочие станции взаимодействуют друг с другом, и определяется на программном или функциональном уровне.
Две доминирующие конфигурации - шина и кольцо.
Топология логической шины может работать в физической конфигурации шины или звезды, и сообщения одновременно отправляются на все рабочие станции.
Современные сети используют сетевые коммутаторы, которые направляют пакеты только на рабочие станции-получатели.
Это улучшенное поведение, однако, не влияет на топологию логической шины.
В топологии логического кольца пакеты передаются последовательно по сети в заданном порядке.
Физические кольцевые топологии страдают тем недостатком, что каждый узел необходим для нормальной работы сети.
Отказ любого узла приводит к отказу сети.



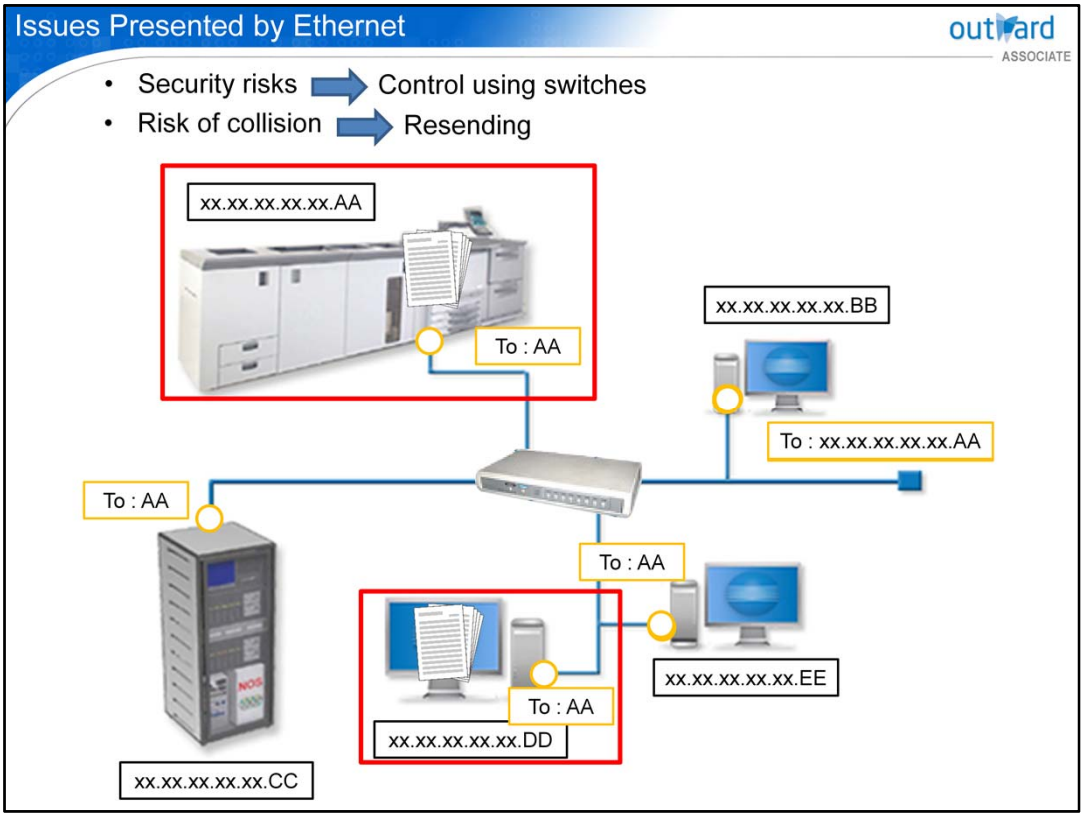
Ethernet is a standardized way of connecting computers to create a network.
It specifies what kind of cables to use, how to connect the cables together, how long cables can be, how computers transmit data to one another using these cables and more. It also specifies the maximum transfer speed.
Because there are rules for the naming of standards, a certain amount of information can be obtained from the name.

Ethernet - это стандартизированный способ соединения компьютеров для создания сети.
В нем указывается, какие кабели использовать, как их соединять, какова длина кабелей, как компьютеры передают данные друг другу с помощью этих кабелей и т. д. Также указывается максимальная скорость передачи.
Поскольку существуют правила именования стандартов, определенное количество информации может быть получено из названия.



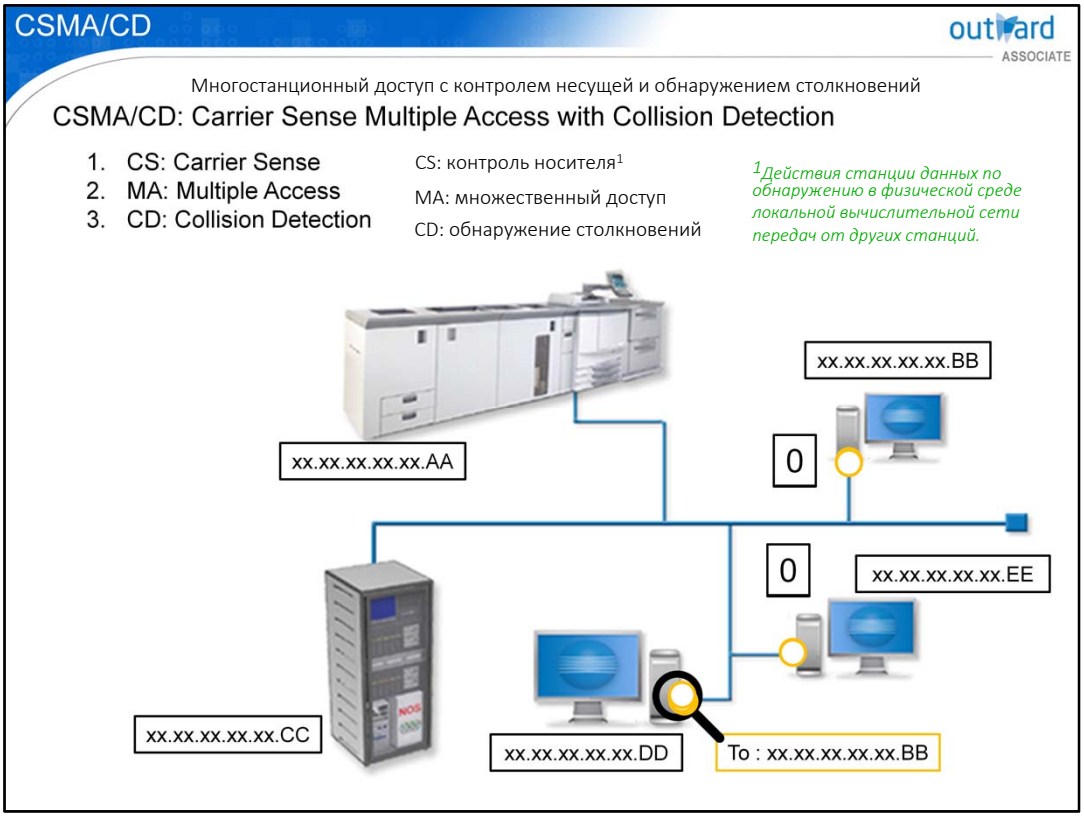
Ethernet works on the following principle.
If a workstation has a message to send, it first checks to see if the line is free.
If the line is busy, the transmitter waits for a random period of time and then tries sending the message again.
It then transmits a data packet containing the address and message information onto the network.
Each workstation receives the message simultaneously. The workstation whose network address matches that attached to the message accepts the message, while all other workstations simply disregard it. This method is called the broadcasting.

Ethernet работает по следующему принципу.
Если на рабочей станции есть сообщение для отправки, она сначала проверяет, свободна ли линия.
Если линия занята, передатчик ожидает случайный период времени и затем пытается отправить сообщение снова.
Затем он передает пакет данных, содержащий адрес и информацию сообщения, в сеть.
Каждая рабочая станция получает сообщение одновременно. Рабочая станция, сетевой адрес которой совпадает с адресом, прикрепленным к сообщению, принимает сообщение, в то время как все остальные рабочие станции просто игнорируют его. Этот метод называется вещанием



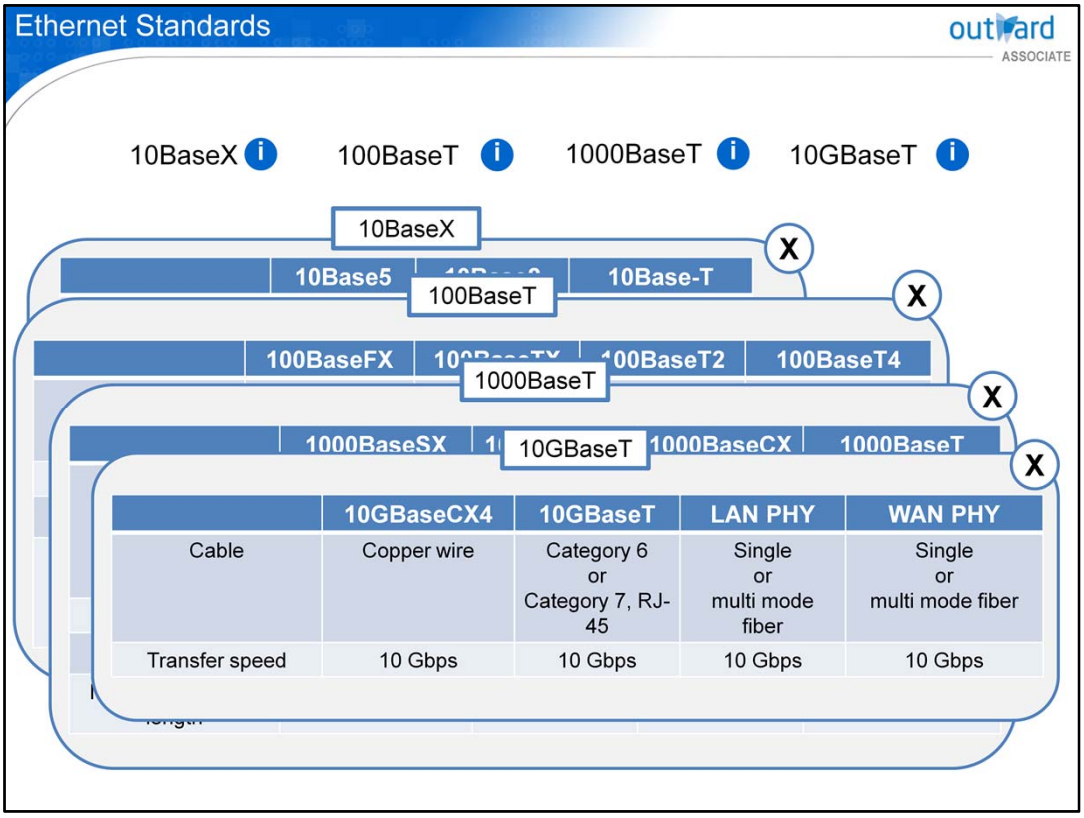
Broadcasting presents a security risk, as every workstation potentially has access to every message sent over the network.
Data collision is also a risk with Ethernet systems, as two workstations may start to transmit messages simultaneously. When a collision occurs, the data is broken and cannot be read. This problem is dealt with in Ethernet systems by reattempting the transmission of the data that was affected by the collision.
In modern LANs where Fast Ethernet is used, it is typical to deploy switches rather than hubs for interconnecting devices to one another.
Switches are more intelligent than hubs and only transmit data to the computer it is destined for, therefore alleviating security issues, as not every workstation on the network is able to receive all transmitted data.

Вещание представляет угрозу безопасности, поскольку каждая рабочая станция потенциально имеет доступ к каждому сообщению, отправляемому по сети.
Столкновение данных также представляет опасность для систем Ethernet, поскольку две рабочие станции могут начать передавать сообщения одновременно. Когда происходит столкновение, данные нарушаются и не могут быть прочитаны.
Эта проблема решается в системах Ethernet путем повторной попытки передачи данных, на которые повлияло столкновение.
В современных локальных сетях, где используется Fast Ethernet, обычно используются коммутаторы, а не концентраторы для соединения устройств друг с другом.
Коммутаторы более интеллектуальны, чем концентраторы, и передают данные только на тот компьютер, для которого они предназначены, что устраняет проблемы безопасности, поскольку не каждая рабочая станция в сети может принимать все передаваемые данные.



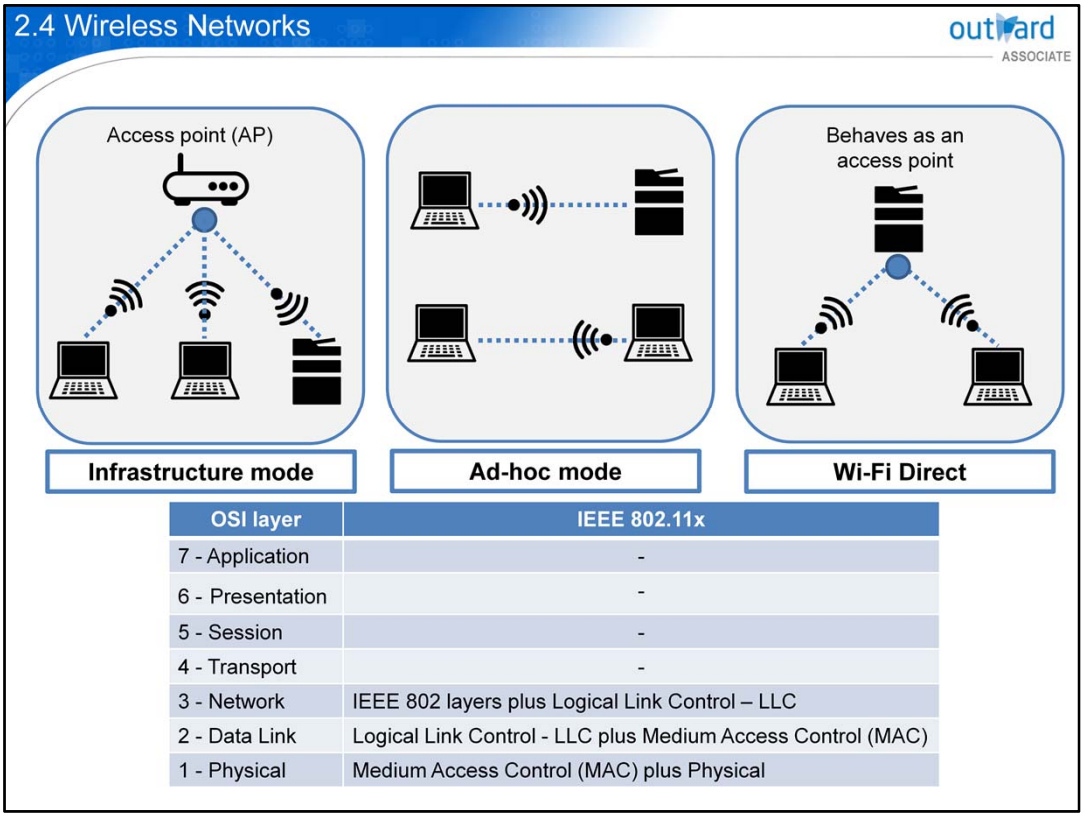
CSMA/CD provides instructions on how to send data and how to deal with collisions.
The following procedure is used when sending data.
1. Carrier Sense is a process for confirming that another node is not transmitting before commencing transmission. Data is sent if no other nodes are transmitting, and data is sent after waiting for a random period of time if another node is transmitting.
2. Multiple Access means that multiple nodes share the same line and multiple pieces of data can be present on the same line at once.
Each node compares its own address data with the destination address, and only reads data addressed to itself, while discarding all other data.
3. Collision Detection destroys data if a collision occurs within a cable when multiple nodes are transmitting at the same time. Because abnormal signal patterns and voltage levels occur when data collides, each node detects collisions based on these.
Transmission is promptly terminated when a collision is detected, and transmission of data is resumed after waiting for a random period of time.

CSMA / CD содержит инструкции о том, как отправлять данные и как справляться с коллизиями.
Следующая процедура используется при отправке данных.
1. Carrier Sense - это процесс подтверждения того, что другой узел не осуществляет передачу до начала передачи.
Данные отправляются, если никакие другие узлы не передают, и данные отправляются после ожидания в течение случайного периода времени, если другой узел передает.
2. Множественный доступ означает, что несколько узлов совместно используют одну и ту же строку, и несколько фрагментов данных могут присутствовать в одной строке одновременно.
Каждый узел сравнивает свои собственные адресные данные с адресом назначения и считывает только данные, адресованные самому себе, при этом отбрасывая все остальные данные.
3. Обнаружение столкновения уничтожает данные, если в кабеле происходит столкновение, когда несколько узлов осуществляют передачу одновременно. Поскольку аномальные шаблоны сигналов и уровни напряжения возникают при столкновении данных, каждый узел обнаруживает коллизии на их основе.
Передача незамедлительно прекращается при обнаружении коллизии, а передача данных возобновляется после ожидания в течение случайного периода времени.



There are a number of Ethernet network variants. Each standard is defined by factors such as the cable type, transfer speed and number of nodes.
10Base5 was standardized by IEEE in 1983, and became the first Ethernet standard to become popular in the private sector.
10Base5, 10Base2 and 10Base-T were standardized, in that order. A bus topology using a co-axial cable was used until 10Base2.
A star topology using a Unshielded twisted pair cable, or UTP cable for short, and a hub similar to the modern configuration has been used since 10Base-T. Since then, 100BaseT, known as Fast Ethernet, has become standards, enabling transfers at 100 Mbps, as has Gigabit Ethernet, enabling transfers at 1Gbps. Now, 1000BaseT is the most widely used standard in general environments.
There are also standards for 10Gbps or more, but they are currently only used in certain data centers and have not become widespread.
Click the information button to display details on each standard.

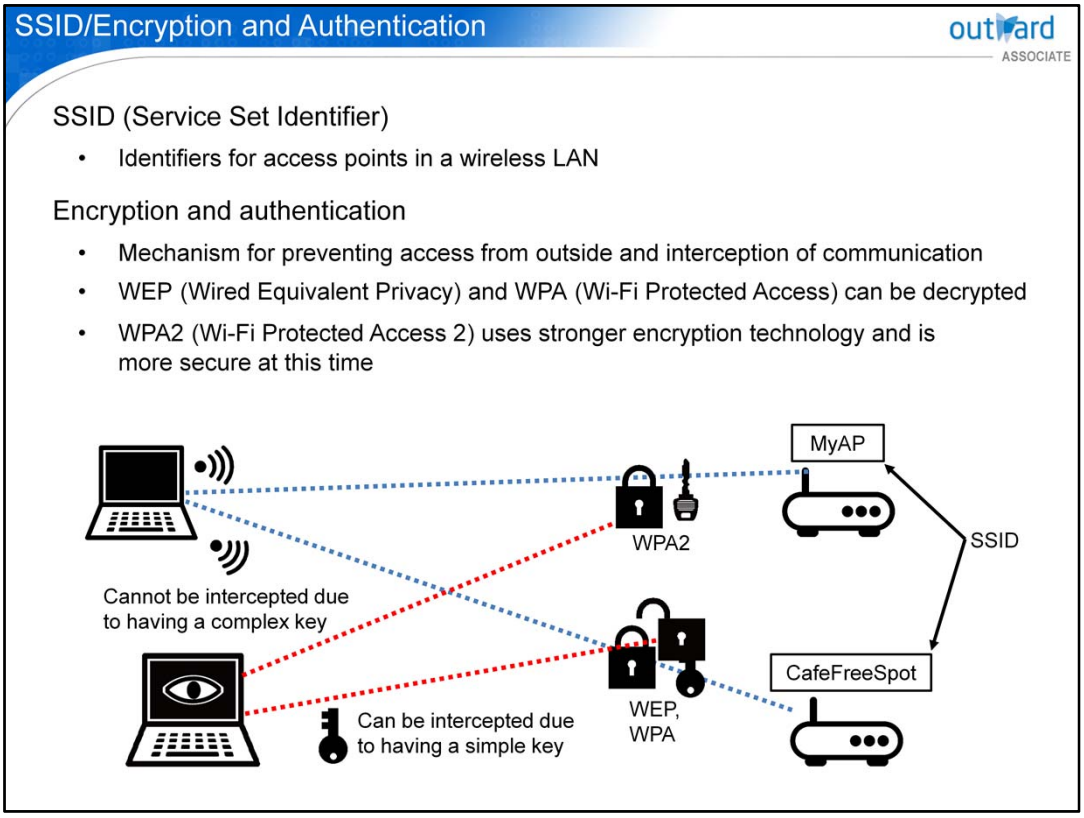
Существует несколько вариантов сети Ethernet. Каждый стандарт определяется такими факторами, как тип кабеля, скорость передачи и количество узлов.
10Base5 был стандартизирован IEEE в 1983 году и стал первым стандартом Ethernet, ставшим популярным в частном секторе.
10Base5, 10Base2 и 10Base-T были стандартизированы в этом порядке. Топология шины с использованием коаксиального кабеля использовалась до 10Base2.
Топология «звезда» с использованием неэкранированной витой пары или кабеля UTP для краткости, а также концентратор, аналогичный современной конфигурации, используется с 10Base-T. С тех пор 100BaseT, известный как Fast Ethernet, стал стандартом, обеспечивающим передачу данных со скоростью 100 Мбит / с, так же как и Gigabit Ethernet, обеспечивая передачу данных со скоростью 1 Гбит / с.
В настоящее время 1000BaseT является наиболее широко используемым стандартом в обычных условиях.
Существуют также стандарты для 10 Гбит / с и более, но в настоящее время они используются только в определенных центрах обработки данных и не получили широкого распространения. Нажмите кнопку информации, чтобы отобразить детали по каждому стандарту.



OSI layer	IEEE 802.11x
7 - Application	-
6 - Presentation	-
5 - Session	-
4 - Transport	-
3 - Network	IEEE 802 layers plus Logical Link Control – LLC
2 - Data Link	Logical Link Control - LLC plus Medium Access Control (MAC)
1 - Physical	Medium Access Control (MAC) plus Physical

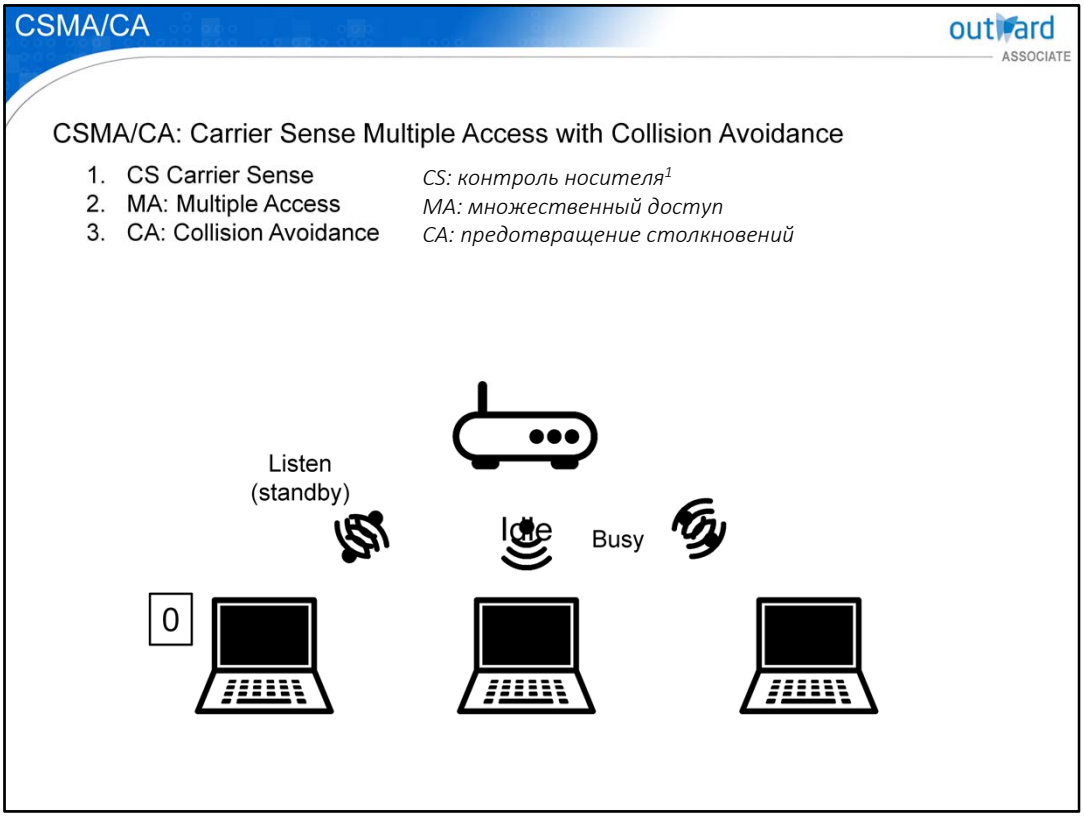
A wireless network uses radio waves to create a LAN without cables.
There are several ways to connect, and infrastructure mode is the wireless LAN format most widely used now.
It is a star network where communication is carried out through an access point without direct connections between clients.
Ad-hoc mode provides direct peer-to-peer communication between clients.
It enables direct exchanges of data and printing on printers without an access point, but the configuration is somewhat complicated.
Wi-Fi Direct uses a software approach in which one device has an Access Point function and behaves as the AP, and the clients directly communicate with each other. Devices negotiate which one will act as the AP on the first connection. It is a direct connection, but configuration of the connection and security can use infrastructure mode because it is seen as a normal access point by clients.
A commonly used wireless network standard is IEEE802.11x, which is defined by the Institute of Electrical and Electronics Engineers, or IEEE.
The OSI reference model described in Lesson 3 and the IEEE standard map to each other as shown in the table.

Беспроводная сеть использует радиоволны для создания ЛВС без кабелей.
Существует несколько способов подключения, и режим инфраструктуры является наиболее распространенным форматом беспроводной локальной сети.
Это звездная сеть, в которой связь осуществляется через точку доступа без прямых соединений между клиентами.
(Ad-hoc) Специальный режим обеспечивает прямую одноранговую связь между клиентами.
Он позволяет осуществлять прямой обмен данными и печать на принтерах без точки доступа, но конфигурация несколько сложна.
Wi-Fi Direct использует программный подход, при котором одно устройство имеет функцию точки доступа и ведет себя как точка доступа, а клиенты напрямую общаются друг с другом. Устройства согласовывают, какой из них будет действовать в качестве точки доступа для первого соединения. Это прямое соединение, но при настройке соединения и безопасности можно использовать режим инфраструктуры, потому что клиенты видят его как обычную точку доступа.
Обычно используемым стандартом беспроводной сети является IEEE802.11x, который определен Институтом инженеров по электротехнике и электронике или IEEE.
Эталонная модель OSI, описанная в уроке 3, и стандарт IEEE сопоставляются друг с другом, как показано в таблице.



