

Taller de Mantenimiento III (Entrega Final)

Autor: DvS
Docente: Sergio Silva

Personas que colaboraron en la realización de este documento:

Sebastián Bermúdez. 3° IE
Brandon Larrosa. 3° IE
Ezequiel Moreira. 3° IE
Sergio Maine, 3° IE
Brahian Puschiassis. 3° IE

Febrero de 2014

Índice

1. Introducción.....	5
2. Marco teórico.....	6
3. Parte del Anexo.....	8
3.1 Planificación del direccionamiento IP.....	8
3.2 Características de los switch.....	9
3.3 Características de los router.....	10
3.3.1 Conectividad.....	11
3.3.2 Funciones de seguridad.....	12
3.4 Terminales.....	13
3.5 RACK 42u.....	16
4. Parte del proyecto.....	17
4.1 Plano del Instituto con Diagrama de Red.....	18
5. Servidor.....	19
5.1 Características del servidor.....	20
5.2 Elección del servidor.....	21
5.3 Controlador de red.....	21
6. Configuración de los equipos.....	22
6.1. Switch.....	22
6.2. Switch 2.....	23
6.3. Firewall.....	24
6.4. Router.....	25
6.5. ACL.....	26
7.0. DHCP.....	31
7.1. Funcionamiento.....	27
7.2. Modos.....	27
7.3. Conculsi3n.....	28

8. VPN.....	28
8.1 Tipos de VPN's.....	29
8.2 Requerimientos para la implementación de una VPN... ..	30
8.3 Herramientas de una VPN.....	30
8.4 Tipos de conexión de las VPN's.....	31
8.5 Conclusión.....	31
 9. VOIP.....	 32
9.1 ¿Qué es la VOIP?.....	32
9.2 Conceptos de VOIP.....	32
9.3 Elementos de la voz sobre IP.....	33
9.4 Características de la voz sobre IP.....	33
9.5 Como funciona la voz sobre IP.....	34
9.6 Elementos de una red VOIP.....	34
9.7 Conexión de la comunicación IP.....	35
9.7.1 Conexión de voz sobre IP usando IP.....	35
9.7.2 Conexiones entre centrales.....	36
9.7.3 Conexiones a Internet.....	36
9.8 Como se usa la voz sobre IP.....	37
9.9 Ventajas de la VOIP.....	38
9.10 Desventajas de la VOIP.....	38
9.11 Configuración VOIP.....	39
9.12 Hardware a utilizar.....	41
 10. Access-List.....	 42
 11. Cableado estructurado.....	 47
11.1 Definición.....	47
11.2 Cableado estructurado a utilizar.....	48

12. Software de Monitoreo.....	49
12.1 Requerimientos.....	49
12.2 Licenciamiento y soporte.....	50
13 Anexos.....	51
14. Bibliografía.....	69
15. Hoja Testigo.....	70

Introducción:

Este proyecto consiste en la elaboración de una red con el fin de comunicar distintas zonas dentro del instituto para así poder ver información necesaria para cada alumno como lo son sus notas de exámenes u finales, a su vez permite una mejor forma de gestionar la información de dichas reuniones cuando se presentan en el año, una mayor comodidad para ver la información sin necesidad de hacer fila en adscripción; una mejor forma de ingresar los datos en las reuniones de manera organizada y fácil; estas cosas son las que busca como finalidad el proyecto además de tener seguridad en todos sus aspectos, en el servidor por ejemplo no va a poder acceder cualquiera y está todo estructurado como para que cada usuario cumpla específicamente su rol.

Dicho proyecto es para instalar una red paralela a la actual, de esa forma evitamos un alto nivel de tráfico y cumplimos la finalidad específica que va a tener la red sin necesidad de que tráfico con otros fines estén circulando por la misma.

Marco teórico:

HSRP:

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Es un protocolo muy similar a VRRP, que no es propietario. Es por ello que CISCO reclama que VRRP viola una serie de patentes que le pertenecen.

Fail-over:

La IP fail-over puede pasarse de un servidor a otro en unos segundos. Su alojamiento en una IP fail-over funciona así sin interrupción y permite solucionar problemas hardware, sobrecarga de sus máquinas y todo tipo de problemas de infraestructura.

Firewall:

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, es decir podemos filtrar que se conecta o no a nuestra red, de esa forma garantiza mayor seguridad a la misma además de manejabilidad, es decir al poder filtrar lo que se quiere podemos seguir usando la red para trabajar así como bloquear conexiones no deseadas.

Backup:

Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

Switch:

Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

Router:

También conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

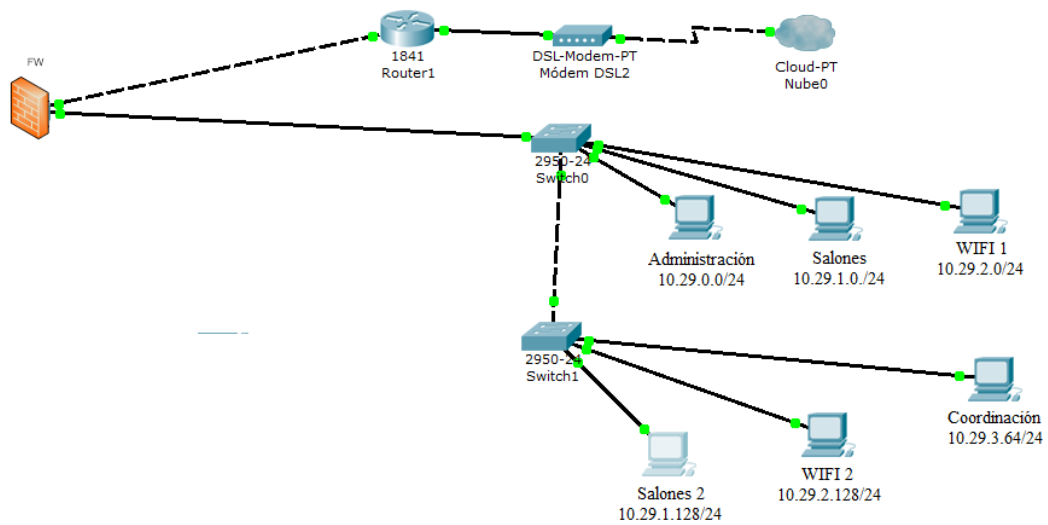
Servidor:

Es un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes.

Telefonía IP:

La Telefonía IP es una tecnología que permite integrar en una misma red - basada en protocolo IP - las comunicaciones de voz y datos. Muchas veces se utiliza el término de redes convergentes o convergencia IP, aludiendo a un concepto un poco más amplio de integración en la misma red de todas las comunicaciones (voz, datos, video, etc.).

3.0. Parte del Anexo



3.1. Planificación del direccionamiento IP:

Nombre	Dirección	Máscara de red	Primer host	Ultimo host	Broadcast
Administración	10.29.0.64	255.255.255.192	10.29.0.65	10.29.0.126	10.29.0.127
Salones	10.29.1.64	255.255.255.192	10.29.1.65	10.29.1.126	10.29.1.127
WI fi 1	10.29.2.64	255.255.255.192	10.29.2.65	10.29.2.126	10.29.2.127
Salones 2	10.29.1.128	255.255.255.192	10.29.1.129	10.29.1.190	10.29.1.191
WI fi 2	10.29.2.128	255.255.255.192	10.29.2.129	10.29.2.190	10.29.2.191
Coordinación	10.29.3.64	255.255.255.192	10.29.3.65	10.29.3.126	10.29.3.127

Para esta parte utilizaremos 2 switch de 24 bocas, 1 router, 1 firewall y servicio ADSL para conectarnos a internet.

3.2. Características de los switch:

Cisco SG200-26P:

Elegimos el switch de 24 bocas rj45 marca cisco modelo sg200-26p para el proyecto ya que es un switch reconocido que cumple con los requerimientos para desarrollar la red, con fluidez suficiente y resto para una futura expansión.

Los crecimiento de las necesidades de una red son incesantes, esta pequeña diferencia podría salvarnos de generar una gran re-inversión en un plan de expansión del proyecto a un leve costo.

Debido a esto y que cumple con lo solicitado, que soporte Vlan, fibra óptica y gigaehternet, el cisco sg200-26p es el switch es el elegido.



3.3. Características de los router:

Cisco 892:

Elegimos este router porque la serie Cisco 890 cumple con los requisitos de pequeñas sucursales empresariales y proveedores de servicios gestionados. Tiene un gran rendimiento, cuenta con posibilidades de seguridad avanzada, y en el ámbito inalámbrico cuenta con antenas dipolo omnidireccional y certificados 802.11n Draft v2.0 de WIFI y selección automática de velocidad para 802.11a/g/n. También cuenta con un soporte de hasta 14 (Vlans cifrados y no cifrados), gigabit ethernet, 8 bocas RJ45, y protocolo HSRP entre otras cualidades.



3.3.1. Conectividad

- Protocolo de Información de Enrutamiento versiones 1 y 2 (RIPv1 y RIPv2)
- Encapsulación de enrutamiento genérico (GRE) y multipunto GRE (mGRE)
- Cisco Express Forwarding
- Estándar 802.1d Spanning Tree Protocol
- Capa 2 Tunneling Protocol (L2TP)
- Layer 2 Tunneling Protocol Version 3 (L2TPv3)
- Traducción de direcciones de red (NAT)
- Servidor de Protocolo de configuración dinámica de host (DHCP), relé y cliente
- Sistema de Nombres de Dominio (DNS)
- Proxy DNS
- DNS Spoofing
- Listas de control de acceso (ACL)
- IPv4 e IPv6 Multicast
- Ruta más corta primero Abierto (OSPF)
- Border Gateway Protocol (BGP)
- Performance Routing (PdR)
- Interior Gateway Routing Protocol mejorado (EIGRP)
- Desvío de ruta virtual (VRF) Lite
- Next Hop Resolution Protocol (NHRP)
- Detección de Reenvío Bidireccional (BFD)
- Protocolo de comunicación de caché Web (WCCP)

3.3.2. Funciones de seguridad:

- SSLVPN para el acceso remoto seguro
- DES acelerado por hardware, 3DES, AES 128, AES 192 y AES 256
- Soporte de clave pública-infraestructura (PKI)
- Cincuenta túneles IPsec
- Cisco Easy VPN cliente y servidor
- Traducción de direcciones de transparencia de red (NAT)
- DMVPN
- Túnel-menos Grupo cifrada Transporte VPN
- IPsec stateful failover
- IPsec VRF-aware
- IPsec con IPv6
- La tecnología de control adaptativo
- Protocolo de Iniciación de Sesión (SIP) de puerta de enlace de capa de aplicación
- Cisco IOS Firewall:
 - Firewall Política Zone-Based
 - Inspección de estado VRF-aware firewall enrutamiento
- Cortafuegos transparente • inspección Stateful
- Inspección de aplicaciones avanzadas y control
- Secure HTTP (HTTPS), FTP y Telnet Proxy de autenticación
- Seguridad de puertos dinámicos y estáticos
- Firewall stateful failover
- Firewall VRF-aware
- Cisco ScanSafe Conector
- Cisco IOS Software negro y las listas blancas
- Control de amenazas integrado:
 - IPS
- Plano de Control Policial
- Flexible Packet Matching
- Protección de la fundación Red

3.4. Terminales

HP Compaq Pro 6300 Microtower PC



Especificaciones resumidas:

Procesador: i3 Sandy Bridge 3.3GHz

Memoria RAM: 4gb ddr3

Almacenamiento: 1 x HDD 500gb

DVD±RW (±R DL) / DVD-RAM

Conectividad: Gigabit LAN

Especificaciones detalladas:

General	
	1
Compatibilidad	PC
Fabricante	Hewlett-Packard
Gama de productos	HP Compaq
Kits nacionales	América Latina
Localización	Español
Marca	HP
Modelo	6300 Pro
Almacenamiento óptico	
Tipo	DVD SUPERMULTI
Carcasa	
Diseño del fabricante	Diseño pequeño
Factor de forma	De sobremesa
Conexión de redes	
Protocolo de interconexión de datos	Ethernet , Fast Ethernet , Gigabit Ethernet
Dimensiones y peso	
Altura	10 cm
Anchura	33.8 cm
Peso	7.6 kg

Disco duro	
Clase de interfaz	Serial ATA
Tipo	HDD
Tipo de interfaz	Serial ATA-600
Diverso	
Color de producto	Negro
Memoria caché	
Por tamaño de procesador	3 MB
Tamaño instalado	3 MB
Memoria RAM	
Tamaño instalado	4 GB
Tamaño máximo soportado	32 GB
Tecnología	DDR3 SDRAM
Procesador	
Cantidad instalada	1
Cantidad máxima soportada	1
Capacidad de actualización	Actualizable
Fabricante	Intel
Generación	3
Número de núcleos	Dual-Core
Tipo	Core i3
Velocidad reloj	3.3 GHz
Salida de vídeo	
Compatible con HDCP	Sí
Procesador gráfico	Intel HD Graphics
Sistema	
Capacidad del disco duro	500 GB

Periféricos:

Monitor: AOC e2050Sn - Monitor LED - 20"(1600 x 900,200 cd/m2,600:1,20000000:1 (dinámico),5 ms,VGA,negro)



Teclado: Klip Xtreme KKS-050S - Teclado – USB (Español, negro azabache)



Mouse: Klip Xtreme KMO-104 (Cableado, USB)



Todo el hardware recomendado tiene soporte técnico y son de distribuidores de confianza, además de que cumplen con todo lo necesario para la realización del proyecto (cumplen con todas las características pedidas).

