ANEXOS

ANEXO A

Laboratorio 1.1 — Configuración Básica del Switch

ANEXO 1.- Tabla comparativa	
Marca del dispositivo	Número de empresas que la utilizan
Cisco	23
Nortel	4
3COM	3
Intellinet	2
Netgear	2
Juniper	2
Otros	1

Configuración Switch Cisco

lab@UNAM> show configuration

```
## Last commit: 2012-02-26 15:43:49 UTC by lab
version 11.4R1.6;
system {
    host-name UNAM;
    domain-name UNAM.COM.MX;
    root-authentication {
        encrypted-password "$1$Zkcm12Sr$i89vl0xqVCvc6oyhSJh3M/"; ## SECRET-
DATA
        ssh-dsa "ssh-dss
AAAAB3NzaC1kc3MAAACBAMQrfP2bZyBXJ6PC7XXZ+MzErl8Jl6jah5L4/O8BsfP2hC7E
vRfNoX7MqbrtCX/9gUH9gChVuBCB+ERULMdgRvM5uGhC/gs4UX+4dBbfBgKYYwg
misM8EoT25m7ql8ybpl2YZvHNznvO8h7kr4kpYuQEpKvgsTdH/Jle4Uqnjv7DAAAAFQD
ZaqA6QAgbW3O/zveaLCIDj6p0dwAAAIB1iL+krWrXiD8NPpY+w4dWXEqaV3bnobzP
C4eyxQKBUCOr80Q5YBIWXVBHx9elwBWZwj0SF4hLKHznExnLerVsMuTMA846RbQmSz
62vM6kGM13HFonWeQvWia0TDr78+rOEgWF2KHBSIxL51lmIDW8Gql9hJfD/Dr/NKP97
w3L0wAAAIEAr3FkWU8XbYytQYEKxsIN9P1UQ1ERXB3G40YwqFO484SlyKyYCfaz+yNsa
AJu2C8UebDIR3GieyNcOAKf3inCG8jQwjLvZskuZwrvlsz/xtcxSoAh9axJcdUfSJYMW/g
+mD26JK1Cliw5rwp2nH9kUrJxeI7IReDp4egNkM4i15o= configurator@server1.he"; ##
SECRET-DATA
    }
    name-server {
        192.168.200.35;
    }
```

```
    login {
        announcement "Esta entrando al modo de configuracion del switch todo
cambio debe ser autorizado por el administrador del dispositivo";
        message "Esta entrando a un dispositivo propiedad de la Universidad
Nacional Autonoma de Mexico";
        user CU {
            full-name "Ciudad Universita";
            uid 1251;
            class read-only;
            authentication {
                encrypted-password "$1$nYVcJmTO$.DIga8.JKr4G7Q5LPKtfs1"; ##
SECRET-DATA
            }
        }
        user fi {
            full-name "Facultad de Ingenieria";
            uid 1250;
            class super-user;
            authentication {
                encrypted-password "$1$k7HoOQik$Why1zAWpMk3BwZmkZFqjC0"; ##
SECRET-DATA
            }
        }
        user lab {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$84J5Maes$cni5Hrazbd/IEHr/50oY30"; ## SECRET-
DATA
            }
        }
    }
    services {
        ftp;
        ssh;
        telnet;
    }
    syslog {
        file messages {
            any notice;
            authorization info;
```

```
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    fe-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.200.14/24;
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.200.13/24;
            }
        }
    }
    me0 {
        unit 0 {
            family inet {
                address 10.210.14.147/27;
                address 192.168.200.8/24;
            }
        }
    }
}
{master:0}
```

Configuración Switch Juniper

```
lab@UNAM> show configuration
## Last commit: 2012-02-26 15:43:49 UTC by lab
version 11.4R1.6;
system {
    host-name UNAM;
    domain-name UNAM.COM.MX;
    root-authentication {
        encrypted-password "$1$Zkcm12Sr$i89vl0xqVCvc6oyhSJh3M/"; ## SECRET-
DATA
        ssh-dsa "ssh-dss
AAAAB3NzaC1kc3MAAACBAMQrfP2bZyBXJ6PC7XXZ+MzErl8Jl6jah5L4/O8BsfP2hC7E
vRfNoX7MqbrtCX/9gUH9gChVuBCB+ERULMdgRvM5uGhC/gs4UX+4dBbfBgKYYwg
misM8EoT25m7ql8ybpl2YZvHNznvO8h7kr4kpYuQEpKvgsTdH/Jle4Uqnjv7DAAAAFQD
ZaqA6QAgbW3O/zveaLCIDj6p0dwAAAIB1iL+krWrXiD8NPpY+w4dWXEqaV3bnobzP
C4eyxQKBUCOr80Q5YBIWXVBHx9elwBWZwj0SF4hLKHznExnLerVsMuTMA846RbQmSz
62vM6kGM13HFonWeQvWia0TDr78+rOEgWF2KHBSIxL51lmIDW8Gql9hJfD/Dr/NKP97
w3L0wAAAIEAr3FkWU8XbYytQYEKxsIN9P1UQ1ERXB3G40YwqFO484SlyKyYCfaz+yNsa
AJu2C8UebDIR3GieyNcOAKf3inCG8jQwjLvZskuZwrvlsz/xtcxSoAh9axJcdUfSJYMW/g
+mD26JK1Cliw5rwp2nH9kUrJxeI7IReDp4egNkM4i15o= configurator@server1.he"; ##
SECRET-DATA
    }
    name-server {
        192.168.200.35;
    }
    login {
        announcement "Esta entrando al modo de configuracion del switch todo
cambio debe ser autorizado por el administrador del dispositivo";
        message "Esta entrando a un dispositivo propiedad de la Universidad
Nacional Autonoma de Mexico";
        user CU {
            full-name "Ciudad Universita";
            uid 1251;
            class read-only;
            authentication {
                encrypted-password "$1$nYVcJmTO$.DIga8.JKr4G7Q5LPKtfs1"; ##
SECRET-DATA
            }
        }
        user fi {
```

```
            full-name "Facultad de Ingenieria";
            uid 1250;
            class super-user;
            authentication {
                encrypted-password "$1$k7HoOQik$Why1zAWpMk3BwZmkZFqjC0"; ##
SECRET-DATA
            }
        }
        user lab {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$84J5Maes$cni5Hrazbd/IEHr/50oY30"; ## SECRET-
DATA
            }
        }
    }
    services {
        ftp;
        ssh;
        telnet;
    }
    syslog {
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    fe-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.200.14/24;
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
```

```
            family inet {
                address 192.168.200.13/24;
            }
        }
    }
    me0 {
        unit 0 {
            family inet {
                address 10.210.14.147/27;
                address 192.168.200.8/24;
            }
        }
    }
}
{master:0}
```

