Learning Guide 4: Other Server Services and Resource Management

Information Sheet 4.1: Email Server and VPN

Dr. Patrick D. Cerna (Associate Professor)

4.1 What is a Mail Server?

- A mail server is the computerized equivalent of your friendly neighborhood mailman.
- Every email that is sent passes through a series of mail servers along its way to its intended recipient.
- Often referred to as simply "mail server", an e-mail server is a computer within your network that works as your virtual post office.

What is a Mail Server?

- Generally the person(s) responsible for the maintenance of the e-mail server (editing users, monitoring system activity) are referred to as the postmaster.
- Most mail servers are designed to operate without any manual intervention during normal operation.

Types of Mail Servers

- Mail servers can be broken down into two main categories: outgoing mail servers and incoming mail servers.
- Outgoing mail servers are known as SMTP, or Simple Mail Transfer Protocol, servers.
- Incoming mail servers come in two main varieties

Types of Mail Servers

- POP3, or Post Office Protocol, version 3, servers are best known for storing sent and received messages on PCs' local hard drives.
- IMAP, or Internet Message Access Protocol, servers always store copies of messages on servers.
- Most POP3 servers can store messages on servers, too, which is a lot more convenient.

Types of Mail Servers

The Process of Sending an Email

- **Step #1**: After composing a message and hitting send, your email client - whether it's Outlook Express or Gmail - connects to your domain's SMTP server. This server can be named many things; a standard example would be smtp.example.com.
- **Step #2:** Your email client communicates with the SMTP server, giving it your email address, the recipient's email address, the message body and any attachments.
-

The Process of Sending an Email

- **Step #3:** The SMTP server processes the recipient's email address - especially its domain. If the domain name is the same as the sender's, the message is routed directly over to the domain's POP3 or IMAP server - no routing between servers is needed.
- If the domain is different, though, the SMTP server will have to communicate with the other domain's server.

The Process of Sending an Email

- Step #4: In order to find the recipient's server, the sender's SMTP server has to communicate with the DNS, or Domain Name Server. The DNS takes the recipient's email domain name and translates it into an IP address.
- The sender's SMTP server cannot route an email properly with a domain name alone; an IP address is a unique number that is assigned to every computer that is connected to the Internet. By knowing this information, an outgoing mail server can perform its work more efficiently.

The Process of Sending an Email

- Step #5: Now that the SMTP server has the recipient's IP address, it can connect to its SMTP server. This isn't usually done directly, though; instead, the message is routed along a series of unrelated SMTP servers until it arrives at its destination.

The Process of Sending an Email

- Step #6: The recipient's SMTP server scans the incoming message. If it recognizes the domain and the user name, it forwards the message along to the domain's POP3 or IMAP server.
- From there, it is placed in a send mail queue until the recipient's email client allows it to be downloaded. At that point, the message can be read by the recipient.

