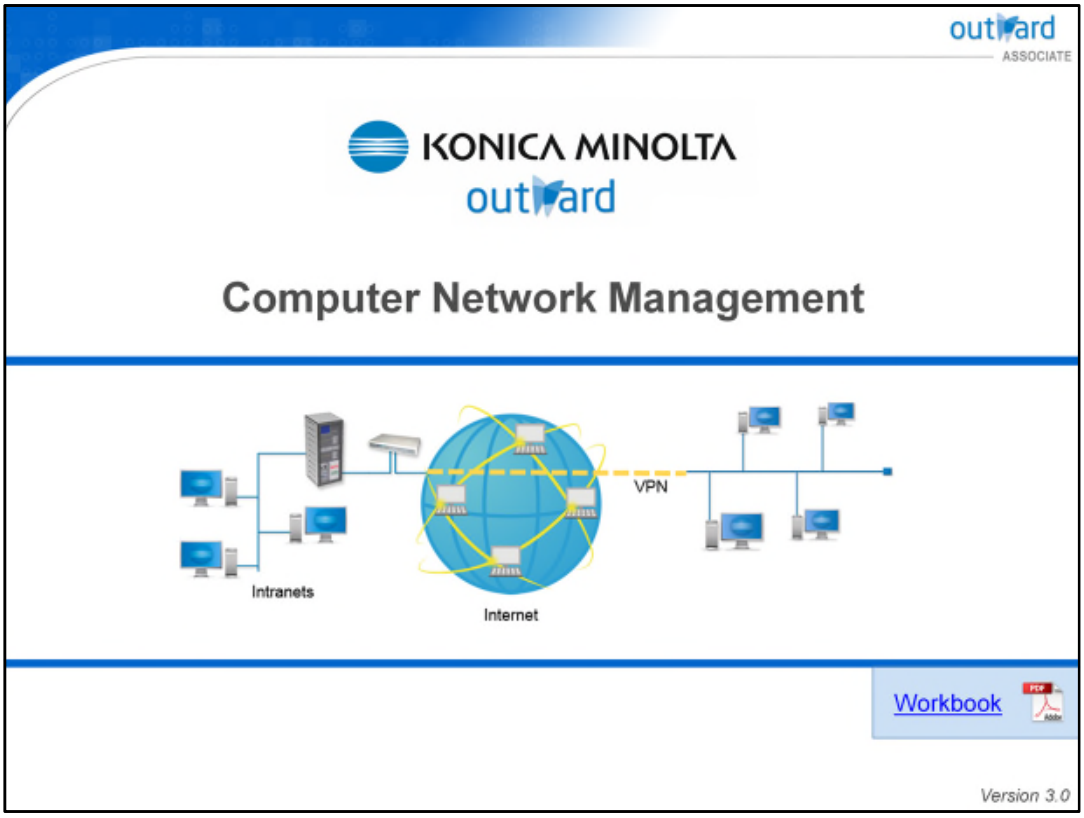
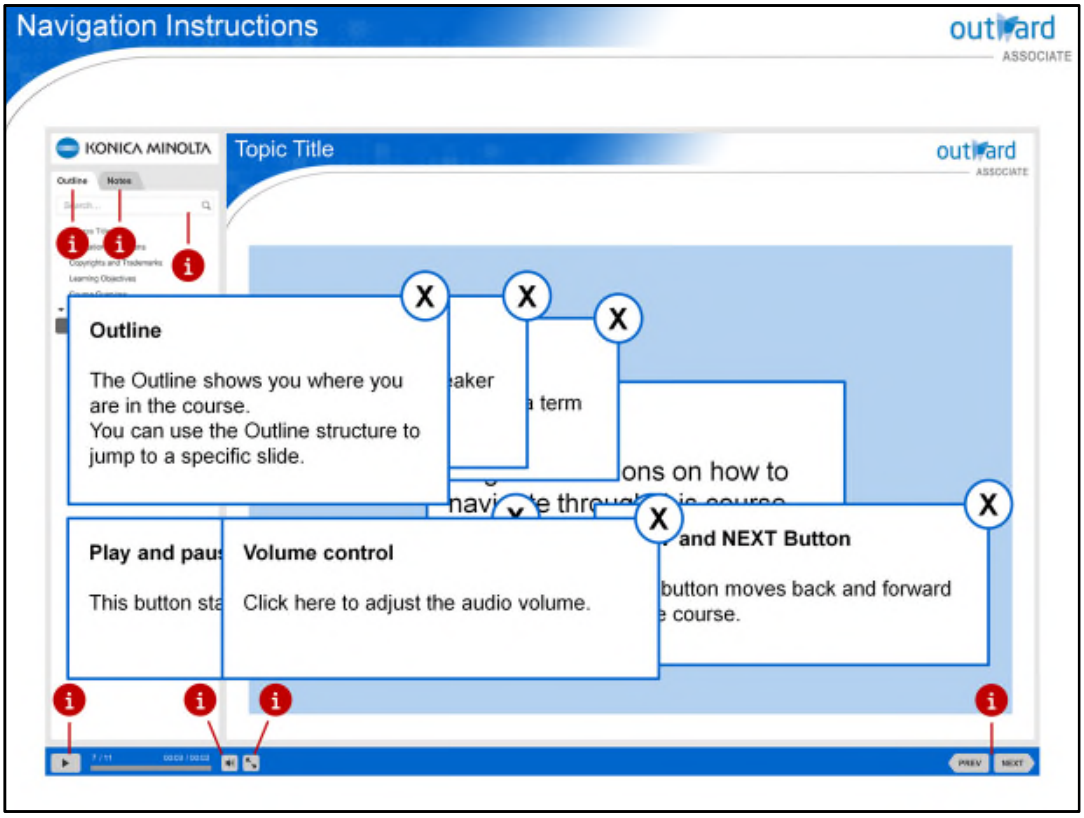
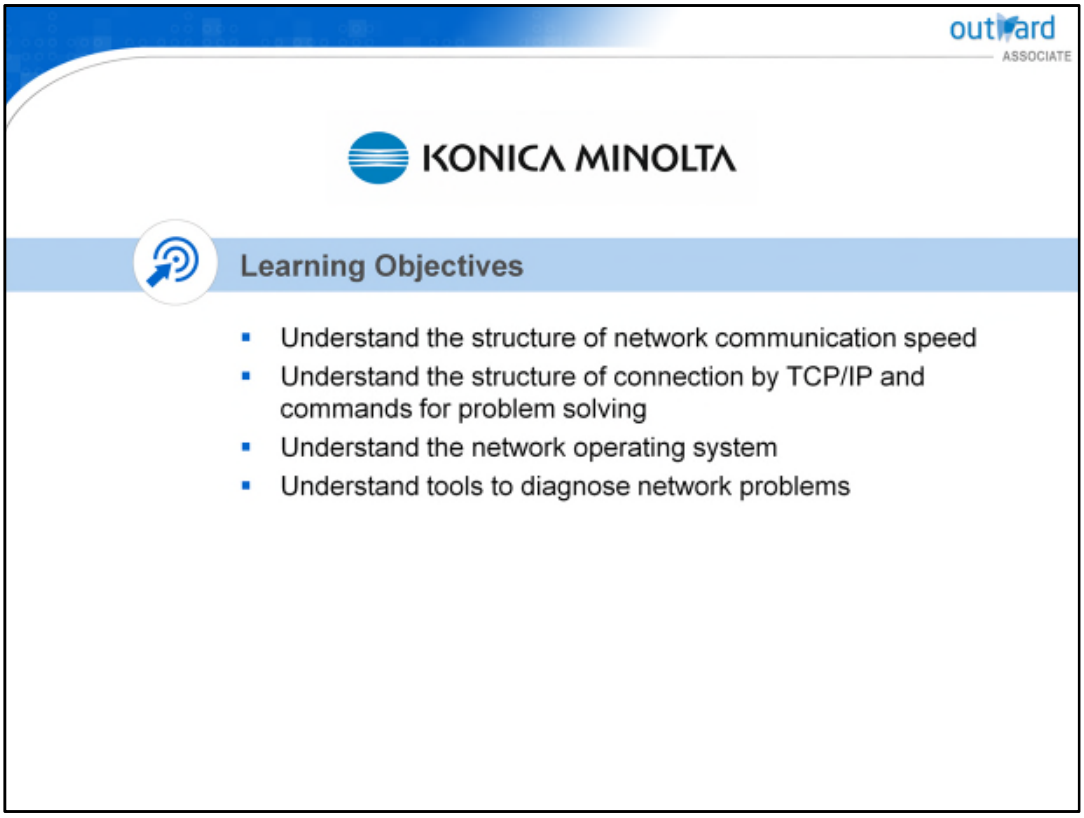


Welcome to the OUTWARD course "Computer Network Management"!
The estimated runtime of this course is 50 minutes.



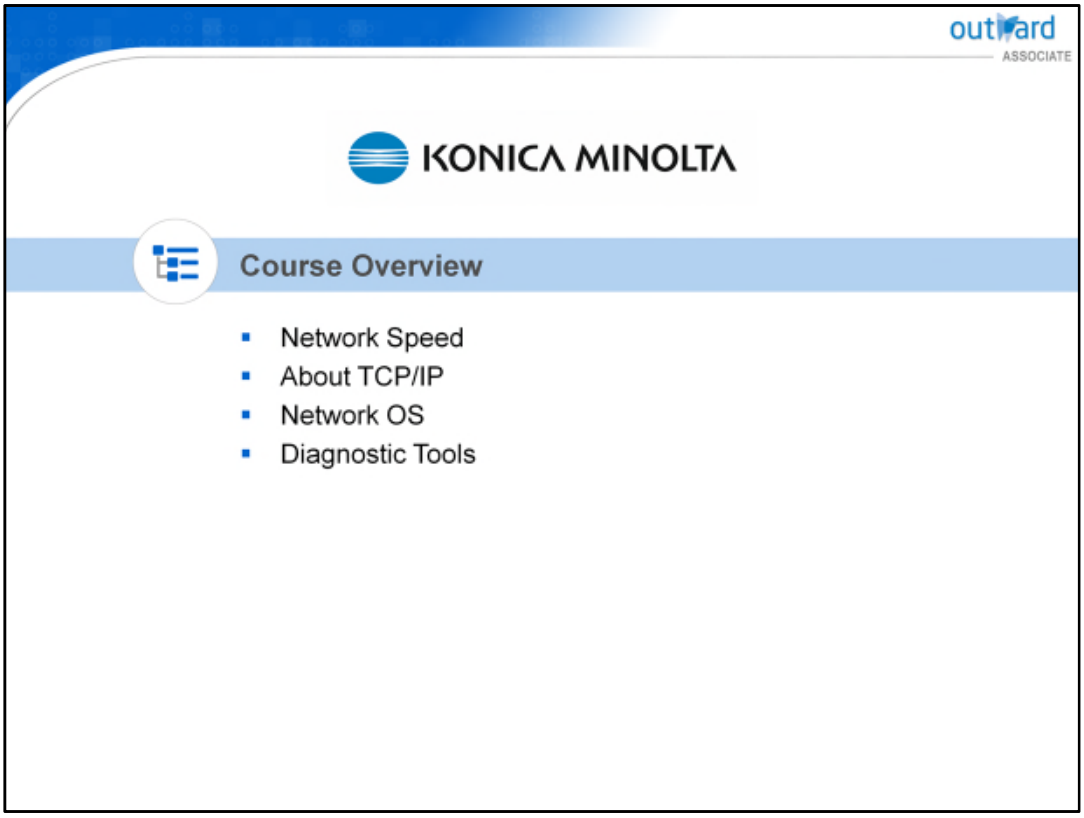
Here you see how to navigate within the course.

Copyrights and Trademarks



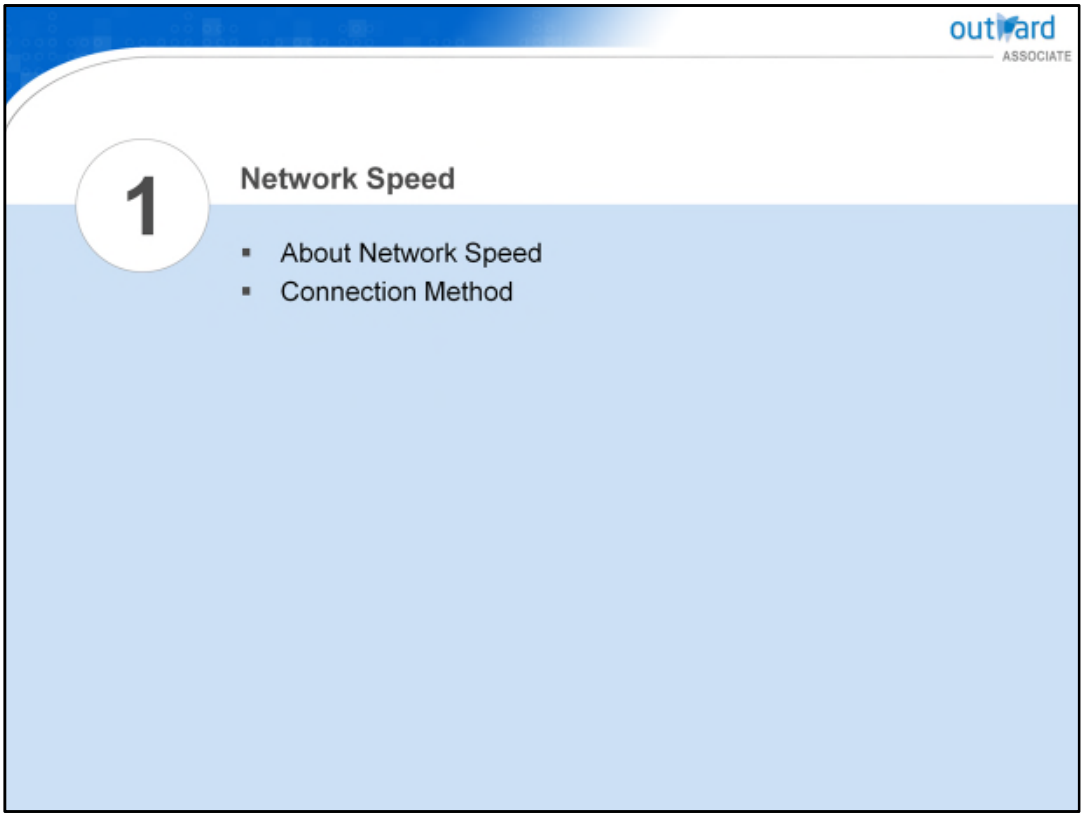
The purpose of this course is to provide you with an understanding of what may impact network processing speed, and what TCP/IP is.
In addition, you will learn why it is important to know about it and to understand what a network operating system is and the tools available to diagnose network problems.

Цель этого курса - дать вам понимание того, что может повлиять на скорость сетевой обработки и что такое TCP / IP.
Кроме того, вы узнаете, почему важно знать об этом и понимать, что такое сетевая операционная система и инструменты, доступные для диагностики сетевых проблем.



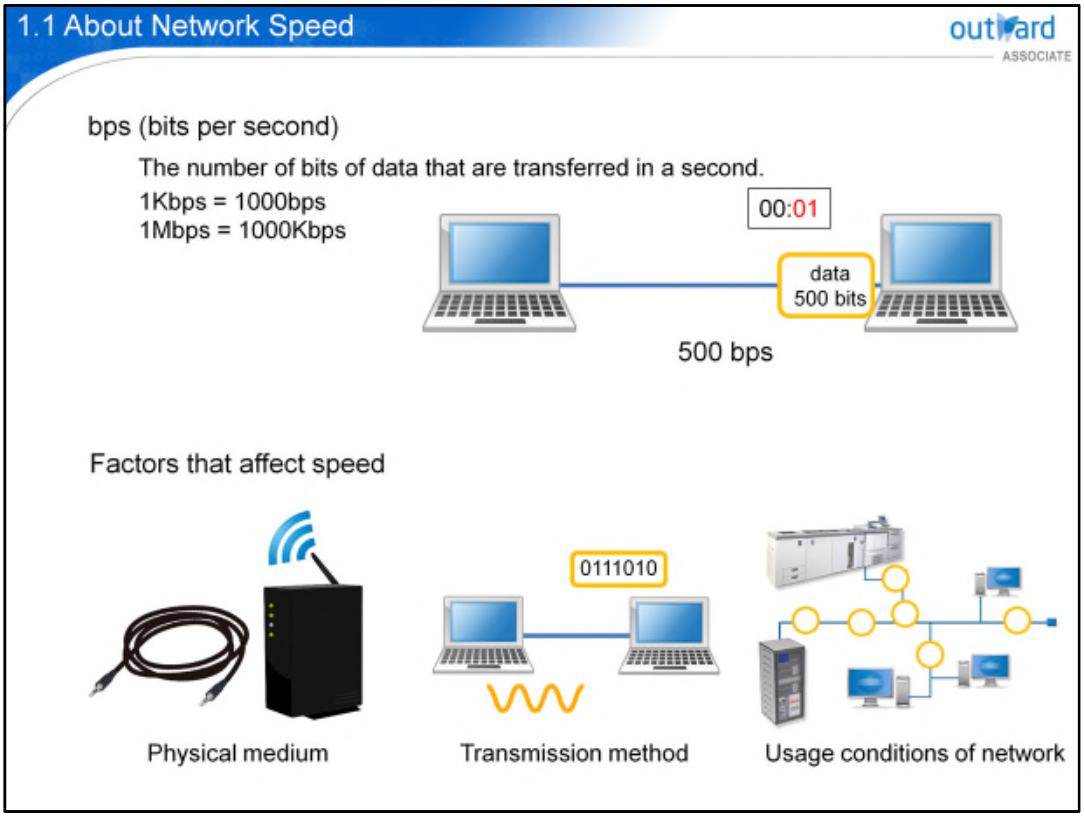
Think about your Internet service provider. If you were to source a new contract for Internet service, what factors would impact your decision?
When you use the Internet, or your local area network, are there things that make it less convenient than you prefer?How about things like network speed and network stability, or perhaps reliability or security?
These are all aspects of network management, and this course explains how to manage the basics of networks such as speed, stability and problem solving.
In addition, we will introduce the operating system and diagnostic tools to maintain an efficient and comfortable network.

Подумайте о своем интернет-провайдере. Если бы вы заключили новый контракт на интернет-услуги, какие факторы повлияли бы на ваше решение?
Когда вы используете Интернет или вашу локальную сеть, есть ли вещи, которые делают его менее удобным, чем вы предпочитаете? Как насчет таких вещей, как скорость сети и стабильность сети, или, возможно, надежность или безопасность?
Все это аспекты управления сетью, и этот курс объясняет, как управлять основами сетей, такими как скорость, стабильность и решение проблем.
Кроме того, мы представим операционную систему и средства диагностики для поддержания эффективной и комфортной сети.



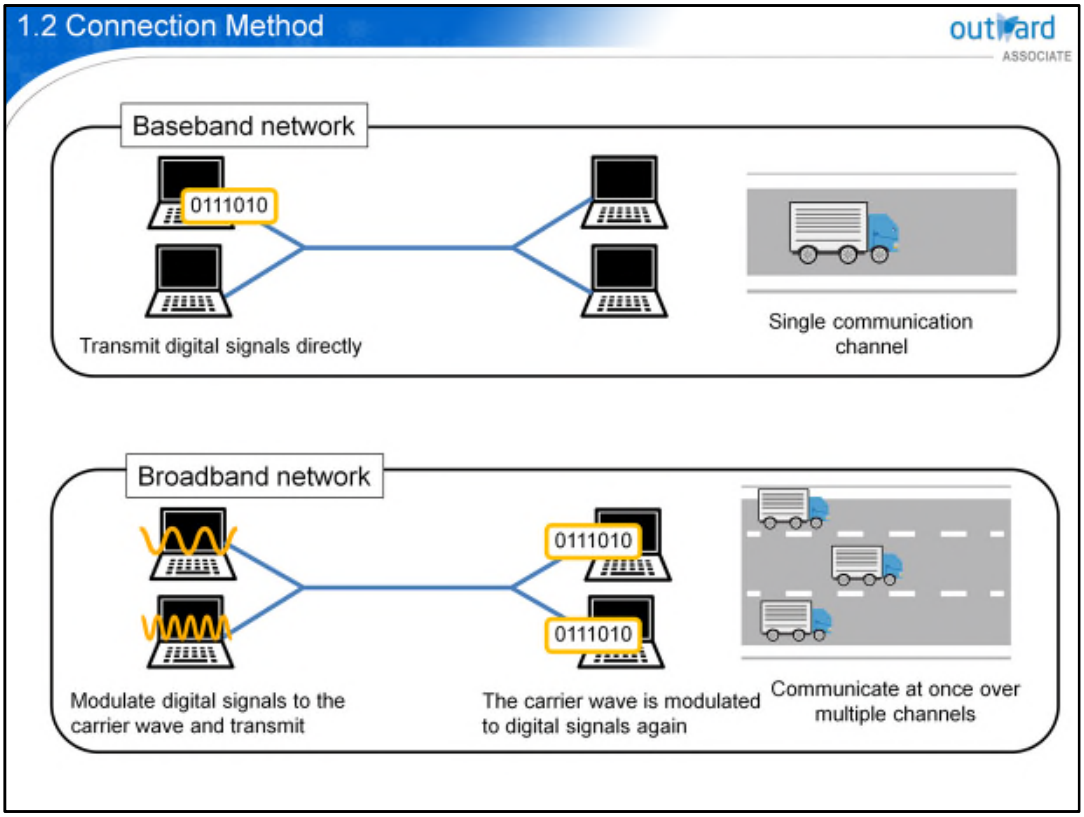
This lesson explains network speed and the circumstances that affect network speed.

Этот урок объясняет скорость сети и обстоятельства, которые влияют на скорость сети.



