UNIVERSIDAD INDUSTRIAL DE SANTANDER

PLANTEAMIENTO TOPOLÓGICO PARA EL MEJORAMIENTO DE LA CONECTIVIDAD SENA REGIONAL SANTANDER

JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNÁNDEZ CELIS

FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERIAS ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2006

PLANTEAMIENTO TOPOLÓGICO PARA EL MEJORAMIENTO DE LA CONECTIVIDAD SENA REGIONAL SANTANDER

JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNÁNDEZ CELIS

Informe Final de Proyecto de Grado en Modalidad de Práctica Empresarial presentado como requisito para optar al título de INGENIERO ELECTRONICO

Director
PhD. OSCAR GUALDRÓN GONZALEZ

Codirector
Ing. ANDRÉS JÁCOME LOBO

Tutores
Ing. JESUS ANTONIO DELGADO ALBA
Ing. HUMBERTO LUIS DURÁN

FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERIAS ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2006

Para Mi Diosito, mis Padres, mis Abuelistos y mi Hermana Lili;
Por su ejemplo, su apoyo y su paciencia.

Y para ti, mi bodoquito;
Por se la fuente más pura de toda mi inspiración.

Jorge

A Dios

A mis padres por su comprensión y apoyo

A mis hermanos por compartir mis sueños y metas

Y a mis amigos con los que he contado toda mi vida

Helber

AGRADECIMIENTOS

Los autores expresan su más sincero agradecimiento y reconocimiento a:

JESÚS ANTONIO DELGADO ALBA Y HUMBERTO LUIS DURÁN, Tutores del presente trabajo de grado.

ANDRÉS AUGUSTO JÁCOME LOBO, Codirector del presente trabajo de grado.

OSCAR GUALDRÓN GONZÁLEZ, Director del presente trabajo de grado.

HUMBERTO RANGEL LIZCANO, Director Regional del SENA Regional Santander.

UNIVERSIDAD INDUSTRIAL DE SANTANDER y a sus excelentes profesores.

Todas las personas que directa o indirectamente contribuyeron en el desarrollo de esta Práctica Empresarial.

Y muy especialmente, a nuestros padres, a Dios y a la Virgen, por iluminarnos y acompañarnos siempre.

Muchas Gracias

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

Se enunciarán los términos técnicos utilizados en el presente documento con la finalidad de proporcionar claridad en su lectura.

Agenda de Conectividad: Programa que impulsa el Ministerio de Comunicaciones que busca masificar el uso de las Tecnologías de la Información y Comunicación (TIC).

ATM: Asynchronous Transfer Mode. Modo de Transferencia Asíncrona.

Backbone: **I**nfraestructura principal de transmisión de datos de una red

Bandwith: Ancho de Banda: cantidad de datos que se pueden transmitir en una unidad de tiempo, normalmente se expresa en bps (bytes por segundo)

BNC: British National Connector, utilizado para conectar dispositivos en red local 10BASE2 Ethernet con un cable coaxial.

BRI: Basic Rate Interfaz. Interfaz de velocidad básica.

Bridge: Interconectan distintas LAN del mismo tipo o generar varias desde una misma.

Capa física: Capa 1 del modelo TCP/IP que describe las características de las conexiones físicas del host hacia la red, en lo que se refiere al medio, características del medio y forma en la que se transmite la información.

Capa de enlace: Capa 2 del modelo TCP/IP que describe cómo son transportados los paquetes a través de la capa física.

Capa de red: Capa 3 del modelo TCP/IP que permite que los datos lleguen desde el origen a su destino, aún cuando ambos no estén conectados directamente. Es decir, se encarga de encontrar un camino para ellos.

Capa de transporte: Capa 4 del modelo TCP/IP que se encarga de aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario y pasarlos a la capa de red.

Capa de aplicación: Capa 5 del modelo TCP/IP que ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizac las aplicaciones para intercambiar datos como correo electrónico, gestores de bases de datos y servidores de archivos.

Conpes: Documentos aprobados por el Consejo Nacional de Política Económica y Social.

Datagramas: Fragmento de un paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el ordenador receptor, de manera indemiendiente a los fragmentos restantes.

Dirección IP: Identificador numérico de 32 bits que identifica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP. Al contrario de la dirección MAC, la dirección IP si se puede cambiar.

Dirección MAC: Media Access Control Address. Identificador alfanumérico de 48 bits que corresponde en forma única con una tarjeta de red. Esta dirección es única y no se puede cambiar.

Tráfico Broadcast: Modo de direccionamiento de la información donde un nodo emisor envía información todos los nodos de la red de manera simultánea.

Tráfico Multicast: Modo de direccionamiento de la información en una red a múltiples destinos simultáneamente.

Tráfico Unicast: Modo de direccionamiento de la información de un único emisor a un único receptor.

DNS: Domain Name System. Sistema de nombres de dominio. Base de datos distribuída u jerárquica que almacena la información asociada a los nombres de dominio de direcciones IP.

DSL: Digital Suscriber Line. Suscripción Línea Digital.

E1: Formato europeo de transmisión digital que lleva datos a una tasa de transferencia de 2048 Kbps y puede llevar 32 canales de 64 Kbps cada uno.

G.703: Estándar internacional de la ITU para transferencia de datos entre dos equipos de comunicaciones a velocidades de 2 Mbps y 64 Kbps y se refiere a las señales físicas y lógicas a través de circuitos digitales

Host: También conocida como una estación de trabajo. Se refiere a una máquina conectada a una red de computadores y que cuenta con un nombre de equipo y dirección IP únicos.

Hub: Concentrador que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás.

Interfaz: Se refiere un puerto por el cual diferentes tipos de datos pueden ser enviados y recibidos.

LAN: Siglas de Local Area Network o en español, Red de área local.

Latencia: Se refiere al tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro.

Mbps: Megabytes por segundo

Medio de transmisión: Soporte físico a través del cual el host emisor y host receptor pueden comunicarse en un sistema de transmisión de datos.

Modelo OSI: (Open Systems Interconnection Reference Model). Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO (Organización Internacional para la Estandarización) en el que se incluyen 7 capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

Modelo TCP/IP: Modelo de interconexión de Internet que incluye 5 capas: física, enlace, red, transporte y aplicación.

Nodo: Punto donde confluye una red.

Oracle: Sistema de administración de base de datos fabricado por Oracle Corporation.

Paquetes: Es la unidad fundamental de transporte de información en las redes de computadores.

PRI: Primary Rate Interfaz. Interfaz de velocidad primaria.

Protocolo ARP: Address Resolution Protocol. Protocolo de resolución de direcciones. Se encarga de traducir las direcciones IP a direcciones MAC y es el responsable de la mayor parte del tráfico broadcast de la red.

Protocolo DHCP: Dymamic Host Configuration Protocol. Protocolo que permite asignar direcciones IP dinámicamente.

Protocolo FTP: File Transfer Protocol. Protocolo de transferencia de archivos. Permite transferir grandes bloques de datos por la red.

Protocolo H.263: Protocolo utilizado para la transmisión de audio y video en tiempo real para aplicaciones de videoconferencia.

Protocolo ICMP: Internet Control Message Protocol. Protocolo de Control de Mensajes de Internet.

Protocolo RTP: Real Time Transport Protoco. Protocolo de transporte en tiempo real. Utilizado para la transmisión de información en tiempo real como por ejemplo audio y video en una videoconferencia.

Protocolo SNMP: Simple Network Management Protocol. Protocolo Simple de Gestión de Redes.

Protocolo TCP: Transmission Control Protocol. Protocolo de control de transmisión. Uno de los protocolos fundamentales de Internet que garantiza que los datos serán entregados en su destino sin errores.

Protocolo TNS: Protocolo utilizado en bases de datos basadas en Oracle.

Protocolo UDP: User Datagram Protocol. Protocolo de datagramas de usuario. Trabaja en capa de transporte.

Protocolos: Conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red

PSTN: Public Switched Telephone Network. Red Telefónica Pública Conmutada.

Puerto: Permite acoplar a un sistema físico un conector o cable.

QoS: Quality of Service. Calidad de Servicio. Es una cualidad que permite programar en el dispositivo la cantidad de ancho de banda máximo y mínimo que utilizarán las aplicaciones IP que se transportarán sobre esta infraestructura de telecomunicaciones.

Repetidores: Efectúan la repetición eléctrica de la señal.

Router: Interconecta segmentos o redes enteras y enruta los paquetes que pasan a través de él, según su destino.

RS-232: Puerto serial que utiliza cableado simple desde 3 hasta 25 hilos.

Switch: Interconecta dos o más segmentos de red.

Telefonía IP: Se habla de telefonía IP cuando se dispone de equipos especializados denominados teléfonos IP que se pueden conectar directamente a la red de datos y a los que se les puede configurar una única dirección IP.

TIC: Tecnologías de la Información y la Comunicación.

Tokens: Se refiere a un paquete especial que va de nodo a nodo según una secuencia dividida.

Topología lógica: Forma en que los host se comunican a través del medio de transmisión.

Topología: Tipo de estructura de la red

Voz sobre IP: Sistema de enrutamiento de conversaciones de voz mediante paquetes IP por una red.

WINS: Servidor de nombres para NetBIOS que mantiene una tabla de correspondencia para direcciones MAC y nombres de hosts. Permite localizar rápidamente a otro host en la red.

TITULO

Planteamiento Topológico Para el Mejoramiento de la Conectividad SENA REGIONAL SANTANDER[1]

AUTORES

JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNANDEZ CELIS[**]

Palabras clave

SENA, Conectividad, Red de Datos, Voz sobre IP, Evaluación de la Red, Documentación de Red, Monitoreo de Red, Ethereal, PRTG, OpManager

Descripción

El presente documento expone los resultados alcanzados durante la práctica empresarial realizada en el SENA REGIONAL SANTANDER. En esta práctica empresarial, se realizó una evaluación detallada de la Red de Datos que interconecta todos los centros del SENA REGIONAL SANTANDER con la Sede Administrativa en la ciudad de Bucaramanga y con la Dirección General en la capital de la República. La evaluación se realizó siguiendo el orden lógico de: Documentación, Monitoreo, Análisis de Resultados y planteamiento de requerimientos mínimos para garantizar una calidad adecuada en los servicios de red.

El objetivo principal del estudio, es evaluar el desempeño de la Red de Datos que se encuentra en funcionamiento actualmente en el SENA REGIONAL SANTANDER y si es el caso, plantear un nuevo esquema de conectividad, adecuado a las necesidades actuales de enlace de datos; Internet, Voz sobre IP y aplicaciones remotas.

Para conseguirlo, como primera medida, se elaborará una documentación detallada de toda la Red de Datos, partiendo de la información recopilada a través de la Oficina de Sistemas y complementándola con la utilización de diversas herramientas para el descubrimiento de la red, buscando documentar de la manera más actualizada posible el estado de la misma. Posteriormente, se realizará un monitoreo de la red, con el fin de observar su comportamiento y determinar su desempeño en cada uno de los nodos que la conforman. Y por último, se elaborará un estudio detallado de los costos actuales de telefonía, que permitan hacerse una idea de los ahorros que se pueden alcanzar en caso de implementar una solución de conectividad que incluya Voz sobre IP para las llamadas institucionales.

Una vez recopilada toda la información, se realizará una evaluación de lo encontrado y se plantearán los requerimientos técnicos necesarios para incrementar el rendimiento de la Red de Datos, acorde con las perspectivas a futuro de la Entidad.

---

[1] Trabajo de Grado
[**] Facultad de Ingenierías Fisicomecánicas, Escuela de Ingenierías Electríca Electrónica y Telecomunicaciones
Director: Oscar Gualdrón González, PhD.

TITLE

Topological exposition for the improvement of the connectivity the SENA REGIONAL SANTANDER*

AUTHORS

JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNANDEZ CELIS**

Keywords

SENA, Connectivity, Data network, Voice on IP, Evaluation of the Network, Documentation of Network, Monitoring of Network, Ethereal, PRTG, OpManager

Description

The present document exposes the results reached during the enterprise practice made in the SENA REGIONAL SANTANDER. In this enterprise practice, a detailed evaluation of the Data network was made that interconnects all the centers of the SENA REGIONAL SANTANDER with the Administrative Seat in the city of Bucaramanga and with the Central office in the capital of the Republic. The evaluation was made following the order logical of: Documentation, Monitoring, Analysis of Results and exposition of minimum requirements to guarantee a quality adapted in the services of network.

The primary target of the study, is to evaluate the performance of the Data network that at the moment is in operation in the SENA REGIONAL SANTANDER and if it is the case, to raise a new scheme of connectivity, adapted to the present necessities of data link; Internet, Voice on IP and remote applications.

In order to obtain it, like first measurement, a detailed documentation of all the Data network will be elaborated, starting off of the information compiled through the Office of Systems and complementing it with the use of diverse tools for the discovery of the network, looking for to document more of the possible way updated the state of the same one. Later, a monitoring of the network will be made, with the purpose of observing its behavior and determining its performance in each one of the nodes that conform it. And finally, a detailed study of the present costs of telephony will be elaborated, that allow to become an idea of the savings that can be reached in case of implementing a connectivity solution that includes Voice on IP for the institutional calls.

Once compiled all the information, an evaluation of the found thing will be made and the necessary technical requirements will consider increasing the yield of the Data network, agreed with the perspective to future of the Organization.

---

* Work of degree

** Physical-mechanical Engineering Faculty, Electrical, Electronic and Telecommunications Engineering School. Director: Oscar Gualdrón González, PhD.

INTRODUCCIÓN

En este momento, en Colombia, el sector educativo está atravesando por una etapa de reestructuración, lo cual ha conllevado a generar una dependencia cada vez mayor de la tecnología, convirtiéndose en una ventaja competitiva y por supuesto en un medio para garantizar la continuidad de las entidades que proveen servicios de educación.

Este es el caso del Servicio Nacional de Aprendizaje (SENA), que desde su creación en 1957, ha tenido por objeto contribuir al desarrollo social, económico y tecnológico del país, extendiendo el alcance de la formación profesional integral a toda la población colombiana.

Para el actual periodo de gobierno, que comprende desde el 2002 hasta el presente año, la institución ha formulado y está ejecutando el Plan Estratégico: “SENA: UNA ORGANIZACIÓN DE CONOCIMIENTO”, en el que se proyecta como ente ejecutora de la política social del gobierno, prioriza el emprendimiento y la creación de empresas, la innovación y el desarrollo tecnológico, la cultura de la calidad, normalización y certificación de competencias laborales, el servicio público de empleo, la internacionalización institucional y por supuesto, la publicación de información a nivel virtual.

De acuerdo con estas perspectivas actuales y futuras del SENA a nivel nacional, surge la necesidad de contar con una Red de Datos Institucional que soporte y permita un óptimo manejo de la información, dada la creciente demanda de aplicaciones de ejecución remota que hacen uso de la red, el aumento en la necesidad de los estudiantes para realizar investigaciones haciendo uso de la red y la necesidad de posibilitar los requisitos de disponibilidad requeridos para acceder a los diferentes servicios que ofrece el SENA.

Es así como en el SENA REGIONAL SANTANDER se requiere una Red de Datos acorde con las exigencias de conectividad planteadas entre la Sede Administrativa, sus Centros en el departamento de Santander y la Dirección General en la ciudad de Bogotá; lo que ha motivado a llevar a cabo el presente estudio, apoyado en la documentación existente y en la información recopilada por el personal a cargo de la administración de la red.

Dada la problemática actual de conectividad que presenta la Red de Datos del SENA REGIONAL SANTANDER y aprovechando la existencia de un convenio marco con la UNIVERSIDAD INDUSTRIAL DE SANTANDER vigente para el 2006[2], el SENA le ha solicitado a la UNIVERSIDAD la elaboración de un estudio detallado de su Red de Datos, que le permita brindar el soporte técnico y económico necesario para justificar un mejoramiento en su esquema actual de conectividad.

De esta manera, el objetivo principal del estudio, es evaluar el desempeño de la Red de Datos que se encuentra en funcionamiento actualmente en el SENA REGIONAL SANTANDER y si es el caso, plantear un nuevo esquema de conectividad, adecuado a las necesidades actuales de enlace de datos; Internet, Voz sobre IP y aplicaciones remotas.

Para conseguirlo, como primera medida, se elaborará una documentación detallada de toda la Red de Datos del SENA REGIONAL SANTANDER, partiendo de la información recopilada a través de la Oficina de Sistemas y complementándola con la utilización de diversas herramientas para el descubrimiento de la red, buscando documentar de la manera más actualizada posible el estado de la misma.

Posteriormente a la documentación, se realizará un monitoreo de la red, con el fin de observar su comportamiento y determinar su desempeño en cada uno de los nodos que la conforman.

Además, se elaborará un estudio detallado de los costos actuales de telefonía, que permitan hacerse una idea de los ahorros que se pueden alcanzar en caso de

[2] Convenio Marco de Cooperación celebrado entra la Universidad Industrial de Santander y el Servicio Nacional de Aprendizaje “SENA”. N 00000052 Revisado el 23 de Febrero de 2005 y con vigencia de 3 años.

implementar una solución de conectividad que incluya Voz sobre IP para las llamadas institucionales.

Una vez recopilada toda la información, se realizará una evaluación de lo encontrado y se plantearán los requerimientos técnicos necesarios para incrementar el rendimiento de la Red de Datos, acorde con las perspectivas a futuro de la Entidad.

A continuación, se presentan los resultados de la documentación, el monitoreo y el estudio de costos de telefonía que se elaboraron. Así como la evaluación del desempeño de la red y los requerimientos técnicos que se plantearon.

1. PRESENTACIÓN DEL PROYECTO

1.1 Planteamiento del problema

Las tecnologías de información y comunicaciones han experimentado un significativo avance en los últimos años en Colombia. Con diferente intensidad y prontitud, los diversos sectores de la sociedad, de la economía y del sector público han comenzado a incorporar las nuevas tecnologías en sus actividades.

Dada la necesidad de asumir cuanto antes acciones para evitar rezagarse, ante los profundos cambios culturales y tecnológicos que están transformando a la humanidad en los inicios del siglo XXI, el Gobierno Nacional estableció una política de largo plazo orientada a lograr una penetración masiva de las Tecnologías de la Información y de las Comunicaciones (TIC) en Colombia y para ello creó mediante el documento Conpes 3072[3] de febrero del año 2000 a la Agenda de Conectividad[4].

El SENA REGIONAL SANTANDER, como empresa del Estado y dada su misión formativa, requiere una infraestructura de red que se adapte a todas las exigencias actuales de velocidad y confiabilidad, que le permita atender la formación de todos los trabajadores colombianos que estén inscritos en sus programas.

Actualmente, se cuenta con una red de datos que comunica todas las sedes de la Regional Santander, pero se presentan algunos inconvenientes considerables como lo son: el no contar con una documentación adecuada de la misma, la carencia de políticas

[3] Este documento presenta a consideración del CONPES la “Agenda de Conectividad”, que busca masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002 "Cambio para Construir la Paz".

[4] Programa que impulsa el Ministerio de Comunicaciones que busca masificar el uso de las Tecnologías de la Información y Comunicación (TIC), y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información. Los grupos hacia los cuales está orientada esta tarea son: La ciudadanía, las empresas, la administración pública.

de uso de la red, la falta de una infraestructura para el soporte de una administración centralizada en la Sede Administrativa y la falta de escalabilidad de la red que permita agregar más estaciones de trabajo sin afectar su rendimiento. Por lo tanto, se requiere plantear un sistema que permita suplir estas falencias y mejorar con esto la conectividad para el SENA REGIONAL SANTANDER, adecuado a las necesidades actuales en enlaces de datos; Internet, Voz sobre IP y aplicaciones remotas con la Sede Administrativa y la Dirección General.

1.2 Justificación

El estudio nace de la solicitud hecha por el SENA REGIONAL SANTANDER dada la problemática actual de conectividad presentada en su red de datos, teniendo como fin presentar el soporte técnico y económico necesario para justificar el mejoramiento de dicha red.

A esto se suma la creciente demanda de aplicaciones de ejecución remota que hacen uso de la red de datos, además del aumento en la necesidad de los estudiantes para realizar investigaciones haciendo uso de la red y posibilitar los requisitos de disponibilidad de esta.

Una red de este tamaño e importancia requiere personas a cargo del manejo y administración de la Red, debido a la necesidad de migrar a nuevas tecnologías para estar a la par con la evolución informática. Por ello el SENA ha dispuesto profesionales del área de Sistemas y Telecomunicaciones y ha requerido de practicantes en esta área para que conjuntamente manejen de forma coordinada y organizada el mantenimiento, administración y continua actualización de la red. Siendo así posible ofrecer un excelente servicio que cubra las necesidades de formación y desempeño para todos los usuarios.

Este proyecto se rige por los lineamientos que se han estipulado en el convenio marco de cooperación entre las dos instituciones que tiene por objeto la realización conjunta de programas, proyectos, eventos académicos y científicos en diferentes áreas y niveles de la educación; facilitando a la Universidad los espacios y campos de prácticas para los estudiantes de las carreras que de acuerdo con un plan de trabajo directamente acordado con las unidades académicas de la Universidad, sean requeridas para la realización de dichas prácticas.

El compromiso del SENA de estar a la vanguardia en tecnología, como modelo de otras empresas del país, es otra de las razones por las cuales se realiza este estudio.

Con la realización de este estudio el SENA REGIONAL SANTANDER, tendrá el soporte necesario para justificar el mejoramiento del esquema de conectividad con que cuenta actualmente.

2. LA EMPRESA

El Servicio Nacional de Aprendizaje (SENA), creado en 1957 como resultado de la iniciativa conjunta de los trabajadores organizados, los empresarios, la iglesia católica y la Organización Internacional del Trabajo, es un establecimiento público del orden nacional, con personería jurídica, patrimonio propio e independiente y autonomía administrativa, adscrito al Ministerio de la Protección Social de la República de Colombia.

El SENA cumple la función que le corresponde al Estado de invertir en el desarrollo social y técnico de los trabajadores colombianos, ofreciendo y ejecutando la formación profesional integral para la incorporación de las personas en actividades productivas que contribuyan al crecimiento social, económico y tecnológico del país.

Además de la formación profesional integral, impartida a través de los Centros de Formación, brindando así servicios de Formación continua del recurso humano vinculado a las empresas; información; orientación y capacitación para el empleo; apoyo al desarrollo empresarial; servicios tecnológicos para el sector productivo, y apoyo a proyectos de innovación, desarrollo tecnológico y competitividad.

2.1 Misión

El Servicio Nacional de Aprendizaje (SENA) se encarga de cumplir la función que le corresponde al Estado de invertir en el desarrollo social y técnico de los trabajadores colombianos, ofreciendo y ejecutando la Formación Profesional Integral gratuita, para la incorporación y el desarrollo de las personas en actividades productivas que contribuyan al desarrollo social, económico y tecnológico del país.

2.2 Visión

Ejercer la Formación Profesional Integral, como un elemento central de función social, enfocada hacia afuera, en función de la dinámica nacional e internacional, contribuyendo a la creatividad y la innovación empresarial, e impulsando los procesos que apoyen la transformación laboral y ocupacional que demanda el país.

2.3 Situación geográfica

A nivel nacional, el SENA está organizado en 24 regionales, dentro de las que se encuentra la Regional Santander, que a su vez está conformada por 8 grandes centros distribuidos a lo largo de todas las provincias del departamento de Santander.

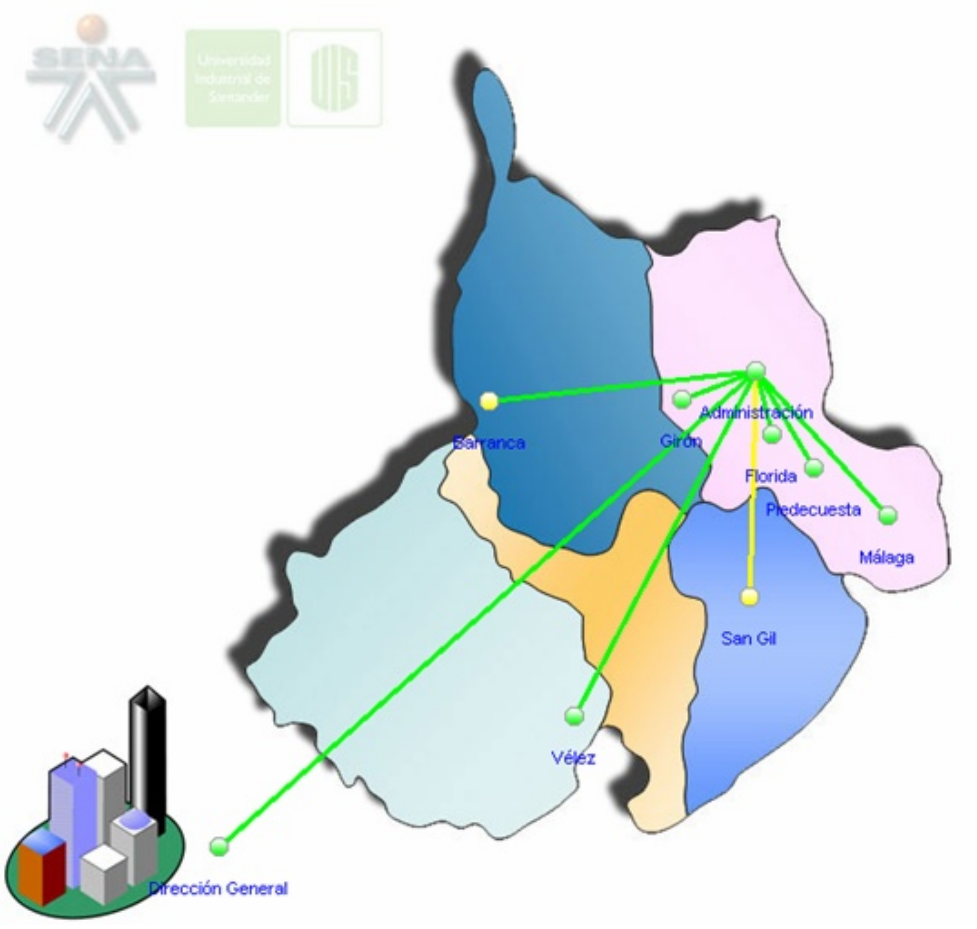


Figura 1.1. Centros que conforman el SENA REGIONAL SANTANDER (Fuente: Autores)

2.3.1 Centro de Comercio y Servicios (Bucaramanga)

El Centro de Comercio y Servicios, contiguo al edificio del área administrativa, atiende a las comunidades que requieren capacitación en el área comercial o formación especial para que el alumno desarrolle su actividad laboral con excelente calidad.

Fuente: Archivo SENA

2.3.2 Centro Multisectorial de Barrancabermeja

Este centro se encarga de capacitar los tres sectores económicos en los niveles local, regional y nacional. Sus esfuerzos están concentrados en impulsar el desarrollo empresarial de la Provincia de Mares, Sur de Bolívar, Sur del Cesar, Norte de Antioquia así como, de todos los municipios adscritos a la zona Centro de Colombia.

Fuente: Archivo SENA

2.3.3 Centro Industrial de Floridablanca

La meta de este centro es aumentar la competitividad del Recurso Humano, aplicando los elementos modernos de la Formación Profesional Integral y los servicios tecnológicos, para disminuir el desempleo regional y nacional e incrementar la productividad y eficiencia en los subsectores básicos de la economía santandereana.

Fuente: Archivo SENA

2.3.4 Centro Industrial de Girón

El Centro Industrial de Girón lidera y desarrolla la capacitación, difusión y transferencia de tecnologías industriales; contribuye al mejoramiento de la calidad de vida, a la modernización y adecuación de procesos y equipos de la micro, la pequeña, la mediana y la gran empresa santandereana y nacional.

Fuente: Archivo SENA

2.3.5 Centro de Atención al Sector Agropecuario (Piedecuesta)

El Centro de Atención Agropecuario, busca impartir formación profesional en las áreas agrícolas, pecuarias, agroindustriales y de mercado, buscando un desarrollo sostenible en el tiempo. Está ubicado en el municipio de Piedecuesta en el área de Guatiguará.

Fuente: Archivo SENA

2.3.6 Centro Multisectorial de Atención a la Provincia de García Rovira (Málaga)

El Centro Multisectorial de la Provincia de García Rovira tiene como función contribuir al desarrollo socio-económico de los municipios que conforman la provincia de García Rovira; la cual esta conformada por 12 Municipios y 15 Municipios de las provincias de norte y Gutiérrez de Boyacá.