3.5. RACK 42u:

Características:

- Paneles laterales con cerradura y de fácil ensamblaje
- Puerta trasera con Cerradura
- 4 Parantes
- 4 Ventiladores Internos
- 2 Bandejas fijas
- Cuadro de montaje
- Soporte Inferior
- Medidas: 600x1100 o 600x800

Diseño:

- Es de estructura robusta, con una puerta de visualización, buen sistema de ventilación, seguridad en las puertas y fácil ensamblaje

Ambientes:

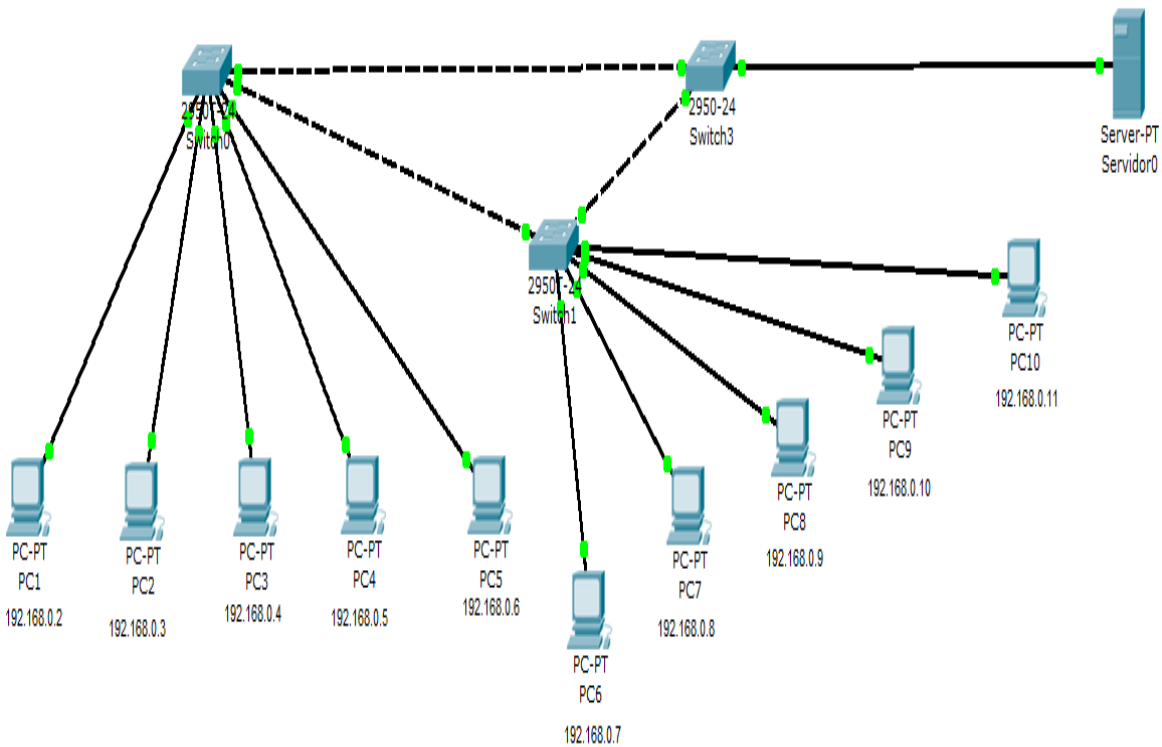
- Centros de datos
- Armario de cableado
- Oficina



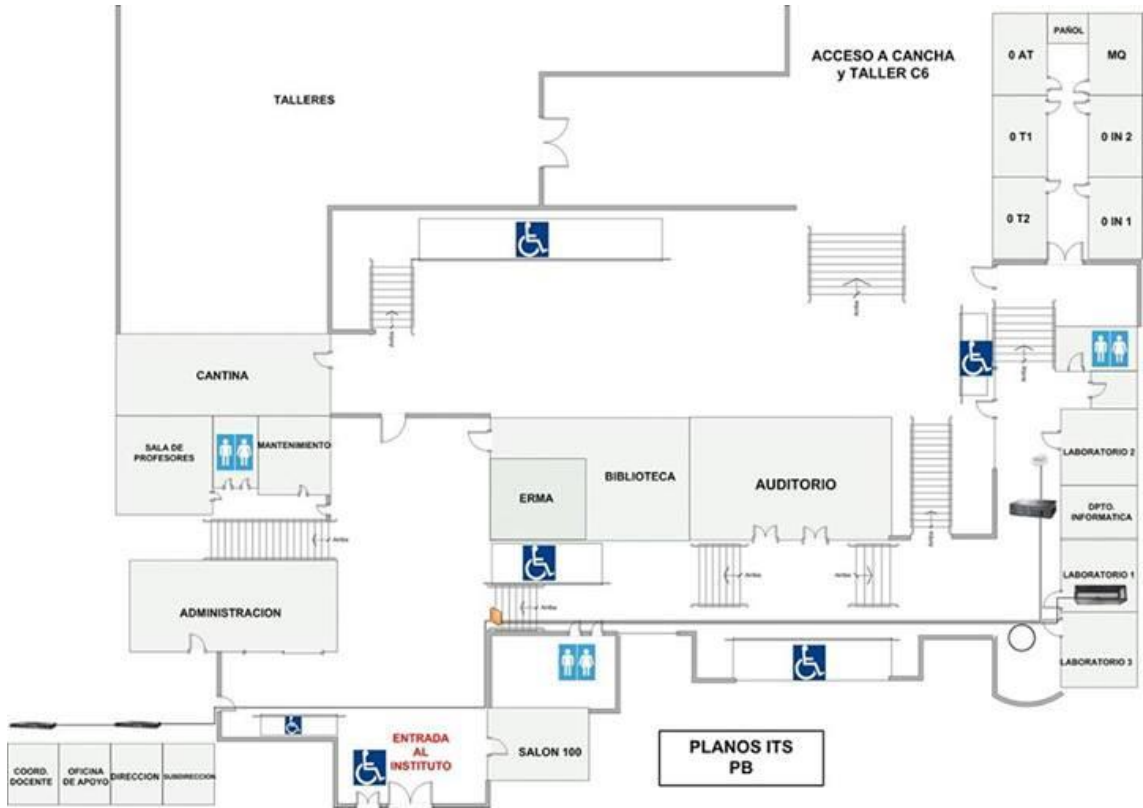
4.0. Parte del proyecto:

Para esta parte utilizaremos 2 switch de 24 bocas, 1 servidor, los switch son con las mismas características que los de Anexo.

PC	Dirección	Máscara de red	Broadcast
PC1	192.168.0.2	255.255.255.0	192.168.0.255
PC2	192.168.0.3	255.255.255.0	192.168.0.255
PC3	192.168.0.4	255.255.255.0	192.168.0.255
PC4	192.168.0.5	255.255.255.0	192.168.0.255
PC5	192.168.0.6	255.255.255.0	192.168.0.255
PC6	192.168.0.7	255.255.255.0	192.168.0.255
PC7	192.168.0.8	255.255.255.0	192.168.0.255
PC8	192.168.0.9	255.255.255.0	192.168.0.255
PC9	192.168.0.10	255.255.255.0	192.168.0.255
PC10	192.168.0.11	255.255.255.0	192.168.0.255



4.1. Plano del Instituto con Diagrama de Red:



5.1. Servidor

5.1. Características del servidor:

Blade de servidor HP ProLiant BL420c Gen8

Número de procesadores: 2 o 1

Núcleo de procesador disponible: 4 ó 6 u 8

Ranuras de memoria: 12 ranuras DIMM

Tipo de memoria: LRDIMM, RDIMM, LVDIMM y UDIMM DDR3

Ranuras de expansión: Dos PCIe 3.0 (1x8; 1x16); Máximo



5.2. Elección del servidor

Elegimos este servidor porque es el que más se adapta a las necesidades. Cuenta con una capacidad suficiente para ser utilizado en este proyecto y cuenta con la capacidad para ser mejorado en caso de que en un futuro la red sea ampliada. Estará configurado con un procesador de 4 núcleos, 2 módulos de 4gb de memoria RAM y discos duros independientes

5.3. Controlador de red:

Adaptador FlexFabric 554FLB de dos puertos y 10 Gb

-Especificaciones:

Controlador de red: Emulex BE3

Transfer rate: 10 Gbps

Protocolos admitidos: Canal de fibra y Ethernet

Velocidad de puerto: 10 Gb

Potencia disponible: 10 W (máximo)



Adaptador Ethernet 361FLB de 2 puertos y 1 Gb

-Especificaciones:

Controlador de red: Controlador Intel® Ethernet I350

Transfer rate: 2 Gb/seg.; Duplex completo por puerto

Protocolos admitidos: IEEE 802.1p, 802.1Q, 802.3, 802.3ad, y 802.3x, 1588, 802.1AS

Velocidad de puerto: 1 Gb/s Ethernet

Potencia disponible: 3 W (máximo)

Descripción de unidad: (2) SAS/SATA/SSD peq. Conexión caliente

Controlador de almacenamiento: (1) HP Dynamic Smart Array B320i; (1) Smart Array P220i / FBWC de 512MB

Formato (totalmente configurado): 8 (c3000); 16 (c7000)

Gestión de infraestructura: Motor de gestión iLO, Insight Control

Memoria, máximo: 384 GB



Los router, switch así como las terminales van a ser las mismas que utilizamos para la parte del anexo.

6.0. Configuración de los equipos:

6.1. Switch 1

```
Switch>enable
Switch#config t
Switch(config)#interface fastethernet 0/1
Switch(config-if)#description firewall
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch#config t
Switch(config)#interface fastethernet 0/2
Switch(config-if)#description switch
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name administracion
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name salones
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name wifi
Switch(config-vlan)#exit
Switch(config)#interface fastethernet 0/3
Switch(config-if)#description administracion
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/4
Switch(config-if)#description salones
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/5
Switch(config-if)#description wifi
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)switchport trunk allowed vlan 10
Switch(config-if)switchport trunk allowed vlan 20
Switch(config-if)switchport trunk allowed vlan 30
```

6.2. Switch 2

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#description switch
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name salones
Switch(config-vlan)#exit
Switch(config)#vlan 50
Switch(config-vlan)#name wifi2
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name coordinacion
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport trunk allowed vlan 40
Switch(config-if)#switchport trunk allowed vlan 50
Switch(config-if)#switchport trunk allowed vlan 60
```

6.3. Firewall (Router)

```
Router(config)#interface FastEthernet0/0
Router(config-if)#description switch
Router(config-if)#no ip address
Router(config-if)#exit
Router(config)#interface fastethernet 0/0.10
Router(config-subif)#description administracion
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 10.29.0.1 255.255.255.0
Router(config)#interface fastethernet 0/0.20
Router(config-subif)#
Router(config-subif)#description salones
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 10.29.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.30
Router(config-subif)#description wifi
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 10.29.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.40
Router(config-subif)#description salones
Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 10.29.4.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.50
Router(config-subif)#description wifi2
Router(config-subif)#encapsulation dot1q 50
Router(config-subif)#ip address 10.29.5.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.60
Router(config-subif)#description coordinacion
Router(config-subif)#encapsulation dot1q 60
Router(config-subif)#ip address 10.29.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#description router
Router(config-if)#ip address 10.20.20.1 255.255.255.252
Router(config-if)#exit
```


6.4. Router

```
Router(config-if)#interface FastEthernet0/1
Router(config-if)#description internet
Router(config-if)#ip address 200.40.200.9 255.255.255.250
Router(config-if)#ip address 200.40.200.9 255.255.255.252
Router(config)#interface FastEthernet0/0
Router(config-if)#description firewall
Router(config-if)#ip address 10.20.20.2 255.255.255.252
Router(config-if)#exit
```

6.5. ACL

ACL a implementar en el proyecto:

Red de Administracion

```
Router# configure terminal
```

```
Router (config)#Access-list 1 permit 10.29.0.64 0.0.0.63 any
```

```
Router (config)#exit
```

Red de Coordinacion

```
Router# configure terminal
```

```
Router (config)#Access-list 2 permit 10.29.3.64 0.0.0.63 any
```

```
Router (config)#exit
```

Red de Salones:

```
Router# configure terminal
```

```
Router (config)#Access-List 3 permit 10.29.1.64 0.0.0.63 10.29.1.128 0.0.0.63
```

```
Router (config)#Access-list 103 permit tftp 10.29.1.64 0.0.0.63 10.29.1.128 0.0.0.63 69
```

```
Router (config)#Access-List 4 deny 10.29.1.64 0.0.0.63 any
```

```
Router (config)#Access-list 101 deny tcp 10.29.1.64 0.0.0.63 any 80
```

```
Router (config)#Access-list 102 deny smtp 10.29.1.64 0.0.0.63 any 25
```

```
Router (config)#exit
```

Red de Salones 2:

```
Router# configure terminal
```

```
Router (config)#Access-List 5 permit 10.29.1.128 0.0.0.63 10.29.1.64 0.0.0.63
```

```
Router (config)#Access-list 106 permit tftp 10.29.1.128 0.0.0.63 10.29.1.64 0.0.0.63 69
```

```
Router (config)#Access-List 6 deny 10.29.1.128 0.0.0.63 any
```

```
Router (config)#Access-list 104 deny tcp 10.29.1.128 0.0.0.63 any 80
```

```
Router (config)#Access-list 105 deny smtp 10.29.1.128 0.0.0.63 any 25
```

```
Router (config)#exit
```

Red de WIFI:

```
Router# configure terminal
```

```
Router (config)#Access-List 7 permit 10.29.2.64 0.0.0.63 10.29.2.128 0.0.0.63
```

```
Router (config)#Access-List 6 deny 10.29.2.64 0.0.0.63 any
```

```
Router (config)#exit
```

Red de WIFI2:

```
Router# configure terminal
```

```
Router (config)#Access-List 7 permit 10.29.2.128 0.0.0.63 10.29.2.64 0.0.0.63
```

```
Router (config)#Access-List 6 deny 10.29.2.128 0.0.0.63 any
```

```
Router (config)#exit
```

7.0. DHCP

Es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet.

La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

7.1. Funcionamiento

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, Gateway, DNS, etc.

Un servidor DHSC (DHCP Server) es un equipo en una red que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones Broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional.

7.2. Modos

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

Asignación manual: El administrador configura manualmente las direcciones IP del cliente en el servidor DHCP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

Asignación automática: Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

Asignación dinámica: El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al cliente Server que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

7.3. Conclusión:

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de las direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

Sintaxis Comando DHCP:

```
Router# configure terminal  
Router (config)#ip dhcp pool nombre
```

```
Router (config)#network x.x.x.x
```

8.0 VPN

Es una red privada dentro de una red pública, la cual permite conectar diferentes sedes o sucursales, usuarios móviles y oficinas remotas entre sí. Es una estructura de red corporativa que utiliza sistemas de gestión y políticas de acceso que permiten al usuario trabajar como si estuviese conectado en su misma red local.

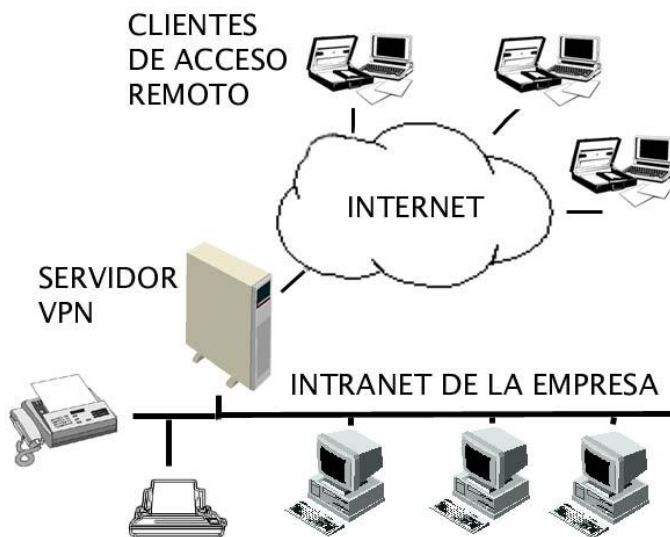
VPN funciona basándose en una tecnología llamada tunneling, la cual es una técnica que consiste en encapsular un protocolo de red sobre otro permitiendo así que los paquetes vayan encriptados de manera que los datos enviados sean ilegibles para extraños.

8.1. Tipos de VPN's

De acceso remoto: modelo más usado actualmente y como su nombre lo dice los usuarios o proveedores se conectan a la empresa desde sitios remotos (desde su casa, hotel, aviones, etc) usando internet como vínculo de conexión, una vez autenticados tienen un nivel de acceso muy similar al de la red local de la empresa.



Punto a Punto: se utiliza para conectar oficinas remotas con la sede central de la organización.



OverLan: es una variante del primer modelo expuesto pero en lugar de usar internet como medio de conexión se usa la misma LAN de la empresa y sirve para aislar zonas y servicios de la red interna.

8.2. Requerimientos para la implementación de una VPN

Identificación de Usuario: debe identificar la identidad de sus usuarios y restringir el acceso a los no autorizados.

Administración de claves: debe generar y renovar las claves de codificación para el cliente y el servidor.

Administración de Direcciones: debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos: los datos deben ser encriptados antes de su transmisión por la red para así evitar que usuarios no autorizados de la red los lean, esta operación puede realizarse a través de algoritmos de cifrado como DES o 3DES o mediante técnicas de encriptación como encriptación con clave secreta o encriptación de clave pública.

Soporte a Protocolos Múltiples: debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen en protocolo IP, el intercambio de paquetes de internet IPX, entre otros.

8.3. Herramientas de una VPN

- VPN Gateway
- Software
- Firewall
- Router Especial
- Dispositivos Hardware especiales que cuenten con software para proveer de capacidad a la VPN

8.4. Tipos de conexión de las VPN's

Conexión de acceso remoto: es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión router a router: la conexión es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentifica ante el router que realiza la llamada y también sirve para la intranet.

Conexión firewall a firewall: donde la conexión es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

8.5. Conclusión

Las VPN's actualmente representan una gran solución para las empresas gracias a todas las ventajas que proporciona este tipo de conexiones en cuanto a confiabilidad, seguridad e integridad de los datos, por otro lado reducen notablemente los costos de transferencia de datos de un lado a otro y son sencillas de usar, además facilita la comunicación entre usuarios en lugares distantes.

9.0. VOIP

9.1. ¿Qué es la VOIP?

La Telefonía IP es una tecnología que permite integrar en una misma red - basada en protocolo IP - las comunicaciones de voz y datos. Muchas veces se utiliza el término de redes convergentes o convergencia IP, aludiendo a un concepto un poco más amplio de integración en la misma red de todas las comunicaciones (voz, datos, video, etc.).

Esta tecnología hace ya muchos años que está en el mercado (desde finales de los 90) pero no ha sido hasta hace poco que se ha generalizado gracias, principalmente, a la mejora y estandarización de los sistemas de control de la calidad de la voz (QoS) y a la universalización del servicio Internet.

Cuando hablamos de un sistema de telefonía IP estamos hablando de un conjunto de elementos que debidamente integrados permiten suministrar un servicio de telefonía (basado en VoIP) a la empresa. Los elementos básicos que forman este sistema son: la centralita IP, el Gateway IP y los diferentes teléfonos IP.

Las principales ventajas de la telefonía IP son la simplificación de la infraestructura de comunicaciones en la empresa, la integración de las diferentes sedes y trabajadores móviles de la organización en un sistema unificado de telefonía - con gestión centralizada, llamadas internas gratuitas, plan de numeración integrado y optimización de las líneas de comunicación - la movilidad y el acceso a funcionalidades avanzadas (buzones de voz, IVR, ACD, CTI, etc.)

9.2. Conceptos de VOIP

La Voz sobre IP (VoIP, VoiceoverIP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos.

Es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, Gateways y teléfonos estándares.

9.3. Elementos de la voz sobre IP

Existen algunos modelos de Voz sobre IP, que está formado por tres principales elementos la cuales son:

El cliente. Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Cabe destacar que el elemento cliente se presenta en dos formas básicas: la primera es una suite de software corriendo en una PC que el usuario controla mediante una interface gráfica (GUI); y la segunda puede ser un cliente "virtual" que reside en el Gateway.

Servidores. El segundo elemento está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.

Gateways. El tercer elemento conforman los Gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La función principal de un Gateway es proveer las interfaces con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales. Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

9.4. Características de la voz sobre IP

Por su estructura el estándar proporciona las siguientes características:

Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

Proporciona el enlace a la red telefónica tradicional.

Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:

Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.

Es independiente del hardware utilizado.

Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

9.5. Como funciona la voz sobre IP

Antes de aclarar lo que es la funcionalidad de voz sobre ip, decimos que voz sobre ip, mandar una señal a un destino remoto también podía hacerse de manera digital: antes de enviar la señal se debía digitalizar con un ADC (análogo digital converter), transmitirla y en el extremo de destino transformarla de nuevo a formato análogo con un DAC (digital to analog converter).

VoIP (voz sobre Ip) funciona de esa manera, digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino.

Básicamente el proceso comienza con la señal análoga del teléfono que es digitalizada en señales PCM (pulse code modulación) por medio del codificador/decodificador de voz (codec).

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, FrameRelay, ATM o SONET. Hoy, las arquitecturas interoperables de voz sobre IP se basan en la especificación H.323 v2.

La especificación H.323 define Gateways (interfaces de telefonía con la red) y gatekeepers (componentes de conmutación inter oficina) y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet.

En la actualidad, se están proponiendo otras especificaciones en los consorcios industriales tales como SIP, SGCP e IPDC, las cuales ofrecen ampliaciones en lo que respecta al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.

9.6. Elementos de una red VOIP.

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audio conferencia múltiple. (MCU Voz).
- Servicios de Directorio.
- Elementos de una red VoIP (Voz sobre IP) las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior, si bien merece la pena recalcar algunas ideas.

9.7. Conexión de la comunicación IP

9.7.1 Conexión de voz sobre IP usando IP

En vez de elegir dos computadoras, y quiere conectar un número importante de computadoras, que quieren hablar entre sí sin tener que estar transmitiéndose los números de IP, y el que les está proveyendo el servicio quiere poder tener un registro de las comunicaciones establecidas, se utiliza un Server SIP (que vendría a ser el equivalente a un Gatekeeper en H323). También se lo suele llamar ProxySIP o Router SIP.

Esto quiere decir que hay que tener un Server, por ejemplo cuando uno hace una llamada uno está enviando una señal al server indicando que quiere uno hablar con otra persona, y este le avisa a la otra persona que quiero hablar con él.

A partir de que se acepta la comunicación, se pasan algunos mensajes más a través del server utilizando SIP para negociar IPS, puestos, protocolo de compresión a utilizar.

Pero una vez que comienzo la comunicación el canal UDP ya no pasa por el server. Una vez terminada la conversación, se utiliza SIP para avisar que se terminó la conversación. Esta es una de las mejores cosas que tiene la telefonía IP, porque por un lado separa la señalización de la transmisión de voz, y por el otro lado la transmisión se hace peer to peer. Pero trae consigo que el server debe confiar en la buena fe de los clientes para saber cuándo una comunicación se terminó realmente.

Un cliente que tenga DHCP tiene que avisarle al server en qué IP está, para esto puede autenticarse contra él, utilizando un nombre de usuario y una clave. De manera que el server puede saber que un determinado usuario no está y poner un contestador, dar ocupado, etc.

Con este principio se puede hacer que un teléfono VOIP (Voz sobre IP) se enchufe en cualquier lugar del mundo donde haya banda ancha y siempre sigue siendo el mismo teléfono. Y de hecho este servicio existe y se vende. Por ejemplo, si a usted le dan una línea en Buenos Aires o en cualquier otro país, y usted quiere llevarse el teléfono VOIP (Voz sobre IP) a cualquier lugar del mundo, lo puede enchufar a un ADSL y puede hablar o lo pueden llamar como si usted estuviera en Buenos Aires.

De la misma manera que con las centrales telefónicas, puede haber varios servers que se comuniquen entre sí, y solamente van a intercambiar la parte correspondiente al protocolo SIP, la parte de RDP/UDP se hace directo entre los dos puntos que se están comunicando. La implementación de referencia del server SIP es Open Source.

Por otro lado, se puede hablar desde una computadora a teléfonos comunes, para esto se necesita un Gateway (GW) que haga la conversión de una tecnología a otra.

9.7.2 Conexiones entre centrales

La llamada que sale de nuestra central tiene que llegar hasta la central donde está la persona con la que queremos hablar. No hay doscientos millones de cables entre una y otra, sino que hay un enlace, el cual puede ser de diversos tipos. Este enlace se debe multiplexar para que todos los abonados de la central puedan hablar por teléfono. Esta multiplexación es la que hace una diferencia a la hora de la calidad del servicio para el usuario.

El sistema de multiplexación que utilizan las centrales telefónicas se llama TDM: Time División Multiplex. Consiste en dividir el stream de datos en partes iguales de 64k (llamadas time-slots), de manera que los datos correspondientes al primer abonado van en el primer time-slot, los correspondientes al segundo en el segundo, y así sucesivamente.

Suponiendo un enlace de 2 Mbps de ancho de banda, como se transmiten 64k, podría haber hasta 32 abonados hablando a la vez. Con esta multiplexación en tiempo se separan y luego vuelven a unir los streams de voz que van de una central a otra, de manera transparente para el que lo está utilizando.

Lo bueno de esta tecnología es que como se divide por un tiempo fijo, se puede garantizar el time-slot y saber que siempre lo que corresponde al primer abonado va en el primer time-slot y así. Una vez establecida la comunicación, sea de acá a una cuadra o de acá a China, está garantizado el ancho de banda necesario para poder hablar sin interrupciones.

Esto, en particular, es muy opuesto a lo que es IP, o cualquier enlace de paquetes en los que pueda haber colisiones, se pierdan paquetes, etc. Ya que en esos enlaces es muy difícil garantizar que la calidad inicial se mantenga a lo largo de toda la conversación, puede pasar que haya paquetes que lleguen antes que otros, que se sature la conexión y muchos otros factores que afectan a la calidad final del audio.

En definitiva, TDM es una de las diferencias esenciales entre la telefonía común y la de Voz sobre IP, permite tener una red predictiva y garantizar calidad.

9.7.3 Conexiones a internet

Sólo lo pueden usar aquellas personas que posean una conexión con Internet, tengan computadora con módem y una línea telefónica; algunos servicios no ofrecen la posibilidad de que el computador reciba una llamada, ni tampoco funcionan a través de un servidor Proxy. La conexión a Internet es la conexión con la que una computadora o red de ordenadores cuentan para conectarse a Internet, lo que les permite visualizar las páginas Web desde un navegador y acceder a otros servicios que ofrece esta red.

Hay compañías que ofrecen conexión a Internet, las que reciben el nombre de servidores Detalles con un poco de Historia

La red de telefonía mundial fue diseñada para reproducir con claridad voces humanas, para realizarlo utiliza un sistema que es capaz de transmitir señales entre 350Hz y 3400Hz. La conversión de estas señales análogas a digitales es llamada PCM ("Pulse CodeModulación").

9.8. Como se usa la voz sobre IP

Es importante conocer cómo se usa esta tecnología de VoIP (Voz sobre IP), básicamente hay que comprar un dispositivo que visualmente es una cajita negra que se conecta por un lado al aparato telefónico y por el otro a la PC (computadora), aunque también hay disponibles teléfonos IP. Por supuesto se necesita instalar un software para que dicho dispositivo funcione.

Este dispositivo casi siempre se vende en los mismos comercios que venden computadoras.

Hay dos posibilidades de conexión:

Una de las partes tiene VoIP (Voz sobre IP) y la otra no.

Ambas partes tienen VoIP (Voz sobre IP)

Si ambas partes tienen VoIP (Voz sobre IP) la llamada es totalmente gratuita, pues se llama de VoIP (Voz sobre IP) a VoIP (Voz sobre IP); sólo tiene que discar el número telefónico y nada más.

Si sólo quien llama tiene VoIP (Voz sobre IP), entonces hace uso de una tarjeta que se compra online (en línea).

La mencionada tarjeta no es una tarjeta de plástico o de cartón como las que se venden en los comercios, más bien es una tarjeta virtual que se compra y carga por Internet.

Uno de los proveedores de esta tarjeta prepaga es: Innosphere y para conocer más de ella cuya dirección electrónica es: http://www.innosphere.net/customer_center.html.

Es necesario aclarar que se puede instalar un VoIP (Voz sobre IP) aunque tenga una central telefónica y más de una línea de teléfono, pues se puede designar una línea para que trabaje directamente con el VoIP (Voz sobre IP), sin perjuicio de seguir utilizándola normalmente.

El VoIP (Voz sobre IP) es una buena alternativa para quien tiene oficinas en el exterior y hace llamadas de larga distancia diariamente o de mucha duración.

9.9. Ventajas de la VOIP

- Barata
- Realizar llamada a Cualquier parte del Mundo
- Identificación de llamadas.
- Servicio de llamadas en espera
- Servicio de transferencia de llamadas
- Repetir llamada
- Devolver llamada
- Llamada de 3 líneas (three-waycalling).
- Desviar la llamada a un teléfono particular
- Enviar la llamada directamente al correo de voz
- Dar a la llamada una señal de ocupado.
- Mostrar un mensaje de fuera de servicio

9.10. Desventajas de la VOIP

- Requiere Conexión de Banda Ancha
- Requiere Conexión Eléctrica a menos que sean inalámbricos
- Llamadas al 911: Estas también son un problema con un sistema de telefonía VOIP. Como se sabe, la telefonía ip utiliza direcciones IP para identificar un número telefónico determinado, el problema es que no existe forma de asociar una dirección ip a un área geográfica, como cada ubicación geográfica tiene un numero de emergencias en particular no es posible hacer una relación entre un número telefónico y su correspondiente sección en el 911. Para arreglar esto quizás en un futuro se podría incorporar información geográfica dentro de los paquetes de transmisión del VOIP. Dado que VOIP utiliza una conexión de red la calidad del servicio se ve afectado por la calidad de esta línea de datos, esto quiere decir que la calidad de una conexión
- VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la perdida de paquetes.
- Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas.
- VOIP es susceptible a virus, gusanos y hacking, a pesar de que esto es muy raro
- En los casos en que se utilice un softphone la calidad de la comunicación VOIP se puede ver afectada por la PC, digamos que estamos realizando una llamada y en un determinado momento se abre un programa que utiliza el 100% de la capacidad de nuestro CPU, en este caso critico la calidad de la comunicación VOIP se puede ver comprometida porque el procesador se encuentra trabajando a tiempo completo, por eso, es recomendable utilizar un buen equipo junto con su configuración voip.

9.11. Configuración VOIP

REQUISITOS NECESARIOS PARA USAR VoIP

1) Conexión ADSL (Con más de 100 Kbps debería funcionar, pero si tenemos 300 Kbps o más, mejor)

2) Un softphone o un teléfono IP.

Softphone: Software que permite establecer la comunicación como si de un teléfono se tratase usando protocolos de VoIP (Voice over IP). Skype es un ejemplo de softphone, pero tiene el grandísimo inconveniente de que solo puedes hablar con otros usuarios de skype, no con usuarios de todos los otros proveedores, que son multitud. La desventaja de los softphones en general es que tu interlocutor tiene que tener el programa corriendo en su ordenador, PPC, o smartphone para recibir la llamada.

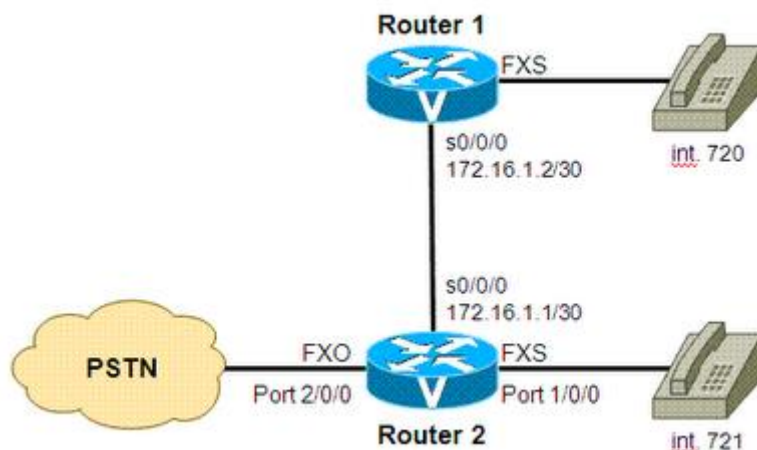
Hardphone o teléfono IP: Son teléfonos que conectados a nuestro router permiten hablar usando protocolos de VoIP (voice over IP). Tienen la gran ventaja de que funcionan como teléfonos normales, es decir, no necesitan que haya ningún ordenador funcionando, simplemente estarán conectados directamente al router y sonarán como un teléfono convencional cuando se reciba una llamada.

3) Una cuenta SIP obtenida de un proveedor de VoIP.

Ejemplo de Configuración de un router Cisco para soporte de VoIP.

Un router puede estar equipado con puertos FXO / FXS que permiten su operación como Gateway de voz con sistemas de telefonía tradicional, a la vez que realizan el transporte de tráfico de voz paquetizada sobre la red IP.

Para la configuración se utilizara el siguiente esquema de red:



Suponemos 2 routers Cisco conectados entre si a través de sus puertos seriales utilizando la subred 172.16.1.0/30. Router1 tiene conectado un teléfono analógico (interno 720) a través de un puerto FXS; el Router2 conecta a la red de telefonía pública utilizando un puerto FXO y da acceso al interno 721 a través de un puerto FXS.

Sintaxis de la configuración.

