Unit 9, Assignment 3, Tasks 1 & 2 (P5, D2)—Computer Networking

Thomas Robinson

SOLIHULL COLLEGE

Thomas Robinson

Task One (P5) – Services Provided by Networks

Directory Services

- **User Account Management**
  There are many types of accounts; local, remote and those managed by a directory server.
- **Active Directory**
  Is Microsoft's implementation of a directory server. It can manage a network's array of computers, permissions, applications and—primarily—users & groups.
- **DNS** (Domain Name System)
  Is the phone book of the internet. Converts a hostname (ex: google.com) to an IP address (142.250.200.46). When a request is made, the hostname is sent to a specified DNS server which then replies with the IP if it is known. A DNS server can be hosted on a local network to resolve local computer names. Examples of publicly available cloud-hosted DNS resolvers include CloudFlare DNS, Google and Quad9. One may chose to use these over their ISP's defaults to provide greater speed or increased privacy through DNS-over-TLS.

Telecommunication Services

- **Email**
  Electronic Mail is a method of sending and receiving messages electronically. Originally for exchanging messages to users on the same computer, it is now widely used over the internet.
- **Forums**
  Are online communities where one can create a "thread" which can be replied to and discussed.
- **Remote Desktop**
  Refers to accessing and controlling a computer while not being physically present at it.
- **Social Network**
  A social network is a website or platform that allows users to post messages and/or images about themselves while maintaining a circle of friends and/or followers.
- **VOIP**
  Voice over Internet Protocol is a method of transmitting telephone calls and voice communication over an IP-based network, such as the internet or an organisation's LAN. It can refer to both traditional

telephone solutions as well as services such as Skype and Microsoft Teams.

File Services

- **File Transfer (FTP)**
  File Transfer Protocol is a standard for transmitting files across a network.
- **File Sharing**
  Allows files and folders to be shared across a network. There are many standards for this, including SMB, NFS, FTP and TFTP.

Application Services

- **Application Software** (databases, web services)
  Application software refers to programs running on a server that are dedicated to hosting or serving an application or service. These can include database software (MySQL, PostgreSQL, Redis, MariaDB), web servers (Apache, NGINX, Caddy, IIS), authentication (LDAP, AD) and more.
- **Shared Resources** (printers, file storage)
  Shared resources refers to sharing the functionality of a device over a network, for example sharing a single printer with the users of an entire network.

Task Two (D2) – Usefulness of DS

Account Management

Account management is useful for providing centralised management capabilities. This can allow automation in account creation, modification and deletion. For example, an educational establishment could sync their database of students with the user account list[1], thus preventing the need to manually input each student individually. Similarly, a payroll system could be configured to disable user accounts of previous employees automatically to prevent unauthorised access.

Individual user accounts allow for file and resource permission management, which can increase data security by preventing people from accessing or modifying information they do not need to. For example, an employee working in a warehouse using a piece of inventory software would not need access to the company accounting documents.

Authentication Management

The Authentication Management options provided by a network operating system often facilitate great flexibility and interoperability.

Policies

Since authentication is centrally managed, it is possible to create policies and procedures that would otherwise not be possible. For example, self-service password resets, password strength requirements and MFA requirements[2].

Devices

When ran on a server, authentication for local devices in an organisation can be handled centrally. When logging into a device, the authentication service is contacted rather than the local devices' user database. This allows users to log in to any device configured to use the authentication server. Through profile roaming, they can get the same experience and access to the same files across any device they may log into.

Online Applications

Microsoft's cloud Active Directory solution enables Single Sign On. This means that a single user account can be used to log into multiple applications and services[3]. This prevents the need to manage multiple

[1] https://simsidlaunchpad.azurewebsites.net/support/wiki/88/active-directory-account-management-overview
[2] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-ops-guide-auth
[3] https://www.microsoft.com/en-gb/security/business/identity-access-management/single-sign-on

databases of accounts which makes memorising multiple passwords or the insecure reuse of passwords unnecessary.
Since the SSO solution is a web service, it is possible to integrate it into many applications across many devices.

Active Directory

Microsoft's Active Directory allows the management and configuration of users, groups, computers and the permissions and properties associated with them.

The centralised management of networked resources prevents the need for the configuration of individual computers. This saves significant amounts of time. The same policies and configuration can be rolled out to an entire organisations' fleet of devices remotely, which would be extremely time consuming and error-prone if it were to be done manually device-by-device.