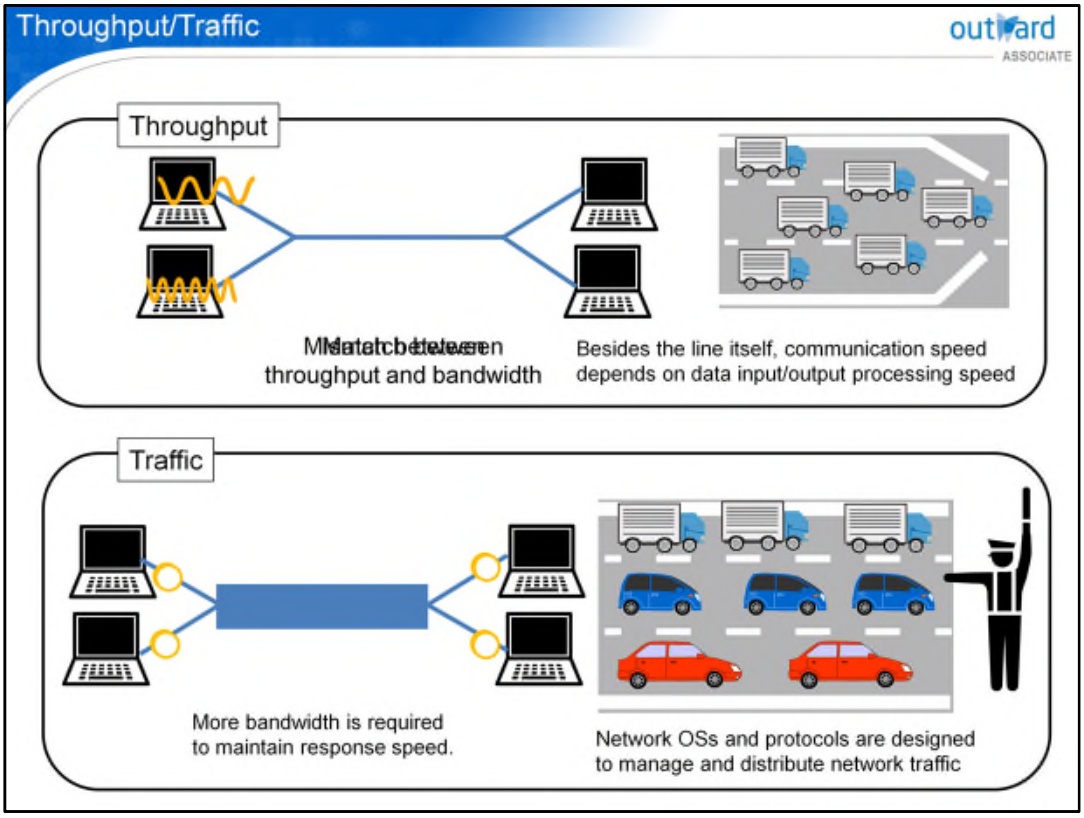
Network speed is the rate of data transmission between network nodes.
The faster the speed, the more data can be transmitted in a given period of time.
For units of speed, bps is used, which indicates the number of bits of data transferred in a second, and Kbps or Mbps are frequently used nowadays.
Speed is largely affected by physical mediums such as cables or wireless LAN technology.
Moreover, differences due to transmission types such as digital transmission vs. analog transmission, or the condition of the network also affects speed.

Скорость сети - это скорость передачи данных между узлами сети.
Чем выше скорость, тем больше данных может быть передано в данный период времени.
Для единиц скорости используется бит / с, что указывает количество бит данных, передаваемых в секунду, и в настоящее время часто используются Кбит / с или Мбит / с.
Скорость в значительной степени зависит от физических сред, таких как кабели или технология беспроводной локальной сети.
Кроме того, различия, связанные с типами передачи, такими как цифровая передача или аналоговая передача, или состояние сети, также влияют на скорость.



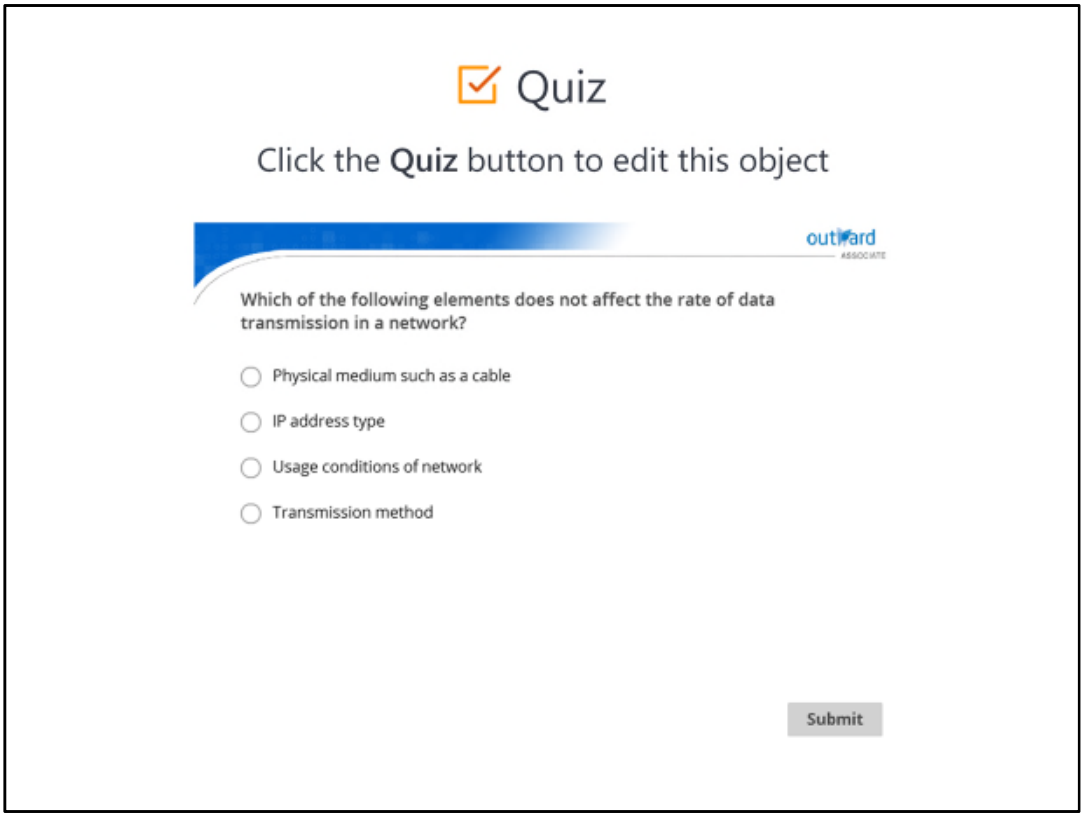
In a baseband network, such as Ethernet, a device transmits digital signals directly without manipulation.
In the baseband system, the transmission method is visualized using line cords.
Only one communication channel can be used, and therefore only one device can transmit signals at a time. It can be compared to a road with a single traffic lane.
• In a broadband network, the digital signals are modulated to the carrier wave. The modulated carrier wave is transmitted to the receiver, which demodulates the signal to digital data again.
The physical bandwidth of the cable is practically separated into multiple channels and each channel has its own carrier frequency.
• In other words, a single cable can be divided by the carrier frequency, so you can send data via multiple channels at the same time, meaning you can transmit them at high speed. It can be compared to a road with multiple traffic lanes.

В основной сети, такой как Ethernet, устройство передает цифровые сигналы напрямую, без манипуляций. В системе основной полосы частот способ передачи визуализируется с использованием линейных шнуров.
Может использоваться только один канал связи, и поэтому только одно устройство может передавать сигналы. Это можно сравнить с дорогой с одной полосой движения.
• В широкополосной сети цифровые сигналы модулируются к несущей. Модулированная несущая передается на приемник, который снова демодулирует сигнал в цифровые данные.
Физическая полоса пропускания кабеля практически разделена на несколько каналов, и каждый канал имеет свою собственную несущую частоту.
• Другими словами, один кабель может быть разделен на несущую частоту, поэтому вы можете отправлять данные по нескольким каналам одновременно, то есть вы можете передавать их с высокой скоростью. Это можно сравнить с дорогой с несколькими полосами движения.

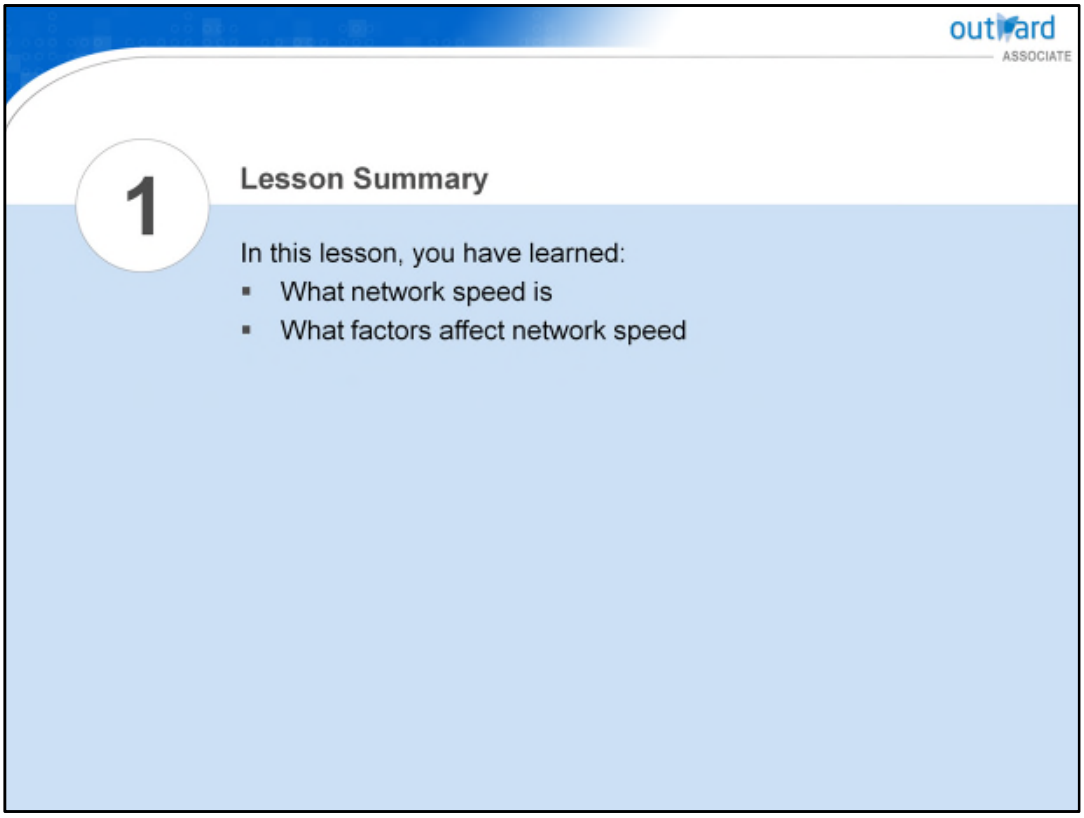


In the context of the network, throughput means the communication speed.
Communication speed is a necessary condition to maximize network efficiency.
In order to maintain the maximum communication speed and maximize the network efficiency, it is important that throughput corresponds to the bandwidth. The throughput can be compared to a car's speed.
When cars run at the maximum speed allowed for each road, cars can use the roadway the most efficiently.
The other major factor in the speed of network response is the amount of data that passes through the network at any one time, referred to as the network traffic.
In large networks where many users are generating messages simultaneously, more bandwidth is required to maintain response speed.
To prevent system congestion, network operating systems and protocols are designed to manage and distribute network traffic.
This feature also prevents the transactions of one user from degrading the performance of the network for other users. Network operating systems and protocols can be compared to the role of directing traffic.

В контексте сети пропускная способность означает скорость связи.
Скорость связи является необходимым условием для максимальной эффективности сети.
Чтобы поддерживать максимальную скорость связи и максимизировать эффективность сети, важно, чтобы пропускная способность соответствовала пропускной способности. Пропускную способность можно сравнить со скоростью автомобиля.
Когда автомобили движутся с максимальной скоростью, разрешенной для каждой дороги, автомобили могут использовать проезжую часть наиболее эффективно.
Другим важным фактором скорости отклика сети является объем данных, которые проходят через сеть в любой момент времени, называемый сетевым трафиком.
В больших сетях, где много пользователей генерируют сообщения одновременно, для поддержания скорости отклика требуется большая полоса пропускания.
Для предотвращения перегрузки системы сетевые операционные системы и протоколы предназначены для управления и распределения сетевого трафика.
Эта функция также не позволяет транзакциям одного пользователя ухудшать производительность сети для других пользователей. Сетевые операционные системы и протоколы можно сравнить с ролью направления трафика.

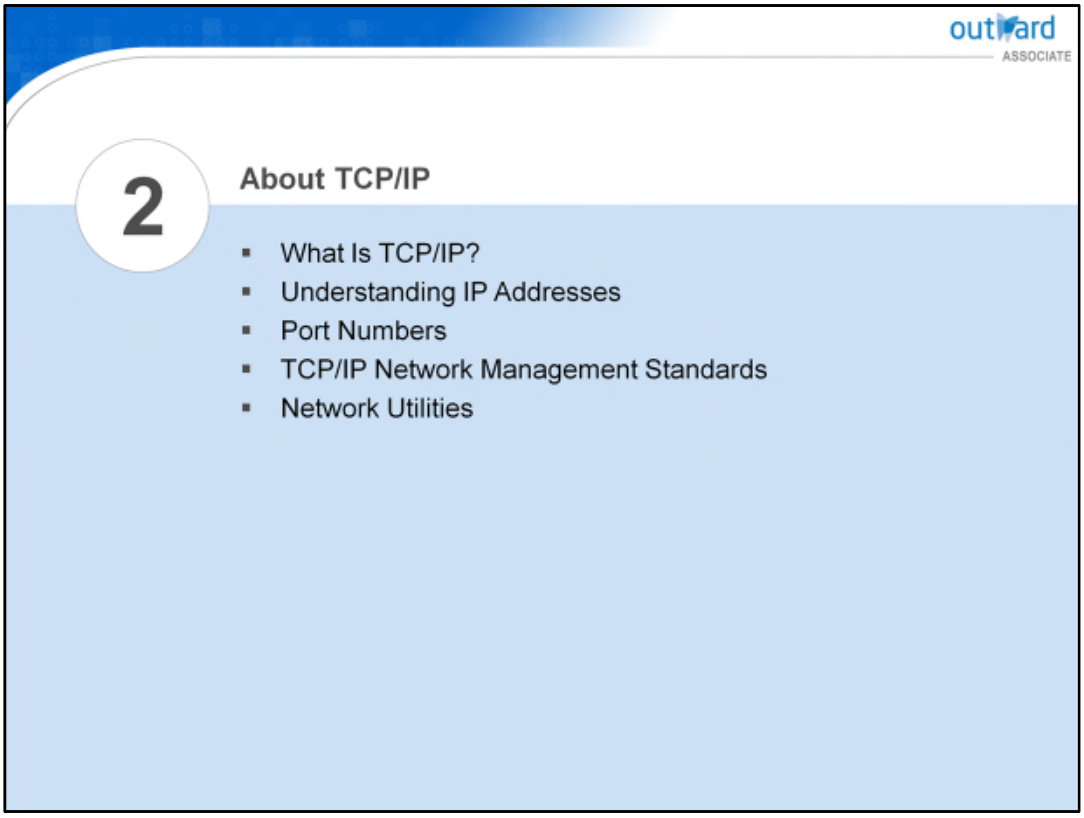


Test your knowledge in a quiz!

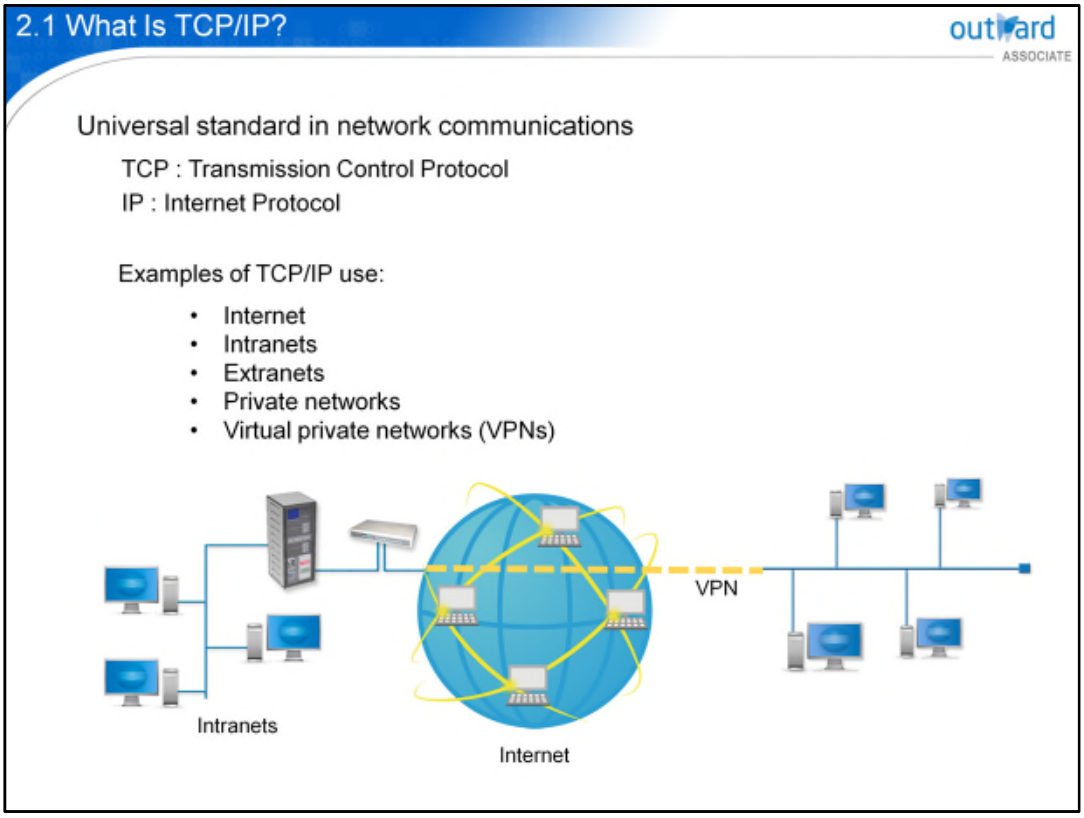


Network speed is expressed by bps, which indicates the number of bits of data transferred in a second.
The faster the speed, the more data can be transmitted in a given period of time.
Network speed is not constant. The speed changes based on various factors, such as the physical medium, transmission method, and amount of traffic.

Скорость сети выражается в бит / с, что указывает на количество бит данных, передаваемых в секунду.
Чем выше скорость, тем больше данных может быть передано в данный период времени.
Скорость сети не постоянна. Скорость изменяется в зависимости от различных факторов, таких как физическая среда, способ передачи и объем трафика.

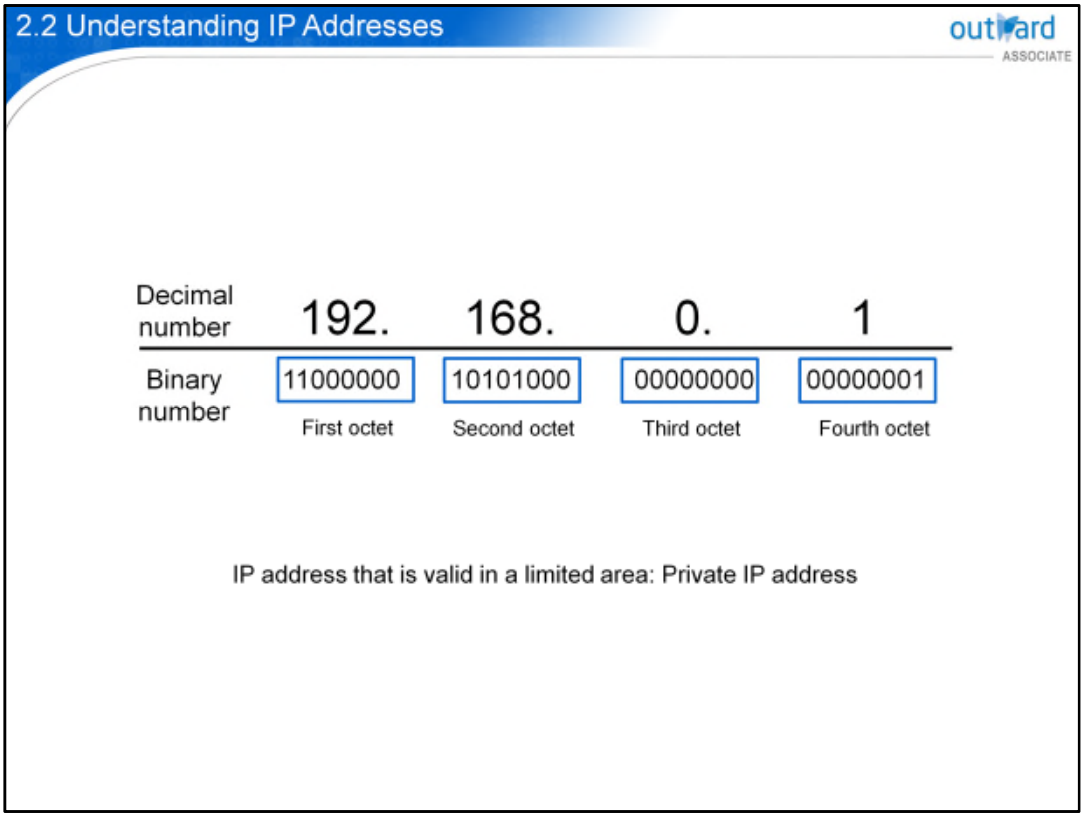


This lesson explains about using TCP/IP to connect network nodes.
It also explains about the use of ports and utilities that help with the management of networks.



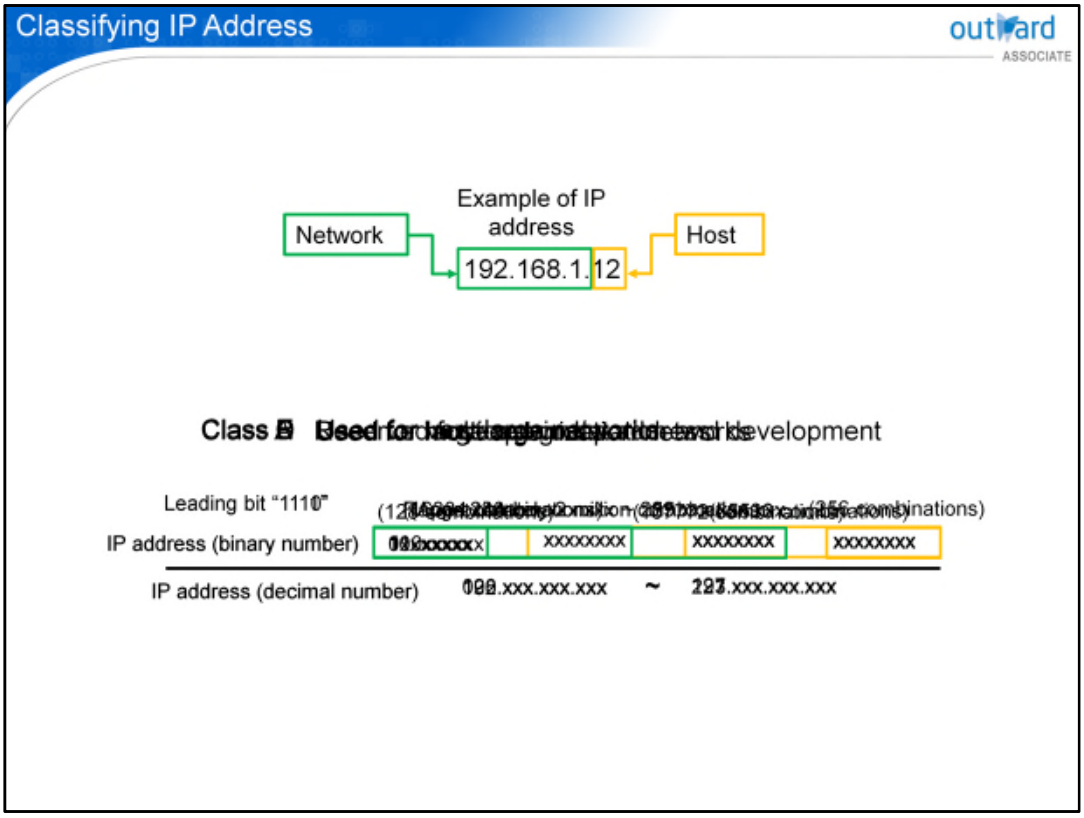
TCP and IP are network protocols. TCP/IP is a general term for protocols such as TCP and IP.
TCP/IP is the universal standard for network communication. As noted on the screen, it is used to support the Internet by facilitating communication between computers all over the world and providing access to data and applications at geographically distributed sites.
It also supports intranets, which are private networks only available to authorized users, and extranets, which allow for the sharing of data among multiple intranets.
TCP/IP is also used in virtual private networks, which are networks where remote users can be given access rights to establish a virtual point-to-point encrypted connection. The virtual connection is connected via a dedicated tunnel over a modem to the resources of a private network.