```
!  
interface Serial0/0/0  
ip address 172.16.1.1 255.255.255.252
```

```
dial-peer voice 1 voip  
destination-pattern 720  
session-target ipv4:172.16.1.2  
!
```

```
dial-peer voice 2 pots  
destination-pattern 721  
port 1/0/0  
!
```

```
dial-peer voice 3 pots  
destination-pattern 9  
port 2/0/0  
!
```

Cada número de interno definido requiere de un "destination-pattern" que define el ID que se recibe. Cuando se trata de una comunicación telefónica tradicional, a ese destination-pattern se asocia el puerto de voz correspondiente, es el caso por ejemplo del interno 721. Cuando se trata de destination-pattern cuyo tráfico debe encaminarse a través de la red IP se define la dirección IP de destino del dispositivo en el cual se encuentra conectado ese interno, como es el caso del interno 720.

9.12. Hardware a utilizar

En el caso de que se quiera implementar la Telefonía VOIP recomendamos el siguiente equipo:



Teléfono inalámbrico Yealink W52P

La capacidad de realizar hasta 4 llamadas paralelas a través de Internet hace del Yealink W52P una solución de comunicación verdaderamente excepcional.

Este producto incluye la estación base que permite conectar hasta 5 terminales Yealink W52P.

Características:

- Hasta 4 llamadas simultáneas
- Hasta 5 microteléfonos, hasta 5 cuentas de VoIP
- Sonido HD en llamadas VoIP
- Ahorro de energía con ECO DECT
- Sonido de alta definición en modo «manos libres»
- Gran pantalla en color de alta resolución
- Agenda con 150 entradas y grupos VIP
- 2 teclas programables, 6 teclas de función, 6 teclas de acceso directo
- Toma auricular 2,5mm
- Poe
- Auto-disposición a través de FTP / TFTP / HTTP / HTTPS
- Auto-disposición con PnP
- Alcance: 50 metros en interior, 300 metros en exterior
- Agenda Local para hasta 500 entradas (en la base)
- Agenda remoto

Precio : 94 Euros aprox 2.728 pesos Uruguayos

10.0. Access-List

Una **Lista de Control de Acceso** o **ACL** (del inglés, *Access Control List*) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Existen dos tipos de ACLs:

- ACL estándar, donde solo tenemos que especificar una dirección de origen; (1-99)
- ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.(100-199)
-

La ACL compraran las mascara con la widlcard si es un 0 revisa, si es un 1 no revisa

ACLs Estándar.

- Usan el rango de (1-99)
- Solo filtran la dirección IP de origen

ACL Extendidas

- Usan el rango de (100-199)
- Filtra la dirección IP de origen, protocolos y puertos/ aplicaciones

¿Cómo usar las wildcard?

Utilizamos las wildcard para comprobar las condiciones, Un bit de máscara wildcard 0 significa “comprobar el valor correspondiente”, Un bit de máscara wildcard 1 significa “No comprobar (ignorar) el valor del bit correspondiente.

Host = máscara comodín 0.0.0.0, utilizada para un host específico

Any = 0.0.0.0 255.255.255.255, utilizado para definir a cualquier host, red o subred

En el caso de permitir o denegar redes o subredes enteras se deben ignorar todos los host pertenecientes a dicha dirección de red o subred. Cualquier dirección de host será leída como dirección de red o subred.

Ejemplo:

Dirección IP	172	16	32	0
IP en binario	10101100	00010000	00100000	00000000
Máscara de red	11111111	11111111	11100000	00000000
Wildcard	00000000	00000000	00011111	11111111
Resultado	Se toman en cuenta los 8 bits	Se toman en cuenta los 8 bits	Se toman en cuenta los 3 primeros bits el resto no	No se toma en cuenta

Sintaxis de ACL:

Access-list n° deny/permit protocol origen destino puerto

Donde protocolo y puerto depende de si es Estándar o Extendida

Y en el caso de que sea Estándar deberemos usar mascara Wildcard en las Dirección IP's

Importante:

- Siempre al final de una lista de acceso está implícito el negar todo, aunque nunca aparece pero es: deny any.
- Las listas de acceso son secuencias de instrucciones que son chequeadas contra el paquete, una vez que se cumpla la condición toman una acción y se salen de la lista de acceso, es decir no se continua chequeando para comprobar que haya otra línea de la secuencia que también resulta cierta. Por lo tanto, es importante diseñar la ACL en la secuencia que nos interese más.
- No se puede insertar líneas en la secuencia de las ACLs, si nos equivocamos al crearla o queremos insertar una línea a la que existe, hay que borrar toda la ACL y volverla a crear. Solamente las listas con nombre permiten cambiar o eliminar instrucciones.
- Una ACL se aplica a la interfaz de entrada o de salida. Se pueden crear una ACL para la interfaz de salida y otra distinta para esa interfaz de entrada.

ejemplo access list:

standard

extended

Como eliminar las listas de acceso:

Desde el modo interfaz donde se aplico la lista:

Router(config-if)#no ip access-group[Nº de lista de acceso]

Desde el modo global elimine la ACL

router(config)#no access-list[Nº de lista de acceso]

Razones para uso de ACL:

- Limitar trafico de red
- Controlar el flujo
- Proporcionar nivel básico de Seguridad
- Se pueden aplicar a nivel individual o grupal

ACL a implementar en el proyecto:

Red de Administracion

Router# configure terminal

Router (config)#Access-list 1 permit 10.29.0.64 0.0.0.63 any

Router (config)#exit

Red de Coordinacion

Router# configure terminal

Router (config)#Access-list 2 permit 10.29.3.64 0.0.0.63 any

Router (config)#exit

Red de Salones:

Router# configure terminal

Router (config)#Access-List 3 permit 10.29.1.64 0.0.0.63 10.29.1.128 0.0.0.63

Router (config)#Access-list 103 permit tftp 10.29.1.64 0.0.0.63 10.29.1.128 0.0.0.63 69

Router (config)#Access-List 4 deny 10.29.1.64 0.0.0.63 any

Router (config)#Access-list 101 deny tcp 10.29.1.64 0.0.0.63 any 80

Router (config)#Access-list 102 deny smtp 10.29.1.64 0.0.0.63 any 25

Router (config)#exit

Red de Salones 2:

Router# configure terminal

Router (config)#Access-List 5 permit 10.29.1.128 0.0.0.63 10.29.1.64 0.0.0.63

Router (config)#Access-list 106 permit tftp 10.29.1.128 0.0.0.63 10.29.1.64 0.0.0.63 69

Router (config)#Access-List 6 deny 10.29.1.128 0.0.0.63 any

Router (config)#Access-list 104 deny tcp 10.29.1.128 0.0.0.63 any 80

Router (config)#Access-list 105 deny smtp 10.29.1.128 0.0.0.63 any 25

Router (config)#exit

Red de WIFI:

Router# configure terminal

Router (config)#Access-List 7 permit 10.29.2.64 0.0.0.63 10.29.2.128 0.0.0.63

Router (config)#Access-List 6 deny 10.29.2.64 0.0.0.63 any

Router (config)#exit

Red de WIFI2:

Router# configure terminal

Router (config)#Access-List 7 permit 10.29.2.128 0.0.0.63 10.29.2.64 0.0.0.63

Router (config)#Access-List 6 deny 10.29.2.128 0.0.0.63 any

Router (config)#exit

11.0. Cableado Estructurado

11.1 Definición

Es un sistema de cables, conectores y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio. La instalación y las características del sistema deben cumplir con ciertos estándares para formar parte de la condición de cableado estructurado.

Lo que permite el cableado estructurado es transportar dentro de un edificio las señales que emite un emisor hasta su correspondiente receptor. Se trata, por lo tanto, de una red física que puede combinar cables UTP, bloques de conexión y adaptadores, entre otros elementos.

Al soportar diversos dispositivos de telecomunicaciones, el cableado estructurado permite ser instalado o modificado sin necesidad de tener conocimiento previo sobre los productos que se utilizarán sobre él.

