Internet Apps

6 Browsers and Email

6.1 Browsers

The browser's main purpose is to present the web resource you choose, by requesting it from the server and displaying it on the browser window. The resource format is usually HTML but also PDF, image and more. The location of the resource is specified by the user using a URL (Uniform Resource Locator).

The way the browser interprets and displays HTML files is specified in the HTML and CSS specifications.

Browsers' user interfaces have a lot in common with each other. Among the common user interface elements are:

- Address bar for inserting the URL
- Back and forward buttons
- Bookmarking options
- Refresh and stop buttons for refreshing and stopping the loading of current documents
- Home button that gets you to your home page

6.1.1 Address bar

The URL that may be typed in the address bar might be something like:

http://google.com.au

The part before the ':' is called the scheme and is usually 'http' or 'https', but 'ftp',' mailto' and 'file' are also possible. The URL might also contain a user name and password and a port number if other than the default 80. So, you might (rarely) see something like:

ftp://user:password@host:21

More commonly, you might see a path added:

http://u3amanningham.org.au/courses.html

6.1.2 How does a browser work?

The web session exists in a client/server relationship. The browser is just half of it (the client). On the other side, there must be a web server waiting for requests, which is the other half of the application.

First the browser has to find the IP address of the web server. It asks the Operating System (OS) to translate the server name (URL). The OS uses its local cache or the DNS server if the address is not known yet.

After finding the IP address, the browser sends an HTTP request to the server requesting the appropriate file (web page). If no file was specified, the server responds with the "default file", usually the home page. The HTTP request may contain data that the server will interpret and use to generate an HTML page on the fly and send that back.

After getting the requested file, the browser has two things to do: interpret and render the HTML page and obtain the remaining objects (images, flash files, JavaScript files, css files, audio, video, etc.) and interpret and display them.

Once the browser has completed displaying the page it basically forgets (mostly) what it has done and the server keeps no record of what it has done (well, almost – see *cookies* below). If you move away from the page (using back or forward buttons or clicking a link) then you may have to start again from scratch (especially if you have entered data but failed to save it.

The browser does keep copies of web pages you visit but not necessarily for long. If you request a page again, the browser will look in the cache first to see if the copy is still there and hasn't expired.

Different browsers may display the same page differently.

6.1.3 HTML

HyperText Markup Language (HTML) is the language used to create web pages. Almost everything you see on your web browser is created in HTML.

Example:

```
<html>
<head>
<title>
A Simple HTML Document
</title>
</head>
<body>
<p>This is a very simple HTML document</p>
<p>It only has two paragraphs</p>
</body>
</html>
```

Click on the file *SimpleHtmlPage.htm* to see how the browser renders it.

6.1.4 JavaScript

JavaScript is a programming language embedded in HTML used to make web pages interactive.