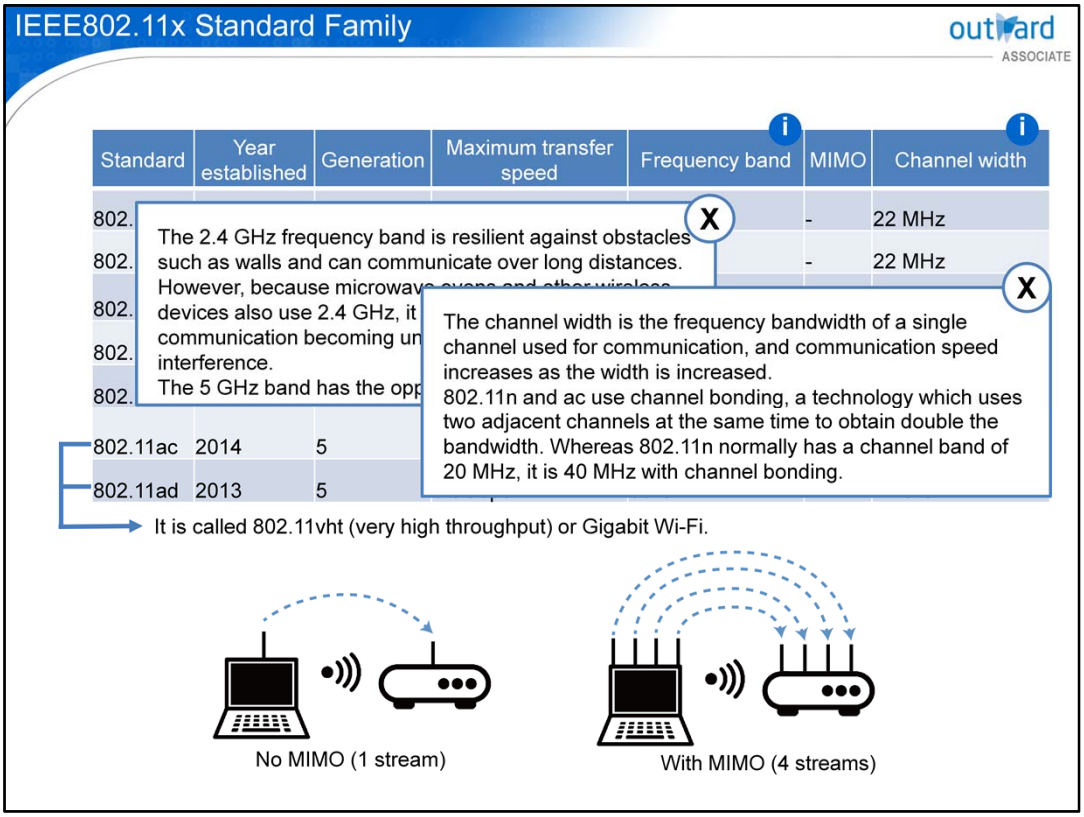
SSIDs are identifiers for access points in a wireless LAN. They can be set for each access point using up to 32 alphanumeric characters.
Access points are identified based on this name when connecting to a wireless LAN.
A wired LAN cannot be joined without connecting a LAN cable, but wireless LAN can be accessed or intercepted from outside within the range of the signal. This problem is prevented by encryption. At present there are three types of encryption: WEP, WPA and WPA2.
However, the use of WEP and WPA is not recommended because the encryption has already been broken.
WPA2 is an improved version of WPA, and is currently the most secure because it uses the more robust Advanced Encryption Standard, or AES for short, for encryption. It can also communicate with devices supporting WPA because it has backward compatibility with WPA.

SSID - это идентификаторы точек доступа в беспроводной локальной сети. Они могут быть установлены для каждой точки доступа, используя до 32 буквенно-цифровых символов.
Точки доступа определяются на основе этого имени при подключении к беспроводной локальной сети.
Проводная ЛВС не может быть подключена без подключения кабеля ЛВС, но беспроводная ЛВС может быть доступна или перехвачена снаружи в пределах диапазона сигнала. Эта проблема предотвращается с помощью шифрования. В настоящее время существует три типа шифрования: WEP, WPA и WPA2.
Однако использование WEP и WPA не рекомендуется, поскольку шифрование уже было нарушено.
WPA2 - это улучшенная версия WPA, и в настоящее время она наиболее безопасна, поскольку для шифрования используется более надежный расширенный стандарт шифрования, или сокращенно AES. Он также может связываться с устройствами, поддерживающими WPA, поскольку он имеет обратную совместимость с WPA.



Ethernet protocols use CSMA/CD. However, wireless networks use CSMA/CA because CSMA/CD cannot be implemented.
Under the control of CSMA/CA, the station needs to listen to the channel during a preset time in order to confirm whether other stations are transmitting.
When there are other activities, the channel is called “busy” and the station continues to listen until the channel becomes “idle”, or free status.
When the channel becomes idle, the station is allowed to transmit finally.
However, an inevitable collision sometimes occurs when the station cannot detect the busy status correctly because of obstructions that are difficult for radio waves to pass through.

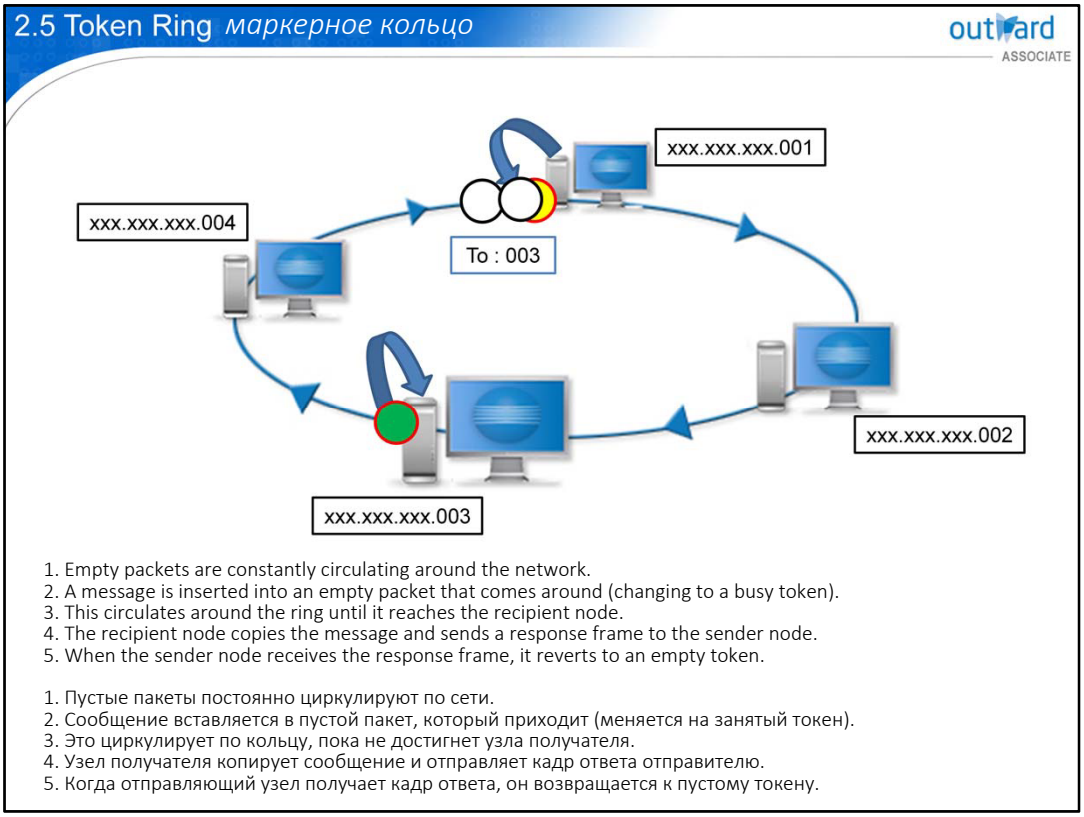
Протоколы Ethernet используют CSMA / CD. Однако беспроводные сети используют CSMA / CA, потому что CSMA / CD не может быть реализован.
Под управлением CSMA / CA станции необходимо прослушивать канал в течение предварительно установленного времени, чтобы подтвердить, что другие станции передают.
Когда есть другие действия, канал называется «занят», и станция продолжает слушать, пока канал не станет «свободным» или свободным статусом.
Когда канал становится свободным, станции разрешается передавать в конце концов.
Однако иногда возникает неизбежное столкновение, когда станция не может правильно определить состояние занятости из-за препятствий, которые трудно пройти радиоволнам.



Ширина канала - это ширина полосы частот одного канала, используемого для связи, и скорость связи увеличивается с увеличением ширины.
802.11n и AC используют связывание каналов, технологию, которая использует два соседних канала одновременно для получения удвоенной полосы пропускания.
В то время как 802.11n обычно имеет полосу канала 20 МГц, она составляет 40 МГц со связыванием каналов.

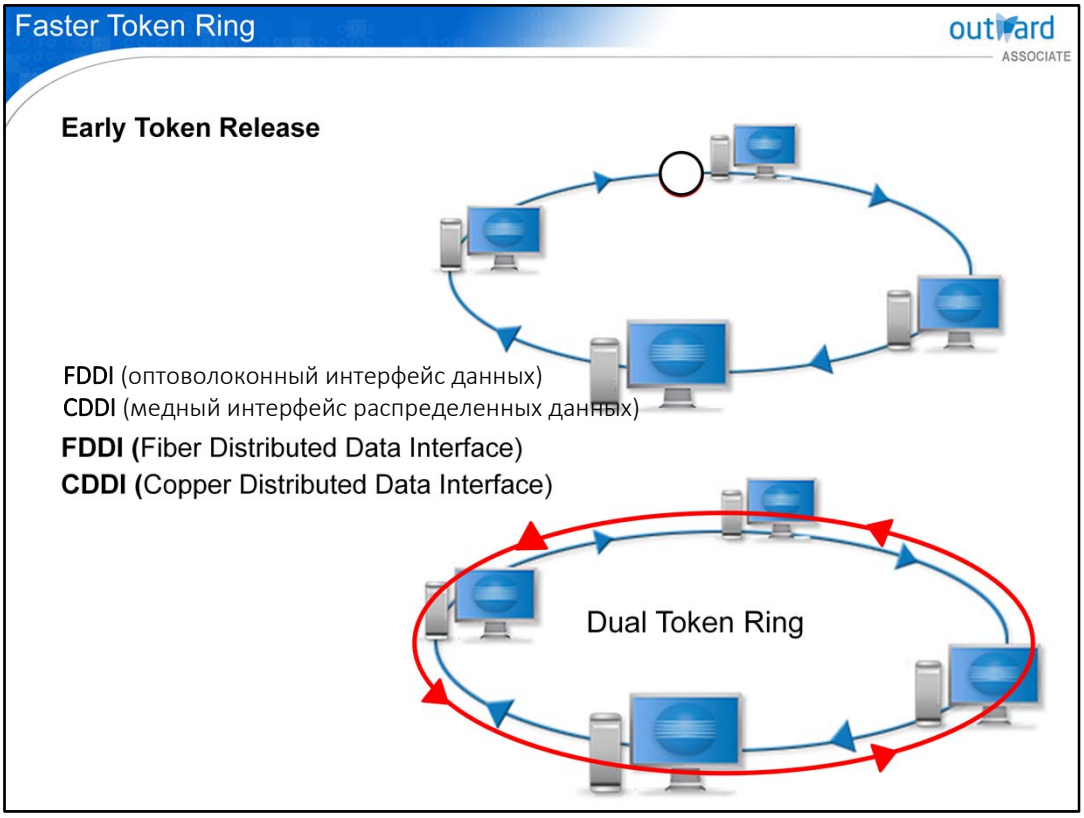
The IEEE802.11x family of standards used now is shown in the table.
MIMO is an acronym for Multiple Input Multiple Output, and has been adopted in 802.11n and ac to significantly increase transfer speeds.
MIMO is a technology that simultaneously transmits and receives using multiple antennas to increase transfer speed. 4x4 refers to having four antennas for transmitting and receiving respectively, and enables communication at approximately four times the speed without MIMO. 802.11ac/ad is a 5th-generation standard enabling extremely high-speed transfers, which is also referred to as 802.11vht or Gigabit Wi-Fi.
802.11ac uses 5 GHz like 802.11a/n and is backwards compatible.
802.11ad uses the extremely high frequency of 60GHz, making it susceptible to obstacles and giving it an extremely short range of around 10 meters. However, because it has a large channel width, high-speed communication is possible without using MIMO.

Используемое в настоящее время семейство стандартов IEEE802.11x показано в таблице.
MIMO является аббревиатурой от множественных входов и множественных выходов, и был принят в 802.11n и ac для значительного увеличения скорости передачи.
MIMO - это технология, которая одновременно передает и принимает с использованием нескольких антенн для увеличения скорости передачи. 4x4 относится к наличию четырех антенн для передачи и приема соответственно, и обеспечивает связь примерно в четыре раза быстрее без MIMO. 802.11ac / ad - это стандарт 5-го поколения, обеспечивающий чрезвычайно высокоскоростную передачу, который также называется 802.11vht или Gigabit Wi-Fi.
802.11ac использует 5 ГГц, как 802.11a / n, и обратно совместим.
802.11ad использует чрезвычайно высокую частоту 60 ГГц, что делает его восприимчивым к препятствиям и дает ему чрезвычайно короткую дистанцию около 10 метров. Однако, поскольку он имеет большую ширину канала, высокоскоростная связь возможна без использования MIMO.



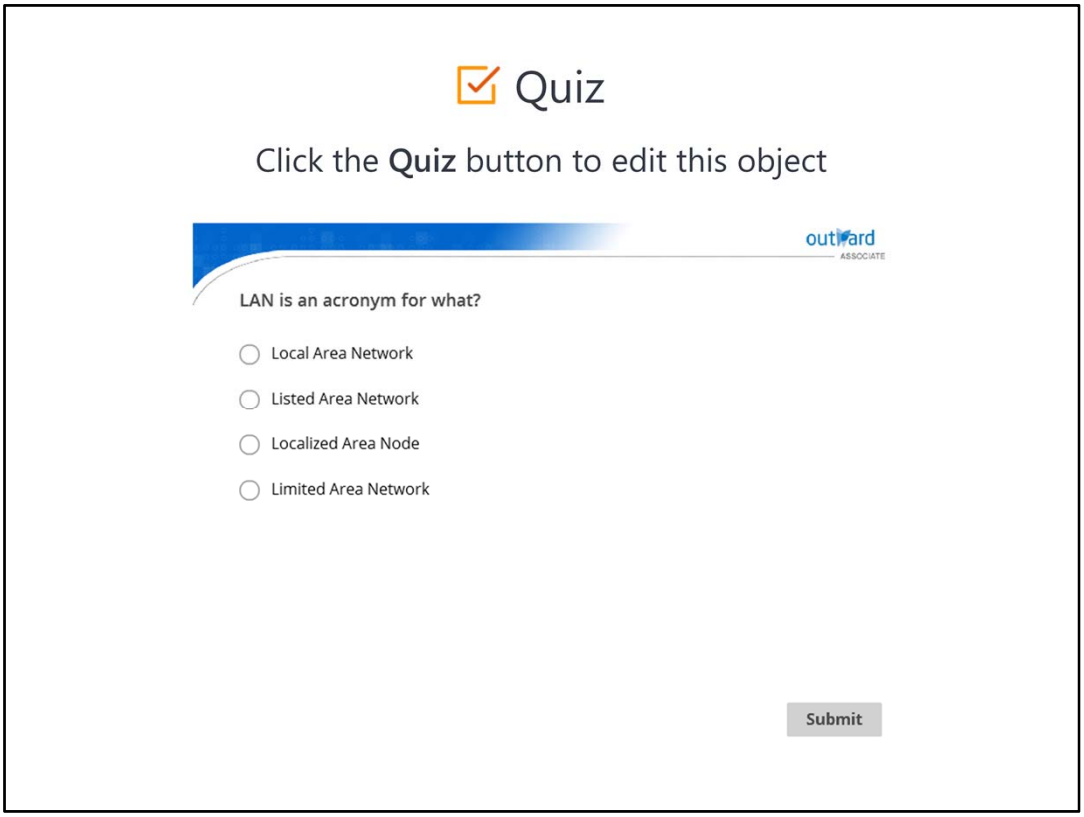
Token ring network technology, developed by IBM, is based on a logical ring topology.
The data collisions experienced on Ethernet systems do not occur in a token ring.
The token ring system works by circulating a token, which is an empty packet, in one direction only.
When a workstation is ready to send a message, it has to wait until it receives the token.
This prevents two senders from transmitting simultaneously. The sender copies its message, including the data, address and source, into the empty packet. When data packet is filled, its status is set to “full”.
The full data packet circulates around the ring until it reaches the recipient.
The recipient copies the message and sends a response frame to the sender.
Once acknowledgment of receipt has been delivered, the status of the token is set to “empty” and it continues to circulate, ready to carry another message. As a result, most token ring systems have been replaced by Ethernet.

Технология сети Token Ring, разработанная IBM, основана на топологии логического кольца.
Коллизии данных, возникающие в системах Ethernet, не происходят в Token Ring.
Система Token Ring работает, распространяя токен, который является пустым пакетом, только в одном направлении.
Когда рабочая станция готова отправить сообщение, она должна дождаться получения токена.
Это предотвращает одновременную передачу двух отправителей. Отправитель копирует свое сообщение, включая данные, адрес и источник, в пустой пакет. Когда пакет данных заполнен, его статус устанавливается на «полный».
Полный пакет данных циркулирует по кольцу, пока не достигнет получателя.
Получатель копирует сообщение и отправляет кадр ответа отправителю.
Как только подтверждение о получении получено, статус токена устанавливается на «пустой», и он продолжает циркулировать, готовый передать другое сообщение. В результате большинство систем Token Ring были заменены Ethernet.

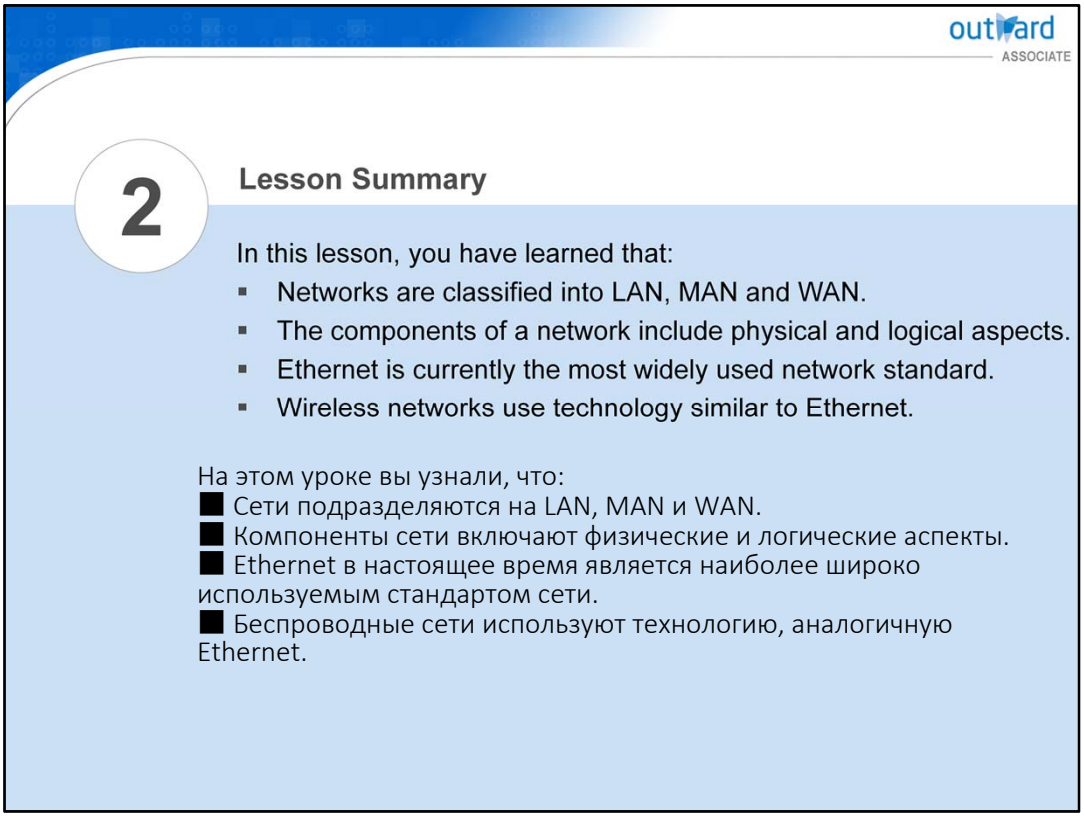


With the early token release method, the node that sent data releases the token after a certain period of time without waiting for arrival confirmation from the receiving node. This mechanism increases speed by circulating multiple tokens and data on the network.
FDDI is a standard for a dual token-ring network using fiberoptic cable to transmit data at up to 100Mbps.
The high speed of FDDI makes it suitable as a link between LANs or in high-performance networks transferring large amounts of data.
By using fiberoptic cable, an FDDI network can cover great distances of up to 60 kilometers between nodes without loss of signal.
The same type of network can run over shielded and unshielded twisted-pair cabling for shorter distances, and is known as CDDI.

При использовании метода раннего освобождения токена узел, отправивший данные, освобождает токен через определенный период времени, не ожидая подтверждения прибытия от принимающего узла. Этот механизм увеличивает скорость за счет распространения нескольких токенов и данных в сети.
FDDI - это стандарт для сети с двойным токен-кольцом, использующей оптоволоконный кабель для передачи данных со скоростью до 100 Мбит / с.
Высокая скорость FDDI делает его пригодным в качестве канала связи между локальными сетями или в высокопроизводительных сетях, передающих большие объемы данных.
При использовании оптоволоконного кабеля сеть FDDI может покрывать большие расстояния до 60 километров между узлами без потери сигнала.
Один и тот же тип сети может работать на экранированной и неэкранированной кабельной витой паре для более коротких расстояний и известен как CDDI.

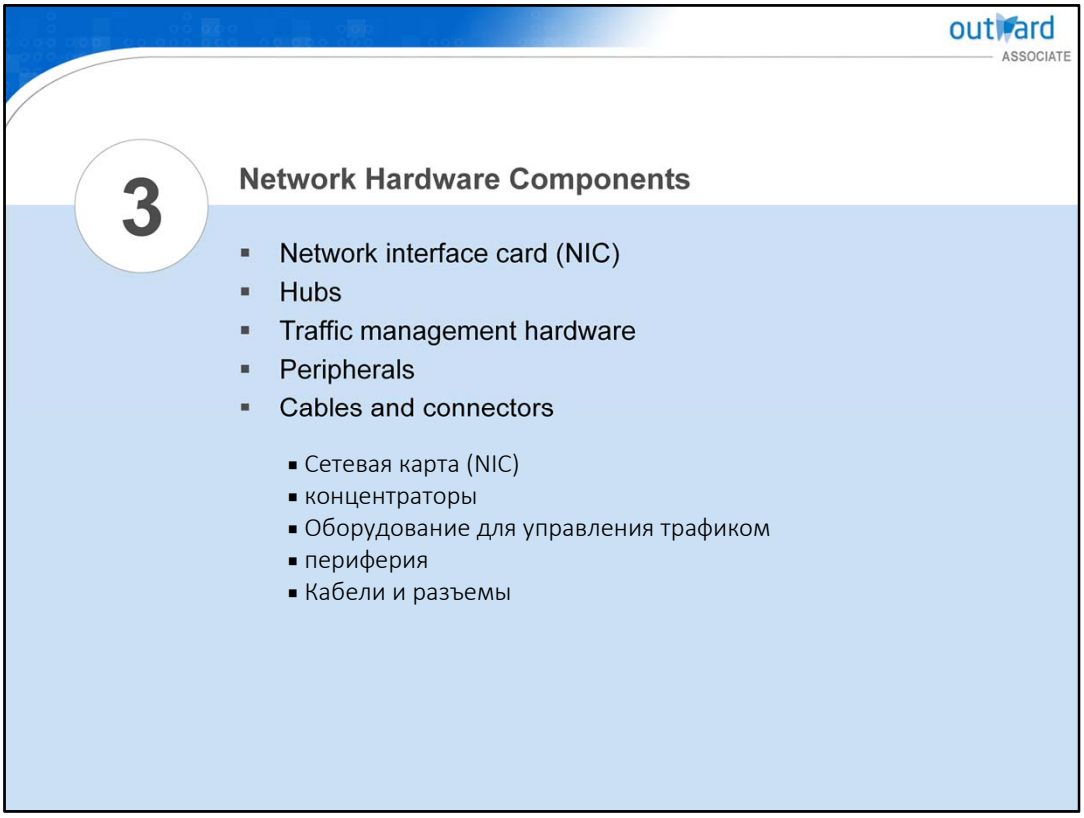


Test your knowledge in a quiz!



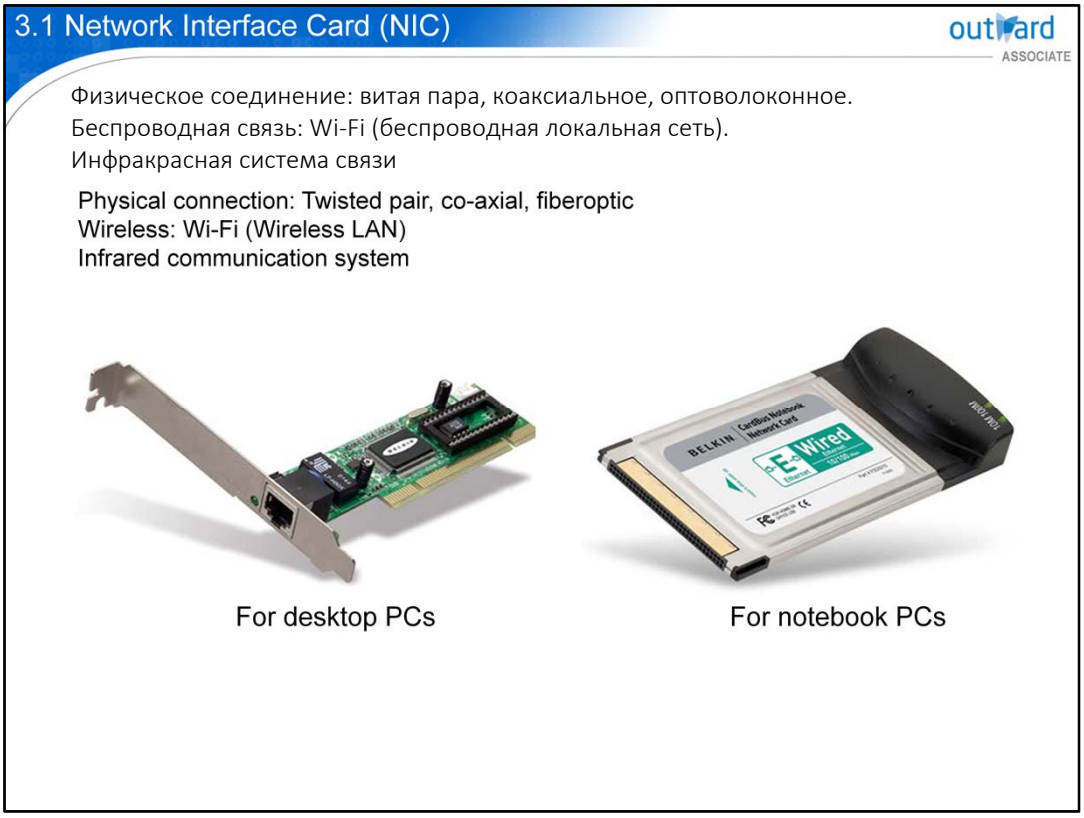
Networks can be classified into LAN, MAN and WAN depending on their size, and the format used for their respective connections differ greatly.
To connect network hardware components, it is necessary to understand both the hardware aspect such as cabling and the logical aspect such as the path data actually follows. Ethernet is currently the most widely used connection standard. Although there are technical issues such as data collisions and security, these have been resolved now, resulting in the standard becoming widespread.
The use of hubs and the mechanism for dealing with collisions are used in current wireless network access points and CSMA/CA, forming the basis for the latest systems.