TCP и IP являются сетевыми протоколами. TCP / IP - это общий термин для таких протоколов, как TCP и IP.
TCP / IP является универсальным стандартом для сетевого общения. Как отмечено на экране, он используется для поддержки Интернета, облегчая связь между компьютерами по всему миру и обеспечивая доступ к данным и приложениям на территориально распределенных площадках.
Он также поддерживает интрасети, которые являются частными сетями, доступными только авторизованным пользователям, и экстрасети, которые позволяют обмениваться данными между несколькими интрасетями.
TCP / IP также используется в виртуальных частных сетях, которые представляют собой сети, где удаленным пользователям могут быть предоставлены права доступа для установления виртуального двухточечного зашифрованного соединения. Виртуальное соединение подключается через выделенный туннель через модем к ресурсам частной сети.



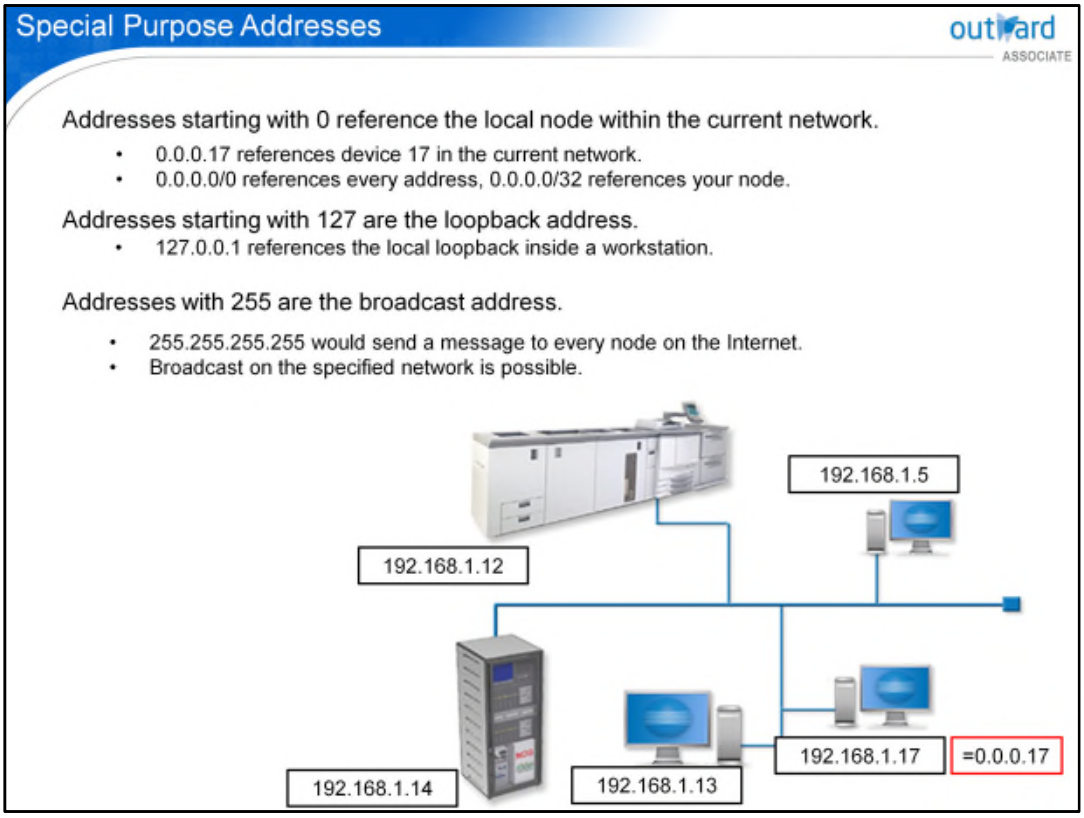
IP addresses are unique numbers assigned to each computer or node on the network.
It is compared to a "network address" that is assigned to recognize each computer.
There are two ways to describe network addresses, decimal numbers and binary numbers.
Although the actual IP address is described as a binary number, it can be described as a decimal number.
A 32-bit long number that is described as a binary number is divided into four 8-bit groups and each group is converted to decimal numbers.
This 8-bit unit is called an "octet".
There are two types of IP addresses, IPv4 and IPv6. IPv6 was created to support the extremely high number of IP addresses expected to be needed in the near future. This course deals with IPv4 addresses.
IP addresses that are valid in a limited area, such as inside a company, are called "private IP addresses".
Private IP addresses do not allow nodes on the network to communicate directly with the Internet. In addition, private IP addresses may be used in other networks.

• IP-адреса - это уникальные номера, назначаемые каждому компьютеру или узлу в сети.
Он сравнивается с «сетевым адресом», который назначается для распознавания каждого компьютера.
Существует два способа описания сетевых адресов, десятичных и двоичных чисел.
Хотя фактический IP-адрес описывается как двоичное число, его можно описать как десятичное число.
32-битное длинное число, которое описывается как двоичное число, делится на четыре 8-битные группы, и каждая группа преобразуется в десятичные числа.
Этот 8-битный модуль называется «октет».
Существует два типа IP-адресов: IPv4 и IPv6. IPv6 был создан для поддержки чрезвычайно большого числа IP-адресов, которые, как ожидается, понадобятся в ближайшем будущем. В этом курсе рассматриваются адреса IPv4.
IP-адреса, действительные в ограниченной области, например внутри компании, называются «частными IP-адресами». Частные IP-адреса не позволяют узлам в сети напрямую связываться с Интернетом. Кроме того, частные IP-адреса могут использоваться в других сетях.

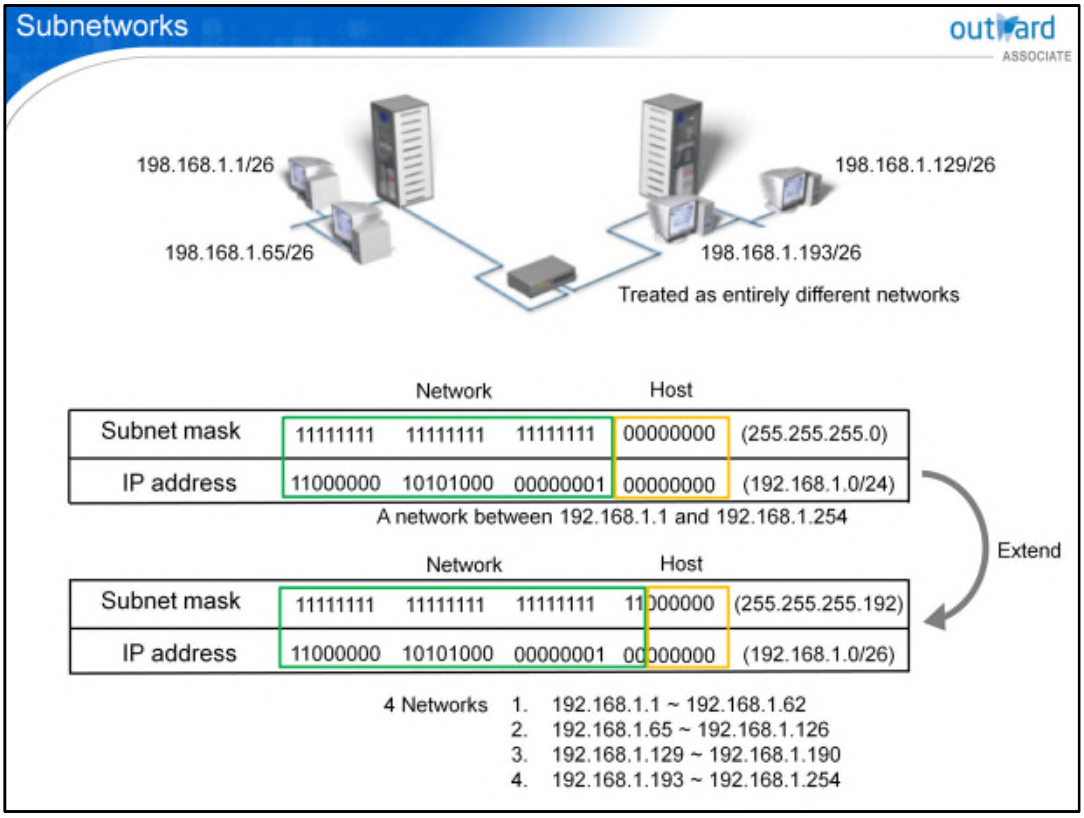


IP addresses are divided into a network ID and a host ID. The division point is regulated by the class assignment of the default net mask.
Class A is when the most significant bit is 0, and the leading octet 0 to 127 applies.
In Class A, the leading 8 bits is defined as the network ID, and it has 128 combinations of network addresses and approximately 160,000 host addresses for each. They are used for very large networks because the number of nodes is enormous.
Class B is when the most significant bit starts from 10, and the leading 16 bits is defined as the network ID. They are used for large networks for the same reason. Class C is when the most significant bit starts from 110, and the leading 24 bits is defined as the network ID.
They are used for most organization networks.
Class D is for multicast group addresses used to send sound or image data at once.
Class E is reserved for experimentation and development,
and is not in use.

IP-адреса делятся на идентификатор сети и идентификатор хоста. Точка деления регулируется назначением класса сетевой маски по умолчанию.
Класс A - это когда старший значащий бит равен 0, а применяется старший октет от 0 до 127.
В классе A ведущие 8 битов определены как идентификатор сети, и он имеет 128 комбинаций сетевых адресов и приблизительно 160 000 адресов хоста для каждого. Они используются для очень больших сетей, потому что количество узлов огромно.
Класс B - это когда старший значащий бит начинается с 10, а первые 16 бит определяются как идентификатор сети.
Они используются для больших сетей по той же причине. Класс C - это когда старший значащий бит начинается со 110, а первые 24 бита определяются как идентификатор сети.
Они используются для большинства организационных сетей.
Класс D предназначен для групповых адресов, используемых для одновременной отправки звуковых или графических данных.
Класс E зарезервирован для экспериментов и разработки, и не используется.

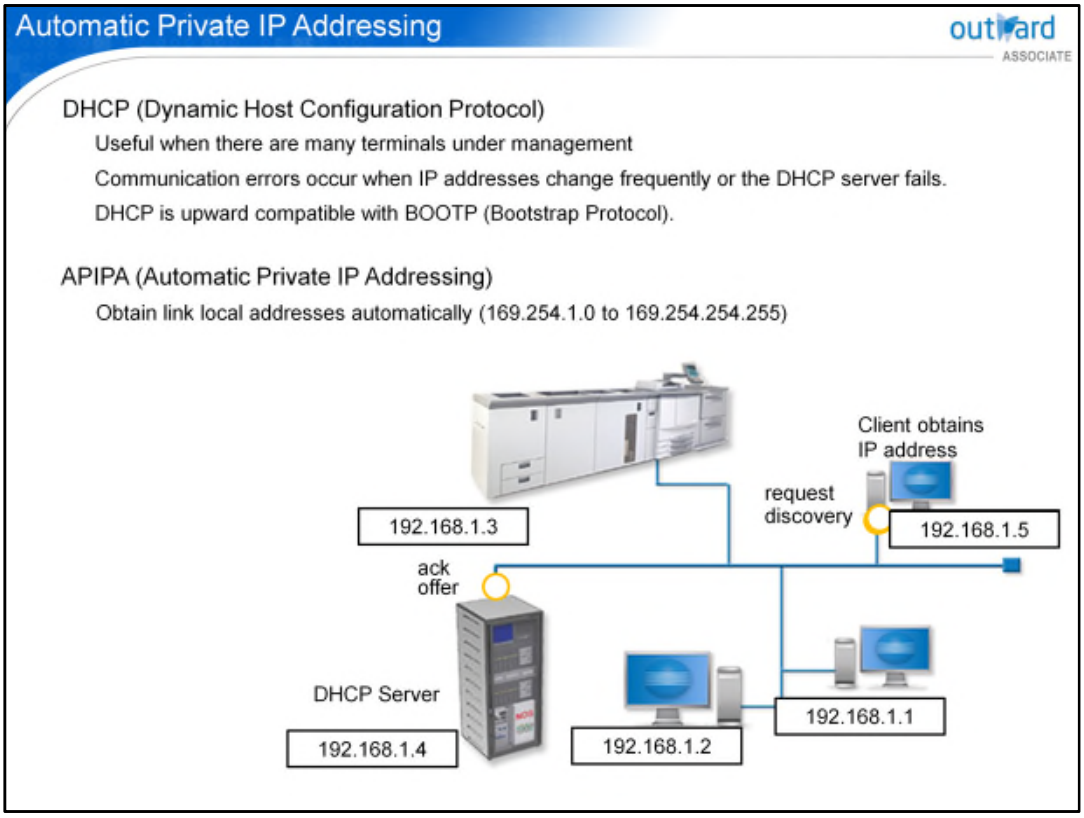


Specific IP addresses are assigned for special purposes and therefore cannot be used for other purposes.
An address starting with 0 references the local node within the current network. For example, 0.0.0.17 references device 17 in the current network.
127.0.0.1 references the local loopback inside a workstation, and is used to test whether TCP/IP is successfully installed. An address with 255 is the broadcast address. 255.255.255.255 sends a message to every node on the Internet.
Moreover, when the address is 192.168.2.255/24, messages are sent to the entire network belonging to 192.168.2.xxx. When divided into subnets, the highest IP address of that network is used.
Определенные IP-адреса назначаются для специальных целей и поэтому не могут использоваться для других целей.
Адрес, начинающийся с 0, ссылается на локальный узел в текущей сети. Например, 0.0.0.17 ссылается на устройство 17 в текущей сети.
127.0.0.1 ссылается на локальный шлейф внутри рабочей станции и используется для проверки успешной установки TCP / IP. Адрес с 255 является широковещательным адресом. 255.255.255.255 отправляет сообщение каждому узлу в Интернете.
Кроме того, когда адрес 192.168.2.255/24, сообщения отправляются всей сети, принадлежащей 192.168.2.xxx. При разделении на подсети используется самый высокий IP-адрес этой сети.



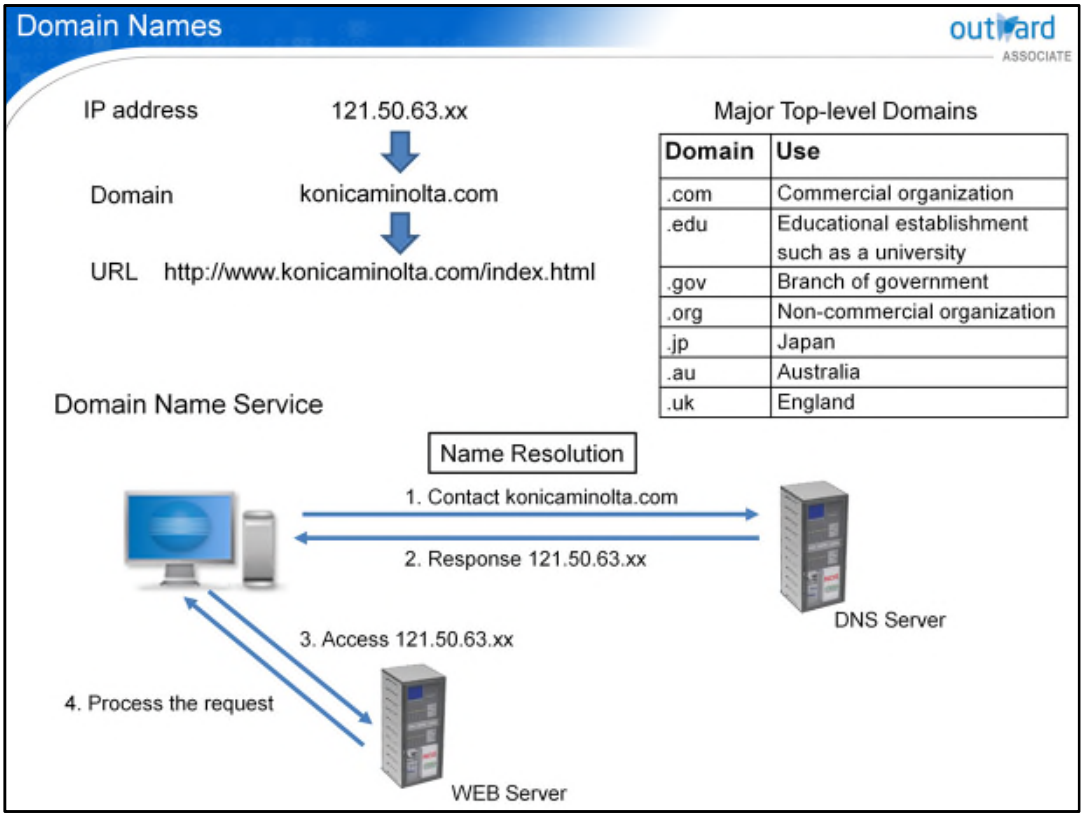
As mentioned previously, IP addresses are separated into the network ID and the host ID, but there are some exceptions.
Therefore, subnetworks are used which separate the Network ID and Host ID using a subnet mask.
In subnet networks there are cases when routers or gateways physically separate segments or cases when they are physically part of the network but separated logically. An example is a Class C network; by expanding the subnet mask up to 26 bits, 00, 01, 10 and 11 subnetworks can be added in the expanded area.
As a result, 254 host users in 1 network are divided into 62 host users on 4 networks.

Как упоминалось ранее, IP-адреса разделены на идентификатор сети и идентификатор хоста, но есть некоторые исключения.
Поэтому используются подсети, которые разделяют идентификатор сети и идентификатор хоста, используя маску подсети.
В сетях подсетей существуют случаи, когда маршрутизаторы или шлюзы физически разделяют сегменты, или случаи, когда они физически являются частью сети, но логически разделены. Примером является сеть класса C; Расширяя маску подсети до 26 бит, можно расширить подсети 00, 01, 10 и 11 в расширенной области.
В результате 254 хост-пользователя в 1 сети делятся на 62 хост-пользователя в 4 сетях.

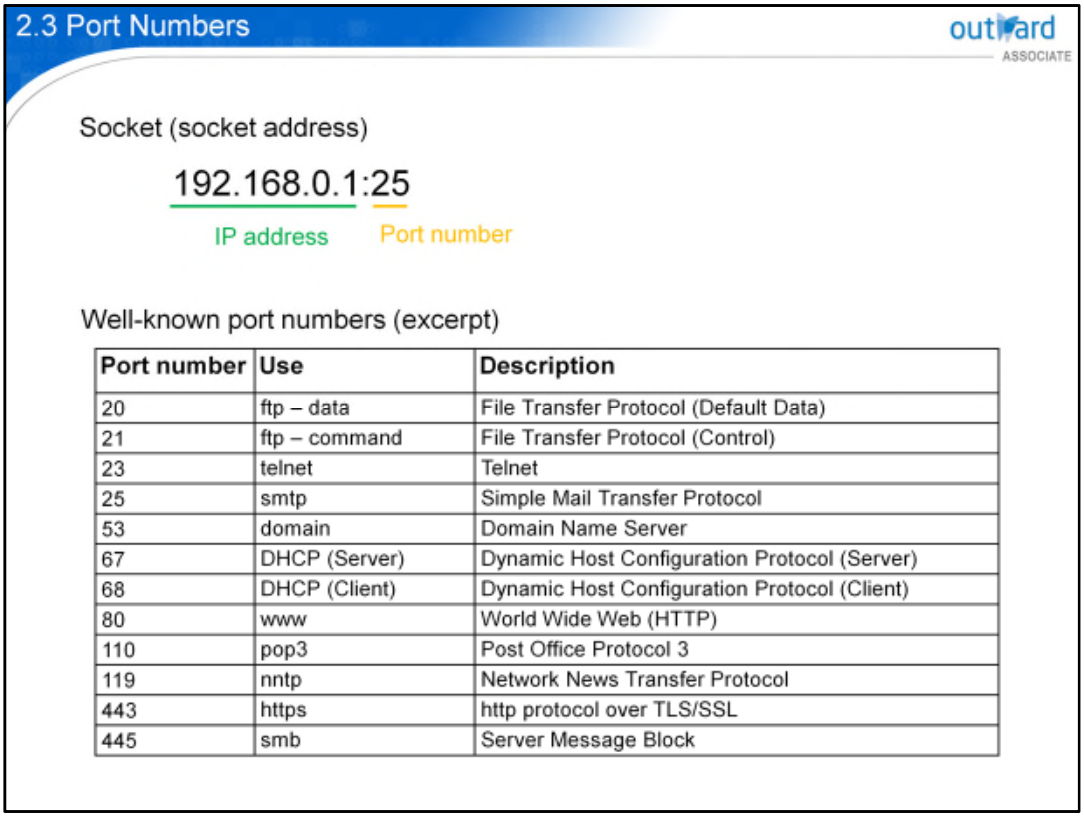


DHCP is used to automatically allocate IP addresses. Clients acquire an IP address with DHCP by temporarily setting their IP address to 0.0.0.0, and broadcasting a message.
DHCP servers receive the message and send a message with an available IP address.
Clients then receive the message and broadcast the available IP address.
• When DHCP servers response to the message, clients can officially set up the IP address.
As DHCP can be used to automatically set up IP addresses, it is effective when there are many terminals under management.
However, one disadvantage of DHCP is that there may be communication errors if different IP addresses are allocated frequently or the DHCP server fails.
As DHCP is upward compatible with BOOTP, BOOTP is no longer used.
Moreover, when DHCP cannot acquire an IP address, APIPA may automatically allocate IP addresses. However, as link local addresses will not be routed, communication with other networks and the Internet is not possible.

DHCP используется для автоматического распределения IP-адресов. Клиенты получают IP-адрес с помощью DHCP, временно устанавливая свой IP-адрес 0.0.0.0 и передавая сообщение.
DHCP-серверы получают сообщение и отправляют сообщение с доступным IP-адресом.
Затем клиенты получают сообщение и транслируют доступный IP-адрес.
• Когда DHCP-серверы отвечают на сообщение, клиенты могут официально настроить IP-адрес.
Поскольку DHCP может использоваться для автоматической настройки IP-адресов, он эффективен, когда под управлением находится много терминалов.
Однако одним из недостатков DHCP является то, что могут возникать ошибки связи, если часто назначаются разные IP-адреса или происходит сбой DHCP-сервера.
Поскольку DHCP совместим с BOOTP и выше, BOOTP больше не используется. Кроме того, когда DHCP не может получить IP-адрес, APIPA может автоматически распределять IP-адреса.
Однако, поскольку локальные адреса ссылок не будут маршрутизироваться, связь с другими сетями и Интернетом невозможна.

