

# 3

## Understanding Wide Area Networks

Historically, organizations in the early days of networking were concerned with the sharing of information and data internally. However, as more organizations began to own their own computer systems, it became increasingly evident that it would be beneficial to share information between organizations, such as universities. From this, the idea of wide area networking began to take shape to become what it is today. There are very few organizations in the developed world that have not taken to the internet. Gaining a good foundation knowledge of how some of the basic **wide area network (WAN)** infrastructure works will give you a good grounding to be able to support your organization and troubleshoot any issues as they arise.

This chapter moves out of your own networks and discusses the principles behind WANs. It focuses on the services offered by service providers, discussing the characteristics of each of the different methods, including use cases.

The following topics will be covered in this chapter:

- Introduction to WANs
- Setting up a broadband connection
- Leased lines
- Dial-up
- Carrier standards

## Technical requirements

To complete the exercises in this chapter, you will require a PC or virtual machine running Windows 7 or above (preferably Windows 10) with a working internet connection.

## Introducing WANs

In the previous chapter, we defined a LAN as a network that covered a small geographical area. In contrast, a **WAN is one that covers a large geographical area**. We can further define this by saying that **a WAN is also used to link LANs**, and a prime example of this is the internet. Pretty much every resource we access on the internet is located within someone's LAN. Because of the size of the network involved in a WAN, we will usually find parts of the infrastructure are hosted and controlled by third-party service providers.

For the purposes of the MTA exam, the definitions I have used for LAN and WAN should be adhered to. However, **in the real world, you will likely find that uses of the terms LAN and WAN are used incorrectly**. For example, I once worked for a global company with offices across the world. You can't get much larger. Resources we accessed could be in the UK, Japan, the United States, or anywhere the company was based. Yet we referred to the network as a LAN, and not a WAN.

Pretty much **every organization will connect to a WAN via a third-party service provider**, and your service provider will have some **form of reciprocal agreement** with other service providers to allow each other's traffic across their respective infrastructure. Which service provider you use for that initial connection will depend on a number of factors, which are beyond the scope of this book and the exam, however, ultimately you will need to choose a provider that can meet your requirements. One of the key considerations, though, will be the choice of whether you want a dedicated connection or a shared connection. We will discuss these in the following sections.

## Setting up a broadband connection

In the 1990s, when I got my first computer, most ISPs would provide you with a CD that included software that configured your home connection to their service. These usually would configure your dial-up modem, and in some cases also gave you a graphical user interface to navigate the internet. However, the use of CDs has pretty much faded with the demise of modems. **Nowadays, our ISP will provide us with some form of preconfigured home router that will connect directly to the ISP, and all you have to do is connect your devices to the router.**

While we can usually connect directly to our ISP-provided hub/router, there may be times when we need to manually configure this broadband connection. In the following activity, we will manually set up a broadband connection.



Because in the real world this requires an account with a service provider, we will set up the connection, but it will not connect. Your screens may differ slightly depending on the OS used.

## Setting up a broadband connection

**Activity 1:** Setting up a broadband connection is relatively straightforward, and in the real world the ISP would provide you with some of the configuration values that we use in the following process:

1. Open **Network and Sharing Center** on your PC.
2. Select **Set up a new connection or network**:

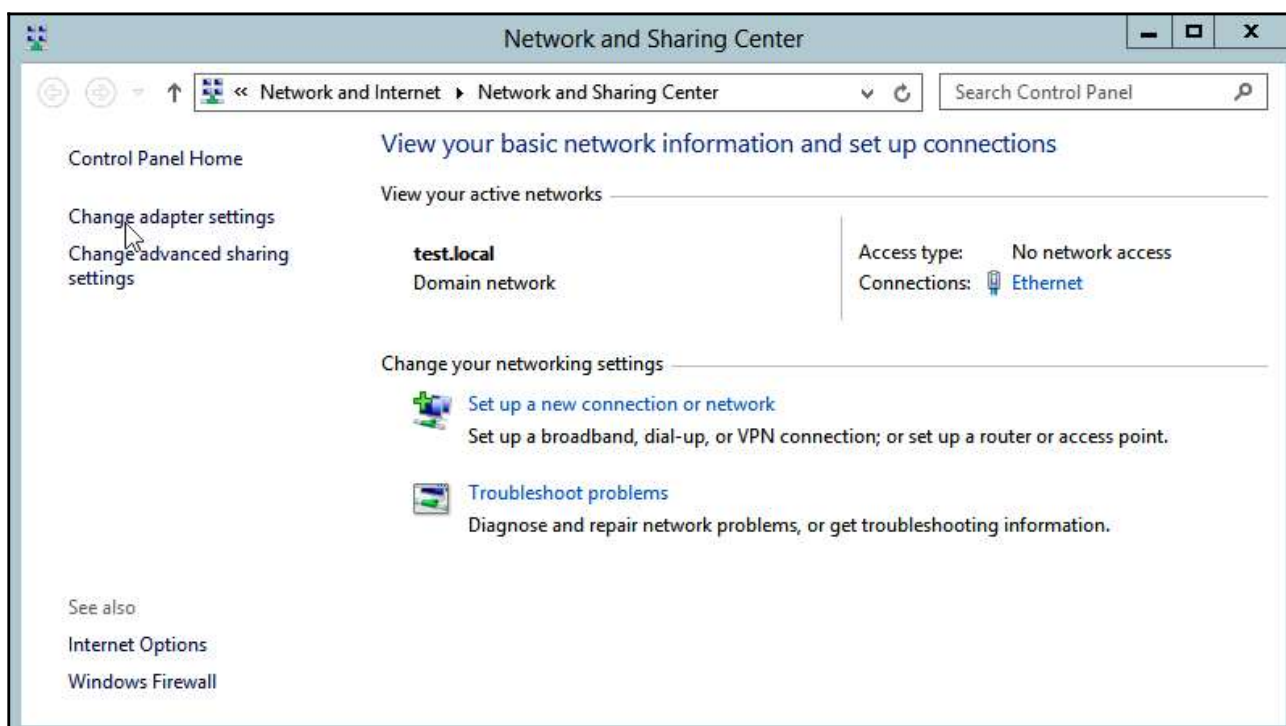


Figure 3.1: Network and Sharing Center

3. Select **Connect to the Internet** and click **Next**:

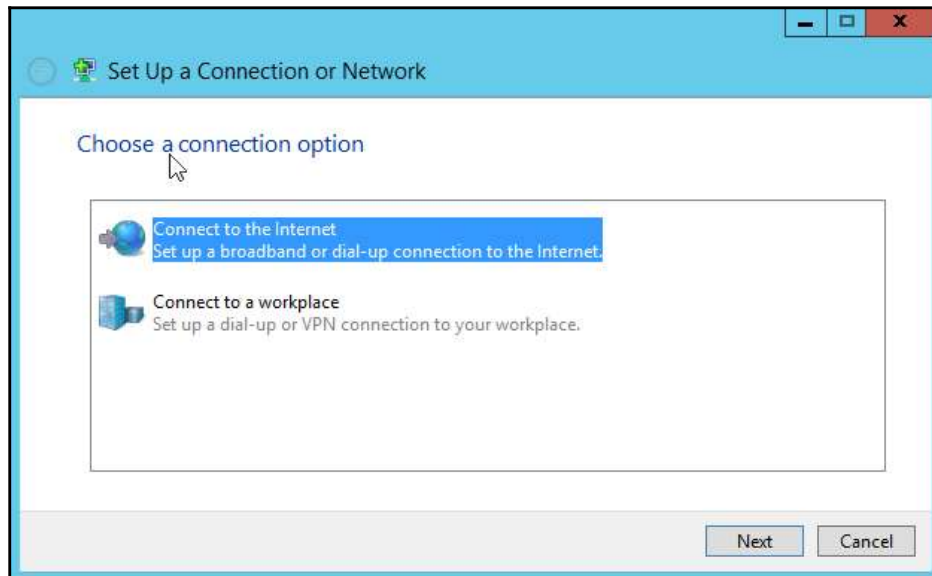


Figure 3.2: Setting up a connection or network

4. Choose the appropriate option to connect. In this case, you can see that I only have one option:

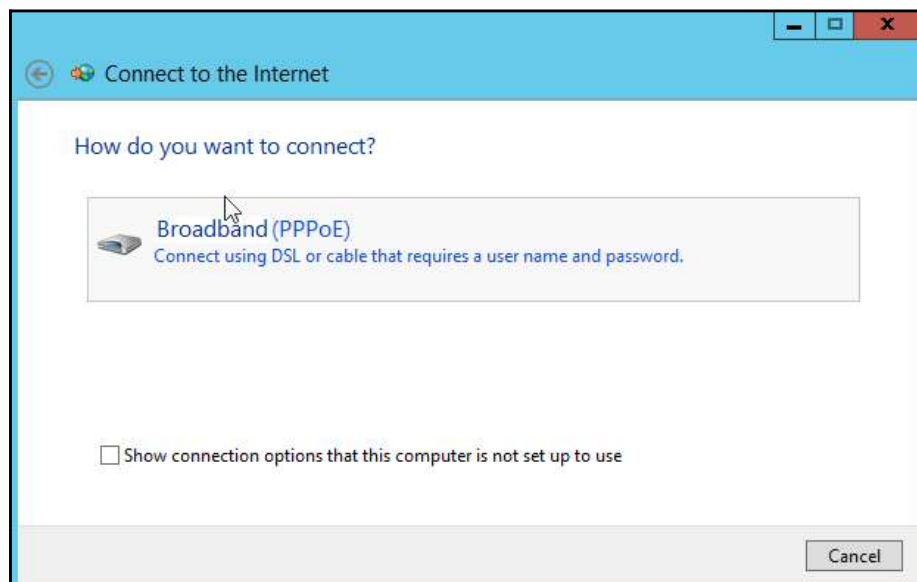


Figure 3.3: Connecting to the internet

5. Enter the credentials provided by your ISP, provide a **Connection name**, and, if appropriate, check the box to allow other users of the device to use the connection. Then, click **Connect**:

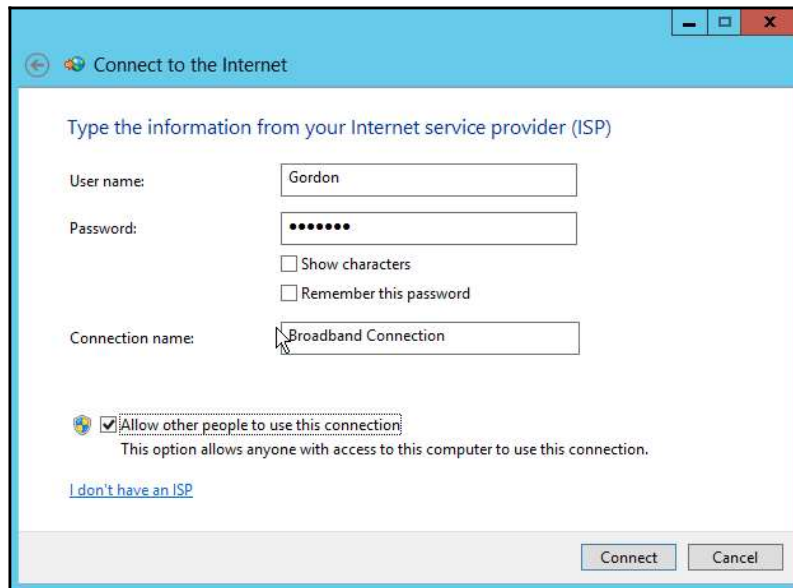


Figure 3.4: Inserting your credentials

6. The device will now try to connect. As we do not have a connection, you can either click **Skip** here, or wait for it to time out, then click **Set up connection anyway**, followed by **Close**:

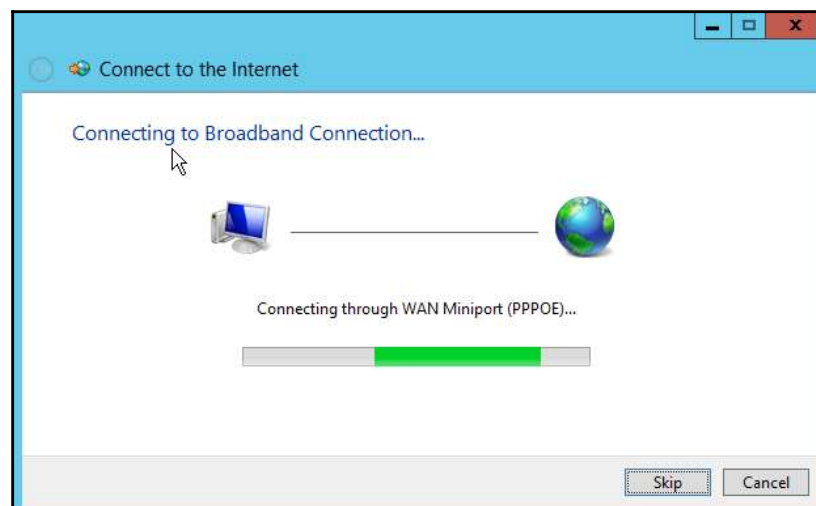


Figure 3.5: Trying to connect

In the preceding activity, we configured the initial setup of a broadband connection. Now we have an internet connection set up, let's look at some of the properties.

## Configuring connection properties

**Activity 2:** There are a number of properties that we can configure for each connection. We cover a number of these in the following activity:

1. Click on **Internet Options**:

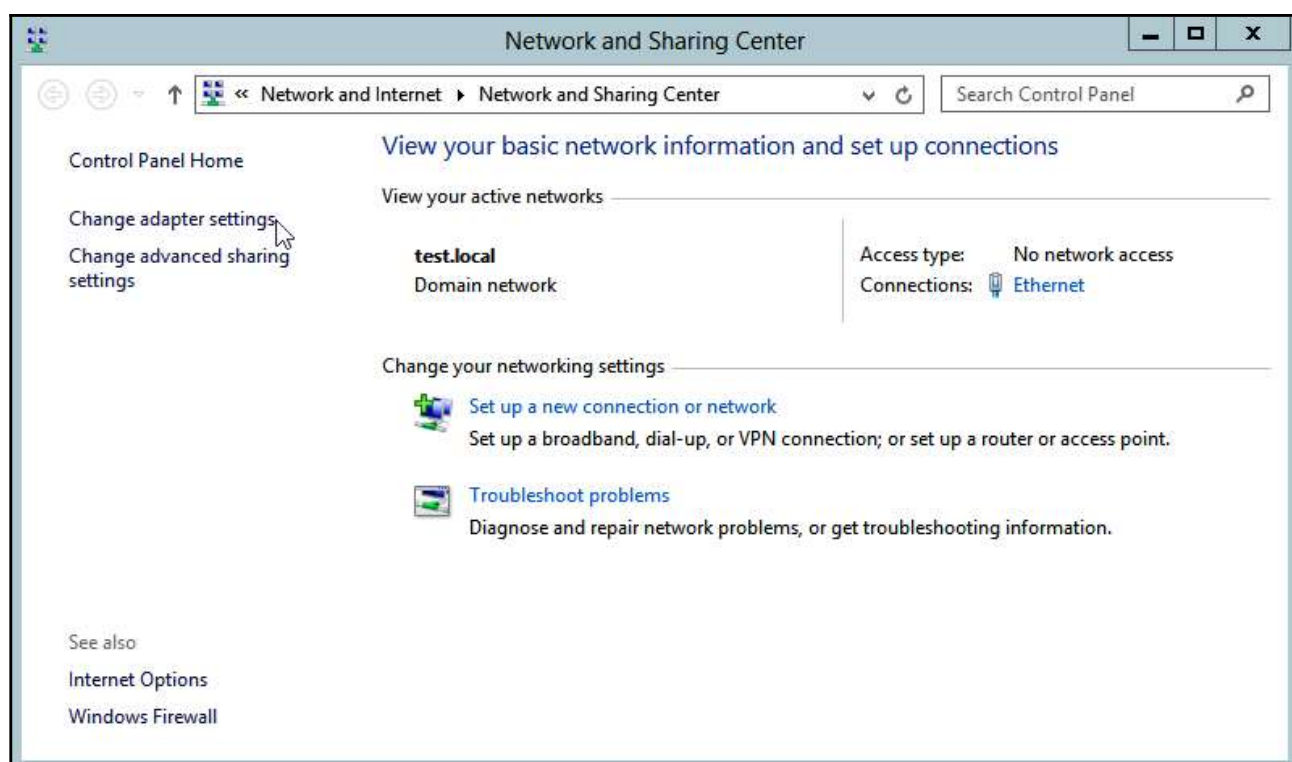


Figure 3.6: Network and Sharing Center

2. Select the **Connections** tab on the **Internet Properties** dialog box:

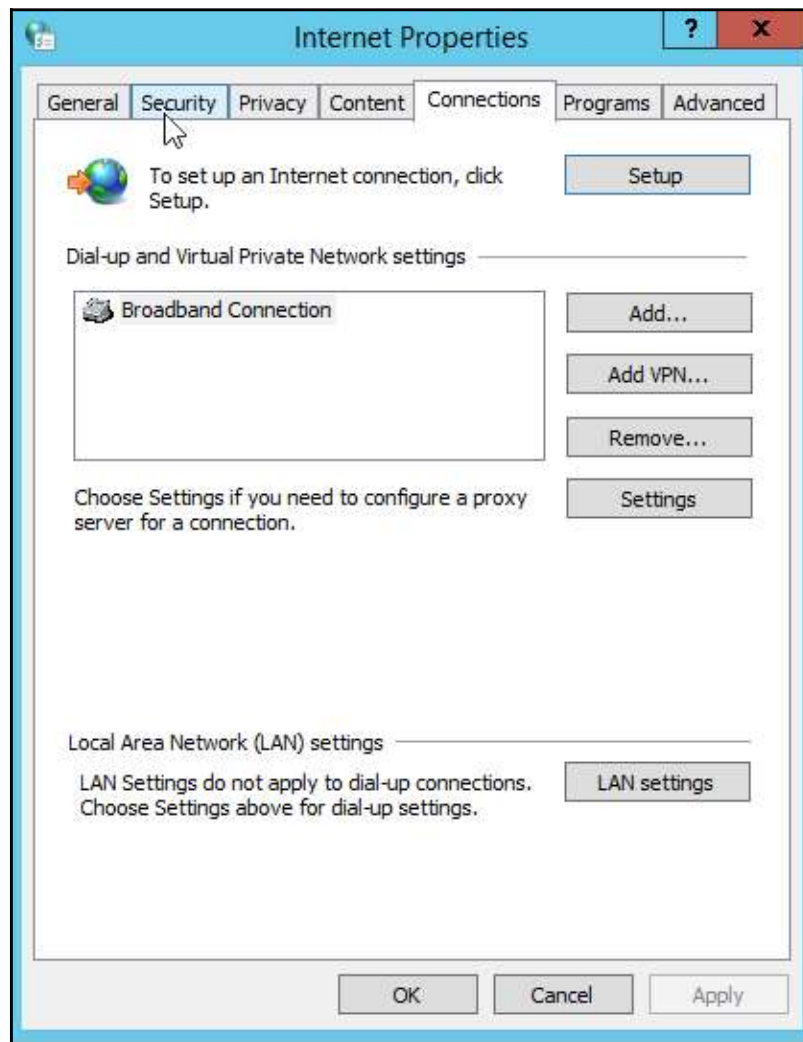


Figure 3.7: Internet Properties dialog box

3. The **Setup** option allows you to repeat the previous activity, but also allows you to select an existing connection. The **Add...** option allows you to create a new connection.
4. Select the connection you created in the previous activity and click **Settings**.