Сети могут быть классифицированы на LAN, MAN и WAN в зависимости от их размера, и формат, используемый для их соответствующих соединений, сильно различается.
Чтобы подключить сетевые аппаратные компоненты, необходимо понимать как аппаратный аспект, такой как кабели, так и логический аспект, такой как данные пути фактически следуют. В настоящее время Ethernet является наиболее широко используемым стандартом подключения. Хотя существуют технические проблемы, такие как коллизии данных и безопасность, они уже решены, в результате чего стандарт становится широко распространенным.
Использование концентраторов и механизма для устранения коллизий используются в современных точках доступа беспроводной сети и CSMA / CA, образуя основу для новейших систем.



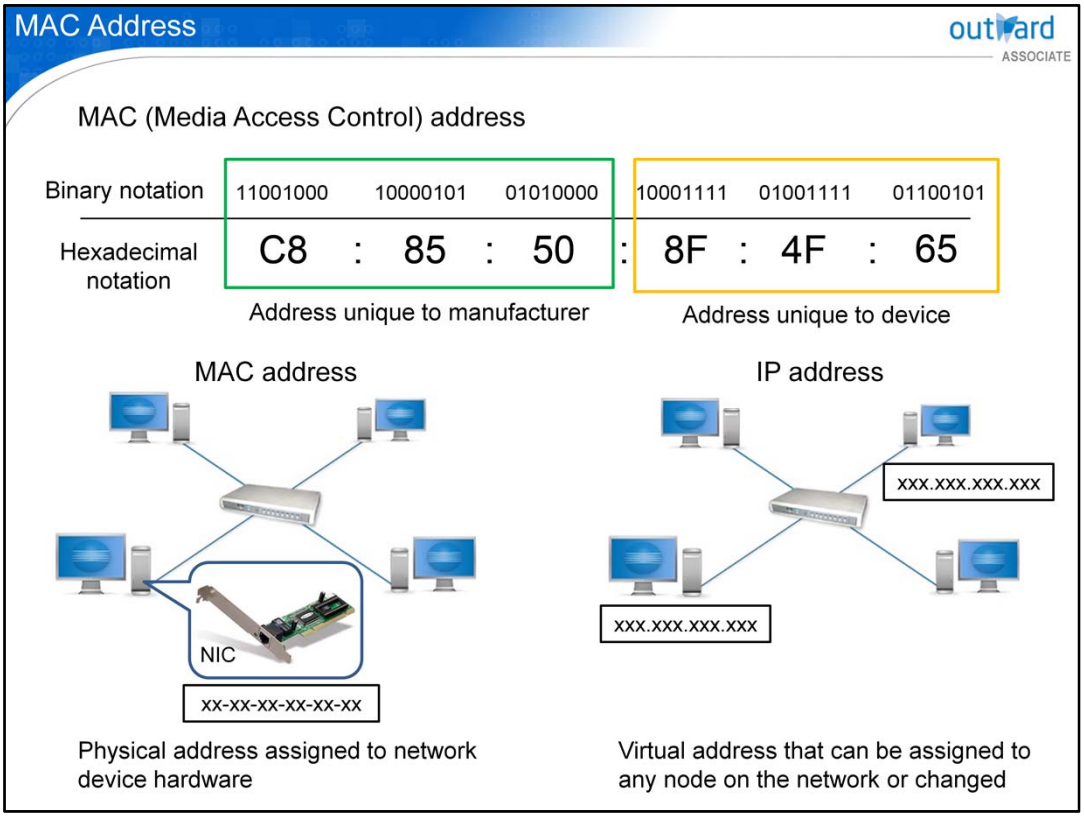
Cables, cable connectors, and hubs and traffic management hardware for connecting numerous workstations are essential for connecting to networks. This lesson introduces the hardware required for creating networks.

Кабели, кабельные разъемы, а также концентраторы и оборудование для управления трафиком для подключения многочисленных рабочих станций необходимы для подключения к сетям. Этот урок знакомит с оборудованием, необходимым для создания сетей.



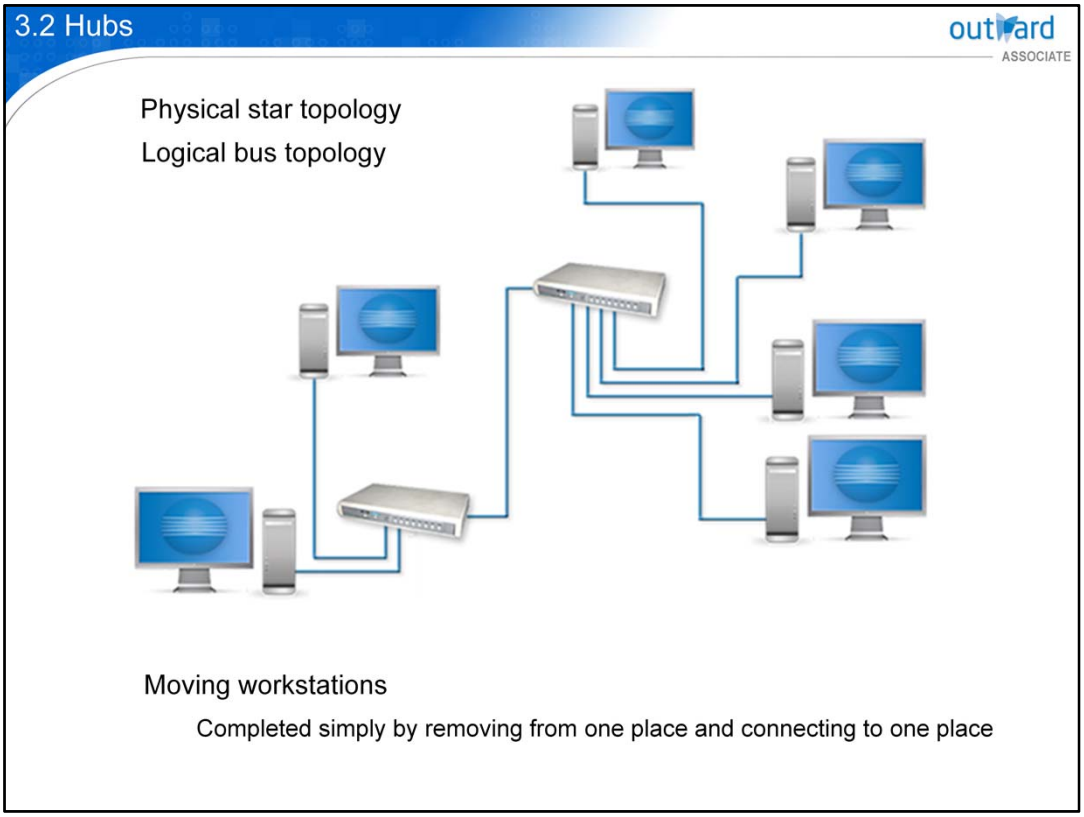
A NIC is a device that allows an individual hardware component to communicate with a network.
The card translates and controls information flow between the device and the network.
Physically, NIC's are usually electronic component cards that are slotted into the computer's motherboard.
The card is connected to the network either by a physical connection, or by wireless systems.
However, most recent new computers have a built-in NIC on the motherboard.

NIC - это устройство, которое позволяет отдельному аппаратному компоненту взаимодействовать с сетью.
Карта переводит и контролирует поток информации между устройством и сетью.
Физически, сетевые карты - это, как правило, карты электронных компонентов, которые вставляются в материнскую плату компьютера.
Карта подключена к сети либо через физическое соединение, либо через беспроводные системы.
Тем не менее, большинство новых компьютеров имеют встроенную сетевую карту на материнской плате.



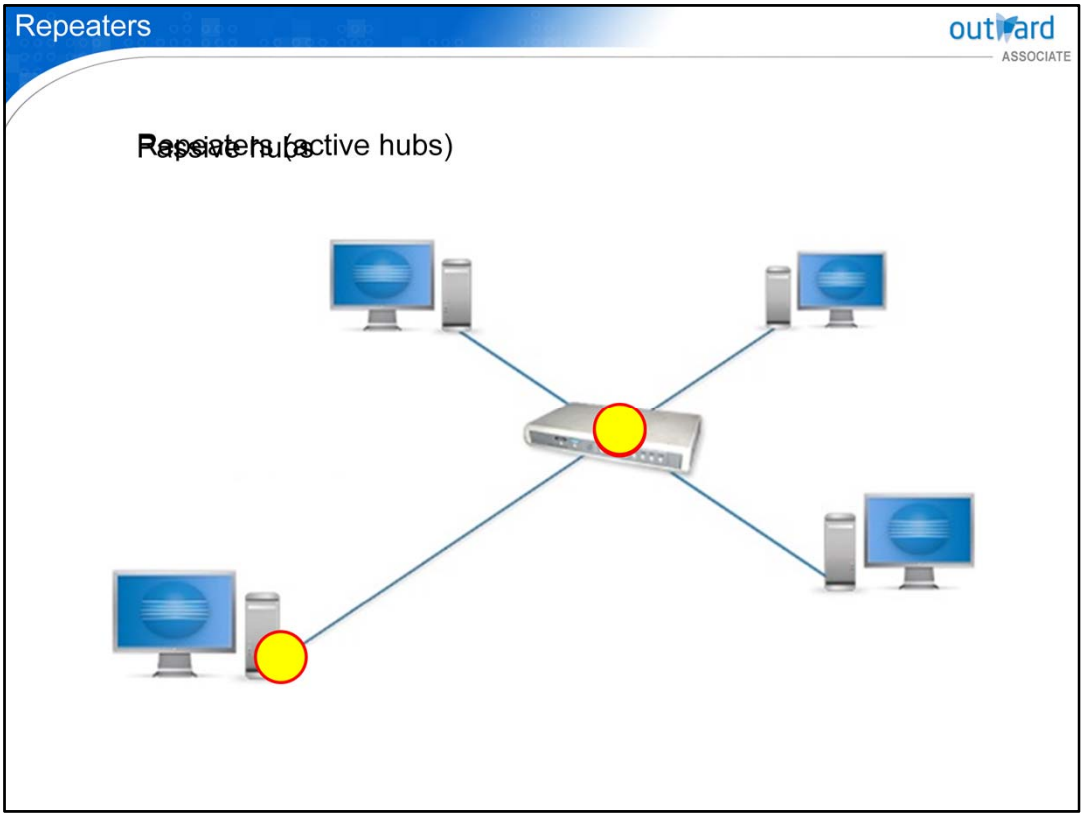
Each NIC has its own address, and other nodes are able to communicate by identifying the address. This address, called the MAC address or, less commonly, the NIC address, is a 12-digit hexadecimal unique identifier. The first six digits of the MAC address are assigned by IEEE and identify the manufacturer. The remaining six digits are unique numbers for identifying individual devices and are assigned by the manufacturer. This identifier should not be changed.
The IP address is a virtual address, identifying an entity in a network, and can be allocated to any node within the network, but the MAC address is assigned to a separate physical device.
In a TCP/IP network, the component of the IP address that identifies the host device needs to be mapped to the MAC address of the individual machine. The NIC monitors network traffic for packets addressed to its unique MAC address, only decoding those packets that match.

Каждый сетевой адаптер имеет свой собственный адрес, а другие узлы могут общаться, идентифицируя адрес.
Этот адрес, называемый MAC-адресом или, реже, адресом NIC, представляет собой 12-значный шестнадцатеричный уникальный идентификатор. Первые шесть цифр MAC-адреса присваиваются IEEE и указывают производителя. Остальные шесть цифр являются уникальными номерами для идентификации отдельных устройств и присваиваются производителем. Этот идентификатор не должен быть изменен.
IP-адрес является виртуальным адресом, идентифицирующим объект в сети, и может быть назначен любому узлу в сети, но MAC-адрес назначен отдельному физическому устройству.
В сети TCP / IP компонент IP-адреса, который идентифицирует хост-устройство, должен быть сопоставлен с MAC-адресом отдельной машины. Сетевая карта контролирует сетевой трафик для пакетов, адресованных на его уникальный MAC-адрес, декодируя только те пакеты, которые совпадают.



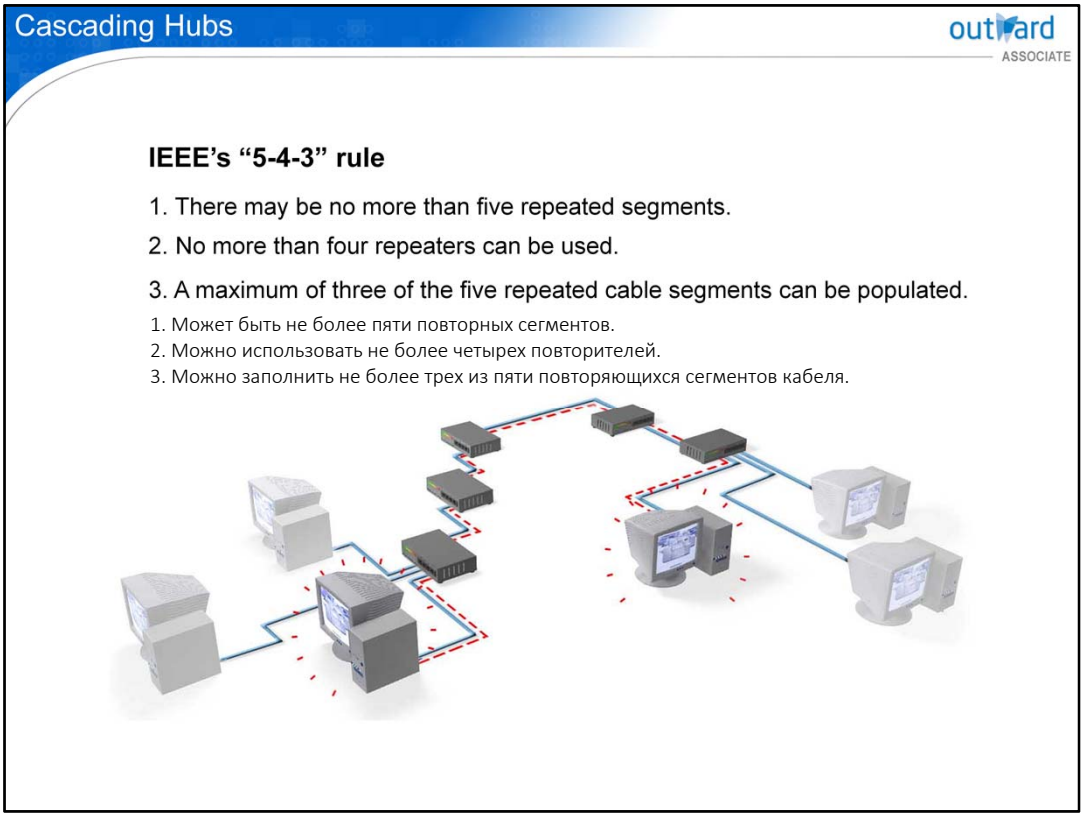
Hubs perform the task of interconnecting network devices. Ethernet often operates in a physical star topology, based on a hub, with a logical bus topology.
Hubs are also widely used in networks of all topologies to extend the network by acting as the central communication point distributing signals to a new group.
Centralizing the network's wiring is an advantage, making it easier to manage a large and potentially complicated cabling system.
When physically relocating workstations, a workstation can be removed from one part of the system and simply plugged into a different part of the network. Physically, a basic hub is a collection of connectors and switches.
In current LANs, switches are generally used instead of hubs as devices interconnecting different network nodes.

Концентраторы выполняют задачу соединения сетевых устройств. Ethernet часто работает в физической звездной топологии на основе концентратора с топологией логической шины.
Концентраторы также широко используются в сетях всех топологий для расширения сети, выступая в качестве центральной точки связи, распределяющей сигналы для новой группы.
Централизация проводки сети является преимуществом, облегчая управление большой и потенциально сложной кабельной системой.
При физическом перемещении рабочих станций рабочую станцию можно удалить из одной части системы и просто подключить к другой части сети. Физически базовый концентратор представляет собой набор разъемов и переключателей.
В современных локальных сетях коммутаторы обычно используются вместо концентраторов в качестве устройств, соединяющих различные сетевые узлы.



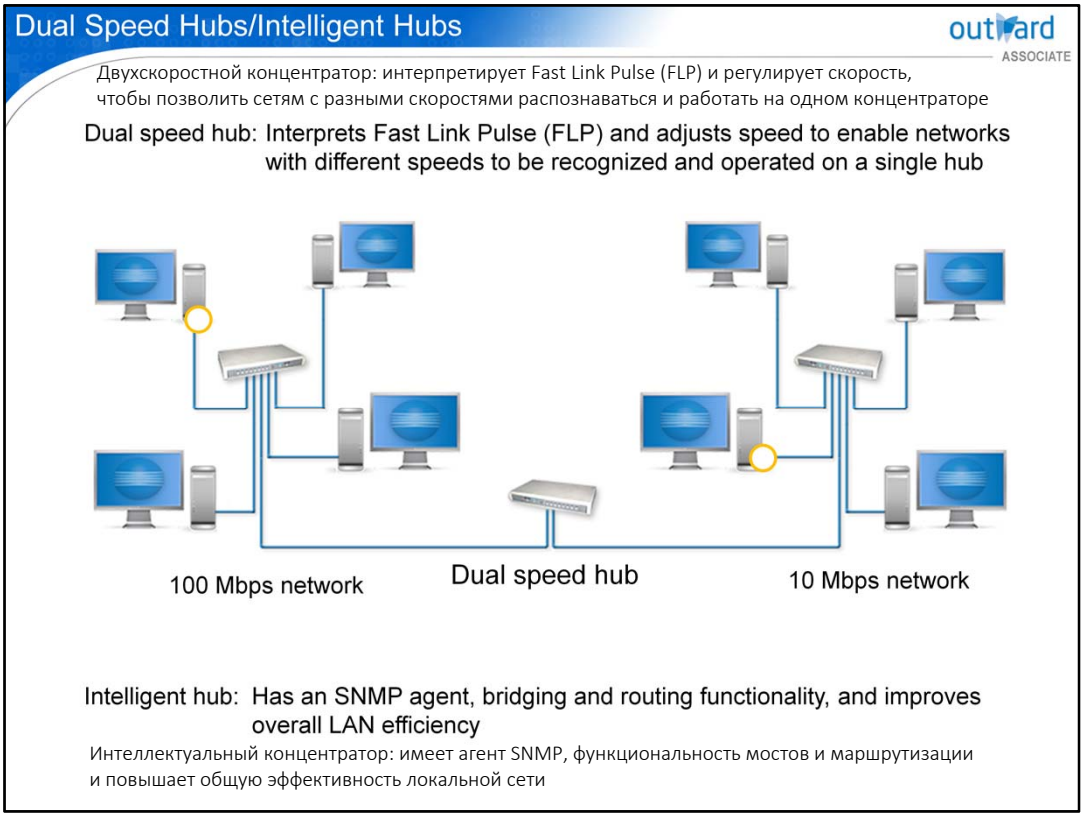
Passive hubs deliver transfer signals without doing anything to each workstation.
In this configuration, the distance between the hub and workstation is limited, and the danger of losing the signal is eliminated.
However, if the connection distance is long the signal strength becomes weaker.
An active hub, or repeater, boosts the signal strength before re-transmitting it, allowing connection distances to be extended.

Пассивные концентраторы доставляют сигналы передачи, ничего не делая для каждой рабочей станции.
В этой конфигурации расстояние между концентратором и рабочей станцией ограничено, и опасность потери сигнала устранена.
Однако, если расстояние соединения велико, уровень сигнала становится слабее.
Активный концентратор или ретранслятор повышает уровень сигнала перед его повторной передачей, что позволяет увеличить расстояния соединения.



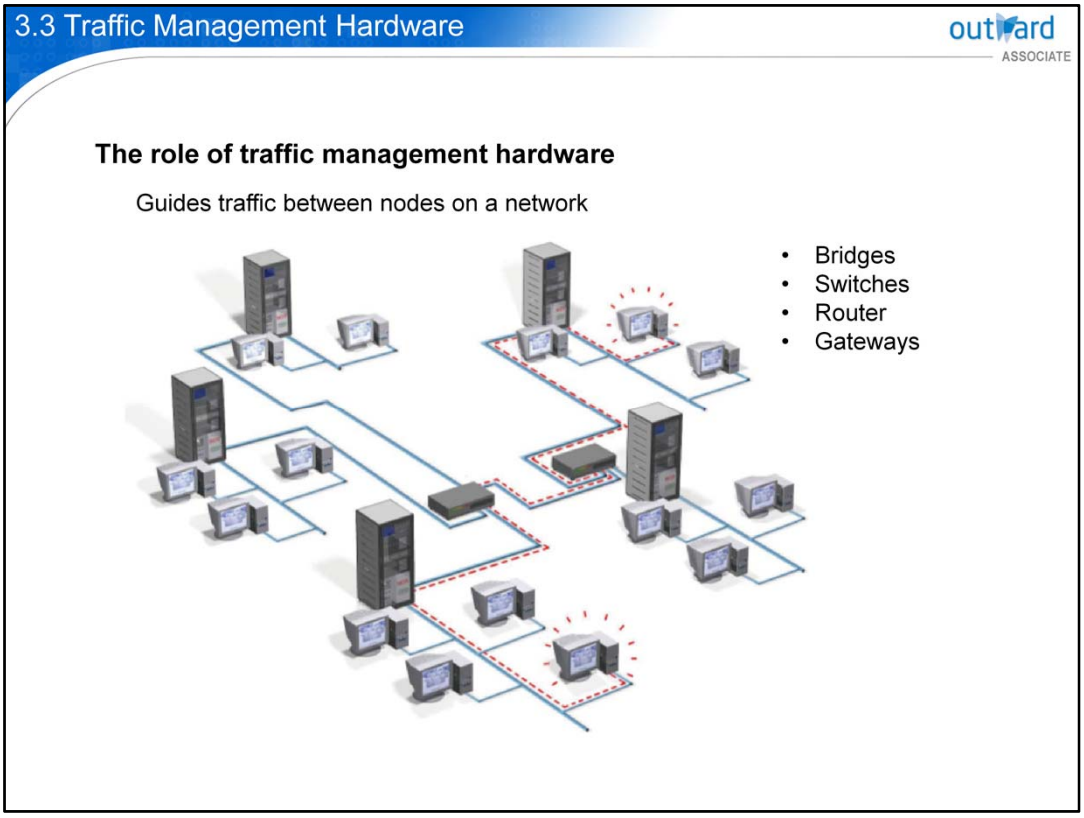
In star networks connecting multiple devices through line concentrators such as hubs, the network can be expanded by connecting line concentrators. This method is called cascading.
However, there are limitations to extending a network and the limitations are best explained by the IEEE's "5-4-3" rule. There may be no more than five repeated segments between any two Ethernet network devices.
No more than four repeaters can be used between any two Ethernet network devices.
A maximum of three of the five repeated cable segments can be populated.
If the network cascades through repeating hubs, this rule has to be observed to ensure point to-point communication. IEEE's 5-4-3 rule does not apply to the ends on switches or switch ports.

В звездных сетях, соединяющих несколько устройств через линейные концентраторы, такие как концентраторы, сеть может быть расширена путем подключения линейных концентраторов. Этот метод называется каскадным.
Однако существуют ограничения на расширение сети, и эти ограничения лучше всего объясняются правилом IEEE «5-4-3». Между любыми двумя сетевыми устройствами Ethernet может быть не более пяти повторяющихся сегментов.
Между любыми двумя сетевыми устройствами Ethernet можно использовать не более четырех повторителей.
Можно заполнить не более трех из пяти повторяющихся сегментов кабеля.
Если сеть соединяется каскадом через повторяющиеся концентраторы, необходимо соблюдать это правило для обеспечения связи точка-точка. Правило IEEE 5-4-3 не применяется к концам коммутаторов или портов коммутаторов.



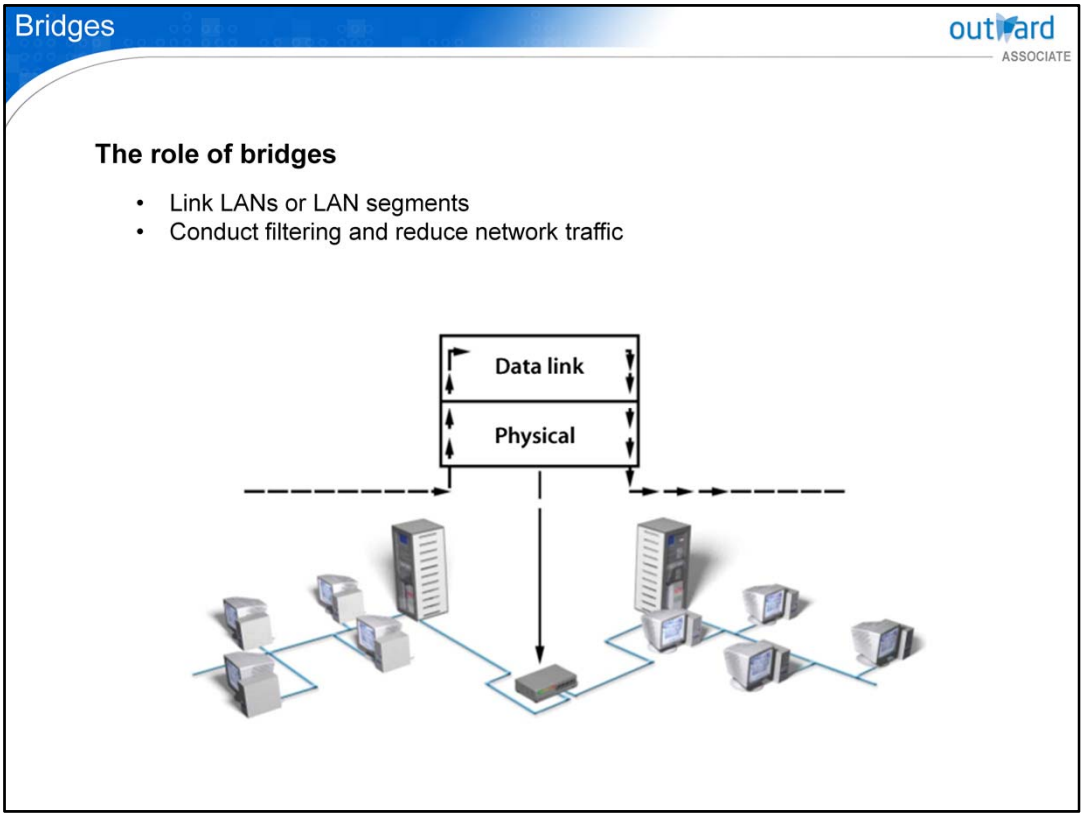
Dual speed hubs have the ability to negotiate network traffic between segments operating at different speeds.
For example, different speeds such as 10BASE-T, 100BASE-T, Fast Ethernet and Gigabit Ethernet are able to be recognized and operated on a single hub.
Dual speed hubs use speed-sensing to interpret Fast Link Pulses interspersed between the packets, and set the port to the appropriate speed for the incoming traffic. An internal switch connects between the 10Mbps and 100Mbps domains. LED indicators on the front panel of the hub show the speed of each port.
A dual speed hub can be cascaded with other 100 Mbps and 10M bps hubs to provide more ports.
Intelligent hubs communicate network management information, thus increasing overall LAN efficiency. They have SNMP agent functionality and can also provide bridging and routing functions.

