FIT9137 Applied Week 12

Topics:

- Accessing the Internet
  - ADSL, Cable, NBN & Wireless Internet
  - NAT
  - Internet Structure, Autonomous Systems (AS)
  - Content Delivery Networks (CDN)

Covered Learning Outcomes:

- identify and describe fundamental concepts of Internet access technologies, Autonomous Systems, Network Address Translation (NAT), and Content Delivery Networks (CDN)

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (online) or more for face-to-face to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

1. **Compare and contrast these Internet access networks?**
   A. **DSL (Digital Subscriber Line)** denotes internet access technology that uses digital connections between a modem and a phone line, it represents the services that provide internet connections using a digital modem and an existing telephone network. In DSL the upload and download speed is almost the same, hence the name symmetric.
   The DSL allows the use of internet connection even while making calls as it works within the frequencies. There will be no interruptions. The only issue is that one has to be near the telephone exchange network to have the recommended speeds of DSL internet speeds. As you move far from the telephone network you may have a less speed internet connection. The telephone copper wires have a large number of frequencies. Out of this, a small amount is used for telephone communications. Hence, both, the telephone as well as the DSL modem can be used simultaneously.

   B. **Asymmetrical Digital Subscriber Line**: Asymmetrical Digital Subscriber Line. ADSL is a technology that also offers high-speed internet connection through existing telephone lines. In the ADSL network, the data sending speed is called upstream, and the data receiving speed is called downstream. Both speeds are not the same, rather their speeds differ from time to time.
   When one uses an ADSL broadband network a low pass filter is put into his phone connection which splits up the frequency of his phone line and his broadband

connection. With the help of this low pass filter and the ADSL modem, he can use the web even while using our phone.

C. **Cable internet access:** Cable Internet access, simply called cable Internet, is a form of broadband Internet access which uses the same infrastructure as a cable television. It is integrated into the cable television infrastructure existing cable network. Uses the standard called Data Over Cable Service Interface Specifications (abbreviated as DOCSIS) is a globally recognized telecommunications standard that enables high-bandwidth data transfer via existing coaxial cable systems that were originally used in the transmission of cable television program signals (CATVS).

2. What's a National Broadband Network (NBN)?

The National Broadband Network (NBN) was rolled out by the Australian Government to provide high-speed broadband network access throughout the country. The government provided the wholesale network infrastructure and network access technology and services to end users, Internet Service Providers and telecom companies that offer NBN plans for residents and businesses. The network technology is an upgrade to the existing phone and broadband service currently installed across Australia. This technology relies greatly on several telecommunication components, including fixed wireless, Hybrid Fibre Coaxial network, optical fiber cable, satellite and existing copper line in order to provide fast and reliable network services using FTTN, FTTP, FTTB and FTTC.

3. What Wireless Internet access technologies are available?

The terms '4G' and '5G' refer to generations of mobile network technology. A 'generation' is a term that categorizes major developments in how these mobile networks operate and transmit information.

4G is the fourth generation of mobile network technology, the successor to 3G. Likewise, 5G refers to the fifth generation, and the next step up from 4G in terms of speed, performance, and applications in use.

To sum up each wireless cellular generation so far:

1G: The first generation of mobile network, 1G was an analog two-way calling system that is now obsolete.

2G: The first mobile network to send digital radio signals, this generation brought us text and picture messages over mobile. It allowed mobile phones to send and receive emails and access the internet.

3G: The generation to make mobile internet faster and easier, its ability to transmit more data enabled touch-screen smartphones to go mainstream.

4G: The first generation to focus on data over voice calls, offering speeds 10 times faster than 3G and supporting more intensive activity such as high-definition video streaming.

5G: The newest generation of mobile, designed for super-fast speeds, more network capacity, and to enable technology such as smart homes, AI and connected vehicles.

This is the current technology that uses high-band 5G uses frequencies of 25–39 GHz, near the bottom of the millimeter wave band, although higher frequencies may be used in the future. It often achieves download speeds of in the gigabit per second (Gbit/s) range, comparable to cable-based internet.

5G Ultra Wideband, millimeter wavelength (mmWave)-based 5G, operates at frequencies of about 28 GHz and 39GHz. This is considerably higher than 4G networks, which use about 700 MHz-2500 MHz frequency to transfer information.