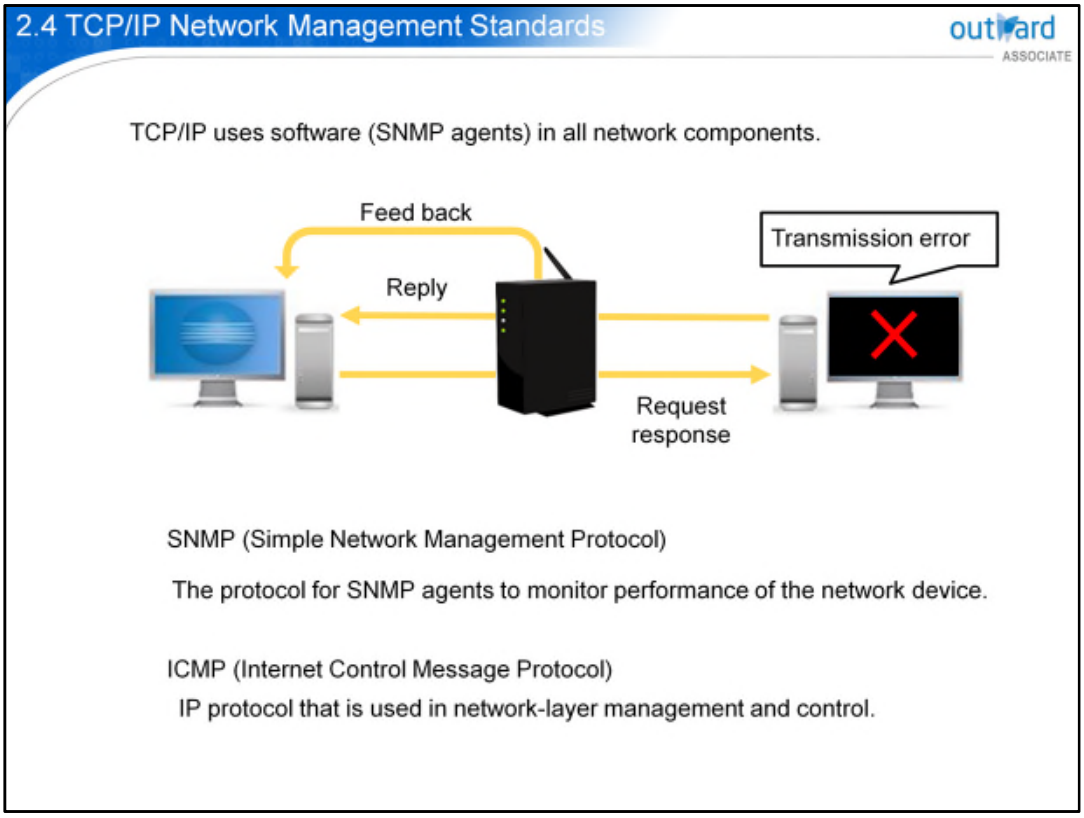


As memorizing IP addresses is difficult, it is possible to add domains which have supported names.
Domains are acquired by combining a free name and a top-level domain tailored to the intended use.
Furthermore, domains can be accessed using browsers and the like by specifying protocols, servers and files to be accessed, forming a URL.
Domains are managed by the DNS system. DNS servers maintain domains and corresponding IP addresses.
When accessing a web server using a URL, first the DNS server is asked for the domain name and the IP address is acquired.
This procedure is called name resolution. You can access necessary data by accessing the acquired IP address.
If the name is not resolved, the DNS server contacts the name server. A name server exists for each domain hierarchy.
The DNS server sends repeated inquiries from the top of the hierarchy until target IP address is obtained.
Поскольку запоминание IP-адресов затруднено, можно добавить домены, которые поддерживают имена.
Домены приобретаются путем сочетания свободного имени и домена верхнего уровня с учетом предполагаемого использования.
Кроме того, к доменам можно получить доступ с помощью браузеров и тому подобного, указав протоколы, серверы и файлы, к которым осуществляется доступ, и сформировав URL.
Домены управляются системой DNS. DNS-серверы поддерживают домены и соответствующие IP-адреса.
При доступе к веб-серверу с использованием URL-адреса сначала у DNS-сервера запрашивается имя домена, и IP-адрес получается.
Эта процедура называется разрешением имени. Вы можете получить доступ к необходимым данным, получив доступ к IP-адресу.
Если имя не разрешено, DNS-сервер связывается с сервером имен. Сервер имен существует для каждой иерархии доменов.
DNS-сервер отправляет повторные запросы из верхней части иерархии, пока не будет получен целевой IP-адрес.



Port number	Use	Description
20	ftp – data	File Transfer Protocol (Default Data)
21	ftp – command	File Transfer Protocol (Control)
23	telnet	Telnet
25	smtp	Simple Mail Transfer Protocol
53	domain	Domain Name Server
67	DHCP (Server)	Dynamic Host Configuration Protocol (Server)
68	DHCP (Client)	Dynamic Host Configuration Protocol (Client)
80	www	World Wide Web (HTTP)
110	pop3	Post Office Protocol 3
119	nntp	Network News Transfer Protocol
443	https	http protocol over TLS/SSL
445	smb	Server Message Block

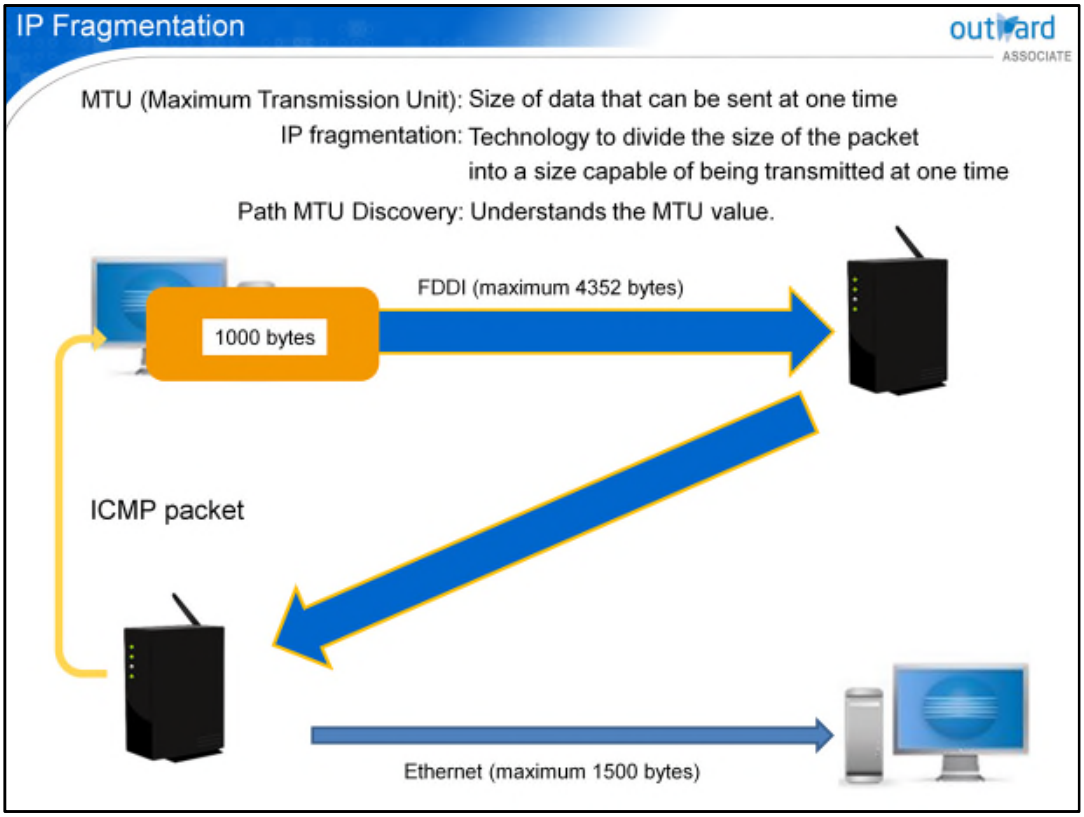
TCP or UDP identifies the application transmitting data across the network by a 16-bit port number attached to the IP address.
UDP, an abbreviation for User Datagram Protocol, is used when immediacy is more important than reliability regarding data communication.
The IP address combined with the port number is called a socket or socket address and written as ":25".
Put simply, port numbers indicate which process or service to send the transmitting data to.
If it is compared to our world, the IP address is the location of the apartment building and the port number is the apartment number.
Port numbers 0 to 1023 are called well-known port numbers and are mainly assigned to server applications.
For example, TCP/IP systems that function as an FTP server all use port 21.
Port numbers 1024 or higher are called high ports and are assigned to custom applications.
By combining the IP address with port numbers, one network computer can access multiple different services at the same time.
The client IP address and port number plus the server IP address and port number are referred to as socket pairs and they identify each TCP or UDP connection on the network.
TCP или UDP идентифицирует приложение, передающее данные по сети, по 16-битному номеру порта, присоединенному к IP-адресу.
UDP, сокращение от User Datagram Protocol, используется, когда непосредственность важнее, чем надежность передачи данных.
IP-адрес, объединенный с номером порта, называется сокетом или адресом сокета и записывается как «: 25».
Проще говоря, номера портов указывают, в какой процесс или службу отправлять передаваемые данные.
Если сравнивать с нашим миром, IP-адрес - это местоположение многоквартирного дома, а номер порта - это номер квартиры.
Номера портов от 0 до 1023 называются хорошо известными номерами портов и в основном назначаются серверным приложениям.
Например, все системы TCP / IP, которые работают как FTP-сервер, используют порт 21.
Номера портов 1024 или выше называются старшими портами и назначаются пользовательским приложениям.
Комбинируя IP-адрес с номерами портов, один сетевой компьютер может одновременно обращаться к нескольким различным службам.
IP-адрес и номер порта клиента, а также IP-адрес и номер порта сервера называются парами сокетов, и они идентифицируют каждое TCP или UDP-соединение в сети.



The SNMP agent monitors the performance of the network device and notifies the SNMP manager.
The SNMP protocol is used for communicating this information.
TCP/IP provides for management of all links and nodes in the network through the use of the SNMP agent in all network components that feed back information to SNMP managers.
For example, it is possible to require a response from an address, or to notify transmission errors when addresses are down.
The system is based on a management information database, called MIB, that sets out the standards for continued operation of each network component.
ICMP is another IP protocol used in network-layer management and control, and to report network errors.
If a message cannot be delivered by a router, the router will return it to the source with an ICMP message.

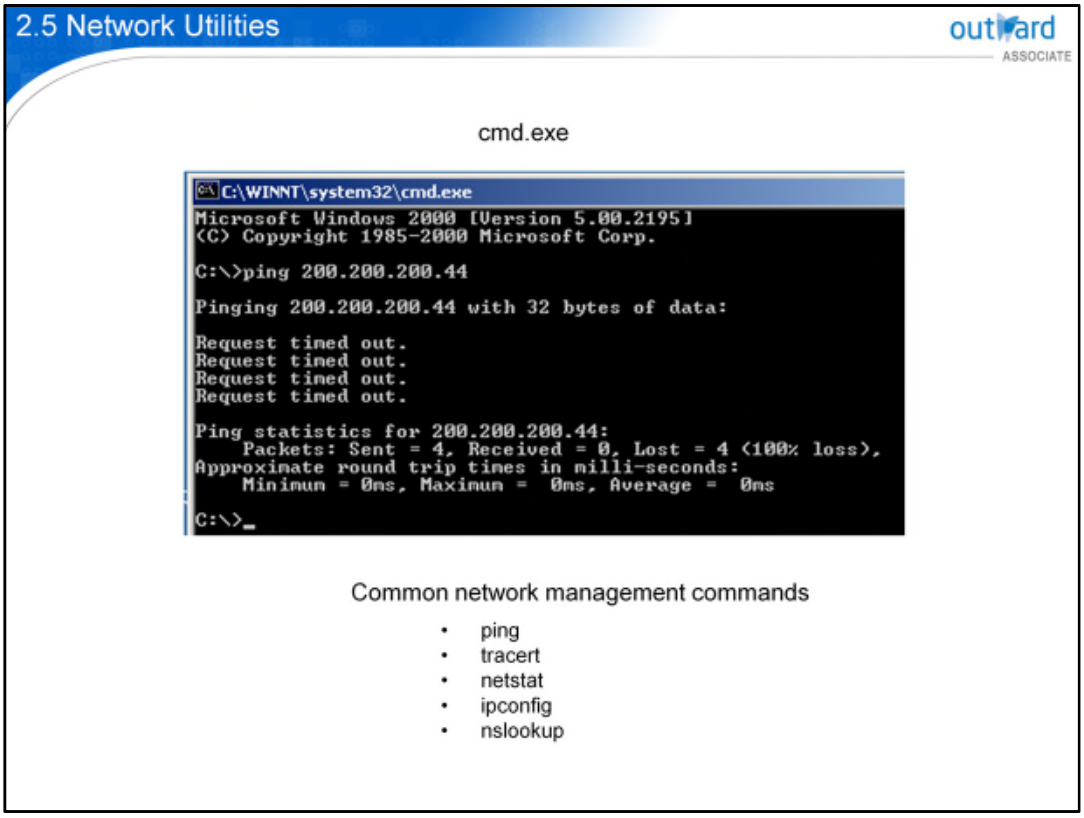
Агент SNMP контролирует производительность сетевого устройства и уведомляет менеджер SNMP.
Протокол SNMP используется для передачи этой информации.
TCP / IP обеспечивает управление всеми ссылками и узлами в сети посредством использования агента SNMP во всех сетевых компонентах, которые передают информацию менеджерам SNMP.
Например, можно потребовать ответ от адреса или уведомить об ошибках передачи, когда адреса не работают.
Система основана на базе данных управляющей информации, называемой MIB, которая устанавливает стандарты для непрерывной работы каждого компонента сети.
ICMP - это еще один протокол IP, используемый для управления и контроля сетевого уровня, а также для сообщения об ошибках сети.
Если сообщение не может быть доставлено маршрутизатором, маршрутизатор вернет его источнику с сообщением ICMP.

MTU (максимальная единица передачи): размер данных, которые могут быть отправлены за один раз.
Фрагментация IP: технология разделения размера пакета в размер, который может быть передан за один раз.
Path MTU Discovery: Понимает значение MTU.



There are differences in the packet size that can be transmitted, depending on the type of data link.
For example, Ethernet can transmit up to 1500 bytes, while FDDI can transmit up to 4352 bytes.
FDDI stands for Fiber Distributed Data Interface and is a network for large scale LANs to send data via optical fiber. The size of the packet transmitted is called the MTU. Furthermore, dividing the size of the packet into a size that can be sent at one time is called IP fragmentation.
In order to understand the MTU value, Path MTU Discovery is used.
If the packet size exceeds the upper limit, the router sends an ICMP message back to the source.
When the workstation receives an ICMP message, it divides and sends the packet data in a smaller size.
The work station measures the MTU by repeating this data transfer. This process is called Path MTU Discovery.

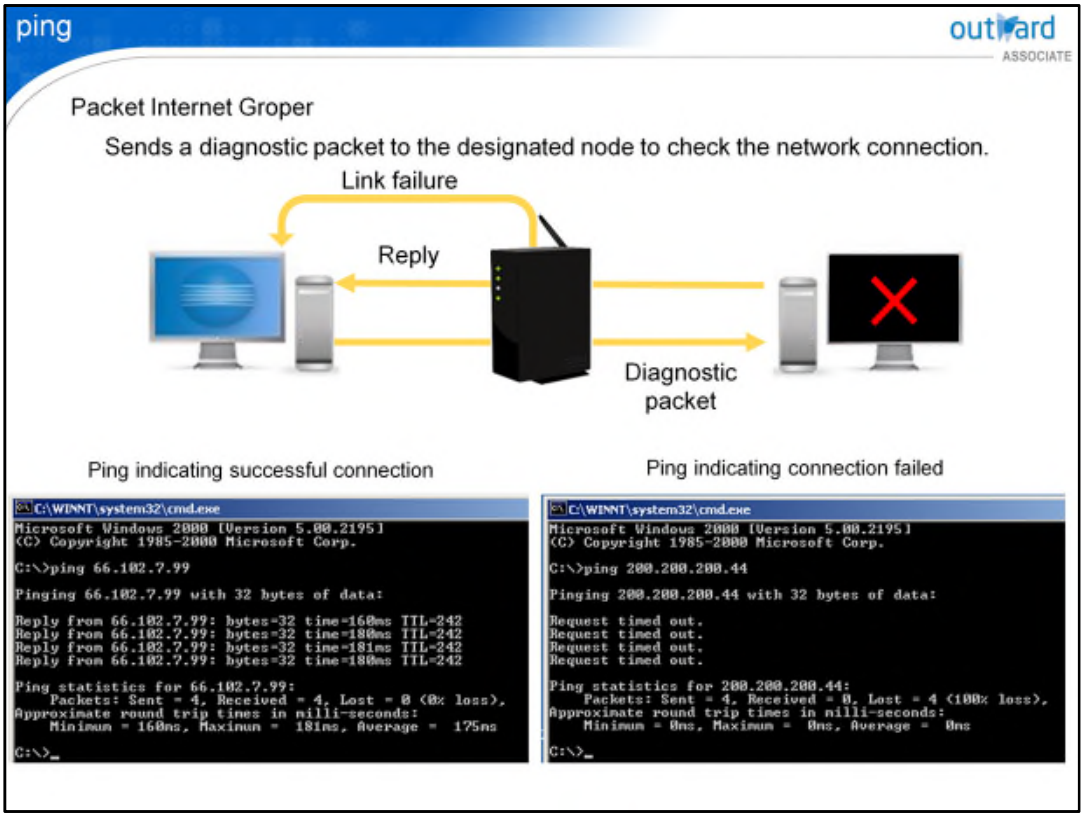
Существуют различия в размере пакета, который может быть передан, в зависимости от типа канала передачи данных.
Например, Ethernet может передавать до 1500 байтов, а FDDI может передавать до 4352 байтов.
FDDI расшифровывается как Fibre Distributed Data Interface и представляет собой сеть для крупномасштабных локальных сетей для отправки данных через оптоволокно. Размер передаваемого пакета называется MTU. Кроме того, деление размера пакета на размер, который может быть отправлен за один раз, называется IP-фрагментацией.
Чтобы понять значение MTU, используется Path MTU Discovery.
Если размер пакета превышает верхний предел, маршрутизатор отправляет сообщение ICMP обратно источнику.
Когда рабочая станция получает сообщение ICMP, она разделяет и отправляет пакетные данные в меньшем размере.
Рабочая станция измеряет MTU, повторяя эту передачу данных. Этот процесс называется Path MTU Discovery.



Network utilities can help to investigate network performance or resolve connection issues.
In Windows, the command prompt can be used for this purpose.
Let us learn more about command prompts such as ping, tracert, netstat, ipconfig and nslookup.

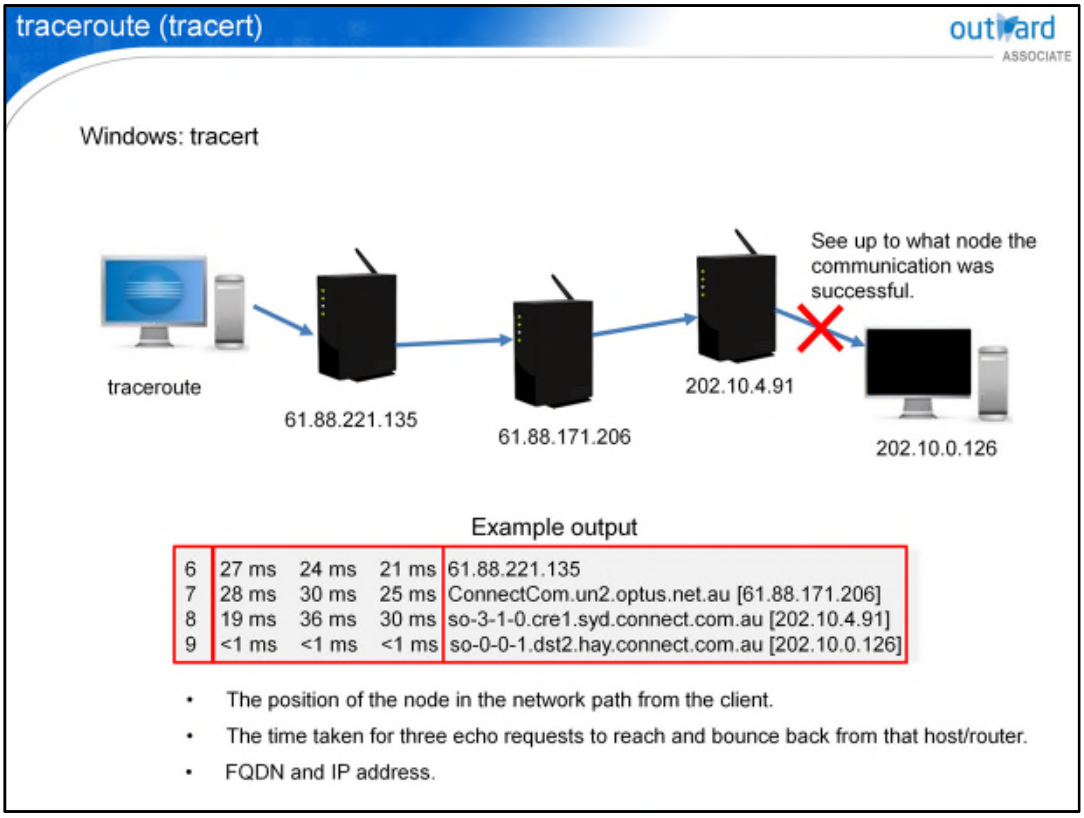
Сетевые утилиты могут помочь исследовать производительность сети или решить проблемы с подключением.
В Windows для этой цели может использоваться командная строка.
Давайте узнаем больше о командной строке, такой как ping, tracert, netstat, ipconfig и nslookup.

Пакетный Интернет Групер
Отправляет диагностический пакет на назначенный узел для проверки сетевого подключения.