Through the user of roaming profiles and folder redirection, it is possible for no user data to be stored locally on a device. This means that user data can be stored centrally which makes it easier to back-up and safeguard[4]. The same is true for the AD database itself; there is no need to back-up every computer individually since they only have the information that has been given to them by AD.

DNS

The Domain Name System is widely referred to as the phone book of the internet. It is the system used for converting a hostname or FQDN into an IP address[5].

The most obvious benefit of DNS is providing more memorable and identifiable names for devices, sites and resources rather than strings of numbers. This is especially important for IPV6, where an address can be 32 characters long when written in hexadecimal or on the Internet where there are millions of websites and services that we frequently access.

Additionally, a DNS record can be updated if the underlying IP address changes, for example if a website is migrated to a different provider or a business changes their ISP. This ensures an individual or business is not restricted to one provider in the long-term.

DNS is also a critical component of an Active Directory Domain. It is how AD determines the IP address of servers and resources on the network.

[4] https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview
[5] https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/

For example, when a user makes a request to a network file share, the AD server needs to know which IP address to relay to the user.

Threats & Mitigations

Unit 9, Assignment 3, Task 3 (M3)

Threats to a Network

AND HOW THEY CAN AFFECT A BUSINESS

Physical Threats

Natural Disasters

- Fires
- Floods
- Storms

Inevitable Threats

- Component Failure

Deliberate Vandalism

- Theft
- Destruction

Accidents

- Spills
- Drops

Software Threats

- **Virus**
  Replicates itself to infect other devices
- **Worm**
  Infects other hosts throughout a network/networks
- **Ransomware**
  Holds data/functionality hostage in exchange for a demand, often cryptocurrency
- **Spyware**
  Covertly collects personal information by way of keylogging, camera access, browser access

Remote Access

- **Hackers**
  Can target potentially vulnerable computer systems and networks to plant viruses or gain access to sensitive information
- **Attackers**
  Can use social engineering tactics (phishing, impersonation, threats) to coarse employees into giving up information or providing access
- **Organised Groups**
  Can target multiple companies or weaknesses in a single company to achieve their goals

Impact on an Organisation

- In the event of a major incident, the company's reputation could be irreparably damaged and the public's trust in the company severely eroded.
- Company information such as trade secrets could be leaked, payroll and employee information and other important documents could be irrecoverably lost.
- The company or individual employees could face fines, penalties or prison sentences if the incident resulted in an offence such as mishandling of data
- Employees may feel embarrassed to work for an organisation and leave prematurely
- All of these possibilities have the potential to cost the organisation a large amount of money, potentially taking them out of business entirely.

Threat Mitigation

HOW TO MINIMISE THE IMPACT OF THREATS TO A NETWORK

Physical Security

- **Locks**
  Locks can secure doors to areas that contain valuables
  Kensington Locks can be used to secure equipment to help prevent theft
- Keys, passes and biometrics can all be used to unlock both devices and doors.
- Biometric authentication include recognition of faces, irises, fingerprints and other unique features.
- **Security Guards & Cameras**
  Can notice suspicious individuals or any nefarious activity taking place.
- **Checking in/out**
  To prevent unauthorised access to a building, guests and employees can be made to log their entries and exits

Software Security

DEVICE-LEVEL

- Anti-Virus software can detect known/suspected malicious program before it is downloaded or executed
- Regular backups and version control can prevent successful ransomware attacks from causing major damage
- Keeping applications and operating systems up-to-date ensures that known vulnerabilities are patched

NETWORK-LEVEL

- Intrusion Prevention and Detection Systems can flag potential attacks and alert an administrator or outright block the offending client
- Firewalls can block everything but the necessary traffic from appearing in a network
- Honeypots can provide a diversion for black-hat hackers

Unit 9, Assignment 3, Task 4 (P6)