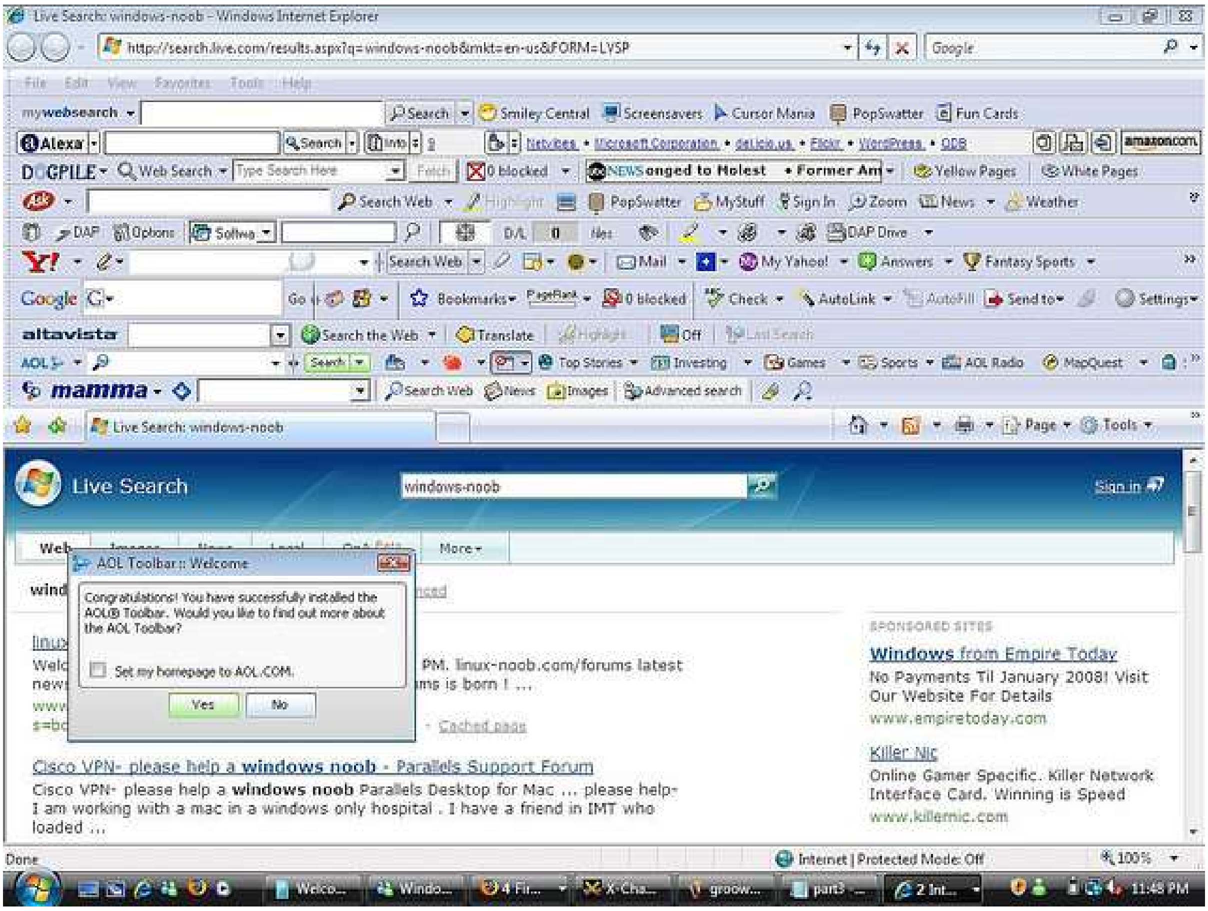
Click on the file *SimpleJSPage.html* to see how the browser renders it.

6.1.5 Cookies

A cookie is a small piece of data sent from a website and stored in the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). They can also be used to remember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers.

6.1.6 Common problems:

- Cache corrupted or gets too large
- Too many or corrupted cookies
- Browser incompatibility
- Corrupted HTML
- Unwanted pop-ups, ads
- Unwanted add-ons and menu bars
- JavaScript errors
- Too many toolbars



Congratulations! You have successfully installed the AOL® Toolbar. Would you like to find out more about the AOL Toolbar?

☐ Set my homepage to AOL.COM.

PM. linux-noob.com/forums latest ... ms is born ! ...

Cisco VPN- please help a **windows noob** - Parallels Support Forum

Cisco VPN- please help a **windows noob** Parallels Desktop for Mac ... please help- I am working with a mac in a windows only hospital . I have a friend in IMT who loaded ...

SPONSORED SITES

Windows from Empire Today
No Payments Til January 2008! Visit Our Website For Details
www.empiretoday.com

Killer Nic
Online Gamer Specific. Killer Network Interface Card. Winning is Speed
www.killernic.com

6.1.7 Secure browsing?

Many websites use the term "secure server" giving the impression that their server is perhaps more secure than others, when what they really mean is that their server uses HTTPS.

HTTPS is an encrypted version of HTTP. What this means is that the communication link between you and the server is encrypted, making it almost impossible for anyone to spy on that session and steal your password, for example. This does not mean than someone cannot exploit vulnerabilities (bugs) in the server software and steal your details later – especially if it hasn't been encrypted properly.

What it does not mean is that your computer or their server is in any way secure.

Your computer might be infected with a key logger that records every keypress and sends it to a site in Russia. Their server might have been hacked and all their customers' account details stolen.

6.1.8 Browser extensions

- Adblock
- HTTPS Everywhere
- Tabs to the Front (Chrome)
- Password manager

6.1.9 Safe practices

- Many users tend to click on links without considering the risks of their actions.
- Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities are often discovered after the software is configured and packaged by the manufacturer.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates.
- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.