- Investigate the options available to you here. You will not need to know these for the exam but it is worthwhile knowing they exist for the real world. Of the options shown in this dialog box, I will draw your attention to the **Proxy server** option, which we will discuss in more detail in Chapter 14, *Network Services*:

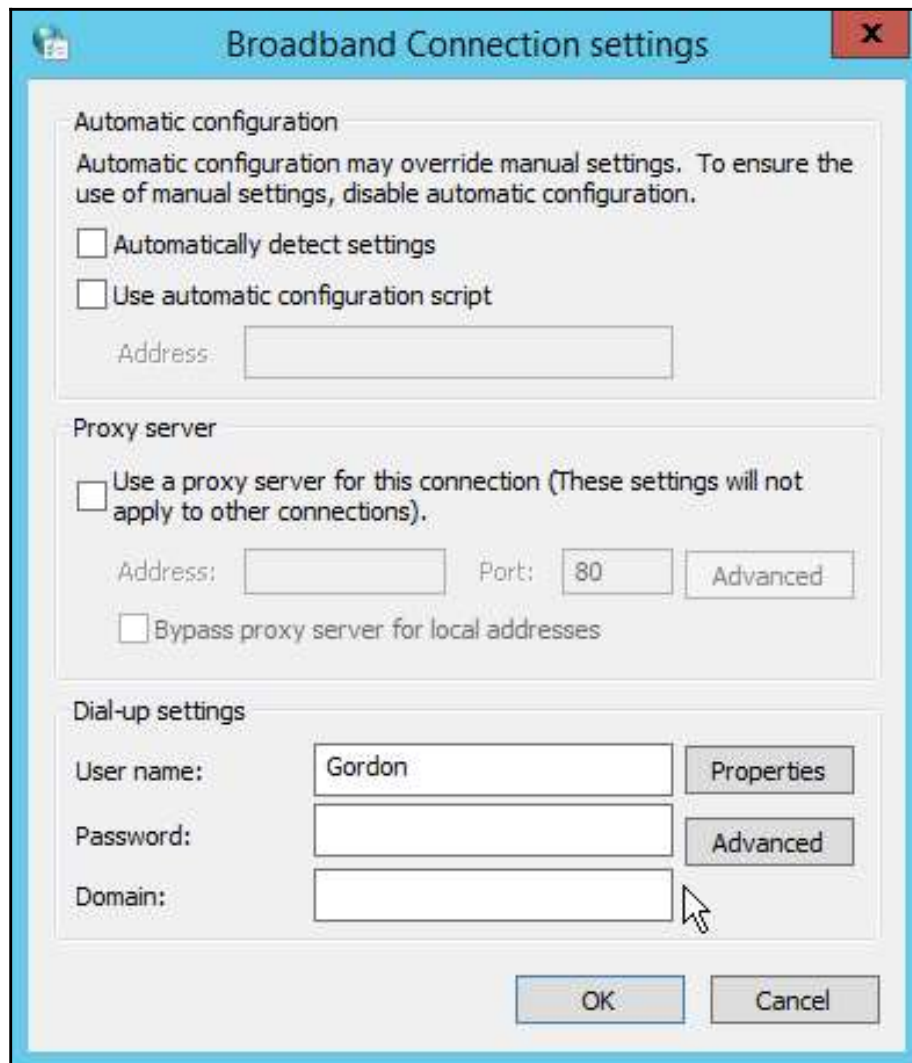


Figure 3.8: Broadband Connection settings



6. Click on **Properties** and investigate the options there. In the **Sharing** tab, you will see that you can share the device's internet connection. This is seldom used nowadays and is a throwback to the days when you only had one modem and wanted to share it in a household. You would connect the PCs to a hub, and one of the PCs would be connected to the modem. This allowed the other devices to share the modem-connected PC's internet connection:

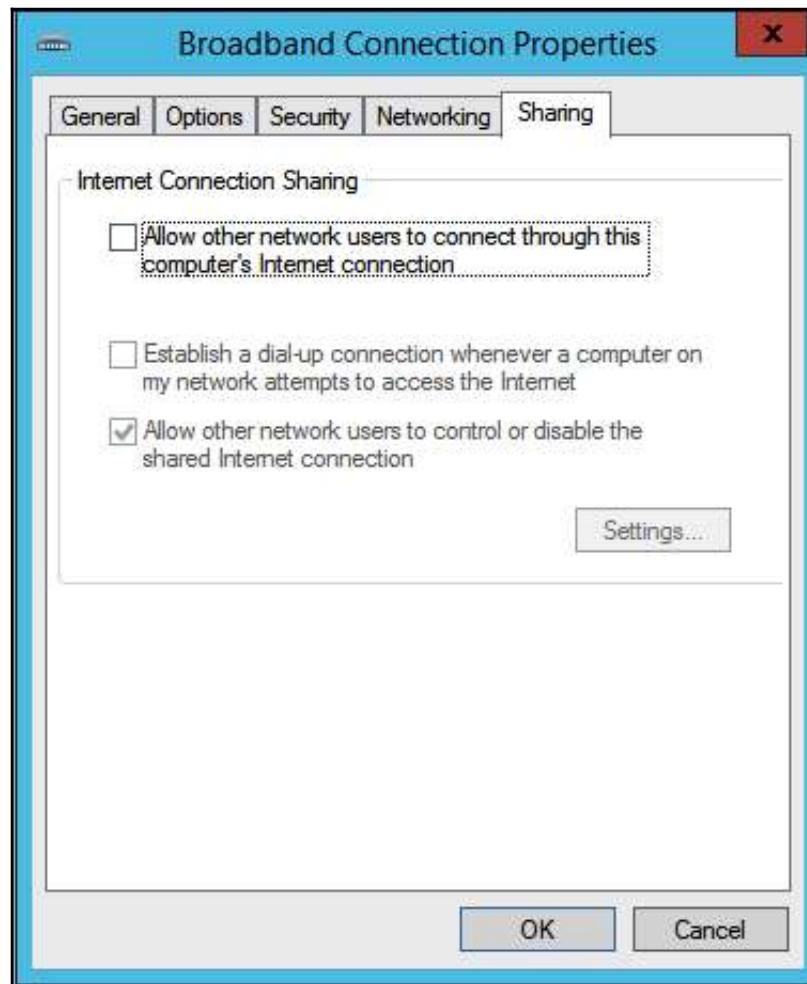


Figure 3.9: Broadband Connection Properties

Once the data has been received on the WAN, it has to be moved around to get to its destination. To do this, we use some form of packet switching technology; usually, this will be either X.25 or Frame Relay. Before these technologies came along, when the only means of connection was via dial-up, we used circuit switching.

## Circuit switching

With circuit switching, the telephone system created a physical connection from the person initiating the call to the person receiving the call. This is not to say there was a cable that ran my house to my friend's house. There would be a cable that connected my house to the telephone exchange, and from there another cable was then connected to create a connection to another exchange where the process was repeated until the final exchange would connect me to my friend's house.

You may have seen this in action if you have seen an old black and white movie with a scene at a telephone exchange. The telephone operators would manually plug and unplug the cables to make or end the physical connection. Because it would only be my call on this connection, the bandwidth was dedicated to me, and thus the quality of the call was guaranteed. However, circuit switching was not without its drawbacks. If there was a break in the connection, there was no redundancy in place, and a new connection had to be initiated. If it failed during a data transfer, you would have to re-transmit. Figure 3.10 shows an example of how a circuit switching connection may have been made:

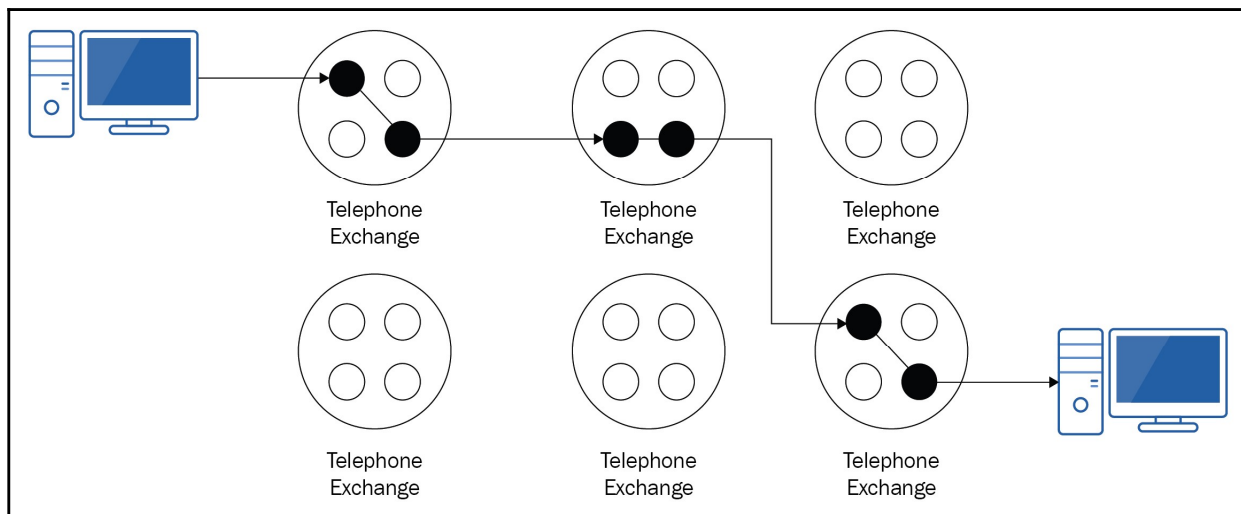


Figure 3.10 Circuit switching example

As circuit switching was not without its faults, an alternative was required to address them. Packet switching was the solution, and we will cover this next.