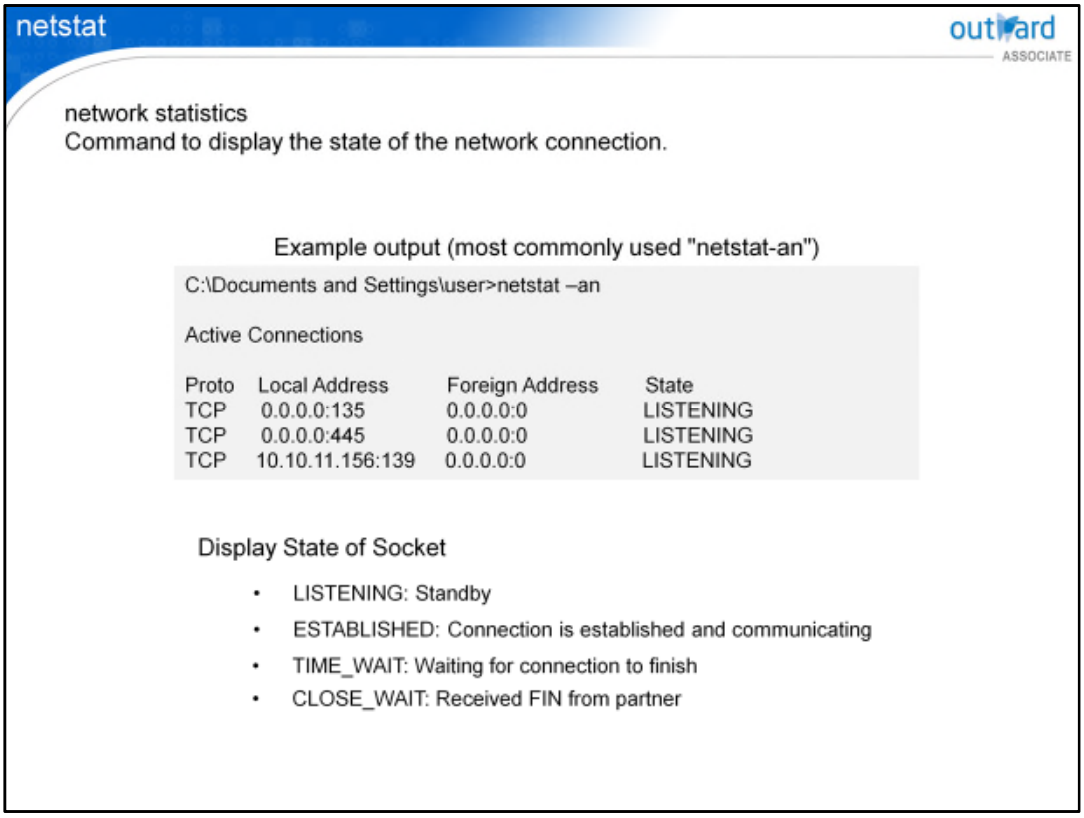
"ping" stands for Packet Internet Groper.
A ping command sends a diagnostic packet to a designated network node to check the network connection.
If the node receives the packet, it responds, confirming that the link is operational. If the node does not respond, the user is alerted to a link failure.
Ping uses ICMP to send the request and return the response or the fact that the message could not be delivered.
A network administrator will ping nodes to try to identify and isolate problems on the network and to measure performance.

«ping» означает Packet Internet Groper.
Команда ping отправляет диагностический пакет на назначенный сетевой узел для проверки сетевого подключения.
Если узел получает пакет, он отвечает, подтверждая, что канал работает.
Если узел не отвечает, пользователь получает предупреждение о сбое соединения.
Ping использует ICMP для отправки запроса и возврата ответа или того факта, что сообщение не может быть доставлено.
Сетевой администратор будет пинговать узлы, чтобы попытаться выявить и изолировать проблемы в сети и измерить производительность.



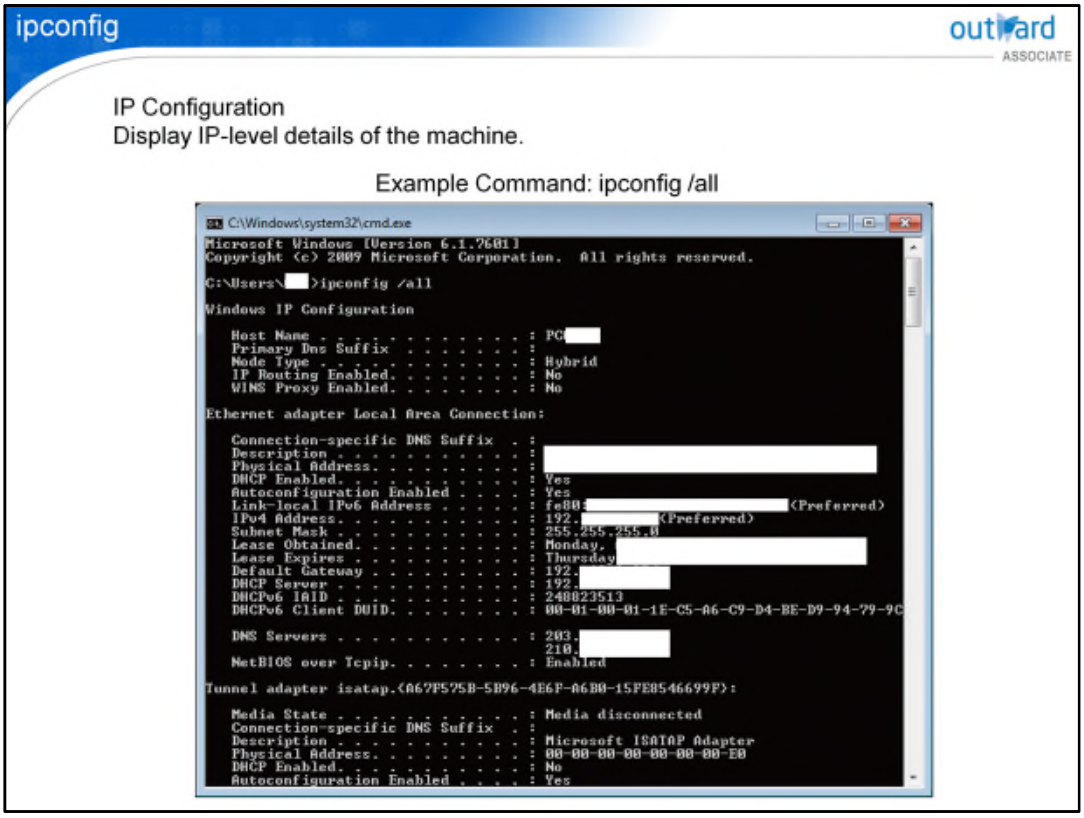
The "tracert" command is used to perform a trace route and it is a very useful diagnostic tool that goes hand in hand with ping in diagnosing common network connection issues. The tracert command is able to show the individual network nodes a packet goes through to reach its destination.
If at any point connectivity is lost using tracert it is possible to see up to what node communication was successful.
It might be that not all network nodes will return the ping. The first number corresponds to the position of the node in the network path from the client to the server.
The next three numbers indicate the time taken for three echo requests to reach and bounce back from that host/ router.
Finally, the Fully Qualified Domain Name, or FQDN for short, and Internet Protocol, or "IP", address, of the host/router is shown.
ICMP or UDP is used in tracert.
Starting with Microsoft Windows 2000, a new tool called "pathping" is also available and although it is similar to "tracert" it computes better average response times for each node on the network path.

Команда «tracert» используется для выполнения маршрута трассировки, и это очень полезный диагностический инструмент, который идет рука об руку с пингом при диагностике распространенных проблем с сетевым подключением. Команда tracert способна показать отдельным узлам сети, через которые проходит пакет, чтобы достичь пункта назначения.
Если в любой момент связь теряется с помощью tracert, можно увидеть, до какого узла связь была успешной. Может случиться так, что не все узлы сети вернут эхо-запрос. Первое число соответствует положению узла в сетевом пути от клиента к серверу.
Следующие три числа указывают время, необходимое для трех эхо-запросов, чтобы достичь и отскочить от этого хоста / маршрутизатора.
Наконец, отображается полное доменное имя, или сокращенно полное доменное имя, и интернет-протокол или IP-адрес хоста / маршрутизатора.
ICMP или UDP используется в tracert.
Начиная с Microsoft Windows 2000, новый инструмент под названием «pathping» также доступен, и хотя он похож на «tracert» вычисляет лучшее среднее время отклика для каждого узла на сетевом пути.



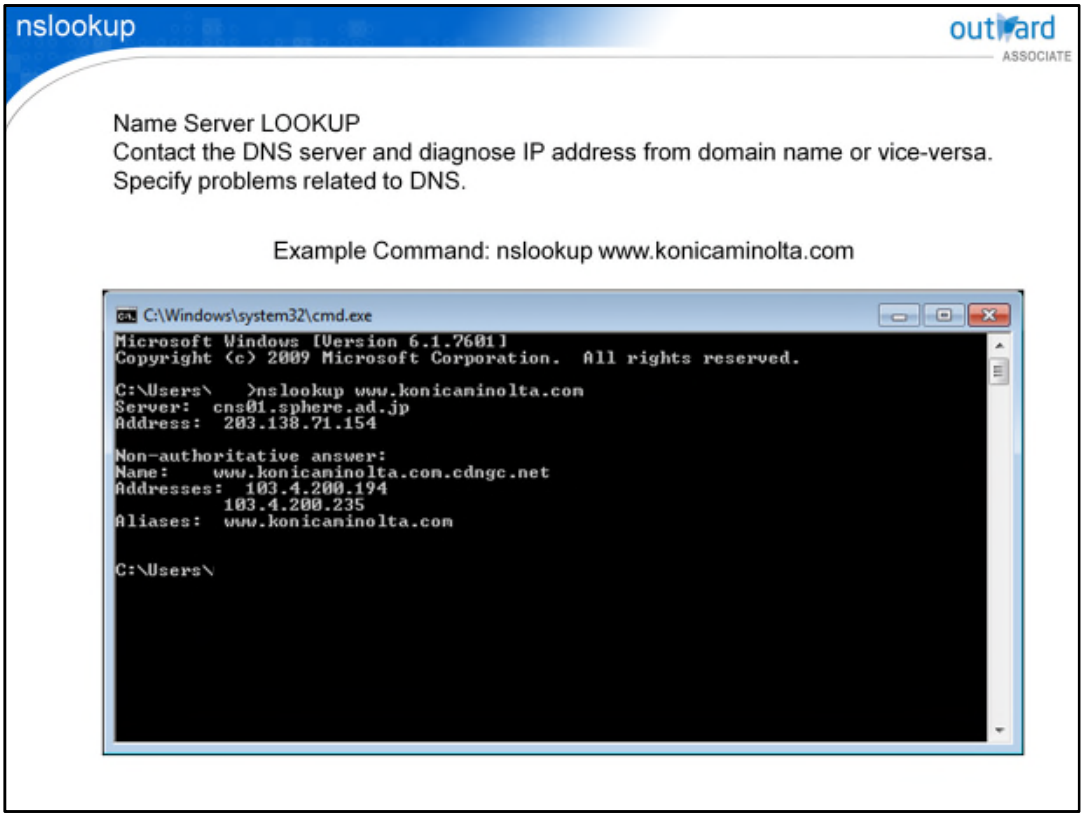
The command "netstat" stands for network statistics.
It is useful mostly on servers when you want to ensure that a particular process is running and it is correctly listening on the network for incoming connections. The "netstat" command has a number of parameters, the most commonly used one being "netstat -an".
When running "netstat -an" you can see the protocol, port number and IP address that each process is listening with on the network.
Addresses shown as 0.0.0.0 indicate that this process is listening on all available IP addresses of the host machine.

Команда «netstat» обозначает сетевую статистику.
Это полезно в основном на серверах, когда вы хотите убедиться, что конкретный процесс запущен и он правильно прослушивает в сети входящие соединения. Команда "netstat" имеет несколько параметров, наиболее часто используемым является "netstat-an".
При запуске «netstat –an» вы можете видеть протокол, номер порта и IP-адрес, который каждый процесс прослушивает в сети.
Адреса, показанные как 0.0.0.0, указывают, что этот процесс прослушивает все доступные IP-адреса хост-машины.



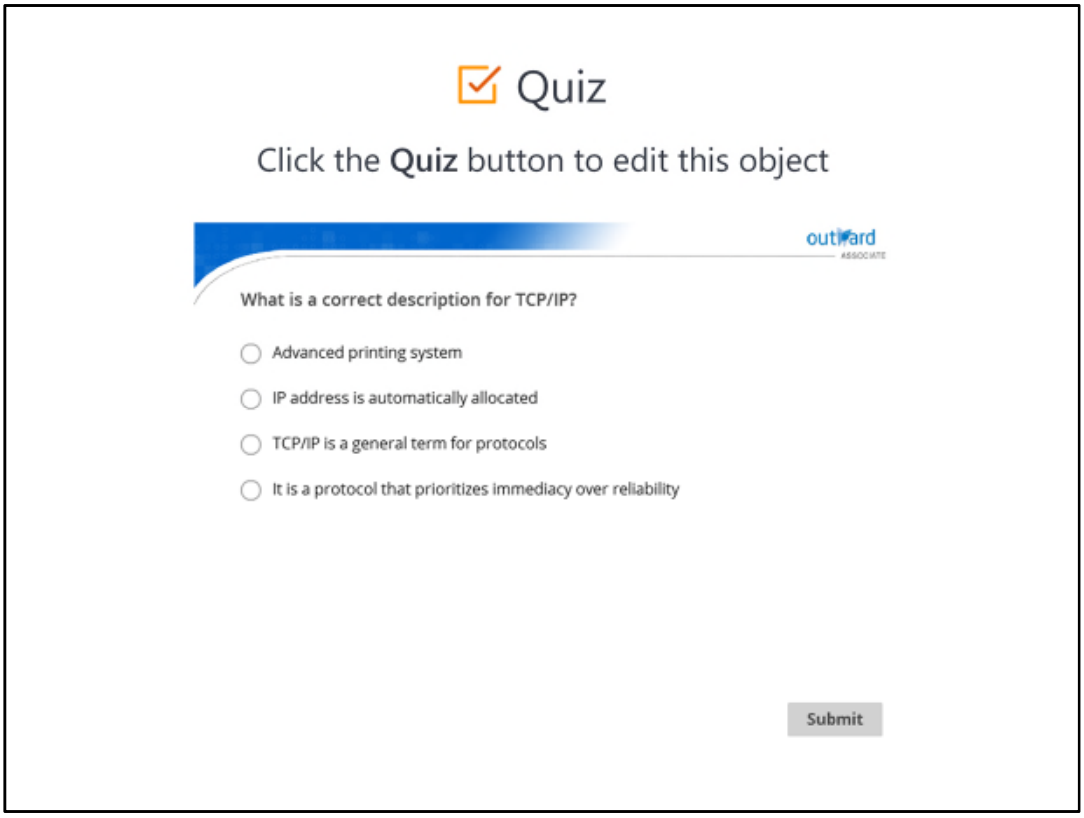
The "ipconfig" command stands for IP configuration and it is used to display IP-level details of the machine.
By default, ipconfig returns a concise view that only shows the DNS suffix, current IP address, subnet mask and default gateway.
When troubleshooting, it is best to run ipconfig using "ipconfig /all" in order to get a more complete listing of IP-level details.
In this instance, in addition to the above, you will also be able to see DNS, WINS and DHCP server details, as well as the NICs MAC address.
In older versions of Windows, before the introduction of "ipconfig", the command "winipcfg" returned similar results in regard to the networking setting of the system.
The ifconfig command is used on Linux systems.

Команда «ipconfig» обозначает конфигурацию IP и используется для отображения подробностей IP-уровня машины.
По умолчанию ipconfig возвращает краткое представление, в котором отображаются только суффикс DNS, текущий IP-адрес, маска подсети и шлюз по умолчанию.
При устранении неполадок лучше всего запустить ipconfig, используя «ipconfig / all», чтобы получить более полный список деталей уровня IP.
В этом случае, в дополнение к вышесказанному, вы также сможете увидеть сведения о DNS, WINS и DHCP-сервере, а также MAC-адрес сетевых карт.
В старых версиях Windows, до введения «ipconfig», команда «winipcfg» вернула аналогичные результаты в отношении сетевых настроек системы.
Команда ifconfig используется в системах Linux.

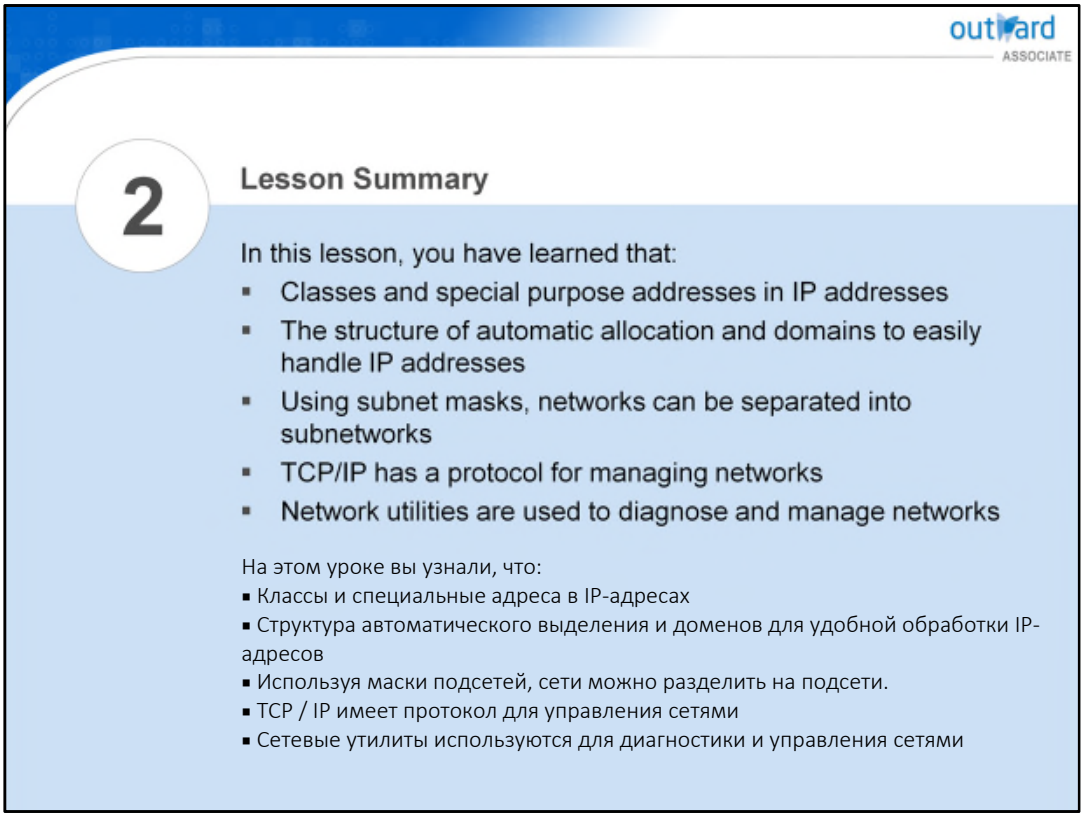


"nslookup" stands for Name Server LOOKUP.
It is possible to validate network problems, by contacting the DNS server and diagnosing the IP address from the domain name, and vice-versa.
For example, when a ping shows that connectivity exists but the FQDN fails to resolve correctly to the IP address, nslookup can be used to query and resolve the DNS server used by the client machine.
In this manner, it is also useful in diagnosing problems with the local DNS server.

«nslookup» означает сервер имен LOOKUP.
Проверить сетевые проблемы можно, связавшись с DNS-сервером и выполнив диагностику IP-адреса по доменному имени, и наоборот.
Например, когда эхо-запрос показывает, что подключение существует, но полное доменное имя не может правильно разрешить IP-адрес, nslookup можно использовать для запроса и разрешения DNS-сервера, используемого клиентским компьютером.
Таким образом, это также полезно при диагностике проблем с локальным DNS-сервером.

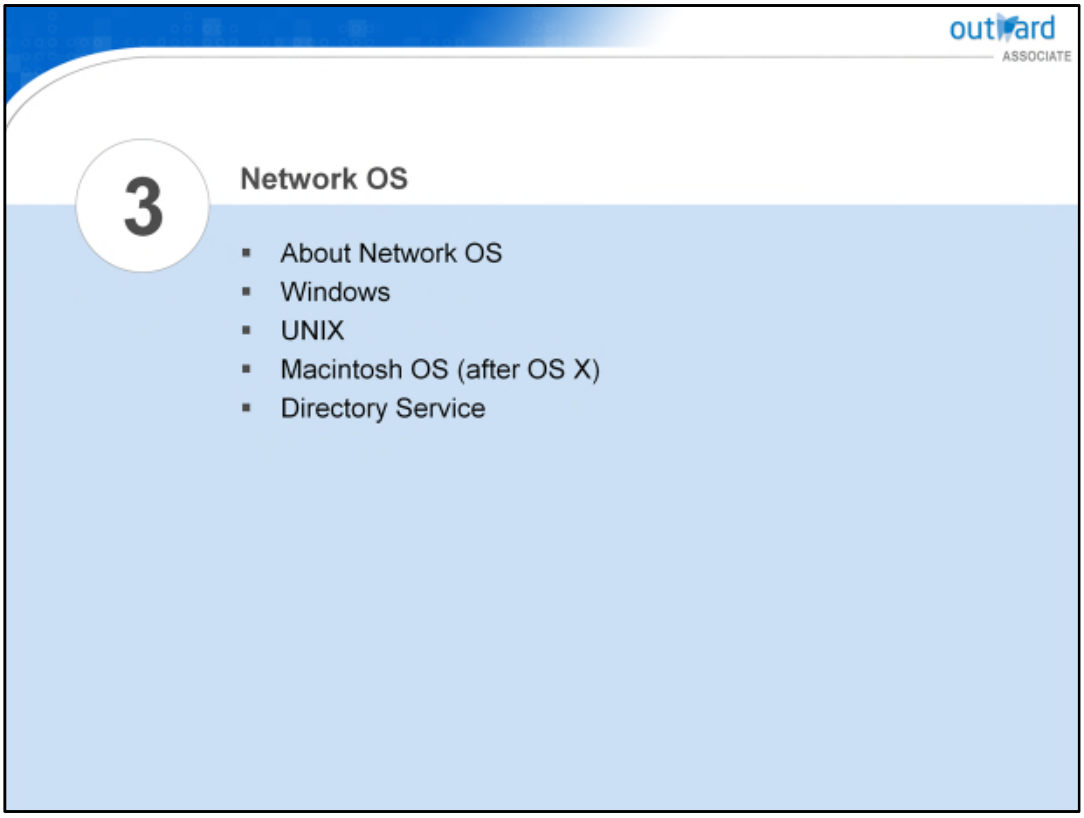


Test your knowledge in a quiz!