A la hora del tendido, hay que tener en cuenta la extensión del cableado, la segmentación del tráfico, la posible aparición de interferencias electromagnéticas y la eventual necesidad de instalar redes locales virtuales.

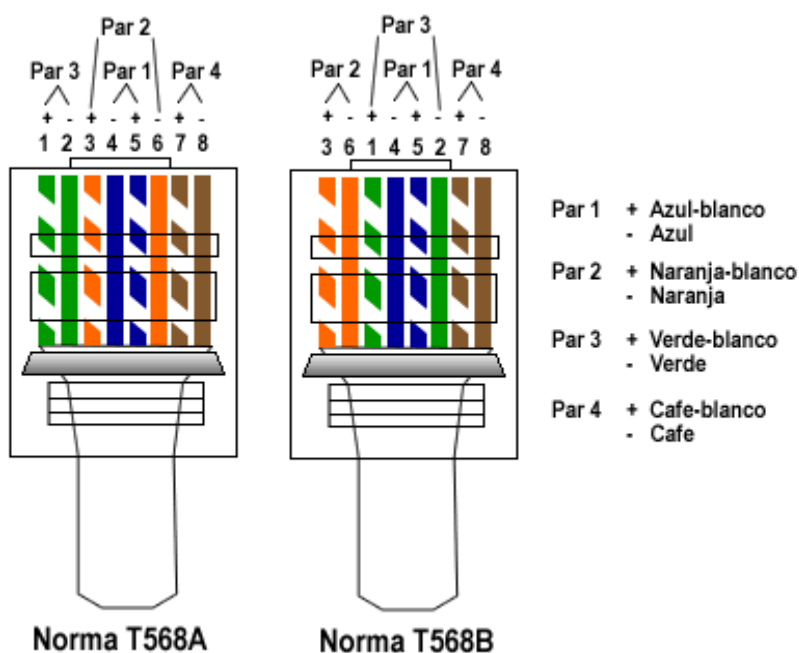
Entre los elementos principales del sistema de cableado estructural se encuentran el cable horizontal (que corre horizontalmente entre el suelo y el techo), el cable vertical, troncal o backbone (que interconecta diversos cuartos) y el cuarto de telecomunicaciones (con los equipos de telecomunicaciones).

11.2 Cableado estructurado a utilizar

Cable UTP

Para la implementación de la red hemos elegido el cable utp categoría 5E, en la cantidad 800m ya que si en un futuro la red necesitara una modificación se tendría cable para hacerlo.

En caso de comprar solamente el cable sin las fichas rj-45 ya puesta se tendrá que colocarla a parte, para esto se tendrá que utilizar según el uso del cable las normas T568a y T568b a continuación se muestra una imagen de la normas.



12.0 Software de Monitoreo

Para nuestra red hemos elegido utilizar Open NMS 1.10.4 como software de monitoreo, el cual se instalara en el servidor host.

Fue seleccionado dado que cuenta con:

- Un sistema de funcionamiento, que permite analizar de manera efectiva nuestra red.
- Realiza una minuciosa recolección de datos de tareas hechas en la red, recolectando todo dato que pase por los nodos de la red, sin hacer distinción del protocolo que utilicen, gracias a ello registra todo movimiento de datos.
- Permite realizar reportes digitales completos de cada dato para posteriormente evaluarlos y analizarlos en búsqueda de posibles errores, funcionamientos defectuosos o conexiones ilegales.
- No menos importante es la interfaz gráfica que facilita la labor de administrar una red.
- Además de posee la funcionalidad de notificaciones al administrador de la red mediante un correo electrónico.
- Detecta de forma automática los equipos y dispositivos conectados en una o más redes.

12.1. Requerimientos

- ➔ JDK.
- ➔ PostgreSQL.
- ➔ 256 MB de RAM

12.2 Licenciamiento y soporte

Open NMS es un software libre y de código abierto por lo que claramente la licencia es gratuita.

No obstante el soporte supera ampliamente las expectativas para un software libre dado que cuenta con un soporte muy completo. Cuenta con un grupo de recursos para brindar un soporte satisfactorio, ellos son:

- **Wikipedia:** El repositorio principal de OpenNMS se puede encontrar en la web, más exactamente en un sitio web orientado a la comunidad que permite a cualquier usuario registrado, añadir, mejorar y modificar las entradas obteniendo así un actualizado sitio donde consultar.
- **Listas de Discusión:** Para una experiencia más interactiva, están disponibles las listas de discusión. Hay una lista para los nuevos usuarios, una lista general y una lista para los desarrolladores.
- **JIRA:** es un sitio donde los usuarios pueden denunciar errores con el programa donde un grupo de desarrolladores solucionaran y notificaran la solución.
- **Libro OpenNMS:** Como última opción de soporte OpenNMS cuenta con un libro/tutorial el cual se podrá descargar gratuitamente desde www.amazon.com

Además del soporte que nos ofrece nosotros brindaremos un total de 20 horas comunitarias por mes, los días hábiles, durante 2 años de soporte incluidas en el precio final del sistema, teniendo en cuenta que si existiese la necesidad de un número mayor de horas, cada hora extra tendrá un costo de 40 dólares americanos.

Para poder instalar correctamente el (Open NMS), se deberá instalar, paquete JDK de java y el programa Postgre SQL, el cual nos brindara una basa de datos en nuestro sistema y será fundamental para la ejecución del Open NMS

13.0 Anexos

Anexo A

UPS – S.A.I

➤ ¿Qué es una UPS o un S.A.I

Un UPS es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida de energía eléctrica). UPS significa en inglés UninterruptiblePowerSupply.

Los UPS suelen conectarse a la alimentación de las computadoras, permitiendo usarlas varios minutos en el caso de que se produzca un corte eléctrico. Algunos UPS también ofrecen aplicaciones que se encargan de realizar ciertos procedimientos automáticamente para los casos en que el usuario no esté y se corte el suministro eléctrico.

➤ **Componentes típicos de los UPS:**

Rectificador: rectifica la corriente alterna de entrada, suministrando corriente continua para cargar la batería. Desde la batería se alimenta el inversor que nuevamente convierte la corriente en alterna. Cuando se descarga la batería, ésta se vuelve a cargar en un lapso de 8 a 10 horas, por este motivo la capacidad del cargador debe ser proporcional al tamaño de la batería necesaria.

Batería: se encarga de suministrar la energía en caso de interrupción de la corriente eléctrica. Su capacidad, que se mide en Amperes Hora, depende de su autonomía (cantidad de tiempo que puede proveer energía sin alimentación).

Inversor: transforma la corriente continua en corriente alterna, la cual alimenta los dispositivos conectados a la salida del UPS

Conmutador: (By-Pass) de dos posiciones, que permite conectar la salida con la entrada del UPS (By Pass) o con la salida del inversor.

En nuestro caso, el tipo de UPS que vamos a usar es Standby o también llamado smart.
El UPS usado en cuestión es el siguiente:

FORZA 1000-VA SL-IOI

Regulador Automático de Voltaje

660 Joules de protección contra sobretensión

- Sistema de alimentación ininterrumpida
- Protección de poder para equipo de casa u oficina
- Regulador de voltaje (AVR), regula subidas y bajadas de tensión
- 6 tomas de salida- supresor de picos, respaldo de batería, AVR, supresión de picos solamente
- Protección de teléfono, fax y módem (RJ-45)
- Puerto USB para comunicación con PC
- Indicador LED de carga y modo de batería
- Botón de encendido iluminado
- Largo tiempo de respaldo
- 660 Joules de protección
- Software de manejo de energía



Alimentación de energía:

- Permite el control y vigilancia de múltiples UPSs vía Lan e Internet
- Análisis gráfico de poder con interfaz amigable
- Apagado Seguro de sistema operativo y protección contra pérdida de datos durante falla eléctrica
- Notificaciones de Advertencia mediante alarma audible, mobile messenger y e-mail
- Apagado y encendido de UPS programable, prueba de batería, control de tomacorriente programable y alarma audible
- Protección de seguridad con Contraseña y administración de acceso remoto
- Soporta múltiples Sistemas Operativos: familia Windows, Linux, Mac OS X
- Soporta múltiples idiomas

ESPECIFICACIONES TÉCNICAS	
Capacidad	1000VA / 600W
Entrada:	Compatibilidad de voltaje de entrada: 220 VAC Margen de voltaje de entrada: 162 - 268 VAC Frecuencia: 45 - 55 HZ
Salida	Voltaje nominal de salida: 220 VAC Frecuencia de salida: 50Hz Onda de salida: Onda sensorial modificada
Batería	Tiempo y número de batería: 12V / 7.2AH x 2 PC Tiempo de respaldo (basado en consumo de 1 PC con monitor de 17"): 40 minutos Tiempo de recarga: 10 horas al 90% tras haberse agotado por completo.
Interface	Windows 98 / 2000 / XP / Vista, Mac OS, Linux.
Indicador	Modo CA: LED azul permanente Modo de batería: LED verde intermitente / LED azul, capacidad de batería (1ero-4to)
	Modo de falla: LED roja encendida
Alarma audible	Modo de batería / bajo voltaje de batería / sobrecarga / reemplazar la batería / falla
Protección	Protección total: Regulación de tensión de línea / Modo de batería