Fuente: Archivo SENA

2.3.7 Centro Multisectorial de Atención a la Provincia Guanentina y Comunera

Se ubica en el municipio de San Gil y tiene como función, contribuir al desarrollo socio-económico de los municipios que conforman las provincias de Guanentina y Comunera, con sus 34 municipios que la componen.

Fuente: Archivo SENA

2.3.8 Centro Multisectorial de Atención a la Provincia de Vélez

Este centro se propone contribuir al crecimiento y desarrollo de la Provincia de Vélez a través de sus 19 Municipios, mediante la formación integral de los estudiantes, convirtiéndolos en trabajadores capaces y generadores de empresa.

Fuente: Archivo SENA

3. ESTADO DEL ARTE Y MARCO TEORICO

3.1 Redes LAN

Una red LAN (Local Area Network)[5] es un sistema de comunicaciones que comprende un conjunto de equipos (hardware) y herramientas (software), que permiten compartir recursos a grandes velocidades entre dispositivos, terminales y estaciones de trabajo dentro una determinada extensión geográfica (del orden de los Km). Son redes con velocidades típicas entre 10 y 100 Mbps, con baja latencia[6] y baja tasa de errores.

Un esquema básico de una red LAN es el siguiente:

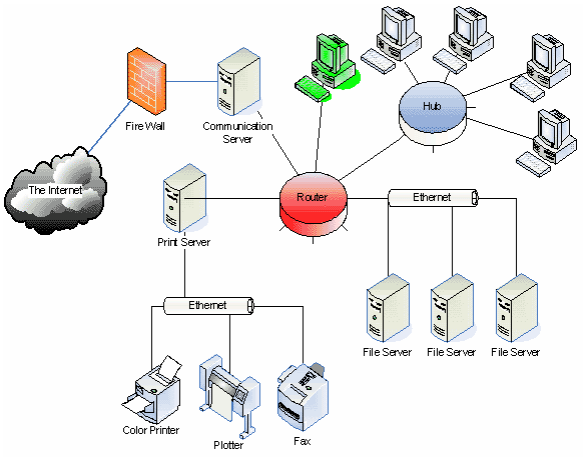


Figura 3.1. Esquema básico de una red LAN (Fuente: [26])

Al momento de hablar de una red LAN se definen dos aspectos fundamentales que la caracterizan:

- Topología
- Medio de Transmisión

[5]Local Area Network: Red de Area Local.
[6] Latencia: Se refiere al tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro.

Topología de red

La topología de red define la estructura de una red. Hay dos tipos de topología, la topología física y topología lógica, la primera se refiere a la forma en que las estaciones acceden al medio para compartir información y la topología física se refiere a la disposición real de los cables o medios de transmisión.

Las topologías físicas más comúnmente usadas son las siguientes:

- **Topología de anillo:** Esta topología conecta las estaciones una a una, la primera con la segunda, ésta con la tercera y así sucesivamente; hasta que la última se conecte con la primera, formando así un lazo o anillo. La información solo se transmite en un sentido, por lo tanto si un host[7] falla, la estación adyacente no recibirá datos.

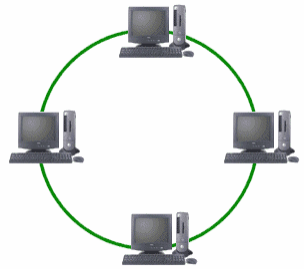


Figura 3.2. Topología en anillo (Fuente: [27])

- **Topología estrella:** En la topología estrella se conectan todas las estaciones a un nodo central y este irradia todos los enlaces hacia las demás estaciones. La ventaja principal es que permite que todas las estaciones se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

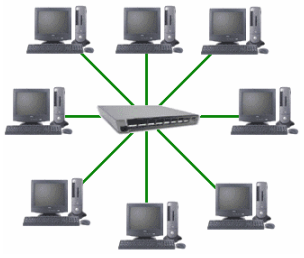


Figura 3.3. Topología en estrella (Fuente: [27])

[7] Host: Estación de trabajo.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens[8].

- **Topología Broadcast:** La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red.

- **Topología de transmisión de Tokens:** La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red.

Medios de transmisión:

El medio de transmisión constituye el soporte físico a través del cual el host emisor y host receptor pueden comunicarse en un sistema de transmisión de datos.

Se distinguen dos tipos de medios: guiados y no guiados.

- **Guiados:** Los medios guiados conducen (guían) los datos a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el par trenzado.

- **No guiados:** Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como por ejemplo, el aire y el vacío. En esta categoría entran los microondas, infrarrojos y radio enlaces de VHF y UHF.

[8] Token: Se refiere a un paquete especial que va de nodo a nodo según una secuencia dividida.

Dispositivos de red:

- **Repetidores (Capa Física)[9]:** Efectúan la repetición eléctrica de la señal, permitiendo de esta forma el aislamiento eléctrico entre extremos del cable y la extensión de la LAN en un área mayor. Los repetidores no dividen el tráfico; todo el tráfico pasa de un extremo al otro.

- **Hub (Capa de Enlace):** Un Hub es un concentrador que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. También es llamado **repetidor** multipuesto.

- **Bridge (Capa de Enlace):** También conocido como puente**.** Permiten interconectar distintas LAN del mismo tipo o generar varias desde una misma, esto hace que la red tenga mayor disponibilidad al generar LAN autosuficientes, reduciendo el tráfico entre las secciones de red.

- **Switch (Capa de Enlace):** Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los bridges, pasando datos de una red a otra, de acuerdo con la dirección MAC[10] de destino de los datagramas en la red. Un switch es el centro de una red en topología estrella. También es llamado **puente** multipuesto.

- **Router (Capa de Red):** Es el dispositivo más importante en una red, interconecta segmentos o redes enteras y enruta los paquetes que pasan a través de él, según su destino. El Router puede segmentar datagramas muy largos en caso de congestión, pero no pueden ensamblar datagramas.

- **Switch-Router (Capa de Red):** Es un **switch** que trabaja en capa de red y realiza la operación de enrutamiento mediante acciones de hardware; en tanto que es un **router** cuando las mismas se realizan mediante acciones de software.

[9] Se refiere a las capas del modelo TCP/IP.
[10] MAC (*Media Access Control)*: Control de Acceso al Medio

3.1.1. Gestión de red

La gestión de red consiste en monitorizar y controlar los recursos de una red de datos, con el fin de garantizar un adecuado nivel de servicio.

Las funciones básicas de la gestión de red son:

- **Monitorización**: Consiste en obtener información de la red con el fin de detectar anomalías y fallas en la misma. Estas acciones son pasivas y su único objetivo es conocer el comportamiento de la red, respecto a su tráfico.

- **Control***:* Consiste en modificar y aplicar cambios en la configuración de los dispositivos desde la estación de gestión para adaptarlos a nuevos requerimientos o en respuesta a fallos reportados.

Protocolos de Gestión de redes:

Se toman en consideración dos protocolos utilizados en la gestión de redes, el ICMP[11] y el SNMP[12]:

- **ICMP**: Este protocolo ofrece mecanismos para la transferencia de mensajes de control a partir de los routers o las estaciones de trabajo, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

- **SNMP**: Es un protocolo para soportar mensajes de control y gestión. El modelo de capas TCP/IP ubica a SNMP en la capa de aplicación y utiliza mensajes de tipo UDP[13] en la capa de transporte.

[11] ICMP (Internet Control Message Protocol): Protocolo de Control de Mensajes de Internet.
[12] SNMP (Simple Network Management Protocol): Protocolo Simple de Gestión de Redes.
[13] UDP (User Datagram Protocol): Protocolo de datagramas de usuario

3.1.2. Herramientas para el monitoreo y la gestión de redes

Existen numerosas herramientas que facilitan la tarea del administrador de la red, las cuales ofrecen funciones de descubrimiento, seguridad y estadísticas del tráfico. Es posible encontrarlas tanto de distribución gratuita como licenciadas.

En el desarrollo de esta practica se trabajaron unas cuantas de ellas, dentro de las cuales están: Solarwinds, PRTG, OpManager y Ethereal entre otras.

3.1.2.1 Solarwinds

Es una herramienta que contiene cerca de 45 funciones para la gestión de configuración, la administración de ancho de banda, monitorización del desempeño de la red, administración de direcciones, descubrimiento de dispositivos de red y gestión de fallas. [15]

Características principales:

- Descubrimiento de Red
- Monitorización de Fallas
- Gestión del desempeño
- MIB[14] Browser
- Monitorización de ancho de banda (Bandwidth Monitor)
- Seguridad
- Herramientas de gestión de routers CISCO

[14] MIB (*Management Information Base*): Bases de información de administración.

3.1.2.2 Ethereal

Es un analizador de paquetes de red, usado para localizar fallos en la red, evaluar los distintos protocolos y detectar el mal uso de los recursos Web. Este analizador de protocolos captura los paquetes que fluyen por la red y los visualiza de una forma explicita y organizada, funciona sobre sistemas como Unix, Linux y Windows. **[12]**

Características:

- Captura de los datos de paquetes en tiempo real.
- Información detallada de los paquetes y los protocolos usados.
- Permite guardar y cargar los datos de paquetes capturados.
- Posee diferentes opciones de filtrado de paquetes
- Proporciona estadísticas.

3.1.2.3 PRTG

Esta es una herramienta destinada a la realización de estadísticas sobre el ancho de banda. Existe una versión demo que permite controlar y monitorizar hasta 50 dispositivos de manera simultanea. Con este software se mide el ancho de banda de entrada y salida de un dispositivo SNMP

Es importante dejar claro que esta aplicación precisa que el dispositivo a monitorizar y analizar sea compatible con el protocolo SNMP, que permite acceder a esta clase de funcionalidades. [28]

Características:

- Compatible con SNMP.
- Descubrimiento de elementos activos de red.
- Proporciona estadísticas graficas sobre el tráfico unicast[15], no unicast y errores.

[15] Transmisiones punto a punto

3.1.2.4 OpManager

Es un software de Gestión de Redes que permite obtener información combinada de la red LAN en cuanto a sus enlaces, sus dispositivos y sus interfaces o puertos. Integra funciones de gestión de fallas y gestión de desempeño. [29]

Características:

- Gestión de Fallas.
- Manejo de Alarmas.
- Permite realizar reportes.
- Descubrimiento de elementos activos de red.
- Es completamente personalizable a la red en la que se instale.
- Detecta problemas de rendimiento de la red.
- Identifica problemas de rendimiento de las aplicaciones de los servidores.

3.2 Acceso a Internet

Existen distintas formas de obtener acceso a Internet entre las cuales se incluyen:

- **Dial-up:** Un Dial up establece una conexión a Internet mediante una línea telefónica permitiéndole acceder a todas las herramientas disponibles en Internet. La velocidad de transmisión de de 56 Kbps y la velocidad promedio disponible es de 33.6 Kbps

- **Enlace dedicado:** Este tipo de conexión establece un circuito permanente mediante línea dedicada a un grupo de computadoras o red. Un canal dedicado envían voz, datos y video a una ubicación específica; tienen diferentes anchos de banda y su costo varía según el ancho de banda.

- **Frame relay:** Proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. Su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red. Ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps o superiores.

- **ATM**[16]**:** Es actualmente una tecnología estable y ampliamente utilizada en redes públicas y privadas. ATM permite alcanzar altas velocidades de transmisión (Gigabit/s) e integrar todo tipo de aplicaciones sobre la misma red, garantizando a cada aplicación la calidad de servicio que necesita, de una forma flexible y eficiente.

- **xDSL**[17]**:** Está formado por un conjunto de tecnologías que proveen un gran ancho de banda sobre circuitos locales de cable de cobre sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo de la red.

- **ISDN**[18]**:** En español RDSI. La idea básica de RDSI es que cualquier información (voz, datos, imágenes, etc.), una vez codificada digitalmente puede ser tratado de igual manera, con la única diferencia de las velocidades requeridas en cada caso. Provee canales de 64 kbps cada uno.

- **X.25:** La X.25 se define como la interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos públicas basada en el protocolo HDCL[19].

- **DDR**[20]: Entrega una conexión de la red IP a la red pública telefónica **PSTN**[21]. Se implementa sobre líneas conmutadas de circuitos para reducir el costo de conexión. Puede ser desarrollada sobre interfaz serial sincrónica o asincrónica o sobre líneas ISDN usando interfaz **BRI**[22] o **PRI**[23]. La topología es muy simple: generalmente punto-a-punto entre routers hacia un router central que funciona de concentrador. El router dispone de un mapa estático de direcciones telefónicas que actúa en forma similar a ARP[24] en las LAN; relaciona la dirección IP con un número telefónico.

[16] ATM (Asynchronous Transfer Mode): Modo de Transferencia Asíncrona.
[17] DSL (Digital Suscriber Line): Suscripción Línea Digital.
[18] ISDN (Integrated Services Digital Network): Red Digital de Servicios Integrados.
[19] HDCL (High-Level Data Link Control): Interfase de control de datos de alto nivel.
[20] DDR (Dial- on-Demand Routing):
[21] PSTN (Public Switched Telephone Network): Red Telefónica Pública Conmutada.
[22] BRI (Basic Rate Interfaz): Interfaz de velocidad básica.
[23] PRI (Primary Rate Interfaz): Interfaz de velocidad primaria.
[24] ARP (Address Resolution Protocol): Protocolo de resolución de direcciones.

3.3 Voz sobre IP y Telefonía IP

Primero que todo, es necesario precisar la definición de voz sobre IP y telefonía IP. La voz sobre IP o voz sobre Internet no es otra cosa que la conversión de la voz en paquetes de datos y su transmisión a través de la Red utilizando el protocolo IP. Por otra parte, la telefonía IP tiene que ver con teléfonos con direcciones IP, que hacen por si solos la conversión de voz a protocolo IP y viceversa, y que, además, permiten efectuar aplicaciones de datos, no exclusivamente de voz.[10]

La voz sobre redes IP (VoIP[25]) inicialmente se implementó para reducir el ancho de banda mediante la compresión de la voz (aprovechando los procesos de compresión diseñados para sistemas celulares) y en consecuencia para disminuir los precios en la transmisión de los datos. Sin embargo, migró rápidamente a una red de servicios integrados sobre la misma LAN.

3.3.1 Tendencia Actual [11]

Por diversas razones, no sólo tecnológicas, las empresas se encuentran en un fuerte proceso de integración de aplicaciones en tiempo real sobre redes IP, en particular Voz (Telefonía), fax, video, etc.

En la siguiente figura se muestra el escenario clásico sobre el cual se manejan actualmente la telefonía y las redes de datos a nivel corporativo.

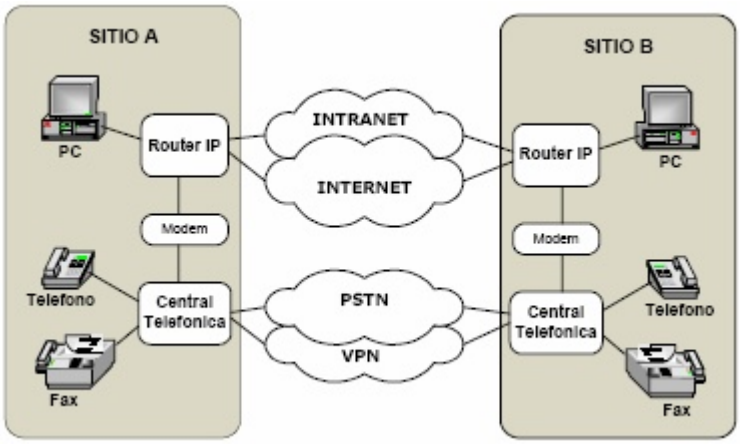


Figura 3.4 Arquitectura Corporativa Clásica de Redes de Voz y Datos (Fuente [11])

[25] VoIP (*Voice over IP*): Voz sobre IP.

Está planteado un horizonte de solución tecnológica con teléfonos IP y prescindiendo de conmutación de circuitos, pero en la actualidad hay pocas implementaciones de ese modelo debido a la imposibilidad de migrar completamente a ese tipo de tecnología. Se utiliza entonces la tecnología Voz sobre IP para las conexiones troncales entre las centrales telefónicas (PBX) como se muestra en la siguiente figura.

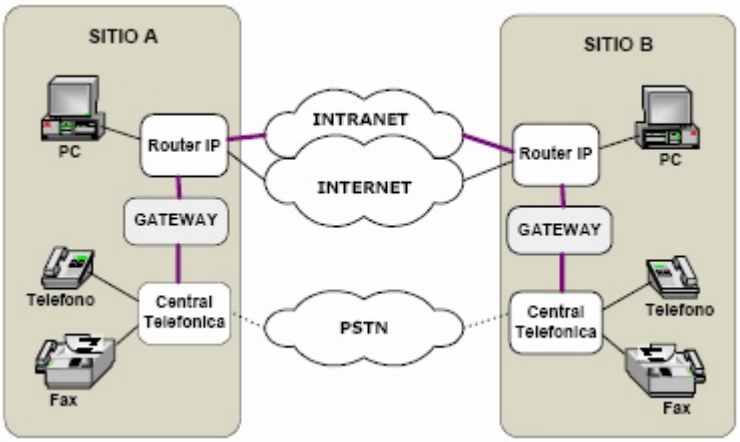


Figura 3.5 Arquitectura VoIP (Fuente [11])

El principal beneficio que motiva esta convergencia es la reducción de costos, que debería ser analizada en cada caso. En este análisis además de la inversión en equipamiento específico VoIP (Gatekeeper, terminales, gateways), hay que considerar los costos asociados a los nuevos requerimientos de la red IP y el costo del soporte técnico más especializado.

Para las soluciones de redes privadas en las que se requiere tener beneficios en el costo de la red para el transporte de tráfico de voz y datos sobre enlaces de 64 Kbps., la tecnología de voz sobre IP es la alternativa viable de solución ya que ofrece compresión de voz a 16 ó 8 Kbps. (16 Kbps. representa muy buena calidad y 8 Kbps. representa aceptable calidad) que permitirá explotar el ancho de banda para el transporte de voz y datos. Además, con la supresión de silencios, la voz sobre IP ofrece aprovechar más el ancho de banda al eliminar todos los paquetes vacíos originados durante una llamada telefónica.

3.3.2 Componentes [11]

El estándar VoIP definido en 1996 por la ITU, define los tres elementos fundamentales en su estructura:

- Terminales: Son los dispositivos extremos de la comunicación por medio de la red IP. Pueden ser teléfonos convencionales o teléfonos especialmente diseñados denominados teléfonos IP. Este tipo de teléfonos también pueden ser implementados en software y utilizarse en una estación de trabajo conectada a la red de datos.

- Gateways: Es el componente clave de una solución de voz IP, debido a que facilita la conversión de las llamadas telefónicas convencionales al mundo IP. Se encargan de enlazar la red telefónica tradicional con la red de datos, actuando de forma transparente para el usuario.

- Gatekeepers: Son las centrales de comunicaciones que proporcionan servicios de control de llamadas, traducción de direcciones, control de admisión, facilita el control del ancho de banda utilizado y localiza los distintos gateways de la red. Es un componente opcional.

4. DOCUMENTACIÓN DE LA RED

Una de las principales falencias identificadas en la red de datos del SENA REGIONAL SANTANDER, es la ausencia de una documentación actualizada que corresponda con el funcionamiento real de la red.

La tarea de documentar una red, es un proceso largo y tedioso para el administrador de la misma, lo que conlleva a que muchas veces este proceso sea relegado para último momento o nunca se realice. Además, la demanda inmediata de nuevos servicios y aplicaciones y el rápido crecimiento en la cantidad de usuarios dificulta el correcto diseño de la red y de su respectiva documentación.

En ese orden de ideas, como punto de partida para el presente trabajo, se elaboró la siguiente documentación de la red, haciendo uso de la información que maneja la base de datos de la empresa, el conocimiento del personal a cargo del mantenimiento de la red y complementándolas con el uso de la herramienta de software, IP Network Browser de Solarwinds, que permite hacer el descubrimiento de la red, basado en los agentes SNMP.

Una vez recolectados estos datos se elaboró un inventario físico y lógico de la red y sus componentes, y de cómo están interconectados entre sí, para ser integrados posteriormente en diagramas detallados de red de cada uno de los centros que conforman el SENA REGIONAL SANTANDER.

4.1 Red Nacional

Actualmente, el SENA tiene una infraestructura de redes LAN y WAN que soporta la arquitectura empresarial de la entidad y permite la comunicación entre todas las dependencias del SENA a nivel nacional: Dirección General en Bogotá con sus Regionales en las principales ciudades del país, entre ellas, la Regional Santander.

4.1.1 Estructura de la Red Nacional del SENA

La estructura física de la Red Nacional del SENA corresponde a una topología tipo estrella que tiene como nodo central un Router Huawei NetEngine 08E con puertos suficientes para conectar a todas las Regionales con la Dirección General ubicada en la Capital de la República.[26]

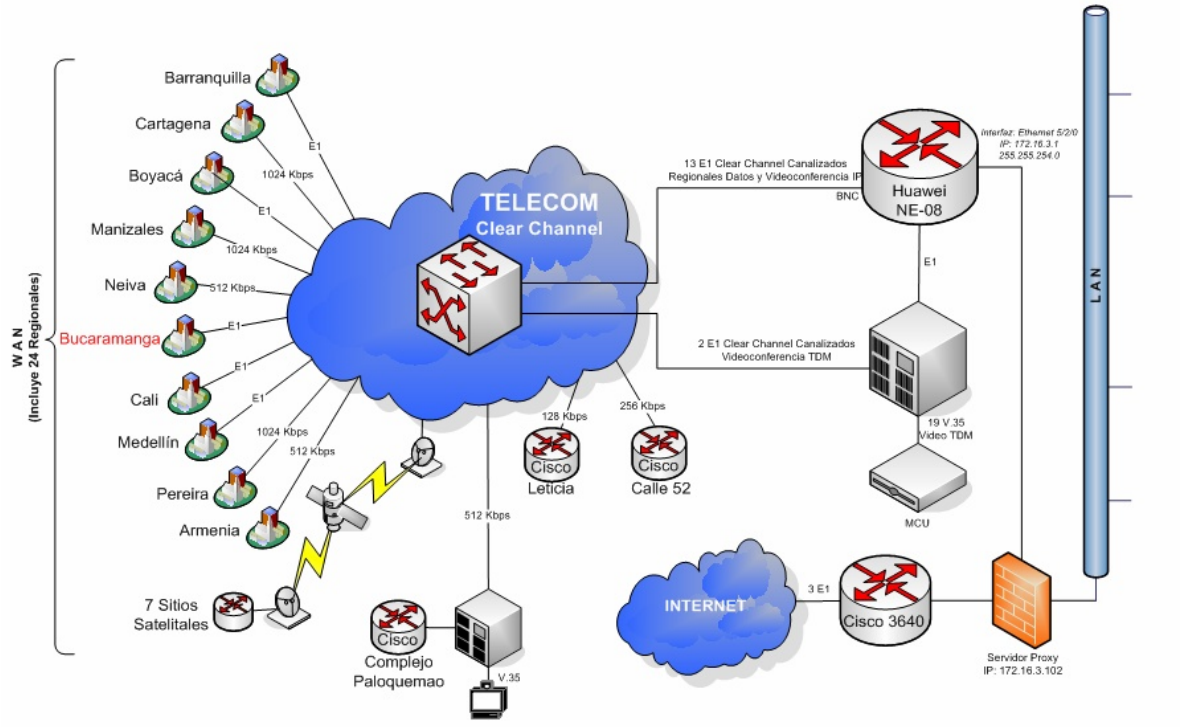


Figura 4.1. Esquema básico de la red de datos del SENA a nivel Nacional (Fuente: Autores)

Toda la conectividad de la red de datos del SENA se hace a través de Colombia Telecomunicaciones S.A. ESP (TELECOM), por medio de enlaces clear channel para cada una de las 24 regionales que se muestran en el esquema y por medio de enlaces satelitales para otras 7 regionales de difícil acceso, dada su posición geográfica.

[26] Ver Anexo A.2 Interfaces y Tablas de Rutas de los routers

4.1.2 Asignación de Direcciones IP

Algunos rangos de direcciones IP han sido reservados para la operación de redes privadas que usan el protocolo IP. Cualquier organización puede usar estas direcciones IP en sus redes privadas sin la necesidad de solicitarlo a algún Registro de Internet ya que el uso de estas direcciones no es regulado y no se debe pagar por ellas.

La principal condición establecida para el uso de direcciones IP privadas es que los dispositivos que usen estas direcciones IP no necesiten ser alcanzados desde Internet, lo cual resulta ideal para la implementación de una Red Interna.

Según el RFC 1918, la IANA (Internet Assigned Numbers Authority) ha reservado los siguientes tres bloques de direcciones IP para su utilización libre en Redes Internas:

Clase	Dirección de Red	Máscara de Subred
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Tabla 4.1. Rangos de Direcciones IP Privadas

Tomando en cuenta lo anterior y con el fin de implementar una Red de Datos lo más organizada posible, la División de Sistemas de la Dirección General del SENA en la ciudad de Bogotá, se encargó de asignar las direcciones IP para cada una de sus regionales y sus centros de formación, haciendo uso del bloque de direcciones privadas clase B, que va desde la 172.16.0.0 hasta la 172.31.255.255[27]

[27] Ver: Anexo A.1 Rangos de direcciones IP asignadas por la Dirección General

4.2 Red Regional

La red de datos del SENA REGIONAL SANTANDER incluye cada uno de sus centros principales y los interconecta con la Sede Administrativa permitiendo la comunicación y el intercambio de información entre ellos.

4.2.1 Descripción General de la topología de red

La topología física de la red de datos del SENA REGIONAL SANTANDER corresponde a una estrella, con 7 nodos periféricos; uno en cada centro, y un nodo central ubicado en la Sede Administrativa que corresponde a dos enrutadores: un Cisco 3640 y un Quidway 3640.

Además, también se incluye un nodo en la Dirección General, que hace parte de la Red Nacional

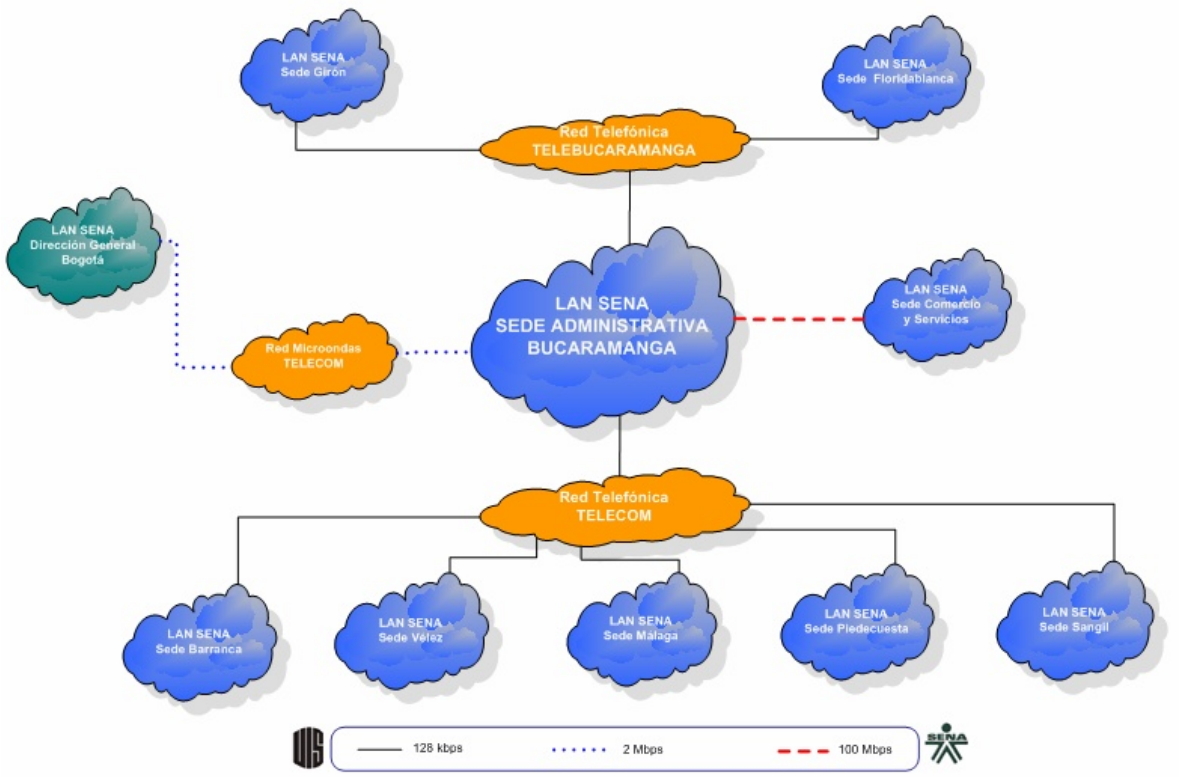


Figura 4.2. Topología de la Red de datos del SENA REGIONAL SANTANDER (Fuente: Autores)

4.2.2 Inventario lógico de subredes

El rango de direcciones IP usados en la red local del SENA se asigno de acuerdo a la tabla especificada por la Dirección General del SENA para cada una de las regionales.[28]

Las direcciones que no se encuentran dentro del rango comprendido en la Tabla A.1.1 (Rangos de Direcciones IP de las Regionales del SENA a nivel Nacional), como las de San Gil, Comercio y Servicios, Vélez, Málaga y Piedecuesta, fueron asignados posteriormente a Febrero de 1999 dadas las necesidades de conectividad del SENA Regional Santander con todas sus sedes.