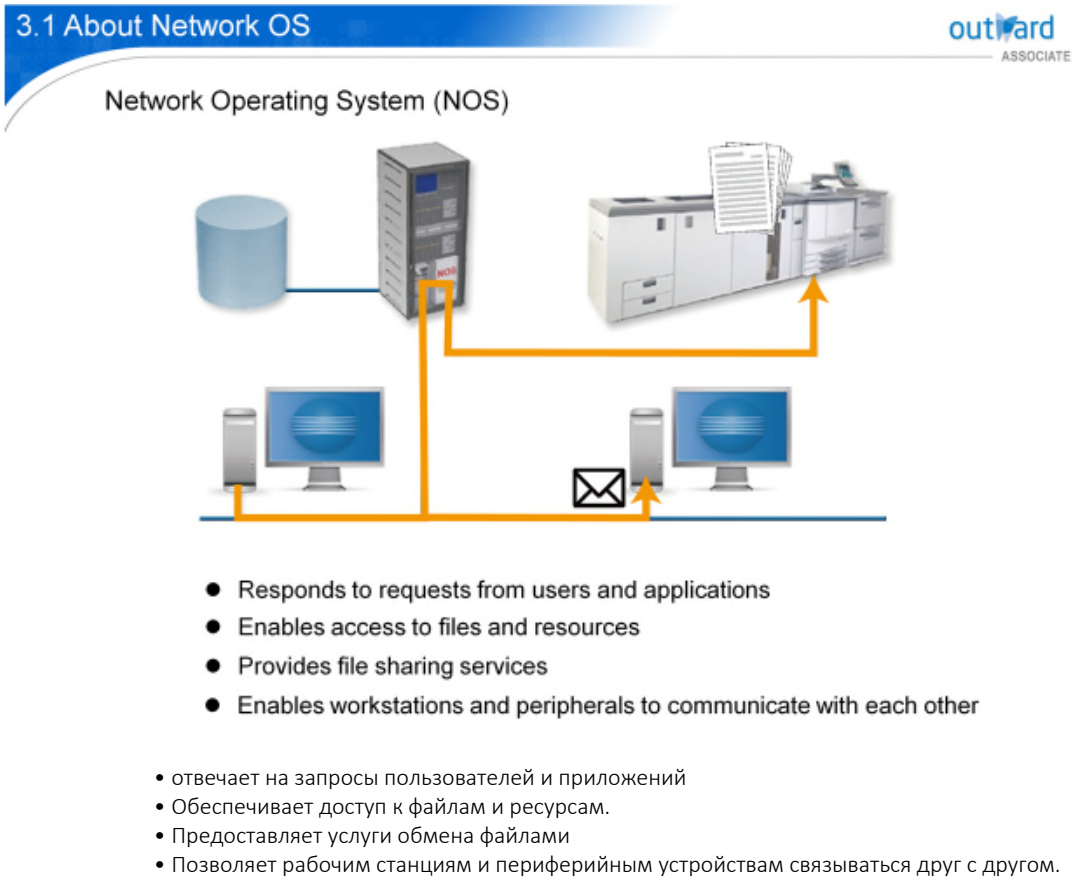


There are classes and special purpose addresses in IP addresses.
Some are not available, therefore use the appropriate number depending on your purpose.
To make IP address management easier, there is an automatic allocation method.
Moreover, since IP addresses are a series of numbers and are hard to remember, there is a system called DNS which converts them into alphanumeric characters.
Networks can effectively use limited IP addresses when they are simply sorted into classes. For that reason, they may be divided into subnetworks.
TCP/IP has a protocol to manage networks. They are widely used with network utilities such as ping.

В IP-адресах есть классы и специальные адреса.
Некоторые из них недоступны, поэтому используйте соответствующий номер в зависимости от вашей цели.
Чтобы упростить управление IP-адресами, существует метод автоматического выделения. Более того, поскольку IP-адреса представляют собой последовательность чисел и их трудно запомнить, существует система DNS, которая преобразует их в буквенно-цифровые символы.
Сети могут эффективно использовать ограниченные IP-адреса, когда они просто сортируются по классам. По этой причине они могут быть разделены на подсети.
TCP / IP имеет протокол для управления сетями. Они широко используются с сетевыми утилитами, такими как ping.

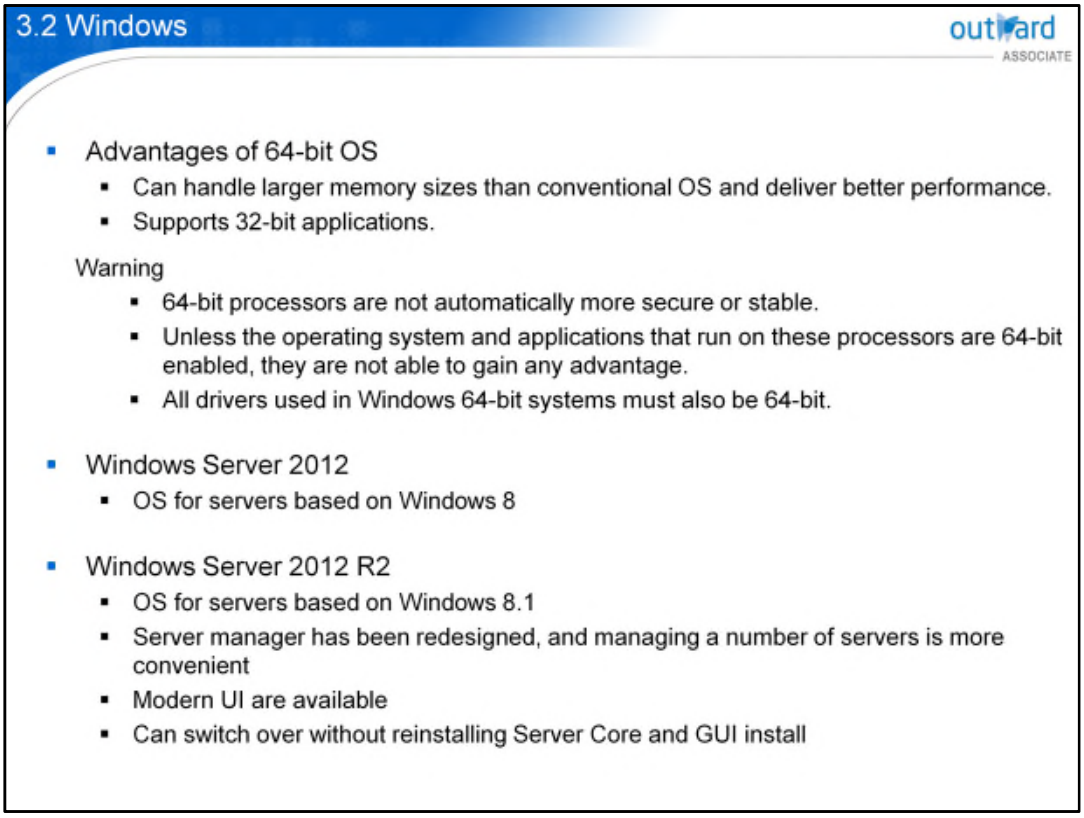


This lesson explains how network operating systems enable workstations to use networks.



A network operating system, or NOS, is a computer operating system that enables workstations to use network resources and services.
In addition, a NOS makes such resources and services available to the rest of the clients on the network via servers. Examples of commonly used NOS are Mac OS, Windows and Linux.
NOS respond to requests from users and applications, and delivers a variety of services.
NOS enable access to files and resources, and provide file sharing services. It can enable workstations and peripherals to communicate with each other.

Сетевая операционная система, или NOS, является компьютерной операционной системой, которая позволяет рабочим станциям использовать сетевые ресурсы и сервисы.
Кроме того, NOS делает такие ресурсы и сервисы доступными для остальных клиентов в сети через серверы. Примерами обычно используемых NOS являются Mac OS, Windows и Linux.
NOS отвечает на запросы пользователей и приложений и предоставляет различные услуги.
NOS обеспечивает доступ к файлам и ресурсам, а также предоставляет сервисы обмена файлами. Это может позволить рабочим станциям и периферийным устройствам связываться друг с другом.



Преимущества 64-битной ОС
- Может обрабатывать больший объем памяти, чем обычные ОС, и обеспечивать лучшую производительность.
- Поддерживает 32-битные приложения.

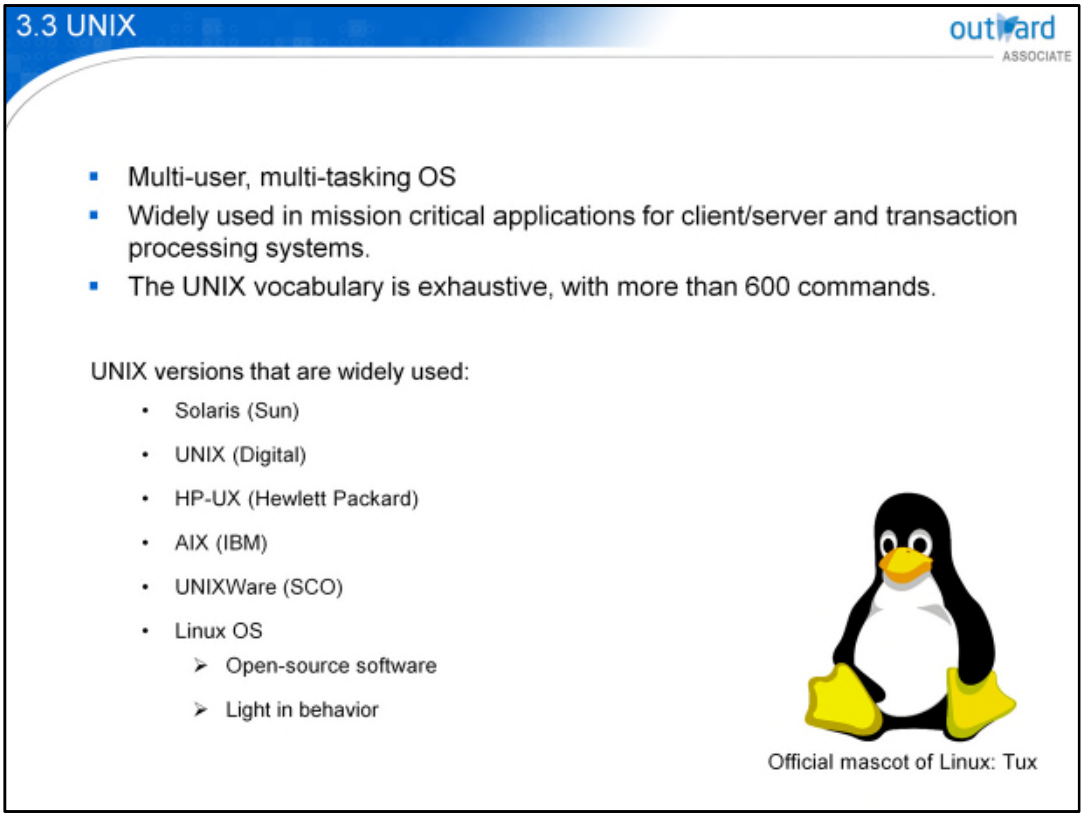
Предупреждение
- 64-разрядные процессоры не являются автоматически более безопасными или стабильными.
- Если операционная система и приложения, работающие на этих процессорах, не являются 64-разрядными включены, они не могут получить никакого преимущества.
- Все драйверы, используемые в 64-разрядных системах Windows, также должны быть 64-разрядными.

Windows Server 2012
- ОС для серверов на базе Windows 8

Windows Server 2012 R2
- ОС для серверов на базе Windows 8.1
- Диспетчер серверов был переработан, и управление несколькими серверами стало более удобным
- Современный пользовательский интерфейс
- Может переключаться без переустановки Server Core и установки с графическим интерфейсом

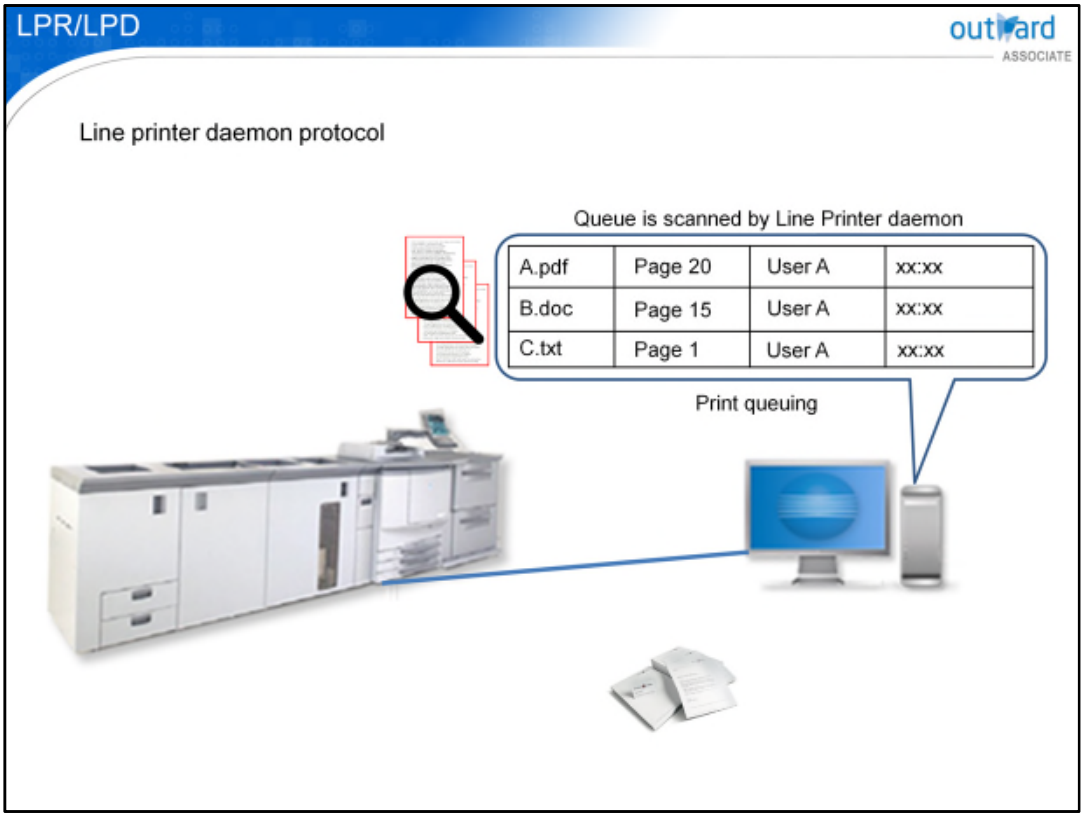
Recent developments in central processing units, commonly known as CPUs, have allowed 64-bit processors to become affordable and easily accessible for purchase by the general public. 64-bit processors can offer significant advantages in speed, the size of memory they are able to address and in other areas and potentially deliver better performance. However, operating systems that support 64-bit processors are not automatically more secure or stable.
Moreover, unless the operating system and applications that run on these processors are 64-bit enabled they are not able to gain any advantages.
Microsoft Windows operating editions have provided 64-bit support since Windows XP and Windows Server 2003. Windows 64-bit systems support 32-bit applications as well for backwards compatibility. 32-bit drivers are not supported, therefore all drivers used in Windows 64-bit systems must also be 64-bit.
Windows Server 2012 is Microsoft's operating system for servers.
It is an OS for servers based on Windows 8, and is a successor OS to Windows Server 2008 R2.
Windows Server 2012 is based on Windows 8.1.
As server managers have been redesigned, managing a number of servers is more convenient, and unless Server Core mode is installed, modern UI are available.
Unlike Windows Server 2008 R2, Windows Server 2012 can switch over without reinstalling Server Core and GUI install.

Последние разработки в центральных процессорах, обычно называемые процессорами, позволили 64-разрядным процессорам стать доступными и легко доступными для приобретения широкой публикой. 64-разрядные процессоры могут предложить значительные преимущества в скорости, объеме памяти, к которому они могут обращаться и в других областях, и потенциально могут обеспечить более высокую производительность. Однако операционные системы, которые поддерживают 64-разрядные процессоры, не являются автоматически более безопасными или стабильными.
Более того, если операционная система и приложения, работающие на этих процессорах, не поддерживают 64-разрядную архитектуру, они не смогут получить никаких преимуществ.
Операционные выпуски Microsoft Windows предоставляют 64-разрядную поддержку начиная с Windows XP и Windows Server 2003. 64-разрядные системы Windows поддерживают 32-разрядные приложения, а также обеспечивают обратную совместимость. 32-разрядные драйверы не поддерживаются, поэтому все драйверы, используемые в 64-разрядных системах Windows, также должны быть 64-разрядными.
Windows Server 2012 - это операционная система Microsoft для серверов.
Это ОС для серверов на базе Windows 8 и преемник ОС Windows Server 2008 R2.
Windows Server 2012 основан на Windows 8.1.
Поскольку менеджеры серверов были переработаны, управление несколькими серверами стало более удобным, и, если не установлен режим Server Core, доступен современный пользовательский интерфейс.
В отличие от Windows Server 2008 R2, Windows Server 2012 может переключаться без переустановки Server Core и установки с графическим интерфейсом.

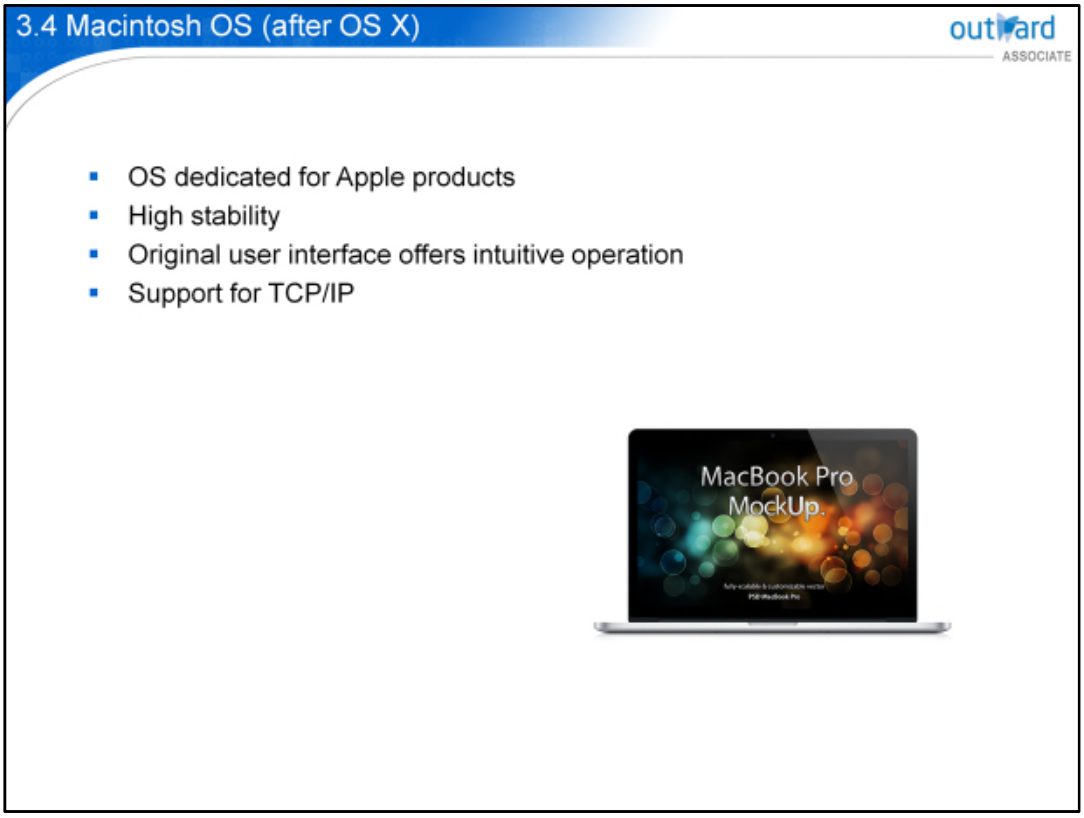


UNIX is a multi-user, multi-tasking operating system that is widely used as the master control program in workstations and servers. There are many versions of UNIX on the market. Many IBM mainframes also run UNIX applications. Because UNIX interfaces have been added to the operating system, they have obtained UNIX branding such as MVS and OS/390.
Although the majority of general computers are Windows, UNIX is widely used in mission critical applications for client/server and transaction processing systems.
Gnu/Linux is also built on the same principles as UNIX and utilizes a similar architecture.
The UNIX vocabulary is exhaustive, with more than 600 commands that manipulate data and text.
Linux is one of the operating systems that is compatible with UNIX.
It is written without diverting other OS and published as open-source software.
Linux has a similar specification to UNIX, operates lightly, is widely used and continues to grow in popularity.

UNIX - это многопользовательская многозадачная операционная система, широко используемая в качестве основной программы управления на рабочих станциях и серверах.
На рынке существует много версий UNIX. Многие мэйнфреймы IBM также работают с приложениями UNIX. Поскольку интерфейсы UNIX были добавлены в операционную систему, они получили маркировку UNIX, такую как MVS и OS / 390.
Хотя большинство обычных компьютеров являются Windows, UNIX широко используется в критически важных приложениях для систем клиент-сервер и обработки транзакций.
Gnu / Linux также построен на тех же принципах, что и UNIX, и использует аналогичную архитектуру.
Словарь UNIX является исчерпывающим, с более чем 600 командами, которые манипулируют данными и текстом.
Linux является одной из операционных систем, совместимых с UNIX.
Он написан без использования других ОС и опубликован как программное обеспечение с открытым исходным кодом. Linux имеет спецификацию, аналогичную UNIX, работает слабо, широко используется и продолжает расти в популярности.

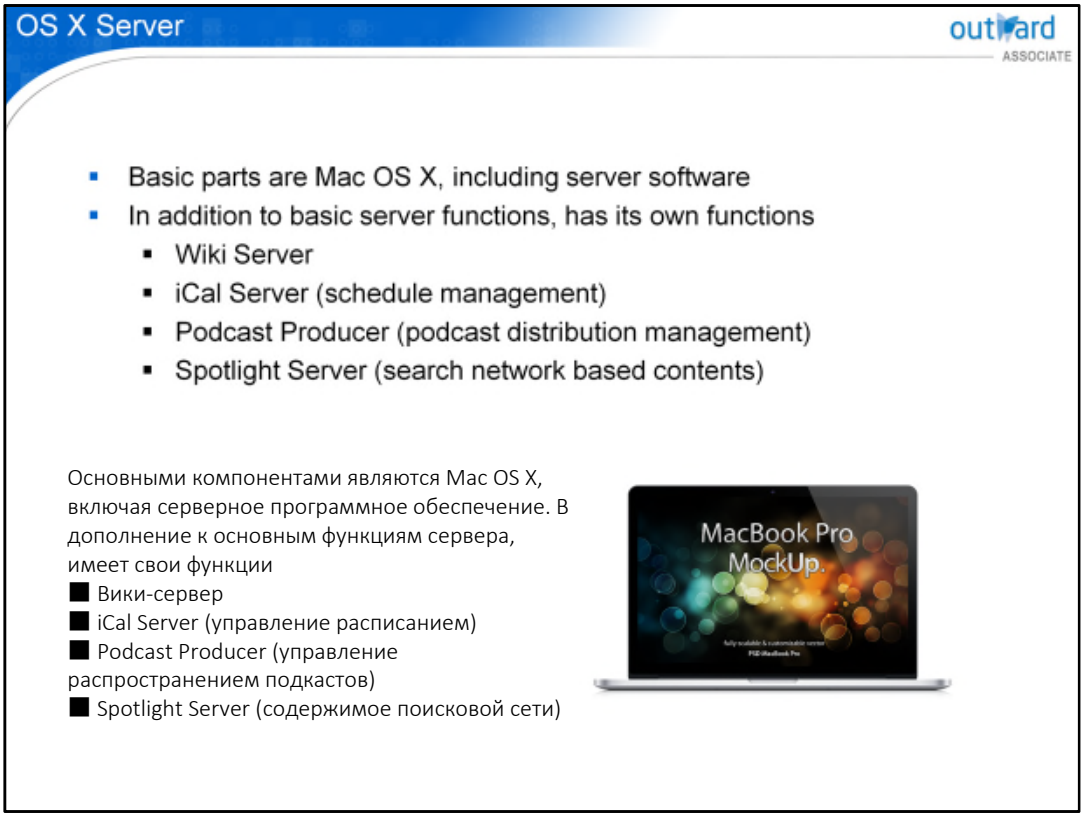


UNIX has a sophisticated set of printing utilities that are sometimes used under other operating systems. They are called the LPR system and are TCP/IP based protocol.
In this system, data to be printed is "spooled" to a file, where it waits until the printer is free to print. This is known as print queuing.
The queue is scanned by the line printer daemon, which acts as the print server.
The benefit of the LPR system is that it quickly moves the file to the spool area, freeing up the operating system to carry out other tasks, while the LPD manages the printing.
LPR is used with TCP/IP under NOS such as Windows and Mac OS to increase print speed.
However, today most Linux and some UNIX systems use the Common UNIX Printing System, CUPS for short, instead of LRP/LPD.
CUPS is an open-source printing system modularized for the UNIX OS. Users can use CUPS with a web browser.
UNIX имеет сложный набор утилит печати, которые иногда используются в других операционных системах.
Они называются системой LPR и основаны на протоколе TCP / IP.
В этой системе данные, которые будут напечатаны, «помещаются в буфер» в файл, где он ожидает, пока принтер не освободится для печати. Это известно как очередь печати.
Очередь сканируется демоном линейного принтера, который действует как сервер печати.
Преимущество системы LPR заключается в том, что она быстро перемещает файл в область спула, освобождая операционную систему для выполнения других задач, а LPD управляет печатью.
LPR используется с TCP / IP под NOS, например, Windows и Mac OS, для увеличения скорости печати.
Однако сегодня большинство систем Linux и некоторых систем UNIX используют общую систему печати UNIX, сокращенно CUPS, вместо LRP / LPD.
CUPS - это система печати с открытым исходным кодом, модульная для ОС UNIX. Пользователи могут использовать CUPS с веб-браузером.