Características físicas (aprox.):	Dimensiones de la unidad: 392*145*205 mm Peso neto de la unidad: 9.8 kg

NOTA:

No se recomienda conectar la UPS a impresoras láser, estufas, aspiradoras cafeteras, etc.

Debido al gran consumo de energía y a la corta duración de reserva

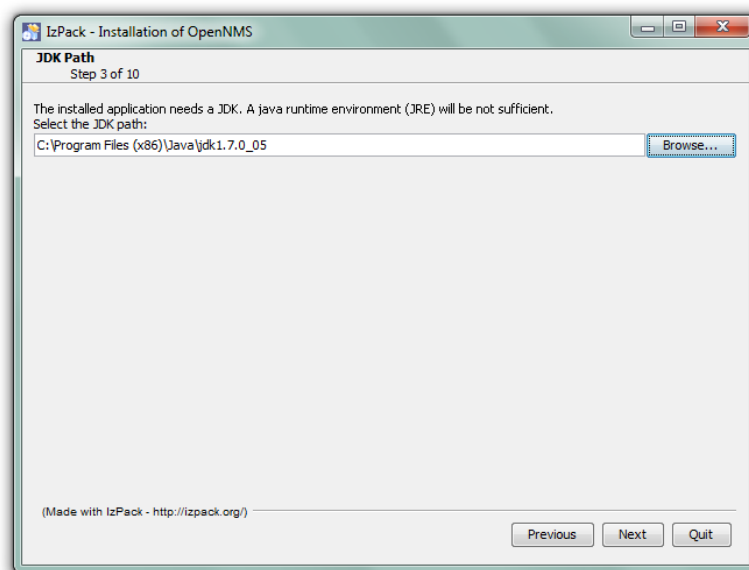
Para un óptimo funcionamiento y una vida máxima de las baterías, la sala donde se encuentre ubicado el SAI debe mantenerse como máximo a 25°C de temperatura.

Para garantizar una buena ventilación habría que evitar colocar las UPS contra alguna pared y obstruir su ventilación, por lo tanto verificar ubicación de las mismas.

Anexo B

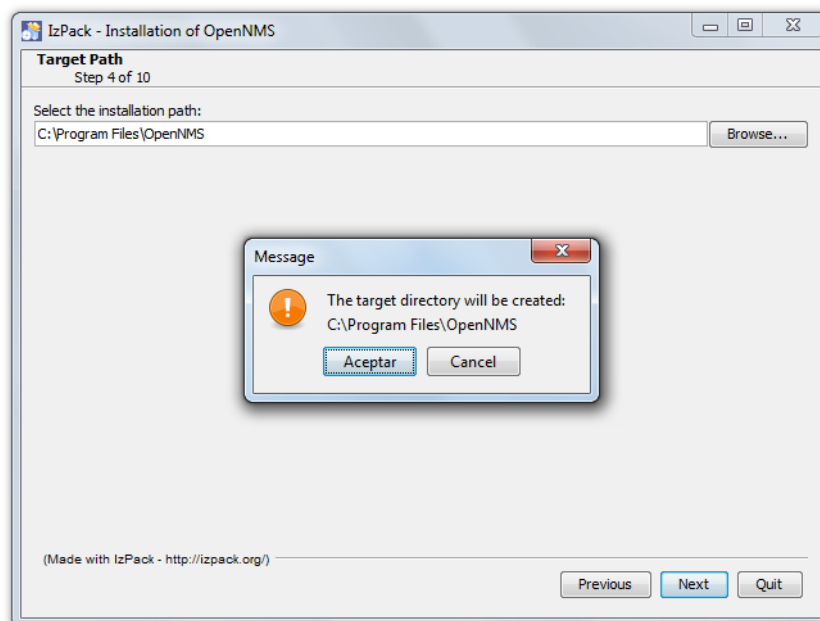
Instalación Open NMS

1. Una vez descargado el instalador de Open NMS versión 1.10.4 ejecutaremos el instalador dependiendo de si nuestro S.O es de 32 o 64 bits.
2. Una vez ya ejecutado el instalador nos aparecerá una imagen de bienvenida al instalador en la cual deberemos seleccionar el botón “Next”.
3. A continuación se muestra la licencia del producto siendo que deberemos seleccionar la opción “I accept the terms of this license agreement” y luego presionar nuevamente el botón “Next”.
4. El programa de instalación nos mostrará un cartel el cual nos pedirá que indiquemos la ubicación de instalación del kit “JDK” (sea de 32 o 62 bits dependiendo de nuestro S.O) de Java enviroment (JRE) siendo que este no es suficiente para continuar con nuestra instalación. Una vez aclarada dicha dirección presionaremos el botón “Next” para continuar con la instalación. La siguiente imagen ilustra la ubicación por defecto de dicho kit:

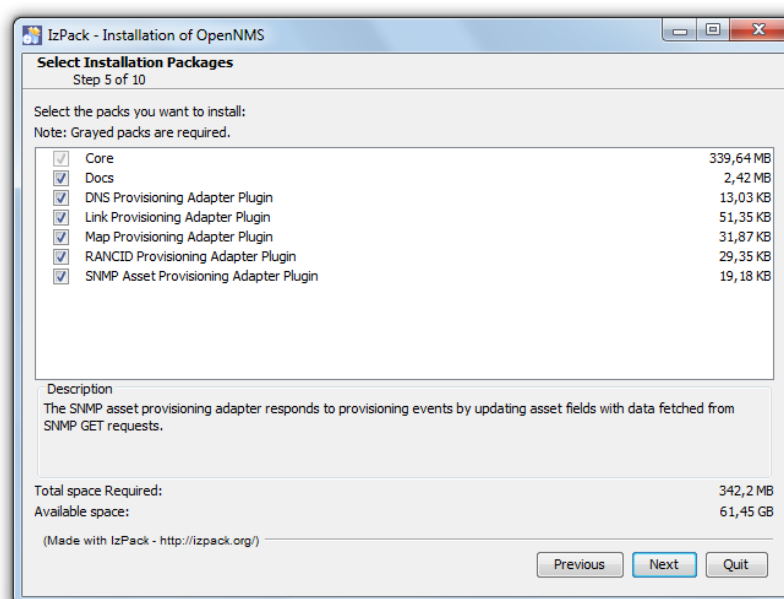


5. En la siguiente imagen se nos muestra el directorio donde se instalará “Open NMS” en nuestro sistema. Si deseáramos cambiar esta dirección deberemos aclararla presionando el botón “Browse...” y a continuación el botón “Next”.

6. Si el directorio no existe actualmente en la máquina, aparece un cartel indicando que “va a ser creado” en el cual presionaremos el botón “Aceptar”; de lo contrario (siendo que ya exista el directorio) se pasara directamente a la siguiente etapa de instalación. Esta imagen muestra el caso de que no existiese dicho directorio:



7. En la séptima etapa de instalación seleccionaremos la cantidad de paquetes a instalar en conjunto con Open NMS, cabe destacar que el paquete “Core” es el fundamental y es el que aparece marcado (permanentemente) en el instalador, por ultimo presionaremos el botón “Next” para continuar la instalación. A continuación mostramos una ilustración de la quinta etapa de instalación con todos sus paquetes seleccionados:



8. En esta pantalla se muestra las características de nuestra Base de Datos, de la misma se deberá ingresar la contraseña del nuevo usuario que creara el programa de instalación (“postgres” por defecto), es de saber que podemos cambiar cualquier dato que ya este dado previamente. La siguiente imagen ilustra los datos que se nos da por defecto:

IzPack - Installation of OpenNMS

User Data
Step 6 of 10

Configure Database

Database Host:	localhost
PostgreSQL Database Name:	opennms
Database Username (Administrator):	postgres
Database Password (Administrator):	
Database Username (Runtime):	opennms
Database Password (Runtime):	opennms

(Made with IzPack - <http://izpack.org/>)

Previous Next Quit

9. En la novena etapa de nuestra instalación se deberá ingresar el rango de IP en el cual Open NMS detectara nuestro dispositivos conectados a nuestra red, marcando la mínima en las casillas superiores y la máxima en la inferior; a continuación presionaremos el botón “Next” para iniciar la instalación. Estaimagenmuestra el rangopordefecto dado:

IzPack - Installation of OpenNMS

User Data
Step 7 of 10

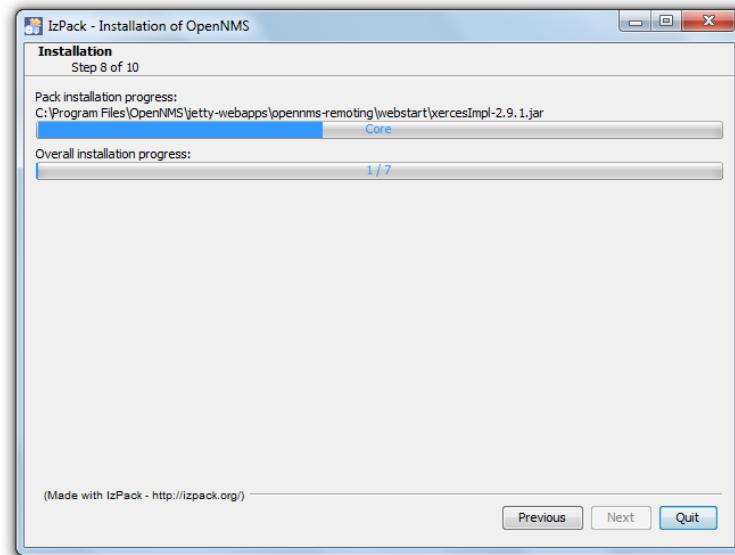
Configure Discovery Range

Start:	192	.	168	.	0	.	1
End:	192	.	168	.	0	.	254

(Made with IzPack - <http://izpack.org/>)

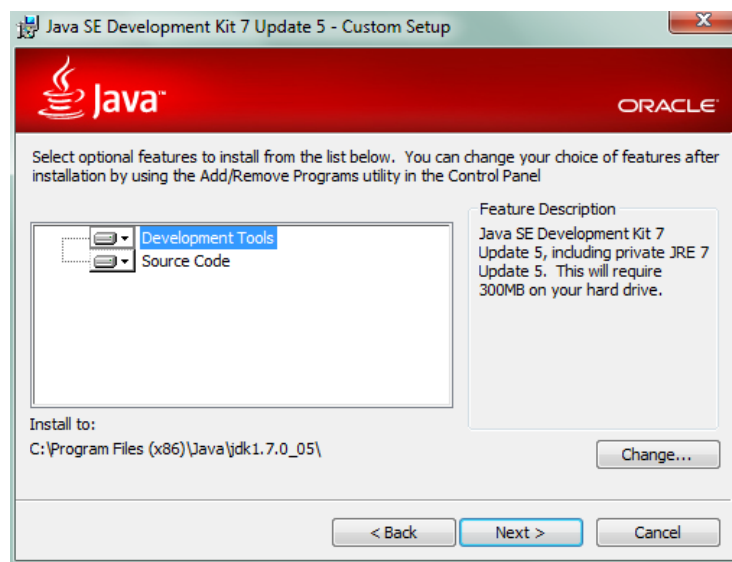
Previous Next Quit

10. En la decima etapa se inicia la instalación del programa, lo cual tiene una demora dependiente de cuantos paquetes se seleccionaron, al finalizar la carga deberemos presionar el botón “Next”. Esta imagen muestra la carga total de todos sus paquetes a instalar:



Instalación de JDK

1. Primero deberemos descargar el programa desde <http://www.oracle.com>, una vez descargado el programa (JDK – 7u5 para Windows) lo ejecutaremos y así iniciaremos su consecuente instalación.
2. En esta pantalla se nos muestra un mensaje de bienvenida a la instalación, en donde deberemos acceder al botón “Next”.
3. A continuación ingresaremos la ruta en donde se instalara JDK en nuestro sistema, siendo “C:\Archivos de programa\Java\jdk1.7.0_05\ “, en caso de querer modificar esta ruta deberemos presionar el botón “Change” e ingresando deseada ruta. Esta imagen muestra la dicha etapa de instalación con la ruta por defecto:

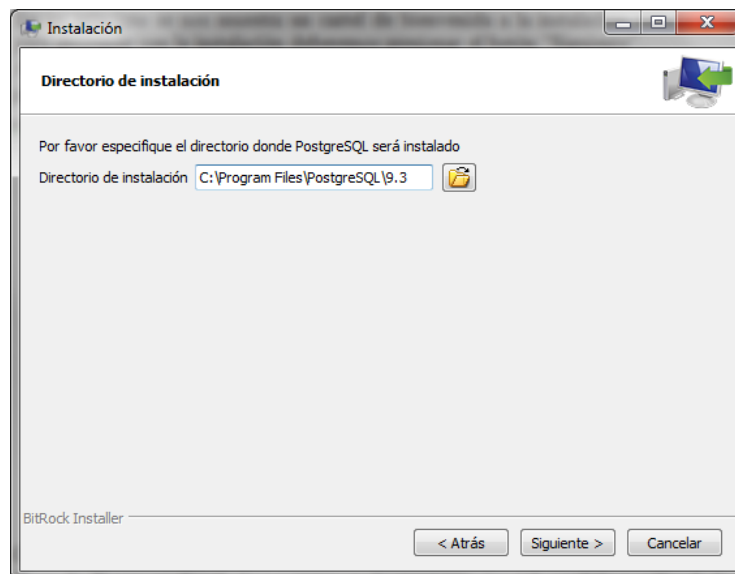


4. En esta etapa se inicializa la instalación del JDK packet en nuestro sistema. Una vez finalizada la instalación se nos muestra una pantalla en donde se menciona el registro que se puede realizar (o no) en la página oficial de Java; para finalizar nuestra instalación deberemos presionar el botón “Continue”, como se muestra en la siguiente imagen:

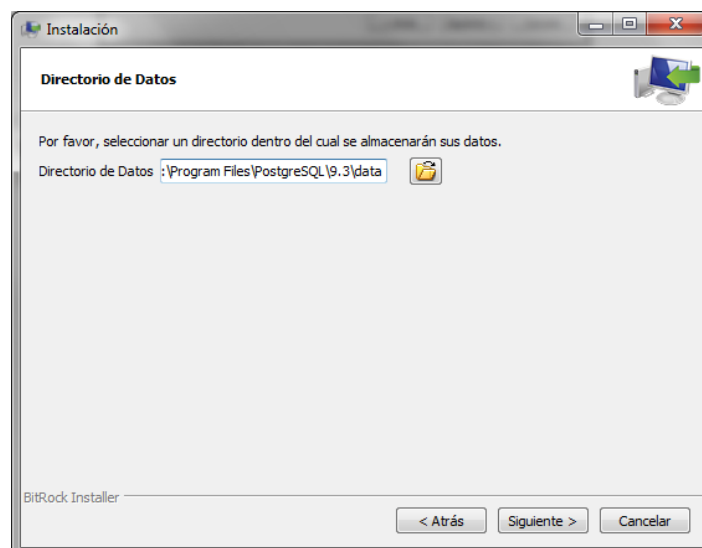


Postgre SQL

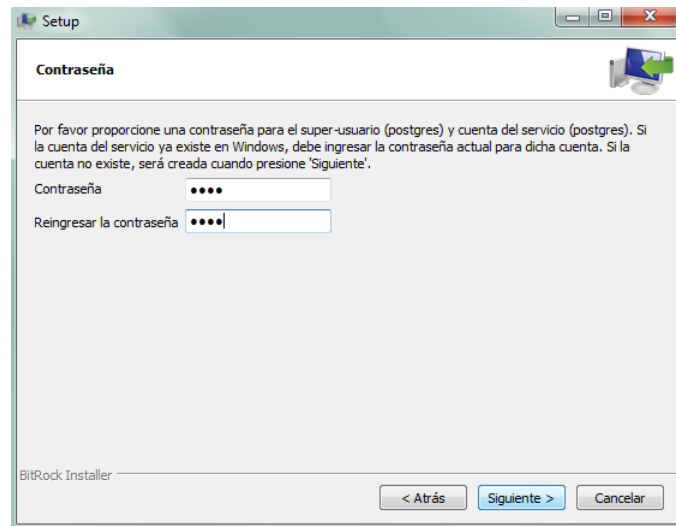
1. Una vez descargado el programa ejecutaremos su instalador para iniciar la instalación consecutivamente.
2. En un principio se nos muestra un cartel de bienvenida a la instalación, siendo que para proseguir con la instalación deberemos presionar el botón “Siguiente”.
3. A continuación se deberá ingresar la ruta de instalación, o utilizar la dada por defecto Y para continuar la instalación se deberá presionar el botón “Siguiente”. Aquí se muestra una imagen con la ruta dada por defecto:



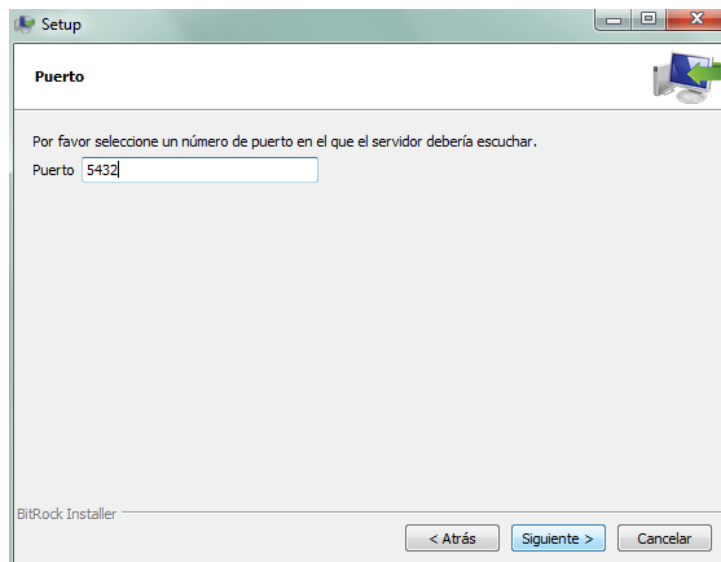
4. Consecuentemente ingresaremos la ruta en donde se almacenaran los datos de nuestra Base de Datos, pudiendo hacer como en la etapa anterior (eligiéndola o utilizada la ya dada). La imagen a continuación ilustra la selección de la ruta por defecto:



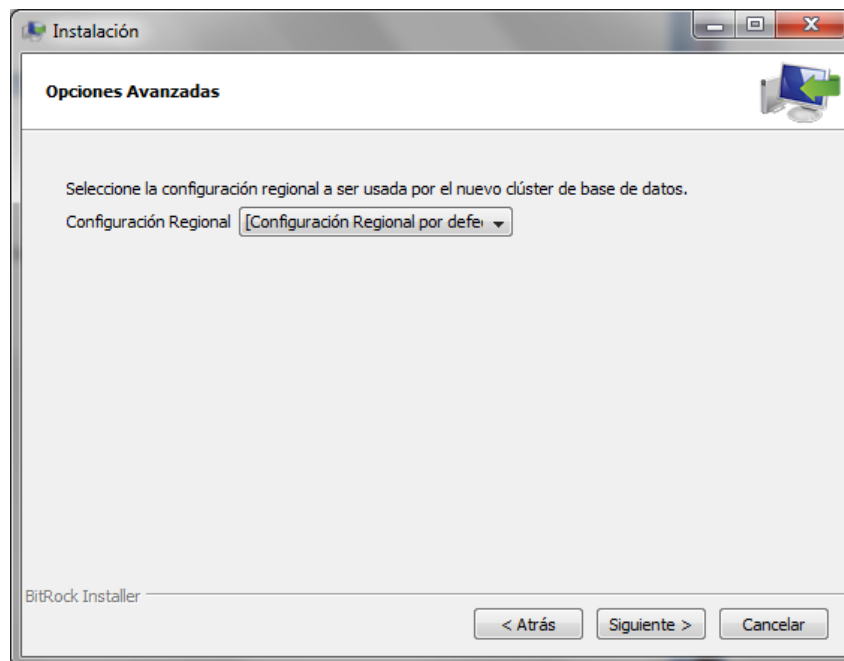
5. Nuestra base de datos nos genera un usuario determinado como “super-usuario” (postgres), deberemos ingresar en primera instancia su correspondiente contraseña y por ultimo un re-ingreso de la misma.



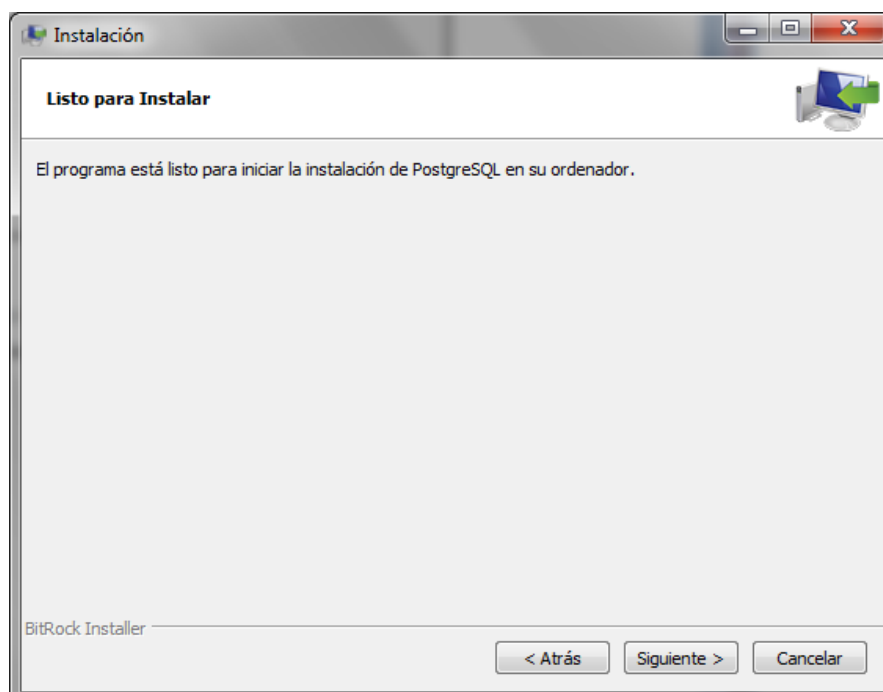
6. La siguiente etapa nos genera el hecho de ingresar el número de puerto (en nuestra pc) donde la Base de Datos “escuchara”.



7. A continuación se deberá seleccionar la “región” en la que trabajara nuestra Base de Datos



8. Consecuentemente se nos menciona que se inicializara la instalación, y para ello daremos click o enter en el botón “siguiete”.



9. Al ya estar finalizada la instalación, se nos muestra un mensaje el cual menciona si deseamos instalar en consiguiente el programa “Lanzar StackBuilder” el cual nos descarga e instala componentes, controladores y aplicaciones para nuestro PostgreSQL (ya instalado); por ultimo tendremos que presionar el botón “terminar”. Imagen en la cual deseccionamos dicho programa (por un tema de indisponibilidad de tiempo en un futuro para controlar todo cambio dado por dicha aplicación):



10. A continuación deberemos iniciar nuestra Base de Datos accediendo al símbolo de sistema e ingresando los siguientes comandos:

```
____cd C:\Archivos de programa\PostgreSQL\9.1\bin
____initdb -E UTF-8 -U postgres..\data
```

Manual Open NMS

Introducción

OpenNMS es una aplicación fácil de utilizar. Podemos manipular cada una de las características de la red, así como, analizar y detallar cada uno de los archivos que se transfieren, y realizar una serie de tareas de gestión y de conexiones de red.

Este software realiza un análisis de cada una de las conexiones entrantes y salientes de nuestra red, con el principal objetivo de verificar si existen conexiones no autorizadas. También, genera reportes completos de gestión, para documentar cada una de las situaciones que se presenten en la red.





Crear un usuario

En este paso tenemos que crear un usuario para sí mismo, vamos a utilizar un usuario de prueba “tutorial”

Hacemos click en Configuración de Usuarios, y haga click en “Añadir nuevo usuario”, aquí colocaremos el usuario a crear y la contraseña para ese usuario.

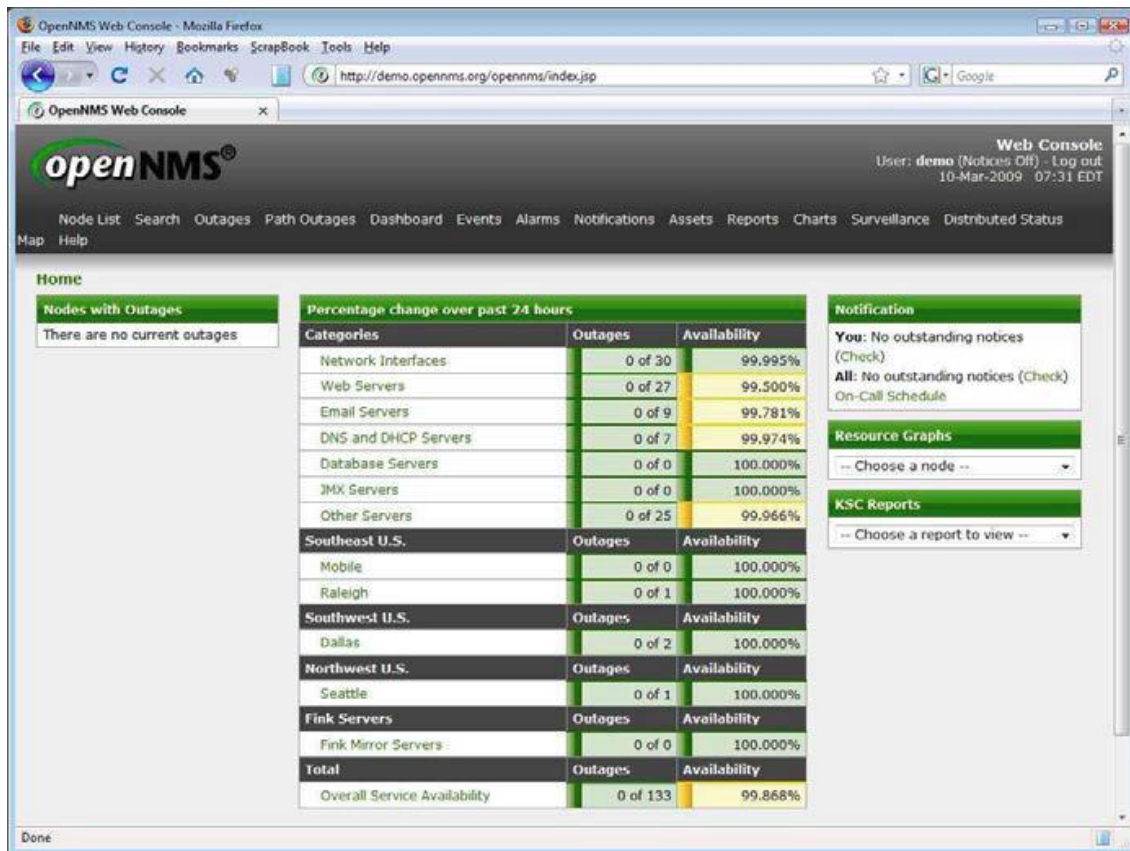
Luego de hacer click en Aceptar, completamos la información que nos parezca que sea relevante para el usuario.

Cuando haya terminado, haga click en “Finalizar” en la parte inferior de la pantalla. Usted debe de estar visible en esta lista de usuarios:

Delete	Modify	Rename	User ID	Full Name	Email	F
		<input type="button" value="Rename"/>	admin	Administrator		
Default administrator, do not delete						
		<input type="button" value="Rename"/>	tutorial	Tutorial User	tutorial@example.com	
No Comments						

Funcionalidades

OpenNMS está dividido en una serie de funcionalidades que cumplen con unas determinadas características.



- **Gestión de Eventos y Alarmas**

- **Recolección de Eventos:** Open NMS puede registrar todo tipo de eventos ocurridos: Triggers (es un procedimiento que se ejecuta cuando se cumple una condición establecida al realizar una operación), evaluación de eventos, automatización de acciones en función del procesado de la tabla de alarmas.

Los eventos se controlan con el proceso Eventd el cual recibe y graba toda la información. Este proceso escucha el puerto 5817 por el cual los demás procesos envían peticiones e incluso se pueden enviar desde sistemas externos a OpenNMS.

openNMS®

User: demo (Notices On) - Log out
24-Sep-2008 17:09 EDT

Event List

Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Distributed Status Map Help

Home / Events / List

View all events Advanced Search Severity Legend Acknowledge entire search

Event Text: Time: Any Search

Results: (1-10 of 24557)

Search constraints: Event(s) outstanding [-]

Legend

Ack	ID	Severity	Time	Node	Interface	Service	Ackd
<input type="checkbox"/>	3850706	Normal [+] [-]	24/09/08 17:09:13 [-] [-]	uei.opennms.org/internal/authentication/sessionRemoved [+] [-]			
OpenNMS user 'rnt' has been logged out of the WebUI, most likely due to a session timeout.							
<input type="checkbox"/>	3850651	Normal [+] [-]	24/09/08 17:08:26 [-] [-]	uei.opennms.org/internal/authentication/successfulLogin [+] [-]			
OpenNMS user rtc has logged in from 127.0.0.1.							
<input type="checkbox"/>	3850634	Minor [+] [-]	24/09/08 17:08:12 [-] [-]	ams.ni.eu.fimomms.net (finc... [+] [-]	213.84.134.230 [+] [-]	SNMP [+] [-]	
uei.opennms.org/nodes/dataCollectionFailed [+] [-]							
SNMP data collection on interface 213.84.134.230 failed.							
<input type="checkbox"/>	3850541	Normal [+] [-]	24/09/08 17:04:01 [-] [-]	uei.opennms.org/internal/authentication/successfulLogin [+] [-]			
OpenNMS user demo has logged in from 80.250.16.10.							
<input type="checkbox"/>	3850527	Normal [+] [-]	24/09/08 17:02:37 [-] [-]	uei.opennms.org/internal/authentication/loggedOut [+] [-]			
OpenNMS user 'demo' logged out of the WebUI.							
<input type="checkbox"/>	3850441	Normal [+] [-]	24/09/08 16:59:24 [-] [-]	uei.opennms.org/internal/authentication/sessionRemoved [+] [-]			
OpenNMS user 'demo' has been logged out of the WebUI, most likely due to a session timeout.							
<input type="checkbox"/>	3850267	Normal [+] [-]	24/09/08 16:54:05 [-] [-]	nen.opennms.org [+] [-]	216.216.217.254 [+] [-]	SMTP [+] [-]	
uei.opennms.org/nodes/nodeRegainedService [+] [-]							
The SMTP outage on interface 216.216.217.254 has been cleared. Service is restored.							
<input type="checkbox"/>	3850226	Normal [+] [-]	24/09/08 16:53:42 [-] [-]	nen.opennms.org [+] [-]	216.216.217.254 [+] [-]	HTTP [+] [-]	
uei.opennms.org/nodes/nodeRegainedService [+] [-]							
The HTTP outage on interface 216.216.217.254 has been cleared. Service is restored.							
<input type="checkbox"/>	3850168	Minor [+] [-]	24/09/08 16:53:10 [-] [-]	nen.opennms.org [+] [-]	216.216.217.254 [+] [-]	SMTP [+] [-]	
uei.opennms.org/nodes/nodeLostService [+] [-]							
SMTP outage identified on interface 216.216.217.254 with reason code: did not connect to host with timeout: 3000ms retry: 1 of 1.							

- **Correlación de Alarmas:** Se utiliza un mecanismo de Alarma para manejar traps de recolección de alarmas o traps de anulación de alarmas en un entorno de gestión de alarmas cíclico.

Aquí podemos ver el listado de alarmas

Alarm List

User: **demo** (Notices On) - Log out
 24-Sep-2008 17:00 EDT

[Node List](#) [Search](#) [Outages](#) [Path Outages](#) [Dashboard](#) [Events](#) [Alarms](#) [Notifications](#) [Assets](#) [Reports](#) [Charts](#) [Surveillance](#) [Distributed Status](#) [Map](#) [Help](#)

Home / Alarms / List

[View all alarms](#) [Advanced Search](#) [Severity Legend](#) [Acknowledge entire search](#)

Alarm Text: Time: Any

Results: (1-4 of 4)