Centro	Rango Direcciones IP	Máscara de red	Puntos Voz[29]	Puntos Datos[30]	Porcentaje de Asignación (%) Respecto a Rango de Direcciones IP	Puntos Uso[31]	Porcentaje de Uso (%) Respecto a Puntos de Datos
Sede Administrativa	172.16.54.1 – 172.16.55.254	255.255.254.0	176	228	44,88 %	139	60,96 %
Barranca	172.16.114.1 – 172.16.115.254	255.255.254.0	63	281	55,31 %	26	9,25 %
Girón	172.16.116.1 – 172.16.117.254	255.255.254.0	78	149	29,33 %	9	6,04 %
Florida	172.16.118.1 – 172.16.119.254	255.255.254.0	32	138	27,17 %	14	10,14 %
San Gil	172.16.122.1 – 172.16.123.254	255.255.254.0	47	85	16,73 %	37	43,52 %
Comercio y Servicios	172.16.124.1 – 172.16.125.254	255.255.254.0	65	169	33,27 %	100	59,17 %
Vélez	172.16.131.1 – 172.16.131.254	255.255.255.0	7	82	32,28 %	15	18,29 %
Piedecuesta	172.16.178.1 – 172.16.178.254	255.255.255.0	25	42	16,54 %	22	52,38 %
Málaga	172.16.182.1 – 172.16.183.254	255.255.254.0	10	50	9,84 %	11	22 %

Tabla 4.2. Rangos de Direcciones IP de los centros

De esta manera, la red de Datos del SENA REGIONAL SANTANDER, está conformada por 9 subredes, cada una de las cuales se encuentra asociada a un Centro o Sede, como por ejemplo, la subred de la Sede Administrativa, la subred de Vélez entre otras, que pese a encontrarse en ubicaciones tan distantes se comportan como una subred más dentro de la Red Regional.

[28] Ver Anexo A.1 Rangos de direcciones IP asignadas por la Dirección General
[29] Número de puntos de voz disponibles en la Sede
[30] Número de puntos de datos disponibles en la Sede
[31] Al momento del escaneo con Solarwinds

La asignación de direcciones IP para cada una de las estaciones de la red de datos del SENA REGIONAL SANTANDER, se hace por medio de un servidor DHCP[32], que permite distribuir de forma centralizada las direcciones IP necesarias, y automáticamente asignar y enviar una nueva IP si una estación de trabajo es conectada en un punto de red diferente que se encuentre habilitado.[33]

Por medio de la herramienta SNMP Sweep de Solarwinds[34], se identificaron las estaciones de trabajo que se encuentran funcionando en cada subred en el momento del escaneo y con estos datos se determinó su porcentaje de utilización, que se muestra en la tabla anterior. Sin embargo estos datos son aproximados, ya que constantemente pueden estar entrando y saliendo estaciones de la red, por esta razón se realizó también el cálculo del porcentaje de utilización teniendo en cuenta los puntos de red disponibles en cada Centro.

De esta manera, la subred que cuenta con un mayor número de puntos de red es la correspondiente a la Sede Barranca, incluso más que los de la Sede Administrativa, con aproximadamente 281, lo cual si estuvieran todos asignados corresponde a un porcentaje de uso del rango de direcciones del 55,31%. En segundo lugar se encuentra la subred de la Sede Administrativa con 44,88% y la del Centro de Comercio y Servicios con un 33,27% de utilización del rango de direcciones. Sin embargo, si se tienen en cuenta las estaciones detectadas con las herramientas de autodescubrimiento de Solarwinds, se presenta en primer lugar a la Sede Administrativa y en segundo lugar al Centro de comercio y Servicios, como era de esperarse, mientras que en la Sede de Barrancabermeja es donde menos se detectan estaciones.

Pese a ser las subredes con mayor utilización de direcciones IP, el porcentaje de asignación sigue siendo bajo y por lo tanto se puede afirmar que para todas las subredes, sobretodo para las de los centros más pequeños, el diseño logico de las subredes está sobredimensionado.

[32] DHCP: Dymamic Host Configuration Protocol, definido en el estándar RFC 2131
[33] Se habla de que un punto de red está habilitado cuando se encuentra conectado físicamente a un puerto del switch
[34] SNMP Sweep: Realiza un barrido de un rango de direcciones e indica cuáles se encuentran en uso

4.2.3 Plataforma tecnológica y aplicaciones

La plataforma tecnológica que se encuentra actualmente funcionando en el SENA a nivel nacional, plantea el manejo descentralizado de ciertas aplicaciones de gestión del tipo Cliente/Servidor, lo cual supone la necesidad de contar con múltiples servidores locales y con la existencia de una infraestructura técnica de soporte y coordinación en cada regional, que envíe oportunamente y periódicamente los datos a la Dirección General para su procesamiento.

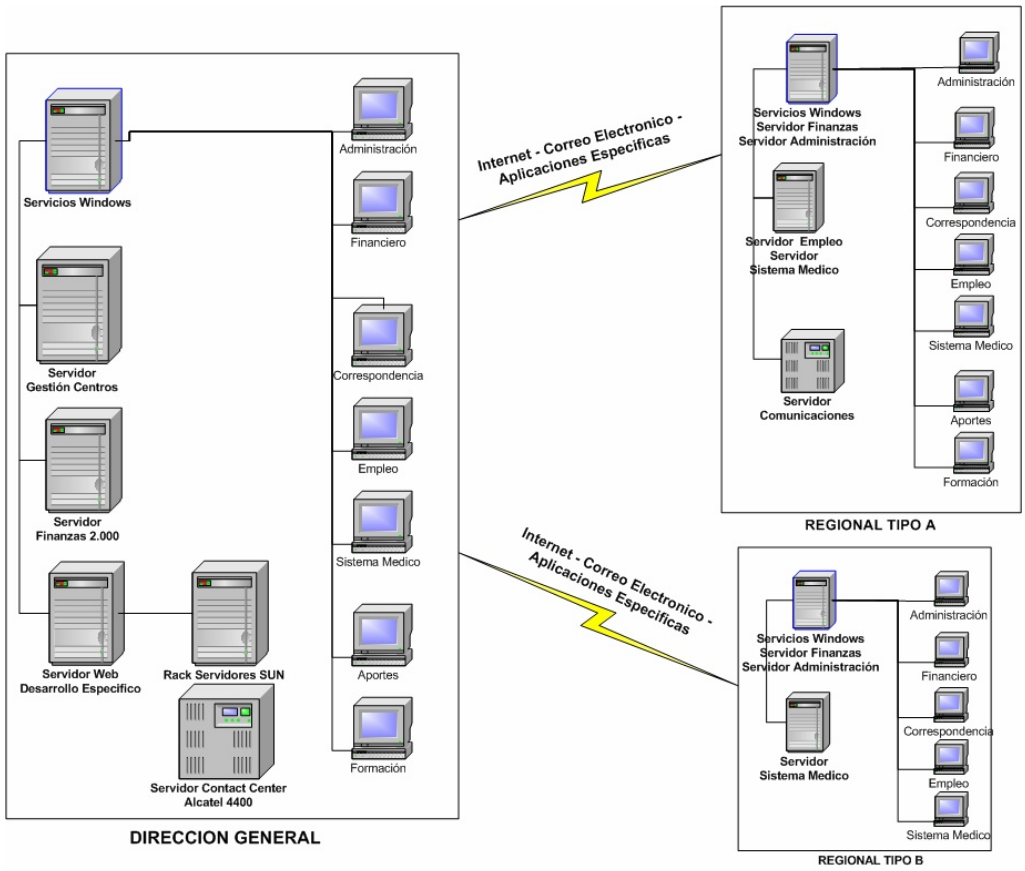


Figura 4.3. Plataforma tecnológica actual del SENA (Fuente: Archivo SENA)

Este tipo de plataforma genera ciertos inconvenientes:

- Múltiples Servidores Locales.
- Cada Regional y Seccional, requieren una infraestructura técnica de soporte.
- Información Distribuida localizada en cada uno de los servidores Regionales.
- Uso de Internet y Correo electrónico para procesos específicos y esporádicos de consolidación de datos.

- Uso Limitado, y en algunos caso ninguno, para equipos de gran capacidad y proceso en Dirección General.
- Generación e implementación de Soluciones locales, con manejo de infraestructura local, en independencia total con los demás puntos remotos, y con políticas y lineamientos centrales.
- La instalación de versiones actualizadas de las aplicaciones clientes, es un proceso tedioso que debe ser realizado por cada estación y en cada dependencia donde estén instaladas.

Las aplicaciones Clientes/Servidor son muy pesadas, robustas y rígidas, ya que incluyen toda la lógica de validación y presentación en pantalla, además, están sobre ORACLE 7.3.2 y desarrolladas con DEVELOPER 2000. También existen algunas aplicaciones Clientes/Servidor, desarrolladas con Visual Basic.

Algunos de las aplicaciones del tipo Cliente/Servidor más ampliamente utilizados por el SENA a nivel nacional y a nivel regional son:

Aplicación	Función
Gestión de Centros	Incluye los procesos de programación de acciones de los Centros y el manejo de alumnos: ingreso, situaciones académicas, registro y certificación.
Sistema Finanzas 2000	Para procesos de ejecución presupuestal, tesorería y contabilidad.
Sistema Administración 2000	Gestión de recursos físicos (compras, almacenes, inventarios, código de barras).
Sistema de Recursos Humanos	Referido a los procesos de administración del recurso humano.
Sistema de Información de Empleo	Para hacer más fácil el contacto entre los empresarios y los colombianos que buscan empleo.
Solución de Aportes	Permite realizar consultas e informes del estado de los pagos efectuados por un aportante y efectuar la depuración de cartera de Aportes Vs. la cartera de contabilidad.
Sistema Médico	Para la administración de documentos del tipo médico.
Sistema de Correspondencia	Para manejar el correo electrónico de la entidad bajo el dominio sena.edu.co y la documentación escrita de la Entidad.
Solución Proyección XXI	Para la formulación de los planes de la Entidad.

Tabla 4.3. Aplicaciones cliente/servidor SENA

A nivel nacional, el SENA ha establecido tres diferentes perfiles de usuarios, según el tipo de aplicaciones que estos utilizan en sus estaciones de trabajo:

Perfil	Localización	Aplicaciones
Usuario Administrativo	• Dirección General • Regionales / Seccionales • Centros	• Gestión de Centros • Finanzas 2000 • Administración 2000 • Kactus (Recursos Humanos) • Sistema de Información de Empleo • Aportes • Archivo y Correspondencia • Siglo XXI • Servicio Médico • Banco de Proyectos • Correo Electrónico (se espera emplear Microsoft® Exchange como estándar) • Microsoft® Office • Acceso a Internet con Microsoft® Internet Explorer • Servicio de Impresión • Aplicaciones en Oracle, empleando SQLNet. El logon es controlado por la aplicación (logon separado del de Microsoft® Windows NT) • Videoconferencia
Usuario Operativo	• Regionales / Seccionales • Centros	• Correo Electrónico (Microsoft® Exchange) • Microsoft® Office. • Acceso a Internet con Microsoft® Internet Explorer • Servicio de Impresión. • Aplicaciones en Oracle, empleando SQLNet. El logon es controlado por la aplicación (logon separado del de Microsoft® Windows NT). • Otras aplicaciones aisladas bajo Novell NetWare, o bajo UNÍX • Videoconferencia
Usuario Estudiante	• Centros	• Aplicaciones de bibliotecas con consultas a información almacenada en torres de CD-ROM • Acceso a Internet con Microsoft® Internet Explorer • Servicio de Impresión • Microsoft® Office • Videoconferencia

Tabla 4.4. Tipos de usuarios y aplicaciones SENA

4.2.4 Hardware disponible[35]

En general, la red de datos cuenta con los siguientes dispositivos:

Dispositivo	Características
Hubs	3COM Superstack HUB 40
Switches	3COM Superstack Switch 1000, Alcatel OmniStack, CISCO Catalyst
Routers	CISCO 3600 Series, CISCO 1700 Series, CISCO 1000 Series, Huawei Quidway 3600 Series
Módem	MODEM Banda Base RAD, MODEM de Radio Sagem
Servidores	Power Edge 6400, IBM Net Finity 5500, Compaq Proliant
Videoconferencia	Policom VSX7000

Tabla 4.5. Características Generales del Hardware de la Red de Datos

Los Routers Cisco 3600 y Huawei 3600 se encuentran en la Sede Administrativa y corresponden al nodo central de la red de datos. Los routers del tipo Cisco 1700 se encuentran en cada una de las sedes y son los responsables de mantener los enlaces en los nodos periféricos de la red.

El servicio de Videoconferencia sólo se tiene disponible en la Sede Administrativa, por lo tanto este equipo se encuentra ubicado en esta sede. Igualmente, los servidores están ubicados exclusivamente en la Sede Administrativa y se reparten tareas como FTP, DHCP, DNS, WINS, correo electrónico y servicio de impresión.

La información adicional relacionada con la conexión de los dispositivos dentro de la red y sus características generales, se presentarán gráficamente en los diagramas e inventarios que se incluyen en las próximas secciones y en los anexos del final del libro.

4.2.5 Routers principales

Como se anotó anteriormente, el nodo central de la red de datos del SENA REGIONAL SANTANDER, está conformado por dos routers principales ubicados en la Sede Administrativa.

El primero, un router Cisco 3640, maneja las sedes de Girón y Florida; mientras que el segundo, un router Huawei Quidway 3640, maneja el resto de las sedes y el enlace con la Dirección General en Bogotá. Estos dos routers se encuentran enlazados entre sí por medio de la red interna de la Sede Administrativa.

[35] Ver Anexo A.6. Inventario de Dispositivos

4.2.5.1 Router Cisco 3640[36]

Interconecta las sedes de Girón y Florida con la Sede Administrativa por medio de enlaces RDSI a 128 kbps.

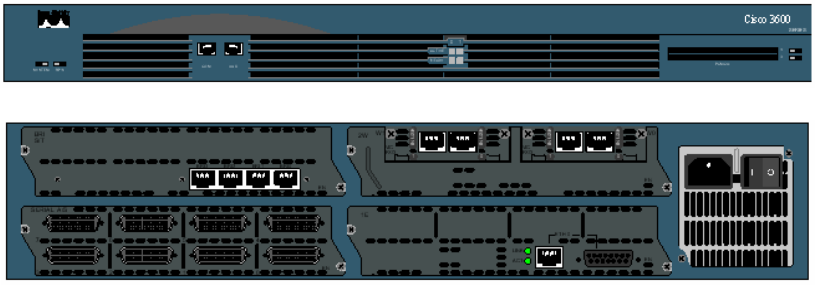


Figura 4.4. Vista Frontal y Posterior del Router Cisco 3640 (Fuente: Autores)

Como se puede observar en la vista posterior, este router cuenta con 4 slots en los que se encuentran instalados los siguientes módulos:

Slot	Descripción	Ref.	Estado
0	1 Puerto Ethernet	NM-1E	Conectado
1	8 Puertos Seriales	NM-8A/S	Desconectado
2	4 Puertos de Voz	NM-2V	Desconectado
3	4 Puertos BRI	NM-4B-S/T	2 Conectados (Bri0-Bri1)

Tabla 4.6. Módulos Instalados en el Router Cisco 3640

De los cuales sólo se encuentran en funcionamiento los módulos 0 y 3, siendo el módulo 0 el que maneja la red interna por medio del puerto Ethernet y el módulo 3 el que interconecta las LAN de las sedes de Girón y Florida por medio de dos de los cuatro puertos BRI disponibles.

Esto hace evidente una subutilización del dispositivo, dada la cantidad de puertos desconectados y que fácilmente podrían aprovecharse para otras funciones.

Las interfaces asignadas del router son las siguientes:

Interfaz	Dirección IP	Sede	Ancho de Banda
Ethernet0	172.16.55.247	Ethernet	100 Mbps
BRI 3/0		Girón	128 kbps
BRI 3/1		Floridablanca	128 kbps

Tabla 4.7. Módulos Instalados en el Router Cisco 3640

Para más detalles sobre este router, en los anexos se incluyen la tabla de rutas y la tabla de interfaces del router.

[36] Ver Anexo A.2. Interfaces y Tablas de Rutas de los Routers

4.2.5.2 Router Huawei Quidway 3640[37]

Interconecta las sedes de Barrancabermeja, Málaga, Piedecuesta, San Gil y Vélez con la Sede Administrativa por medio de enlaces de línea dedicada a 128 Kbps, y la Dirección General con la Sede Administrativa por medio de un enlace E1 a 2 Mbps.

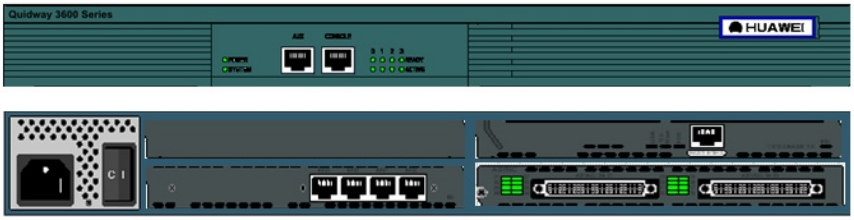


Figura 4.5. Vista Frontal y Posterior del Router Huawei 3640 (Fuente: Autores)

Al igual que el router Cisco, este router también cuenta con 4 slots en los que se encuentran instalados los siguientes módulos:

Slot	Descripción	Ref.	Estado
0	2 Puertos E1	2 E1	Conectados
1	4 Puertos BRI	4 BS	Desconectados
2	1 Puerto Ethernet	1 FE	Conectado
3	Disponible		

Tabla 4.8. Módulos Instalados en el Router Cisco 3640

En este router, los dos puertos E1 son los que manejan todos los enlaces, uno de los cuales está exclusivamente dedicado para el enlace con la Dirección General, mientras que el otro divide todo el ancho de banda del canal entre las 5 sedes que maneja.

En el archivo de configuración del router, los puertos E1 se identifican de la misma manera que los puertos seriales, por lo tanto cada sede tiene asignada una interfaz serial como sigue:

Interfaz	Dirección IP	Sede	Ancho de Banda
Ethernet0	172.16.55.254	Ethernet	100 Mbps
Serial 0/0	192.168.220.2	Dirección General (Bogotá)	2 Mbps
Serial 1/1	192.168.220.29	Piedecuesta	128 kbps
Serial 1/2	192.168.220.21	Velez	128 kbps
Serial 1/3	192.168.220.17	Sangil	128 kbps
Serial 1/4	192.168.220.5	Barrancabermeja	128 kbps
Serial 1/5	192.168.220.25	Malaga	128 kbps

Tabla 4.9. Interfaces Habilitadas Router Huawei 3640

Para más detalles sobre este router, en los anexos se incluyen la tabla de rutas y la tabla de interfaces del router.

[37] Ver Anexo A.2. Interfaces y Tablas de Rutas de los Routers

4.2.5.3 Interconexión de los Routers Principales

A continuación se presenta el esquema que resume la interconexión de cada una de las LAN pertenecientes a las Sedes del SENA REGIONAL SANTANDER, la LAN de la Sede Administrativa y la LAN de la Dirección General, mediante los dos routers principales. Se incluyen las interfaces y las velocidades de cada uno de los enlaces.

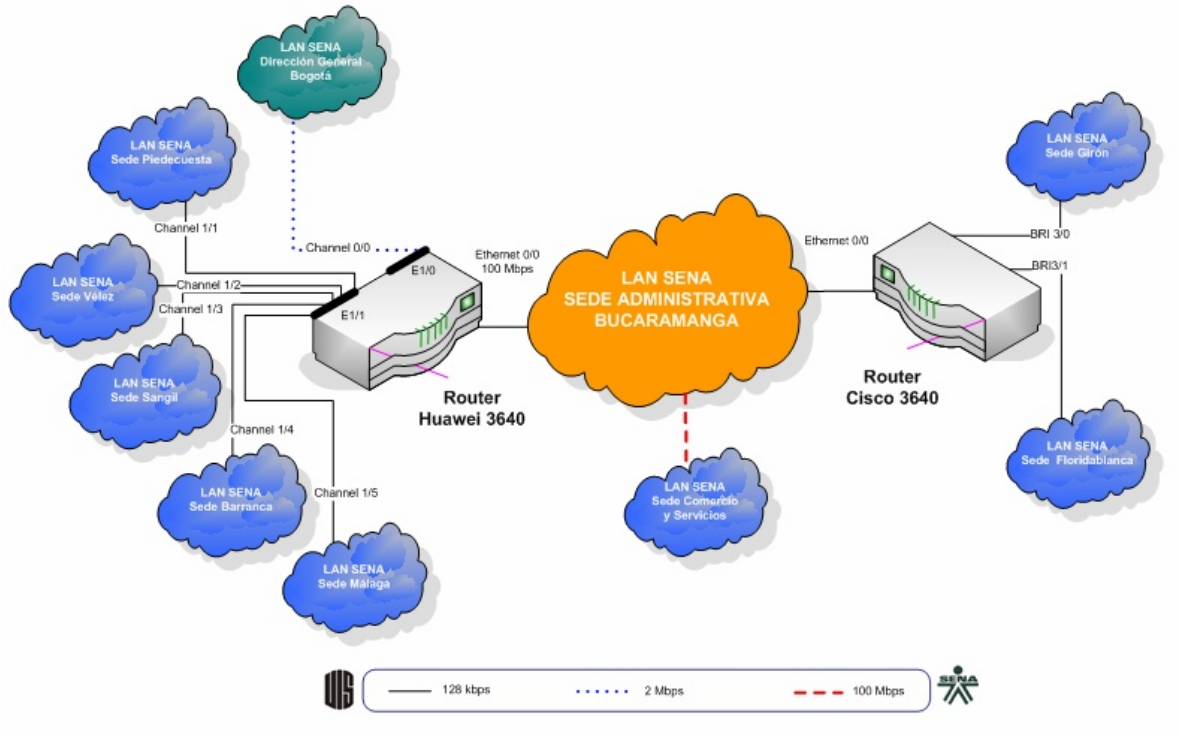


Figura 4.6. Interconexión de los Routers Principales (Fuente: Autores)

4.2.6 Enlace de conexión a Internet

En este momento, el acceso a Internet de todas las Sedes del SENA REGIONAL SANTANDER, se hace a través del Servidor Proxy de la Dirección General: Dirección IP 172.16.3.102 puerto 80, que es un Servidor Proxy AnalogX del tipo software.

Esto implica que al tráfico de aplicaciones en línea presente en el enlace entre la Sede Administrativa y la Dirección General, se le estará sumando el tráfico de Internet de toda la Red Regional, consumiendo así una franja más amplia del canal que si no se llega a priorizar puede llegar a ser crítica para el ágil funcionamiento de las aplicaciones.

Como se puede apreciar en el siguiente diagrama, todas las regionales del SENA a nivel nacional tienen la posibilidad de acceder a Internet a través del Proxy de la Dirección General. Esta conexión destina tres enlaces E1 de 2 Mbps exclusivamente para la salida a Internet de toda la Red Nacional del SENA, por medio de Colombia Telecomunicaciones S.A. ESP (TELECOM).

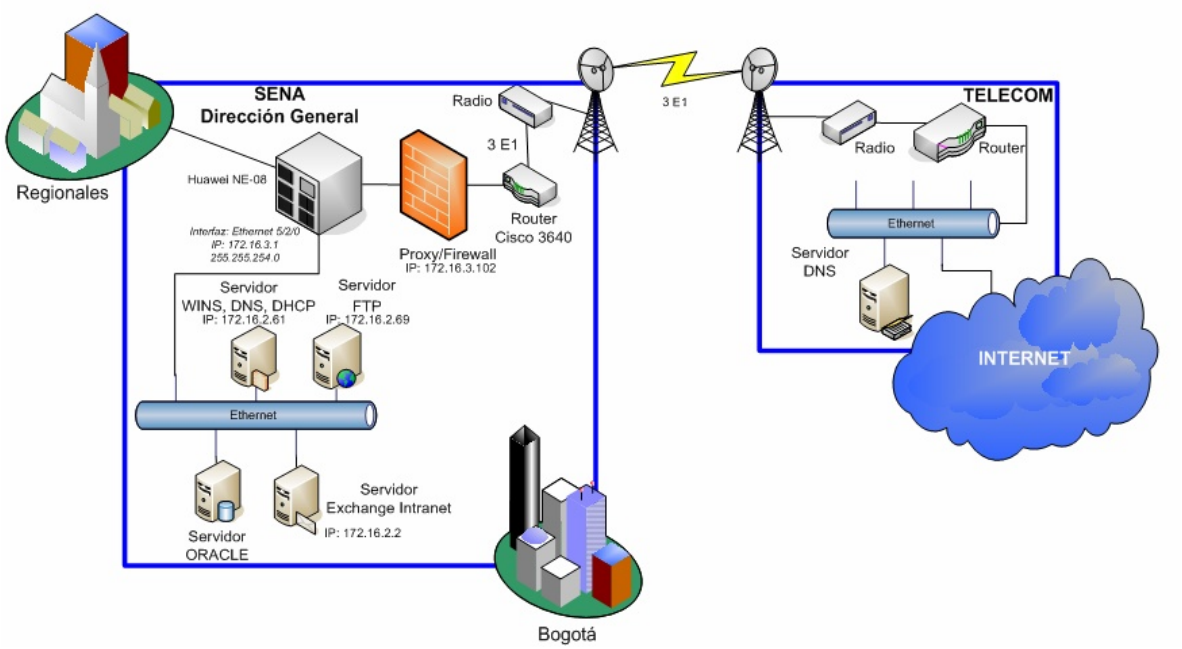


Figura 4.7. Diagrama de salida a Internet (Fuente: Autores)

4.2.7 Interconexión entre Sedes

La red de datos del SENA REGIONAL SANTANDER cuenta con dos tipos principales de enlaces entre Sedes. Un enlace tipo RDSI para las sedes de Girón y Florida, y un enlace tipo Línea Dedicada para las Sedes de Barrancabermeja, Málaga, Piedecuesta, San Gil y Vélez. Ambos tipos de enlaces cuentan con un ancho de banda de 128 Kbps y son operados por Telebucaramanga y Colombia Telecomunicaciones S.A ESP (TELECOM), respectivamente.

Para interconectarse con la Dirección General, se cuenta con un enlace dedicado E1 a 2048 Kbps y además, con un enlace de fibra óptica que interconecta el Centro de Comercio y Servicios, aprovechando su cercanía a la Sede Administrativa.