Laboratorio 1.2 Configuración Básica del Router

Configuración Router Cisco

Router Sucursal A

```
Current configuration : 1065 bytes

version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname sucursal-A

enable secret 5 $1$mERr$IvMzPKRCtQBn.dJGMlbj50

interface FastEthernet0/0
 ip address 192.168.0.126 255.255.255.128
 duplex auto
 speed auto

interface FastEthernet1/0
 ip address 192.168.0.158 255.255.255.224
 duplex auto
 speed auto

interface Serial2/0
 ip address 192.168.0.253 255.255.255.252
 clock rate 56000

interface Serial3/0
 no ip address
 shutdown

interface FastEthernet4/0
 no ip address
 shutdown

interface FastEthernet5/0
 no ip address
 shutdown

router rip
```

```
 version 2
 network 192.168.0.0

ip classless

banner login ^CEsta entrano aun dispositivo propiedad de la Universidad Nacional Autonoma de Mexico^C
banner motd ^CEsta entrando al modo de configuracion toda cambio debe ser permitido por el administrador de la red^C

line con 0
 password bk123
 login
line vty 0 4
 password bk123
 login
line vty 5 15
 password bk123
 login

end
```

Router Sucursal B

```
Current configuration : 978 bytes

version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption

hostname Sucursal-B

enable secret 5 $1$mERr$IvMzPKRCtQBn.dJGMlbj50

interface FastEthernet0/0
 ip address 192.168.0.190 255.255.255.224
 duplex auto
 speed auto

interface FastEthernet1/0
 ip address 192.168.0.206 255.255.255.240
 duplex auto
 speed auto

interface Serial2/0
```

```
 ip address 192.168.0.254 255.255.255.252

interface Serial3/0
 no ip address
 shutdown

interface FastEthernet4/0
 no ip address
 shutdown

interface FastEthernet5/0
 no ip address
 shutdown

router rip
 version 2
 network 192.168.0.0

ip classless

banner login ^CEsta entrando al modo de configuracion todo cambio debe ser permitido
por el administrador del dispositivo^C

line con 0
 password 7 0823471F5B4A
 login
line vty 0 4
 password 7 0823471F5B4A
 login
line vty 5 15
 password 7 0823471F5B4A
 login
end
```