Двухскоростные концентраторы способны согласовывать сетевой трафик между сегментами, работающими на разных скоростях.
Например, различные скорости, такие как 10BASE-T, 100BASE-T, Fast Ethernet и Gigabit Ethernet, могут распознаваться и работать на одном концентраторе.
Двухскоростные концентраторы используют определение скорости для интерпретации импульсов Fast Link, распределенных между пакетами, и устанавливают для порта соответствующую скорость для входящего трафика. Внутренний коммутатор подключается между доменами 10 Мбит / с и 100 Мбит / с. Светодиодные индикаторы на передней панели концентратора показывают скорость каждого порта.
Двухскоростной концентратор может быть соединен каскадом с другими концентраторами со скоростью 100 Мбит / с и 10 Мбит / с для обеспечения большего количества портов.
Интеллектуальные концентраторы передают информацию об управлении сетью, что повышает общую эффективность локальной сети.
Они имеют функции агента SNMP, а также могут обеспечивать функции моста и маршрутизации.



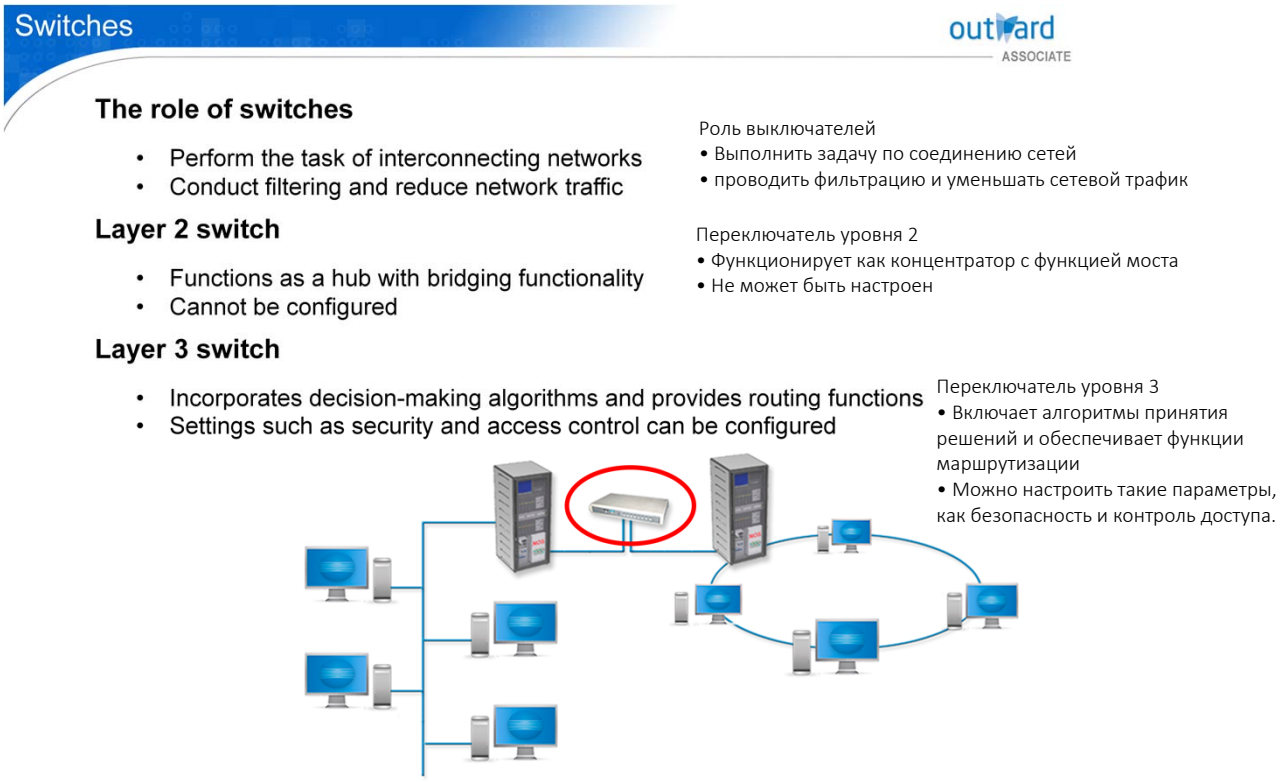
There are a number of devices used to direct traffic from one node to another within a network or across multiple networks. The devices you are most likely to encounter are as follows.

Существует ряд устройств, используемых для направления трафика от одного узла к другому в сети или по нескольким сетям. Устройства, с которыми вы, скорее всего, столкнетесь, следующие.



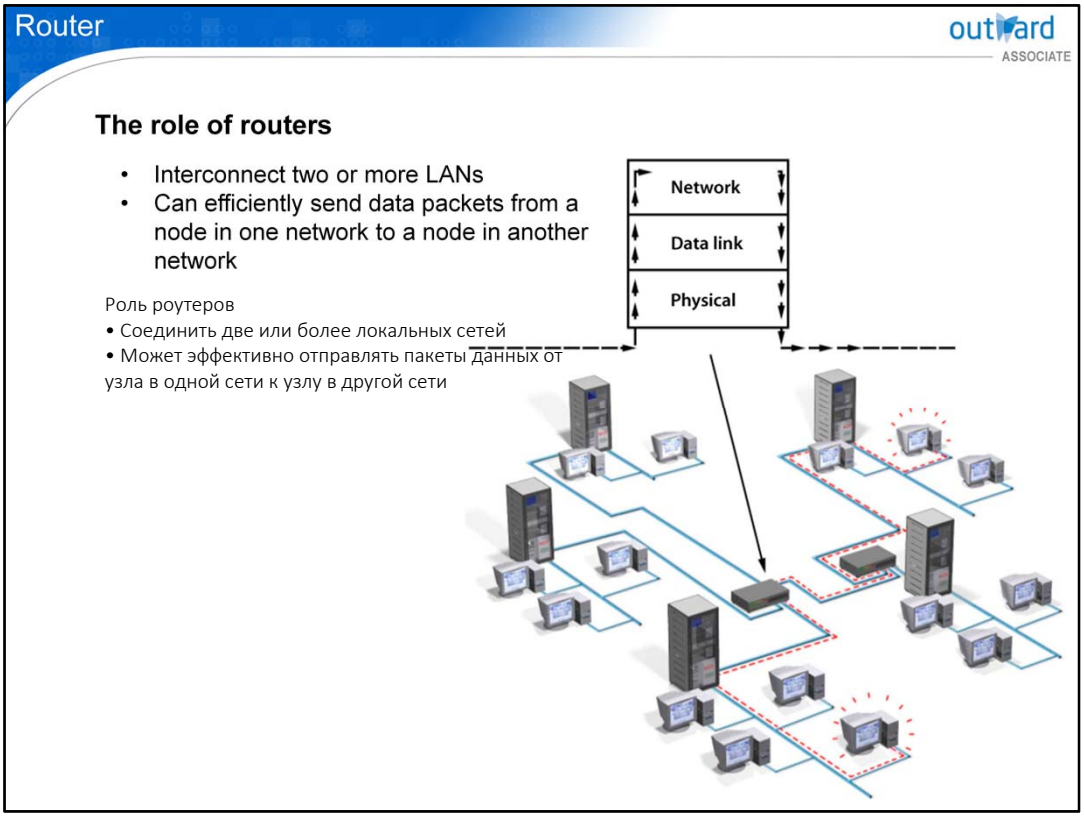
Bridges are devices used to link separate LANs or LAN segments that operate on the same data link layer of the OSI model.
They do not convert network data between protocols as they operate only at the data link level.
If two separate LANs are connected with a bridge they behave as one network.
Bridges serve to reduce network traffic by filtering broadcast messages. They contain a list of workstation addresses.
If the data packet address matches any of the addresses on the list, the message is transmitted to that workstation.
If there are no matching addresses, the packet is forwarded to the next bridge, where the process is repeated.
Filtering can be performed more efficiently because the bridges learn which address belongs to which network and can develop a database.
Bridge features are simpler and cheaper compared to routers.

Мосты - это устройства, используемые для связи отдельных локальных сетей или сегментов локальной сети, которые работают на одном канальном уровне передачи данных модели OSI.
Они не преобразуют сетевые данные между протоколами, поскольку работают только на уровне канала передачи данных.
Если две отдельные ЛВС соединены мостом, они ведут себя как одна сеть.
Мосты служат для уменьшения сетевого трафика путем фильтрации широковещательных сообщений. Они содержат список адресов рабочих станций.
Если адрес пакета данных совпадает с любым из адресов в списке, сообщение передается на эту рабочую станцию.
Если совпадающих адресов нет, пакет пересылается на следующий мост, где процесс повторяется.
Фильтрация может выполняться более эффективно, потому что мосты узнают, какой адрес принадлежит какой сети и могут создать базу данных.
Функции моста проще и дешевле по сравнению с маршрутизаторами.



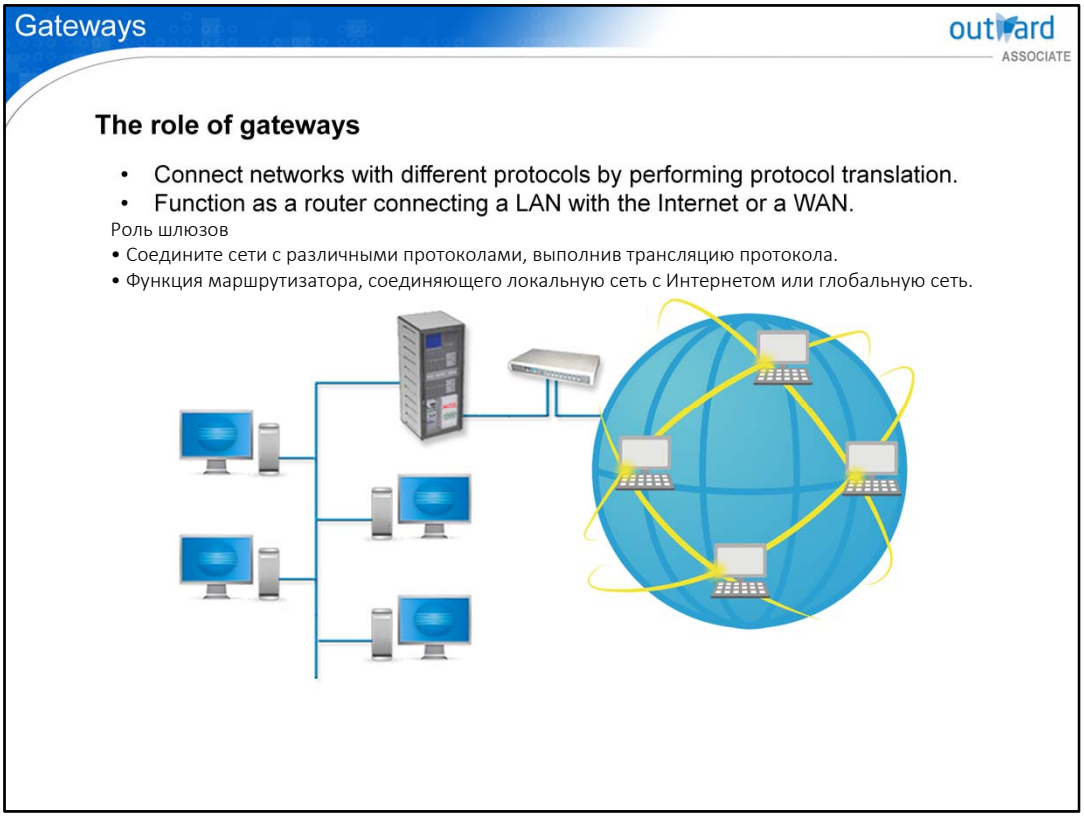
A switch is a device that can interconnect network devices and direct information from one data path to another.
A switch can usually connect several different networks together, including networks using different architectures. In practical terms switches are drop-in replacements for hubs.
Switches vary in their level of sophistication.
A layer 2 switch operates as a hub with a bridge function, but it cannot be configured. It only connects to the network with the power on.
A layer 3 switch incorporates decision-making algorithms and provides routing functions.
They typically have a built-in operating system and can be configured on the fly with security, access control and other settings.

Коммутатор - это устройство, которое может соединять сетевые устройства и передавать информацию из одного тракта данных в другой.
Коммутатор обычно может соединять несколько разных сетей, включая сети с разными архитектурами. С практической точки зрения переключатели являются заменой втулок.
Переключатели различаются по уровню сложности.
Коммутатор уровня 2 работает как концентратор с функцией моста, но его нельзя настроить. Он подключается только к сети при включенном питании.
Коммутатор уровня 3 включает алгоритмы принятия решений и обеспечивает функции маршрутизации.
Как правило, они имеют встроенную операционную систему и могут быть настроены на лету с помощью безопасности, контроля доступа и других параметров.



A router is an intelligent device that connects two or more LANs, which send data packets from nodes on one network to nodes on a different network. Routing is a function associated with the network layer in the OSI model. Routers can send data between networks using different architectures and different low-level protocols, however, they are restricted to operating between networks using the same high level protocols. Routers determine which path a data packet should be sent along in order for it to most efficiently reach its final destination.
They make the determination according to knowledge of the state of each network path such as free, blocked and busy. Routers work to reduce traffic on the network by only allowing data operating with certain protocols to enter the LAN.

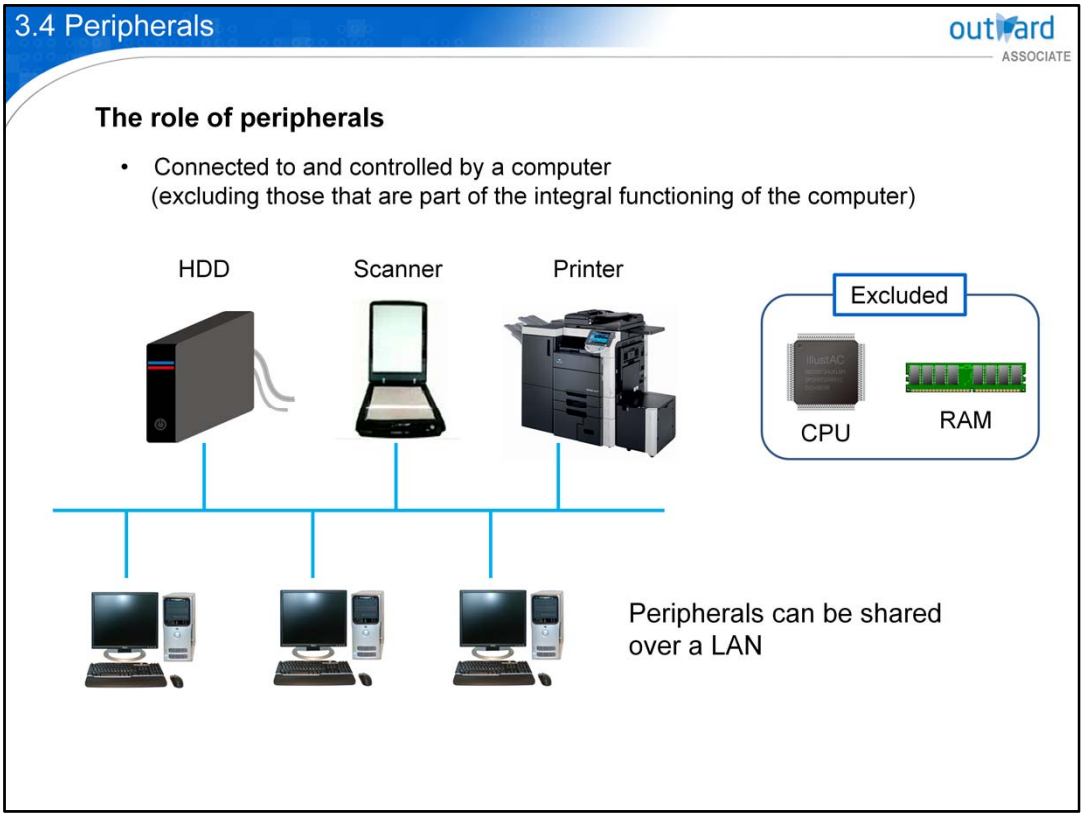
Маршрутизатор - это интеллектуальное устройство, которое соединяет две или более локальных сетей, которые отправляют пакеты данных из узлов одной сети в узлы другой сети. Маршрутизация - это функция, связанная с сетевым уровнем в модели OSI. Маршрутизаторы могут передавать данные между сетями, используя разные архитектуры и разные протоколы низкого уровня, однако они ограничены для работы между сетями, использующими одни и те же протоколы высокого уровня.
Маршрутизаторы определяют, по какому пути должен быть отправлен пакет данных, чтобы он наиболее эффективно достиг конечного пункта назначения.
Они делают определение в соответствии со знанием состояния каждого сетевого пути, например, свободен, заблокирован и занят. Маршрутизаторы работают для уменьшения трафика в сети, позволяя только данным, работающим с определенными протоколами, входить в локальную сеть.



A gateway is a connection between a LAN and another system. For example, it may be used between a LAN and a mainframe computer or a larger network such as the Internet. Gateways perform protocol conversions to transmit messages between these systems. Generally, they are slower than bridges or routers.
In typical business networks that are homogeneous, gateways are essentially routers that interconnect the company's LAN to the Internet, its WAN or other external networks.

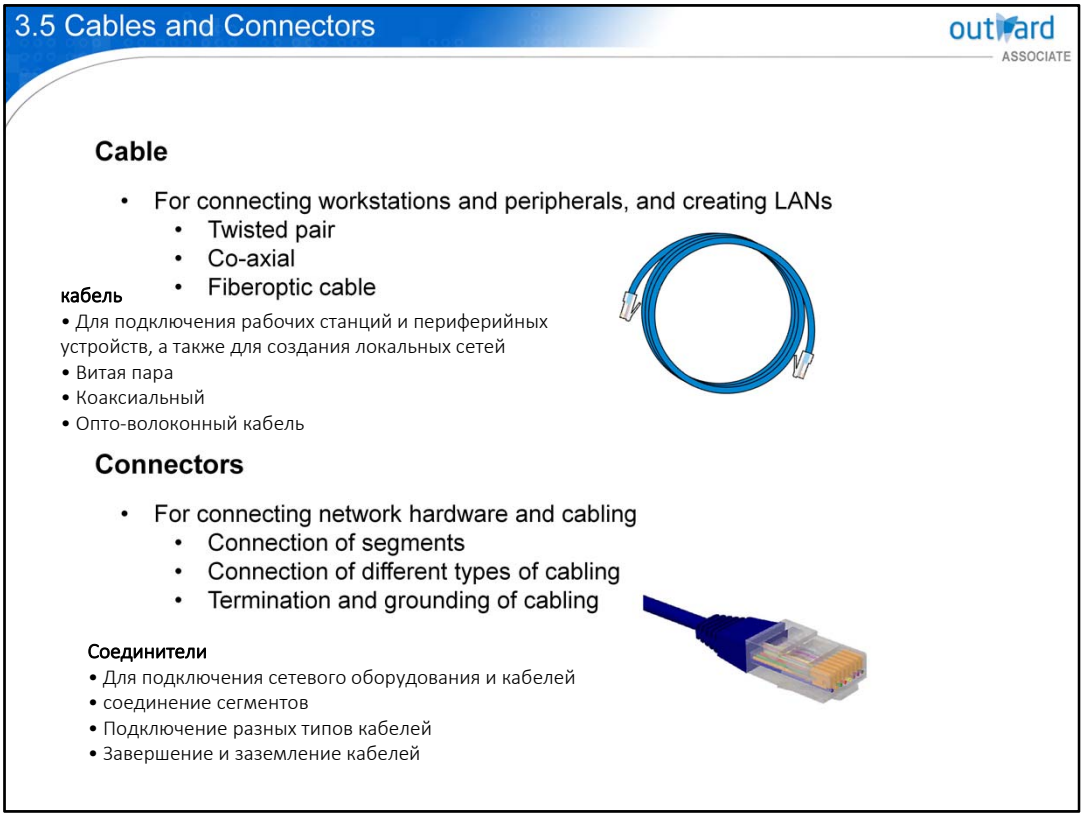
Шлюз - это соединение между локальной сетью и другой системой. Например, он может использоваться между локальной сетью и мэйнфреймовым компьютером или более крупной сетью, такой как Интернет. Шлюзы выполняют преобразование протоколов для передачи сообщений между этими системами. Как правило, они медленнее, чем мосты или маршрутизаторы.
В типичных бизнес-сетях, которые являются однородными, шлюзы - это, по сути, маршрутизаторы, которые соединяют локальную сеть компании с Интернетом, ее глобальной сетью или другими внешними сетями.

Роль периферии
• Подключен и контролируется компьютером
(исключая те, которые являются частью целостного функционирования компьютера)



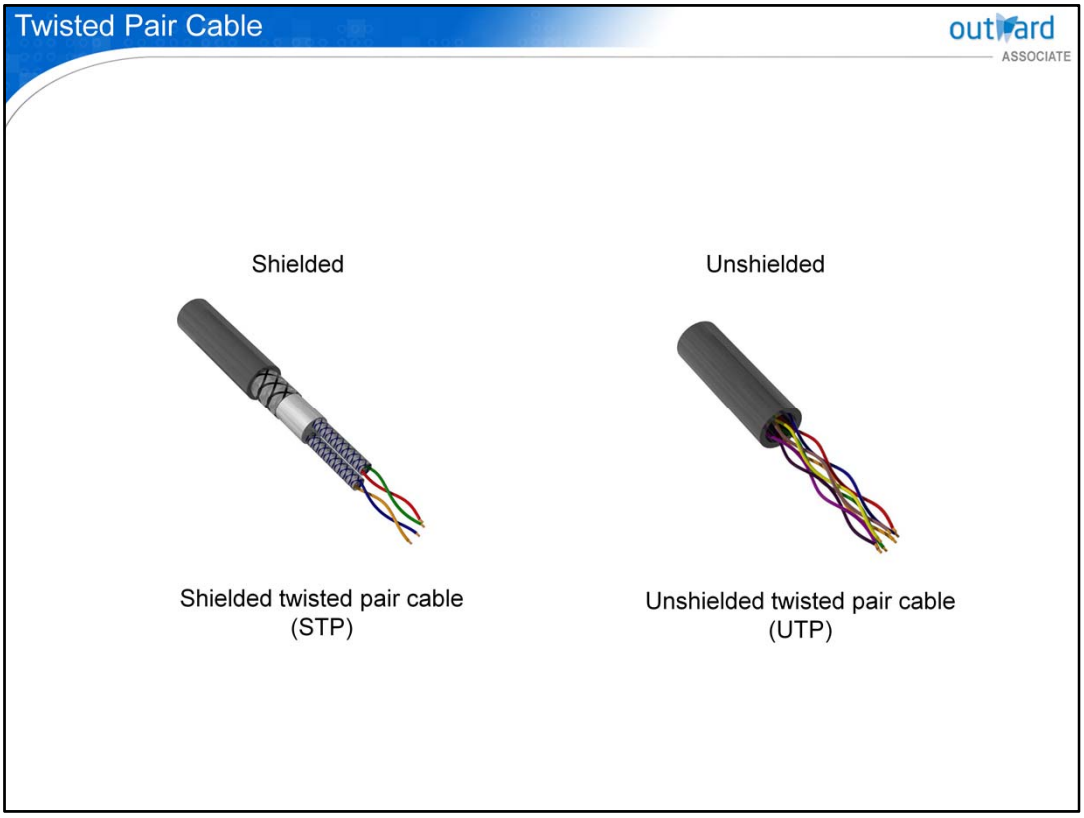
A peripheral is any computer device that can be connected to and controlled by a computer. However, is not part of the integral functioning of the computer in the way that the CPU, RAM memory or the data path are.
Some peripherals such as hard disk drives may be located within a computer housing.
Others are external to the computer, for example, printers and scanners.
One of the major advantages of a LAN is its ability to efficiently share peripheral devices between networked workstations.
Networked printers have increased in popularity because multiple printers can be connected to a single network, serving different needs.

Периферийным устройством является любое компьютерное устройство, которое может быть подключено к компьютеру и управляться им.
Однако это не является частью целостного функционирования компьютера так, как это делает процессор, память ОЗУ или тракт данных.
Некоторые периферийные устройства, такие как жесткие диски, могут быть расположены внутри корпуса компьютера.
Другие являются внешними по отношению к компьютеру, например, принтеры и сканеры.
Одним из основных преимуществ локальной сети является ее способность эффективно обмениваться периферийными устройствами между сетевыми рабочими станциями.
Популярность сетевых принтеров возросла, поскольку к одной сети можно подключить несколько принтеров, удовлетворяя различные потребности.



Cabling is an essential part of any LAN. Cabling must not only link workstations together but also link peripherals. There are many different types of cabling available, such as twisted pair cable and co-axial cable, each having particular advantages and disadvantages.
Connectors are the physical link between network hardware and cabling.
The type of connector used depends upon the components to be coupled and the topology of the network.
A connector can serve a number of functions. For example, connectors may connect equal or near equal segments of co-axial cable, connect different types of cabling such as co-axial and twisted pair, terminate a cable or terminate a cable to ground.