El esquema básico de la Red de Datos del SENA REGIONAL SANTANDER con sus diferentes tipos de enlaces, se muestra a continuación:

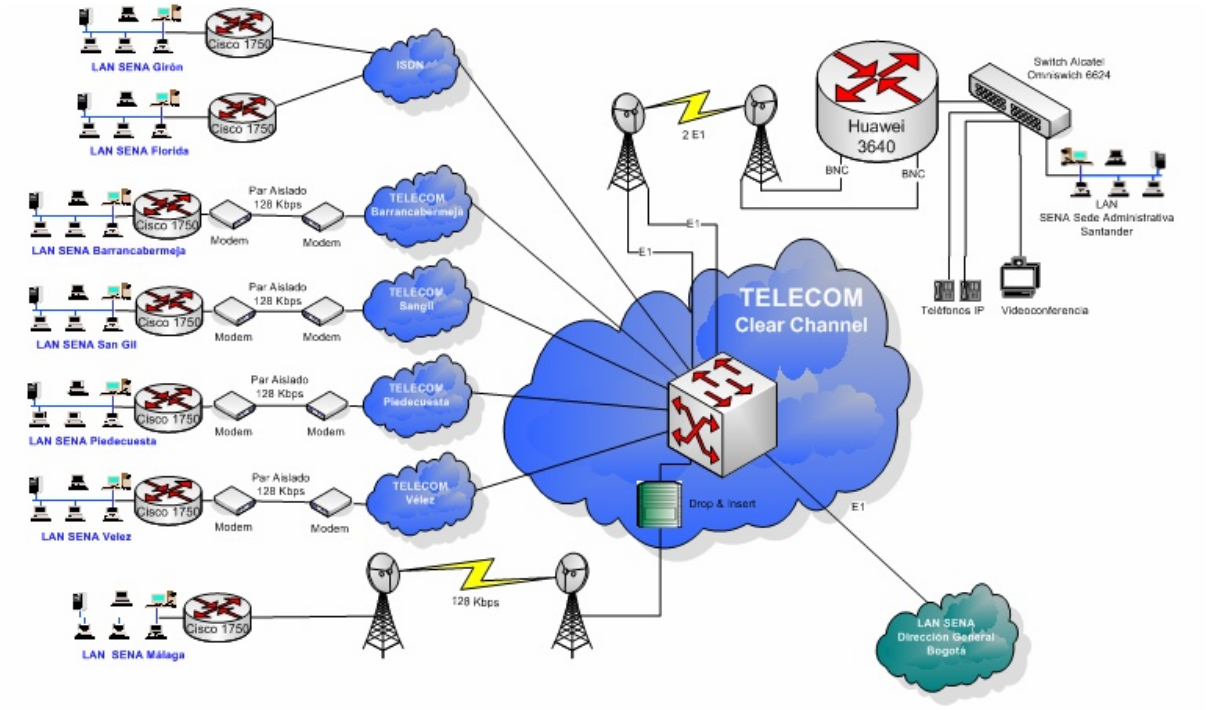


Figura 4.8. Esquema básico de la Red de Datos del SENA a nivel regional (Fuente: Autores)

4.2.7.1 Interconexión con la Dirección General

El enlace con la Dirección General se hace a través de un canal E1 de 2048 Kbps exclusivamente dedicado para tal fin. Este enlace incluye el tráfico proveniente de todas las aplicaciones en línea, videoconferencias e Internet.

Los nodos extremos de este enlace son el router Huawei 3640 ubicado en la Sede Administrativa y el Router NetEngine 08E ubicado en la Dirección General, dispositivo que maneja todos los enlaces de la red de datos a nivel nacional.

La interconexión se hace a través de los servicios de Colombia Telecomunicaciones S.A ESP. (TELECOM) ingresando por medio de microondas a su red de datos en la ciudad de Bucaramanga y posteriormente viajando por un enlace satelital hasta llegar a su destino en TELECOM Bogotá, desde donde; utilizando nuevamente microondas, el enlace se completa al llegar a la unidad ODU[38] de la Dirección General.[39]

[38] ODU : Outdoor Unit
[39] Ver 4.2.7.2. Enlace TELECOM

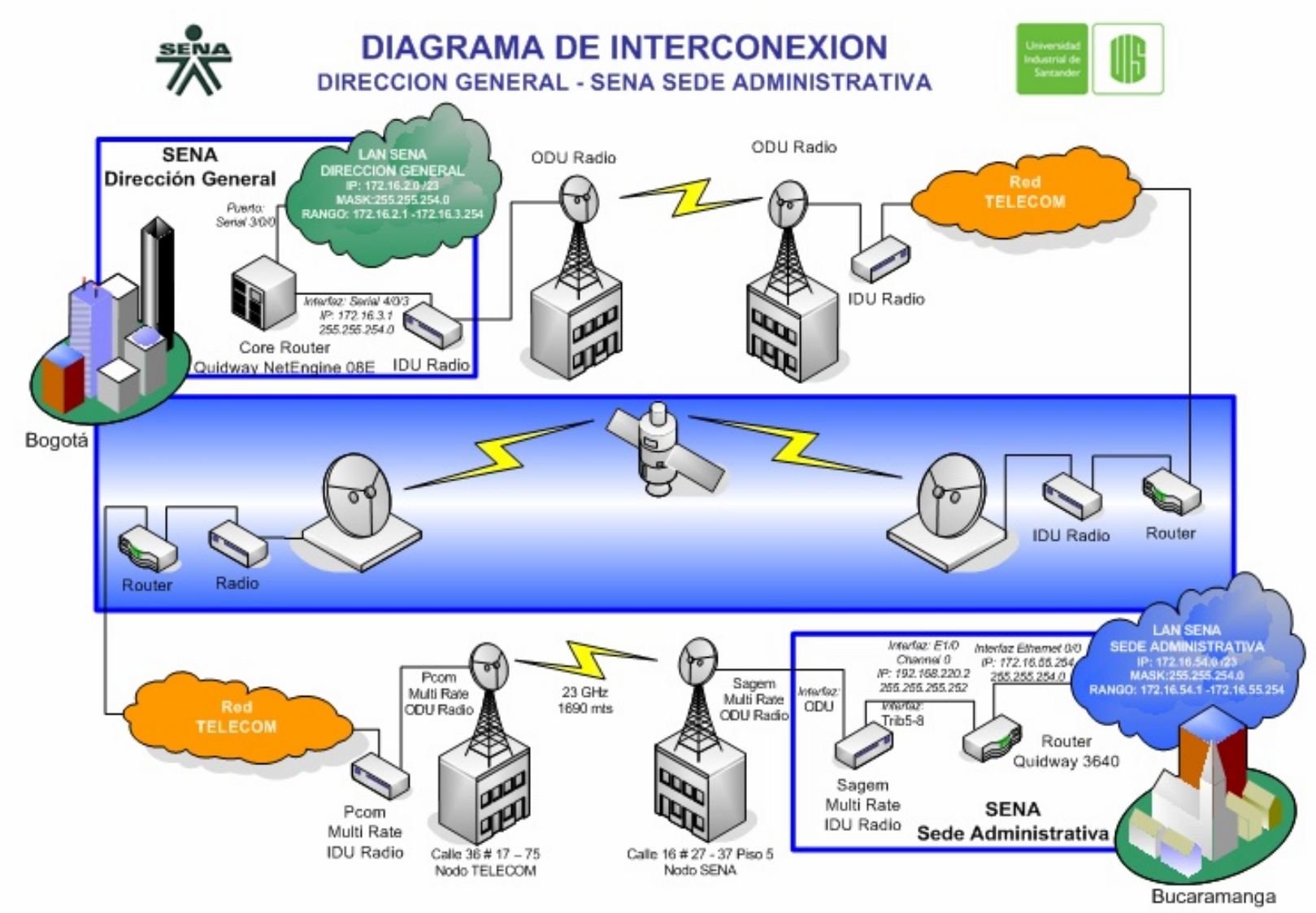


Figura 4.9. Diagrama de interconexión de la Sede Administrativa con la Dirección General (Fuente: Autores)

4.2.7.2. Enlace TELECOM

El enlace de microondas con Colombia Telecomunicaciones S.A. ESP. (TELECOM) parte de las interfaces E1 instaladas en el slot 0 del router Huawei 3640 que se conecta en la interfaz Trib 5-8 del IDU[40] Radio (Sagem) a través de conectores BNC[41]. Posteriormente la unidad IDU del radio se conecta con la unidad ODU utilizando el estándar G.703[42], por medio de un cable coaxial del tipo RG8 y envía la señal a una frecuencia de 23 Ghz hasta la unidad ODU ubicada en el edificio de TELECOM de la calle 36 con 17, por medio de la cual los datos ingresan a la red de TELECOM para ser distribuidos hacia la Dirección General o hacia los 5 centros que se manejan en este enlace.

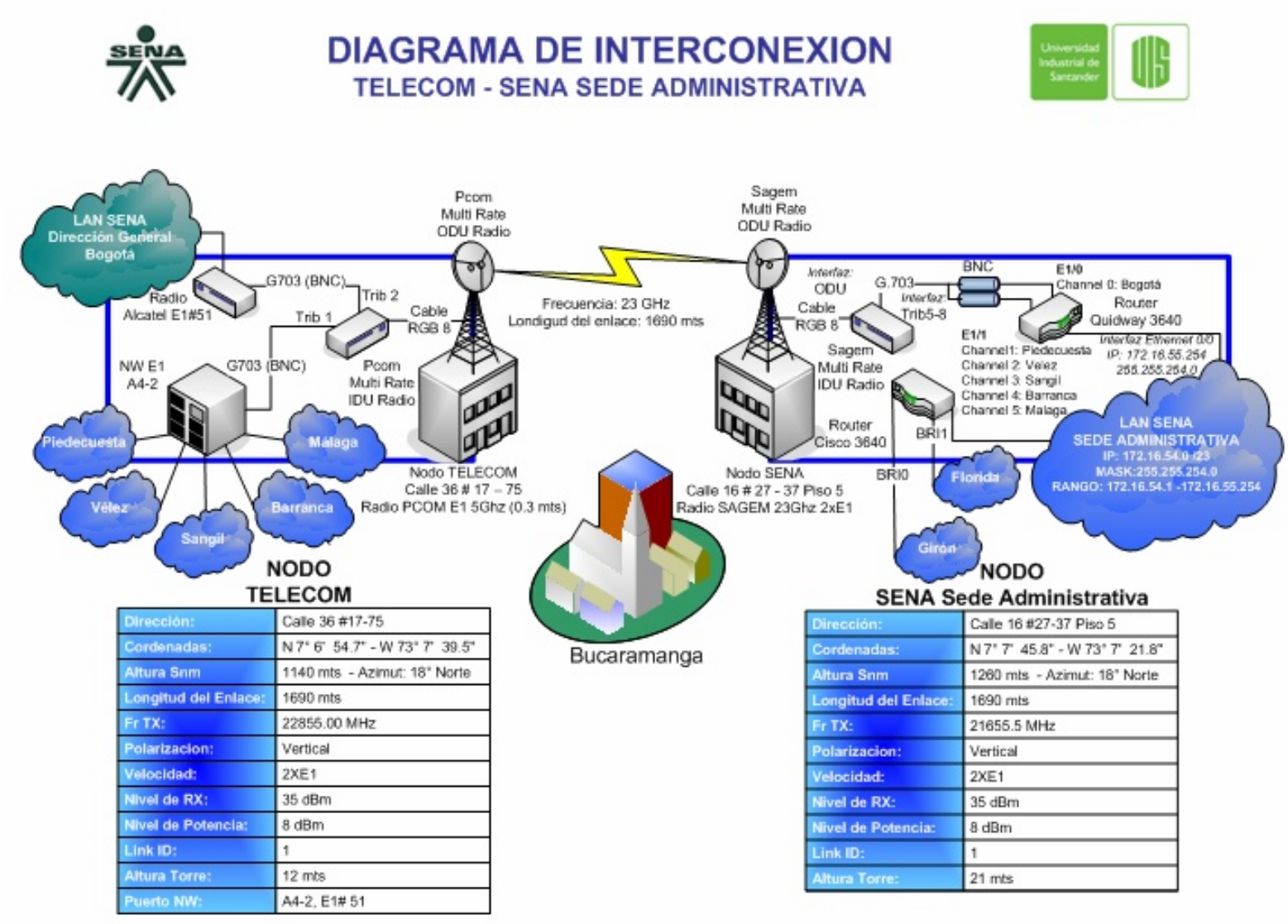
Los dos canales E1 que llegan a la red de Colombia Telecomunicaciones (TELECOM) están distribuidos de la siguiente manera: El canal que corresponde a la interfaz E1/0 del Router Huawei 3640 está dedicado exclusivamente para la interconexión con la Dirección General, por lo tanto el ancho de banda total de este enlace es de 2048 Kbps.

Mientras tanto, el ancho de banda del canal E1/1 está dividido en 5 franjas de 128 Kbps una para cada Sede de las que maneja este enlace: Piedecuesta (1), Vélez (2), Sangil (3), Barranca (4), Málaga (5), lo que da un total de 640 Kbps, que es un valor considerablemente menor al que normalmente maneja un enlace de este tipo, suponiendo la posibilidad de solicitar a TELECOM el aumento del ancho de banda en las sedes que se requiera para mejorar su conectividad.

También es importante destacar que el Multirate Radio Sagem IDU, que maneja este enlace en el nodo SENA, tiene dos canales E1 disponibles, dado que sólo se están utilizando los tributarios[43] 5 y 6 de la interfaz Trib 5-8[44], que tiene la capacidad de manejar hasta cuatro enlaces E1.

Para más detalles sobre el enlace entre el la Sede Administrativa y TELECOM, a continuación se incluye un diagrama detallado del mismo

[40] IDU: Indoor Unit
[41] BNC: British National Connector, utilizado para conectar dispositivos en red local 10BASE2 Ethernet con un cable coaxial
[42] G.703: Estándar internacional de la ITU para transferencia de datos entre dos equipos de comunicaciones a velocidades de 2 Mbps y 64 Kbps y se refiere a las señales físicas y lógicas a través de circuitos digitales
[43] Tributario: Nombre que se le da a las interfaces de los Radios Sagem
[44] Que comprende desde el Tributario 5 al Tributario 8, en total 4 canales E1



Dirección:	Calle 36 #17-75
Cordenadas:	N 7° 6' 54.7" - W 73° 7' 39.5"
Altura Snm	1140 mts - Azimut: 18° Norte
Longitud del Enlace:	1690 mts
Fr TX:	22855.00 MHz
Polarizacion:	Vertical
Velocidad:	2XE1
Nivel de RX:	35 dBm
Nivel de Potencia:	8 dBm
Link ID:	1
Altura Torre:	12 mts
Puerto NW:	A4-2, E1# 51

Dirección:	Calle 16 #27-37 Piso 5
Cordenadas:	N 7° 7' 45.8" - W 73° 7' 21.8"
Altura Snm	1260 mts - Azimut: 18° Norte
Longitud del Enlace:	1690 mts
Fr TX:	21655.5 MHz
Polarizacion:	Vertical
Velocidad:	2XE1
Nivel de RX:	35 dBm
Nivel de Potencia:	8 dBm
Link ID:	1
Altura Torre:	21 mts

Figura 4.10. Enlace SENA Sede Administrativa – Colombia Telecomunicaciones (Fuente: Autores)

4.2.8 Redes de datos de los Centros[45]

En general se identificaron dos tipos de subredes principales en el SENA REGIONAL SANTANDER, las interconectadas por RDSI[46] y las interconectadas por Línea Dedicada.

A continuación, se detallará un caso de cada tipo para no extenderse demasiado, además del detalle de la Red LAN de la Sede Administrativa. Sin embargo, la totalidad de los Diagramas de Interconexión, de Cableado y Tablas de Inventarios de las subredes de todas las Sedes se pueden consultar en el Anexo A: Documentación de la Red.

4.2.8.1 Red LAN Sede Administrativa y Centro de Comercio y Servicios

El backbone[47] de la Red Datos de la Sede Administrativa se encuentra implementado en fibra óptica y dada su cercanía, se extiende hasta el Centro de Comercio y Servicios, lo que agiliza el intercambio de datos entre las dos sedes. Esto se puede apreciar más claramente en siguiente Diagrama de Interconexión.

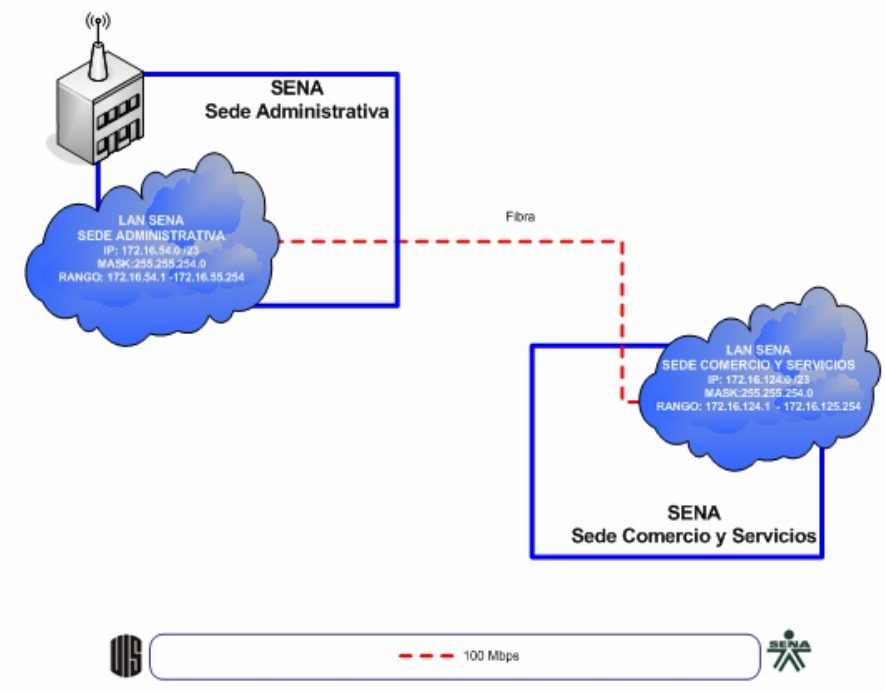


Figura 4.11. Enlace SENA Sede Administrativa – Centro de comercio y Servicios (Fuente: Autores)

[45] Ver Anexo A: Documentación de la Red
[46] RDSI: Red Digital de Servicios Integrados ó ISDN por sus sigas en inglés
[47] Backbone: Infraestructura principal de transmisión de datos de una red

Dentro de los dispositivos que manejan esta red, se encuentran los dos Routers principales, que junto a tres switches Alcatel Omniswitch 6624 de 24 puertos cuya dirección IP de administración es 172.16.55.253, conforman el núcleo de la red de donde parten todos los enlaces hacia cada una de las dependencias.

Estos switches se encuentran apilados[48] o en configuración tipo stack, lo que permite extender el número de puertos disponibles. Cuentan además, con un slot con dos puertos de fibra óptica, sumando un total de 6 puertos de donde parten directamente los 6 enlaces de fibra que conforman el backbone de la red de datos.

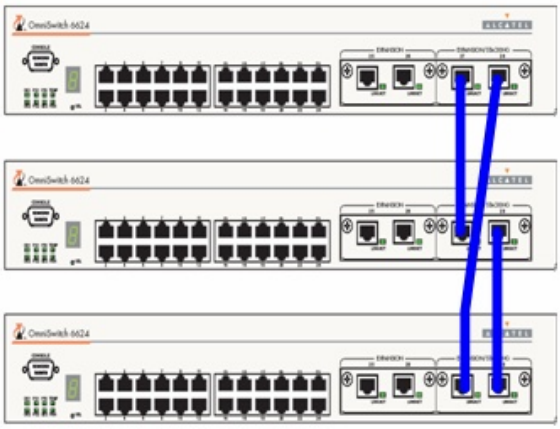


Figura 4.12. Configuración stack de los switches Alcatel (Fuente: Autores)

Cada enlace o par[49], es manejado por una bandeja de fibra óptica que se ubica dentro del rack principal[50] e interconecta cada uno de los pisos del edificio administrativo y las dos torres del Centro de Comercio y Servicios.

Bandeja de F.O.	Enlace
1	Empleo
2	Edificio admón. Piso 2
3	Edificio admón. Piso 3
4	Edificio admón. Piso 4
5	Comercio y Servicios Torre 1
6	Comercio y Servicios Torre 2

Tabla 4.10. Enlaces de F.O. de la Red LAN de la Sede Administrativa –Comercio y Servicios

[48] Esta referencia de switches permite configurar hasta 8 switches apilados o en configuración stack
[49] Se habla de "Par", por que el cable contiene dos hilos de F.O
[50] Ver Anexo A.5. Conexiones en el Rack Principal

En el otro extremo de los enlaces de fibra, se encuentra otra bandeja de fibra óptica. que interconecta los pares directamente con Switches del tipo Alcatel Omnistack 6148, que cuentan con un puerto Gigabit Ethernet, que permite conectar la fibra directamente al switch y evitar la utilización de un conversor de medios de fibra óptica a UTP.

Los Switches Alcatel que corresponden a los enlaces del Backbone de Fibra se listan a continuación

Switch	Ubicación	Dirección IP
Alcatel Omniswitch 6624	Edificio admón. Piso 5	172.16.55.253
Alcatel Omnistack 6648	Empleo	172.16.55.241
Alcatel Omnistack 6648	Edificio admón. Piso 2	172.16.55.248
Alcatel Omnistack 6648	Edificio admón. Piso 3	172.16.55.249
Alcatel Omnistack 6648	Edificio admón. Piso 4	172.16.55.250
Alcatel Omnistack 6624	Comercio y Servicios Torre 1 - Administración	172.16.55.251
Alcatel Omnistack 6624	Comercio y Servicios Torre 1 – Piso 3	172.16.55.244
Alcatel Omnistack 6624	Comercio y Servicios Torre 2 – Apoyo	172.16.55.243
Alcatel Omnistack 6648	Comercio y Servicios Torre 2 - Inglés	172.16.55.245
Alcatel Omnistack 6648	Comercio y Servicios Torre 2 - Aulas	172.16.55.246

Tabla 4.11. Switches principales de la Red LAN de la Sede Administrativa y Comercio y Servicios

Se elaboró un Diagrama de cableado básico de la Red LAN de la Sede Administrativa y del Centro de Comercio y Servicios que se presenta a continuación. En éste diagrama se puede identificar claramente el backbone de fibra y cómo está distribuido entre las dos sedes. Además, se incluyen todos centros de cableado y los dispositivos principales con sus respectivas direcciones IP y referencias, para visualizar de una mejor manera la forma como están interconectados entre sí.

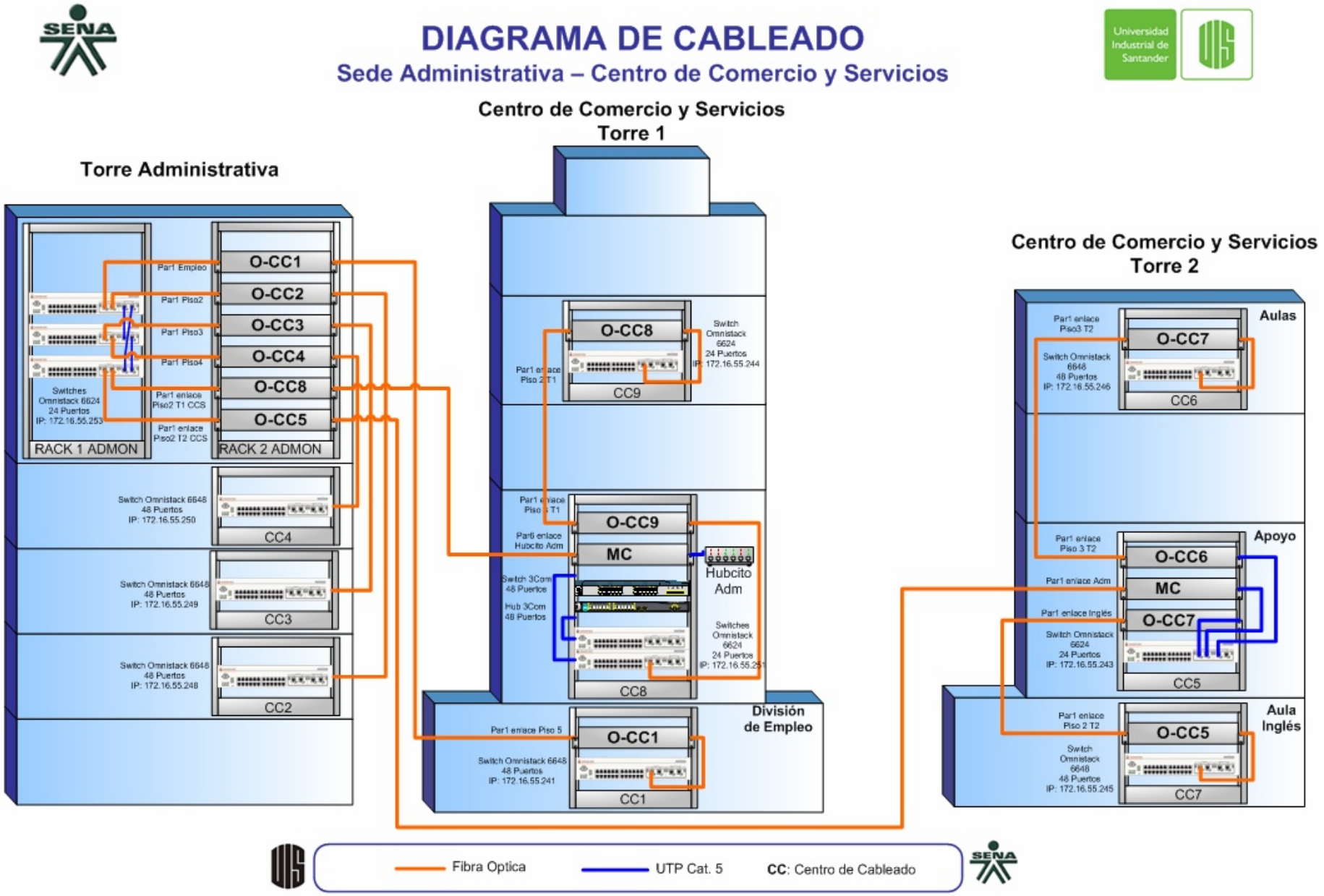


Figura 4.13. Backbone de Fibra de la Red LAN de la Sede Administrativa y el Centro de Comercio y Servicios (Fuente: Autores)

4.2.8.1.1 Inventario de dispositivos activos[51]

Igualmente, se anexa el inventario de todos los dispositivos activos, que conforman esta red de datos, necesario para la elaboración de los diagramas. Además, cabe anotar la existencia de algunos dispositivos que actualmente se encuentran desconectados y que podrían aprovecharse para reemplazos en caso de que otros fallaran o para expandir la capacidad de la red. Tal es el caso de un switch Cisco Catalyst 2900 de 24 puertos y un 3COM Cellplex 7000 que se encuentran en el Rack Principal.

Se cuenta con 3 servidores principales en funcionamiento, que se distribuyen servicios de Windows como FTP, HTTP, WINS, DNS, DHCP, Correo Electrónico basado en Microsoft Exchange y aplicaciones administrativas en Oracle.

Además, la Sede Administrativa también tiene en operación 2 teléfonos IP para comunicarse exclusivamente con la Dirección General y un equipo de Videoconferencia Policom VSX7000 que utiliza todos los días en los cursos que la requieran y en la capacitación de sus funcionarios.

4.2.8.2 Redes LAN Interconectadas por RDSI

Las redes de datos de Girón y Florida se conectan a la red LAN de la Sede Administrativa por medio de éste tipo de enlace que idealmente alcanza los 128 Kbps.

En los dos casos, el enlace parte del slot 3 del router Cisco 3640 que tiene instalado el módulo con los puertos BRI. La interfaz BRI 3/0 maneja la subred de Girón y la BRI 3/1 la de Florida.

Una vez el enlace sale de las interfaces BRI, los datos viajan a través de cable UTP hasta un convertidor Alpha Telecom EP 2300 que se encarga de transformar los cuatro cables que salen de la interfaz BRI en tan sólo dos cables para permitir su ingreso a la red telefónica de Telebucaramanga por donde el enlace seguirá su camino hasta llegar a la oficina respectiva de Telebucaramanga en Girón o Florida, según el caso. Desde allí, por par aislado de cobre, se llega a un Modem Banda Base Rad ASM 30 ubicado dentro de la

[51] Ver Anexo A.6. Inventario de Dispositivos Activos

sede SENA correspondiente. Este último a su vez, se conecta al puerto BRI de un enrutador Cisco 1750 que termina el enlace desde la Sede Administrativa al ingresar a la Red LAN de la Sede por medio del puerto Ethernet.