Configuración Router Juniper

Router Sucursal A

```
system {
    host-name sucursal-A;
    domain-name UNAM.COM.MX;
    root-authentication {
        encrypted-password "$1$HHuqLObU$.hHEXeFnZp.e6nEqd4tMG0"; ## SECRET-DATA
        ssh-dsa "ssh-dss
AAAAB3NzaC1kc3MAAACBAMQrfP2bZyBXJ6PC7XXZ+MzErI8JI6jah5L4/O8BsfP2hC7EvRfNoX7
MqbrtCX/9gUH9gChVuBCB+ERULMdgRvM5uGhC/gs4UX+4dBbfBgKYYwgmisM8EoT25m7ql8
ybpl2YZvHNznvO8h7kr4kpYuQEpKvgsTdH/Jle4Uqnjv7DAAAAFQDZaqA6QAgbW3O/zveaLCI
Dj6p0dwAAAIB1iL+krWrXiD8NPpY+w4dWXEqaV3bnobzPC4eyxQKBUCOr80Q5YBlWXVBHx9el
wBWZwj0SF4hLKHznExnLerVsMuTMA846RbQmSz62vM6kGM13HFonWeQvWia0TDr78+rOEgWF
2KHBSIxL51lmlDW8Gql9hJfD/Dr/NKP97w3L0wAAAIEAr3FkWU8XbYytQYEKxsIN9P1UQ1ERXB3G
40YwqFO484SlyKyYCfaz+yNsaAJu2C8UebDIR3GieyNcOAKf3inCG8jQwjLvZskuZwrvlsz/xtcxSo
Ah9axJcdUfSJYMW/g+mD26JK1Cliw5rwp2nH9kUrJxeI7IReDp4egNkM4i15o=
configurator@server1.he"; ## SECRET-DATA
    }
    name-server {
        192.168.200.35;
    }
    login {
        announcement "Esta entrando al modo de configuracion del router, todo cambio
debe ser autorizado por el administrador del dispositivo";
        message "Esta entrando  un dispositivo de la Universidad Nacional Autonoma de
Mexico";
        user lab {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$84J5Maes$cni5Hrazbd/IEHr/50oY30"; ## SECRET-DATA
            }
        }
        user labredes1 {
            full-name Laboratorio;
            uid 1314;
            class super-user;
            authentication {
                encrypted-password "$1$6WilUfEr$otPMaqdb/kGX/R3u4j/Oj."; ## SECRET-DATA
            }
        }
    }
    services {
```

```
        ftp;
        ssh {
            root-login deny;
        }
        telnet;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 192.168.0.126/32;
            }
        }
    }
    se-1/0/0 {
        serial-options {
            clocking-mode dce;
            clock-rate 2.048mhz;
        }
        unit 0 {
            family inet {
                address 192.168.0.253/32;
            }
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 192.168.0.158/32;
            }
        }
    }
```

```
    fxp0 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
        }
    }
}
protocols {
    rip {
        group rip-group {
            export rip-routes;
            neighbor se-1/0/0.0;
        }
    }
}
policy-options {
    policy-statement rip-routes {
        term 1 {
            from protocol [ direct rip ];
            then accept;
        }
    }
}
```

Router Sucursal B

```
system {
    host-name Sucursal B;
    domain-name UNAM.COM.MX;
    root-authentication {
        encrypted-password "$1$PbFwTLxc$JfKDrp77YRwliipTf2BvT."; ## SECRET-DATA
        ssh-dsa "ssh-dss
AAAAB3NzaC1kc3MAAACBAMQrfP2bZyBXJ6PC7XXZ+MzErI8JI6jah5L4/O8BsfP2hC7EvRfNoX7
MqbrtCX/9gUH9gChVuBCB+ERULMdgRvM5uGhC/gs4UX+4dBbfBgKYYwgmisM8EoT25m7qI8
ybpl2YZvHNznvO8h7kr4kpYuQEpKvgsTdH/Jle4Uqnjv7DAAAAFQDZaqA6QAgbW3O/zveaLCI
Dj6p0dwAAAIB1iL+krWrXiD8NPpY+w4dWXEqaV3bnobzPC4eyxQKBUCOr80Q5YBIWXVBHx9eI
wBWZwj0SF4hLKHznExnLerVsMuTMA846RbQmSz62vM6kGM13HFonWeQvWia0TDr78+rOEgWF
2KHBSIxL51lmIDW8GqI9hJfD/Dr/NKP97w3L0wAAAIEAr3FkWU8XbYytQYEKxsIN9P1UQ1ERXB3G
40YwqFO484SlyKyYCfaz+yNsaAJu2C8UebDIR3GieyNcOAKf3inCG8jQwjLvZskuZwrvlsz/xtcxSo
Ah9axJcdUfSJYMW/g+mD26JK1Cliw5rwp2nH9kUrJxeI7IReDp4egNkM4i15o=
configurator@server1.he"; ## SECRET-DATA
    }
    name-server {
        192.168.200.35;
```

```
    }
    login {
        announcement "Esta entrando al modo de configuracion del router, todo cambio debe ser autorizado por el administrador del dispositivo";
        message "Esta entrando a un dispositivo proiedad de la Universidad Nacional Autonoma de Mexico";
        user lab {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$84J5Maes$cni5Hrazbd/IEHr/50oY30"; ## SECRET-DATA
            }
        }
    }
    services {
        ftp;
        ssh {
            root-login deny;
        }
        telnet;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 192.168.0.190/32;
            }
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 192.168.0.206/32;
```

```
            }
        }
    }
    se-1/0/0 {
        unit 0 {
            family inet {
                address 192.168.0.254/32;
            }
        }
    }
    fxp0 {
        description "MGMT INTERFACE - DO NOT DELETE";
        unit 0 {
            family inet {
                address 10.210.14.132/27;
            }
        }
    }
}
protocols {
    rip {
        group rip-group2 {
            export rip-group2;
            neighbor se-1/0/0.0;
        }
    }
}
policy-options {
    policy-statement rip-group2 {
        term 1 {
            from protocol [ direct rip ];
            then accept;
        }
    }
}
```

ANEXO B

Laboratorio 6.2 Configuración servidor Radius

Se debe de descargar el software Freeradius en la versión freeradius-1.1.X.tar.gz, el cual se obtinE del siguiente Link:

http://freeradius.org/getting.html

Para configurar e instalar el software se requieren de 3 comandos:

./configure
make
make install

Después de haber ejecutados los comandos se tendrá instalado el servidor RADIUS, el cual se encuentra instalado en la siguiente ruta:

/etc/raddb/

1- Configuración de freeradius

Se deben que modificar 4 ficheros, los cuales son:

- **radiusd.conf**
- **users**
- **clients.conf**
- **eap.conf** ,

Dichos archivos están ubicados en el directorio:

/etc/raddb/

- **Cambios en el fichero radiusd.conf:**

En este archivo se debe que encontrar la siguiente línea

"**#with_ntdomain_hack = no**"

Se debe de modificarla y descomentarla, quedando de la siguiente manera:

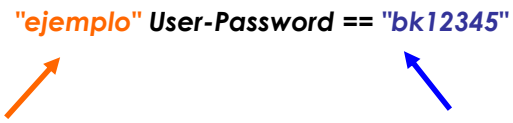
"**with_ntdomain_hack =yes**"

Dentro de radius.conf la oración aparece dos veces, por lo cual es necesario que en ambas se lleve a cabo esta modificación.