Search constraints: [alarm is outstanding \[-\]](#)

Legend

Ack	ID	Severity	Node	Interface	Service	Count	Last Event Time	First Event Time	Log Msg
<input type="checkbox"/>	44129	UEI [+] [-]				1	24/09/08 15:03:08 [-] [-]	24/09/08 15:03:08 [-] [-]	OpenNMS user 'ID%131%140%137' (may be blank) has failed to login from 87.238.157.2. The failure event is BadCredentialsException with the message 'Bad credentials'.
<input type="checkbox"/>	44136	UEI [+] [-]				2	24/09/08 12:53:47 [-] [-]	24/09/08 12:53:34 [-] [-]	OpenNMS user 'brebis337' (may be blank) has failed to login from 90.31.94.140. The failure event is BadCredentialsException with the message 'Bad credentials'.
<input type="checkbox"/>	44131	UEI [+] [-]				1	24/09/08 09:26:01 [-] [-]	24/09/08 09:26:01 [-] [-]	OpenNMS user 'demo' (may be blank) has failed to login from 90.59.39.138. The failure event is BadCredentialsException with the message 'Bad credentials'.
<input type="checkbox"/>	44110	UEI [+] [-]				1	24/09/08 09:11:23 [-] [-]	24/09/08 09:11:23 [-] [-]	OpenNMS user 'demo@NO' (may be blank) has failed to login from 62.214.101.33. The failure event is BadCredentialsException with the message 'Bad credentials'.

4 alarms [Reset](#) [Select All](#) [Acknowledge Alarms](#)

Results: (1-4 of 4)

OpenNMS Copyright © 2002-2008 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

Mientras que aquí vemos el detalle de alarma.

openNMS®

Alarm Detail
User: demo (Notices On) - Log out
24-Sep-2008 17:02 EDT

Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Distributed Status Map Help

Home / Alarms / Detail

Alarm 44126

Severity	Critical	Node		Acknowledged By	
Last Event	9/24/08 12:53:47 PM	Interface		Time Acknowledged	
First Event	9/24/08 12:53:34 PM	Service		Ticket ID	
Count	2	UE1	uci.opennms.org/internal/authentication/failure	Ticket State	
Product Key	uci.opennms.org/internal/authentication/failure:BadCredentialsException:brebs357				

Log Message
OpenNMS user "brebs357" (may be blank) has failed to login from 90.31.84.140. The failure event is BadCredentialsException with the message "Bad credentials".

Description
This event is sent by the WebUI when an authentication failure occurs.

Operator Instructions
No instructions available

Acknowledgment and Severity Actions

Acknowledge

Clear

Go

Acknowledge this alarm

Clear this alarm

OpenNMS Copyright © 2002-2008 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

- **Notificaciones de Usuario y Escalados Programados:** Open NMS soporta múltiples usuarios y proporciona un mecanismo de Escalado de Notificaciones entre los usuarios. Si se detecta un evento, como una alarma Mayor, este mecanismo generará una notificación que se escalará en el tiempo a través de una lista de usuarios si la alarma no se reconoce en un periodo de tiempo definido por el usuario. El sistema también puede generar un sonido, un email o un mensaje instantáneo para llamar la atención sobre la notificación.

openNMS®

Notice List
User: demo (Notices On) - Log out
24-Sep-2008 17:05 EDT

Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Distributed Status Map Help

Home / Notices / List

Currently showing only **acknowledged** notices. [Show outstanding]

Results: (1-25 of 18851)

1 2 3 4 5 Next Last

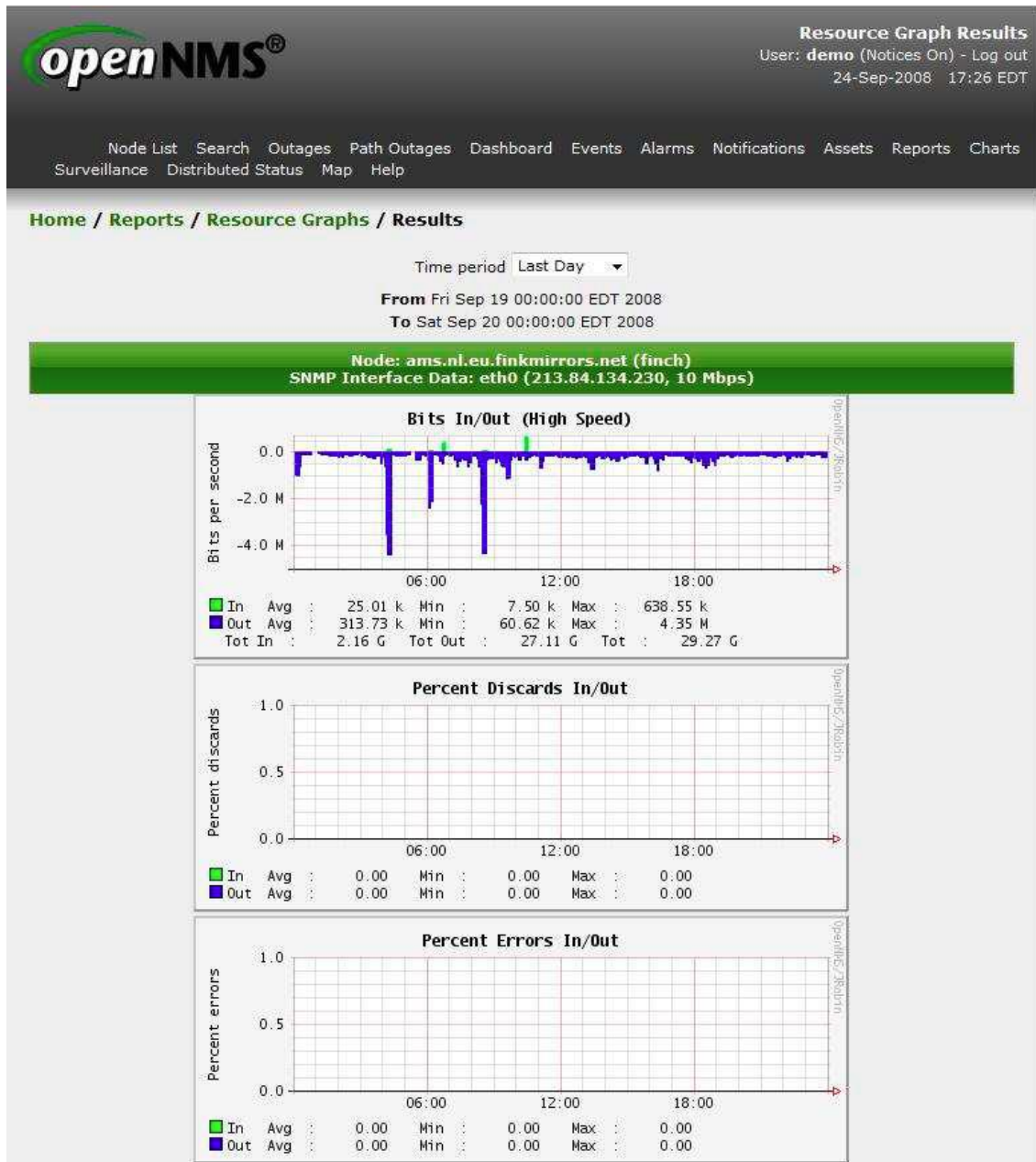
Legend

ID	Event ID	Severity	Sent Time	Resender	Resend Time	Node	Interface	Service
19604	3850168	Minor	9/24/08 4:53:19 PM	auto-acknowledged [+]	9/24/08 4:54:06 PM	nen.opennms.org [+]	216.216.217.254 [+]	SMTP [+]
The SMTP service poll on interface nen (216.216.217.254) on node nen.opennms.org failed at Wednesday, September 24, 2008 4:53:10 PM EDT.								
19603	3850144	Minor	9/24/08 4:53:11 PM	auto-acknowledged [+]	9/24/08 4:53:45 PM	nen.opennms.org [+]	216.216.217.254 [+]	HTTP [+]
The HTTP service poll on interface nen (216.216.217.254) on node nen.opennms.org failed at Wednesday, September 24, 2008 4:52:57 PM EDT.								
19602	3849869	Minor	9/24/08 4:38:40 PM	auto-acknowledged [+]	9/24/08 4:39:31 PM	ams.ni.eu.finkimrirs.net (finc... [+]	213.84.134.230 [+]	HTTP [+]
The HTTP service poll on interface ds026.xs4all.nl (213.84.134.230) on node ams.ni.eu.finkimrirs.net (finc...) failed at Wednesday, September 24, 2008 4:38:40 PM EDT.								
19601	3849814	Minor	9/24/08 4:38:04 PM	auto-acknowledged [+]	9/24/08 4:39:13 PM	ams.ni.eu.finkimrirs.net (finc... [+]	213.84.134.230 [+]	HTTPS [+]
The HTTPS service poll on interface ds026.xs4all.nl (213.84.134.230) on node ams.ni.eu.finkimrirs.net (finc...) failed at Wednesday, September 24, 2008 4:38:03 PM EDT.								
19600	3848987	Minor	9/24/08 3:25:02 PM	auto-acknowledged [+]	9/24/08 3:25:30 PM	nen.opennms.org [+]	216.216.217.254 [+]	HTTP [+]
The HTTP service poll on interface nen (216.216.217.254) on node nen.opennms.org failed at Wednesday, September 24, 2008 3:24:56 PM EDT.								

Aquí podemos observar el listado de notificaciones

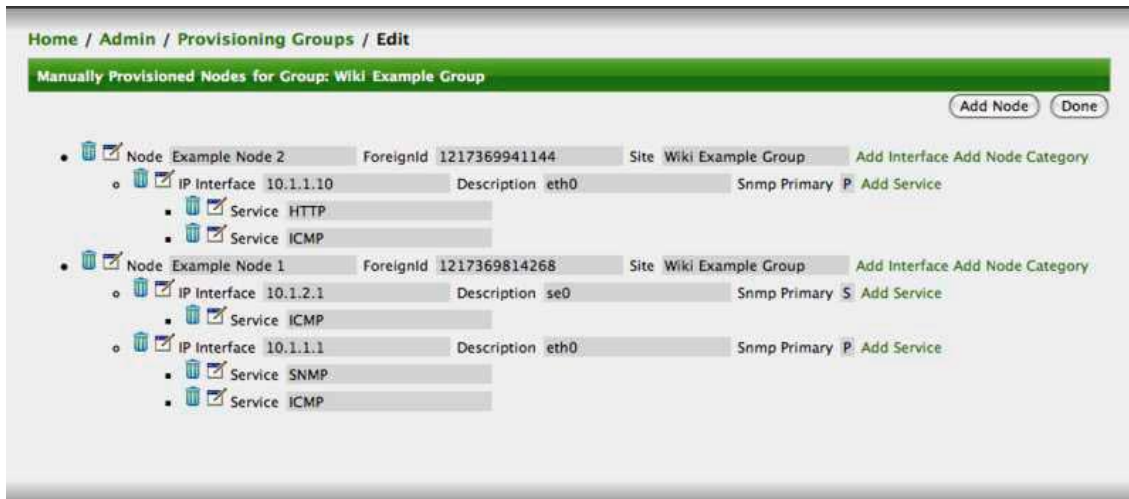
Visualización de Datos

OpenNMS presenta los datos de rendimiento en forma de gráficos. Estos gráficos también se pueden exportar en forma de informes de rendimiento.

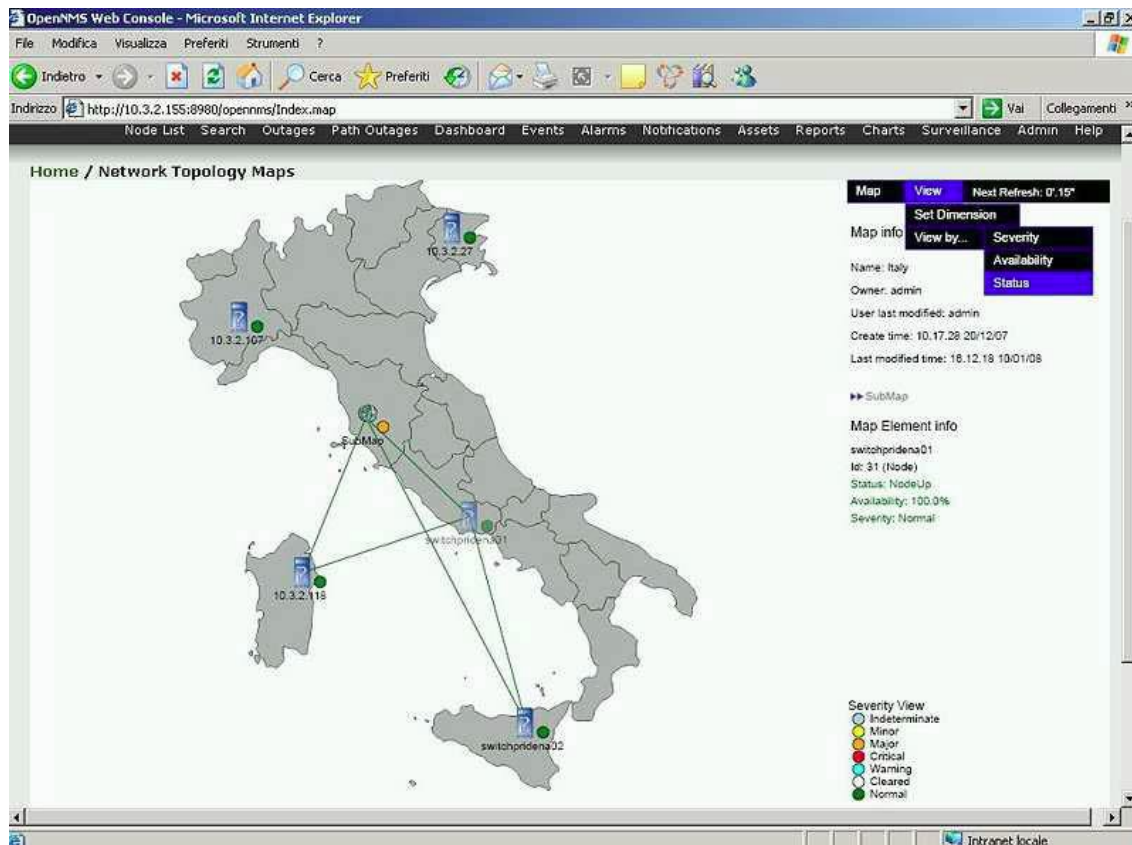


Configuración de interfaces

También se pueden utilizar archivos XML conteniendo la configuración de las interfaces y así modificar el nombre y el inventario de la Red.



El sistema está preparado para utilizar mapas para mostrar la topología de la red tal y como se refleja a continuación.



14.0. Bibliografía

www.telefoniavozip.com

www.urutel.com.uy

www.voz-ip.com

www.hp.com.

www.cisco.com

www.opennms.org

15.0 Hoja testigo