A continuación, se presenta el Diagrama de Interconexión de Floridablanca. El diagrama del enlace de la Sede Administrativa con Girón se incluye en los Anexos al final del presente libro.[52]

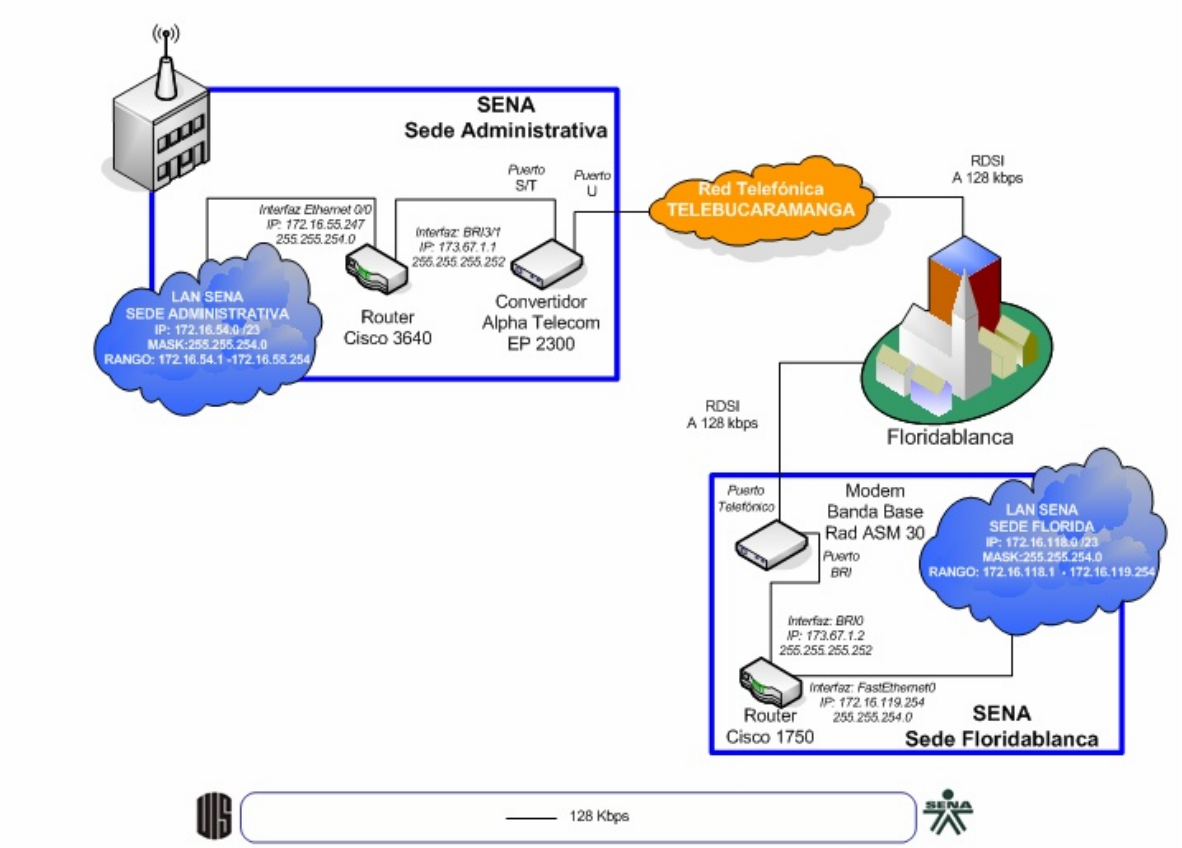


Figura 4.14. Diagrama de Interconexión entre la Sede Administrativa y la Sede Floridablanca (Fuente: Autores)

En los anexos del final del libro también se incluyen los dispositivos activos de red presentes en las redes LAN de Girón y Florida, así como un esquema básico de cableado de las mismas, que busca dar una idea de la forma como están interconectados estos dispositivos.[53] Como se puede apreciar en los diagramas, todo el cableado de las Sedes de Girón y Florida está implementado en cable UTP Categoría 5

[52] Ver Anexo A.3. Diagramas de Interconexión
[53] Ver Anexo A.4. Diagramas de Cableado y Anexo A.6. Inventario de Dispositivos Activos

4.2.8.3 Redes LAN interconectadas por Línea Dedicada

La principal diferencia entre el enlace RDSI y el de Línea Dedicada es que el enlace dedicado es de carácter permanente, mientras que el RDSI no.

Las redes LAN del SENA REGIONAL SANTANDER que se interconectan a través de Línea Dedicada son las de Barrancabermeja, Málaga, Piedecuesta, San Gil y Vélez. Para evitar extenderse demasiado, solamente se describirá un enlace de los cinco, dado que todos corresponden al mismo tipo de esquema, siendo las direcciones IP de las Redes y las interfaces lo único que cambia.

Todos los enlaces en línea dedicada son manejados por el Router Huawei 3640, que tiene destinado un enlace E1 en el slot 0 para tal fin. Este enlace está dividido en 5 franjas o canales, cada una de las cuales maneja una red LAN de una sede.

Channel	Dirección IP	Sede	Ancho de Banda
1	192.168.220.29	Piedecuesta	128 kbps
2	192.168.220.21	Velez	128 kbps
3	192.168.220.17	Sangil	128 kbps
4	192.168.220.5	Barrancabermeja	128 kbps
5	192.168.220.25	Malaga	128 kbps

Tabla 4.12. Canales del enlace E1 para cada sede

Una vez la señal sale por uno de estos canales, utiliza el enlace de TELECOM[54], descrito anteriormente en el numeral 4.2.7.2 para llegar hasta la oficina de TELECOM del municipio correspondiente. Desde allí, mediante par aislado de cobre nuevamente se enlaza la señal con un Módem Banda Base Rad ASM 30, ubicado dentro de las instalaciones de la Sede SENA, que hace la conversión de puerto telefónico a puerto RS-232[55] para conectarse con el puerto serial de un Router Cisco 1720 e ingresar a la LAN de la sede por medio de su interfaz Ethernet.

[54] Ver 4.2.7.2 Enlace TELECOM
[55] Tipo de puerto serial

A continuación, se presenta el Diagrama de Interconexión de San Gil. Los diagramas de las demás sedes se incluyen en los anexos al final del presente libro.[56]

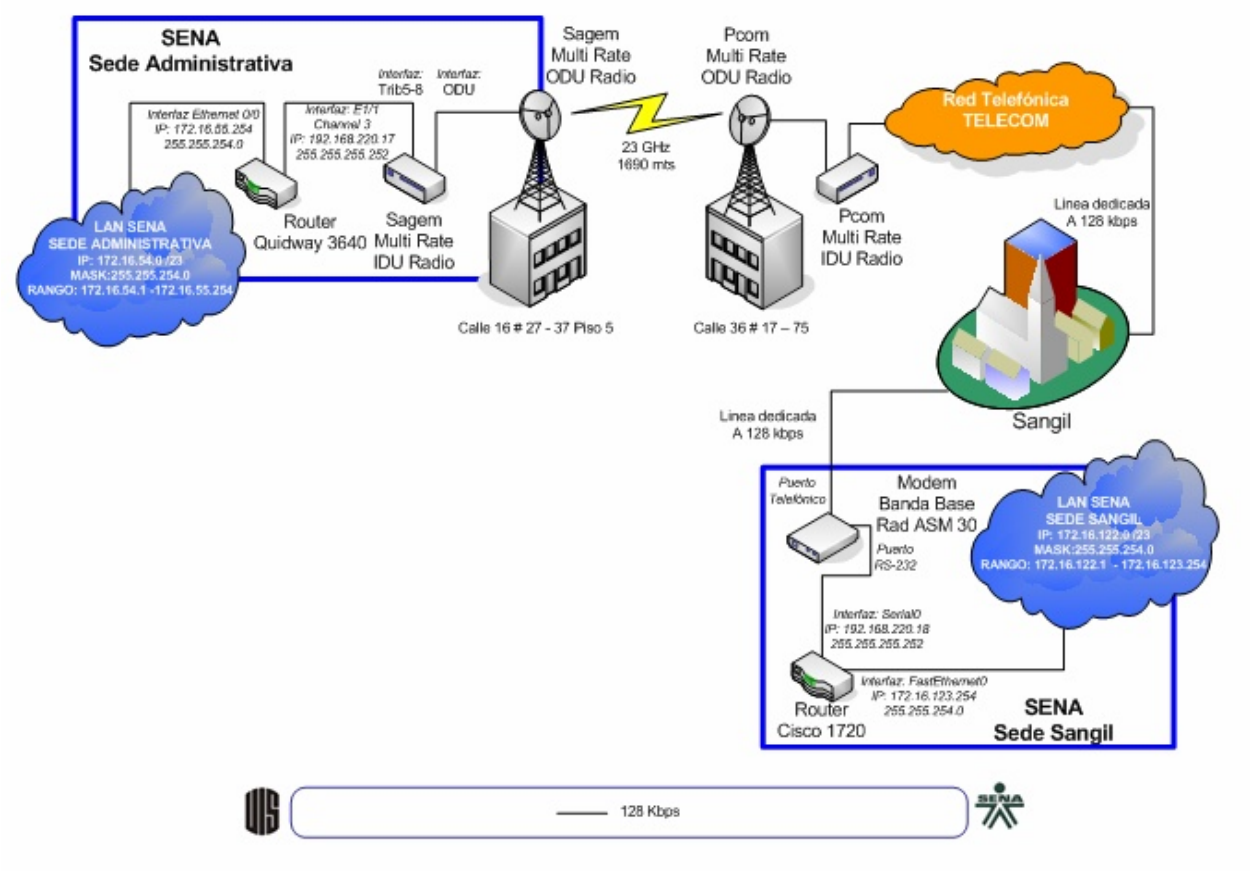


Figura 4.15. Diagrama de Interconexión entre la Sede Administrativa y la Sede San Gil (Fuente: Autores)

En los anexos del final del libro también se incluyen los dispositivos activos de red presentes en las redes LAN de Barrancabermeja, Málaga, San Gil, Piedecuesta y Vélez, así como un esquema básico de cableado de las mismas, que busca dar una idea de la forma como están interconectados estos dispositivos. [57]

Como se puede observar en los diagramas anexados de las sedes, Málaga, Piedecuesta y Vélez, su cableado está implementado en cable UTP categoría 5, mientras que Barrancabermeja y Piedecuesta cuentan con un Backbone en F.O. y cableado Cat. 5e.

[56] Ver Anexo A.3 Diagramas de Interconexión
[57] Ver Anexo A.4: Diagramas de Cableado y Anexo A.5 Inventario de Dispositivos

5. MONITOREO DE LA RED

El monitoreo tiene como objeto determinar el comportamiento de una red por medio de una recolección sistemática y un análisis del tráfico que está circulando por la misma. Una vez recolectados estos datos, deben ser interpretados para identificar fortalezas y falencias y en base a ellas tomar las decisiones más adecuadas que permitan optimizar los recursos de la red.

En un proceso de monitoreo de red, se observa y recolecta información relacionada con el comportamiento de la misma en aspectos como:

- **Utilización de enlaces**
  Su objetivo es determinar las cantidades de ancho de banda utilizado por cada uno de los enlaces de la red.

- **Caracterización del tráfico**
  Su objetivo es determinar los tipos de servicios a los que los usuarios acceden en la red como HTTP, FTP, POP3, etc.

- **Niveles de transmisión y recepción de información**
  Su objetivo es determinar los elementos de la red que atienden y realizan más solicitudes, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos de switches, routers, etc.

- **Gestión de Fallas**
  De nada sirve un buen monitoreo si no se cuenta con una solución que permita detectar, localizar y reportar fallas de manera inmediata para minimizar el tiempo de su atención. Por lo tanto es indispensable contar un tipo de monitoreo en tiempo real, que le permita conocer al administrador el estado de la red en todo momento.

En base a las ventajas que presenta y a lo mencionado anteriormente, se determinó la necesidad de realizar un monitoreo en la red de datos del SENA REGIONAL SANTANDER haciendo uso de herramientas de software, que permitieran recolectar información de todos los aspectos anteriormente descritos.

5.1 Herramientas software de monitoreo

Dentro de las herramientas de software disponibles para el monitoreo de la red, se encontraron muchas posibilidades, sin embargo se determinó como prioritario examinar solamente las de carácter gratuito o con versión de evaluación que se adaptaran a las necesidades del monitoreo.

Herramienta	Fabricante	Función	Versión Freeware	Versión DEMO
PRTG 5.3 	Paessler	• Utilización de enlaces	Funcionalidad completa limitada en número de Enlaces (2)	Funcionalidad Completa limitada en Tiempo (30 días)
Ethereal 0.99.0 	Ethereal	• Caracterización de Tráfico • Niveles de Rx y Tx	Completo	No tiene versión demo por ser completamente gratuito
OpManager 6.0 	AdventNet	• Gestión de Fallas	Funcionalidad completa limitada en número de Dispositivos (20)	Funcionalidad completa limitada en Tiempo (30 días)

Tabla 5.1. Características de las Herramientas de Monitoreo

Cada una de las herramientas se utilizó para cumplir con una función específica de monitoreo.

Las versiones que se utilizaron del PRTG, Ethereal y OpManager, pueden ser descargadas de los siguientes enlaces, respectivamente:
http://www.ethereal.com/distribution/win32/ethereal-setup-0.99.0.exe
http://download.paessler.com/download/prtg.zip
http://download.adventnet.com/products/opmanager/29809517/AdventNet_ManageEngine_OpManager_6_windows.exe

A continuación, se presenta una breve descripción de cómo se utilizaron y los resultaron que se obtuvieron con cada una de ellas.

5.2 Utilización de enlaces (Monitoreo con PRTG)

El Monitoreo con PRTG se realizó para determinar el comportamiento a través del tiempo del tráfico de los enlaces más importantes presentes en la Red de Datos del SENA REGIONAL SANTANDER.

Se identificaron un total de 10 enlaces principales en la red:

Enlace	Ancho de Banda	Router	Interfaz[58]	Comunidad SNMP[59]
Router Huawei	100 Mbps	172.16.55.254	Ethernet0	senalcatel
Router Cisco	100 Mbps	172.16.55.247	Ethernet0	secalcatel
Sede Administrativa – Dirección General	2048 Kbps	172.16.3.1	Serial 4/0/3:0	senalcatel
Sede Administrativa – Floridablanca	128 Kbps	172.16.119.254	Fa0	senalcatel
Sede Administrativa – Girón	128 Kbps	172.16.117.254	Fa0	senalcatel
Sede Administrativa – Barrancabermeja	128 Kbps	172.16.115.253	Fa0	senalcatel
Sede Administrativa – Málaga	128 Kbps	172.16.183.254	Fa0	senalcatel
Sede Administrativa – Piedecuesta	128 Kbps	172.16.178.254	Fa0	senalcatel
Sede Administrativa – San Gil	128 Kbps	172.16.123.254	Fa0	senalcatel
Sede Administrativa – Vélez	128 Kbps	172.16.131.254	Fa0	senalcatel

Tabla 5.2. Características de los enlaces

Para añadir los enlaces en el PRTG es necesario identificar la dirección IP del router del extremo opuesto del enlace, su comunidad SNMP y la interfaz que va a ser analizada

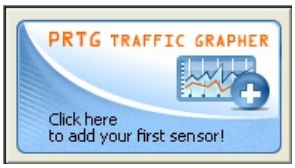
Una vez obtenidos estos datos, se procede a incluir uno a uno los enlaces en la interfaz del PRTG, procedimiento que se describe a continuación

[58] Ver Anexo A.2. Interfaces y Tablas de Rutas de los Routers
[59] El monitoreo de un dispositivo a través del protocolo de gestión de redes SNMP: Simple Network Management Protocol, requiere la autentificación por medio de una contraseña que se denomina “Comunidad” o en inglés, “Community String”.

5.2.1 Manejo del PRTG Traffic Grapher

Para monitorear el tráfico de un enlace en PRTG seguimos los siguientes pasos:

1. Ejecutar el PRTG Traffic Grapher haciendo click en el icono correspondiente



2. Hacer click en “Click here to add your first sensor”

3. En la ventana “Add Sensor Wizard” dar click en “Next”

4. En la ventana “Data Adquisition Type” dejar seleccionada la opción “SNMP” y hacer click en “Next”

5. En la ventana “Sensor Type Selection” dejar seleccionada la opción “Standard SNMP Traffic Sensor” y hacer click en “Next”

6. En la ventana “Device Selection” introducir los datos del enlace y dar click en “Next”

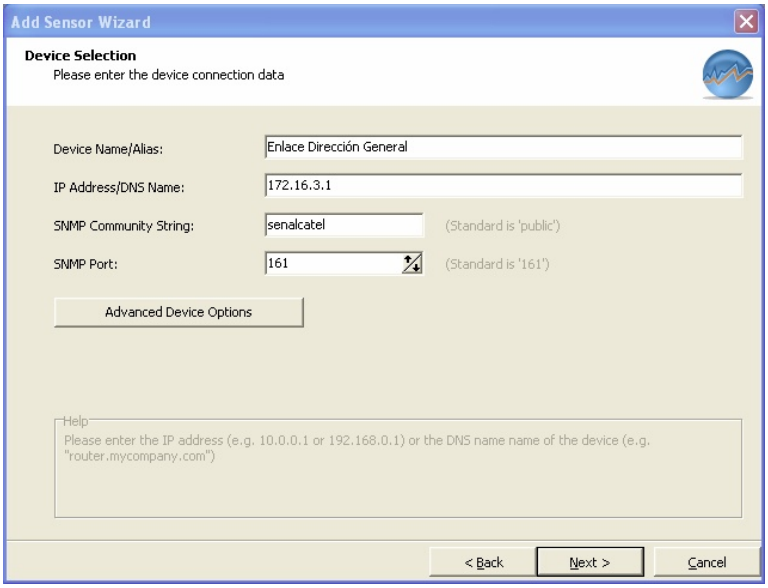


Figura 5.1. Ventana Add Wizard del PRTG (Fuente: Autores)

Después de unos segundos y sólo si se logra establecer una comunicación con el dispositivo, se abrirá la ventana “Port Selection” en la que se debe seleccionar el puerto que se desea monitorear y el tipo de monitoreo en la lista desplegable. (Bandwidth, Unicast-Packets/s, Non-Unicast-Packets/s, Errors/min)

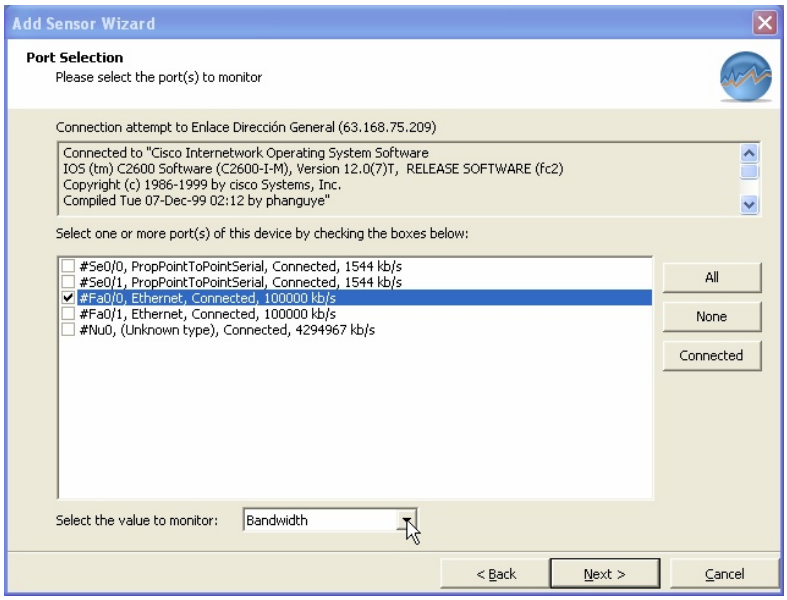


Figura 5.2. Ventana Add Sensor Wizard del PRTG (Fuente: Autores)

7. En la ventana “Aditional Settings”, hacer click en “Finish” e inmediatamente dará inicio al monitoreo del enlace.

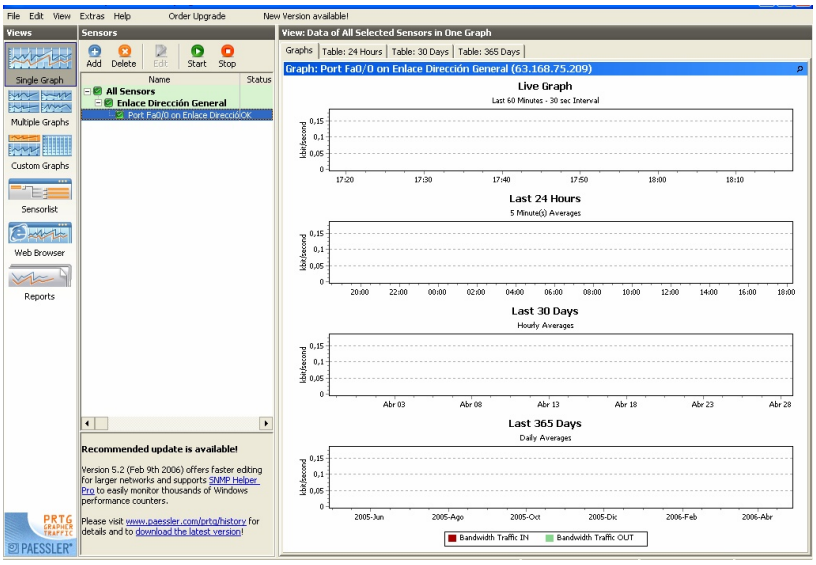


Figura 5.3. Ventana principal del PRTG (Fuente: Autores)

Este proceso deberá repetirse para añadir cada uno de los enlaces que se requieran.

5.2.2 Resultados

Para determinar el comportamiento de cada uno de los enlaces, se monitorearon durante 30 días, en el periodo comprendido entre el 25 de Febrero y el 26 de Marzo de 2006. La totalidad de las gráficas obtenidas se presenta al final del presente libro en los anexos.[60]

PRTG también permite tabular el total de tráfico enviado y recibido por cada uno de los enlaces y la velocidad promedio de transmisión y recepción durante lo 30 días del monitoreo. A continuación se presentan estos resultados:

Enlace	Tráfico Enviado		Tráfico Recibido	
	Bytes Transmitidos (kbyte)	Velocidad (Kbps)	Bytes Transmitidos (kbyte)	Velocidad (Kbps)
Ethernet Huawei	37´592.390,825	134,815	86'810.917,672	311,428
Ethernet Cisco	5´000.990,760	17,917	1´337.351,226	4,790
Dirección General	97'186.754,001	367,396	30'509.185,609	115,376
Floridablanca	533.161,151	1,939	2´038.849,240	7,440
Girón	825.132,145	3,099	2´398.983,284	9,159
Barrancabermeja	1´867.993,034	7,101	4´925.318,002	18,686
Málaga	991.852,304	3,820	4´103.006,334	15,540
Piedecuesta	1´281.478,715	4,913	3,103.823,458	11,784
San Gil	1´332.941,223	5,759	4´398.486,999	18,774
Vélez	1´013.310,065	4,394	4´431.692,293	19,587

Tabla 5.3. Resultados del Monitoreo con PRTG – 30 días

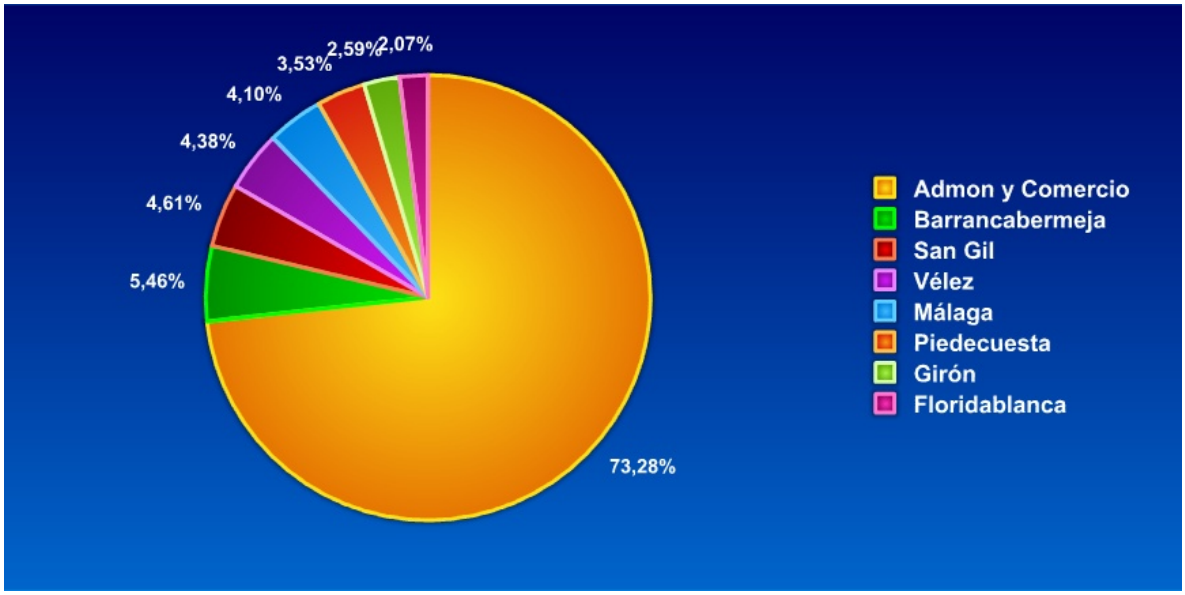


Figura 5.4. Porcentaje de Tráfico en las Sedes (Fuente: Autores)

Como se muestra en la tabla anterior, los enlaces que más tráfico manejan son: el enlace Ethernet del router Huawei, que incluye todo el tráfico correspondiente a las subredes de

[60] Ver Anexo B.1. Resultados gráficos de la utilización de los enlaces – 30 días

la Sede Administrativa, Centro de Comercio y Servicios y la porción de tráfico que corresponde a Internet de las Sedes de Girón y Florida; y el enlace del Router NE-08 de la Dirección General, que interconecta la red del SENA REGIONAL SANTANDER con la red de datos nacional.

Para visualizar con mayor claridad las sedes que manejan una mayor cantidad de tráfico, en la figura 5.4, se presenta el tráfico total para cada enlace de las Sedes (tráfico enviado + tráfico recibido) durante el mes en el que se realizó el monitoreo con el PRTG. Los resultados revelan que las sedes de mayor tráfico corresponden a las de la Sede Administrativa y el Centro de Comercio y Servicios, seguidas por las de Barrancabermeja, San Gil y Vélez.

También se observa claramente que los enlaces de menor tráfico y de menores tasas de transferencia son los implementados en RDSI de Girón y Florida que se manejan a través del Router Cisco, lo cual se hace evidente, dado que en la tabla 5.3 la suma de los bytes transmitidos de estas dos sedes es aproximadamente igual a la cantidad de bytes transmitidos por el router. La diferencia, corresponde a los bytes de la red LAN de la Sede Administrativa, la cual es una cantidad mínima para este dispositivo.

En el caso del Router Huawei, la suma del tráfico de los enlaces que maneja es mucho menor al total de bytes transmitidos y recibidos por la interfaz Ethernet del router, dado que en este caso, además de manejar los enlaces de Barranca, Málaga, Piedecuesta, San Gil y Vélez, maneja las peticiones de las redes LAN de la Sede Administrativa y la Sede de Comercio y Servicios.

Los datos presentados revelan que las tasas de transferencia que se manejan en promedio, están muy por debajo de las ideales, incluso en el enlace con la Dirección General. Sin embargo, hay que tener en cuenta que el monitoreo también incluyó el tráfico correspondiente a horarios no laborales, como nocturnos, domingos y festivos, lo que modifica el resultado del cálculo de la velocidad promedio para cada una de las sedes.

Para tener una mejor idea de estos valores, se analizaron nuevamente todos los enlaces en horario laboral, es decir, de 8 AM a 6 PM durante uno de los días de mayor tráfico, por ser fin de mes; el 28 de febrero de 2006. Se aprovechó la carácterística que incluye en

PRTG para calcular la velocidad de transferencia según la regla del 95% percentil[61], utilizada por la mayoría de los proveedores de servicios de red para tarificar la prestación de sus servicios. Los resultados presentan unas tasas de transferencia por debajo de lo normal (128 Kbps) para las sedes de Girón y Florida.

Enlace	Tráfico Enviado + Tráfico Recibido		
	Bytes (kbyte)	Velocidad (Kbps)	95% (5 min) (Kbps)
Ethernet Huawei	8,659.641,440	821,221	2.087,398
Ethernet Cisco	430.300,705	40,807	115,356
Dirección General	8,171.554,797	774,902	2.055,920
Florida	236.847,710	22,916	71,855
Girón	163.489,533	16,969	70,696
Barranca	517.247,728	49,653	138,442
Málaga	247.773,542	23,671	107,098
Piedecuesta	323.868,888	30,951	110,173
San Gil	245.505,406	24,798	106,553
Vélez	442.876,596	44,895	133,123

Tabla 5.4. Resultados del Monitoreo con PRTG – 1 día

A continuación, incluímos las gráficas resultantes de los enlaces ethernet de cada uno de los routers para así tener una idea más clara de su comportamiento en horario laboral. En los anexos se incluyen todas las gráficas correspondientes a este análisis[62].