- **En el fichero users**

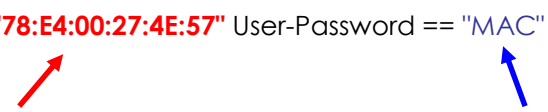
En freeradius existen muchas maneras de autenticar, ya sea mediante de certificados, por bases de datos, entre otras. Sin embargo una de las formas más efectivas y sencillas es escribir los usuarios y passwords directamente en este archivo.

La forma en la que se da de alta cada usuario es de la siguiente manera:



Donde ejemplo **es el usuario** a autenticar y bk12345 **es la contraseña.**

Si es una dirección MAC se realiza de esta forma:



Donde el usuario es la dirección MAC a autenticar y MAC **es la contraseña.**

(Importante: Las comillas se incluyen para diferenciar el nombre de usuario y contraseña, no se acepta dentro del password utilizar "como carácter ya que marca error). **En este archivo es donde se darán de alta, baja o cambios de usuarios**

- **En el archivo clients.conf:**

En este apartado es donde se establecen los puntos de acceso que serán los que tienen comunicación con el servidor RADIUS, en él se establece la dirección IP del dispositivo, y una shared secret que será con la que entre ellos se comunicará.

Es importante que sea la misma para que no exista ningún problema y que se lleve a cabo la autenticación mediante el servidor.

La sintaxis es la siguiente:

client 192.168.50.134

{

secret = misecreto

shortname = radiusceefa

}

- **En el archivo eap.conf:**

Importante: El método de autenticación que fue utilizado debe ser idéntico que en la configuración del Router Inalámbrico o Access Point.

De este fichero modificamos un par de cosas para que pueda autenticar introduciendo un usuario y una contraseña, quedando de la siguiente manera:

```
tls {
        private_key_password = whatever
        private_key_file = ${raddbdir}/certs/cert-srv.pem
        # If Private key & Certificate are located in
        # the same file, then private_key_file &
        # certificate_file must contain the same file
        # name.
        certificate_file = ${raddbdir}/certs/cert-srv.pem
        # Trusted Root CA list
        CA_file = ${raddbdir}/certs/demoCA/cacert.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
        #
        # This can never exceed the size of a RADIUS
        # packet (4096 bytes), and is preferably half
        # that, to accomodate other attributes in
        # RADIUS packet. On most APs the MAX packet
        # length is configured between 1500 - 1600
        # In these cases, fragment size should be
        # 1024 or less.
        #
        fragment_size = 1024
        # include_length is a flag which is
        # by default set to yes If set to
        # yes, Total Length of the message is
        # included in EVERY packet we send.
        # If set to no, Total Length of the
        # message is included ONLY in the
        # First packet of a fragment series.
        #
        include_length = yes
        # Check the Certificate Revocation List
        #
        # 1) Copy CA certificates and CRLs to same directory.
        # 2) Execute 'c_rehash <CA certs&CRLs Directory>'.
        # 'c_rehash' is OpenSSL's command.
        # 3) Add 'CA_path=<CA certs&CRLs directory>'
        # to radiusd.conf's tls section.
        # 4) uncomment the line below.
        # 5) Restart radiusd
        # check_crl = yes
        #
        # If check_cert_cn is set, the value will
        # be xlat'ed and checked against the CN
        # in the client certificate. If the values
        # do not match, the certificate verification
```

```
# will fail rejecting the user.
#
# check_cert_cn = %{User-Name}
        }
```

Como se observa se ha quitado en algunas líneas las #, las cuales se encuentran resaltadas de color azul, se debe validar que estas líneas quedaron tal y como se muestra para establecer una comunicación exitosa.

Se tiene el **peap**, el cual tiene que quedar de la siguiente manera:

```
peap {
# The tunneled EAP session needs a default
# EAP type which is separate from the one for
# the non-tunneled EAP module. Inside of the
# PEAP tunnel, we recommend using MS-CHAPv2,
# as that is the default type supported by
# Windows clients.
default_eap_type = mschapv2
}
```

Llegados a este punto se cuenta con el servidor freeradius configurado, los clientes creados (las direcciones de los Access Point que pedirán la autenticación) y los usuarios.

Antes de probar y conectarlo, se realiza un test para validar que el usuario y contraseña es aceptado, con ello se asegura que la comunicación entre los dispositivos fue establecida.

El comando para realizar el test es el siguiente

radtest ejemplo bk12345 localhost 1812 testing123

Teniendo la siguiente pantalla que lo comprueba.