## Packet switching

Packet switching was introduced to alleviate some of the issues that were found in circuit switching. Using this method, **the data being transferred is broken down into smaller chunks of data called packets.** A virtual connection is made between the devices. One of the key differences between packet switching and circuit switching is that there is no fixed path between the devices, and **each packet may take a different route.** As you can see in *Figure 3.11*, the first packet (single black line) and the second packet (double black line) have gone different paths. Note that, for clarity, I have not added the double black line for the connection between the devices and the central offices:

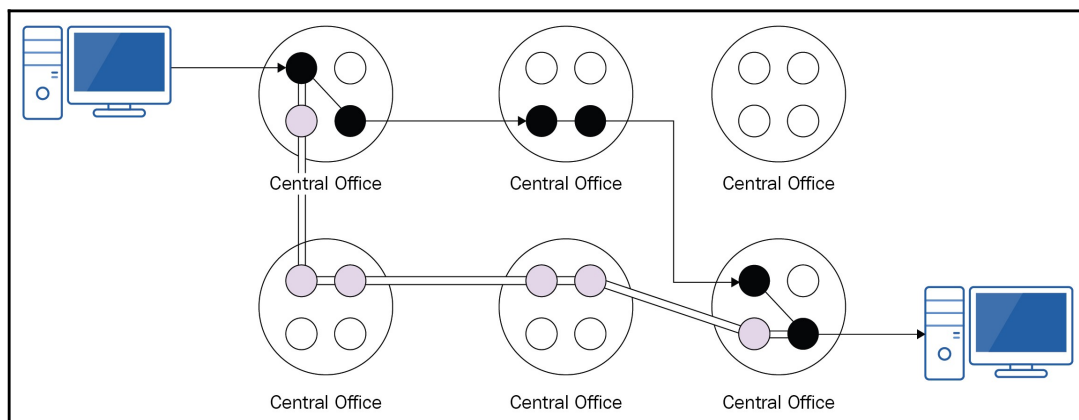


Figure 3.11: Packet switching network

Each of these packets includes a portion of the original data (payload), a header, and a trailer. As the header and trailer are additional to the data being transmitted, they are classed as management overhead. **The header will include information such as the source and destination addresses, and a segmentation number,** as well as other details. The segmentation number is used to rebuild the segmented data at the recipient's end and as a means of accounting for all the data. Has it all been received? The trailer contains a **cyclic redundancy check (CRC) for error checking.** When sending data, the following process is followed:

1. The sending device performs a mathematical calculation on the data being sent.
2. The output of that calculation is added to the trailer.
3. On receipt of any data, the receiving device performs the same calculation.
4. **The receiving device then compares its result with the value stored in the trailer.**
5. **If the two values match, then the data has been transmitted correctly.**
6. If they do not match, then the data is deemed to be corrupted, and some form of correction or re-transmission is required.

How large these packets are is dependent on the network itself. We'll look at an example scenario and identify how many packets need to be transmitted.

Joe wants to send a file that is 4 Kb in size, across a network that supports a fixed packet size of 512 bits. Each packet has 124 bits of overhead (92 bits for the header and 32 bits for the trailer). We can see just from comparing the file size and fixed packet size that the original data needs to be broken down into packets. But how many? To work this out, we need to know how big the payload can be in each packet. We can find this using the following calculation:

- *Payload size = fixed packet size - overhead:*

$$\text{Payload size} = 512 \text{ bits} - 124 \text{ bits}$$

$$\text{Payload size} = 388 \text{ bits}$$

- With this information, we can find out how many packets we would send:

$$\text{Number of packets} = \text{original file size} / \text{Payload size}$$

$$\text{Number of packets} = 4096 \text{ bits} / 388 \text{ bits}$$

$$\text{Number of packets} = 10.55$$

Obviously, we cannot send .55 of a packet, so this would be 10 packets with a payload of 388 bits each, and an 11th packet with a payload of 216 bits.

## X.25 packet switching

While X.25 packet switching is one of the oldest packet-switching technologies, it is still in use today even though frame relay is available. Through the use of X.25 technology, an organization can take advantage of a 64 Kb WAN connection that is *called up* whenever there is data to be transmitted. X.25 provides an end-to-end connection that is digital throughout, thus removing the requirement to convert data from digital to analog and back again. While all data being transmitted across any network will have some form of management overhead included in the transmission, X.25 has a greatly reduced overhead compared to that used in circuit switching. This leads to more efficient use of available bandwidth.

There are a number of components you need to be familiar with to understand how X.25 packet switching works, and I would like to define them before providing an overview of how communication takes place.

- **Packet Assembler Disassembler (PAD):** This is likely to be the router on the sending device's network. It takes the original data and breaks it down into packets. On arrival at the destination network's router, the packets are re-assembled back into their original form.
- **Data Terminating Equipment (DTE):** This is the device where the data being transmitted on a packet-switched network terminates. In most modern iterations, this would be the router, but may actually be a terminal device. The DTE is owned by the client.
- **Data Circuit-Terminating Equipment (DCE):** This device connects your network to the medium that links you to the packet switching network. In a packet-switching network, this would be a device called a **Channel Service Unit/Data Service Unit (CSU/DSU)**. One of the important functions these devices provide is that of clocking. Clocking is a function that allows synchronous transmission of data, that is, all devices are working on the same timings and thus avoid collisions.
- **Central Office (CO):** This is the building owned by your service provider where all the digital connections go to.
- **Packet Switching Exchange (PSE):** A device located in the CO that is used for routing the data. Each PSE contains thousands of circuits, and it will choose one of these circuits to transmit the data through. (This is represented by the small circles in *Figure 3.2*.)
- **Virtual circuit:** The collection of circuits selected for the transmission of a set of data.
- **Demarcation point (Demarc):** This is the point where services from your service provider interface with your own services. This will mark the boundaries of responsibilities, and is quite important to know when troubleshooting. Is it a problem in your devices or with the providers, or possibly subsequent providers, that your data is transiting through. A demarcation point may be an interface on a device or something as simple as a network jack.

Figure 3.12 shows the connection from the end device to the internet, where the CO will be located. The routing that takes place within the internet is shown in Figure 3.12:

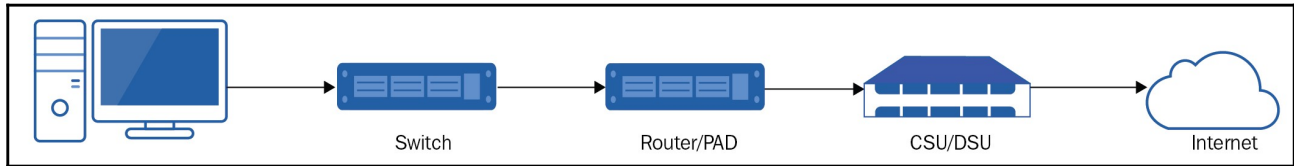


Figure 3.12: X.25 setup

Now you know the components, let's put this all together and discuss the process:

1. Your device sends the data to a router.
2. The router (PAD) disassembles the data into packets.
3. The PAD forwards the packets to the CSU/DSU.
4. The CSU/DSU then forwards the packets via the Demarc to the CO.
5. Once received at the CO, a PSE may disassemble the packets further if they are too big for onward transmission. The PSE will then view the destination information within the packet, and decide which circuit to forward it through. There is no requirement for all of the packets from one set of original data to be sent through the same circuit/path.
6. The PSE sends the data on to the next hop in the path. This may be another PSE or may be the recipient's PAD.
7. Once the data arrives at the recipient's PAD, it is checked (using the CRC) and reassembled.
8. The PAD finally forwards the data to the intended recipient.

X.25 allows for devices on the LAN to share the WAN connection. As you can see from Figure 3.12, the end devices connect to the router via a switch, meaning they can all transmit data to the router. The PSEs have the capacity to store data in their buffers for onward transmission later (store and forward). Because they are storing the data before transmitting it, there is an element of fault tolerance here. If the data being transmitted fails for whatever reason, the PSE still holds it in its buffer and can therefore attempt to forward it on again. This may mean forwarding it via a different circuit if the original one is no longer available.



It is possible to identify the path that the data takes using the `tracert` command. `tracert` traces the route your data takes to reach a destination. The following activity will demonstrate this command in action:

### Activity 3:

1. Open Command Prompt on a Windows PC.
2. `tracert` to Google's public DNS server using this command: `tracert 8.8.8.8`.
3. Review the output.

Your output should look similar to mine (Figure 3.13). If you receive a General failure message, it is likely that the ICMP packets being used by `tracert` are being blocked by the firewall:

```

C:\Users\User>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms    vodafone.broadband [192.168.1.1]
  1  19 ms   21 ms   26 ms   host-212-158-250-32.dslgb.com [212.158.250.32]
  2  13 ms   13 ms   12 ms   63.130.105.130
  3  12 ms   12 ms   12 ms   72.14.216.237
  4  *        *        *        Request timed out.
  5  13 ms   13 ms   13 ms   216.239.63.136
  6  30 ms   31 ms   30 ms   216.239.50.73
  7  13 ms   13 ms   13 ms   google-public-dns-a.google.com [8.8.8.8]

Trace complete.

```

Figure 3.13: tracert output

Looking at my output, we can see a number of things. Firstly, we can see that `tracert` has resolved the IP address of `8.8.8.8` to what is known as a **fully qualified domain name (FQDN)** of `google-public-dns-a.google.com`. We can see that it allowed the route to be a maximum of 30 hops (routers). If the destination was any further than this, it would not have completed the trace. Then, the output provides us with the details of the 8 hops to get to `8.8.8.8`. Hop #1 is my home router (default gateway). There are three sets of timings for each hop. `tracert` sends three packets of data to each hop (basically sends a ping) and records the latency (how long it takes for a reply to come back). Then, I am informed of the IP address of the hop, and, where available, its name. Look at hop #5.



Notice there are no timings, just an asterix, \*, and it says `Request timed out`. This is most likely due to the device at hop #5 being configured not to respond to ICMP requests. It is not unusual to see multiple entries similar to hop #5. However, I would suggest that if you have no connectivity to the end device (in this case 8.8.8.8) and from hop #5 onward you have just received `Request timed out` messages, that there is a problem between hop #4 and hop #5.