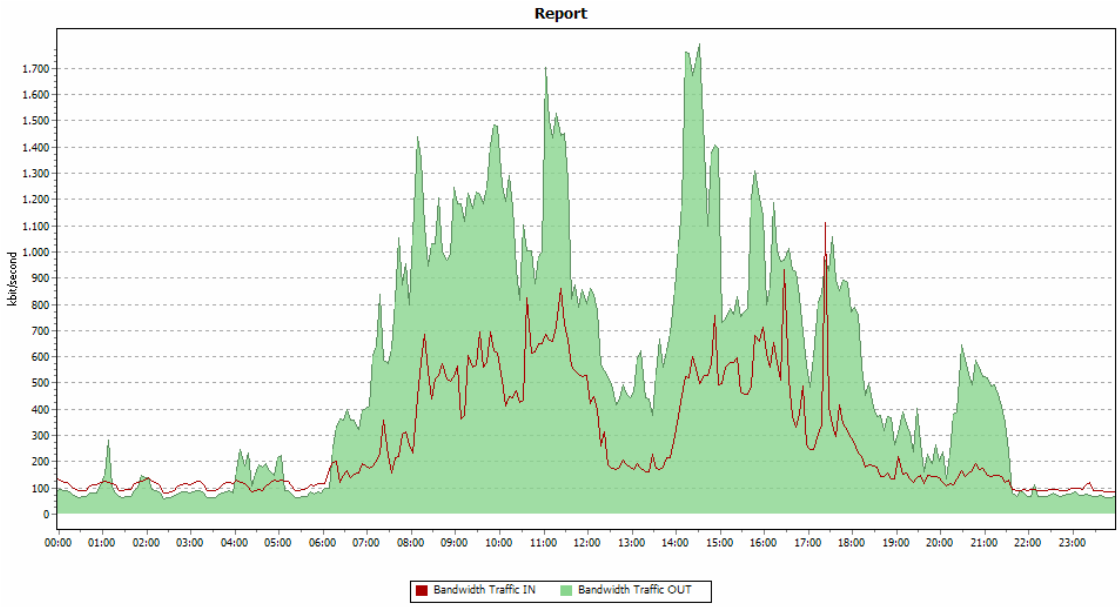


Figura 5.5. Comportamiento diario del puerto Ethernet del router Huawei (Fuente: Autores)

[61] En la regla del 95 percentil se elimina del cómputo del ancho de banda consumido, el 5% de las muestras de mayor tráfico tomadas cada minuto. Dependiendo del proveedor, se hacen mediciones cada 5 mins del ancho de banda que se está usando. Estas mediciones se ordenan de mayor a menor y de todas las medidas se quitan el 5% más alto. El valor facturado corresponde al ancho de banda de la inmediatamente superior.

[62] Ver Anexo B.1. Resultados gráficos de la utilización de los enlaces – 1 día

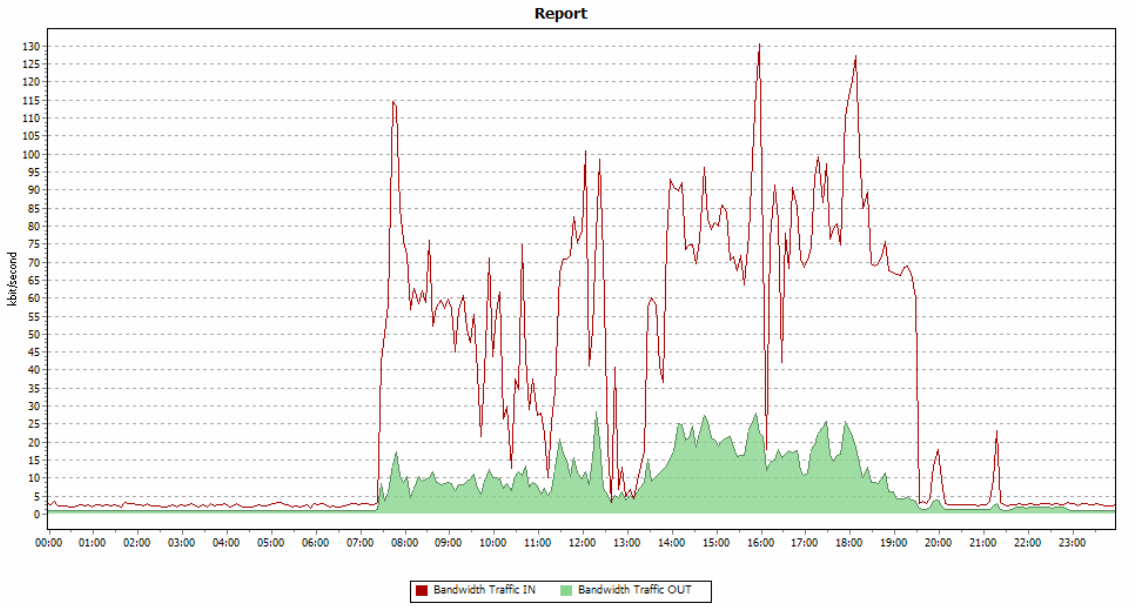


Figura 5.6. Comportamiento diario del puerto Ethernet del router Cisco (Fuente: Autores)

Las dos figuras anteriores revelan que la actividad plena en los enlaces incia aproximadamente a las 8 de la mañana y finaliza a las 6 de la tarde, con un pronunciado decaimiento en la actividad entre las 12 del medio día y las 2 de la tarde.

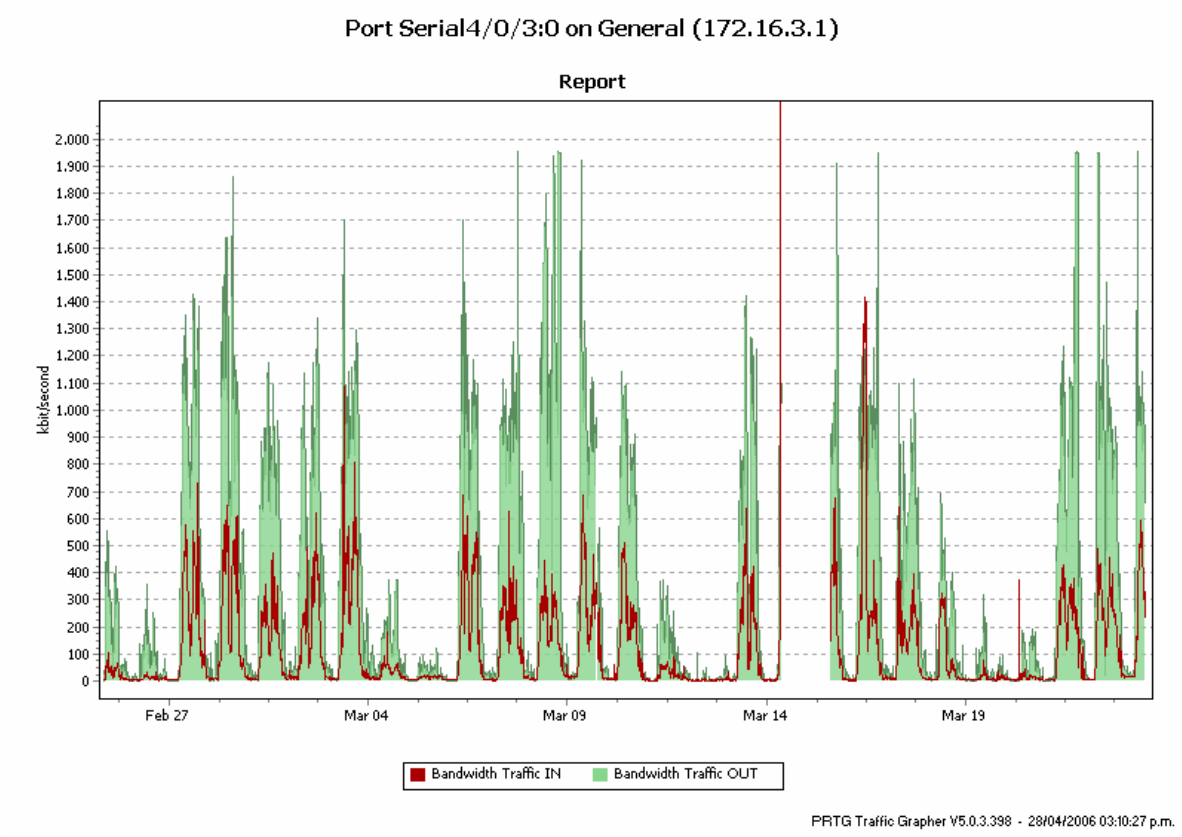


Figura 5.7. Monitoreo del tráfico del enlace con la Dirección General (Fuente: Autores)

Las gráficas también proveen una idea del comportamiento de los enlaces durante cada uno de los días del monitoreo. En ellas es posible identificar cinco picos consecutivos muy pronunciados, que corresponden a los días laborales (Lunes, Martes, Miércoles, Jueves y Viernes), y dos picos de menor tamaño, que se relacionan con los fines de semana, en los que siempre el primero es más alto que el segundo debido a que, aunque muy reducida en comparación a la de los días laborales, la actividad en cada una de las sedes es mucho mayor un sábado que un domingo o que un festivo.[63]

Esta condición se cumple en la mayoría de los enlaces, con excepción del enlace con San Gil[64], en el que se observa un comportamiento del tráfico constante durante todos los días de la semana, por lo que se podría pensar que en días no laborales, el enlace se está destinando para otros usos.

Otra ventaja que ofrecen las gráficas es la identificación de fallos en los enlaces, como por ejemplo el ocurrido entre los días 14 y 15 de marzo, que se puede observar como una interrupción o una atenuación del tráfico en todas las gráficas.

Este fallo[65] se debió a un problema en el Sagem Multi Rate IDU de la Sede Administrativa, por esa razón sólo se observan cortes en las gráficas correspondientes a los enlaces de las sedes que maneja el Router Huawei, mientras que en los de Girón y Florida, que son manejados por el Router Cisco, sólo se advierte una pequeña atenuación. [66]

5.3 Caracterización del tráfico (Monitoreo con Ethereal)

Ethereal es una herramienta que permite capturar todo el tráfico que circula a través de la interfaz de red del equipo en el que se encuentra instalado. Una vez se realicen estas capturas, es posible analizarlas elaborando un trabajo estadístico que permita identificar los servicios más utilizados por los usuarios de la red por medio de la asociación con sus respectivos protocolos, así como también, la identificación de los elementos de la red que envían y reciben más tráfico. Además, también se puede realizar un análisis en cuanto a los modos de direccionamiento del tráfico y al tamaño de los paquetes que circulan por el enlace.[67]

[63] Como se puede observar en todas las gráficas, al ubicarse en el día 20 de marzo, que correspondió a un festivo nacional.
[64] Ver Anexo B.1. Resultados gráficos de la utilización de los enlaces - Enlace con San Gil
[65] Este fallo sólo se pudo resolver hasta que personal capacitado de TELECOM acudió a prestar la asesoría.
[66] Ver Anexo B.1. Resultados gráficos de la utilización de los enlaces
[67] Broadcast, Multicast o Unicast

Dado que en la red de datos del SENA REGIONAL SANTANDER se cuenta con dos routers principales y cada uno enlaza diferentes sedes, se hace necesaria la captura del tráfico que circula por ambos dispositivos.

5.3.1 Enlaces a capturar

Se determinó capturar todo el tráfico que fluye por los enlaces entre las interfaces Ethernet de los Routers y los Switches Alcatel OmniSwitch 6624 que se encuentran apilados conformando el core[68] de la red LAN (172.16.55.253).

5.3.1.1 Enlace Router Cisco

Corresponde a la interconexión presente entre la interfaz Ethernet del Router Cisco 3640 y el Puerto 2 de los Switches Alcatel.

La captura en este enlace permite observar todos los paquetes que viajan desde y hacia las redes LAN de Girón y Florida. Esto se debe a que todo el tráfico, incluyendo el tráfico de Internet, entra a la Red LAN de la Sede Administrativa por el puerto Ethernet de este router. En el caso del tráfico de Internet, dado que la salida se realiza por el Proxy de la Dirección General, los paquetes correspondientes tienen que ingresar al Router Huawei a través de su interfaz Ethernet y seguir hacia Bogotá para llegar hasta Internet.

5.3.1.2 Enlace Router Huawei

Corresponde a la interconexión presente entre la interfaz Ethernet del Router Huawei 3640 y el Puerto 1 de los Switches Alcatel.

A diferencia del enlace en el router Cisco, la captura en este enlace es limitada y solamente permite observar el tráfico total de la Red LAN de la Sede Administrativa y del Centro de Comercio y Servicios. Además, por las razones explicadas anteriormente, en este enlace se observará también todo el tráfico de Internet proveniente de las Sedes de Girón y Florida.

En cuanto a las Sedes de Barrancabermeja, Málaga, Piedecuesta, San Gil y Vélez, en este enlace sólo se podrán observar los paquetes que ingresan a la Red LAN de la Sede

[68] Núcleo de la red

Administrativa, debido a que todo el tráfico de Internet es redireccionado internamente por el mismo router hacia la interfaz Serial0/0[69] que enlaza los datos con el Proxy de la Dirección General.

5.3.2 Métodos de captura

Teniendo en cuenta lo anterior, se hace necesaria la búsqueda de un método que permita enviar todo el tráfico de estos dos puertos, hacia la interfaz de red de la estación de trabajo en la que se tiene instalado Ethereal.

5.3.2.1 Port Mirroring[70]

En un switch, el método de Port Mirroring consiste simplemente en realizar una copia de todo el tráfico que entre y salga por un puerto del switch y redireccionarlo internamente hacia otro. Una vez realizado este proceso, se podrá conectar un equipo de monitoreo a este puerto para realizar las capturas correspondientes.

La implementación de ésta técnica varía según el fabricante y normalmente sólo se puede realizar ingresando a la configuración del switch, ya sea por el puerto consola, por telnet o por Web, para modificar algunos parámetros que en caso de no tener el conocimiento adecuado, pueden introducir fallos en el dispositivo. Esto implica una documentación adecuada según los manuales del switch.

En los anexos[71] se incluye el procedimiento requerido para configurar un Port Mirror o Puerto Espejo en los tres switches Alcatel Omniswitch 6624 que conforman el núcleo de toda la Red de Datos del SENA REGIONAL SANTANDER.

Sin embargo, no fue posible realizar este procedimiento, debido a que los dispositivos principales de la Red LAN del SENA REGIONAL SANTANDER, como Routers y Switches, no son administrados por la Oficina de Sistemas, sino por TELECOM, por lo tanto se requería de una autorización externa a la Entidad, que no fue posible conseguir.

Por esta razón, fue necesaria la consideración de otro de los métodos más comúnmente utilizados para redireccionar el tráfico de un puerto a otro.

[69] Ver Anexo A.2.2 Router Quidway 3640 – Sede Administrativa (IP: 172.16.55.254)
[70] Ver Anexo B.4. Configuración de un puerto espejo en un switch Alcatel Omniswitch 6624
[71] Ver Anexo B.4. Configuración de un puerto espejo en un switch Alcatel Omniswitch 6624

5.3.2.2 Inserción de un Hub en el enlace

Este método consiste en ubicar estratégicamente un Hub entre el puerto Ethernet del Router y el puerto del Switch, permitiendo la conexión del equipo de monitoreo en cualquiera de los puertos libres en el Hub, en los que gracias a su comportamiento como repetidor, se verá exactamente el mismo tráfico que está fluyendo en el enlace entre el puerto Ethernet del Router y el Switch.

A continuación se presenta un esquema que ilustra la implementación del método, aplicado específicamente para el análisis de los dos enlaces requeridos

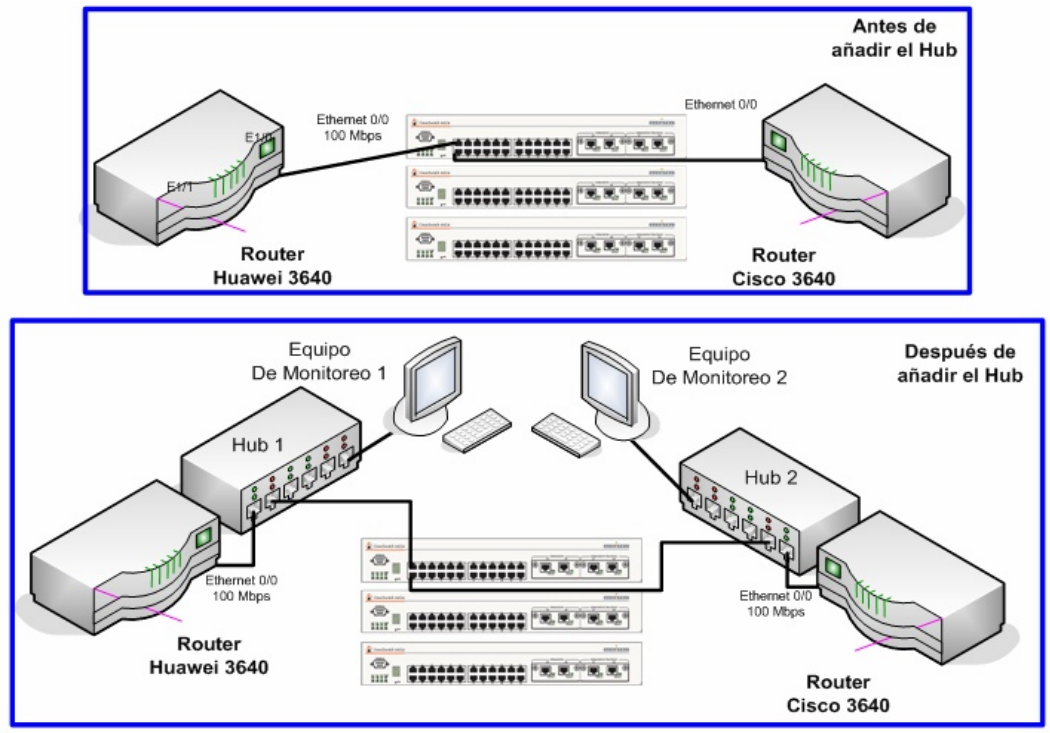


Figura 5.8. Inserción de un Hub en los enlaces principales de la Red (Fuente: Autores)

Una de las desventajas que presenta éste método en comparación al de Port Mirror, es que en este caso, debido a que los enlaces a analizar son dos, se requiere la misma cantidad de Hubs y de equipos de monitoreo disponibles, mientras que con el Port Mirror y gracias a las características de los Switches, se podrían direccionar ambos puertos hacia uno sólo y capturar todo en una sola estación.

Otra desventaja que se identificó, es la necesidad de interrumpir el enlace el tiempo suficiente para instalar el Hub. Esta demora suele ser lo suficientemente larga como para causar interrupciones en las conexiones, algo que no es objeto de preocupación cuando se configura un Port Mirror.

Además, también se corre el riesgo de que al implementar éste tipo de solución, el desempeño de la red caiga, por lo tanto es aconsejable realizar pruebas preliminares para determinar si su implementación es viable.

5.3.3 Pruebas preliminares

La principal característica a tener en cuenta a la hora de implementar el método del Hub, es precisamente la escogencia del mismo. Hay que tener especial cuidado en que la velocidad de transferencia que soporte en sus puertos no sea menor que el del enlace en el que se va a insertar, para que no provoque un cuello de botella que disminuya el desempeño de la red. En este caso, el tipo de Hub utilizado fue 3COM Superstack II Hub 100, que iguala la velocidad de los enlaces Ethernet de 100 Mbps.

Una vez seleccionados los Hubs, se procedió a insertarlos en los enlaces en un horario no laboral y de poco tráfico, y así evitar que la interrupción necesaria para realizar este proceso causara problemas en aplicaciones críticas y molestias para los usuarios de la red.

Las pruebas preliminares se realizaron el día jueves 30 de marzo en las horas de la noche. Al momento de las mismas, se continúo realizando el monitoreo de los enlaces con el PRTG Traffic Grapher, con el fin de determinar el comportamiento de la red una vez insertado el Hub.

Los resultados de dichas pruebas se resumen en la siguiente gráfica, que presenta del desempeño del enlace del puerto Ethernet del Router Huawei con el Switch, en base a su tasa de transferencia, antes y después de insertar el Hub

En la gráfica se hace evidente el momento en el que se realizó la inserción del Hub a manera de un corte de menos de 5 minutos que la divide en dos revelando el comportamiento del enlace antes y después del cambio. Comparando estas dos partes de la gráfica, se puede afirmar que no existe un cambio significativo en el comportamiento del enlace, una vez se ha añadido el Hub, dado que la tendencia se mantiene y no presenta cambios bruscos. La disminución progresiva que se advierte en la tasa de transferencia es completamente normal teniendo en cuenta el horario de realización de la prueba.

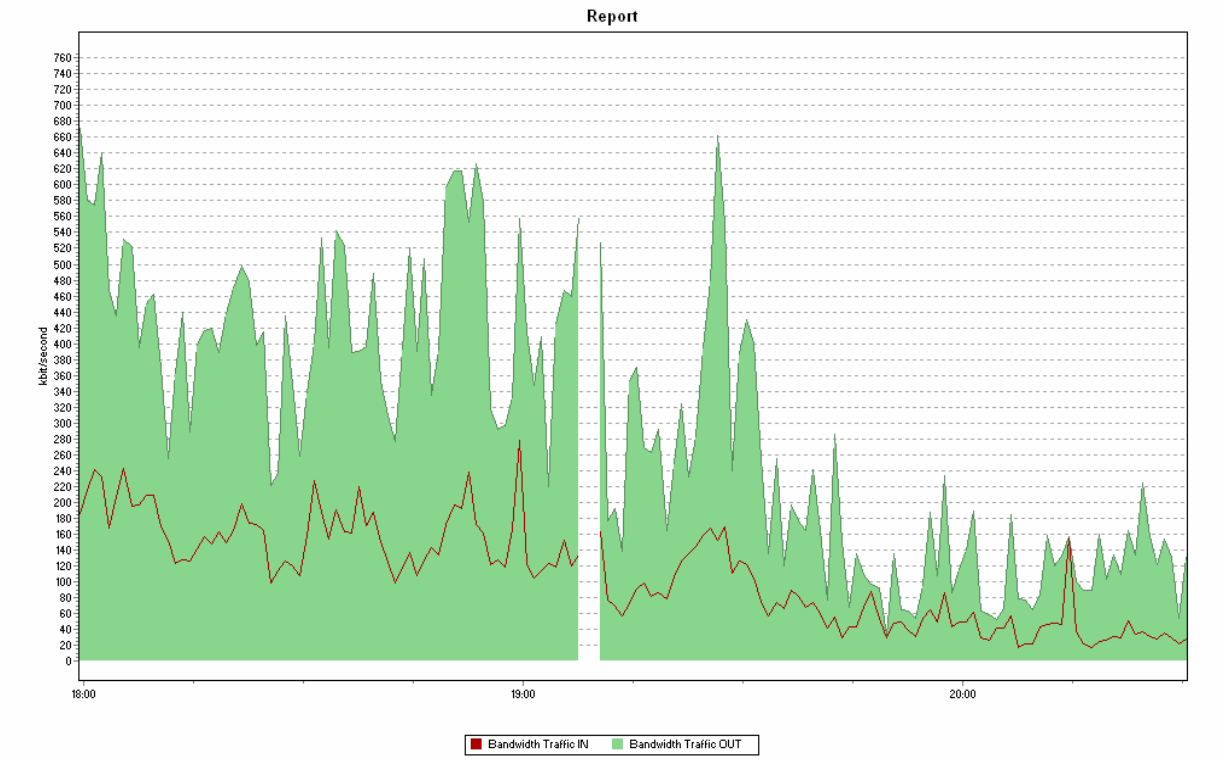


Figura 5.9. Tasa de Transferencia del Puerto Ethernet del Router Huawei antes y después de insetar el Hub (Fuente: Autores)

5.3.4 Esquema de la captura y consideraciones

Según trabajos de grado realizados con anterioridad en la Universidad Industrial de Santander[12],[14] sobre estudios de este tipo, se recomienda realizar la captura durante una semana y sólo durante los días hábiles debido a que durante este periodo, se concentra la mayor cantidad de tráfico en los enlaces, lo cuál se comprobó en el análisis realizado en el numeral 5.2 Utilización de los enlaces (Monitoreo con PRTG) y se puede apreciar con facilidad en las gráficas resultantes.[72]

Siendo así, se definió la semana comprendida entre el 3 y el 7 de Abril para realizar la captura del tráfico.

Posteriormente, se debe decidir el horario de captura de cada día. Nuevamente, se tuvieron en cuenta los resultados obtenidos con el PRTG, que mostraron que la mayor parte de tráfico en los enlaces de los dos routers se concentraba hacia las horas

[72] Ver Anexo B.1 Resultados Gráficos de la Utilización de los Enlaces

laborales. Por lo tanto, se determinó que las capturas deberían ser realizadas en dos jornadas, entre las 8 y las 12 de la mañana y entre las 2 y las 6 de la tarde.

Por último, es indispensable tener en cuenta el tamaño de las capturas para estimar el espacio en disco requerido en el equipo de monitoreo y evitar desbordamientos. Esto se realizó, aprovechando los datos recolectados anteriormente con el PRTG que se muestran en la Tabla 5.3.

Estos datos dan una idea de la cantidad en bytes transmitidos y recibidos a lo largo de un mes por los puertos Ethernet de los dos routers principales de la Red de Datos.

Según esto, durante los 30 días del monitoreo con el PRTG, el puerto Ethernet del Router Huawei transmitió 37´592.390 KB y recibió 86'810.917 KB, lo que en total, equivale aproximadamente a unos 125 GB por mes ó 31.25 GB por semana. Mientras tanto el puerto Ethernet del Router Cisco, transmitió 5´000.990 KB y recibió 1´337.351,226 KB, es decir aproximadamente unos 6.5 GB por mes ó 1.6 GB por semana.

En base a esas estimaciones, se completó la siguiente tabla que resume el esquema de la captura a realizar.

Esquema de la Captura		
Fecha	3 al 7 de Abril de 2006	
Horario	8 am a 12 m y 2 pm a 4 pm	
Interfaz	**Huawei**	**Cisco**
Tamaño Total Estimado para 1 Semana (5 días)	31.25 GB	1,6 GB
Tamaño por día	6,25 GB	320 MB
Tamaño por hora	781 MB	40 MB
Tamaño 10 minutos	130.167 MB	6.7 MB
Capturas cada	10 min	Hora
Cantidad de archivos día	48	8
Cantidad total de archivos	240	40

Tabla 5.5. Esquema de la captura

Es importante escoger un tamaño adecuado para los archivos, ya que de ser muy grandes, se corre el riesgo de no poder abrirlos para procesarlos.

5.3.5 Manejo del Ethereal

Una vez resuelto el problema de enviar todo el tráfico de los enlaces hacia la interfaz de los Equipos de Monitoreo y definido el esquema de captura, es momento de preocuparse por la utilización de Ethereal para capturar los datos.

Sin embargo, este procedimiento ya ha sido descrito en trabajos de grado anteriores[12],[14], por lo tanto no se entrará en detalle y se recomienda al lector remitirse a ellos para profundizar.

5.3.6 Procesamiento de los Datos

El procesamiento de las capturas obtenidas con Ethereal consta de varias etapas: La etapa de filtrado, la etapa de unión, la etapa de procesado con Dice[73], y la etapa de procesado con Access. A continuación se explica cada una de ellas.

5.3.6.1 Etapa de Filtrado[3]

Debido a que los archivos de captura obtenidos contienen tráfico de varias sedes, es necesario realizar un filtrado para separar los paquetes de cada una. Ethereal permite realizar este filtrado de manera sencilla por medio de su interfaz gráfica, sin embargo, dado el tamaño de los archivos de captura y su cantidad, el tiempo requerido para realizar este proceso sería bastante largo y se correría el riesgo de bloquear el equipo en el que se esté realizando el proceso.

Una alternativa para solucionar este inconveniente es utilizar el equivalente en línea de comandos del Ethereal, denominado “tethereal”, el cual permite realizar la mayoría de los procesos que hace Ethereal pero por medio de comandos en la consola MS-DOS.

El comando para filtrar en tethereal es el siguiente:

tethereal –r [Nombre de archivo a filtrar] –R “[Filtro]” –w [Nombre de archivo para guardar]

Ejemplo:
C:\Archivos de programa\Ethereal>tethereal –r Prueba1_cisco_1min –R “ip.addr == 172.16.117.0/23” –w Prueba1_cisco_1min_giron

[73] Software de distribución libre para realizar análisis estadísticos sobre capturas de Ethereal.