Para iniciar el RADIUS se utiliza el siguiente comando: **radiusd –X**

Si marca que el servidor está utilizando otro servicio RADIUS realizamos lo siguiente:

Escribir en líneas de comando: /etc/init.d/radiusd stop y ahora radiusd-X debe mostrar la imagen que se observa en la siguiente figura.

```
linux-radius:/etc # radiusd -X
Starting - reading configuration files ...
reread_config:  reading radiusd.conf
Config:   including file: /etc/raddb/proxy.conf
Config:   including file: /etc/raddb/clients.conf
Config:   including file: /etc/raddb/snmp.conf
```

GLOSARIO DE TÉRMINOS

Término	Descripción
3DES	**(Tripe DES)** Algoritmo de cifrado.
AC	**(Alternating Current)** Corriente Alterna.
ACL	**(Access Control List)** Lista mantenida por un Router de Cisco para controlar el acceso desde o hacia un ruteador para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interface, en particular del ruteador).
Ad-Hoc	Es una red formada por dispositivos de conexión inalámbricos que se conectan por periodos de duración corta. Estos dispositivos se pueden comunicar sin necesidad de ningún AP o infraestructura existente.
AES	**(Advanced Encryption Standard)** Sucesor del Data Encryption Standard (DES). Es uno de los algoritmos más populares utilizados en criptografía simétrica. AES tiene un tamaño de bloque fijo de 128 bits aunque las claves de cifrado pueden ser de 128, 192 y 256 bits. Puede ser implementado tanto en hardware como en software.
AH	**(Authentication Header)** Encabezado de autenticación.
Anycast	Es una forma de direccionamiento en la que la información es enrutada al mejor destino desde el punto de vista de la topología de la red.
AP	**(Access Point)** Transmisor-receptor inalámbrico conectado a una red fija, que permite accede a dicha red desde sistemas o dispositivos equipados con una tecnología inalámbrica. También se utiliza como repetidor para ampliar el alcance de una red inalámbrica.
Apache	Es un servidor Web HTTP de código abierto, para la creación de páginas y servicios Web.
ATM	**(Asynchronous Transfer Mode)** Tecnología para la transmisión conmutada de voz, datos y video. Esta tecnología permite tener conexiones dedicadas de alta velocidad entre un número teóricamente ilimitado de usuarios de la red y también hacia los servidores. Como sistema de comunicación se utiliza en la RSI de banda ancha y también en redes SMDS. ATM también puede ser utilizado en LANs, en forma de emulaciones ATM-LAN.
BGP	**(Border Gateway Protocol)** Es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos definido en el RFC 1163.

BGP4	**(Border Gateway Protocol version 4)** Es la versión 4 del protocolo BGP.
Broadcast	Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.
BWA	**(Broadband Wireless Access)** Acceso de Banda Ancha Inalámbrico, comprende a las tecnologías que proporcionan a los dispositivos un acceso inalámbrico de alta velocidad a las redes de datos.
CDMA	**(Code Division Multiple Access)** es una técnica de acceso múltiple, se refiere a la técnica que permite que varios usuarios puedan acceder a un medio de comunicación y es una función de la capa de enlace de datos del modelo OSI.
Cell Relay	Tecnología de red basada en el uso de celdas o paquetes pequeños y de tamaño fijo. Como las celdas tienen longitud fija, se pueden procesar y conmutar en hardware a altas velocidades.
CIDR	**(Classless Inter-Domain Routing)** Es un estándar de red para la interpretación de direcciones IP. CIDR facilita el encaminamiento al permitir agrupar bloques de direcciones en una sola entrada de la tabla de rutas.
Classfull	Es una arquitectura de direccionamiento de red utilizado en Internet, el método divide el espacio de direcciones de protocolos de Internet versión 4 en cinco clases (A, B, C, D y E).
CLNP	**(Connectionless Network Layer Protoco)** Protocolo utilizado por OSI para transportar datos e indicación de errores en el nivel de red. CLNP es similar a IP y no proporciona detección de errores en la transmisión de datos, delega en el nivel transporte esta función.
CSMA/CD	**(Carrier Sense Multiple Acces/Collision Detect)** Acceso múltiple con escucha de portadora y detección de colisiones. El CSMA/CD es un protocolo de acceso al medio compartido, de tal modo que su uso está especialmente extendido en redes Ethernet donde es empleado para mejorar sus prestaciones. En CSMA/CD, los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión.
DAS	**(Direct Attached Storage)** Almacenamiento dedicado a un servidor particular, normalmente localizado dentro o cerca del servidor adjunto.
DCE	**(Distributed Computing Environment)** Dispositivo usado para convertir los datos del usuario de DTE en una forma aceptable para la instalación del servicio WAN.
DDR	**(Dial On Demand Routing)** Técnica por la que un Router puede iniciar y finalizar automáticamente conexiones a través de una red de conmutación de circuitos.