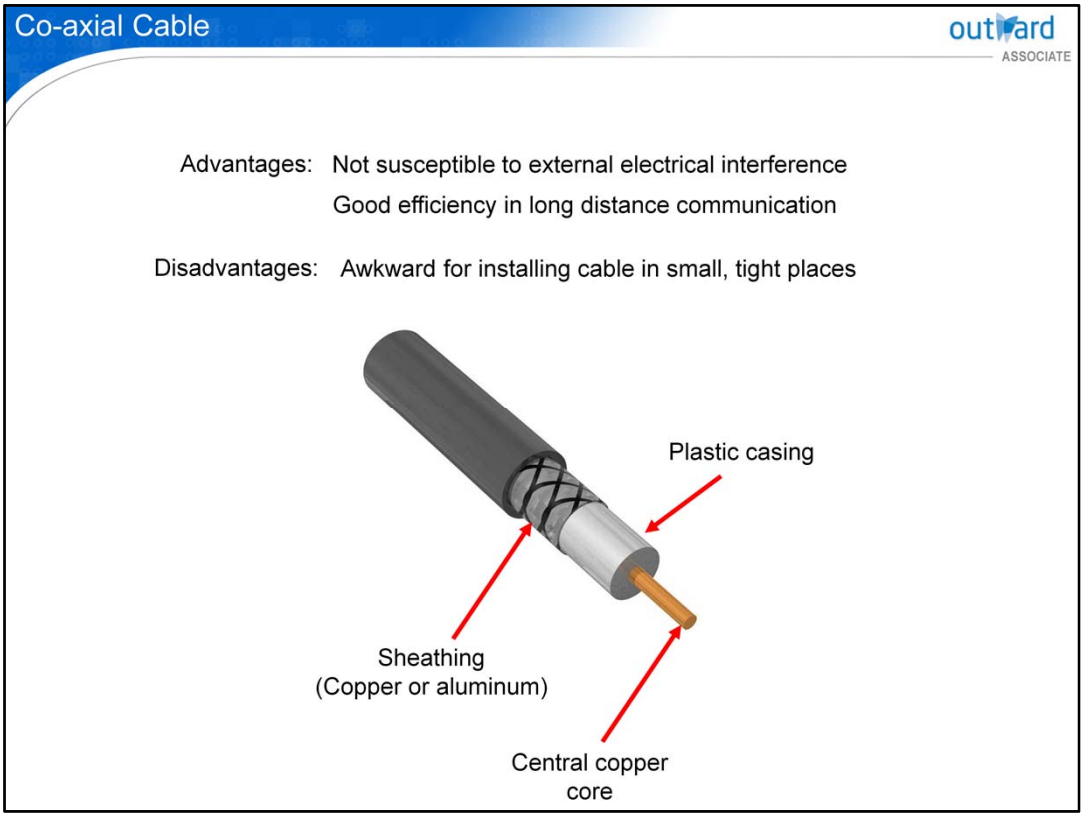
Кабели являются неотъемлемой частью любой локальной сети. Кабели должны соединять не только рабочие станции, но и периферийные устройства. Существует много различных типов кабелей, таких как витая пара и коаксиальный кабель, каждый из которых имеет свои преимущества и недостатки.
Разъемы - это физическая связь между сетевым оборудованием и кабелями. Тип используемого разъема зависит от соединяемых компонентов и топологии сети.
Разъем может выполнять ряд функций. Например, разъемы могут соединять равные или почти равные сегменты коаксиального кабеля, соединять различные типы кабелей, такие как коаксиальная и витая пара, соединять кабель или заземлять кабель.



Twisted pair cabling is by far the least expensive and most commonly used type of LAN cabling.
Twisted pair consists of two separate insulated wires twisted together, which ensures that each cable receives the same amount of outside electrical interference.
Cables can be shielded or left unshielded from electrical interference.
STP cables are more resilient to noise and offer better performance.
However, the LAN port must support STP to provide such performance, and UTP may be more stable in some cases. The advantages of twisted pair cabling are ease of installation, cost effectiveness and the ability to easily add new users to the system.

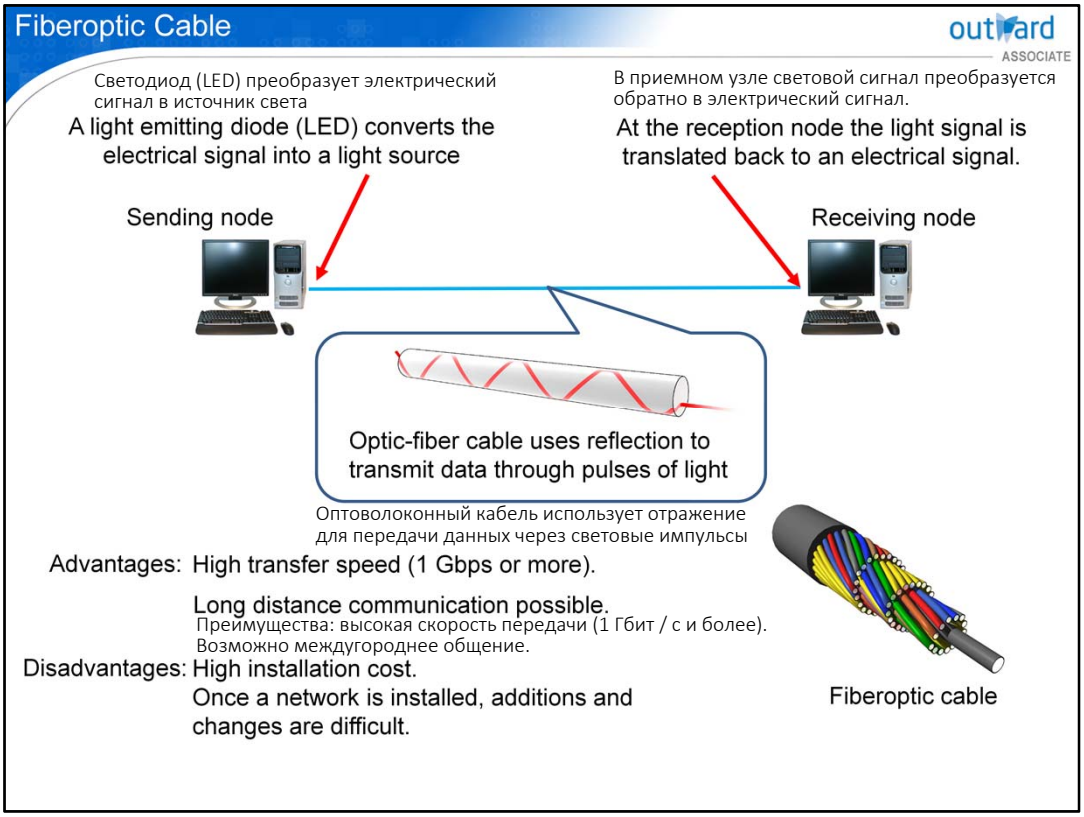
Кабели по витой паре - безусловно, самый дешевый и наиболее часто используемый тип ЛВС.
Витая пара состоит из двух отдельных изолированных проводов, скрученных вместе, что гарантирует, что каждый кабель получает одинаковое количество внешних электрических помех.
Кабели могут быть экранированы или не защищены от электрических помех.
Кабели STP более устойчивы к шуму и обеспечивают лучшую производительность.
Однако порт LAN должен поддерживать STP для обеспечения такой производительности, и в некоторых случаях UTP может быть более стабильным.
Преимущества кабелей по витой паре - простота монтажа, экономическая эффективность и возможность легко добавлять новых пользователей в систему.

Преимущества: не подвержены внешним электрическим помехам.
Хорошая эффективность при большой дистанции связи
Недостатки: неудобно для прокладки кабеля в небольших, узких местах



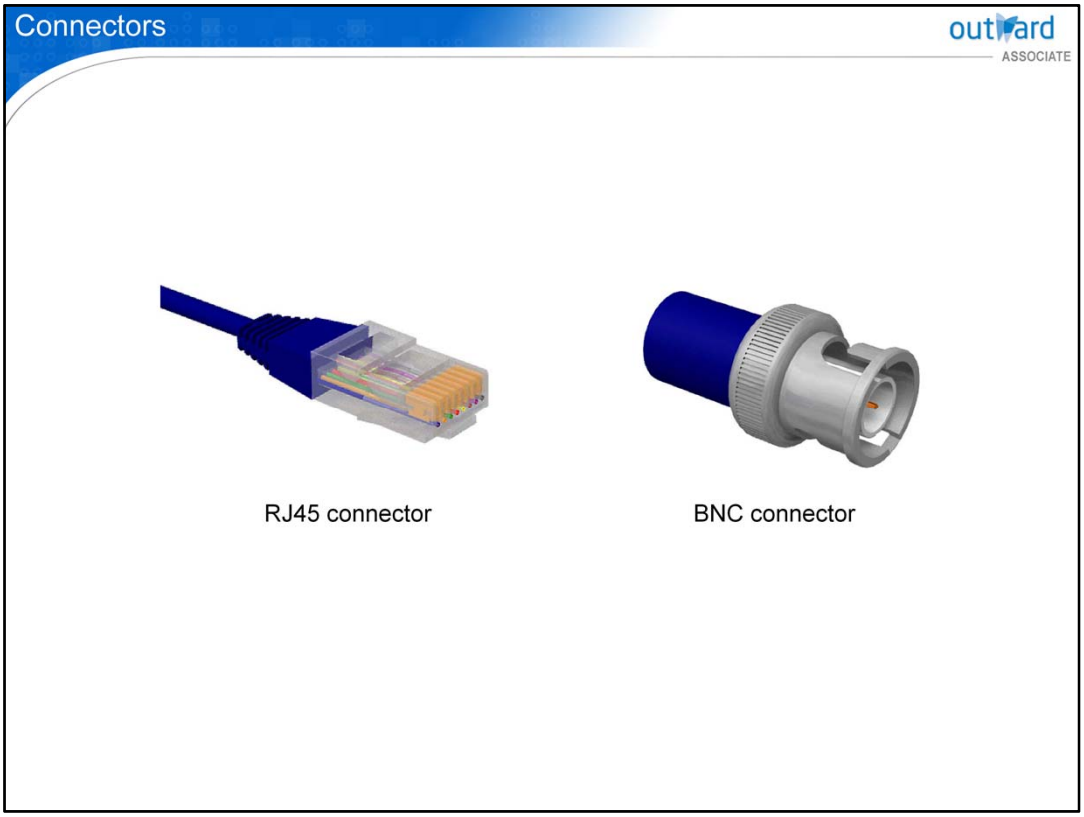
Co-axial cable, or coax, consists of a central copper core encased in a plastic sheath.
It is surrounded by copper or aluminum sheathing and finally encased in plastic.
The signal is transmitted along the central copper core, shielded from electrical interference by the sheath.
The main advantages are insensitivity to outside electrical interference and performance over long distances.
Co-axial cable is almost as easy to install and maintain as twisted pair, however, it is awkward to install in small, tight places.
Co-axial cable is now less popular than it was, having been overtaken by newer technologies such as fiberoptic cable.

Коаксиальный кабель, или коаксиальный кабель, состоит из центрального медного сердечника, заключенного в пластиковую оболочку.
Он окружен медной или алюминиевой оболочкой и, наконец, заключен в пластиковый корпус.
Сигнал передается по центральному медному сердечнику, экранированному от электрических помех оболочкой.
Основными преимуществами являются нечувствительность к внешним электрическим помехам и производительность на больших расстояниях.
Коаксиальный кабель почти так же прост в установке и обслуживании, как и витая пара, однако его неудобно устанавливать в небольших, тесных местах.
Коаксиальный кабель в настоящее время менее популярен, чем раньше, поскольку его настигли новые технологии, такие как волоконно-оптический кабель.



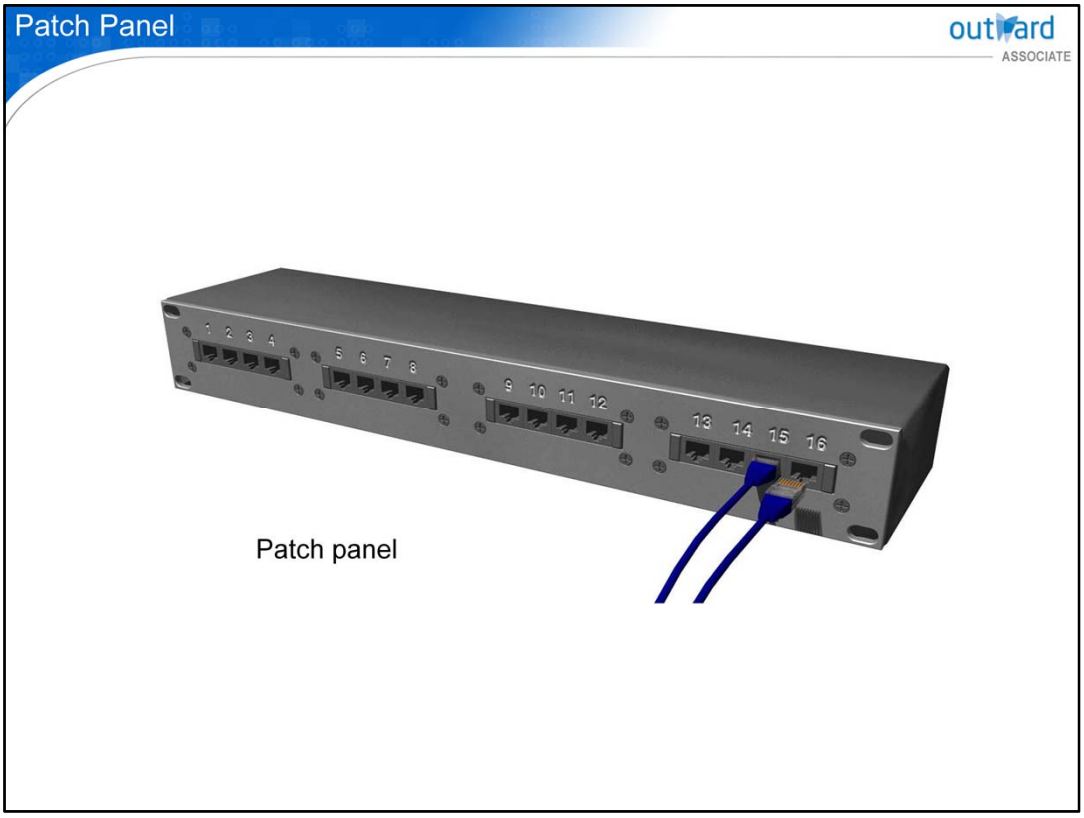
Fiberoptic cabling works by transmitting light pulses instead of electrical signals.
A device called a light emitting diode, or LED, converts electrical signals into a light source.
At the reception node the light signal is translated back to electrical signals for the workstation to process.
Cables are bundled in groups of up to 24 fibers but generally groups contain only two to four pairs.
Fiberoptic cable has a number of advantages over twisted pair and co-axial cabling. It can transmit data at high rates, normally 1 Gbps or more.
It is also completely immune to electrical interference and its low resistance means that cabling distances can be large. However fiberoptic cabling is expensive to install and it is difficult to add new workstations once the network has been installed.
These are the main barriers to wider use of fiberoptic technology in smaller networks.

Волоконно-оптические кабели работают путем передачи световых импульсов вместо электрических сигналов.
Устройство, называемое светодиодом или светодиодом, преобразует электрические сигналы в источник света.
В приемном узле световой сигнал преобразуется обратно в электрические сигналы для обработки рабочей станцией.
Кабели связаны в группы по 24 волокна, но обычно группы содержат только две-четыре пары.
Волоконно-оптический кабель имеет ряд преимуществ по сравнению с витой парой и коаксиальным кабелем. Он может передавать данные с высокой скоростью, обычно 1 Гбит / с или более.
Он также полностью невосприимчив к электрическим помехам, а его низкое сопротивление означает, что расстояние между кабелями может быть большим. Однако волоконно-оптические кабели являются дорогостоящими в установке, и после установки сети сложно добавить новые рабочие станции.
Это основные барьеры для более широкого использования волоконно-оптических технологий в небольших сетях.



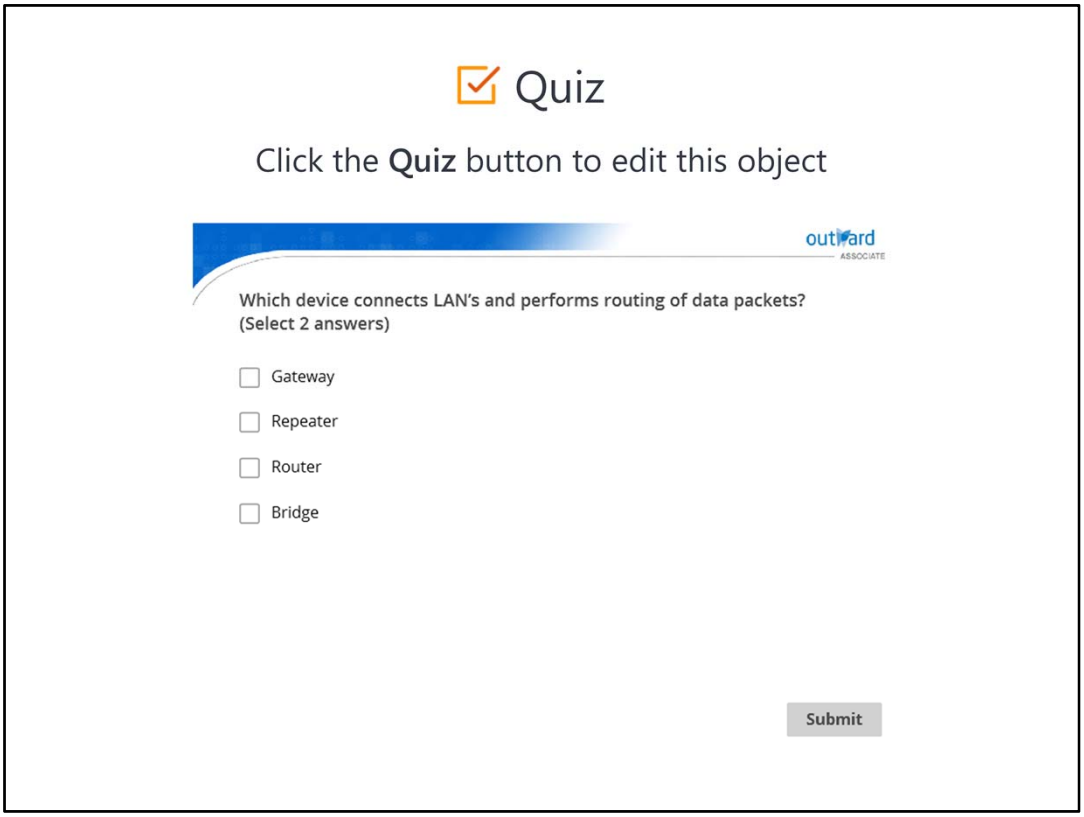
RJ connectors are used for twisted pair cables such as attaching telephone cables to modems.
The most popular are the RJ11 and RJ45, with RJ11 being used for cables of two pairs of and RJ45 for four pairs. BNC connectors connect cable of the same type such as thin and thick co-axial cable.
There are various theories on the unabbreviated form of BNC, including bayonet nut connectors and British Navy connectors.
Fiberoptic connectors are used to connect segments of fiberoptic cable together. Installation of fiberoptic connectors requires special equipment and know-how because a precise connection is required to reduce signal loss. Installation is typically performed by trained technicians.

Разъемы RJ используются для кабелей витой пары, например, для подключения телефонных кабелей к модемам.
Наиболее популярными являются RJ11 и RJ45, причем RJ11 используется для кабелей двух пар и RJ45 для четырех пар. Разъемы BNC соединяют кабель того же типа, что и тонкий и толстый коаксиальный кабель.
Существуют различные теории относительно сокращенной формы BNC, включая байонетные соединители и соединители BMC Великобритании.
Волоконно-оптические соединители используются для соединения сегментов оптоволоконного кабеля вместе. Для установки оптоволоконных разъемов требуется специальное оборудование и ноу-хау, поскольку для снижения потерь сигнала требуется точное соединение. Установка обычно выполняется обученными специалистами.

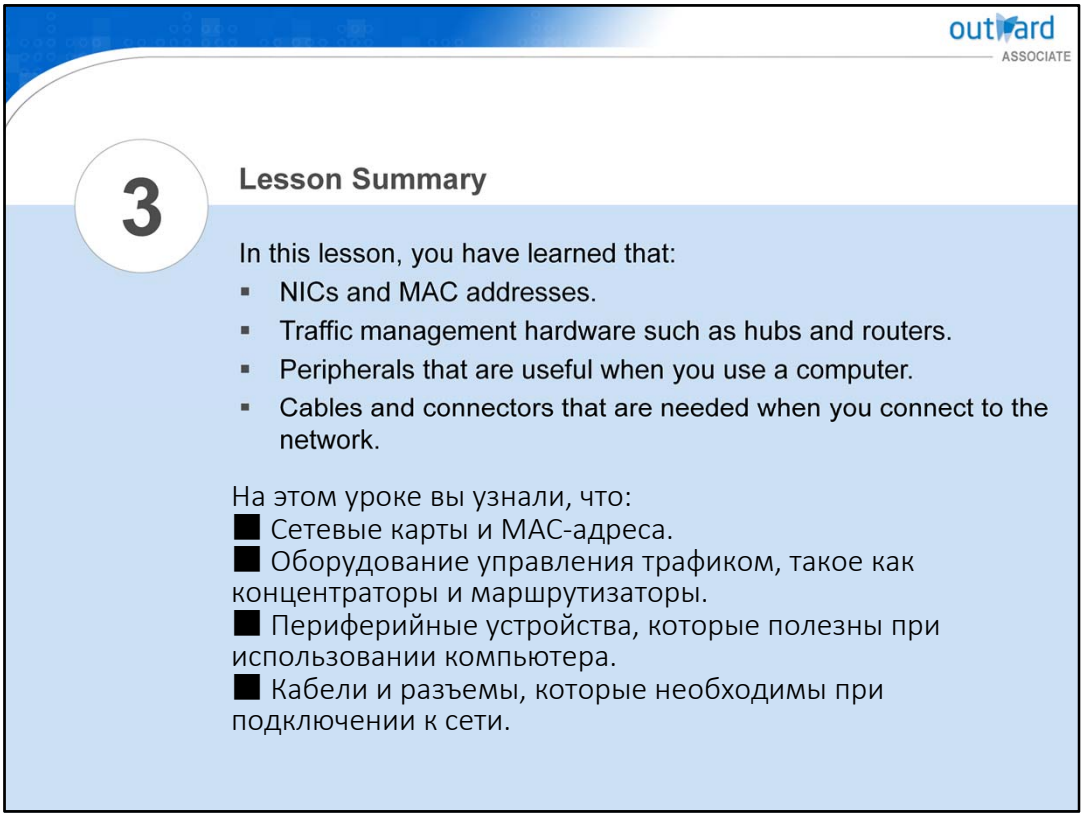


Connectors are sometimes assembled together into a patch panel. A patch panel is a mounted hardware unit containing an assembly of port locations. Patch panels contain ports where the cabling connects to the hardware device such as a hub.
Typically, a network uses a patch panel as a sort of switchboard, using cables to interconnect all of the computers within the area of a LAN.
The interconnecting cables are called patch cords.

Разъемы иногда собираются вместе в патч-панель. Патч-панель - это смонтированный аппаратный блок, содержащий сборку портов. Патч-панели содержат порты, где кабели подключаются к аппаратному устройству, такому как концентратор.
Как правило, сеть использует коммутационную панель в качестве своего рода коммутатора, используя кабели для соединения всех компьютеров в пределах локальной сети.
Соединительные кабели называются патч-кордами.

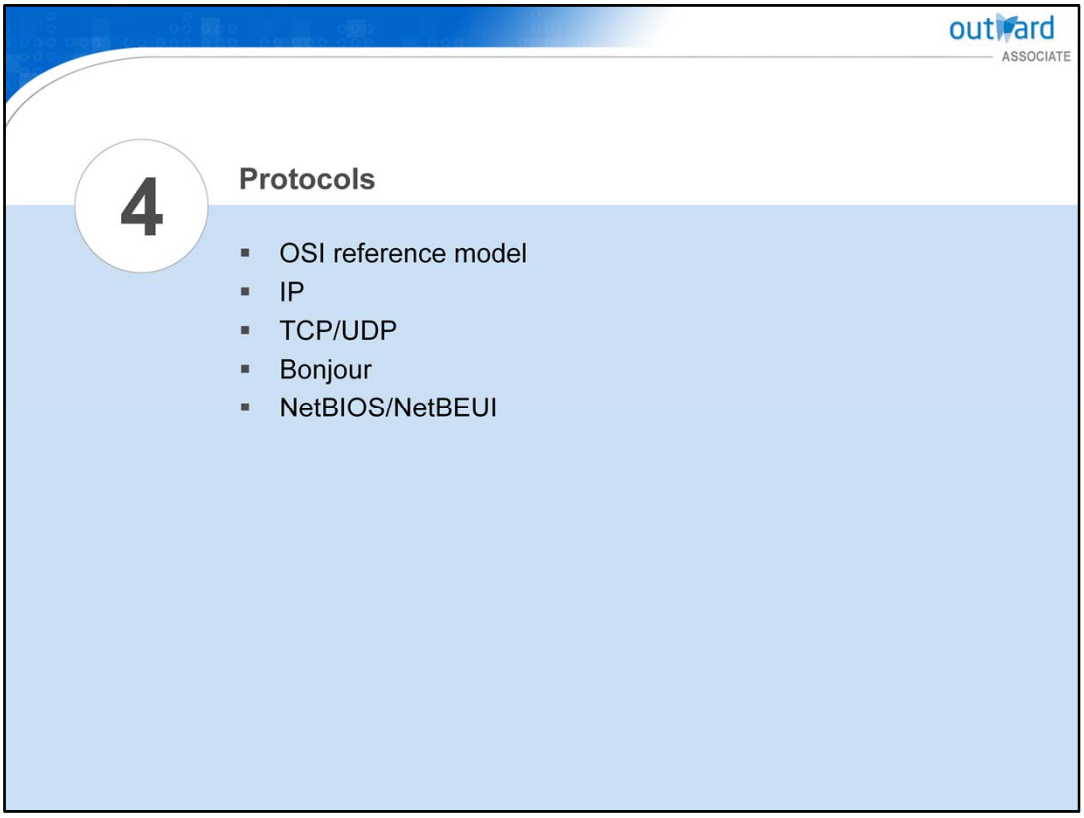


Test your knowledge in a quiz!