Filtra la captura “Prueba1_cisco_1min” con el filtro “ip.addr == 172.16.117.0/23” que identifica los paquetes correspondientes a la red LAN de Girón y los guarda en un archivo con el nombre “Prueba1_cisco_1min_giron”

En la siguiente tabla se incluyen todos los filtros utilizados para cada subred en cada uno de los Routers:

Router Cisco	Girón	ip.addr == 172.16.117.0/23
	Florida	ip.addr == 172.16.119.0/23
	Sede Administrativa	!(ip.addr == 172.16.117.0/23 or ip.addr == 172.16.119.0/23) (ip.src == 172.16.55.0/23 and ip.dst == 172.16.55.0/23) or eth.addr == ff:ff:ff:ff:ff:ff
Router Huawei	Barranca	ip.addr == 172.16.115.0/23
	Girón	ip.addr == 172.16.117.0/23
	Florida	ip.addr == 172.16.119.0/23
	San Gil	ip.addr == 172.16.123.0/23
	Comercio y Servicios	ip.addr == 172.16.125.0/23
	Vélez	ip.addr == 172.16.131.0/24
	Piedecuesta	ip.addr == 172.16.178.0/24
	Málaga	ip.addr == 172.16.183.0/23
	Sede Administrativa	!(ip.addr == 172.16.115.0/23 or ip.addr == 172.16.117.0/23 or ip.addr == 172.16.119.0/23 or ip.addr == 172.16.123.0/23 or ip.addr == 172.16.125.0/23 or ip.addr == 172.16.131.0/24 or ip.addr == 172.16.178.0/24 or ip.addr == 172.16.183.0/23)

Tabla 5.6. Filtros de tethereal para cada una de las Sedes

5.3.6.2 Etapa de Unión[3]

Una vez filtrados todos los archivos de captura para cada una de las sedes, es necesario unir los archivos resultantes por días, para posibilitar el procesamiento de los datos de cada día de la semana.

Nuevamente, se trata de un proceso largo y lento, por lo tanto se acudió una vez más a las ventajas que en velocidad de procesamiento, brinda la línea de comandos.

El Ethereal por defecto tiene instalada una utilidad de línea de comandos para unir los archivos, denominada “Mergecap” que los une cronológicamente según los tiempos de las capturas. El comando es el siguiente:

mergecap –w [Nombre de archivo para guardar] [captura1] [captura2] [captura3]…

Ejemplo:
C:\Archivos de programa\Ethereal>mergecap –w captura1mascaptura2 captura1 captura2

Une cronológicamente los paquetes de los archivos “captura1” y “captura2” y los guarda en otro llamado “captura1mascaptura2”

5.3.6.3 Etapa de procesado con Dice

En etapa del proyecto se precisó recurrir a otra herramienta que permitiera realizar un procesamiento estadístico de los datos de una manera rápida y confiable, debido a que Ethereal no brinda esta posibilidad.

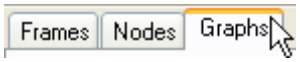
El resultado fue una utilidad de carácter gratuito desarrollada por Nigel G. Thomas, denominada Dice Packet Decoder en su Versión 2.9.9. que puede ser descargada desde la siguiente dirección: http://www.ngthomas.co.uk/Dice/setup.exe

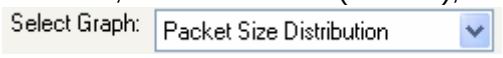
Esta utilidad permite abrir capturas realizadas con Ethereal de tamaño hasta de 2 GB y automáticamente realiza un procesamiento estadístico mostrando resultados de manera gráfica teniendo en cuenta: Distribución de Tamaño de Paquetes, Tipo de Tráfico (Unicast, Broadcast o Múlticast), Distribución de Protocolos, Nodos de Mayor Tráfico Enviado, Nodos de Mayor Tráfico Recibido y Throughput.

Para abrir una captura de Ethereal en Dice y visualizar sus estadísticas, seguimos el siguiente procedimiento:

1. Ejecutar Dice haciendo click en el ícono correspondiente 

2. Click en File > Open File… para seleccionar el archivo que se desea analizar

3. Seleccionar la pestaña Graphs para visualizar las gráficas 

4. Escoger en la lista desplegable la gráfica deseada (Packet Size Distribution, Frame Destination Type, Protocol Distribution, Most Traffic (Sender), Most Traffic (Receiver), Packet Throghput). 

Una vez realizadas varias pruebas con este software, se llegó a la conclusión de utilizarlo solamente para el procesamiento de las capturas en cuanto a Distribución de Tamaño de Paquetes, Tipo de Tráfico y Nodos de Mayor Tráfico. El análisis de Throghput no se tuvo en cuenta y el de Distribución de Protocolos presentó diferencias sustanciales a los resultados obtenidos en las capturas de Ethereal, dado que las librerías de protocolos de Dice, no incluyen una gran cantidad de protocolos y aunque permite añadir más,

asociándolos con los puertos que utilicen, no se logró asociar dos puertos a un mismo protocolo, característica muy común en las aplicaciones actuales.

Por esta razón, para obtener el análisis de la distribución de protocolos se decidió procesar los datos como se propone en uno de los trabajos de grado [12] realizados en la Universidad Industrial de Santander, utilizando la herramienta Microsoft Access.

En esta etapa se obtuvieron como resultados las gráficas de Distribución de Tamaño de Paquetes, Tipo de Tráfico, Nodos de Mayor Tráfico Enviado y Nodos de Mayor Tráfico Recibido para las capturas de cada una de las Sedes encontradas en los enlaces de los Routers Huawei y Cisco.

5.3.6.4 Etapa de procesado con Access

Para procesar los datos en Microsoft Access se requería exportarlos a texto en formato CSV[74], proceso que nuevamente es dispendioso si se realiza con la interfaz gráfica de Ethereal. Sin embargo, se determinó que en este caso esa es la única manera de hacerlo, por lo tanto fue necesario invertir una gran cantidad de tiempo en este proceso.

Una vez con los archivos de texto de cada captura se importaron en Microsoft Access, siguiendo el procedimiento descrito en el trabajo de grado de Hector Alfonso Acevedo Silva y Ronald Martín Zapata.[12]

En esta etapa se obtuvieron como resultado las gráficas de Distribución de Protocolos para las capturas de cada una de las Sedes encontradas en los enlaces de los Routers Huawei y Cisco.

5.3.7 Capturas en el enlace del Router Huawei

Una vez realizado el proceso de filtrado y de unión para clasificar el tráfico capturado entre cada una de las Sedes, se elaboró la siguiente tabla que da una idea de las cantidades de información que diariamente aportó cada una al tráfico total del enlace. Esta cantidad de información por Sede, por día y por semana, corresponde a la que se procesó para realizar los gráficos en Dice y en Microsoft Access.

[74] CSV: Comma Separated Values o Valores separados por comas, un formato de texto que permite ser importado fácilmente en programas de bases de datos como el Microsoft Access.

Lunes

Sede	KBytes
Administración	2´448.180,291
Comercio	1´359.518,285
Girón	145.962,426
Florida	60.908,481
Málaga	31.140,443
Piedecuesta	10.445,268
Sangil	7.861,389
Vélez	3.188,053
Barranca	21,526

Martes

Sede	KBytes
Administración	2´230.654,704
Comercio	1´147.895,543
Girón	148.279,870
Florida	64.887,402
Vélez	13.362,359
Málaga	8.935,658
Barranca	3.697,322
Piedecuesta	3.593,497
Sangil	2.259,052

Miércoles

Sede	KBytes
Administración	2´401.158,754
Comercio	1´463.993,900
Girón	150.382,793
Florida	92.510,523
Vélez	5.291,624
Málaga	4.491,748
Sangil	4.071,339
Barranca	2.538,287
Piedecuesta	2.380,483

Jueves

Sede	KBytes
Administración	2´895.673,771
Comercio	1´352.656,130
Girón	113.365,730
Florida	46.664,848
Málaga	30.772,353
Barranca	6.257,135
Piedecuesta	2.886,615
Sangil	2.433,683
Vélez	445,056

Viernes

Sede	KBytes
Administración	2´137.064,798
Comercio	1´398.716,780
Málaga	220.529,546
Florida	45.572,615
Girón	36.881,227
Barranca	12.492,744
Sangil	5.466,097
Piedecuesta	2.227,016
Vélez	1.197,048

Semana

Sede	KBytes
Administración	14´043.324,559
Comercio	6´722.678,015
Girón	544.429,708
Florida	310.543,869
Málaga	295.867,750
Vélez	23.434,928
Piedecuesta	22.512,890
Sangil	22.091,550
Barranca	21.288,166

Tabla 5.7. KBytes transmitidos por cada una de las sedes del SENA Regional Santander en el enlace del Router Huawei

Estas cantidades corresponden a los siguientes porcentajes:

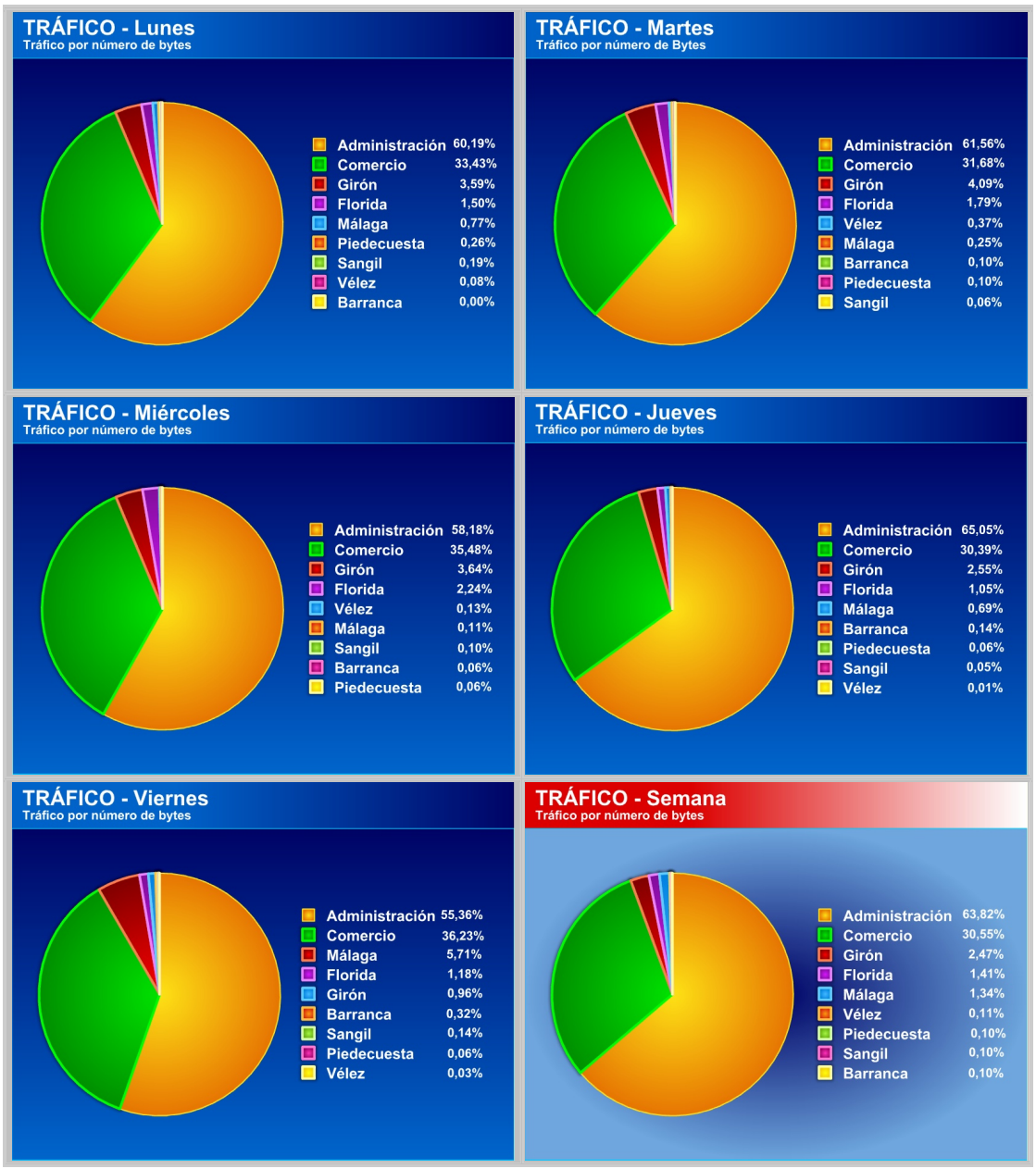


Figura 5.10. Porcentaje de utilización del enlace del Router Huawei por sede (Fuente: Autores)

Como se puede apreciar en las gráficas anteriores, la Sede que aporta más tráfico en el enlace es la Sede Administrativa, que siempre se mantiene sobre el 60%, seguida por el Centro de Comercio y Servicios con un 30%.

Aparecen también sobresaliendo, las Sedes de Girón y Florida, a pesar de que la interconexión no se realiza por medio de este Router. Sin embargo, es entendible que se pueda encontrar tráfico de estas sedes en el enlace, dado que hay que recordar que por medio del Router Huawei todas las sedes salen a Internet, lo que supondría que la gran mayoría de los paquetes de las subredes de Girón y Florida presentes en este enlace corresponden a este tipo de tráfico.

También es de atender el comportamiento del tráfico en la Sede Málaga durante el día viernes, en el que se observa un incremento abrupto hasta casi el 6%, mientras que en los demás días ni siquiera alcanza el 1%. Esta particularidad se debe tener en cuenta a la hora de realizar el análisis de protocolos del día viernes en la Sede Málaga.

Las demás Sedes presentan unos índices de tráfico bastante reducidos dado que las capturas corresponden solamente a la porción de los datos que ingresan a la red LAN de la Sede Administrativa. El tráfico de Internet sigue directamente hacia Bogotá, sin utilizar la interfaz Ethernet del Router, por lo tanto, estos paquetes son invisibles para las capturas. Además, se observa un caso especial en la Sede Barrancabermeja durante el día lunes en el que no se detectó tráfico significativo, lo que supone una falla en el enlace.

5.3.7.1 Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast)[75]

Este tipo de análisis se realizó teniendo en cuenta únicamente la red de datos de la Sede Administrativa, dado que el broadcast se dirige sólo hacia los host de la red en la que se produce. Si se quisiera realizar este tipo de análisis en las demás sedes por medio de este método, se tendría que capturar el tráfico en el enlace Ethernet del router de la sede, lo que implica trasladarse hasta el sitio.

Teniendo en cuenta las gráficas resultantes incluídas en la sección B.2.1.6. de los anexos, es posible observar que durante todos los días el tráfico predominante es Unicast y que el de tipo Broadcast y Multicast son difícilmente apreciables, siempre con menos de un 1%. Esto corresponde a un comportamiento eficiente del enlace en cuanto a tormenta de broadcast y a tráfico multicast.

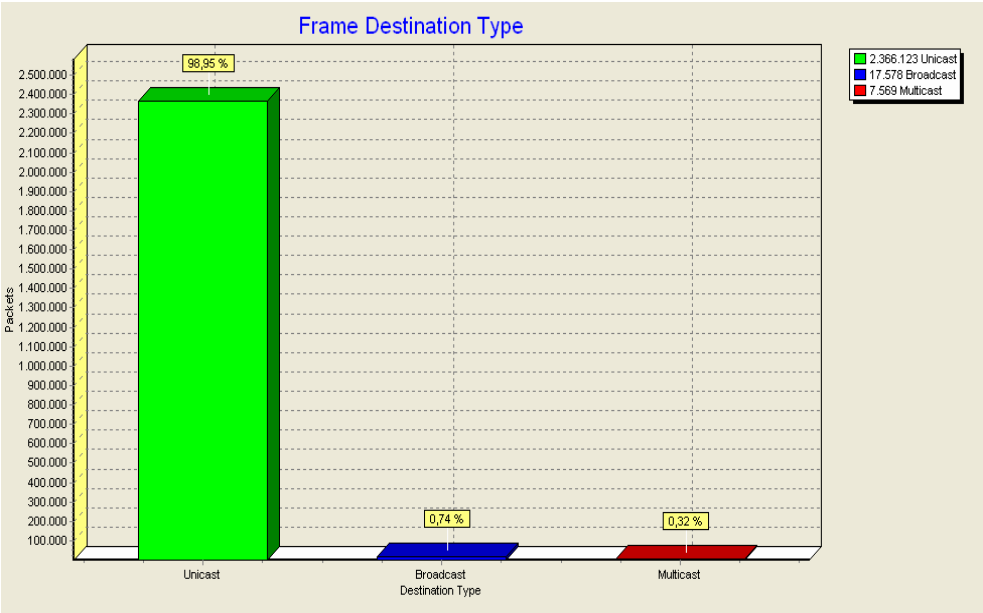


Figura 5.11. Tipo de tráfico en el Router Huawei (Fuente: Autores)

[75] Ver Anexo B.2.1.6. Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast)

5.3.7.2 Distribución de Tamaño de Paquetes[76]

En las siguientes gráficas, se observa la distribución del tamaño de los paquetes en forma de barras con su respectivo valor porcentual, calculado respecto al número total de paquetes transmitidos en la jornada, día o semana, en cada una de las sedes.

Esta característica proporciona una idea del tipo de paquetes habituales en cada subred en cuanto a su tamaño, lo cual afecta el desempeño de la misma de la siguiente manera: Un paquete más grande tarda más tiempo en ser transmitido y liberar el medio, así como también tiene mayor probabilidad de sufrir errores. Sin embargo, no todo es desventaja, ya que si los paquetes son grandes, la utilización del ancho de banda se optimiza, debido a la reducción del número de paquetes requeridos para efectuar una transacción.

En las gráficas se observa una gran concentración de paquetes grandes “>1023” en las Sedes Administrativa, Comercio y Servicios, Girón, Florida y Málaga. Lo cual puede corresponder a una mayor utilización de servicios como Web o FTP, teniendo en cuenta el estudio del tamaño promedio de los paquetes de cada protocolo que se muestra más adelante en la figura 5.11

En este mismo estudio se plantea que los paquetes de menor tamaño corresponden al protocolo ARP (<64), que manejan un direccionamiento tipo broadcast. Por tal razón se hacen más frecuentes en las gráficas de la Sede Administrativa y del Centro de Comercio y Servicios.

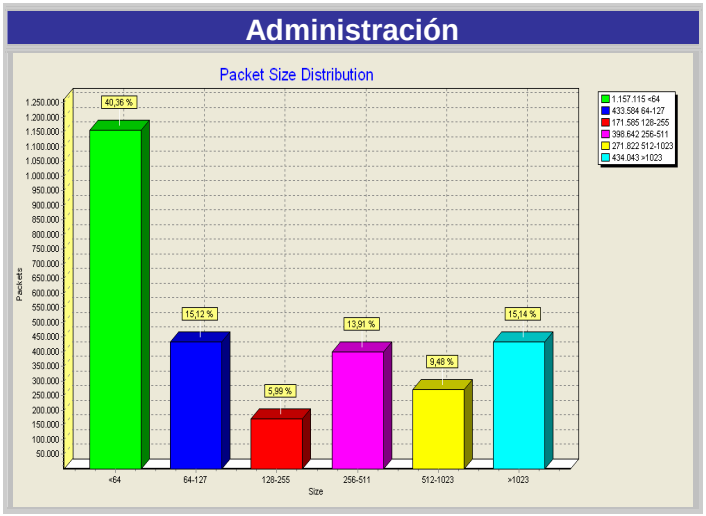


Figura 5.12. Distribución de Tamaño de Paquetes enlace Router Huawei (Fuente: Autores)

[76] Ver Anexos B.2.1.5, B.2.2.5, B.2.3.5, B.2.4.5, B.2.5.5, B.2.6.5, B.2.7.5, B.2.8.5, B.2.9.5

Figura 5.12. Distribución de Tamaño de Paquetes enlace Router Huawei (Fuente: Autores)

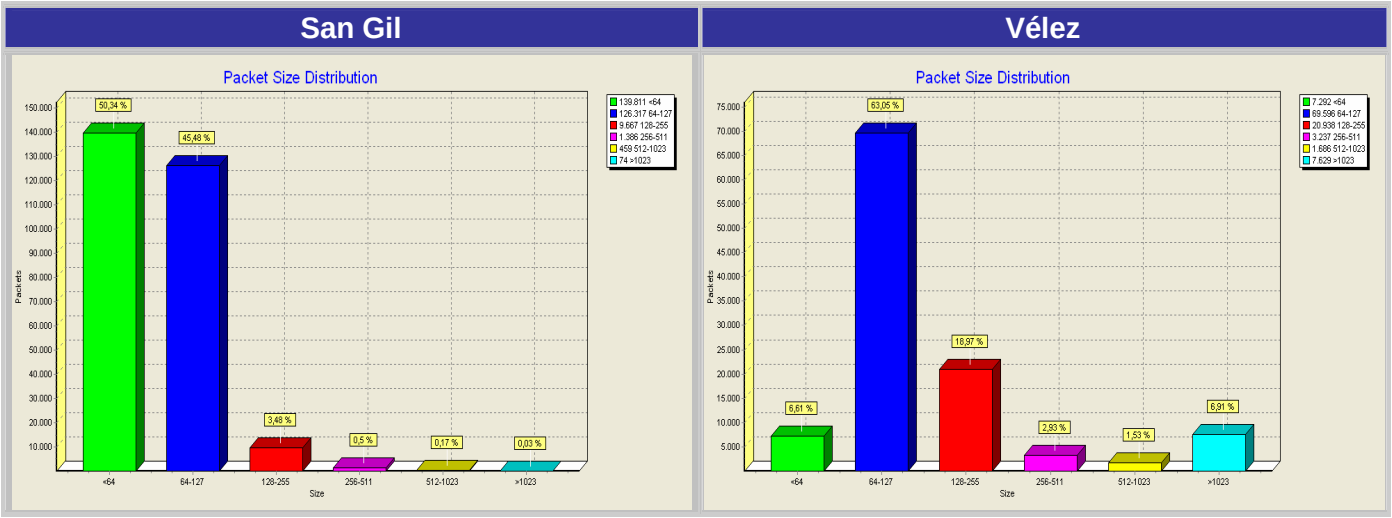


Figura 5.12. Distribución de Tamaño de Paquetes enlace Router Huawei (Fuente: Autores)

5.3.7.3. Distribución de Protocolos[77]

Para facilitar la visualización, se realizaron las gráficas en forma de torta, incluyendo los 10 protocolos con mayores porcentajes en el enlace. El resto de protocolos se agrupó en la categoría denominada “Otros”. Sin embargo, en los anexos de este libro también se incluyen los gráficos en Microsoft Access, que presentan la totalidad de los protocolos calculados y su conteo respecto a número de paquetes o bytes.

Los resultados obtenidos en esta etapa se presentan de dos maneras:

- Protocolos por número de paquetes: Se realiza un conteo de la cantidad de paquetes de cada protocolo.

- Protocolos por número de bytes: Se calcula el número de bytes consumidos por cada protocolo.

[77] Ver Anexos B.2.1.1, B.2.1.2, B.2.1.3, B.2.1.4, B.2.2.1, B.2.2.2, B.2.2.3, B.2.2.4, B.2.3.1, B.2.3.2, B.2.3.3, B.2.3.4, B.2.4.1, B.2.4.2, B.2.4.3, B.2.4.4, B.2.5.1, B.2.5.2, B.2.5.3, B.2.5.4, B.2.6.1, B.2.6.2, B.2.6.3, B.2.6.4, B.2.7.1, B.2.7.2, B.2.7.3, B.2.7.4, B.2.8.1, B.2.8.2, B.2.8.3, B.2.8.4, B.2.9.1, B.2.9.2, B.2.9.3, B.2.9.4

Estas dos características permiten establecer una relación entre el número y el tamaño de los protocolos, para calcular el tamaño promedio de cada uno. La relación se presenta en la siguiente figura en la que se incluyen los protocolos encontrados con mayor frecuencia en las capturas y su respectivo tamaño promedio en bytes.

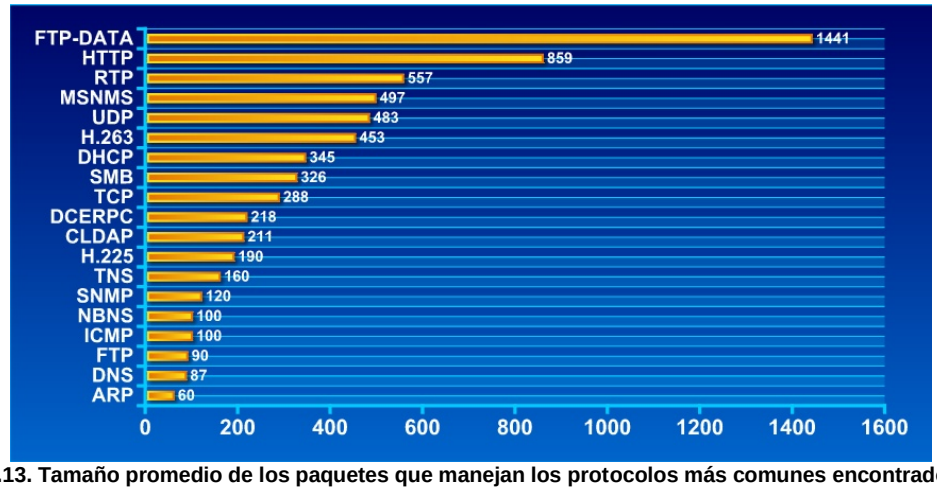


Figura 5.13. Tamaño promedio de los paquetes que manejan los protocolos más comunes encontrados en las capturas (Fuente: Autores)

A continuación se incluyen las gráficas resultantes de la distribución de protocolos de cada una de las sedes durante la semana en la que se realizó la captura. La totalidad de las gráficas por días, se anexan al final de este documento.