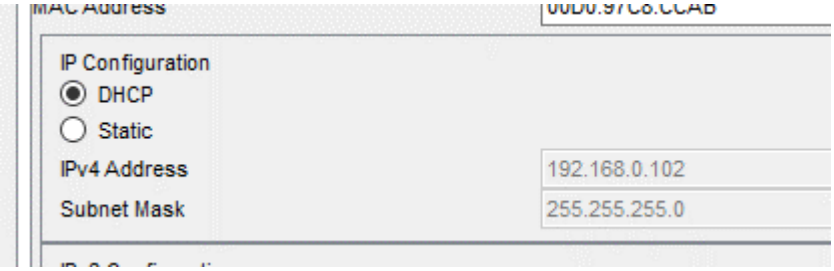
Thomas Robinson

SOLIHULL COLLEGE

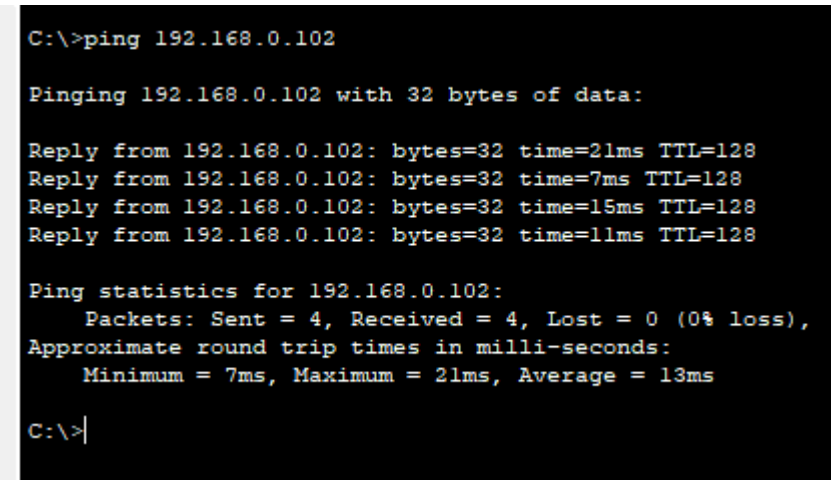
Thomas Robinson

T1: Enabling DHCP

On every device, DHCP was enabled if it was not already. Both the laptop and the server required configuration through their respective network adapter settings.