6.1.10 Secure your browser

- Configure your browser's security and privacy settings.
- Keep your browser updated.
- Sign up for alerts.
- Be cautious when installing plug-ins.
- Make sure you have a good AV installed.
- Install security plug-ins:
    - HTTPS Everywhere
    - WebOfTrust
    - URL Expander
- Disable third-party cookies
- Disable Flash

6.1.11 Practise safe browsing

- Before you click on a link, hover over it to check the link looks OK – the underlying link should appear at the bottom of the browser or maybe in a small pop-up.
- Set your browser not to store passwords.
- Answer requests to store your passwords with 'never for this site'.

6.1.12 Search engines

A web search engine is a software system that is designed to search for information on the World Wide Web (Internet). Search engines work by *Web crawling* – it starts at the home page of a web site (URL), indexes the page and locates every link on the page, then visits each of the links in turn, indexing and visiting each link on that page, and so on.

Currently Google has about 64% of the market, followed by Bing (Microsoft) with about 21%.

Others to try:

- DuckDuckGo – a bit like Google with less clutter
- Google Scholar – a specialised version of Google
- The Internet Archive – find old news and old web sites

6.2 Web servers

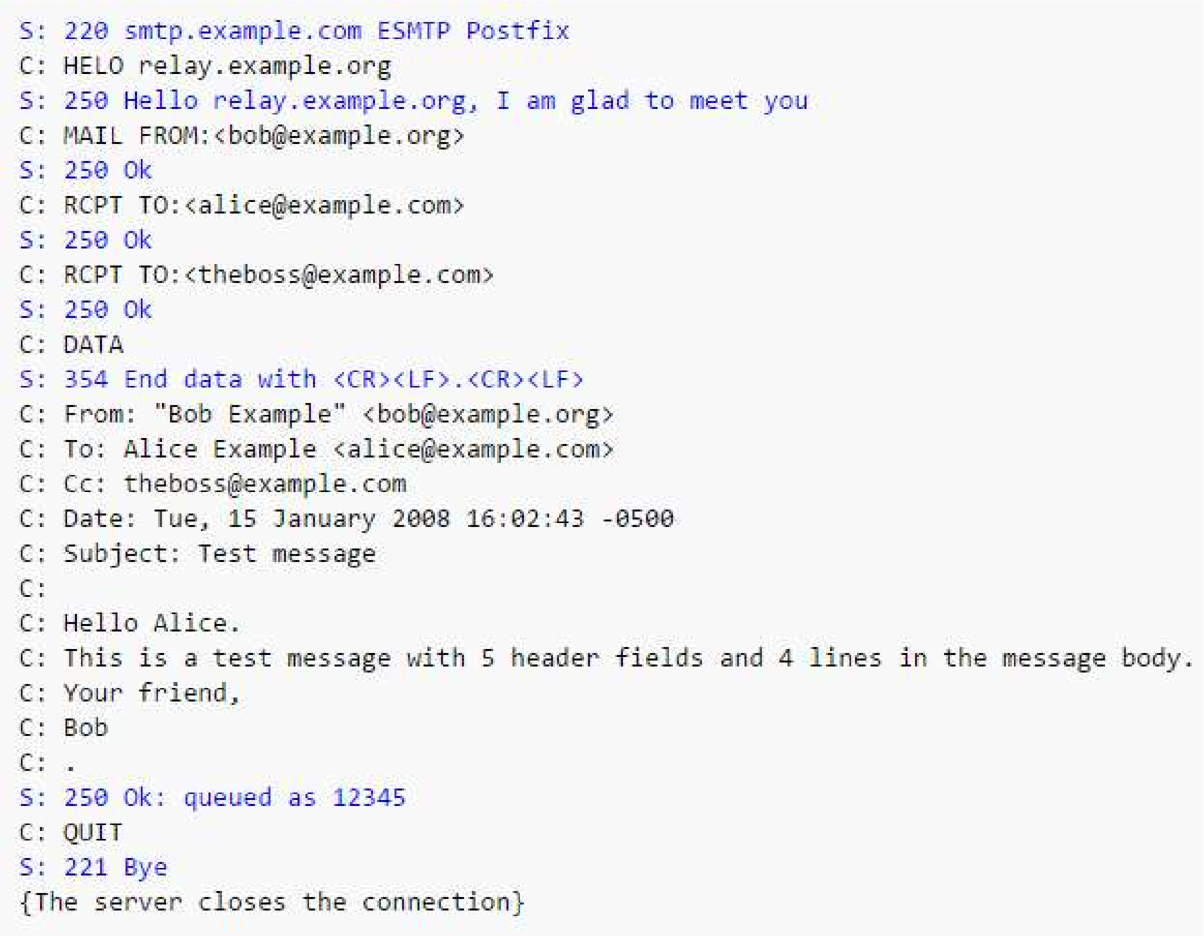
- Apache
- IIS (Internet Information Services)