DES	**(Data Encryption Standard)** Algoritmo de cifrado.
Default Route	**(Ruta por defecto)** Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas por las cuales el próximo salto no está explícitamente mencionado en la tabla de enrutamiento.
DHCP	**(Dynamic Host Configuration Protocol)** Protocolo de configuración dinámica de servidores, protocolo de red, que permite a los nodos obtener los parámetros de configuración de red automáticamente.
Dial-Up	Conexión mediante llamada de marcado, típica de la red telefónica conmutada.
Dirección MAC	Identificador de 48 bits que corresponde de manera única a una tarjeta o a un dispositivo de red.
DLP	**(Data Loss Prevention)** Solución para proteger la información confidencial y crítica de usuarios finales no autorizados.
DNS	**(Domain Name Server)** Sistema de directorios utilizado comúnmente en Internet o publicaciones corporativas, a partir de un nombre se encuentra su dirección IP.
DQDB	**(Distributed Queue Dual Bus)** Mecanismo de control de acceso al medio empleado por las redes metropolitanas normalizadas.
EIGRP	**(Enhanced Interior Gateway Routing Protocol)** Protocolo de enrutamiento propietario de Cisco, utiliza la técnica vector de distancia, mejora al IGRP en cuanto a la detección de bucles mediante el algoritmo dual, permite métricas más complejas que el número de saltos.
ESP	**(Encapsulating Security Payload)** Encabezado de Carga de Seguridad de encapsulamiento, uno de los encabezados de cifrado para IPSec.
Ethernet	Tecnología de redes de computadoras de área local basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y las formas de tramas de nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD.
EUI-64	Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.
FDDI	**(Fiber Distributed Data Interface)** Estándar de LAN definida por el ANSI X3T9.5, que especifica una red de transmisión de token de 100 Mbps que utiliza cable de fibra óptica, con distancia de trasmisión de hasta 2 kilómetros. FDDI es una arquitectura de anillo doble para brindar redundancia.

Fibra óptica	Fibra basada en el vidrio, que sustituye a los cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a una gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda de luz generada por un láser.
Firewall	Dispositivo que se coloca comúnmente entre una red local e Internet y cuyo objetivo es asegurar que toda la comunicación entre los usuarios de dicha red e Internet se realice conforme a las normas de seguridad de la organización que la instala.
Frame	(Trama) Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidas en la unidad.
Frame Relay	Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25 el protocolo para el cual se considera por lo general un reemplazo.
FTP	**(File Transfer Protocol)** Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente/servidor. El servicio FTP es ofrecido por la capa de aplicación del modelo OSI, normalmente utiliza los puertos de red 20 y 21.
Gartner	Gartner proporciona el análisis de investigación y el consejo para profesionales de las TIC (tecnologías de la información y la comunicación), empresas de tecnología y la comunidad de la inversión en varios formatos: reuniones informativas, servicios de pares en red (peer networking service) y programas de socios diseñados explícitamente para CEOs y otros directores ejecutivos. Gartner utiliza para presentar sus análisis los conocidos como Cuadrantes Mágicos.
Gateway	Es un punto de red que actúa como la compuerta hacia otra red u otro tipo de red, puede tener funciones adicionales como servidor de acceso seguro a la red, servidor de registro para terminales troncales, convertidos análogo-digital a IP y controlador de flujo de tráfico entre segmentos de red.
Gbps	**(Gigabytes per second)** Medida de velocidad de transferencia.
GSM	**(Gruop Special Mobile)** Es el sistema global para las comunicaciones móviles, es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital.
HA	**(High Availability)** Alta Disponibilidad, es un concepto asociado con la redundancia y resistencia a fallos de los diferentes servicios y recursos que puede ser activo-activo o activo-pasivo.

HTML	**(HyperText Markup Language)** Hace referencia al lenguaje de marcado para la elaboración de páginas web.
HTTP	**(Hypertext Transfer Protocol)** HTTP es un protocolo de transferencia de hipertexto que se usa en la Web, fue desarrollado por las instituciones internacionales W3C y IETF y se usa en todo tipo de transacciones a través de Internet. El HTTP facilita la definición de la sintaxis y semántica que utilizan los distintos softwares web para interactuar entre sí.
HTTPS	**(Hypertext Transfer Protocol Secure)** Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.
IaaS	**(Infrastructure as a Service)** Modelo de distribución de infraestructura de computación como un servicio, normalmente mediante una plataforma de virtualización.
IDS	**(Intrusion Detecction Service)** Sistema que detecta y alerta las intrusiones suscitadas en un sistema o una red.
IEEE	**(Institute of Electrical and Electronics Engineers)** Es una asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.
IETF	**(Internet Engineering Task Force)** Grupo de trabajo dependiente de la IAB, el cual se dedica al estudio de aspectos técnicos de Internet.
IGP	**(Interior Gateway Protocol)** Protocolo de pasarela interno, hace referencia a los protocolos usados dentro de un sistema autónomo.
IGRP	**(Interior Gateway Routing Protocol)** Protocolo de encaminamiento desarrollado por Cisco, utiliza la técnica de vector de distancia.
IKE	**(Internet Key Exchange)** Es un protocolo que define el método de intercambio de claves sobre IP en una primera fase de negociación segura.
IMAP	**(Internet Message Access Protocol)** Protocolo de acceso a mensajes de Internet), es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet.
Internet	Conjunto de usuarios, aplicaciones y computadoras unidos a nivel mundial a través de redes TCP/IP.
IP	**(Internet Protocol)** Protocolo de capa 3, es el protocolo de mayor uso e implementación en las redes existentes, usualmente se utiliza referirse a una dirección IP que es una etiqueta numérica que identifica, de manera lógica a una interfaz de un dispositivo.
IPS	**(Intrusion Prevention System**) Herramienta reactiva la cual alerta a los administradores ante la detección de un posible intruso.