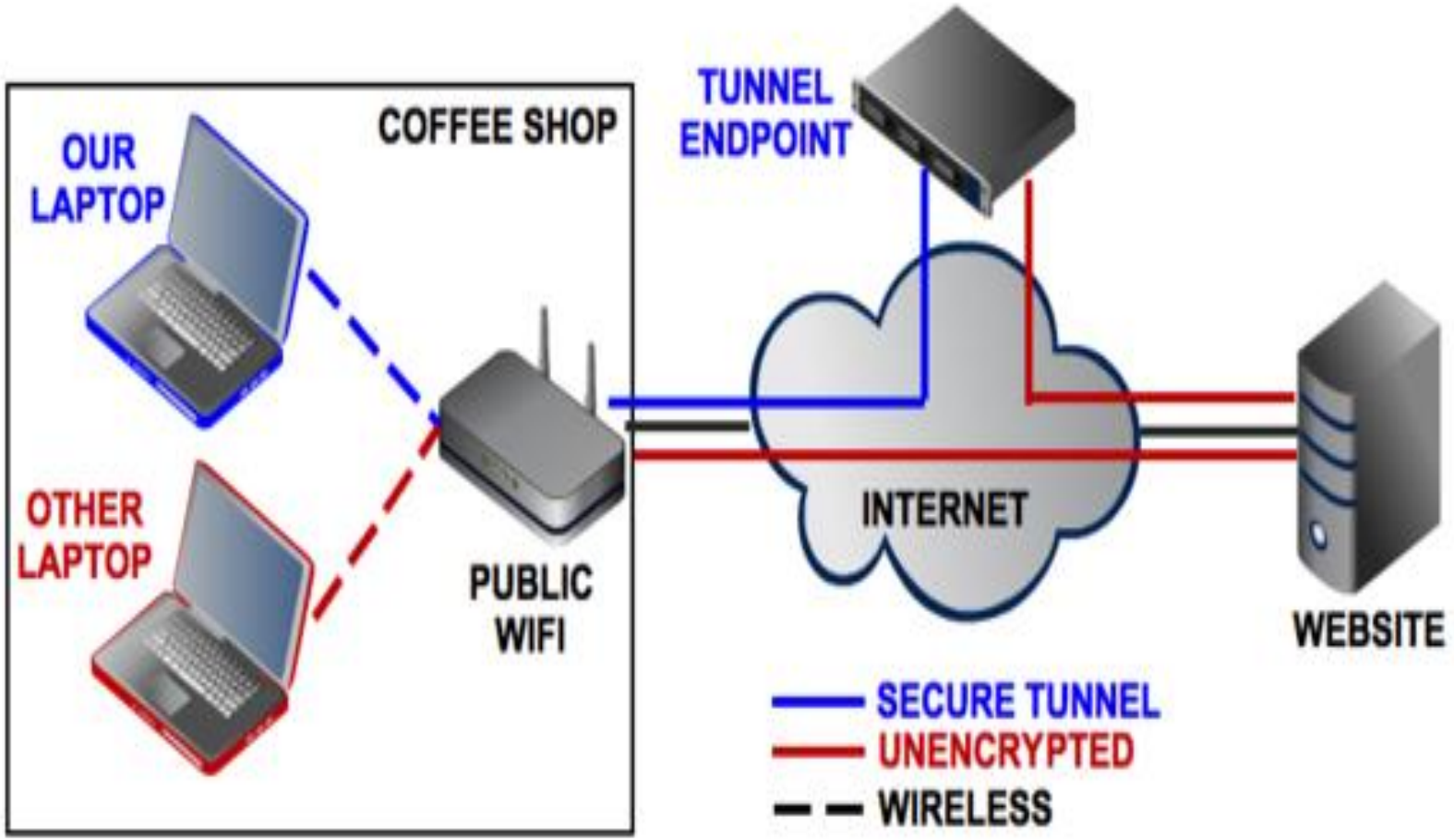
4.2 Virtual Private Network (VPN)

- A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

4.2 Virtual Private Network (VPN)

- A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
- A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

4.2 Virtual Private Network (VPN)



4.2 Virtual Private Network (VPN)

- This diagram illustrates the difference between using an unencrypted connection and using a VPN-secured Internet connection at your average coffee shop.

Types of VPN

- **Point-to-Point Tunneling Protocol (PPTP)** is the least secure VPN method, but it’s a great starting point for your first VPN because almost every operating system supports it, including Windows, Mac OS, and even mobile OSs.

Types of VPN

- **Layer 2 Tunneling Protocol (L2TP)** and **Internet Protocol Security (IPsec)** are more secure than PPTP and are almost as widely supported, but they are also more complicated to set up and are susceptible to the same connection issues as PPTP is.

Types of VPN

- **Secure Sockets Layer (SSL)** VPN systems provide the same level of security that you trust when you log on to banking sites and other sensitive domains. Most SSL VPNs are referred to as "clientless," since you don't need to be running a dedicated VPN client to connect to one of them.

Open VPN Software

- **OpenVPN** is exactly what it sounds like: an open-source VPN system that's based on SSL code. It's free and secure, and it doesn't suffer from connection issues, but using OpenVPN does require you to install a client since Windows, Mac OS X, and mobile devices don't natively support it.

References:

- **References:**

- "*Principles of Network and System Administration" (2nod Edition),* John Wiley and Sons Ltd, Mark Burgess, 2004.
- "*Essential System Administration", 3rd Edition*, O'Reilly and Associates Inc., Len Frisch, 2003.
- "*Running Linux", (5th Edition),* O'Reilly and Associates Inc., Matthias Kalle Dalheimer and Matt Welsh, 2007.