6.3 Email clients

Email clients such as *Outlook*, *Thunderbird* and *eM Client* also work on the client/server model. There are three main protocols used:

1. SMTP – Simple Mail Transfer Protocol is used to send email from the client to the mail server.
2. POP – Post Office Protocol is used to retrieve mail from the mail server.
3. IMAP – Internet Message Access Protocol is also used to access mail on a mail server. IMAP is more versatile than POP in that it supports various message types (eg calendar) and allows the creation of folders on the server.

6.3.1 Sample SMTP session



```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

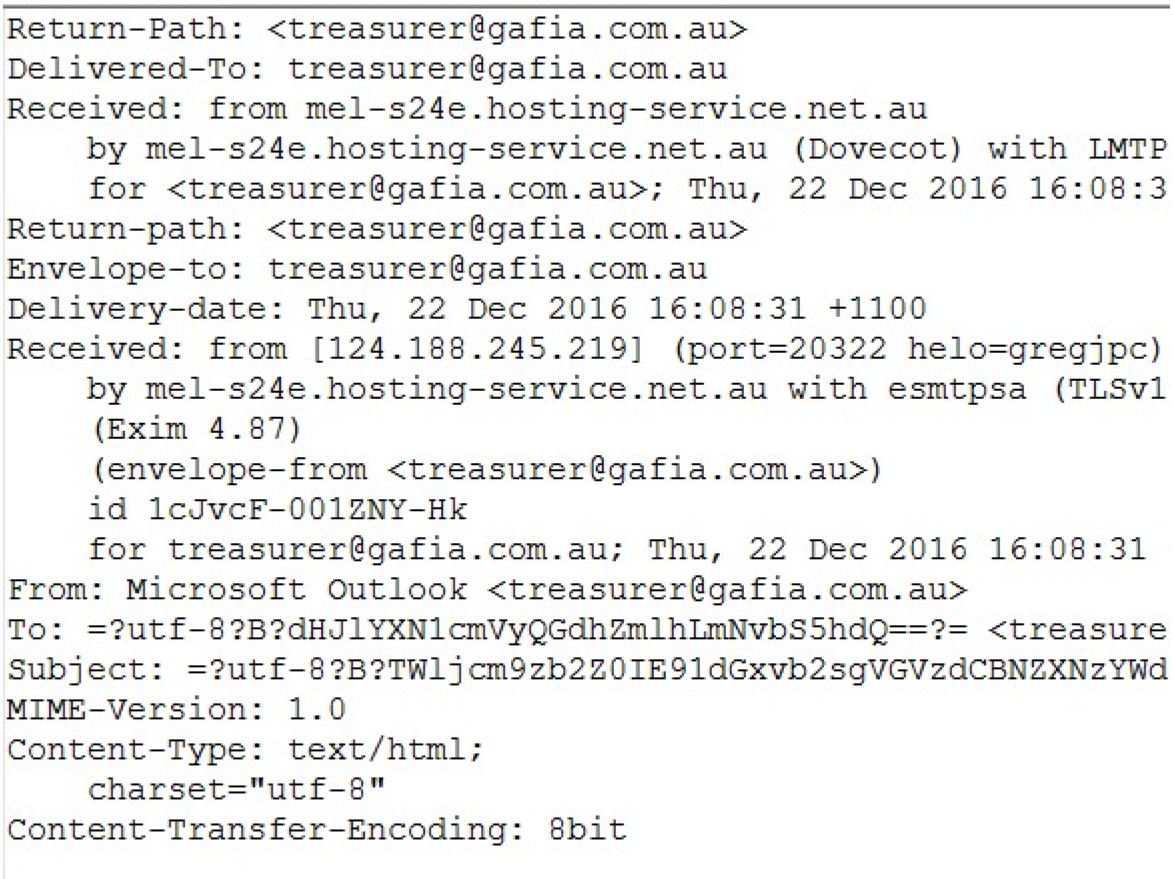
6.3.2 Email headers

Each email message you send or receive contains meta data and routing information. These are called "email headers". They're mostly used by mail servers, but there is a lot of information about who the email really came from and how it got to you.

If you are suspicious about an email, viewing the headers can sometimes reveal the truth about where it came from.

The ability to view the headers depends on the email client and you should use your favorite search engine to find out how to do it.

Example:



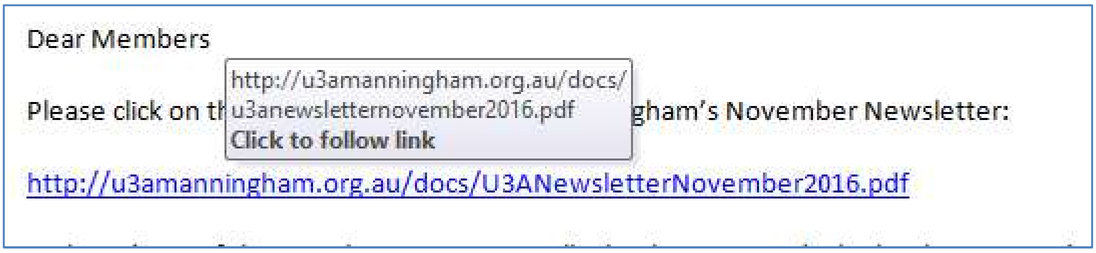
```
Return-Path: <treasurer@gafia.com.au>
Delivered-To: treasurer@gafia.com.au
Received: from mel-s24e.hosting-service.net.au
    by mel-s24e.hosting-service.net.au (Dovecot) with LMTP
    for <treasurer@gafia.com.au>; Thu, 22 Dec 2016 16:08:3
Return-path: <treasurer@gafia.com.au>
Envelope-to: treasurer@gafia.com.au
Delivery-date: Thu, 22 Dec 2016 16:08:31 +1100
Received: from [124.188.245.219] (port=20322 helo=gregjpc)
    by mel-s24e.hosting-service.net.au with esmtpsa (TLSv1
    (Exim 4.87)
    (envelope-from <treasurer@gafia.com.au>)
    id 1cJvcF-001ZNY-Hk
    for treasurer@gafia.com.au; Thu, 22 Dec 2016 16:08:31
From: Microsoft Outlook <treasurer@gafia.com.au>
To: =?utf-8?B?dHJlYXN1cmVyQGdhZmlhLmNvbS5hdQ==?= <treasure
Subject: =?utf-8?B?TWljcm9zb2Z0IE91dGxvb2sgVGVzdCBNZXNzYWd