IPSec	**(Internet Protocol Security)** Es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red para trabajar con IPv4 e IPv6 de modo transparente o modo túnel, este soporta una gran variedad de encriptaciones y autenticaciones.
IPv4	**(Internet Protocol Versión 4)**
IPv6	**(Internet Protocol Versión 6)**
IT	**(Information Technology)** Tecnología de la información.
ISDN	**(Integrated Services Digital Network)** Estándar de la ITU para trasmisión de voz y datos en canales separados.
IS-IS	**(Intermediate System to Intermediate System)** Protocolo de enrutamiento jerárquico de estado de enlace OSI basado en el enrutamiento DECnet Fase V, en el que los IS (ruteadores) intercambian información de enrutamiento con base en una métrica única para determinar la topología de la red.
ISO	**(International Standard Organization)** La Organización Internacional de Estándares, es una organización no gubernamental encargada de producir normas internacionales con la finalidad de facilitar el intercambio de información y el comercio.
ISP	**(Internet Service Provider)** Proveedor de Servicios de Internet.
Kb	**(Kilobit)** Equivalente a 1024 bits.
KB	**(KiloBytes)** Equivalente a 1024 bytes.
Kbps	**(Kilobytes per second)** Unidad de velocidad de transferencia equivalente a 1024 bytes.
LAN	**(Local Area Network)**
MAC	**(Media Access Control)** Control de Acceso al Medio, identificador de 8 bits o 6 bloques hexadecimales que teóricamente corresponde de forma única a un dispositivo de red Ethernet.
MAN	**(Metropolitan Area Network)**
MD5	**(Message Digest version 5)** Algoritmo de autenticación.
MDA	**(Mail Delivery Agent)** Almacena el correo electrónico mientras espera a que los usuarios acepten.
MPLS	**(Multi Protocol Label Switching)** Conmutación Multiprotocolo Mediante Etiquetas, mecanismo de transporte de datos estándar creado por la IETF. Opera entre las capas de enlace de datos y la capa de red del modelo OSI.

MTA	**(Message Transfer Agent)** Se encarga del envío de mensajes de correo electrónico entre maquinas que usan el protocolo SMTP.
MTU	**(Maximum Transmission Unit)** Cantidad máxima de bytes transmitidos por un paquete de red capa 2, en el caso de redes Ethernet el MTU es de 1500.
MUA	**(Mail User Agent)** Programa que permite al usuario leer y escribir mensajes de correo electrónico.
Multicast	Proceso mediante el cual se envía información a múltiples destinos a la vez.
NAS	**(Network Attached Storage)** Es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con computadores personales o servidores clientes a través de una red.
NAT	**(Network Address Translation)** Técnica usada por un dispositivo capa 3 del modelo OSI, generalmente utilizado para permitir la conexión de varias terminales con IPs privadas hacia Internet.
NGFW	**(Next Generation Firewall)** Firewall de Siguiente Generación que basa su funcionamiento en la capa de aplicación del modelo OSI.
NIC	**(Network Interface Card)** Tarjeta de red.
NOC	**(Network Oparations Center)** Sitios desde los cuales se efectúa el control de las redes de datos
ODVC	**(Open DataBase Connectivity)** Proporciona una interfaz para tener acceso a una base de datos SQL heterogenia
OSI	**(Open System Interconnection)** El modelo de Interconexión de Sistema Abierto fue propuesto por el ISO, describiendo como deberán conectarse los distintos equipos de cómputo y redes para interactuar entre sí.
OSPF	**(Open Shortest Path First)** Protocolo de encaminamiento interior sucesor de RIP.
PaaS	**(Platform as a Service)** Modelo en el que se ofrece todo lo necesario para soportar el ciclo de vida completo de implementación y puesta en marcha de aplicaciones y servicios Web completamente disponibles en la Internet.
PLCP	**(Physical Layer Convergence Protocol)** Protocolo de nivel físico que adapta las facilidades de transmisión para manejar las funciones de DQDB.
PMD	**(Physical Layer Medium Dependent)** En redes de área local es el subnivel inferior del medio físico encargado de la transmisión sobre el medio de comunicación.

POP	**(Post Office Protocol)** Cliente de correo electrónico diseñado para ingresar a servidores de correo desde equipos no conectados permanente a la red.
POP3	**(Post Office Protocol versión 3)** Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor. POP3 es la versión más reciente y más utilizada definida en el RFC 1725, la cual tiene tres estados de proceso para controlar la conexión entre el servidor de correo y el cliente de correo electrónico POP3: el estado de autenticación, el estado de transacción y el estado de actualización.
Proxy	Es un equipo que actúa como intermediario entre los equipos de una red de área local e Internet. Generalmente el servidor proxy se utiliza para la Web.
RADIUS	**(Remote Authentication Dial In User Service)** Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
RFC	**(Request For Comments)** Son una serie de notas sobre Internet que comenzaron a publicarse en 1969, cada una de ellas es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.
RIP	**(Routing Information Protocol)** Protocolo interior de encaminamiento.
RIPv2	**(Routing Information Protocol version 2)** Protocolo interior de encaminamiento versión 2.
Router	Dispositivo de red que encamina datagramas, basándose en la dirección de red incluida en la cabecera de éstos y en el algoritmo correspondiente al protocolo de enrutamiento que emplee.
SA	**(Security Associations)** Asociaciones de Seguridad de IPSec.
SaaS	**(Software as a Service)** Modelo de distribución de software donde una empresa sirve el mantenimiento, soporte y operación que usará el cliente durante el tiempo que haya contratado el servicio.
SFTP	**(Secure File Transfer Protocol)** Es un protocolo de transferencia de archivos que utiliza SSH para asegurar los comandos y los datos que se transfiere entre el cliente y el servidor, lo que evita que usuarios no autorizados tengan acceso a ellos.
SMTP	**(Simple Mail Transfer Protocol)** Protocolo estándar de Internet para la transferencia de correo electrónico entre sistemas.
SNMP	**(Simple Network Management Protocol)** Protocolo convencional que facilita la administración de trabajo entre redes al utilizar agentes para almacenar y recuperar información directiva de los diversos productos de los vendedores.