**Exam tip:** I would encourage you to refer to `tracert` as **trace route**. A lot of people refer to it as *trace R T*, and then forget what it is used for. By referring to it in full, you can easily recognize its function. I would, however, be remiss not to include a caveat to this. In Linux, the command is `traceroute`, not `tracert`. If you follow my recommendation of referring to `tracert` as *trace route*, be careful as the Linux variant may be in the answer set as a distractor.

## Frame relay

We discussed previously how X.25 segmented the original data being transmitted by breaking it down into packets. Frame relay utilizes a similar technique, but **breaks the original data into chunks of data known as frames**. However, confusingly, it is still referred to as packet-switching technology. Devices in a frame relay network are similar to those used in an X.25 network, except the former uses a **Frame Relay Access Device (FRAD)** instead of a PAD, and the DCE is a device known as **frame relay switch** instead of the CSU/DSU (Figure 3.14):

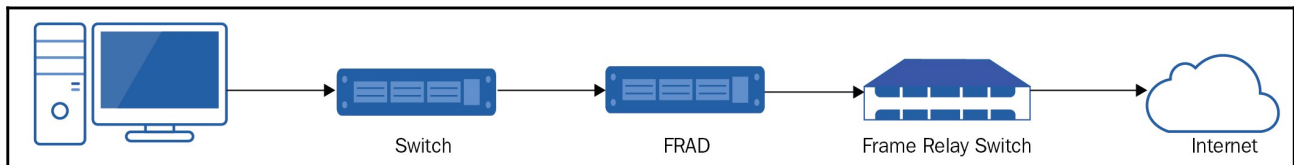


Figure 3.14: Frame relay

With frame relay, **the virtual circuits created are not dedicated to just you and are shared with other organizations**. This raises some obvious concerns regarding privacy, and also leads to decreased transmission speeds as you share the connection. This doesn't sound too appealing, so why use frame relay? Quite simply, it is cheaper and uses fewer devices. To try and help alleviate the issue of decreased speed, **frame relay does not attempt to correct any errors** it detects during the transit of the data. If a frame is detected as having an error, it is simply discarded. Error correction is left to the relevant endpoint devices. They will identify that data is missing and attempt to correct the issue, usually by re-transmission.

Unlike X.25, which is needed to *call up* to transmit data, frame relay uses **permanent virtual circuits (PVCs)**. As the name implies, these are permanently connected and do not need to *call up* to transmit data. These PVCs connect to PSEs sitting in a frame relay cloud and are likely to be paired. One PVC will be for transmission, and the other for receiving, giving you a full-duplex connection.

Organizations will need to decide on what bandwidth they are likely to use and agree this with the service provider. The normal bandwidth you select is known as the **committed information rate (CIR)**. There may be instances when this is not quite enough, and frame relay allows for burst transmissions of up to two seconds. This provides you with additional bandwidth, with two additional rates, **burst rate (BR)** and **burst excess (BE)**. The BR is double the CIR, and the BE is BR plus half the CIR. There are lots of abbreviations there, so let me clarify that:

*Burst rate (BR) = 2 x committed information rate (CIR)*

*Burst excess = Burst rate + (committed information rate/2)*

Both frame relay and packet switching utilize a shared infrastructure. Although this means it is a cheaper option compared to alternatives, it is not without issues. In the next section, we will look at a more costly alternative.

## Leased lines

I find people struggle a little with differentiating leased lines from other forms of connectivity, purely due to the use of the term *leased*. All of these connections require you to lease some form of service from your provider, and that's what confuses people. What I would ask you to do to combat this is to prefix leased lines with the word *dedicated*.

Unlike other forms of connection discussed here, a leased line is a dedicated link between you and another location. It's dedicated in that it is only you using it, and, unlike the others we will discuss, it is not shared with other subscribers. You may have noticed that I refer to *another location* rather than specifically mentioning the connection is to your service provider. This is deliberate, because although most leased lines will connect you to your service provider, you may also have a dedicated connection between company sites. Because the lines are dedicated to you, the service providers can guarantee a level of quality. They also tend to offer full-duplex connectivity with the same speed for uploads as that available for downloads.

Leased lines offer *always-on* communication. They are permanently connected and ready to send and receive data at any time of day, and there is no requirement to initiate the connection. Because of this, leased lines are a more expensive option, and potentially you are paying for the connection when it is not being used, such as night time or weekends. It is unlikely, therefore, that a leased line will be used to connect a residential home to a service provider. In fact, in 18 years of working in IT, I have only once come across a home user that had a dedicated lease line.

## Dial-up connectivity

You may be looking at the title of this section and wondering why are we covering such an old technology. The simple answer to this is that, despite its age, dial-up is still used. However, unless you're living in rural areas where faster methods are not available, it is unlikely that it would be used as a primary means of connection to a WAN. In most instances, dial-up would be used as a backup means of connectivity, used for allowing support staff to connect and rectify any issues with the primary means of connection. Imagine that you are an on-call network engineer, and someone calls you up in the middle of the night to report that there is no internet access. You try to connect to the router from home, but there is no connectivity. You then use a dial-up connection to dial into the network, connect to the router via its internal interface, and rectify the fault.

Dial-up connections utilize the traditional telephone network. You may hear this referred to as **public switched telephone network (PSTN)** or more informally, **plain old telephone service (POTS)**. The telephone network was designed to carry voice communications, and its use for carrying data was piggy-backed on to the existing infrastructure. The performance of dial-up can vary significantly depending on a number of factors. For example, distance can impact the quality of the signal, likewise the environments where the telephone line is shared, such as a workplace or a hotel, will suffer from degradation.

To connect using dial-up, a user needs to use a device called a **modulator/de-modulator (modem)**. A modem may be a standalone device, maybe on an expansion card added to the computer, or embedded on the motherboard, although this is unlikely on modern PCs. If using a standalone device, you will need to connect it to the PC. **The modem is then connected to the telephone socket in your building.** The purpose of the modem is to convert the digital signals from your PC into analog signals for transfer across the telephone lines. **The destination modem reverses this process, taking the analog signal, and converting them back into a digital format that can be understood by the recipient PC.** Figure 3.15 shows a simplified dial-up network. In reality, the modem connects to a telephone socket at the wall, and does not connect directly to the telephone pole:

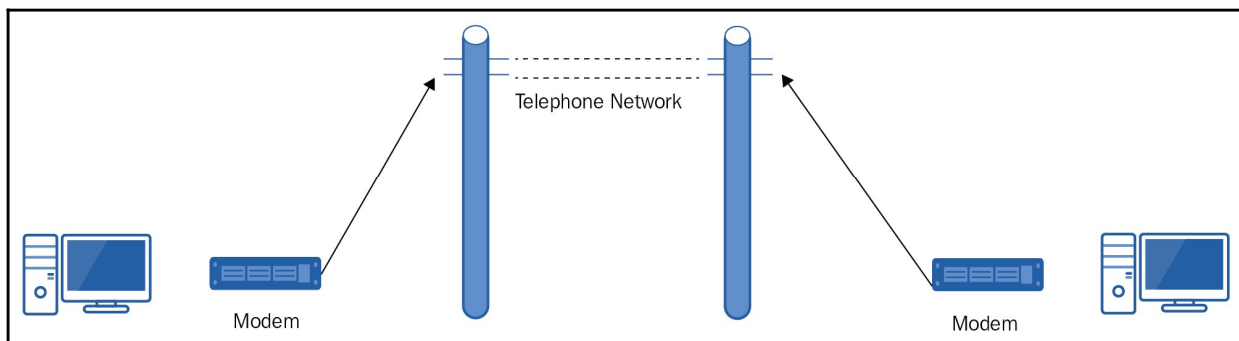


Figure 3.15: Dial-up connection

Compared to modern technologies, **dial-up offers a very slow service.** Although the telephone lines can transmit 64 Kb/s, only 54 Kb/s is used for data, and the remaining 8 Kb/s is used for signaling purposes. As modem technology advanced, compression was used to transfer data at a higher rate. For example, V.44 would boost the speed up to the equivalent of 320 Kb/s. ISPs were able to extend this further by using compression to reduce the size of web page content such as text and images.

**Activity 4: Setting up a dial-up connection:** In this activity, we will go through setting up your computer to use a dial-up connection:



As it is unlikely that you have access to a modem and a relevant dial-up account with your ISP, this activity will include some steps that you are unlikely to see if you're doing this for real.