MIME-Version: 1.0
Content-Type: text/html;
    charset="utf-8"
Content-Transfer-Encoding: 8bit
```

6.3.3 Avoid spam

- If you are overloaded with spam, it is probably best to get a new email address.
- Create separate email accounts, one that you give to friends and family; another that you give out online (and be prepared to change from time to time).
- Use a reliable email host that has good anti-spam filtering (eg Google mail).
- Obscure your email address on any web sites [eg myname(at)gmail(dot)com]

6.3.4 Avoid scams and fraud

- Do not click on links without checking them first:



Dear Members

Please click on th gham's November Newsletter:

http://u3amanningham.org.au/docs/U3ANewsletterNovember2016.pdf

http://u3amanningham.org.au/docs/
u3anewsletternovember2016.pdf
Click to follow link

This example is from Outlook. Other email clients behave differently.

- If you don't know who sent the email, delete it
- Create separate email accounts
- Block a sender
- Never send money or provide credit card details to unsolicited offers, emails or calls
- Banks will never send emails asking you to confirm details
- Don't confirm your identity to an unsolicited call – Telstra is good at this:

  - “Hi I’m Joe Bloggs from Telstra, can you confirm your date of birth?”
  - “No, you called me, you need to confirm who you are.””
  - “Um…”
- Never respond to requests for personal information (DOB is a common one) or update information
- View email headers – Gmail, Outlook, Thunderbird
- Scams, spoofing, phishing, masquerading

6.4 Phishing

Phishing scams are attempts by scammers to trick you into giving out personal information such as your bank account numbers, passwords and credit card numbers.

Warning signs:

- You receive an email, text or phone call claiming to be from a bank, telecommunications provider or other business you regularly deal with, asking you to update or verify your details.
- The email or text message does not address you by your proper name, and may contain typing errors and grammatical mistakes.