SOC	**(Security Operations Center)**
Spyware	Software que se instala sin el consentimiento del usuario e intercepta información o toma control parcial de la interacción entre el usuario y la computadora. Envía información a otra computadora para su uso ilegal.
SSH	**(Secure Shell)** Protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor.
SSL	**(Secure Socket Layer)** Protocolo de capa de conexión segura, proporciona autenticación y privacidad de la información entre los extremos de una conexión a través de Internet mediante el uso de algoritmos de cifrado.
Switch	Dispositivo que tiene como objetivo principal unificar redes entre sí, sin la necesidad de examinar a fondo las tramas enviadas y recibidas, debido a que sólo examina la dirección MAC de destino.
Syslog	Es un protocolo que permite a un dispositivo enviar mensajes de notificación a través de una red IP para que sean almacenados en otro dispositivo o servidor colector.
TCP	**(Transmisión Control Protocol)** Protocolo de transporte orientado a conexión, utilizado en Internet para establecer comunicaciones confiables.
TCP/IP	**(Tranmission Control Protocol/ Internet Protocol)** Conjunto de protocolos que rigen el intercambio de información secuencial, diseñado por el departamento de Defensa de Estados Unidos, para enlazar computadoras diferentes a través de distintos tipos de redes. Desde entonces, se ha convertido en una forma común para equipos y aplicaciones comerciales. Es el protocolo con el que trabajan las redes actuales de comunicación.
TDM	Es el tipo de multiplexación más utilizado en la actualidad, especialmente en los sistemas de transmisión digitales. En ella, el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).
TDMA	**(Time Division Multiple Access)** Es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión
Telnet	Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).

TI/E1	Una conexión T1 es un paquete compuesto por 24 canales de multiplexado por división de tiempo (TDM) de 64 kbps (DS0) a través de circuito de cobre de cuatro hilos. Esto crea un ancho de banda total de 1.544 Mbps.
Token Ring	Es una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo. Token Ring se recoge en el estándar IEEE 802.5
UDP	**(User Datagram Protocol)** Protocolo de Datagrama a nivel de Usuario, es un protocolo de nivel de transporte basado en el intercambio de datagramas a través de la red sin necesidad de que se haya establecido con anterioridad una conexión.
UMTS	**(Universal Mobile Telecommunications System)** Es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM
Unicast	Es el envío de información desde un único emisor a un único receptor.
URL	**(Uniform Resource Locator)** Sirve para nombrar recursos en Internet. Este nombre tiene un formato estándar y tiene como propósito asignar una dirección única a cada uno de los recursos disponibles en Internet,
VLAN	**(Virtual Local Area Network)** Es una red de área local que agrupa un conjunto de equipos de manera lógica.
VLSM	**(Variable Length Subnet Mask)** Método de direccionamiento utilizado para segmentar redes.
VoIP	**(Voice Over IP)** Denominación genérica de las técnicas que permiten la transmisión de voz sobre redes IP.
VPN	**(Virtual Private Network)** Red Privada Virtual, permite al tráfico IP viajar de manera segura sobre una red TCP/IP, encriptando todo el tráfico de una red a otra. Una VPN utiliza tecnología de tunneling para cifrar toda la información a nivel de IP.
WAN	**(Wide Area Network)** Conexión de varias computadoras en un área de gran extensión, normalmente mediante circuitos de datos digitales.
WEB 2.0	El termino Web 2.0 fue acuñado por O´Relly Media en 2004 para referirse a una segunda generación de Web basada en comunicaciones de usuarios y una gama especial de servicios, como las redes sociales, los blogs o los wikis, que fomentan la colaboración y el intercambio de información entre usuarios.
Wi-Fi	**(Wireless Fidelity)** Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11. Se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet. Wi-Fi es una marca de la Wi-Fi

	Alliance, la organización comercial que prueba y certifica que los equipos cumplen los estándares IEE 802.11x.
WiMAX	**(Worldwide Interoperability for Microwave Access)** Es la marca que certifica que un producto está conforme a los estándares de acceso inalámbrico IEEE 802.16
WLAN	**(Wireless Local Area Network)** Es una red de área local inalámbrica.
WWAN	**(Wireless Wide Area Network)** Es una red de computadores que abarca un área geográfica relativamente extensa
WWW	**(World Wide Web)** Servicio que ofrece capacidades multimedia uniendo diferentes recursos de Internet.
X.25	Estándar UIT-T que define la manera en la que las conexiones entre DTE y DCE se mantienen para el acceso a la terminar remota y las comunicaciones en computadoras en las redes de datos públicas.