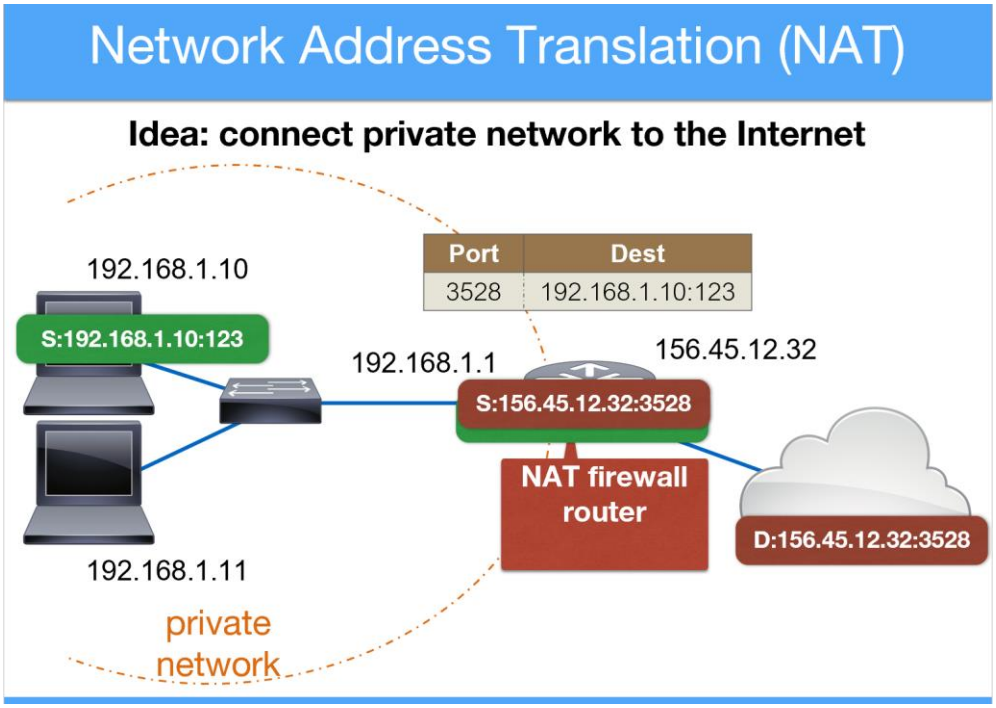
The disadvantages of 5G are its obstructions can impact connectivity. The range of 5G connectivity is not great as the frequency waves are only able to travel a short distance, hence the 5G network cells are small, and the cellular coverage and ranges are short distances.

4. Explain what's Network Address Translation (NAT) and why it is used?

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. This is popularly used when we have the shortage of public IPv4 addresses and also to avoid exposing the internal network devices to the public domain the internet.

The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both low-cost and security purposes.

The most common form of NAT or network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.



5. Explain the operation of NAT?

NAT is usually built-in Modems that has router-firewall that provide internet access connectivity via ISP. All Internet requests that require Network Address Translation (NAT)

are quite complex but happen so rapidly that the end user rarely knows it has occurred. A workstation inside a internal private network makes a request to a computer on the Internet. Routers within the network recognize that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet. When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public address is needed for hundreds or even thousands of users.

Most modern firewalls are stateful - that is, they are able to set up the connection between the internal workstation and the Internet resource. They can keep track of the details of the connection, like ports, packet order, and the IP addresses involved. This is called keeping track of the state of the connection. In this way, they can keep track of the session composed of communication between the workstation and the firewall, and the firewall with the Internet. When the session ends, the firewall discards all of the information about the connection.