- The website address does not look like the address you usually use and is requesting details the legitimate site does not normally ask for.
- You notice new icons on your computer screen, or your computer is not as fast as it normally is.

6.5 Ransomware

Superficially ransomware (also known as a cryptolocker) is similar to phishing scams – it looks legitimate and contains fake links. The insidious part is that the fake link takes you to a website that downloads and installs malware that locks your computer. The software typically demands a payment to unlock your computer.

Protection:

- Keep your operating system up-to-date
- Back up your computer regularly
- Install well regarded anti-virus software
- Use a well-regarded browser and email client
- Do not use your computer in administrator mode

6.6 Tools

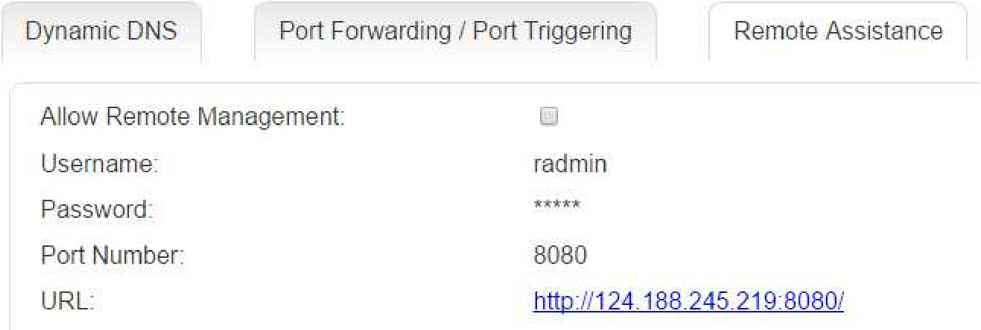
- getmac
- GRC website
- ipconfig
- myip website
- netstat
- Network scanner – NetScan, Nmap, iNet (iPhone)

- nslookup
- ping
- Speedtest
- traceroute (tracert)
- whois

6.7 Secure your router

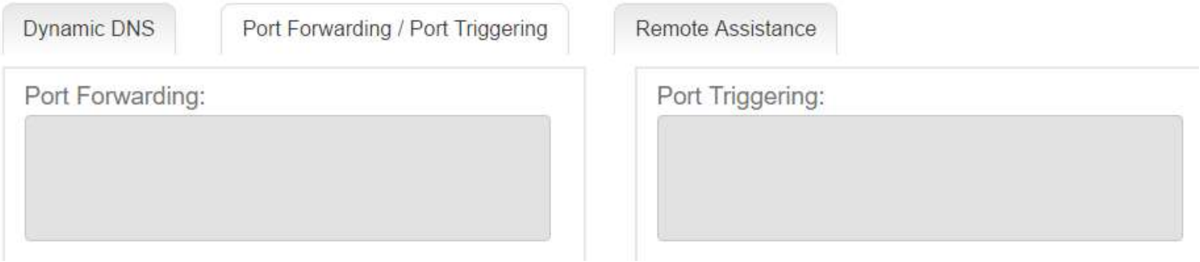
This is the part of the router that is connected to the world. It is very important to make yourself invisible to the Internet.

- Enable firewall. Make sure all external ports are closed
- Change default settings
- Disable remote administration and /or remote assistance



Allow Remote Management: ☐
Username: radmin
Password: *****
Port Number: 8080
URL: http://124.188.245.219:8080/

- Turn off port forwarding



- Disable ‘Respond to ping’

6.8 Links

- https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/
- https://en.wikipedia.org/wiki/HTTP_cookie
- https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/
- https://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914
- https://mxtoolbox.com/Public/Content/EmailHeaders/
- https://perezbox.com/2015/07/https-does-not-secure-your-website/
- http://refreshyourcache.com/en/home/
- http://speedtest.net/
- http://wikihow.com/Fix-Common-Internet-Problems