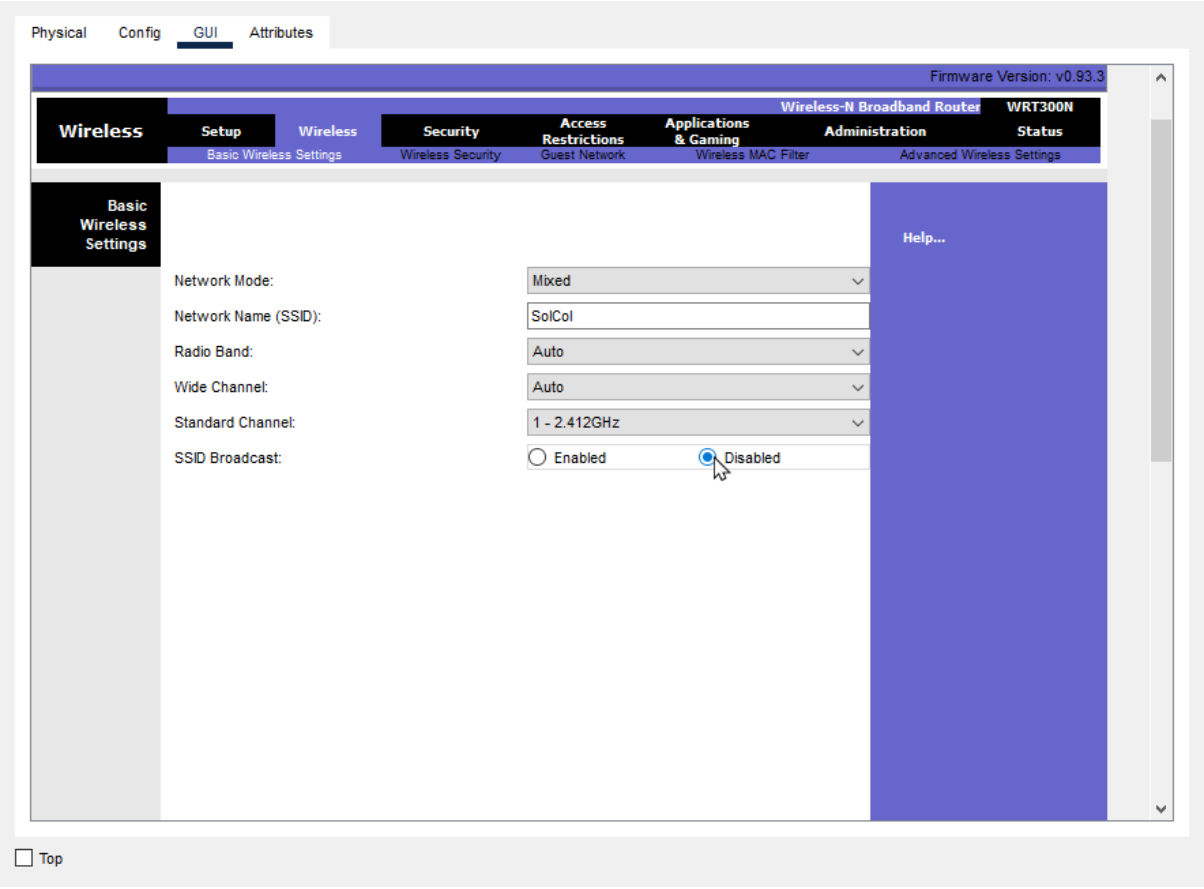


Checking Connectivity



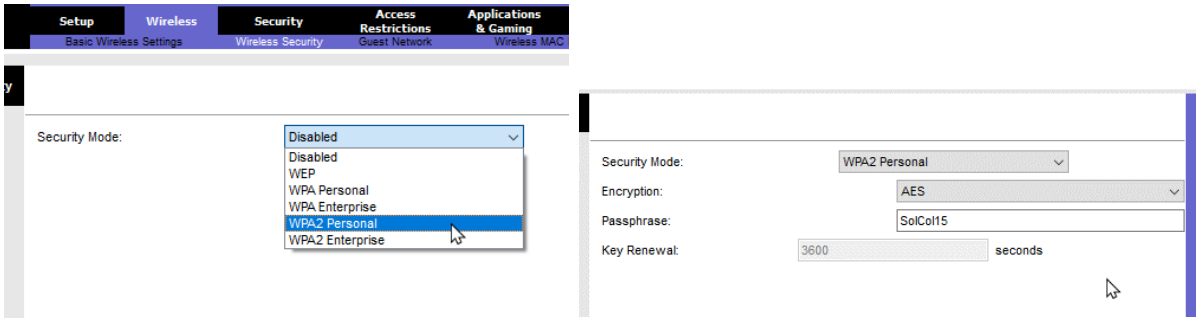
Pinging the server (192.168.0.102) from PC0 to show they are both connected and able to communicate.

T2: SSID Broadcasting



From the wireless router's GUI, SSID broadcast was disabled from the "Wireless" page. This prevents those who do not know the network name from easily connecting.

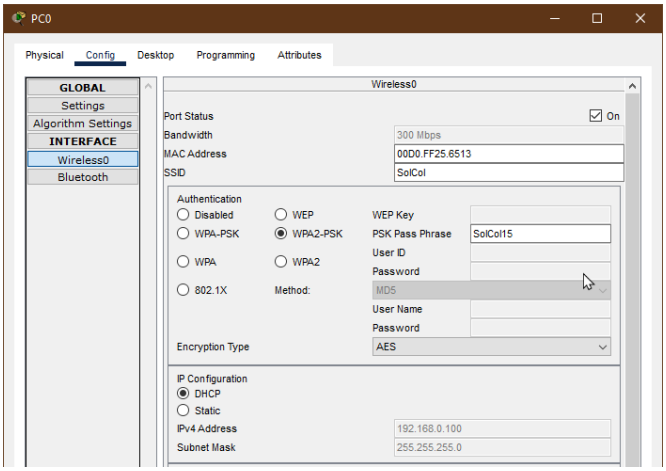
T3: WPA2 Encryption



From the "Wireless Security" page, WPA2 encryption was selected and a passphrase set. This prevents those without the passphrase from connecting to the network.

T4: Connecting the PCs

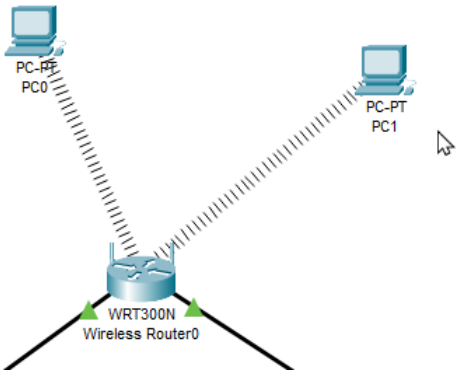
To wirelessly connect the PCs to the network now we have reconfigured it, we must update their respective settings.



This is done by modifying the interface Wireless0 from the configuration window. The SSID, Authentication and Pass Phrase settings were all updated. The IP configuration was kept as DHCP. This process was repeated for the other PC on the network.