Additionally, NAT can be used to allow selective access to the outside of the network, too. Workstations or other computers requiring special access outside the network can be assigned specific external IPs using NAT, allowing them to communicate with computers and applications that require a unique public IP address. Again, the firewall acts as the intermediary, and can control the session in both directions, restricting port access and protocols. NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

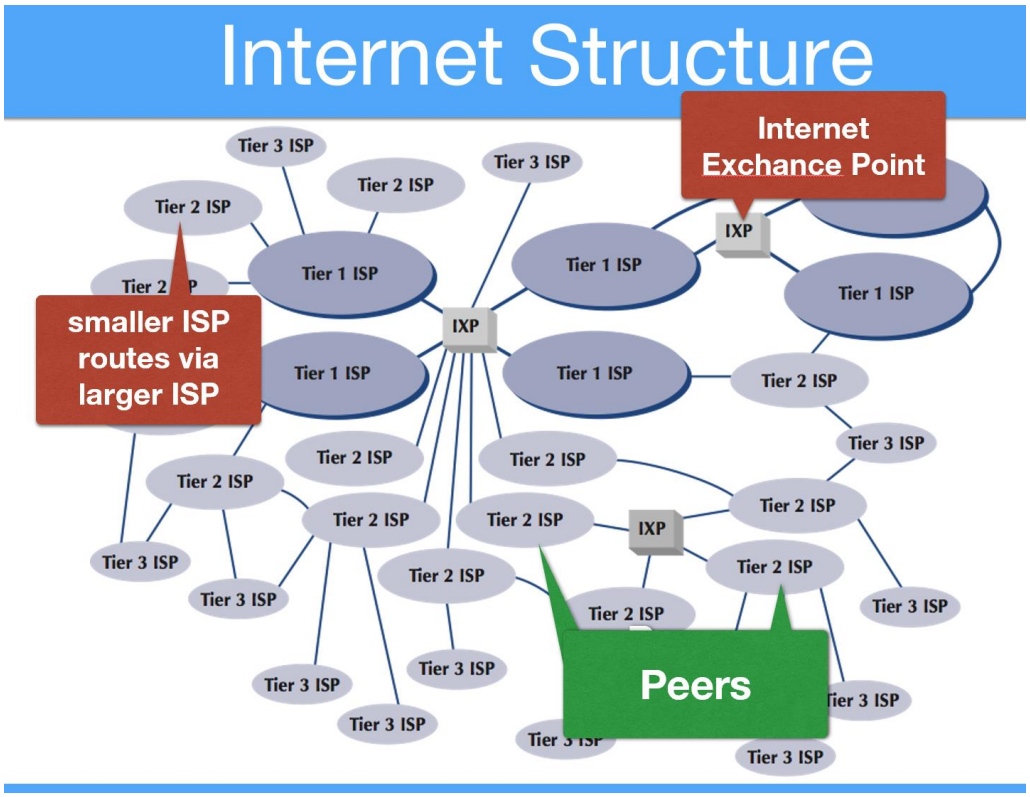
6. Explain these concepts:

A. structure of the Internet: The internet is a global network of interconnected networks called Autonomous systems. These Autonomous systems are networks such as ISP's, public and private networks of different sizes, that communicate using a common set of standards and protocols. These networks are owned and managed by a wide range of organizations, such as international, national, regional, governments, private companies, and academic institutions to form the global Internet.

The infrastructure of the internet consists of well-connected hierarchy of ISPs, each ISP operates an Autonomous system (AS). Routing information is shared between ASs using Border Gateway Protocol (BGP), and Internet exchange Points interconnect these hierarchy of ISPs and Autonomous systems. An Internet exchange point (IX or IXP) is the physical infrastructure through which Internet service providers (ISPs) and content delivery networks (CDNs) exchange Internet traffic between their networks (autonomous systems).

B. An autonomous system (AS): AS is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet.

C. **Border Gateway Protocol (BGP)**: BGP is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is classified as a path vector protocol.



D. **Content Delivery Networks:** On the Internet, content delivery (sometimes called content distribution, content distribution delivery, or content caching) is the service provided to internet subscribers.
A content delivery network or content distribution network (CDN) is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and high performance by distributing the service spatially relative to end-users. CDNs serve a large portion of the Internet content today, including rich web content, downloadable objects (media files, software, documents), applications (e-commerce, portals), live streaming media, on-demand streaming media, and social media sites. CDNs are a layer in the internet ecosystem. Content owners such as media companies and e-commerce vendors pay CDN operators to deliver their content to their end users. In turn, a CDN pays ISPs, carriers, and network operators for hosting its servers in their data centers.