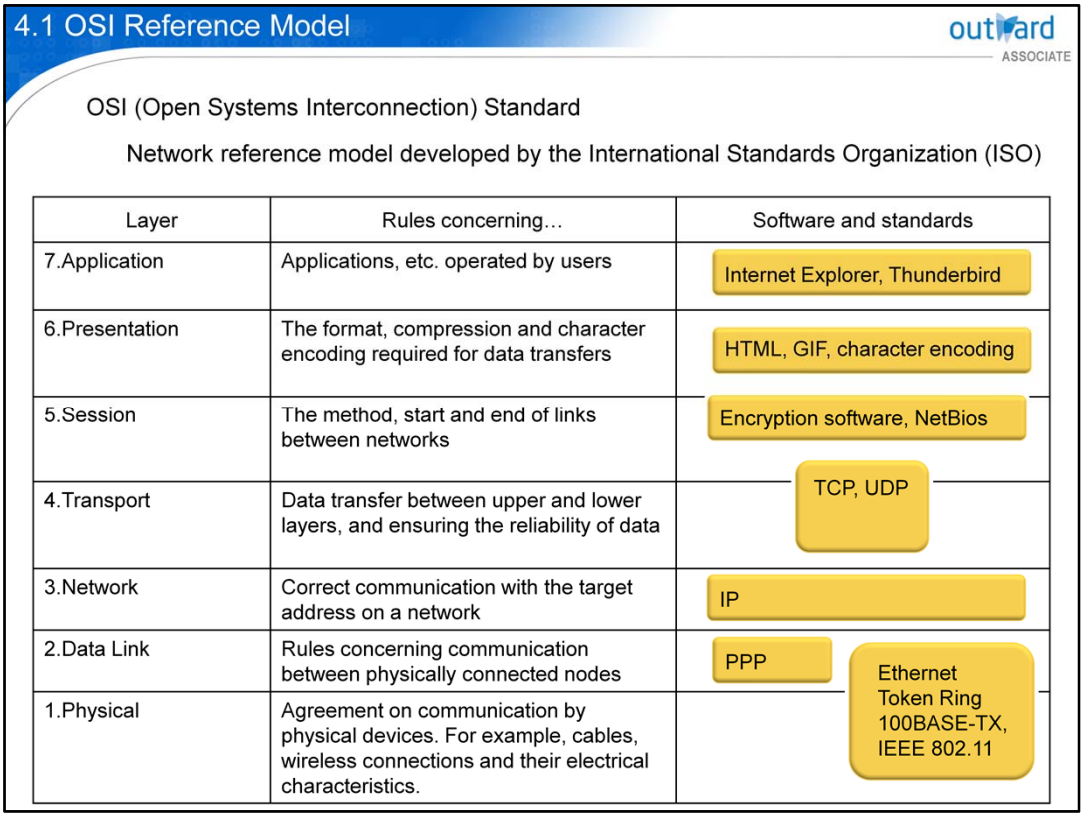
A network interface card is a piece of hardware required for a workstation to connect to a network.
Each card has a MAC address that is unique to the NIC for identification on the network.
Traffic management hardware not only connects to different LANs and the Internet, but also enables efficient communication by reducing network traffic.
Peripherals work by connecting to a computer. Peripherals can be shared between the work stations that are connected to the network.
Each type of connection cable have strengths and weaknesses, and need to be selectively used as appropriate.

Сетевая карта - это часть оборудования, необходимая для подключения рабочей станции к сети.
У каждой карты есть MAC-адрес, уникальный для сетевой карты для идентификации в сети.
Аппаратное обеспечение управления трафиком не только подключается к различным локальным сетям и Интернету, но также обеспечивает эффективную связь за счет сокращения сетевого трафика.
Периферийные устройства работают при подключении к компьютеру.
Периферийные устройства могут быть разделены между рабочими станциями, которые подключены к сети.
У каждого типа соединительного кабеля есть свои сильные и слабые стороны, и их необходимо выборочно использовать по мере необходимости.



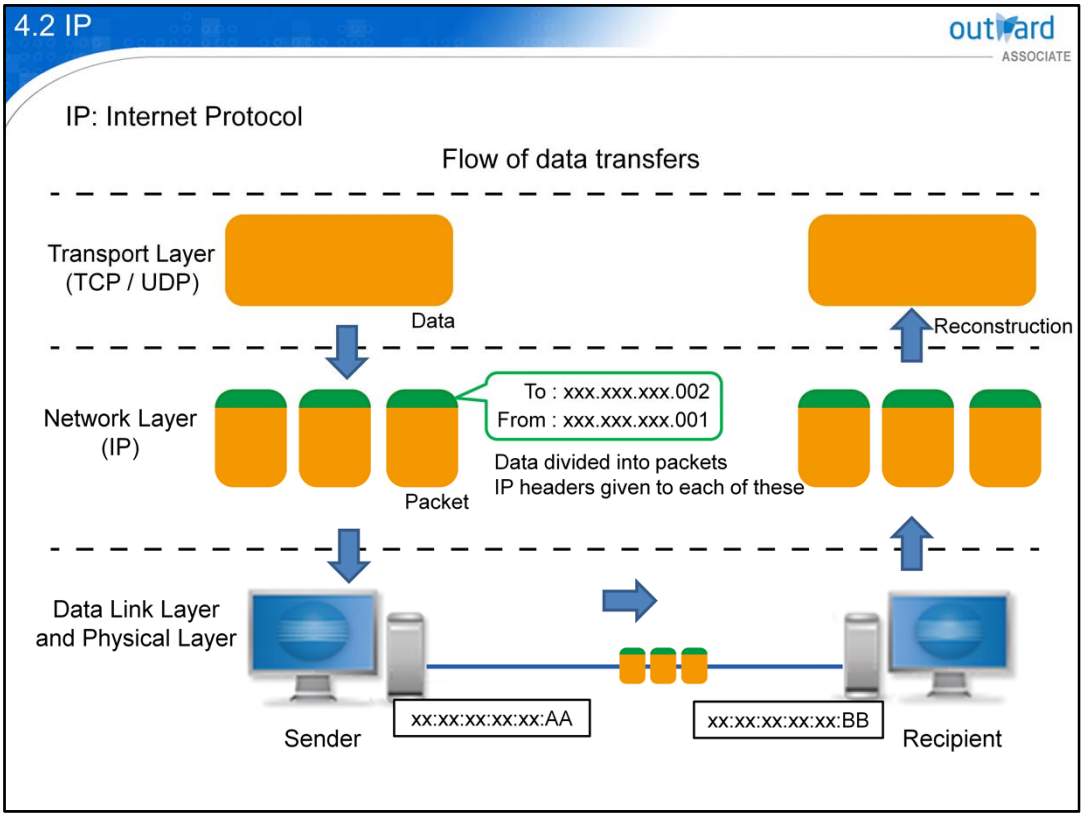
Protocols are sets of rules that govern the overall network communication process.
Just as it is impossible to have a conversation if you speak different languages, communication is not possible if different protocols are supported.
Protocols can be divided into hardware and communication protocols.
Hardware protocols determine standards for network hardware devices to maximize compatibility when modifying networks with new pieces of hardware.
Communication protocols govern the rules about how a communication session should be set up, carried out and terminated.
This lesson introduces the OSI reference model used as a standard for considering protocols and explains details on communication protocols concerning IP, TCP/UDP, Bonjour and NetBIOS/NetBEUI.

Протоколы - это наборы правил, которые управляют всем процессом взаимодействия с сетью.
Так же, как невозможно разговаривать, если вы говорите на разных языках, общение невозможно, если поддерживаются разные протоколы.
Протоколы можно разделить на аппаратные и коммуникационные протоколы.
Аппаратные протоколы определяют стандарты для сетевых аппаратных устройств, чтобы максимизировать совместимость при модификации сетей с помощью нового оборудования.
Протоколы связи определяют правила о том, как сеанс связи должен быть установлен, проведен и завершен.
Этот урок знакомит с эталонной моделью OSI, используемой в качестве стандарта для рассмотрения протоколов, и объясняет детали протоколов связи, касающихся IP, TCP / UDP, Bonjour и NetBIOS / NetBEUI.



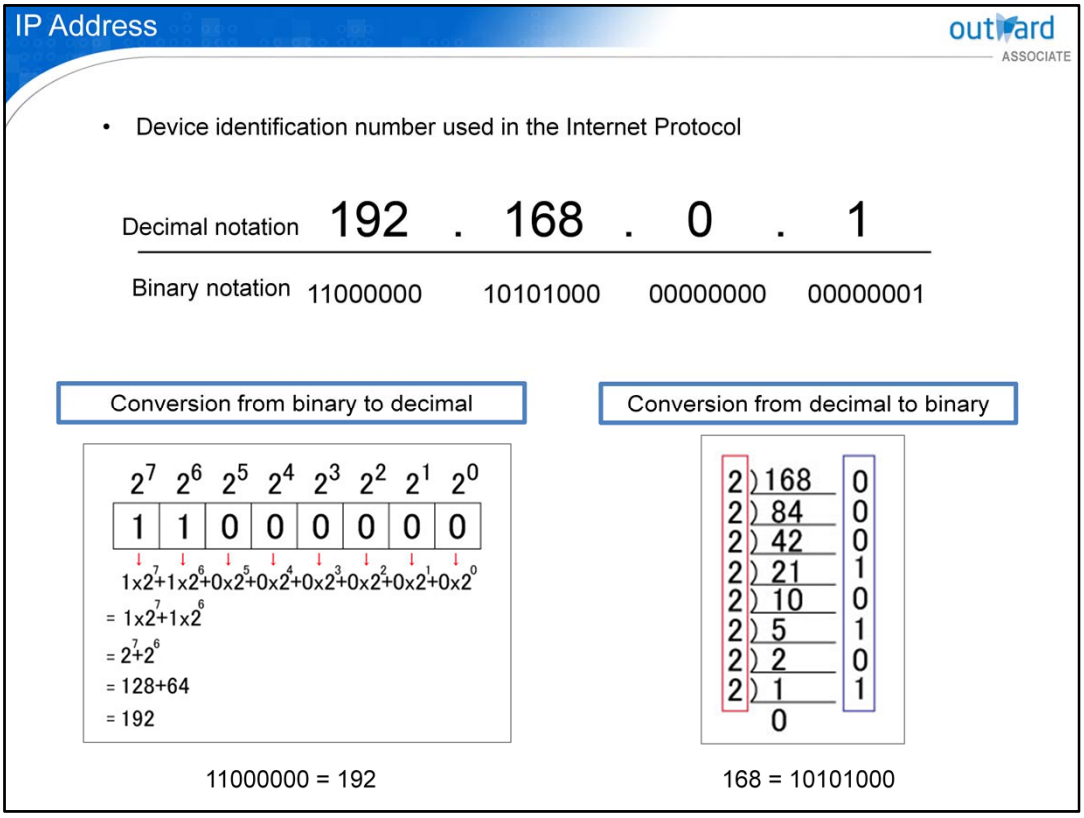
ISO, an organization that develops industry standards, developed the OSI standard.
ISO provides a performance standard to allow the flexibility to add and replace network devices independent of the vendor.
OSI is a model only, and reflects a way of looking at things rather than hard and fast rules, but it is accepted as a standard way of understanding networks. The table shows the OSI reference model, its content, and the related software and standards.
OSI specifies 7 layers of protocols that communicating systems should adopt.
They are the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.
Each layer's protocol is written so that it works together with the protocol above and directly below it.
When two different operating systems are communicating with each other, each layer communicates with the corresponding layer in the other system.

ISO, организация, которая разрабатывает отраслевые стандарты, разработала стандарт OSI.
ISO предоставляет стандарт производительности, позволяющий гибко добавлять и заменять сетевые устройства независимо от поставщика.
OSI является только моделью и отражает взгляд на вещи, а не жесткие и быстрые правила, но он принят как стандартный способ понимания сетей. В таблице приведены эталонная модель OSI, ее содержание, а также соответствующее программное обеспечение и стандарты.
OSI определяет 7 уровней протоколов, которые должны принимать взаимодействующие системы.
Это физический уровень, канальный уровень, сетевой уровень, транспортный уровень, сеансовый уровень, уровень представления и прикладной уровень.
Протокол каждого уровня написан так, чтобы он работал вместе с протоколом выше и непосредственно под ним.
Когда две разные операционные системы связываются друг с другом, каждый уровень связывается с соответствующим уровнем в другой системе.



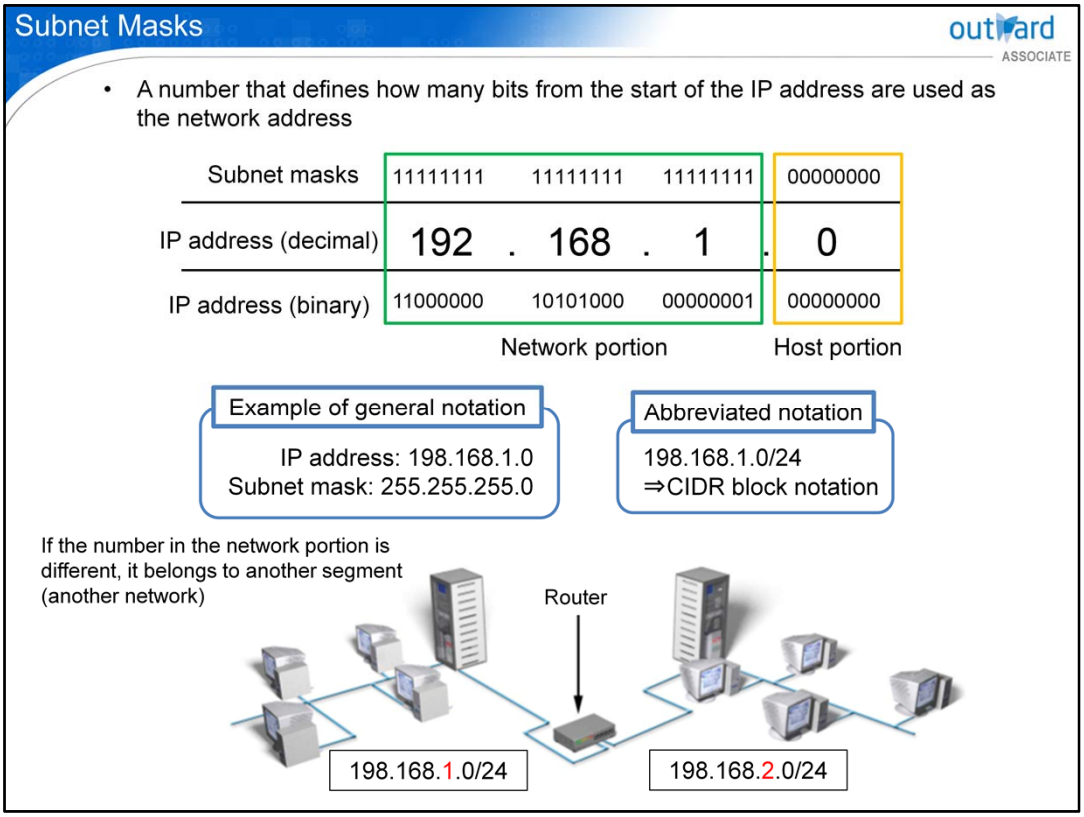
IP is an abbreviation for Internet Protocol, and plays an extremely important role in today's networks.
First, IP divides data into the packets that are the basic unit of communication.
After that, IP transfers data by delivering these to the lower data link layer after adding an IP header containing the address information.
The recipient side reconstructs the packet and sends it to the transport layer.
A packet is made up of the IP header containing information on the data's destination and source, and the payload storing the content being communicated. The destination and source information in the IP header is specified by the IP address mentioned later.

IP является аббревиатурой от интернет-протокола и играет чрезвычайно важную роль в современных сетях.
Во-первых, IP делит данные на пакеты, которые являются основной единицей связи.
После этого IP передает данные, доставляя их на нижний уровень канала передачи данных после добавления заголовка IP, содержащего информацию об адресе.
Сторона получателя восстанавливает пакет и отправляет его на транспортный уровень.
Пакет состоит из IP-заголовка, содержащего информацию о назначении и источнике данных, а также о полезной нагрузке, хранящей передаваемый контент.
Информация о назначении и источнике в заголовке IP указывается с помощью IP-адреса, упомянутого ниже.



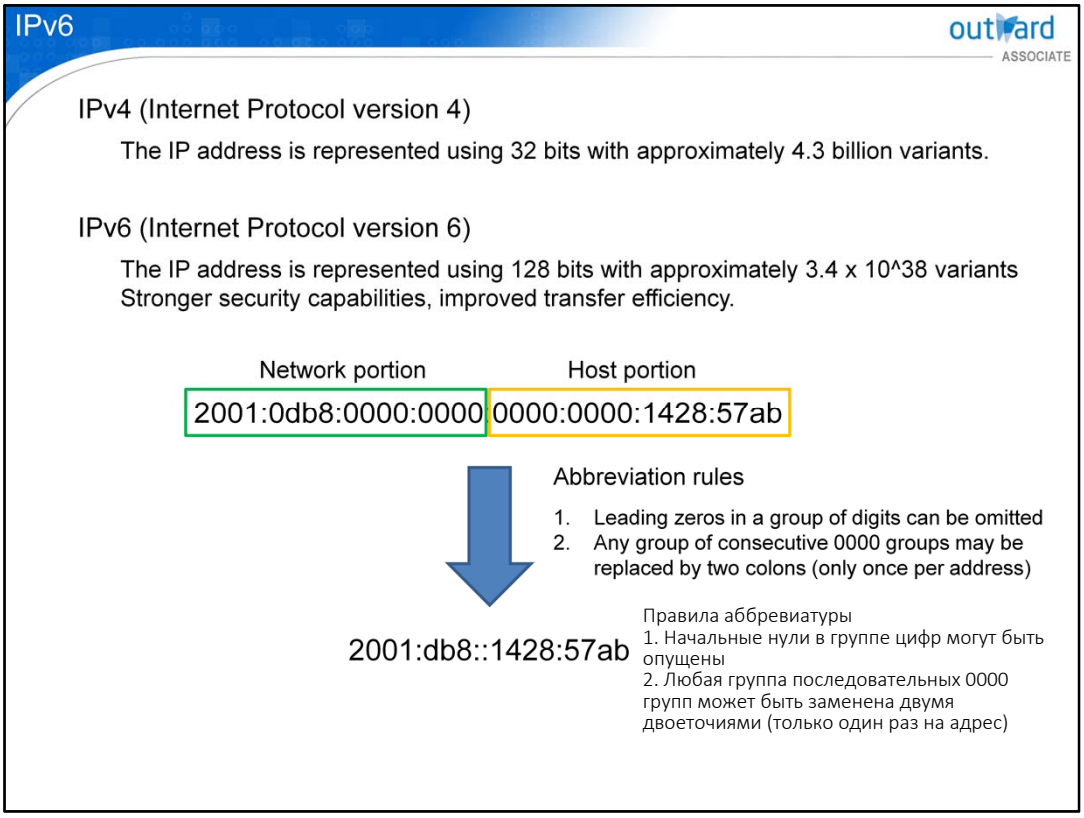
An IP address is an identification number in the network layer specified for identifying devices on the network under the Internet Protocol.
Whereas the MAC address in the data link layer is called the physical address, this is called the logical address.
In IPv4, which is currently the prevailing protocol, the IP address is a 32-bit integer.
To make this easier to understand, it is divided into four sets of 8 bits divided by dots expressed in dotted decimal notation. This conversion can be calculated. The conversion from binary to decimal is calculated using the sum of the weights of each binary digit.
The conversion from decimal to binary is obtained by continuing to divide the decimal number by two and obtaining the quotient and remainder until the quotient is zero. The remainders obtained are the result of conversion into binary.

IP-адрес - это идентификационный номер на сетевом уровне, указанный для идентификации устройств в сети по интернет-протоколу.
В то время как MAC-адрес на канальном уровне называется физическим адресом, он называется логическим адресом.
В IPv4, который в настоящее время является преобладающим протоколом, IP-адрес представляет собой 32-разрядное целое число.
Чтобы это было легче понять, он разделен на четыре набора по 8 бит, разделенных точками в десятичной записи с точками. Это преобразование может быть рассчитано.
Преобразование из двоичной системы в десятичную рассчитывается с использованием суммы весов каждой двоичной цифры.
Преобразование из десятичной в двоичную получается путем продолжения деления десятичного числа на два и получения коэффициента и остатка до тех пор, пока коэффициент не станет равным нулю. Полученные остатки являются результатом преобразования в двоичный файл.



The subnet mask is a 32-bit number that defines how many bits from the start of the IP address are used as the network address.
If the subnet mask is defined as follows, the first 24 bits are the network portion and the last 8 bits are the host portion. There are two main ways to represent this, and the most common is to state both the IP address and subnet mask. This is the notation system that is based on Classless Inter Domain Routing, so it is called CIDR notation.
However, simplified notation can also be used because it is only necessary to specify how many bits of the subnet mask to fill with ones.
If the network portion is different, this is treated as belonging to a different network, and it is necessary to pass through a router, and so on, to communicate. To use an analogy, the network portion represents the country, and the host portion represents the address within the country.

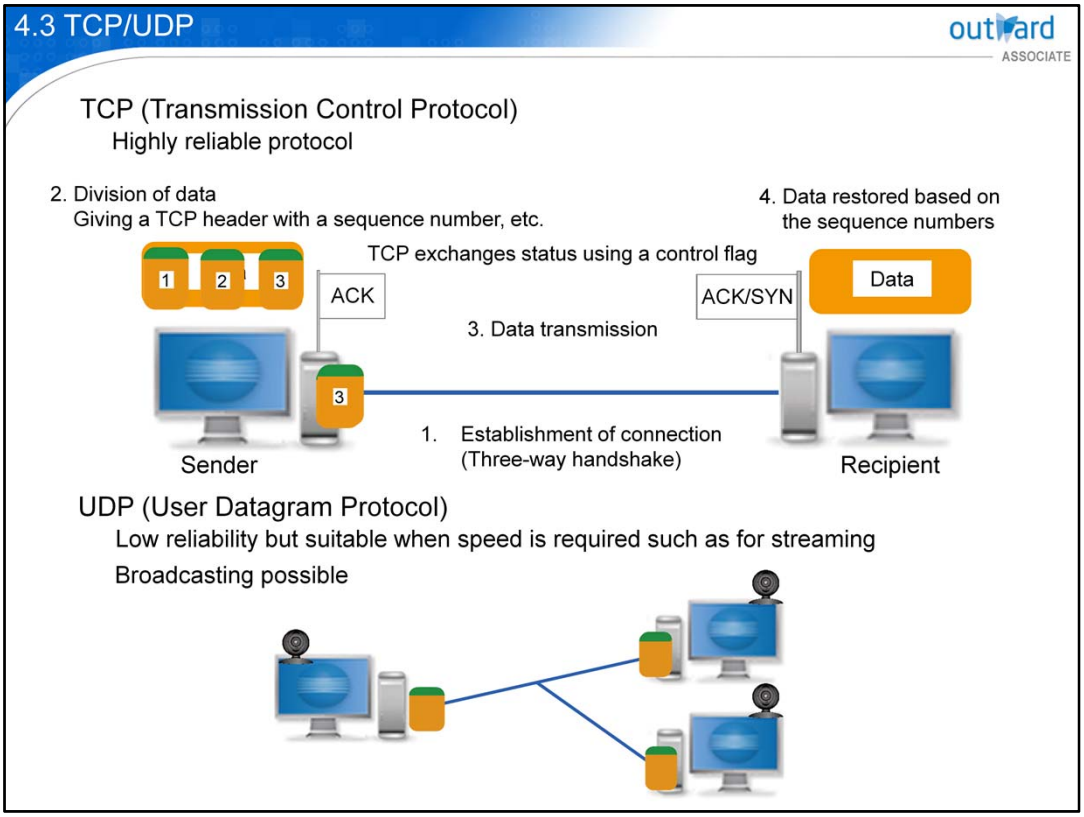
Маска подсети - это 32-разрядное число, которое определяет, сколько битов с начала IP-адреса используются в качестве сетевого адреса.
Если маска подсети определена следующим образом, первые 24 бита являются сетевой частью, а последние 8 бит являются хост-частью. Существует два основных способа представления этого, и наиболее распространенным является указание как IP-адреса, так и маски подсети. Эта система обозначений основана на бесклассовой междоменной маршрутизации, поэтому она называется нотацией CIDR.
Однако можно также использовать упрощенную систему обозначений, поскольку необходимо только указать, сколько битов маски подсети следует заполнить.
Если сетевая часть отличается, это рассматривается как принадлежащий другой сети, и для связи необходимо пройти через маршрутизатор и т. Д. Чтобы использовать аналогию, часть сети представляет страну, а часть узла представляет адрес внутри страны.



The IP addresses mentioned until now are called IPv4. The IP address is represented using 32 bits and is able to identify approximately 4.3 billion devices.
However, the rapid spread of the Internet has led to fears of depletion of these IP addresses in future.
In response to this, it is scheduled to be replaced by IPv6 as a new standard.

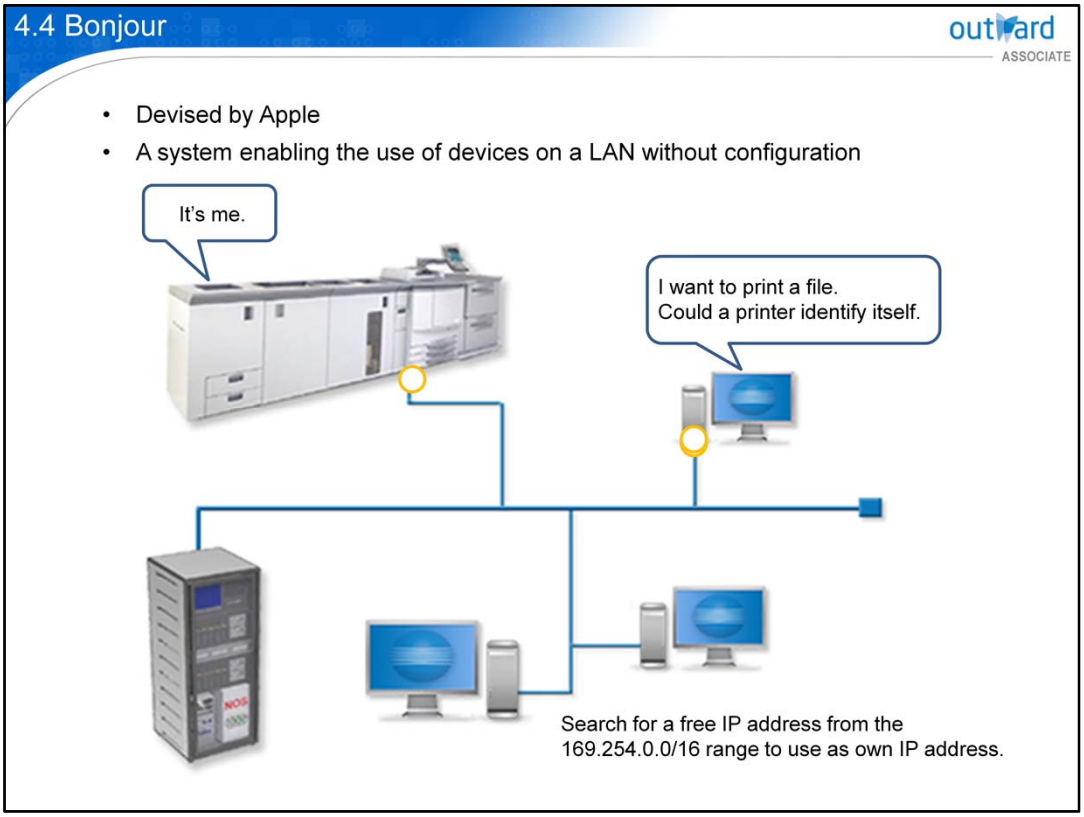
IPv6 is represented using 128 bits, and approximately 3.4×10^38, or 2^{128} addresses can be used.
In addition, improvements have been made such as stronger security through IPSec and so on, and increased transfer efficiency.
IPv6 notation is hexadecimal and divided into 16-bit sections by semicolons.
The first 64 bits are the network portion and the past 64 bits are the host portion, and in contrast to IPv4, this division does not change.
Because IPv6 addresses are very long and tend to have many zeros, they can be abbreviated according to certain rules.
However, it must be noted that there is some variation in notation even when these rules are followed.