Checking Connectivity

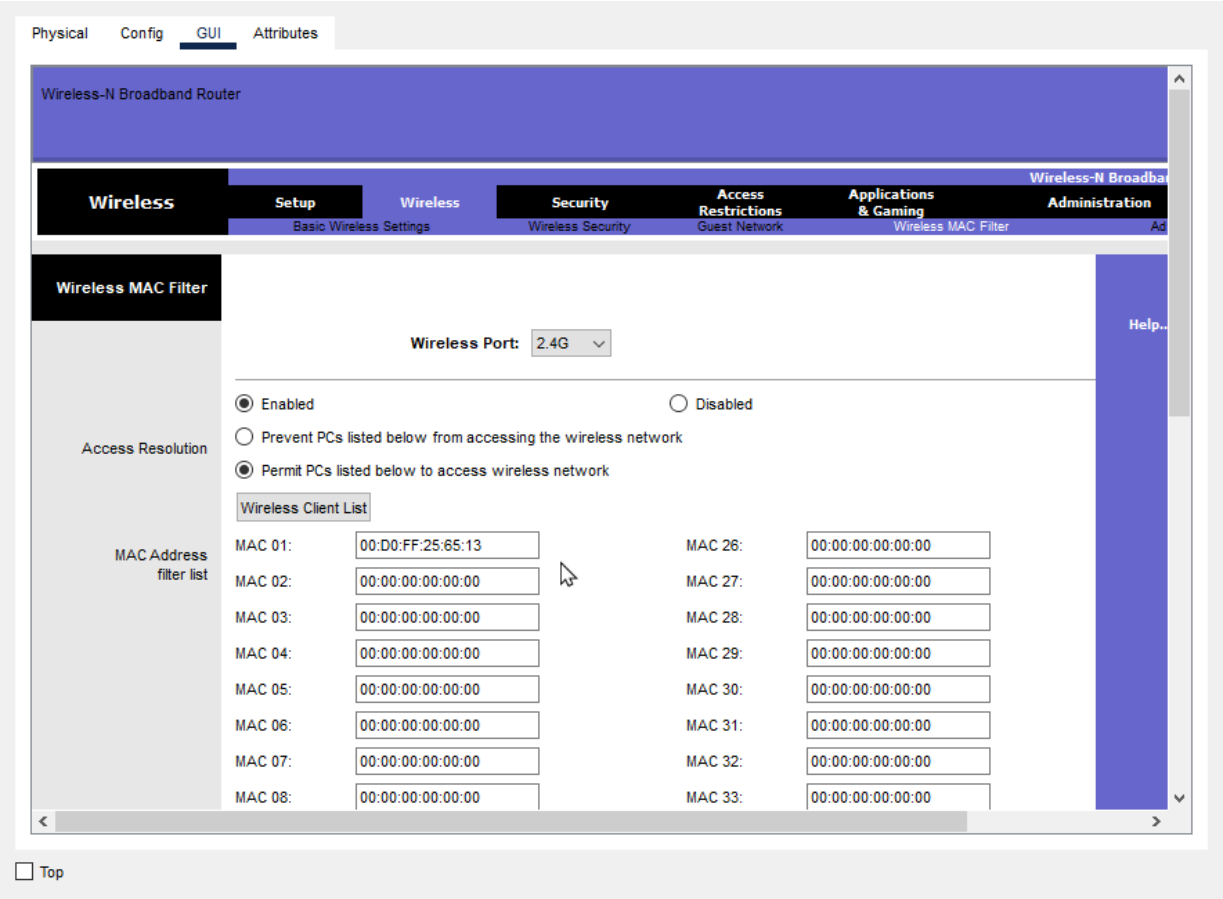
Since both PCs are able to ping the server, they are both correctly configured and connected successfully.




```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:

Reply from 192.168.0.102: bytes=32 time=25ms TTL=128
Reply from 192.168.0.102: bytes=32 time=7ms TTL=128
Reply from 192.168.0.102: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.0.102:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 25ms, Average = 12ms

Control-C
^C
C:\>
```

T5: MAC Filtering

To only allow certain devices to connect wirelessly to the network, MAC address filtering was configured from the GUI of the wireless router.



PC0's WLAN Adapter's MAC Address was added to the permitted devices' list. This enables it to connect to the WLAN. Since PC1's MAC Address was not added, it is not permitted to establish a connection.