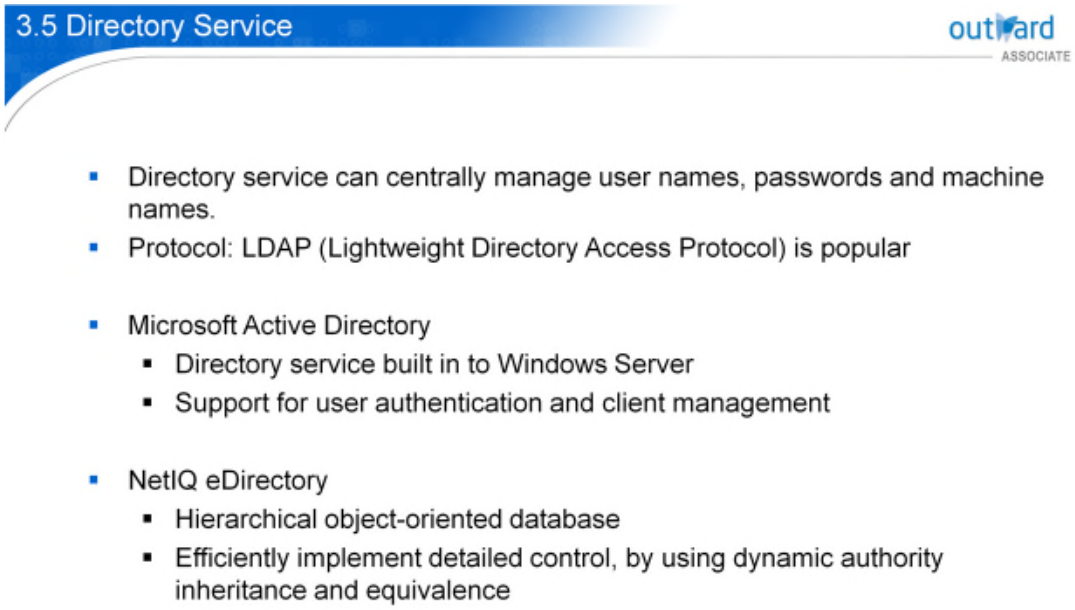
Apple's Mac OS X is designed to run only on Apple's line of hardware. High stability is ensured by creating hardware and OS in one company.
A window system that is established in an original user interface called Aqua is built-in and offers intuitive operation. Mac OS was developed based on UNIX, so this is also a robust OS like UNIX and has comprehensive command-line tools.
Apple now supports TCP/IP as the base communication protocol for Mac OS X, unlike some of its earlier operating systems.
As a result Mac OS X machines can co-exist on the same network as Linux and Windows workstations, and connect to the same file and print servers and to one another easily.

Apple Mac OS X предназначена для работы только на линейке оборудования Apple. Высокая стабильность обеспечивается созданием оборудования и ОС в одной компании.
Оконная система, которая установлена в оригинальном пользовательском интерфейсе под названием Aqua, является встроенной и предлагает интуитивно понятное управление. Mac OS была разработана на основе UNIX, так что это также надежная ОС, такая как UNIX, и имеет комплексные инструменты командной строки.
Apple в настоящее время поддерживает TCP / IP в качестве базового протокола связи для Mac OS X, в отличие от некоторых его более ранних операционных систем.
В результате машины Mac OS X могут сосуществовать в той же сети, что и рабочие станции Linux и Windows, и легко подключаться к одним и тем же серверам файлов и печати и друг к другу.



OS X Server is a server operating system only for Macintosh, developed and sold by Apple.
Basic parts such as the operating screen are the same as Mac OS X, and include open source and server software. In addition to basic server functions such as Web server, mail server, and directory service, original functions such as Wiki Server and iCal Server, Podcast Producer, Spotlight Server are available as well.

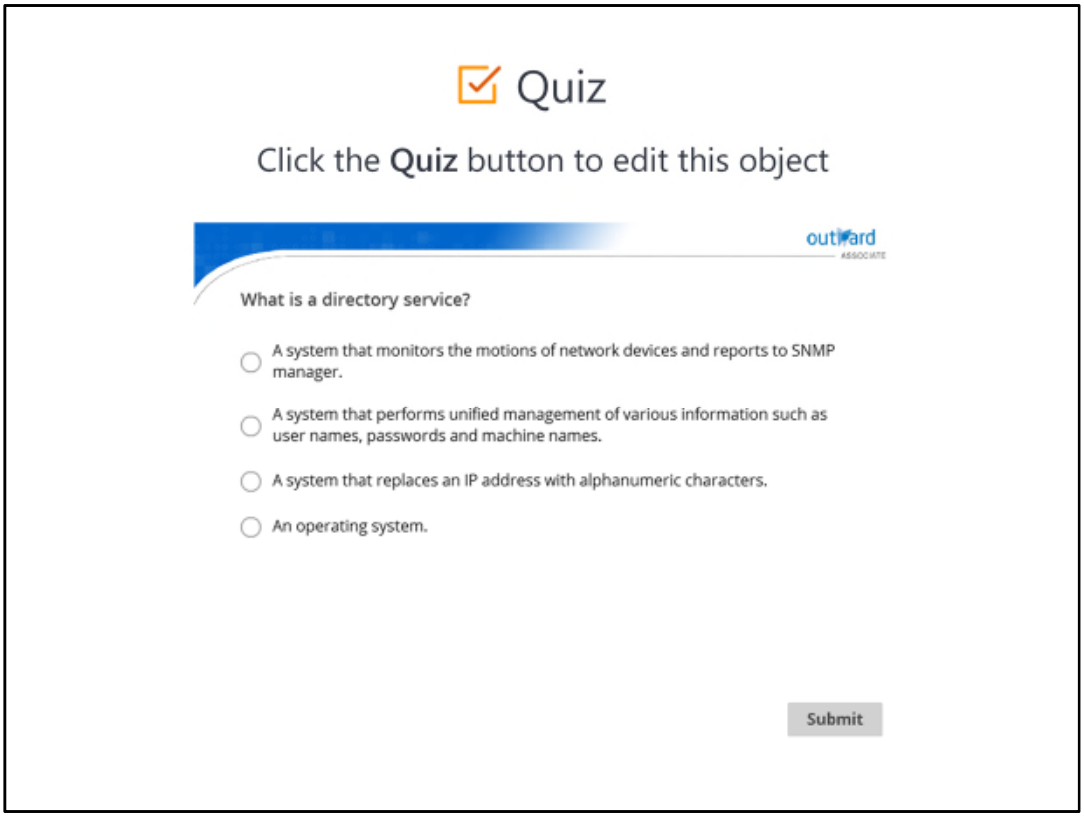
OS X Server - это серверная операционная система только для Macintosh, разработанная и продаваемая Apple.
Основные части, такие как рабочий экран, такие же, как Mac OS X, и включают в себя программное обеспечение с открытым исходным кодом и серверное программное обеспечение. В дополнение к базовым функциям сервера, таким как веб-сервер, почтовый сервер и служба каталогов, также доступны оригинальные функции, такие как Wiki-сервер и iCal Server, Podcast Producer, Spotlight Server.



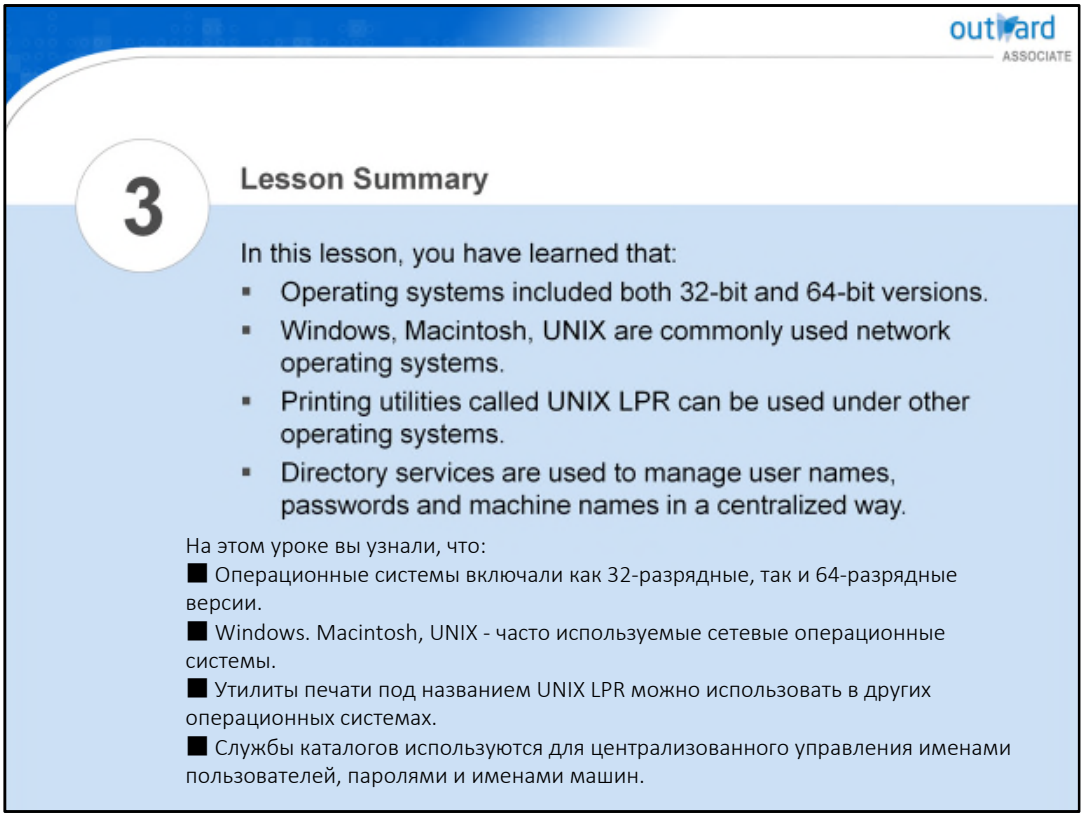
Служба каталогов может централизованно управлять именами пользователей, паролями и именами компьютеров.
Протокол: LDAP (облегченный протокол доступа к каталогам) популярен
Microsoft Active Directory
■ Служба каталогов, встроенная в Windows Server
■ Поддержка аутентификации пользователя и управления клиентом
NetIQ eDirectory
■ Иерархическая объектно-ориентированная база данных
■ Эффективно реализовать детальное управление, используя динамическое наследование и эквивалентность полномочий.

Directory services hold various information such as user names and passwords to use the network, machine names, and the like, and LDAP is a popular communication protocol. Typical directory services include NetIQ eDirectory, Apple Open Directory, Microsoft Active Directory.
LDAP is a communication protocol to access directory service using TCP/IP networks.
Microsoft Active Directory is a directory service built in to Windows server since Windows 2000, and is used to centrally manage various data or authority on resources and users on the network.
In addition to the directory service, it also provides support for user authentication and client management.
NetIQ eDirectory is a hierarchical object-oriented database that represents every asset in the organization in a logic tree. Assets include people in the enterprise, network devices, network applications, relationships between information, and so on.
By using dynamic authority inheritance and equivalence, detailed control can be implemented efficiently.

Службы каталогов содержат различную информацию, такую как имена пользователей и пароли для использования сети, имена компьютеров и тому подобное, а LDAP является популярным протоколом связи. Типичные службы каталогов включают NetIQ eDirectory, Apple Open Directory, Microsoft Active Directory.
LDAP - это протокол связи для доступа к службе каталогов с использованием сетей TCP / IP.
Microsoft Active Directory - это служба каталогов, встроенная в сервер Windows начиная с Windows 2000 и используемая для централизованного управления различными данными или полномочиями в отношении ресурсов и пользователей в сети.
Помимо службы каталогов, она также обеспечивает поддержку аутентификации пользователей и управления клиентами.
NetIQ eDirectory - это иерархическая объектно-ориентированная база данных, которая представляет каждый актив в организации в логическом дереве. К активам относятся люди на предприятии, сетевые устройства, сетевые приложения, взаимосвязи между информацией и т. Д. Используя динамическое наследование и эквивалентность полномочий, можно эффективно реализовать детальное управление.

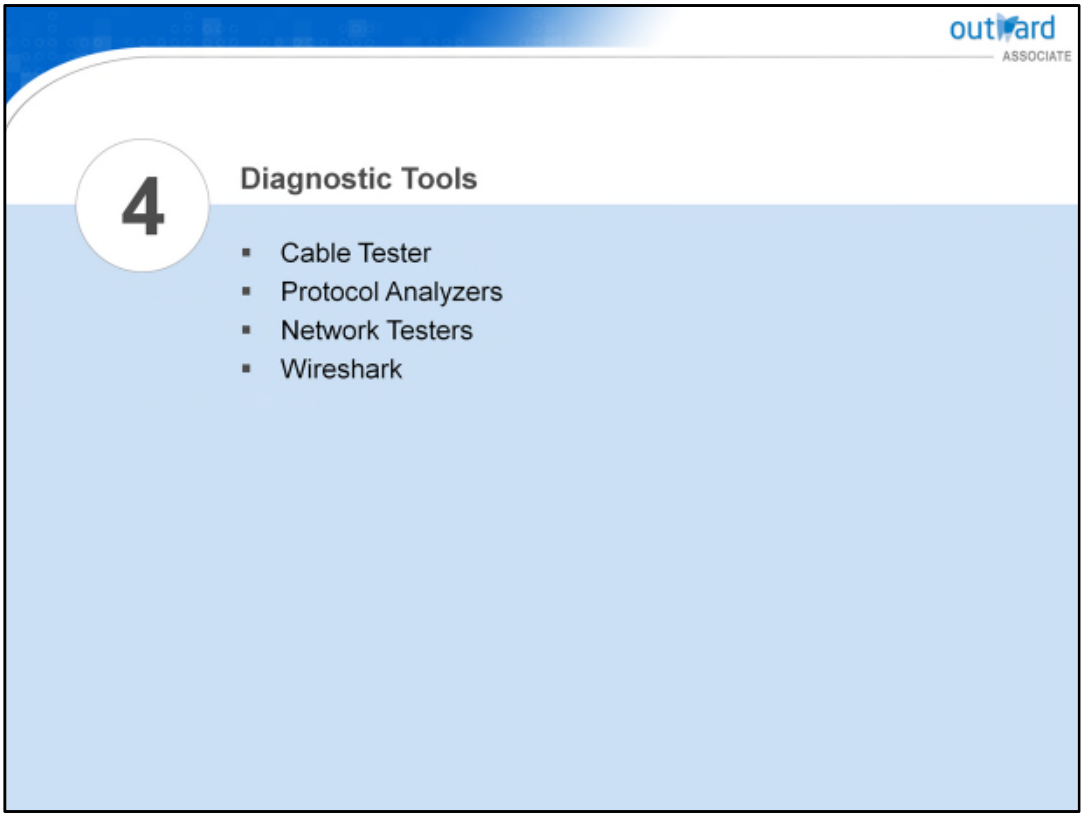


Test your knowledge in a quiz!



Currently, operating systems include both 32-bit and 64-bit versions.
64-bit processors provide the maximum amount of memory usage, but users need to be cautious in terms of compatibility aspects.
Windows, Macintosh, UNIX are commonly used network operating systems.
Each product provides different features, therefore each plays an active roll in different scenes.
Besides UNIX, which plays an important role in large companies and financial systems, an advanced printing utility called LPR are adopted for use with other NOS. Moreover, by adopting directory services such as NetIQ Directory or Microsoft Active Directory, it is possible to manage network user names, passwords, and machine names in a centralized way.

В настоящее время операционные системы включают как 32-разрядные, так и 64-разрядные версии.
64-разрядные процессоры обеспечивают максимальный объем использования памяти, но пользователи должны быть осторожны с точки зрения совместимости.
Windows, Macintosh, UNIX - часто используемые сетевые операционные системы.
Каждый продукт предоставляет различные функции, поэтому каждый играет активный ролл в разных сценах.
Помимо UNIX, который играет важную роль в крупных компаниях и финансовых системах, для использования с другими NOS приняты расширенные утилиты печати под названием LPR. Более того, приняв такие службы каталогов, как NetIQ Directory или Microsoft Active Directory, можно централизованно управлять именами пользователей, паролями и именами компьютеров в сети.



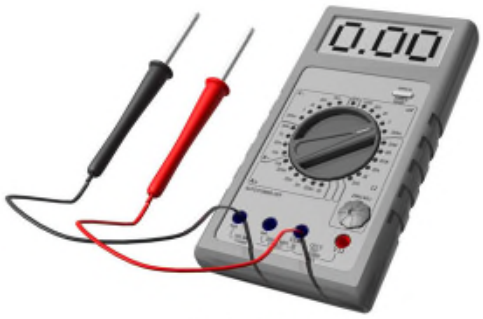
Ongoing network maintenance is essential for efficient network performance.
Networks require both hardware and software maintenance, which in turn requires a range of different network tools. This section explains typical network tools, including cable testers, protocol analyzers, network testers and Wireshark.

Текущее обслуживание сети имеет важное значение для эффективной работы сети.
Сети требуют обслуживания как аппаратного, так и программного обеспечения, что, в свою очередь, требует целого ряда различных сетевых инструментов. В этом разделе описываются типичные сетевые инструменты, в том числе кабельные тестеры, анализаторы протоколов, сетевые тестеры и Wireshark.

4.1 Cable Tester

outpard ASSOCIATE

Electrical analysis of cables and connections

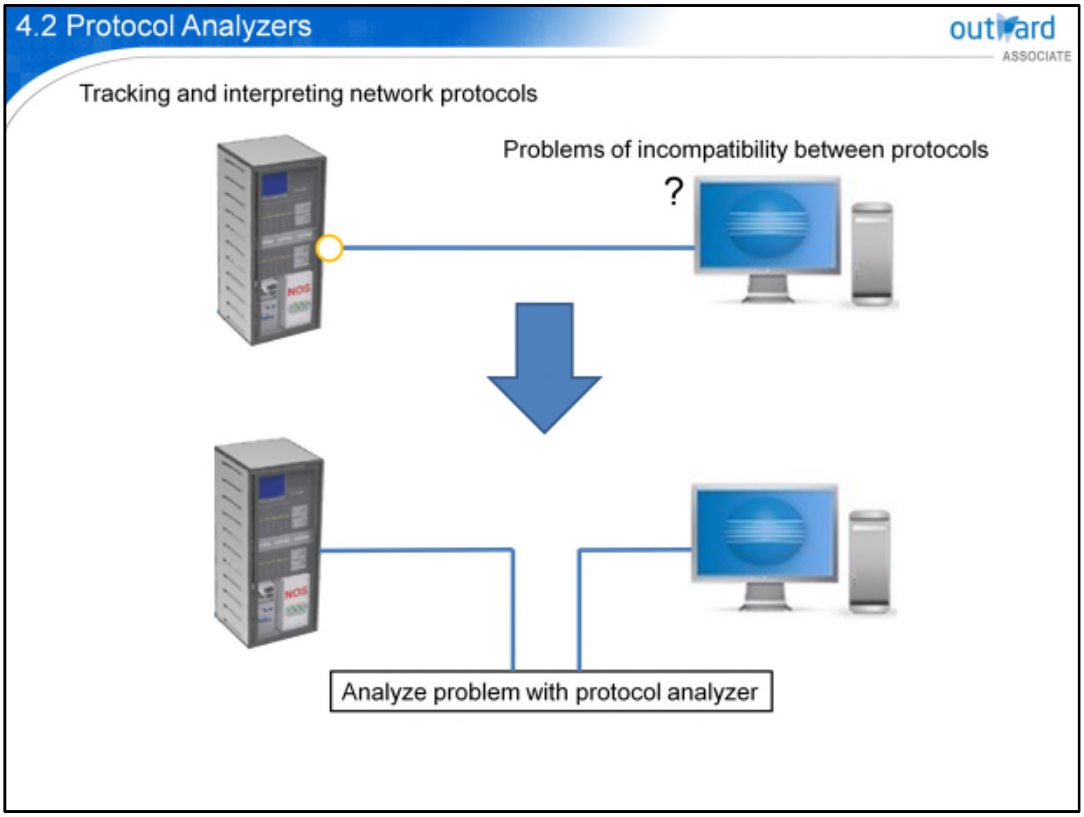


Cable Tester

Type	Target	Use
Voltmeters	Voltage	Check that network signals are at appropriate levels
Ohmmeters	Resistance	Check the integrity of connections between cabling and network hardware
Multimeters	Open circuits in a network	Test for open circuits or bad cable connections

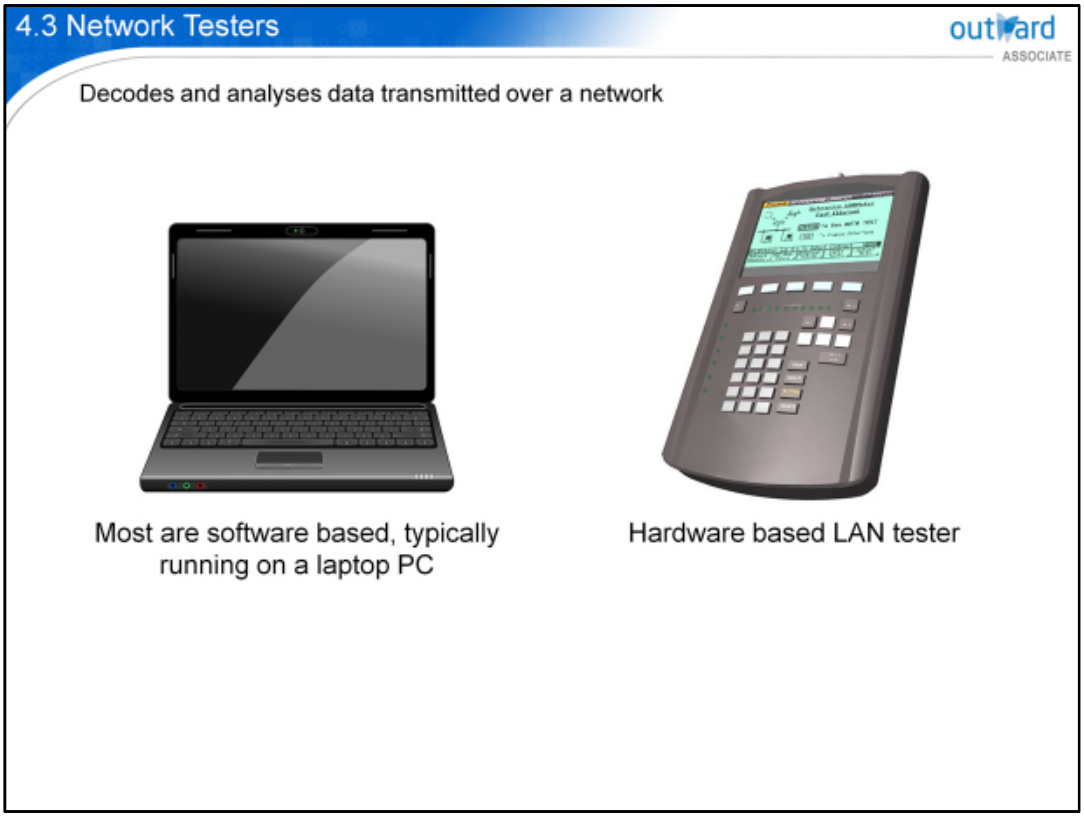
A cable tester is essential for analyzing considerable amounts of cabling and numbers of connections. They measure voltage and resistance levels at as many nodes as possible around the network.
Voltmeters are instruments that measure system voltages and inform the engineer if network signals are at appropriate levels.
Ohmmeters measure the resistance of a device in ohms. Ohmmeters typically test for open and short circuits in network hardware, thus informing the engineer of the integrity of connections between cabling and network hardware.
Multimeters are devices that can be used to test voltage or resistance and can be used to test for open circuits or signals within networks.
By measuring the resistance between two connectors, it is possible to test for open circuits or bad cable connections.