IP-адреса, упомянутые до сих пор, называются IPv4. IP-адрес представлен с использованием 32 битов и способен идентифицировать приблизительно 4,3 миллиарда устройств.
Однако быстрое распространение интернета привело к опасениям истощения этих IP-адресов в будущем.
В ответ на это планируется заменить IPv6 в качестве нового стандарта.
IPv6 представлен с использованием 128 битов, и можно использовать приблизительно 3,4 × 10 ^ 38 или 2^{128} адресов.
Кроме того, были внесены улучшения, такие как усиление безопасности с помощью IPSec и т. Д., А также повышение эффективности передачи.
Обозначение IPv6 является шестнадцатеричным и разделено на 16-битные разделы точкой с запятой.
Первые 64 бита являются частью сети, а последние 64 бита являются частью хоста, и в отличие от IPv4 это разделение не изменяется.
Поскольку адреса IPv6 очень длинные и имеют много нулей, их можно сокращать в соответствии с определенными правилами.
Тем не менее, следует отметить, что существуют некоторые различия в обозначениях, даже если эти правила соблюдаются.



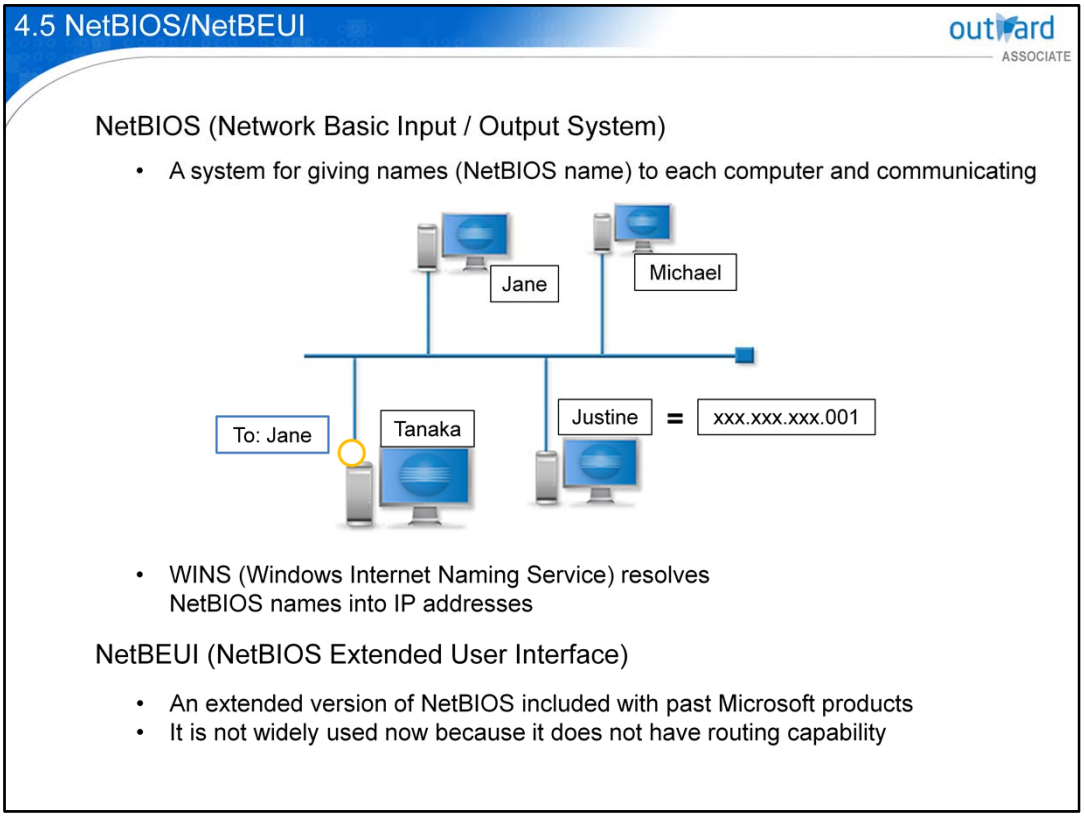
TCP and UDP are both transport layer protocols, and bridge data via IP in the network layer and protocols in the session layer and higher.
TCP is a highly reliable protocol that transfers data while exchanging information called control flags to confirm receipt, or others.
When commencing communication, the connection is established between the sending and receiving devices using a procedure called a three-way handshake.
After the connection is established, the data is divided and given TCP headers including sequence numbers, and delivered to the network layer to be communicated.
The recipient restores the data by rearranging it based on the sequence numbers, enabling highly reliable data transfer. UDP does not perform confirmation as TCP does, and does not guarantee the reliability of data.
However, it is suitable for situations that need speed and real-time access more than reliability, such as streaming playback.
In addition, TCP always uses 1:1 communication to establish connections, but UDP is able to broadcast, making it the perfect protocol for telephony and videoconferencing systems.

TCP и UDP являются протоколами транспортного уровня и обеспечивают передачу данных через IP на сетевом уровне и протоколы на уровне сеанса и выше.
TCP является высоконадежным протоколом, который передает данные во время обмена информацией, называемой контрольными флагами для подтверждения получения или другими.
При начале связи между отправляющим и принимающим устройствами устанавливается соединение с использованием процедуры, называемой трехсторонним рукопожатием.
После установления соединения данные разделяются и получают заголовки TCP, включая порядковые номера, и доставляются на сетевой уровень для передачи.
Получатель восстанавливает данные, переставляя их на основе порядковых номеров, обеспечивая высокую надежность передачи данных. UDP не выполняет подтверждение, как TCP, и не гарантирует надежность данных.
Тем не менее, он подходит для ситуаций, когда скорость и доступ в реальном времени больше, чем надежность, например потоковое воспроизведение.
Кроме того, TCP всегда использует связь 1: 1 для установления соединений, но UDP способен транслировать, что делает его идеальным протоколом для систем телефонии и видеоконференций.



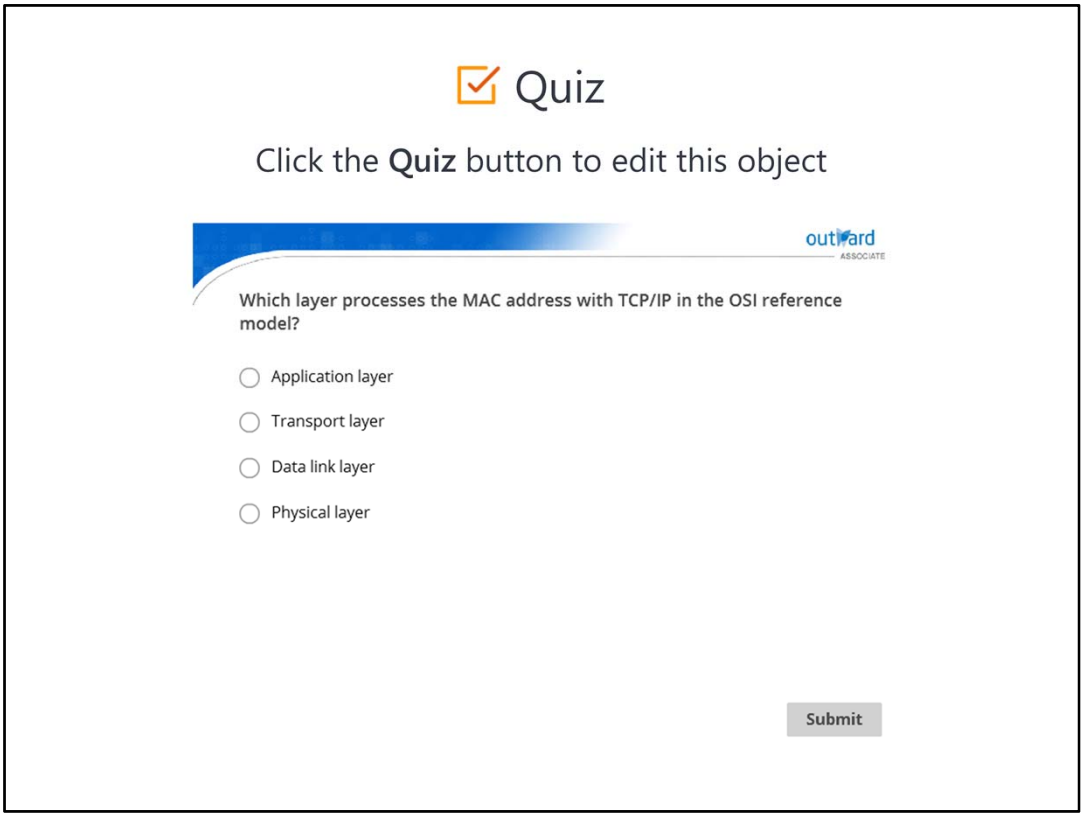
Bonjour is a network technology not requiring configuration that was devised by Apple. It is mainly used in LANs to use devices without the need for any configuration.
The main functions are automatic assignment of IP addresses and host names, and automatically searching for services.
Devices connected to a Bonjour network do not need a DHCP server or a DNS server.
Bonjour is used for both Ethernet and Wireless connections, however, our equipment mainly uses it for wireless purposes. When devices are connected, they search for a free IP address from the 169.254.0.0/16 range to use as their own IP address.
Another characteristic is that all devices connected to the network are queried for their host names, and connections are made to the matching host name.
For example, if you wish to print something, a query about whether there are any devices providing print services is made over the LAN by multicast. Only the relevant devices respond, enabling communication to take place.
Normally, to reduce load, host information is cached instead of multicasting every time.

Bonjour - это сетевая технология, не требующая настройки, разработанная Apple. Он в основном используется в локальных сетях для использования устройств без какой-либо конфигурации.
Основными функциями являются автоматическое назначение IP-адресов и имен хостов, а также автоматический поиск сервисов.
Устройствам, подключенным к сети Bonjour, не требуется DHCP-сервер или DNS-сервер.
Bonjour используется как для Ethernet, так и для беспроводных подключений, однако наше оборудование в основном использует его для беспроводных целей. Когда устройства подключены, они ищут свободный IP-адрес из диапазона 169.254.0.0/16 для использования в качестве своего собственного IP-адреса.
Другая характеристика заключается в том, что все устройства, подключенные к сети, запрашивают свои имена хостов, а соединения устанавливаются с соответствующим именем хоста.
Например, если вы хотите что-то напечатать, запрос о наличии каких-либо устройств, предоставляющих услуги печати, выполняется по локальной сети посредством многоадресной рассылки. Отвечают только соответствующие устройства, позволяющие установить связь.
Обычно, чтобы уменьшить нагрузку, информация о хосте кэшируется вместо многоадресной рассылки каждый раз.

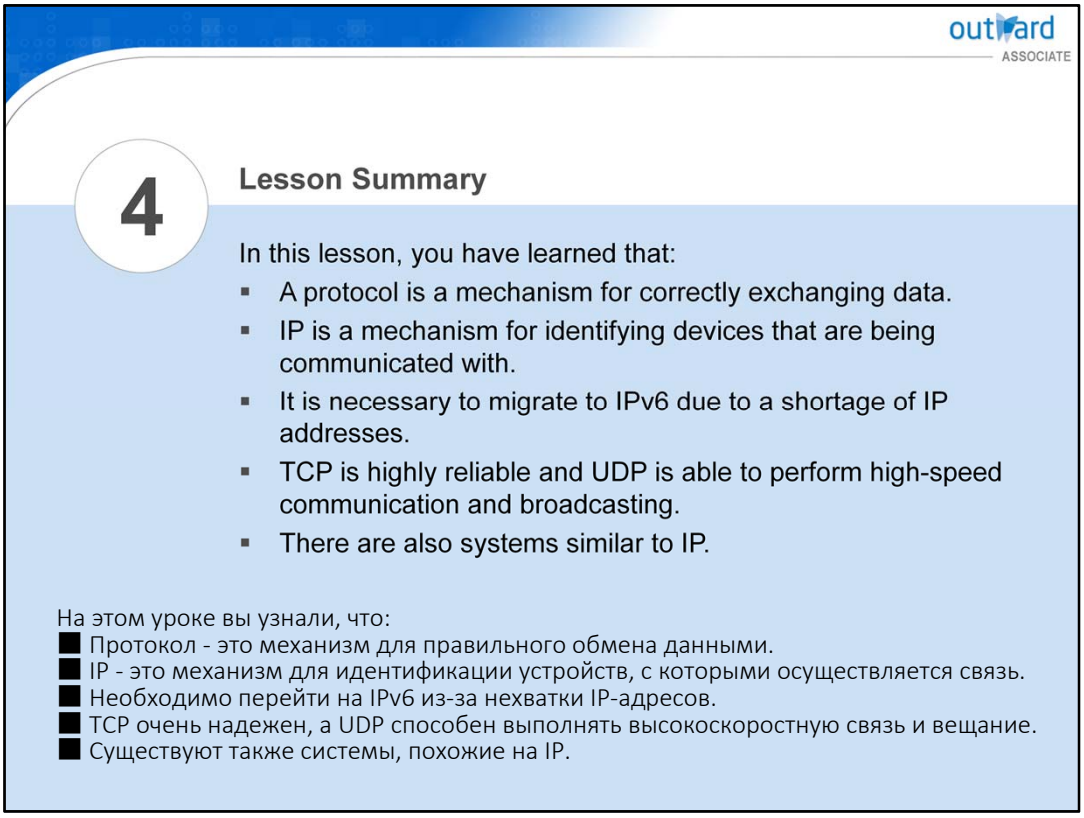


NetBIOS is a system enabling small-scale communication based on the names given to each computer by users. NetBIOS defines the fundamental configuration of how data is passed in and out of workstations within a LAN, and it operates at the Session layer of the OSI model.
NetBIOS's API provides a common interface between applications and the underlying network operating system for the purpose of transmitting messages between nodes. Furthermore, NetBIOS functions can be used through TCP/IP. When doing so, the NetBIOS name is mapped to an IP address by WINS.
NetBEUI is an extended version of NetBIOS which has become the industry standard as part of a network's general communication protocol.
It was supplied with Microsoft's LAN Manager, Windows for Workgroups, and Windows NT.
It is generally used only in small networks because it has no routing capability.

NetBIOS - это система, обеспечивающая мелкомасштабную связь на основе имен, данных каждому компьютеру пользователями. NetBIOS определяет фундаментальную конфигурацию того, как данные передаются на рабочие станции и из них в локальной сети, и работает на уровне сеансов модели OSI.
API-интерфейс NetBIOS обеспечивает общий интерфейс между приложениями и базовой сетевой операционной системой для передачи сообщений между узлами. Кроме того, функции NetBIOS можно использовать через TCP / IP. При этом имя NetBIOS сопоставляется с IP-адресом WINS.
NetBEUI - это расширенная версия NetBIOS, которая стала отраслевым стандартом как часть общего сетевого протокола связи.
Он был поставлен с LAN Manager от Microsoft, Windows для рабочих групп и Windows NT.
Обычно он используется только в небольших сетях, поскольку не имеет возможности маршрутизации.

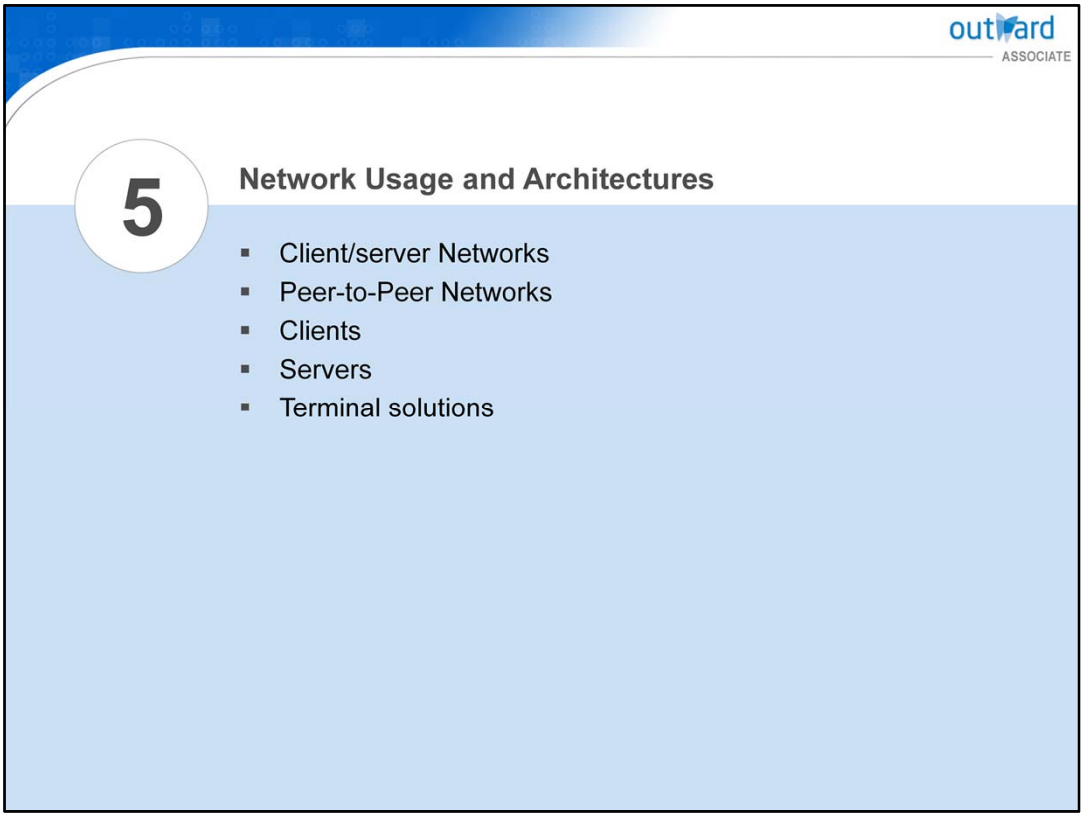


Test your knowledge in a quiz!



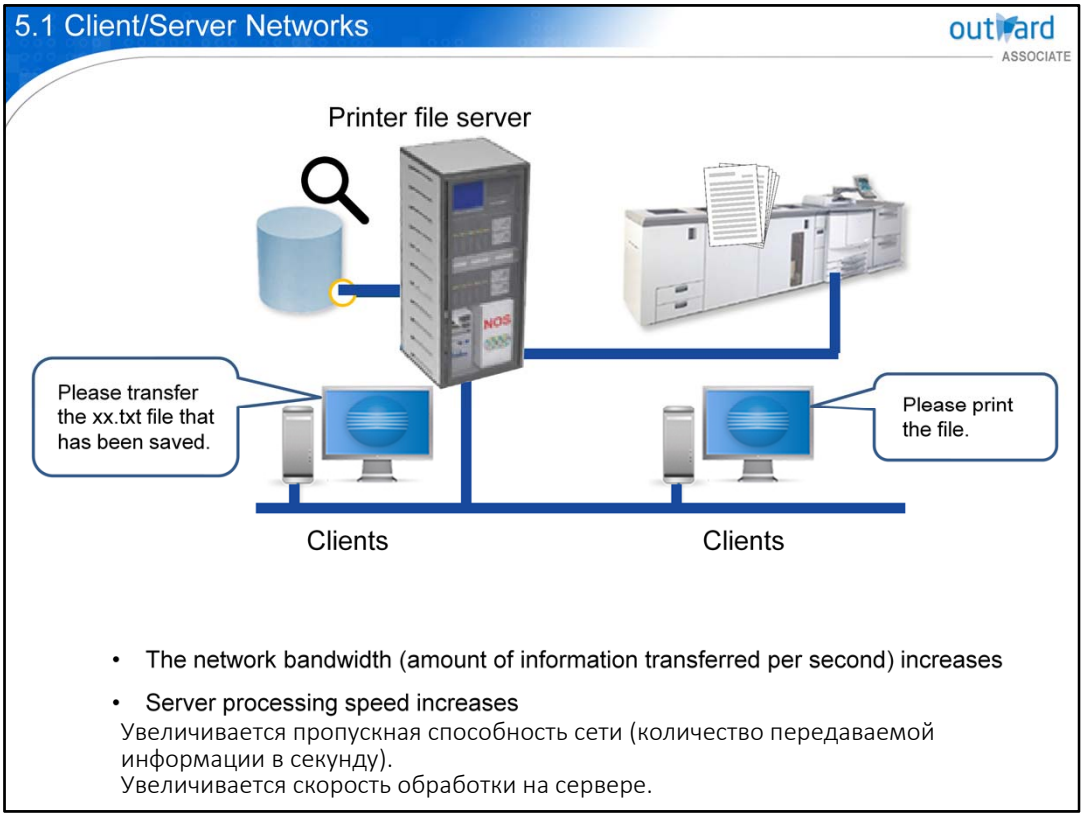
Protocols are rules for communicating with each other, and communication is made possible by adding a variety of information to data being transferred through multiple protocols.
IP serves the role of identifying the nodes communicating on a network with many nodes.
Now, there are concerns about a shortage of IP addresses due to network advances, and it will be necessary to migrate to the IPv6 system in the near future.
TCP and UDP are protocols on the same network layer, but their applications differ greatly.
Whereas the objective of TCP is to correctly transfer data, the objective of UDP is to transfer data at high speed in multiple directions.
Now, IP is used in most networks, but there are also systems such as NetBIOS that are not reliant on IP addresses.

Протоколы - это правила общения друг с другом, и связь становится возможной благодаря добавлению разнообразной информации к данным, передаваемым по нескольким протоколам.
IP выполняет роль идентификации узлов, взаимодействующих в сети со многими узлами.
Теперь существуют опасения по поводу нехватки IP-адресов из-за расширений сети, и в ближайшем будущем необходимо будет перейти на систему IPv6.
TCP и UDP являются протоколами на одном сетевом уровне, но их приложения сильно различаются.
В то время как целью TCP является правильная передача данных, целью UDP является передача данных с высокой скоростью в нескольких направлениях.
Теперь IP используется в большинстве сетей, но есть также системы, такие как NetBIOS, которые не зависят от IP-адресов.



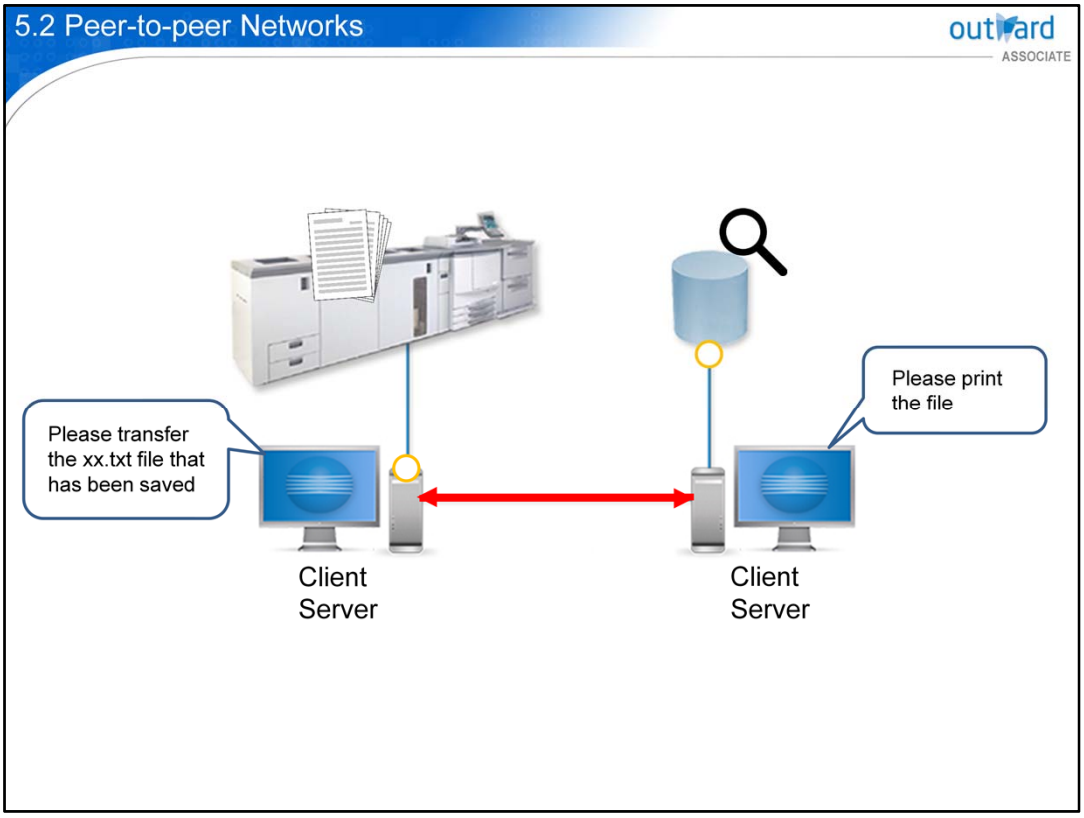
There is a lot of network usage and architectures.
This lesson introduces the model of client/server networks and peer-to-peer networks.
Plus, this lesson describes the roles of servers and clients used for the effective utilization of networks.

Существует много использования сети и архитектуры.
Этот урок представляет модель клиент-серверных сетей и одноранговых сетей.
Кроме того, в этом уроке описываются роли серверов и клиентов, используемые для эффективного использования сетей.