1. Open **Network and Sharing Center** on your PC.
2. Select **Set up a new connection or network**:

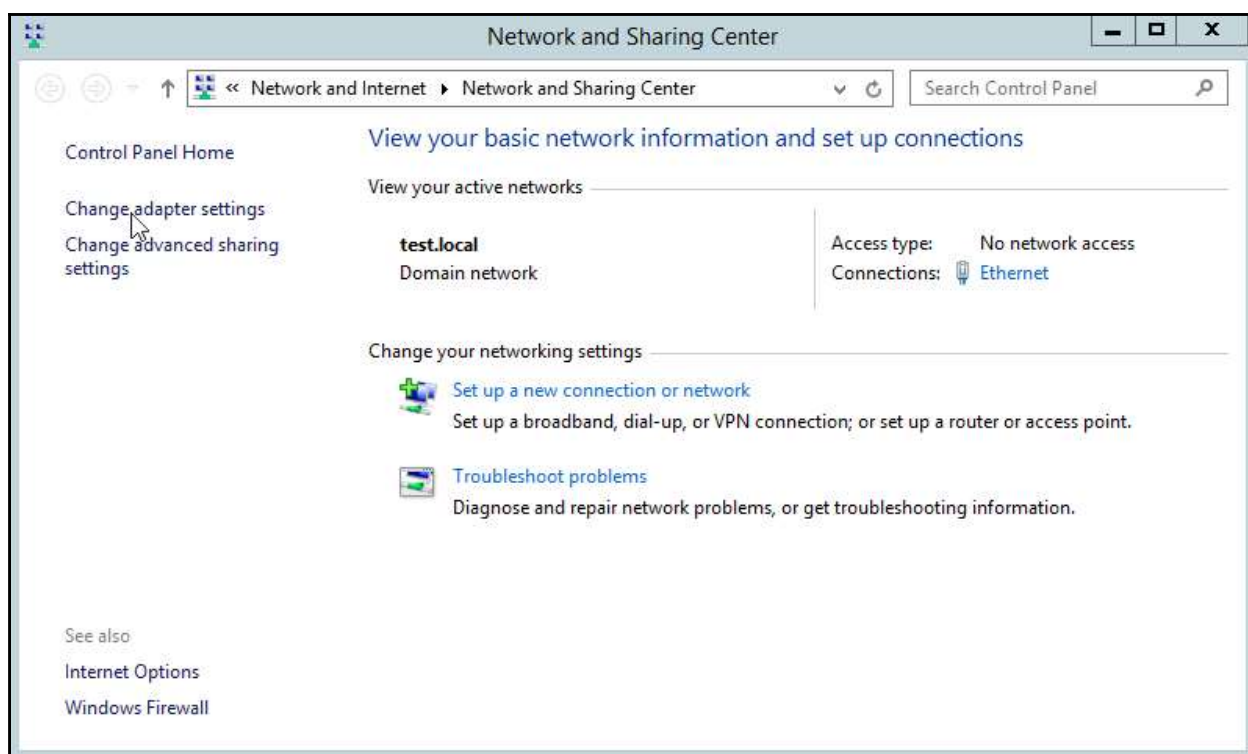


Figure 3.16: Setting up a new connection

3. Select **Connect to the Internet** and click **Next**:

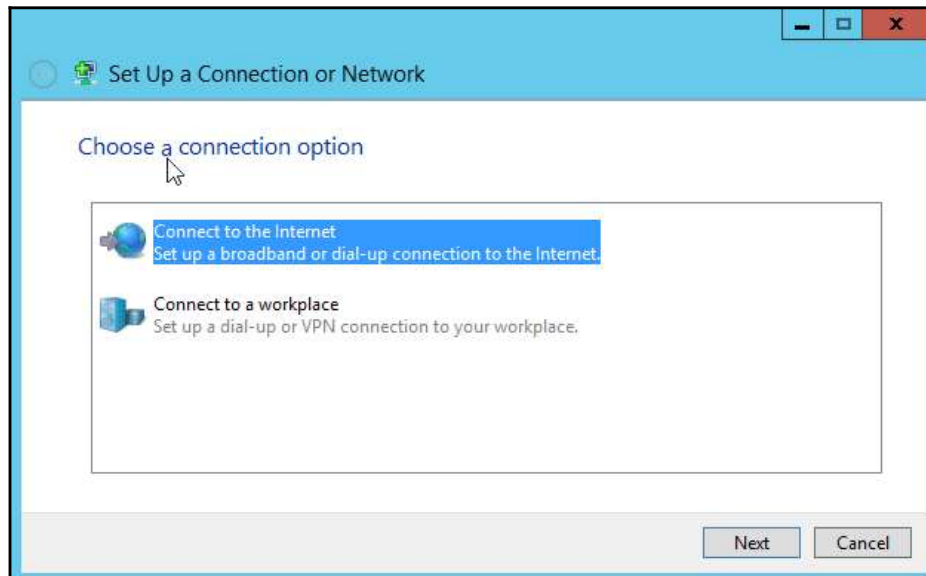


Figure 3.17: Connecting to the internet

4. Choose **Dial-up** (note: as I do not have a modem connected, I had to choose **Show connection options that this computer is not set up to use** for it to show):

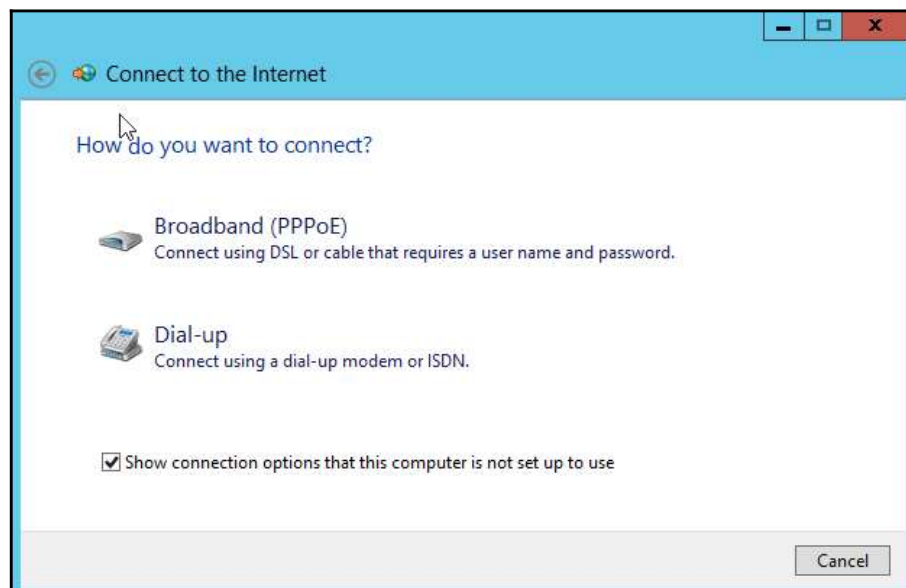


Figure 3.18: The Dial-up option

5. Enter in the details provided by your ISP. Then, click **Dialing Rules**:

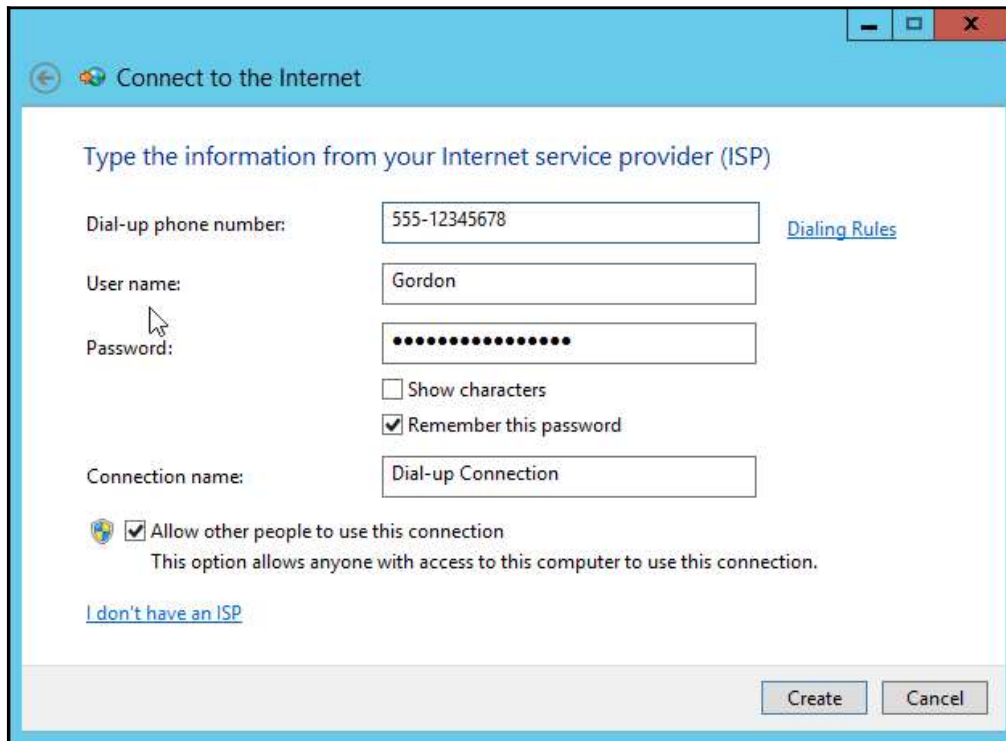


Figure 3.19: Inserting your credentials

6. In the **Dialing Rules** dialog box, you can configure the following options. The option to set a number in the **If you dial a number to access an outside line, what is it?** field is useful for you when you are in a hotel or workplace where you have to dial a **9** to get an outside line. Click **OK** to close this dialog box:



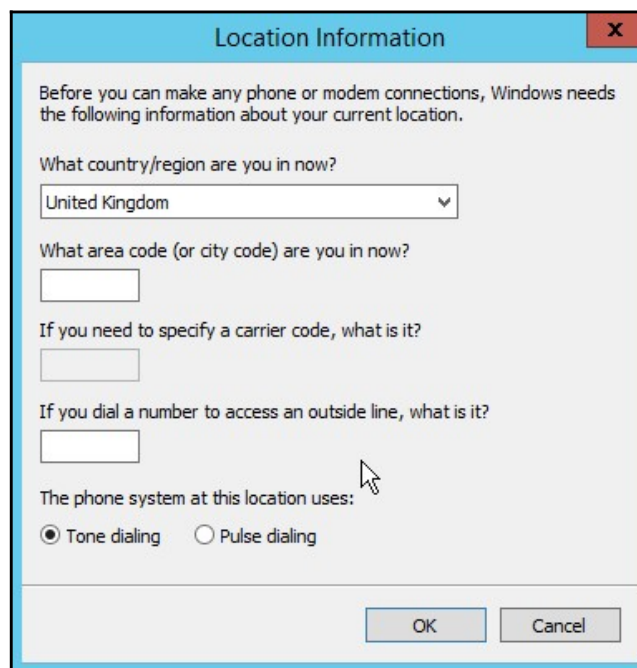


Figure 3.20: Dialing rules dialogue box

7. To use this connection, repeat *steps 1 to 3* again. Then, from the presented connections, choose **Dial-up Connection**, and click **Next** to connect:

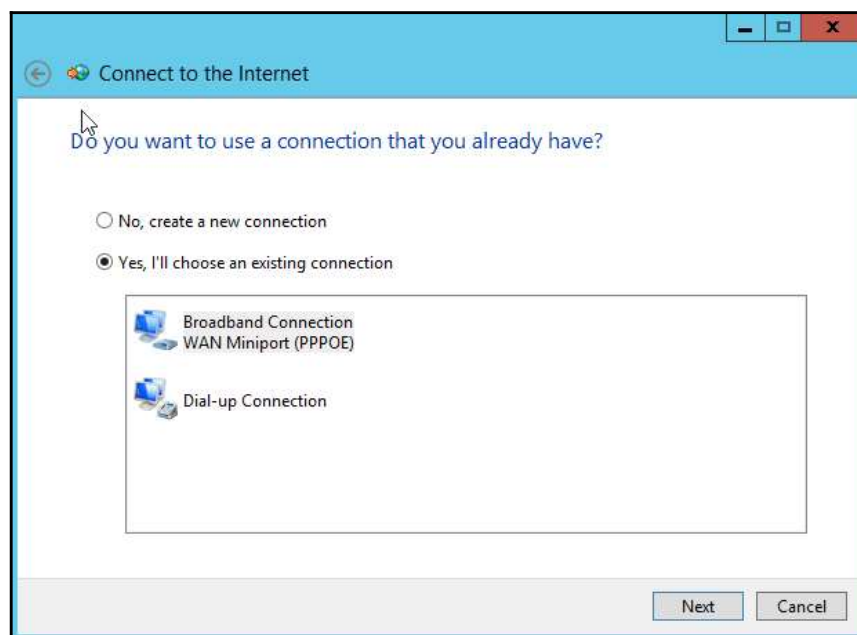


Figure 3.21: Setting up a connection

As you can see from the preceding activity, this is quite a convoluted process and would be difficult for a lot of users, especially at the height of dial-up's popularity when people were not as computer-savvy as they are now. Because of this, most ISPs would provide a setup CD that would do all the donkey work for you. In fact, at one point you could not buy a computer magazine, or go into a supermarket, without being presented with a free CD for a trial with some ISP or other.

Obviously, in a business environment, you don't want just anyone being able to dial in. To avoid this, we need to configure the system to authenticate and authorize the user before allowing them to gain access to the network. Traditionally, this was carried out by a **Remote Authentication Dial In User Service (RADIUS) server**, and in modern implementations this role is carried out by a **Network Policy Server (NPS)**. As can be seen in Figure 3.22, the client device connects to the dial-in server, and the server forwards the user's credentials to the RADIUS server for approval. **The RADIUS server sends back either an approval or rejection based on credentials and the user's permissions.** If approved, the client device is allowed on the network. It should be noted that, despite its name, a RADIUS server provides authentication for more than just dial-in remote users:

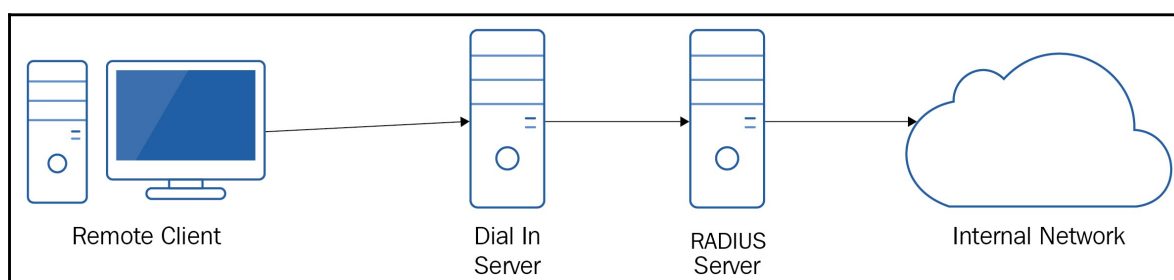


Figure 3.22: RADIUS server setup

The user's dial-in permissions are set in their user profile. Figure 3.23 shows the options available. At the top, we either allow or block connection, or we can allow the connection based upon the settings in the **Network Policy (NP)**. This policy simply states what criteria a user or device has to meet to be considered safe to be allowed on the network. The next section is an option to verify caller ID. This only allows calls to come in from a predefined phone number. As companies tend to get cheaper calls due to business rates, it is usually more cost-effective to *call back* the user rather than them calling up from their individual houses (assuming they can claim the calls back on expenses), so there is an option to call the user back on the number they dialed in on. As an added security option, you can specify a number that is called back to. The obvious restriction to this is that the user dialing in is restricted to that one location if it is a landline number. The last options allow the allocation of static IP addresses (as opposed to DHCP-issued ones) and static routing. We cover routing in more detail in Chapter 7, *Routers and Routing - Beyond a Single Network*:

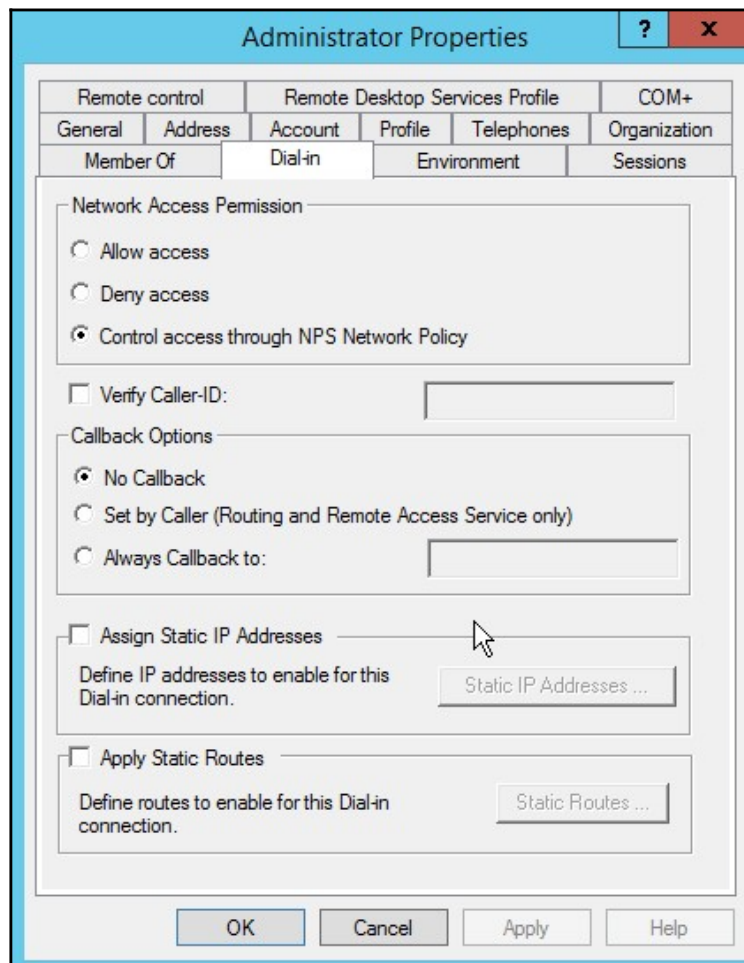


Figure 3.23: User dial-in settings

With the need to provide faster inter-connectivity to accommodate the requirements of more dynamic and demanding services, the days of dial-up were numbered. The following section discusses the various *successors* to this standard.

## Understanding carrier standards

The term *carrier standards* refers to standards that have been agreed upon for the various different carrier technologies. These standards cover a whole range of areas, including coding mechanisms, modulation, voltages, and physical attributes. However, for the exam we only need to have a high-level understanding.

We will now look at some of the common individual carrier standards.

## Integrated Services Digital Network

As technology developed, the limitations of dial-up began to become a hindrance. Faster and better methods of communication were required. **Integrated Services Digital Network (ISDN)** was one of those methods. While improving on dial up, ISDN still utilized the existing telephone network. However, dial-up only allowed one device to use the line at a time, whereas ISDN allowed numerous network devices and voices to utilize the line at the same time.

To connect to the internet using ISDN, an ISDN modem is required. It should be noted that although a modem used with ISDN shares its name with a modem used with dial-up, that is pretty much where the similarities end. Recall that a dial-up modem converts digital signals to analog and back again. However, with ISDN the signal used is digital throughout the journey, and no conversion to/from analog is required. Removal of the conversion step helped improve performance, as did faster connection times. ISDN modems also tend to have more ports to connect devices to than their dial-up counterparts, although connecting too many devices may impact the individual experience of those devices due to having to share a finite bandwidth.



It is easy to think of modems being used for dial-up only. If a question mentions conversion of analog signals, then the answer is definitely leaning toward dial-up, but ensure you read the question and the answer set fully.

ISDN uses the concept of channels for the transmission of data and the management of such transmissions. These channels are split into two types, a bearer channel (B) and a data channel (D). Rather confusingly, the B channel is used to *bear* the data, and the D channel is mainly used to carry the management data for signaling and control. Oddly, because this seems the wrong way round to me, it actually sticks in my mind more. Each B channel is capable of carrying 64 Kb/s, and the D channel is also capable of carrying 64 Kb/s.

There are two types of access available in ISDN, **Basic Rate Interface (BRI)** and **Primary Rate Interface (PRI)**. BRI utilizes two B channels and a single D channel. This provides 128 Kb/s for data. In contrast, PRI varies depending on the region. In North America, it uses what is known as a T1 connection (one of a number of T-Carriers discussed later), Japan uses a J1 connection, and Europe and the majority of the world uses an E1 connection. A T1 and J1 connection utilizes 24 B channels providing a bandwidth of 1,544 Kb/s (or 1.544 Mb/s), whereas E1 uses 32 B channels providing a bandwidth of 2,048 Kb/s (or 2.048 Mb/s).

## Asynchronous Transfer Mode

**Asynchronous Transfer Mode (ATM)** is another method that allows the integration of data and voice communications, and is used within PSTN and ISDN networks. ATM splits the data into fixed-size *cells* of data, and requires a connection to be made between endpoints before any data is transferred. This helps make the network more efficient. If no connection can be established, then no data is transmitted.