Кабельный тестер необходим для анализа значительного количества кабелей и количества соединений.
Они измеряют уровни напряжения и сопротивления на максимально возможном количестве узлов в сети.
Вольтметры - это приборы, которые измеряют напряжение в системе и информируют инженера, находятся ли сетевые сигналы на соответствующих уровнях.
Омметры измеряют сопротивление устройства в омах. Омметры обычно тестируют на обрыв и короткое замыкание в сетевом оборудовании, таким образом информируя инженера о целостности соединений между кабелем и сетевым оборудованием.
Мультиметры - это устройства, которые могут использоваться для проверки напряжения или сопротивления и могут использоваться для проверки обрыва цепи или сигналов в сетях.
Измеряя сопротивление между двумя разъемами, можно проверить на обрыв цепи и плохие кабельные соединения.



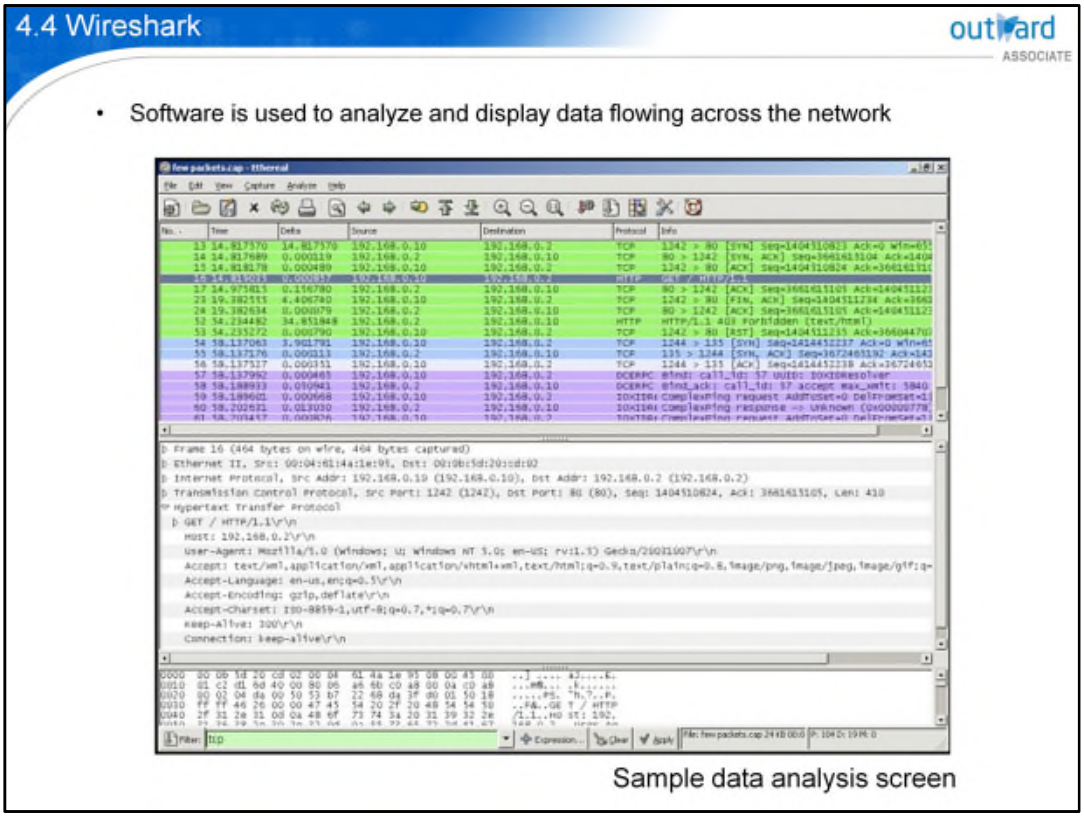
Protocol analyzers are software testers for tracking and interpreting network protocols. Protocols are essential for the efficient operation of networks and provide information on interactions between workstations, servers and peripheral devices. Therefore, protocol analyzers can help diagnose intricate problems of incompatibility between different network devices. Because of stable standards that define LAN and WAN interconnectivity and communication, there are very few protocol incompatibilities in software and hardware components that are shipped for use by businesses.
This has lead to the diminishing use of protocol analyzers by everyday network technicians and administrators. However, they remain extremely important and useful tools for network designers and other IT specialists.

Анализаторы протоколов - это программные тестеры для отслеживания и интерпретации сетевых протоколов.
Протоколы необходимы для эффективной работы сетей и предоставляют информацию о взаимодействиях между рабочими станциями, серверами и периферийными устройствами. Таким образом, анализаторы протоколов могут помочь диагностировать сложные проблемы несовместимости между различными сетевыми устройствами. Из-за стабильных стандартов, определяющих взаимосвязь и связь LAN и WAN, очень мало несовместимостей протоколов в программных и аппаратных компонентах, которые поставляются для использования предприятиями.
Это привело к уменьшению использования анализаторов протоколов обычными сетевыми техниками и администраторами. Тем не менее, они остаются чрезвычайно важными и полезными инструментами для разработчиков сетей и других ИТ-специалистов.



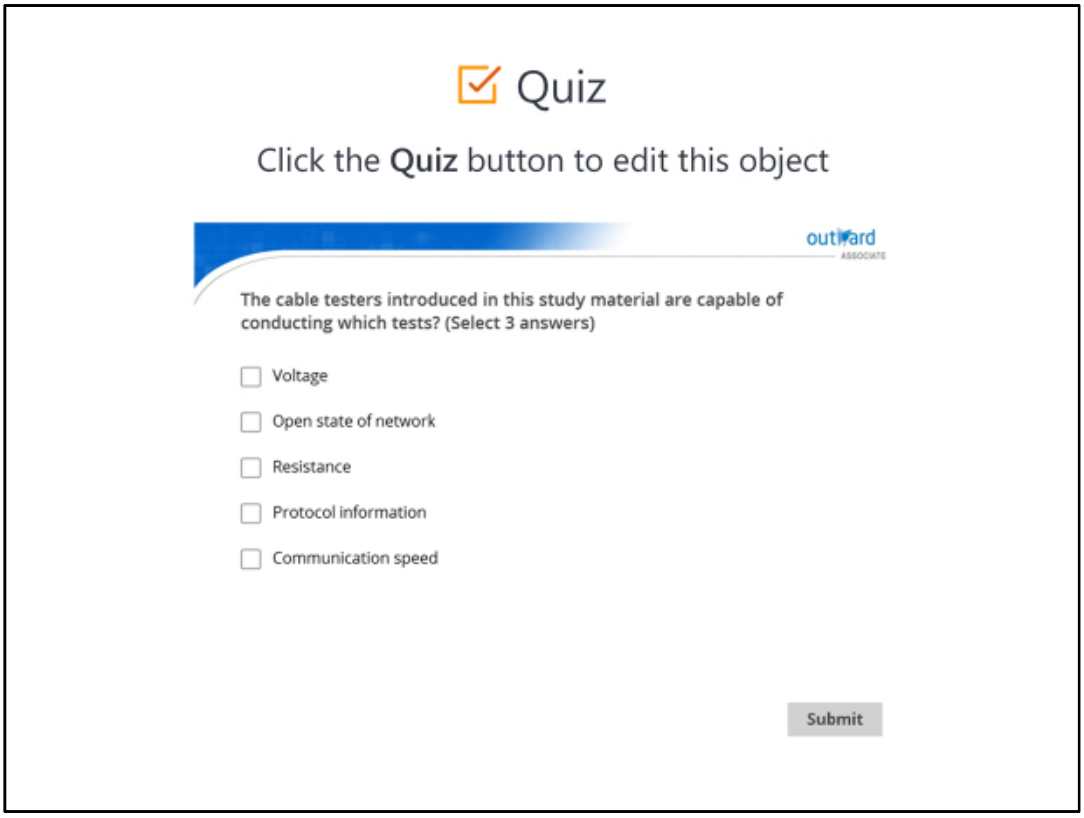
A network tester decodes and analyses data transmitted over a network.
There are numerous types of testers available, ranging from relatively simple software programs to purpose specific workstations.
Testers not only receive existing network data, they can also formulate and transmit data packets designed to test specific aspects of the network.
Most network testers are software-based, typically running on a laptop PC.
However, there are still some that are hardware-based, such as the one shown here.

Тестер сети декодирует и анализирует данные, передаваемые по сети.
Существует множество типов тестеров, начиная с относительно простых программ и заканчивая конкретными рабочими станциями.
Тестеры не только получают существующие сетевые данные, они также могут формулировать и передавать пакеты данных, предназначенные для тестирования определенных аспектов сети.
Большинство сетевых тестеров основаны на программном обеспечении и обычно работают на ноутбуке.
Тем не менее, есть некоторые, которые основаны на аппаратном обеспечении, такие как показанный здесь.

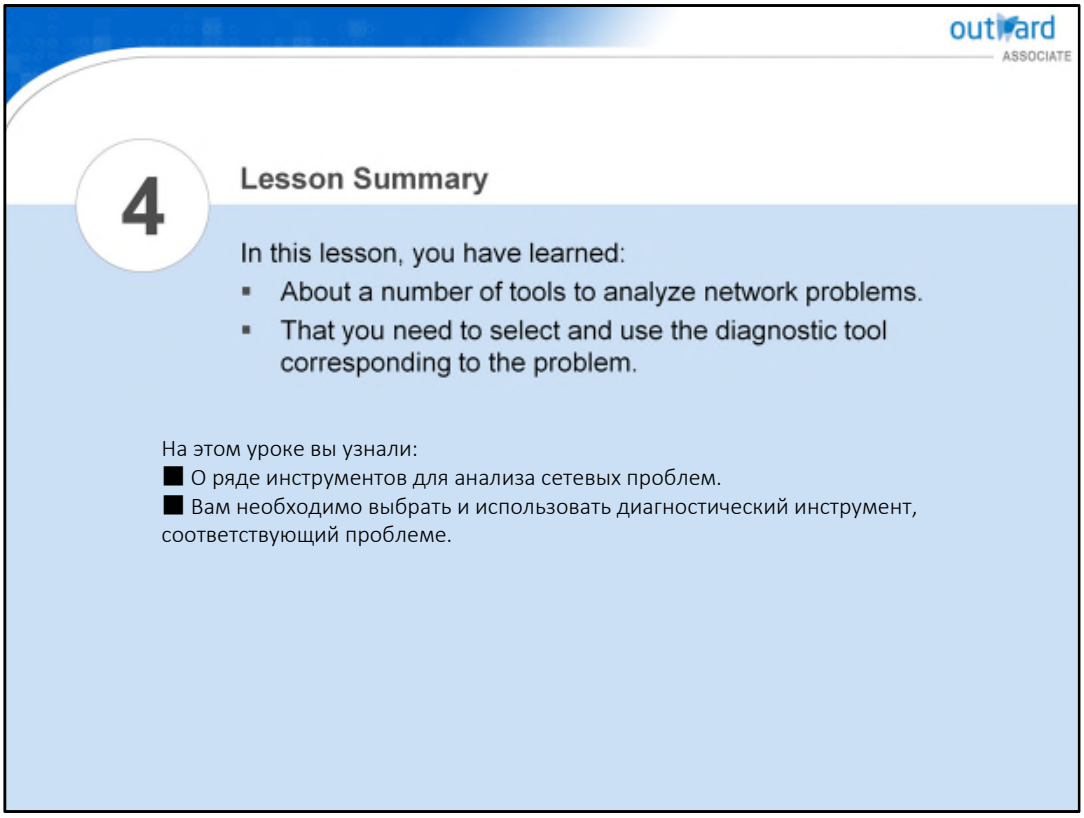


Wireshark is network analyzer software used to analyze and display data flowing across the network.
Computers running Wireshark can collect and record network packets, analyze protocols, display unique control information for each protocol, and can be used to investigate the cause of network faults and trouble.
Wireshark has a function to analyze more than 600 protocols, including IP and DHCP, and supports many other file formats such as Sniffer Pro and tcpdump.

Wireshark - это программное обеспечение для анализа сети, используемое для анализа и отображения данных, передаваемых по сети.
Компьютеры, на которых работает Wireshark, могут собирать и записывать сетевые пакеты, анализировать протоколы, отображать уникальную управляющую информацию для каждого протокола и могут использоваться для расследования причин сбоев и проблем в сети.
Wireshark имеет функцию для анализа более 600 протоколов, включая IP и DHCP, и поддерживает многие другие форматы файлов, такие как Sniffer Pro и tcpdump.

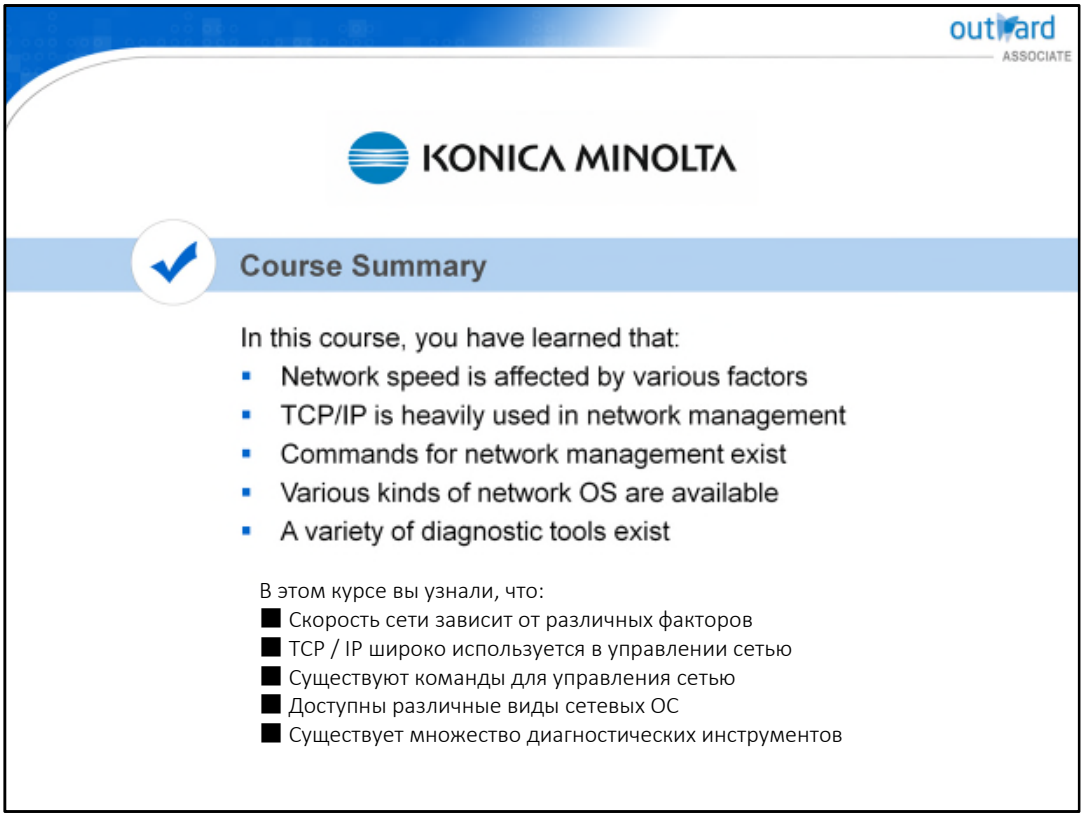


Test your knowledge in a quiz!



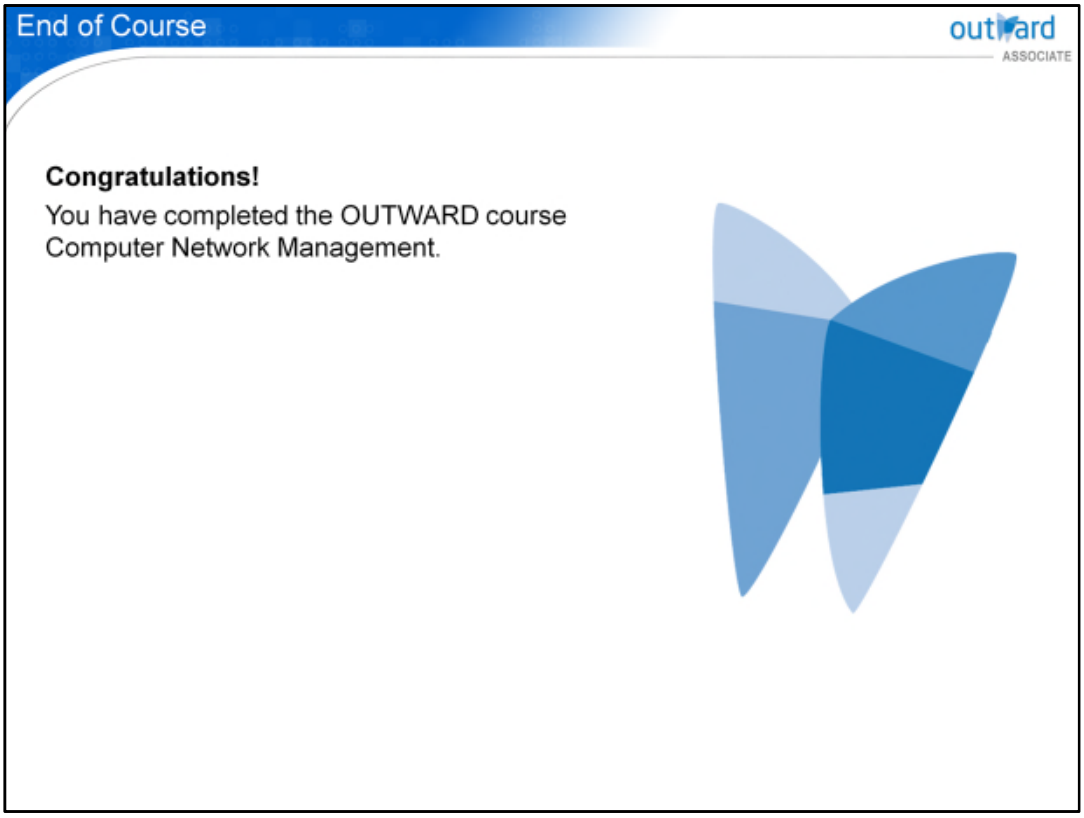
To solve network problems, diagnostic tools are necessary to understand the cause.
For example, a cable tester can be used if there could be a problem with cabling, or a protocol analyzer if there could be a problem with a protocol.
It is necessary to identify the problem according to the situation and use appropriate tools to specify the cause.

Для решения сетевых проблем необходимы диагностические инструменты, чтобы понять причину.
Например, кабельный тестер может использоваться, если может быть проблема с кабелем, или анализатор протокола, если может быть проблема с протоколом.
Необходимо определить проблему в соответствии с ситуацией и использовать соответствующие инструменты для определения причины.



This is the end of the course. Let us look back what you have learned in this course.
Transmission speed is a very important factor when using a network.
Speed is affected by various factors, therefore, you must pay attention to show optimal performance when managing networks.
TCP/IP, which controls communication, is extremely important in network management.
It is necessary to grasp the usage of IP addresses and management in TCP correctly, and to diagnose or solve problems by using appropriate commands for the situation. Workstations can be connected to a network by introducing a network OS.
It is necessary to grasp the characteristics of various operating systems and manage them appropriately. Diagnostic tools may be helpful in understanding network issues.
A variety of diagnostic tools are available, ranging from tools to understand electrical problems with cables, to items that can be used to analyze information in units of packets.

Это конец курса. Давайте посмотрим назад, что вы узнали в этом курсе.
Скорость передачи является очень важным фактором при использовании сети.
На скорость влияют различные факторы, поэтому вы должны обратить внимание, чтобы показать оптимальную производительность при управлении сетями.
TCP / IP, который контролирует связь, чрезвычайно важен в управлении сетью.
Необходимо правильно понимать использование IP-адресов и управление в TCP, а также диагностировать или решать проблемы с помощью соответствующих команд для данной ситуации. Рабочие станции можно подключить к сети, представив сетевую ОС.
Необходимо понимать характеристики различных операционных систем и управлять ими соответствующим образом. Инструменты диагностики могут быть полезны для понимания проблем сети.
Доступно множество диагностических инструментов, начиная от инструментов для понимания электрических проблем с кабелями до элементов, которые можно использовать для анализа информации в единицах пакетов



Congratulations! You have now completed the OUTWARD course on computer network management.