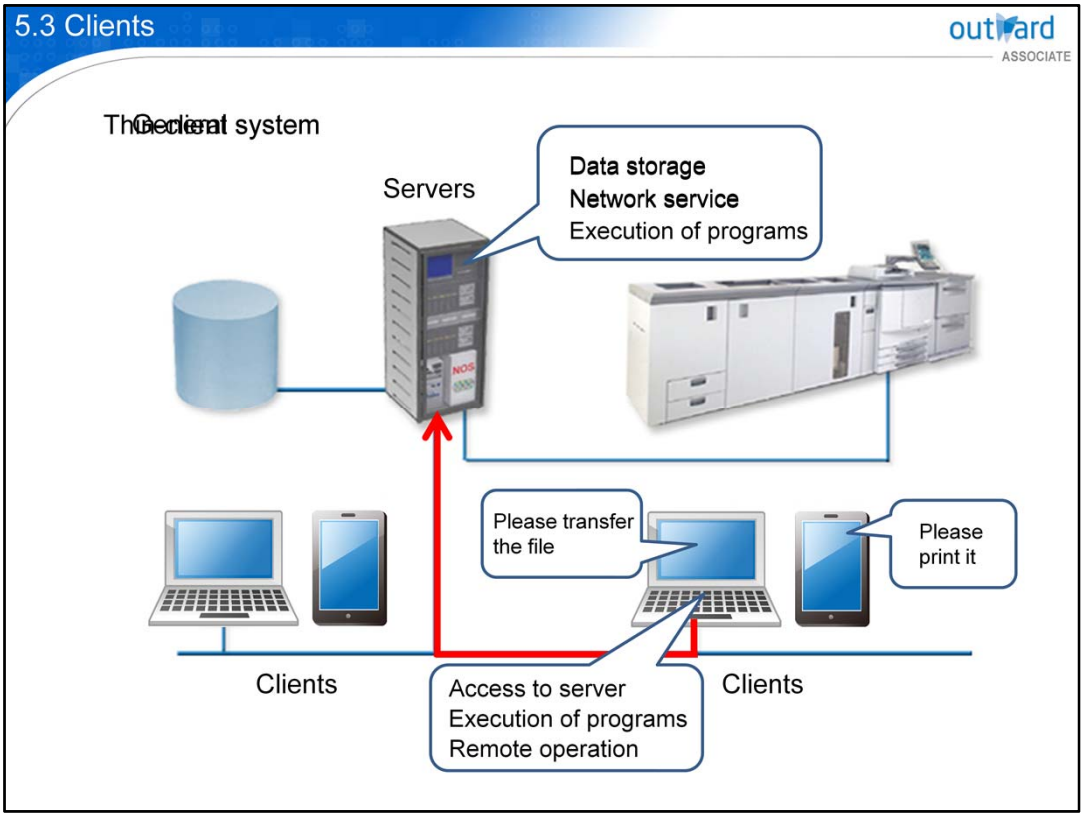
The majority of substantial business network installations are client/server systems.
In this type of network, services such as printing and file storage and retrieval are centralized and managed by a program called a server.
There are various types of servers. Print servers manage print requests and file servers handle the storage and retrieval of data.
The advantages of client/server networks are efficient use of network resources.
This topology also helps keep the network environment consistent and under control and offers ease of management. However, by introducing a client/server network, the user can expect an increase in network traffic and slower response times.
In this case, this can be minimized by increasing network bandwidth or by increasing the server processing speed.

Большинство существенных установок бизнес-сети - системы клиент / сервер.
В сети такого типа такие службы, как печать, хранение и извлечение файлов, централизованы и управляются программой, называемой сервером.
Существуют различные типы серверов. Серверы печати управляют запросами на печать, а файловые серверы управляют хранением и поиском данных.
Преимуществами клиент-серверных сетей являются эффективное использование сетевых ресурсов.
Эта топология также помогает поддерживать целостность и контроль сетевой среды и обеспечивает простоту управления. Однако, введя клиент-серверную сеть, пользователь может ожидать увеличения сетевого трафика и более медленного времени отклика.
В этом случае это можно минимизировать, увеличив пропускную способность сети или увеличив скорость обработки на сервере.



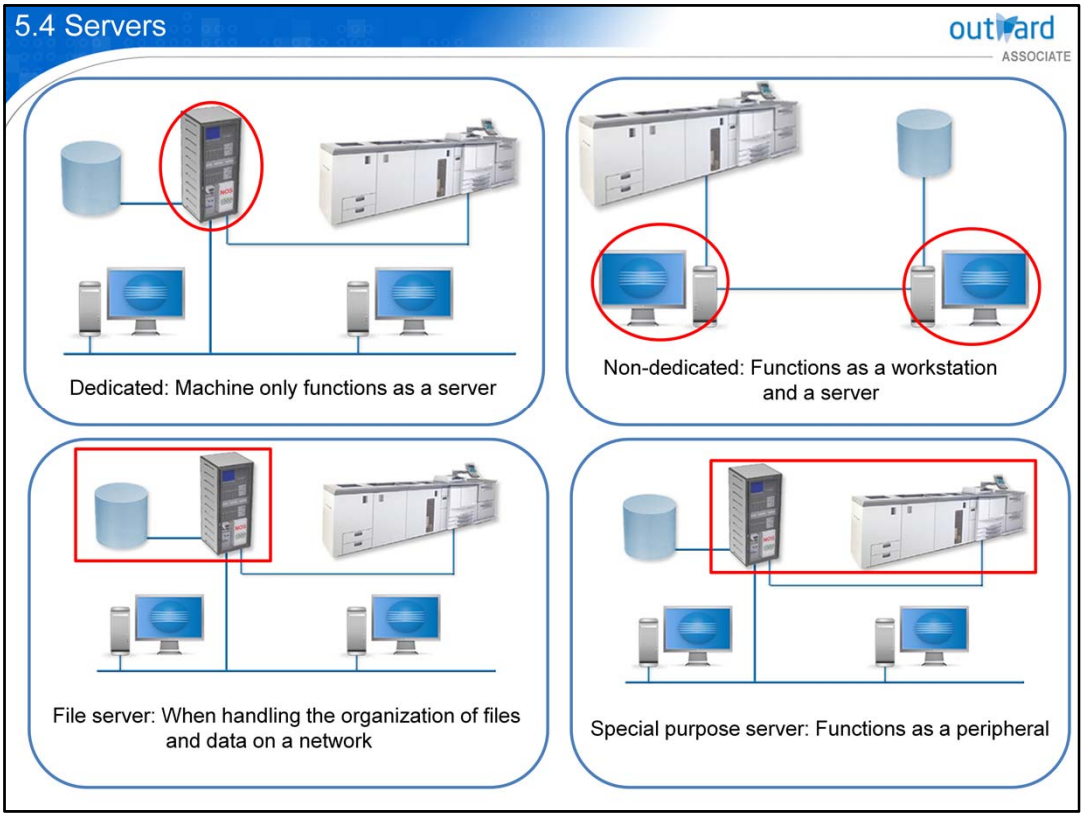
Peer-to-peer networks provide access to files, software and peripheral devices via communication between individual workstations.
Each workstation has the same network status as any other, and any workstation can initiate a communication session. In some cases, peer-to-peer communication is implemented by giving each workstation both server and client capabilities. Any workstation can behave as a server to other software and interconnect to other networks using different operating systems.
Printing is usually accomplished by either sharing a device physically connected to a workstation, or by a third party utility to share a standalone device attached to the network.

Одноранговые сети обеспечивают доступ к файлам, программному обеспечению и периферийным устройствам через связь между отдельными рабочими станциями. Каждая рабочая станция имеет тот же статус сети, что и любая другая, и любая рабочая станция может инициировать сеанс связи. В некоторых случаях одноранговая связь осуществляется путем предоставления каждой рабочей станции возможностей как сервера, так и клиента. Любая рабочая станция может вести себя как сервер для другого программного обеспечения и подключаться к другим сетям с использованием разных операционных систем.
Печать обычно выполняется путем совместного использования устройства, физически подключенного к рабочей станции, или с помощью сторонней утилиты для совместного использования автономного устройства, подключенного к сети.



In a client-server system, the client can request the server to perform tasks such as file retrieval and printing.
A workstation can function as both a client and as a server, but there are several ways to configure a client in networks with dedicated servers.
The most popular approach places all program logic in the client workstations and uses servers to store data and provide network services.
Other approaches vary the division of program logic and data stored on the server and workstations.
In a thin-client system, all storage, applications and handling of peripheral devices are provided by the server, and the clients only serve as terminals for accessing and remotely controlling the server.
Therefore, clients need not have a lot of memory or processing power, hence they are called thin.

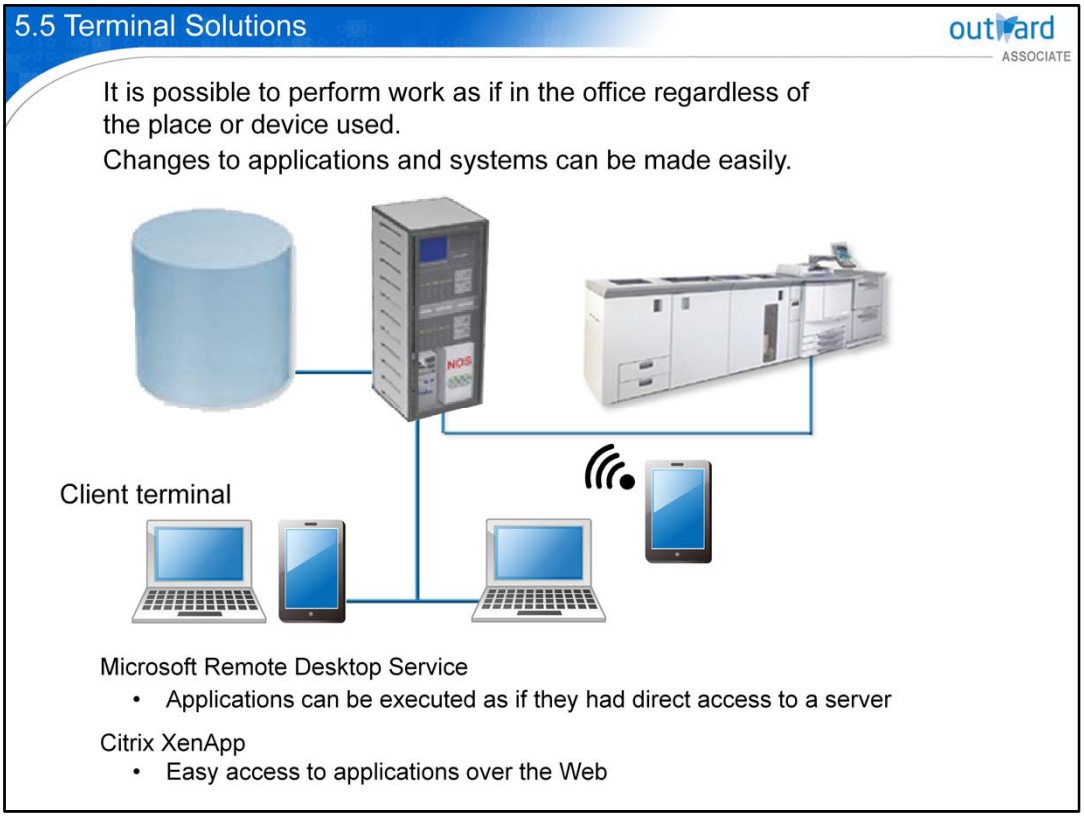
В системе клиент-сервер клиент может запросить сервер выполнить такие задачи, как поиск файла и печать.
Рабочая станция может функционировать как клиент и как сервер, но есть несколько способов настроить клиента в сетях с выделенными серверами.
Самый популярный подход размещает всю программную логику на клиентских рабочих станциях и использует серверы для хранения данных и предоставления сетевых услуг.
Другие подходы варьируют разделение программной логики и данных, хранящихся на сервере и рабочих станциях.
В системе с тонким клиентом все хранилище, приложения и обработка периферийных устройств предоставляются сервером, а клиенты служат только терминалами для доступа и удаленного управления сервером.
Поэтому клиентам не нужно много памяти или вычислительной мощности, поэтому их называют тонкими.



A dedicated server is a permanent operating server that is used for a certain task or service. This server is not used as a workstation.
For non-dedicated servers, the server software is running on a host. This server may also be used as a workstation.
A shared server is a server that may be used for different or multiple tasks or services.

Выделенный сервер - это постоянный работающий сервер, который используется для определенной задачи или службы. Этот сервер не используется в качестве рабочей станции.
Для невыделенных серверов серверное программное обеспечение работает на хосте. Этот сервер также может использоваться в качестве рабочей станции.
Общий сервер - это сервер, который может использоваться для разных или нескольких задач или услуг.

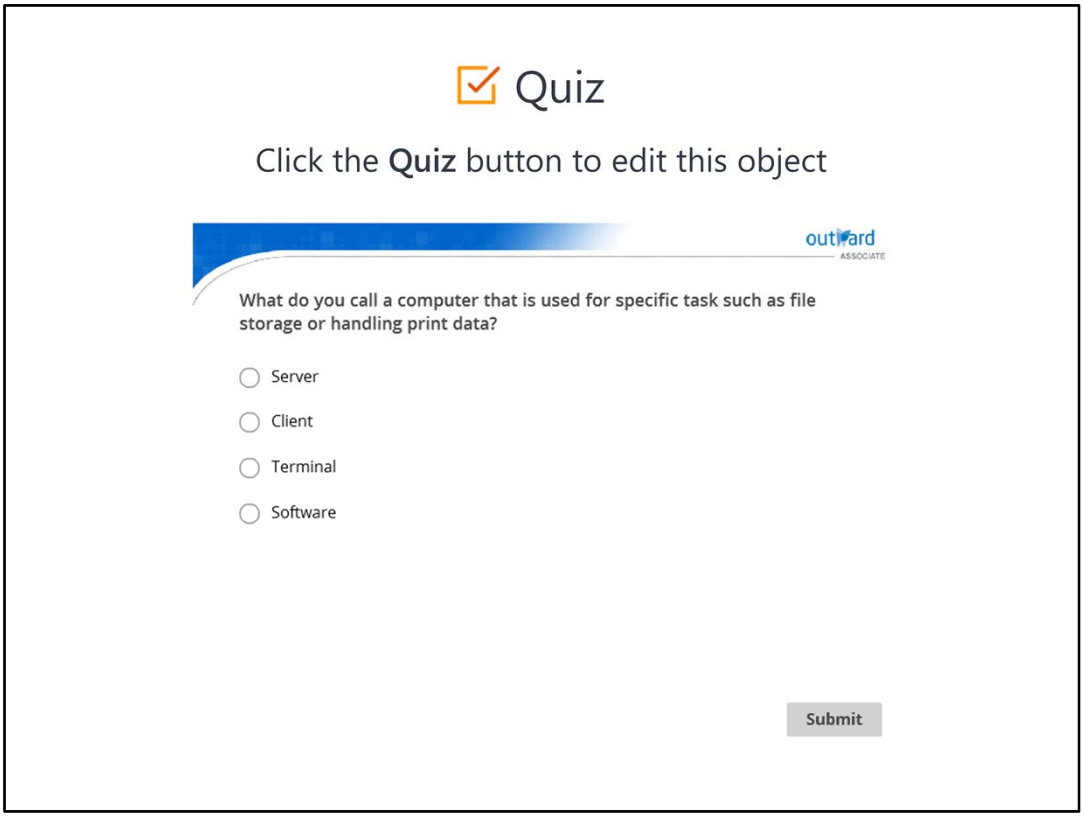
Работу можно выполнять как в офисе, независимо от места и устройства.
Изменения в приложениях и системах могут быть сделаны легко.



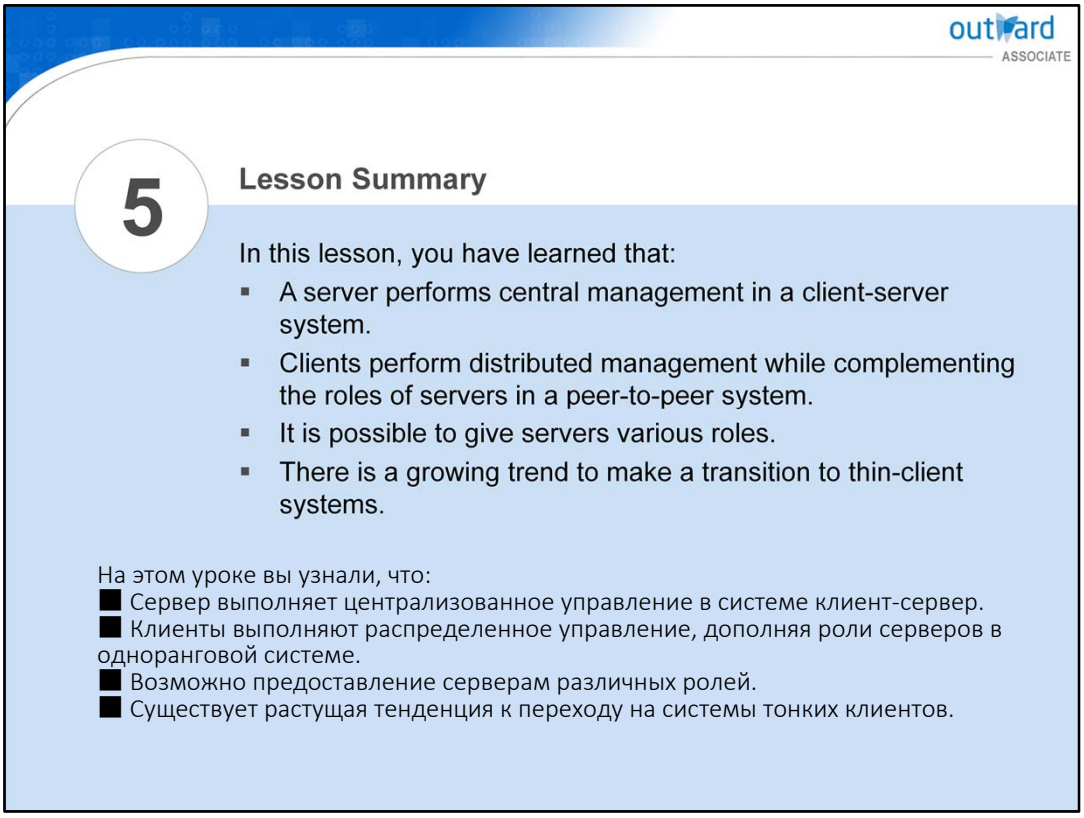
Служба удаленного рабочего стола Microsoft
• Приложения могут выполняться так, как если бы они имели прямой доступ к серверу
Citrix XenApp
• Легкий доступ к приложениям через Интернет

In the past, file management and the execution of applications was performed by the client without heavy reliance on the server.
However, recently the increase in wireless LAN speed and the emergence of tablets has led to a migration to terminal-based solutions.
For example, by virtualizing desktops and applications, it is possible to perform work as if in the office regardless of the place or device used.
In addition, by unifying computing resources, applications and systems can be updated and upgraded economically.
The use of computers in business is increasingly moving toward terminal-based thin-client systems.
Examples of terminal solutions include Microsoft Remote Desktop Service and Citrix XenApp.
Using remote desktop services, end users can execute applications as if they had direct access to a server.
The Citrix solution for remote access incorporates functions exceeding terminal services in additional products.
For example, a complete client software application is not required and access to applications can be easily requested through a Web browser.

В прошлом управление файлами и выполнение приложений выполнялись клиентом без сильной зависимости от сервера.
Однако в последнее время увеличение скорости беспроводной локальной сети и появление планшетов привело к переходу на терминальные решения.
Например, виртуализируя рабочие столы и приложения, можно выполнять работу как в офисе, независимо от места или используемого устройства.
Кроме того, объединяя вычислительные ресурсы, приложения и системы могут быть обновлены и модернизированы экономически. Использование компьютеров в бизнесе все больше переходит к системам тонких клиентов на базе терминалов.
Примеры терминальных решений включают Microsoft Remote Desktop Service и Citrix XenApp.
Используя службы удаленного рабочего стола, конечные пользователи могут выполнять приложения, как если бы они имели прямой доступ к серверу.
Решение Citrix для удаленного доступа включает функции, превосходящие терминальные сервисы, в дополнительных продуктах.
Например, полное клиентское программное приложение не требуется, и доступ к приложениям можно легко запросить через веб-браузер.

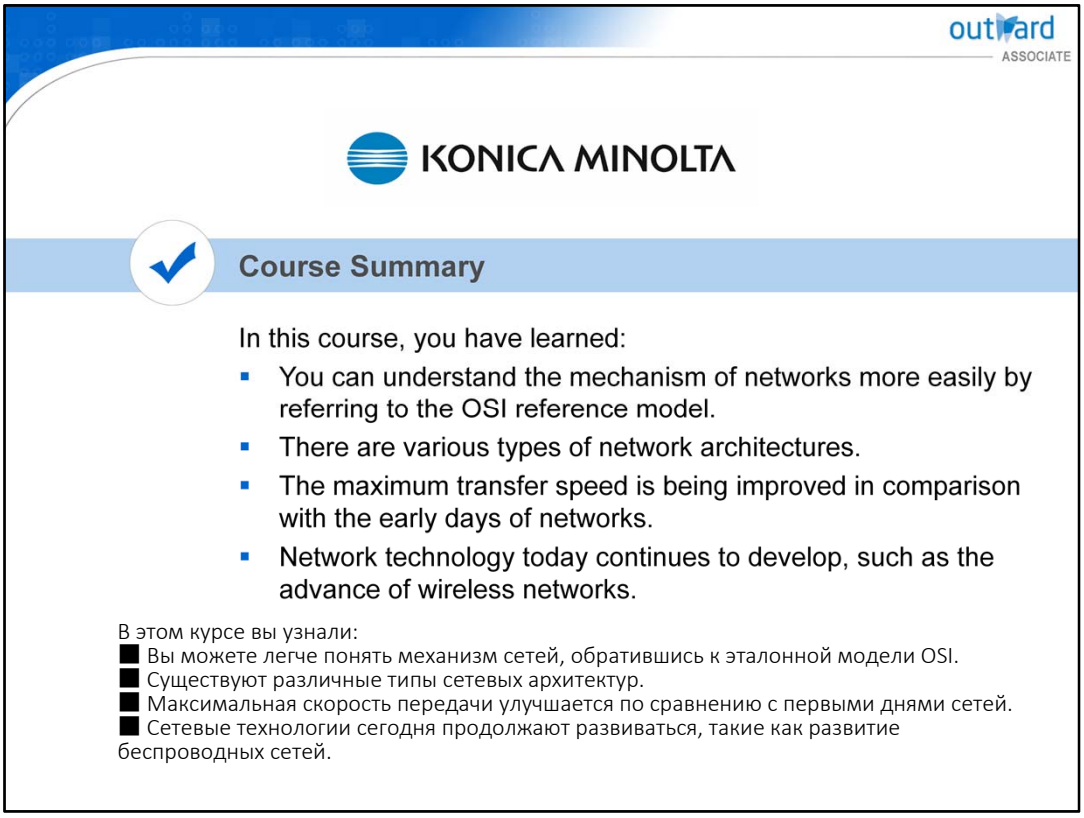


Test your knowledge in a quiz!



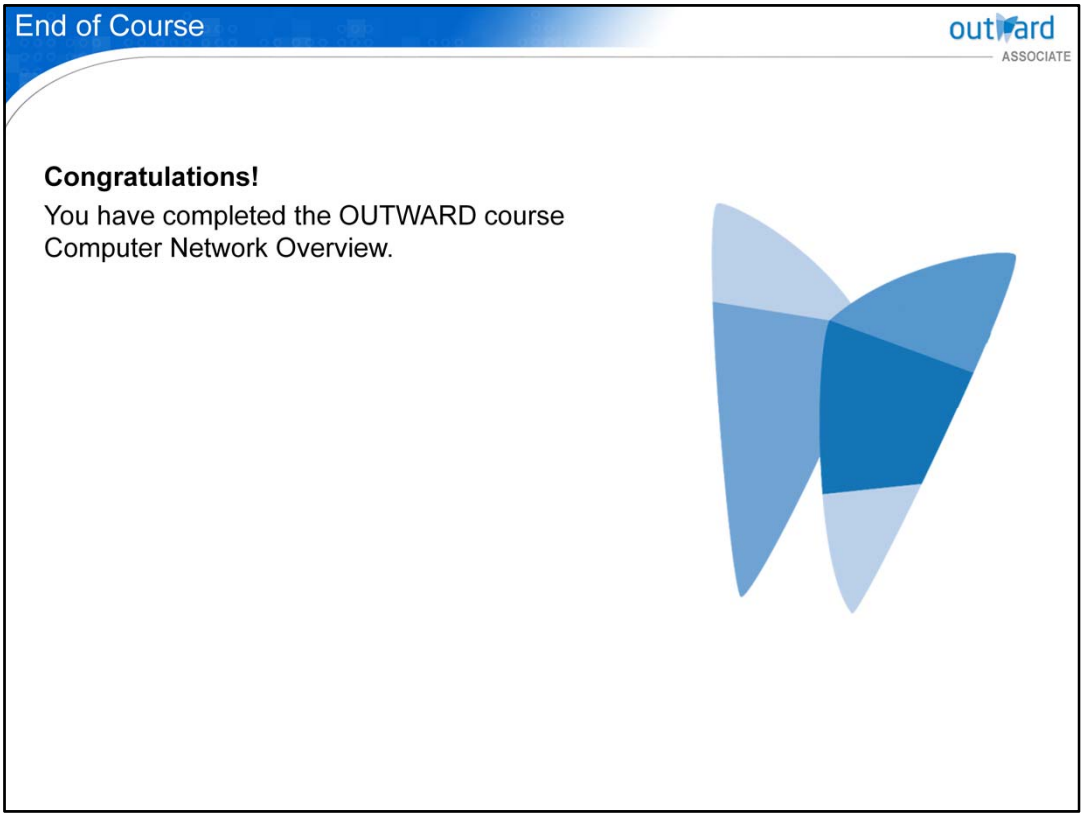
The client-server approach most commonly used by enterprises now centrally manages services such as printing and file storage and retrieval on a server. In contrast, clients are equal in a peer-to-peer system, and act as servers as required, while managing the network.
Servers not only manage files and printers, but are also able to perform actions normally handled by the client side such as execution of applications.
Now, there is a growing trend of moving toward thin-client systems in which the client terminal only plays the role of accessing data and applications.

Клиент-серверный подход, наиболее часто используемый предприятиями, теперь централизованно управляет такими службами, как печать, хранение и извлечение файлов на сервере. Напротив, клиенты равны в одноранговой системе и при необходимости управляют сетью как серверы.
Серверы не только управляют файлами и принтерами, но также могут выполнять действия, обычно выполняемые на стороне клиента, такие как выполнение приложений.
В настоящее время наблюдается тенденция к переходу на системы тонких клиентов, в которых клиентский терминал играет роль доступа к данным и приложениям.



This concludes the Computer Network Overview course. In closing, let's look back on what you have learned. Networks enable communication by combining a variety of technologies.
Each technology basically interacts with upper and lower layers, and this is easier to understand by referring to the OSI reference model.
Most of the use of networks in enterprises previously used client-server systems.
However, this is moving toward thin-client systems as the specs of servers and networks improve.
Early networks had a maximum transfer speed of around 10 Mbps despite using thick cables that were awkward to use. However, there are now Ethernet standards with a theoretical transfer speed in excess of 10 Gbps despite using thin cables.
Wireless networking is becoming more advanced with the latest standards enabling communication at Gigabit speeds, and network technologies continue to evolve.

На этом мы завершаем курс «Обзор компьютерной сети». В заключение давайте вернемся к тому, что вы узнали. Сети позволяют общаться, комбинируя различные технологии.
Каждая технология в основном взаимодействует с верхним и нижним уровнями, и это легче понять, обратившись к эталонной модели OSI.
Большая часть использования сетей на предприятиях ранее использовалась клиент-серверными системами.
Тем не менее, это движется в сторону систем тонких клиентов по мере улучшения характеристик серверов и сетей.
Ранние сети имели максимальную скорость передачи около 10 Мбит / с, несмотря на использование толстых кабелей, которые были неудобны в использовании. Тем не менее, в настоящее время существуют стандарты Ethernet с теоретической скоростью передачи более 10 Гбит / с, несмотря на использование тонких кабелей.
Беспроводные сети становятся все более современными благодаря новейшим стандартам, обеспечивающим связь на гигабитных скоростях, и сетевые технологии продолжают развиваться.



Congratulations! You have now completed the OUTWARD course "Computer Network Overview”.