## Digital Subscriber Line

Similar to ISDN, **Digital Subscriber Line (DSL)** provides a means of transmitting digital signals across the existing telephone network. Again a modem is required, but unlike ISDN a digital to analog conversion does take place. Although the data being transmitted is now an analog signal, both data and voice communications can take place simultaneously as the data is being transmitted at a higher frequency than the voice communications. Common forms of DSL are **Asymmetric DSL (ADSL)** and **Symmetric DSL (SDSL)**:

- **ADSL**: Most homes utilized ADSL, so this became synonymous with the term DSL. ADSL offers a faster download speed than upload speed. This made sense at the time. Most home users would only be downloading from the internet, even if this was just web pages, and the only uploads they would be doing were the commands from their devices to pull those websites down.
- **SDSL**: SDSL was more the domain of organizations, as this was a dedicated line, and therefore more expensive. As can probably be deduced from its name, SDSL could upload and download at the same speed.

There are a number of other variations of DSL, and you may see the acronym xDSL to represent DSL; however, ADSL and SDSL are the two main ones. ADSL can provide around about 24 Mb/s download and 1 Mb/s upload, and SDSL provides a speed of about 2 Mb/s. The speeds mentioned here are dependent on the distance from the central office. As the distance increased, the speed would reduce due to attenuation (degradation of the signal).

## Synchronous Optical Network

**Synchronous Optical Network (SONET)** is a means of sending digital data down a high-speed optical connection. One of the benefits of SONET was the ability to send multiple data streams through a single connection. The following table shows the details of the speeds of each level:

Level	Transmission speeds
OC-1	51.84 Mb/s
OC-3	155.52 Mb/s
OC-12	622.08 Mb/s
OC-24	1.244 Gb/s
OC-48	2.488 Gb/s
OC-192	9.953 Gb/s



If you can remember the speed of OC-1, then to find the other speeds you just multiply that value by the OC level number.

While SONET utilized optical cabling, other technologies utilized copper cabling and T-carriers, which we will discuss in the next subsection.

## T-carriers

T-carriers or Transmission carriers are utilized by some of the technologies listed previously to transmit data at high speed. In addition, they may be used as a link between LANs to provide a high-speed connection with the added benefit of privacy. The following table shows the details of the relevant speeds per standard:

Europe		Japan		North America	
Level	Speed	Level	Speed	Level	Speed
E1	2.048 Mb/s	J1	1.544 Mb/s	T1	1.544 Mb/s
E3	34.368 Mb/s	J3	32.064 Mb/s	T2	44.736 Mb/s
E4	139.264 Mb/s	J4	97.728 Mb/s	T3	274.176 Mb/s

SONET and T-carriers will usually be used in organizations where the additional bandwidth offered by these technologies prevents any performance issues. Let's look at an option for the home environment.

## Broadband cable

At this point, you may have read through all of the preceding sections and are now thinking, my home network does not use any of these. If this is true for you, it is likely you use some form of broadband cable, especially if your TV and internet is provided by the same supplier, for example, Sky in the UK. This one connection probably uses a single RG-6 coaxial cable.

## Fiber to the X

While not specifically mentioned in the exam objectives, I would like to discuss other WAN technologies that I feel it is worth knowing exist, namely **Fiber to the X (FTTx)**, satellite, and cellular.

FTTx is a term that will crop up in the real world. FTTx is a generic term referring to the varying levels of **Next Generation Access (NGA)** that fiber optic connections and services provide. The following sums up the common versions of FTTx:

- **Fiber to the home (FTTH):** A form of **Fiber to the Premises (FTTP)**. It provides a fiber connection to your house. It should be noted the fiber connection usually ends at some form of junction box attached to your outside wall, and the connection from that box to devices inside, such as the modem, will not be fiber.
- **Fiber to the building/business (FTTB):** Another form of FTTP. This is similar to FTTH but is geared towards either business or multi-tenancy buildings such as apartment blocks. Fiber is used to the building but from that point to the offices or different apartments a different medium is used.
- **Fiber to the curb/kerb (FTTC/K):** In this instance, the service provider lays fiber connections to the communications cabinet at the end of the road (realistically this could be anywhere within 300 m of your premises).

In *Chapter 8, Media Types - Connecting Everything Together*, we discuss the characteristics of various cabling technologies including fiber. In that chapter, we will discuss the speeds of fiber. It is important to note that although the various FTTx implementations provide fast speeds to the various endpoints (home, business, curb, and so on) the onward connection from there to your end devices is likely to be slower, and you will not be able to take the full advantage of the speeds fiber offers.



## Satellite

Satellite WAN is an ideal connectivity solution in areas where the laying of cables is problematic, such as rural locations, hazardous terrain, on board ships, and so on. Laying cables to each of the aforementioned locations would be either prohibitively expensive or impossible. Although still a relatively expensive option, satellite avoids the problem of laying cables to these areas by utilizing satellites in a geo-stationary orbit above the equator. Geo-stationary means the satellite orbits the earth at the same speed the earth is rotating, thus allowing the satellite to be easily located. End user devices will connect to a modem-like device, which in turn is connected to a satellite dish. For communication to take place, the dish needs to have a clear line of sight to the satellite for the signal to get through. When installing and aligning a satellite dish, an engineer will have to take into consideration potential environmental factors. An example of this is trees. An engineer may have obtained a perfect signal during a wintertime installation, but come spring, leaves return to the tree and block the line of sight.

Satellite communication is known to have high latency. The signal has to go from earth to the satellite, and from the satellite to your provider's **Network Operations Center (NOC)** back on earth, from the NOC to the destination device. The data sent back in response follows that route in reverse. In ideal conditions, this can take about half a second to complete, but in reality is usually going to be slower due to internet traffic, heavy rain, snow, solar interference, and so on. In early satellite implementations, this latency resulted in maximum speeds of approximate 2 Mbp/s, which limited you to either web browsing or file downloading. Video conferencing, streaming, and online gaming was a definite non-starter. However, speeds have now increased dramatically, and at the time of writing (2019), Viasat offers a connection of 100 Mbp/s. *Figure 3.24* gives an overview of a satellite network:

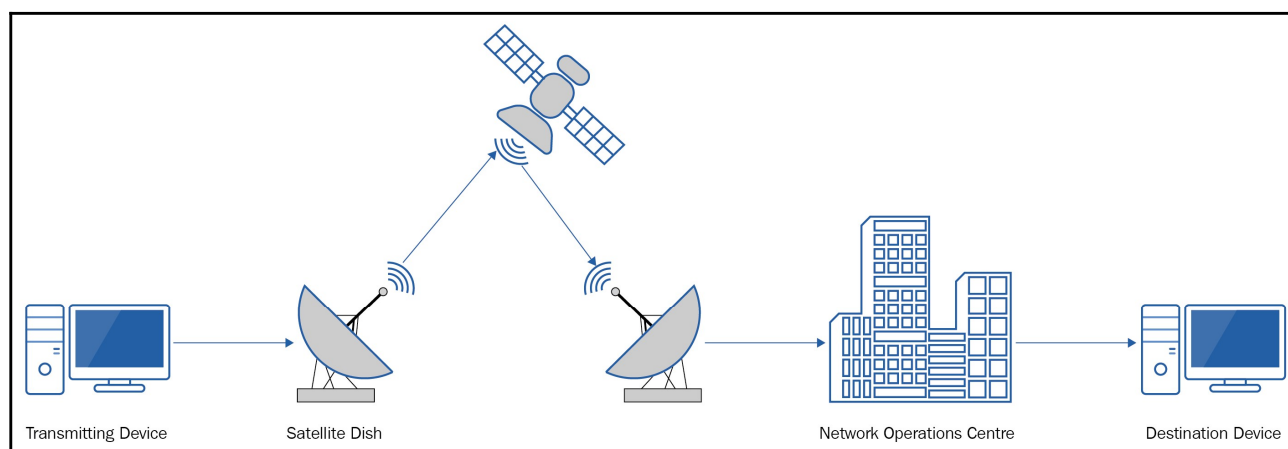


Figure 3.24: Satellite network

Interestingly, until recently I had a mindset that the use of satellite was few and far between and performance was relatively poor in comparison to wired connections. However, having just purchased a cave house in an area of Spain (trust me – Google them), I realized most of the village does not have the ability to have wired connections physically laid down and satellite is the only viable option. In addition, the quality of streaming video seemed to be better than my wired broadband connection in the UK.

As the price of cellular connections has started to drop or the data allowance per dollar has increased, the use of cellular connectivity as a means of sole connectivity has started to grow. My latest cellular contract offers me 100 GB of data per month for a reasonable price. This is more than enough for most people and moves us away from the need to have a fixed base station. In the next section, we discuss this technology in a little more detail.

## Cellular

Cellular technology has improved in leaps and bounds since its inception, and has become one of the main methods of accessing a **wireless WAN (WWAN)**. The majority of modern cell phones have the ability to connect through either 3G or 4G to provide information at our fingertips. A number of tablet devices and laptops also have cellular data connectivity functionality. This technology, along with cloud services, has allowed businesses to truly embrace the concept of having a mobile workforce.

To be able to utilize 3G or 4G, as with the other technologies, you need to have a subscription with a service provider and a mobile device. The mobile device will use either **Global System for Mobile (GSM)** or **Code Division Multiple Access (CDMA)** technology. GSM devices require a **Subscriber Identity Module (SIM)** card, whereas CDMA doesn't and providers use the device's **Electronic Serial Number (ESN)** to identify and authorize it on their network. CDMA is the prominent technology in the USA, and GSM elsewhere.

3G and 4G are the third and fourth generations (the G) of mobile data technology. As no formal standards have been agreed on as to what constitutes each of these technologies, it is difficult to state a maximum speed possible. 3G using HSPA+ can, theoretically, reach 21.6 Mb/s, and 4G can achieve 300 Mb/s. The caveat to these speeds is that they are achievable under ideal conditions rarely seen in the real world. There is also an impact on the speed obtained if the user is moving, as there is slowdown as they switch between cell towers.