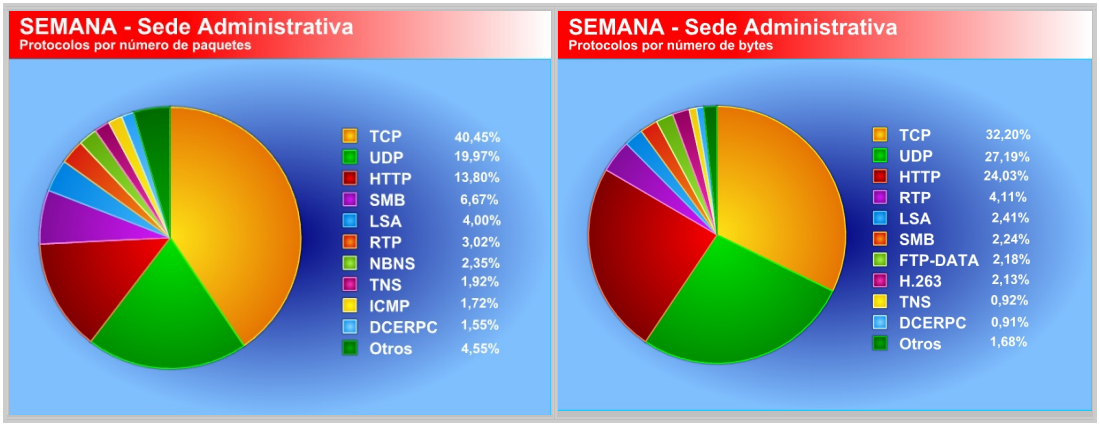


Figura 5.14. Distribución de protocolos durante la semana de la captura en cada una de las sedes (Fuente: Autores)

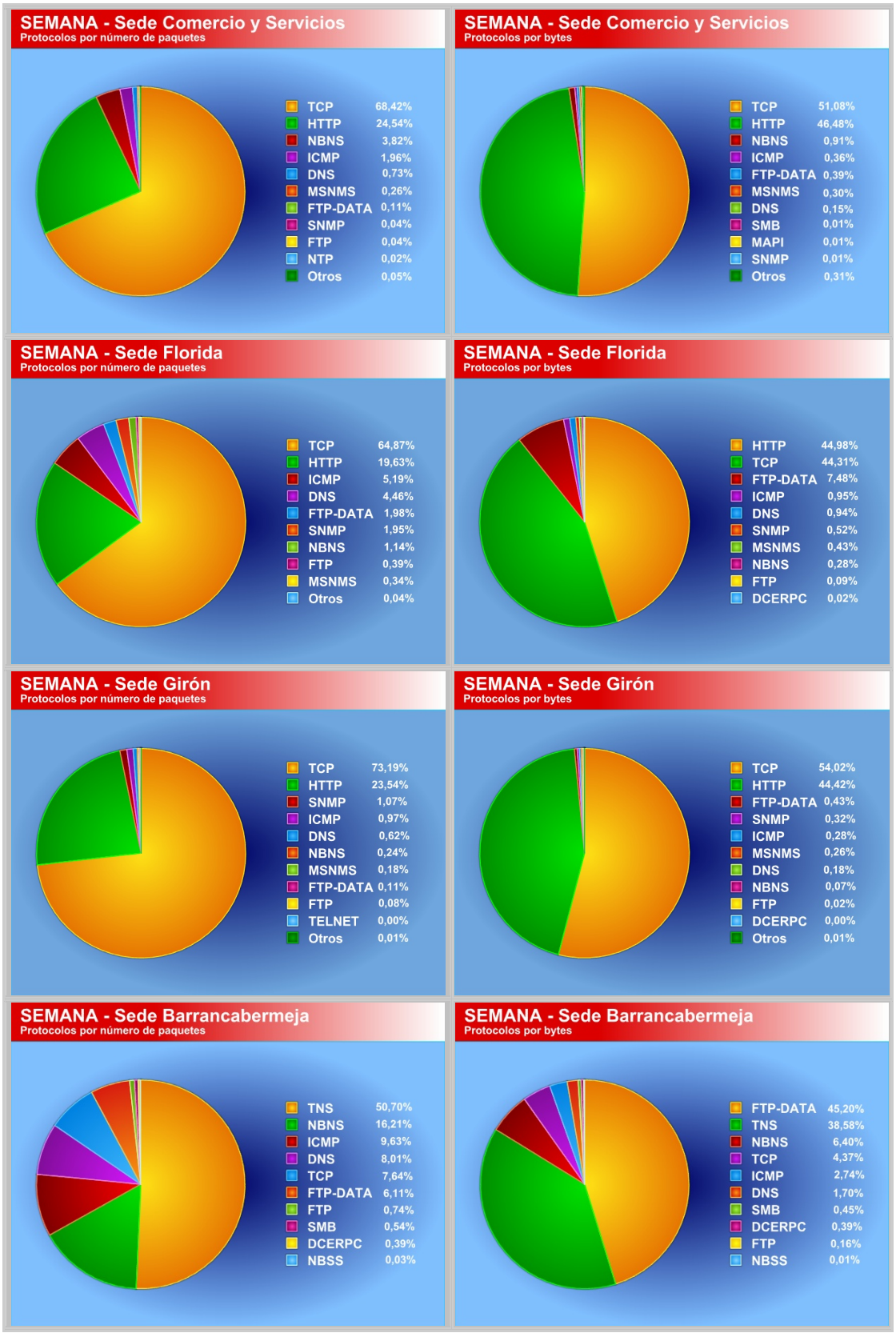


Figura 5.14. Distribución de protocolos durante la semana de la captura en cada una de las sedes (Fuente: Autores)

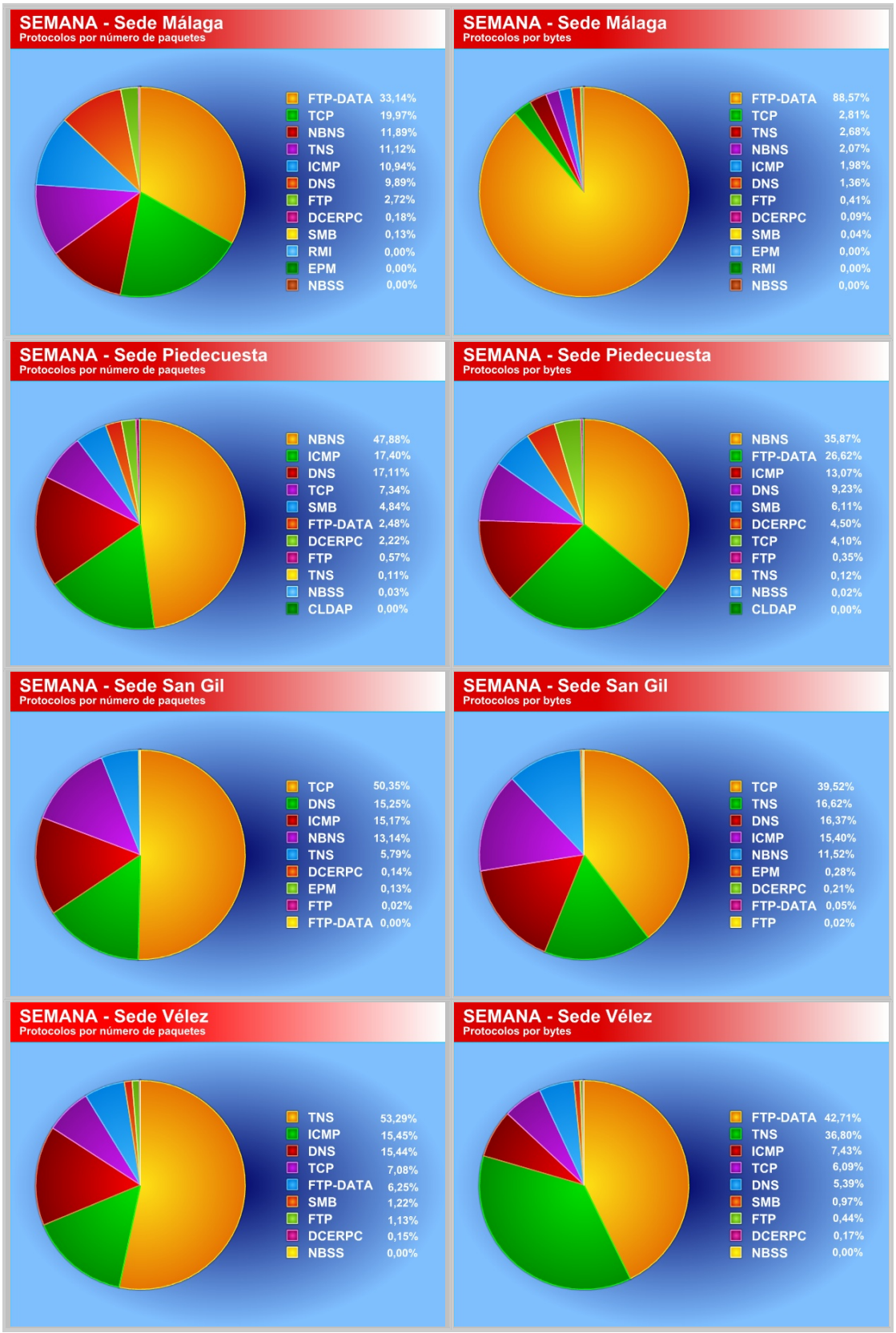


Figura 5.14. Distribución de protocolos durante la semana de la captura en cada una de las sedes (Fuente: Autores)

En todas las gráficas es evidente el predominio de los protocolos de la capa de transporte TCP y UDP. Estos protocolos están asociados a la utilización de ciertas aplicaciones que los requieren. Por esta razón más adelante se realizará un análisis detallado para determinar cuál es su origen.

Otro de los protocolos más utilizados es el HTTP, consumiendo un 25% del tráfico de la red LAN de la Sede Administrativa y casi un 50% de las redes de Florida, Girón y Comercio y Servicios. Sin embargo, es destacable que en las demás Sedes no se encontró tráfico correspondiente a este protocolo, debido a que, como ya se había comentado anteriormente, el Router Huawei los redirecciona internamente hacia el Proxy de la Dirección General, sin necesidad de que tengan que ingresar a la Red LAN de la Sede Administrativa.

El protocolo FTP-DATA, presenta alto índice de utilización de los enlaces en las sedes de Piedecuesta, Vélez, Barranca y especialmente en la Sede de Málaga, donde corresponde a casi el 90% del tráfico de toda la semana. Al revisar las gráficas de la Sede Málaga de la distribución de protocolos día por día[78], efectivamente se encuentra que el día viernes se realizó una transferencia hacia el servidor FTP de un archivo de más de 200 MB. Esta cantidad de tráfico inusual ya se había detectado con anterioridad en el numeral 5.3.3 al analizar la figura 5.8

De todas las sedes, la que presenta una mayor gama de protocolos es la Sede Administrativa, ya que es allí donde se corren todas las aplicaciones del tipo cliente/servidor sobre Oracle que ya se mencionaron. Estas aplicaciones utilizan protocolos como el TNS, para comunicarse con el servidor de la base de datos. Mientras tanto, el protocolo SMB, es el utilizado por Windows para compartir archivos.

También se encuentran protocolos como el RTP (Real Time Transport Protocol) que corresponde a aplicaciones de Voz sobre IP y videoconferencia, al igual que el protocolo de aplicación H.323 que también aporta grandes cantidades de tráfico al enlace. Por esta razón este par de protocolos solamente aparecieron en las capturas en las jornadas que se efectuaron videoconferencias con la Dirección General: Durante todas las jornadas, con excepción del martes en la tarde y el miércoles en la mañana.

[78] Ver Anexo B.2.6.4 Distribución de protocolos por bytes (Porcentajes) - Sede Málaga

5.3.7.4 Nodos de mayor tráfico

A continuación, se presentan los resultados obtenidos en cuanto a los nodos de mayor tráfico en el enlace del router Huawei, para cada una de las sedes que interconecta.

5.3.7.4.1 Sede Administrativa[79]

En la Sede Administrativa, se identificó que los nodos de mayor tráfico enviado corresponden al servidor Proxy de la Dirección General que provee la salida a Internet, a los equipos de videoconferencia y a los servidores de aplicaciones en línea. Esto se comprobó al verificar los nombres de los equipos según sus direcciones IP, en los escaneos efectuados previamente con la herramienta SNMP Sweep de Solarwinds para realizar la documentación de la red. Solamente se identificó un host diferente a los servidores con la dirección IP: 172.16.54.136 con un tráfico enviado significativo

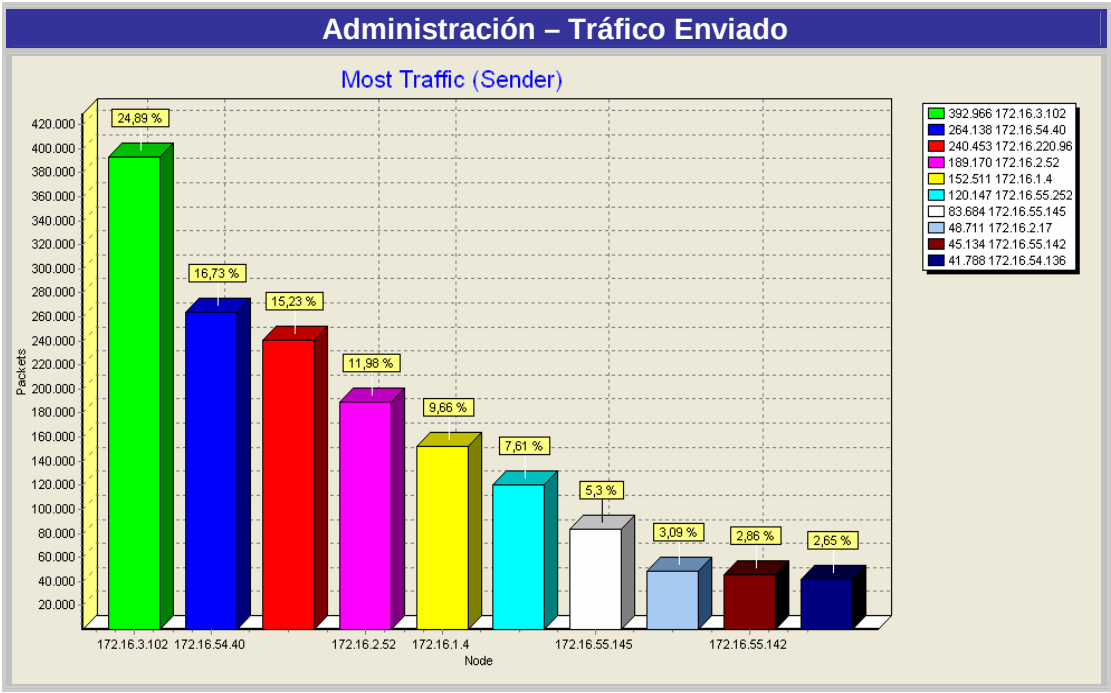


Figura 5.15. Nodos de Mayor Tráfico Enviado – Sede Administrativa (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.3.102	Servidor Proxy
172.16.55.252	Equipo de Videoconferencia Bucaramanga
172.16.1.4	Equipo de Videoconferencia Bogotá
172.16.2.52	s-dig-bog-52-m.sena.edu.co
172.16.2.107	mdigbogsisg018.sena.red
172.16.54.40	sanbucsiswg002.sena.red
172.16.2.62	ddigbogsisg002.sena.red
172.16.54.136	DVALENZUELA

Tabla 5.8. Nombres de los Servidores y de los Equipos de Mayor Tráfico Enviado – Sede Administrativa

[79] Ver Anexo B.2.1.7 Nodos de Mayor Tráfico Enviado – Sede Administrativa y B.2.1.8. Nodos de Mayor Tráfico Recibido – Sede Administrativa.

En cuanto al tráfico recibido, nuevamente el primer lugar fue para el servidor Proxy, seguido de los equipos de videoconferencia y algunos servidores de aplicaciones. Sin embargo, durante ciertas jornadas se identificaron algunos host recibiendo grandes cantidades de tráfico, incluso en ocasiones hasta en un porcentaje mayor que algunos servidores.

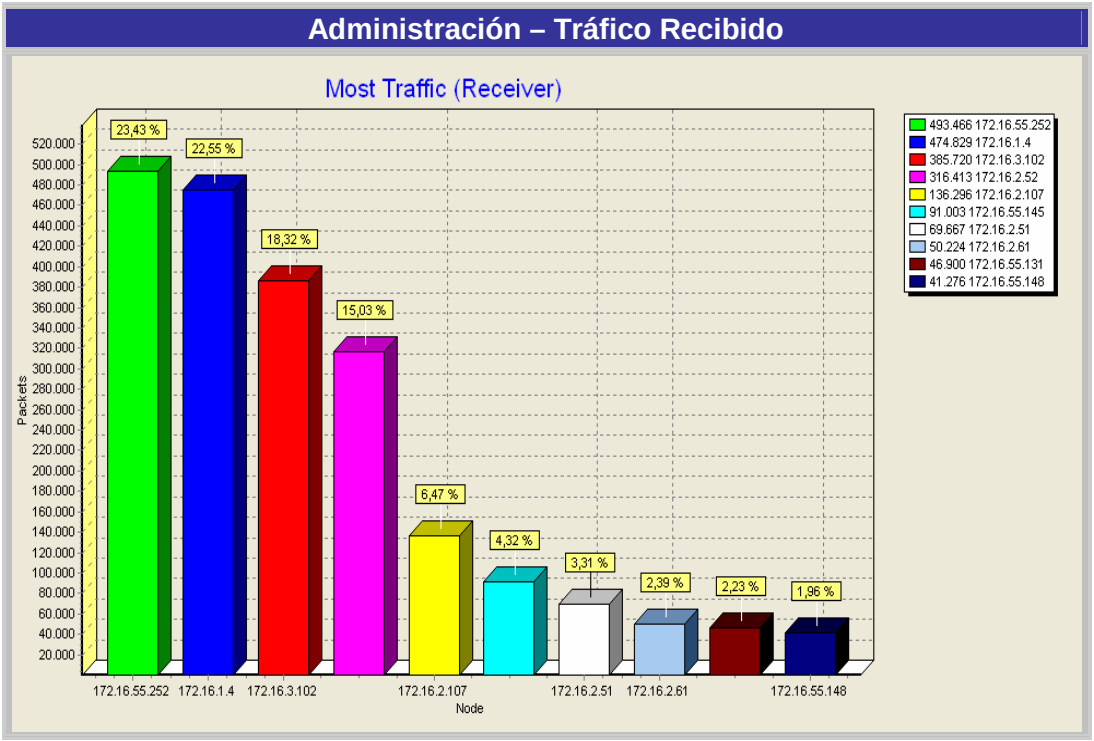


Figura 5.16. Nodos de Mayor Tráfico Recibido – Sede Administrativa (Fuente: Autores)

Dirección IP	Nombre de Equipo	Jornada	Tráfico Recibido (%)
172.16.55.134	recepcionempleo	Lunes Mañana	3,63%
172.16.55.148	empleoreinaldo	Lunes Mañana	2,67%
172.16.55.145	recepcionemp2	Lunes Tarde	4,32%
172.16.55.131	consul01	Lunes Tarde	2,23%
172.16.55.148	empleoreinaldo	Lunes Tarde	1,96%
172.16.55.145	recepcionemp2	Martes Manana	3.33%
172.16.54.75	EQUIPO24	Martes Tarde	3,89%
172.16.55.145	recepcionemp2	Martes Tarde	3,79%
172.16.55.145	recepcionemp2	Miércoles Manana	2,81%
172.16.55.145	recepcionemp2	Jueves Manana	1,94%
172.16.55.145	recepcionemp2	Jueves Tarde	2,53%
172.16.55,147	aleon	Jueves Tarde	2,07%
172.16.54.147	aleon	Viernes Manana	6,89%
172.16.55.145	recepcionemp2	Viernes Manana	3,09%
172.16.55.145	recepcionemp2	Viernes Tarde	4,54%

Tabla 5.9. Nombres de los hosts de Mayor Tráfico Recibido – Sede Administrativa

5.3.7.4.2 Sede Comercio y Servicios[80]

Al analizar las gráficas resultantes correspondientes al tráfico enviado, se encontró que al igual que en la Sede Administrativa, el aporte más significativo en cantidad de información enviada, está dada por el Servidor Proxy, superando siempre el 70%, lo que sugiere una amplia utilización del enlace para la navegación web. Este comportamiento ya se observó anteriormente en la Distribución de protocolos de ésta Sede.[81]

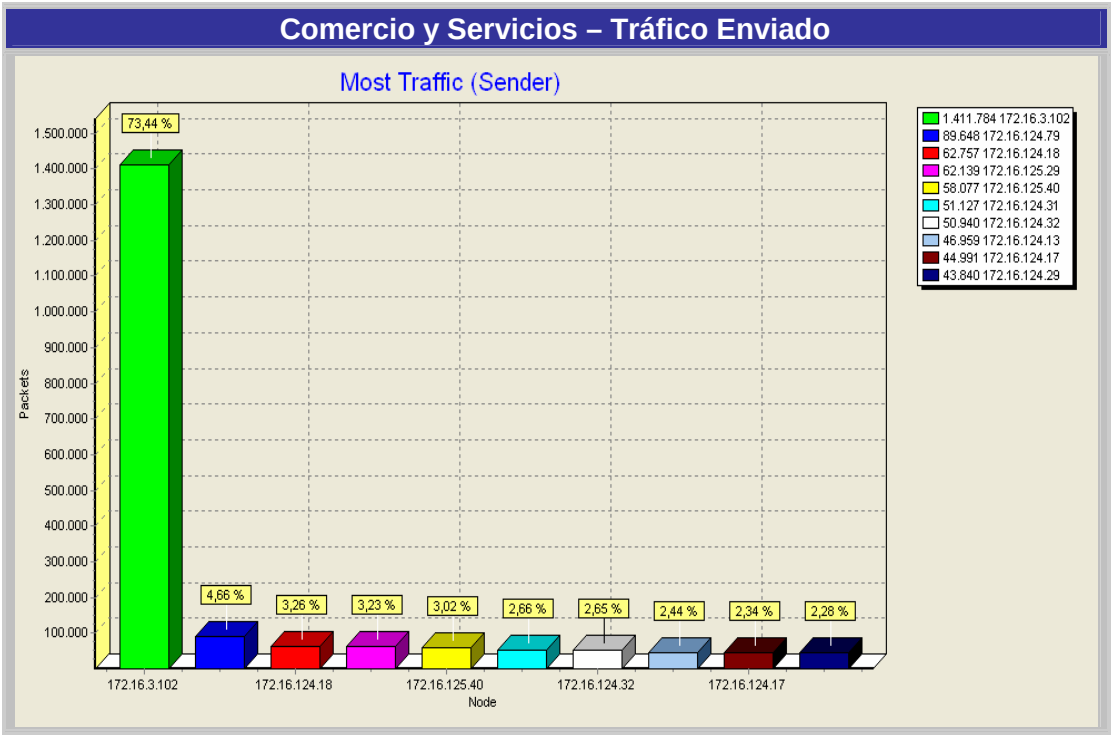


Figura 5.17. Nodos de Mayor Tráfico Enviado – Sede Comercio y Servicios (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.124.79	ADMINISTRADOR
172.16.125.29	SANBUCDESWG02
172.16.125.12	3sic
172.16.125.40	aux_coordinacion
172.16.125.32	bdiaz

Tabla 5.10. Nombres de los Servidores y de los Equipos de Mayor Tráfico Enviado – Sede Comercio y Servicios

[80] Ver Anexo B.2.2.6 Nodos de mayor tráfico enviado - Sede Comercio y Servicios y B.2.2.7 Nodos de mayor tráfico recibo - Sede Comercio y Servicios
[81] Ver Anexo B.2.2.4 Distribución de protocolos por bytes (Porcentajes) - Sede Comercio y Servicios

En cuanto al tráfico recibido en la Sede de Comercio y servicios, una vez más el servidor Proxy es el que presenta la mayor cantidad de peticiones desde estaciones dentro de la red. Lo siguen algunos hosts y servidores de aplicaciones que se muestran a continuación:

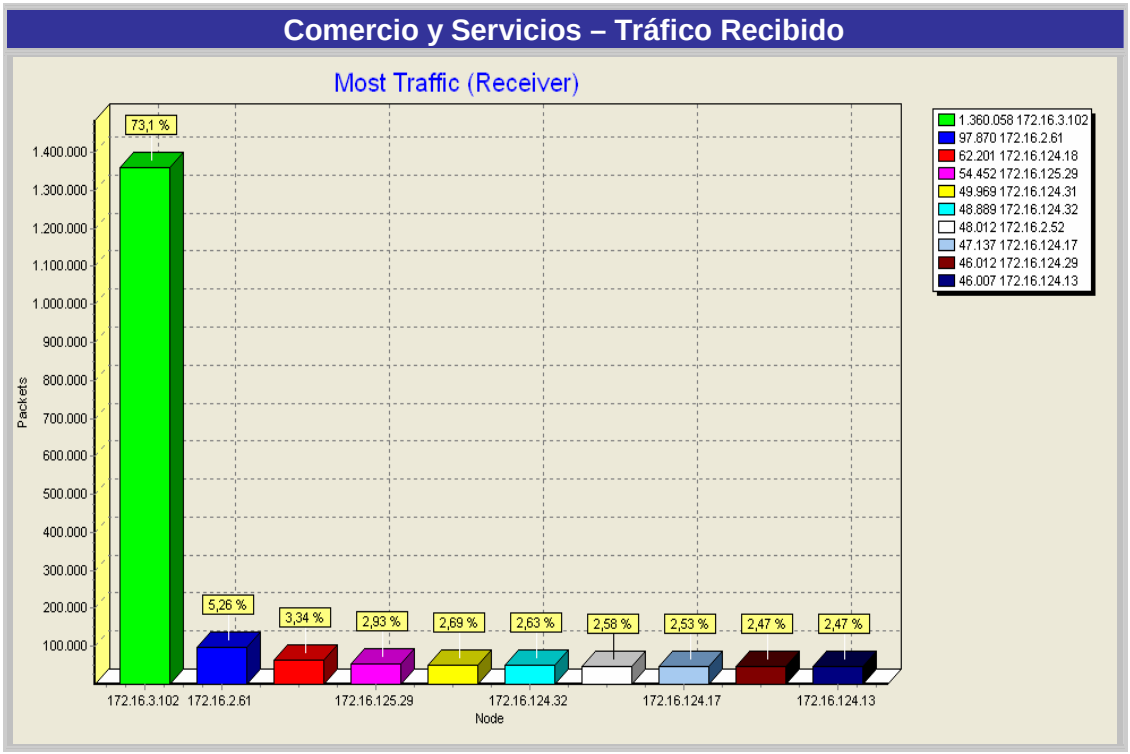


Figura 5.18. Nodos de Mayor Tráfico Recibido – Sede Comercio y Servicios (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.124.18	ADMINISTRADOR
172.16.125.29	SANBUCDESWG02
172.16.125.12	3sic
172.16.125.30	auxpromocion
172.16.124.32	1_a2.sena.edu.co

Tabla 5.11. Nombres de los Servidores y de los Equipos de Mayor Tráfico Recibido – Sede Comercio y Servicios

5.3.7.4.3 Sede Florida[82]

La red LAN de la Sede Florida, presentó una gran cantidad de peticiones hacia el Servidor Proxy de la Dirección General, de más del 50%, indicando un alto tráfico de Internet en esta Sede.

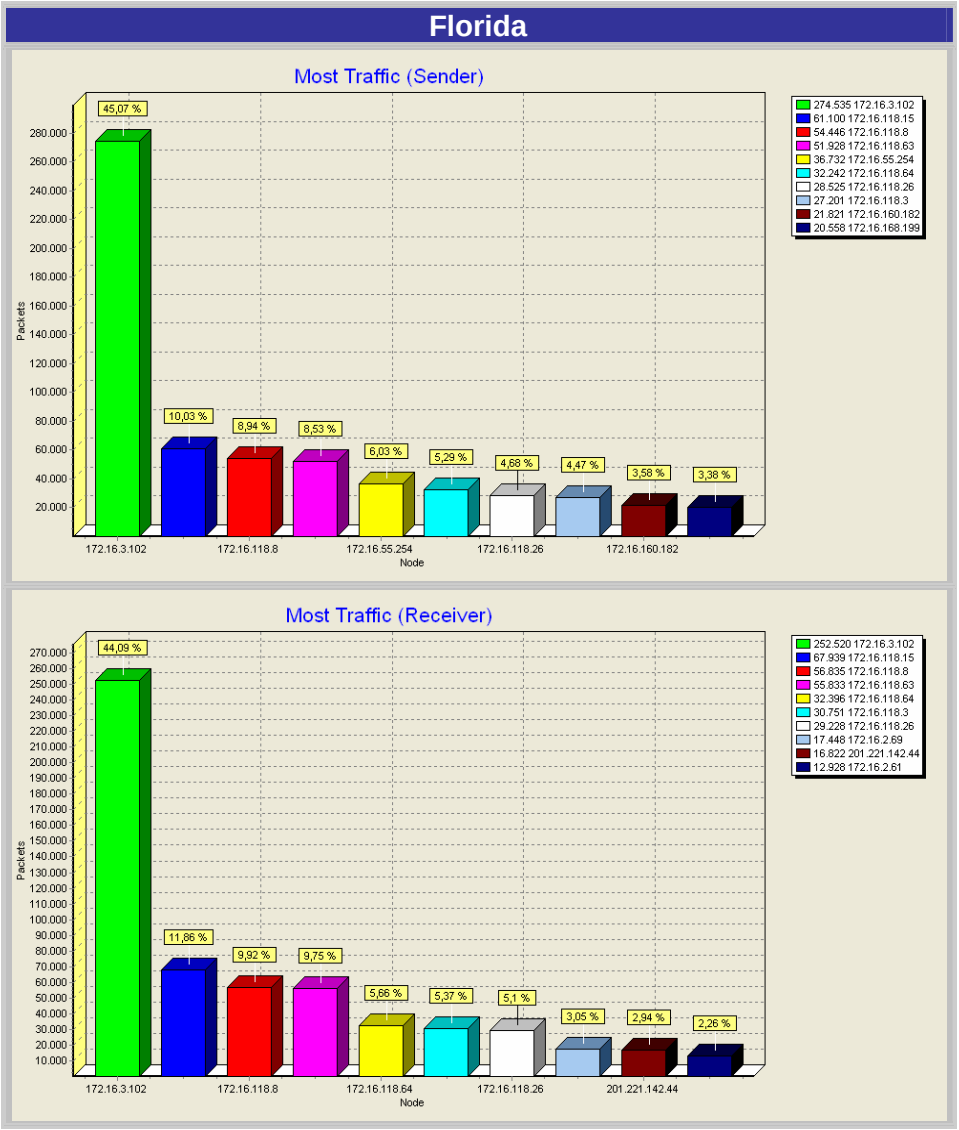


Figura 5.19. Nodos de Mayor Tráfico Enviado y Recibido – Sede Florida (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.118.15	EQUIPO15
172.16.118.8	FGOMEZ
172.16.118.63	EQUIPO9
172.16.118.64	BIBLIOTECA
172.16.118.26	SGCFLORIDA
172.16.118.3	EQUIPO3

Tabla 5.12. Nombres de los Servidores y de los Equipos de Mayor Tráfico - Sede Florida

[82] Ver Anexo B.2.3.6 Nodos de mayor tráfico enviado - Sede Florida y B.2.3.7 Nodos de mayor tráfico recibo - Sede Florida

5.3.7.4.4 Sede Girón[83]

Del mismo modo, en la red LAN de la Sede Girón se advierte un alto porcentaje de tráfico de Internet, debido a la elevada utilización del Proxy de la Dirección General para enviar y recibir datos.

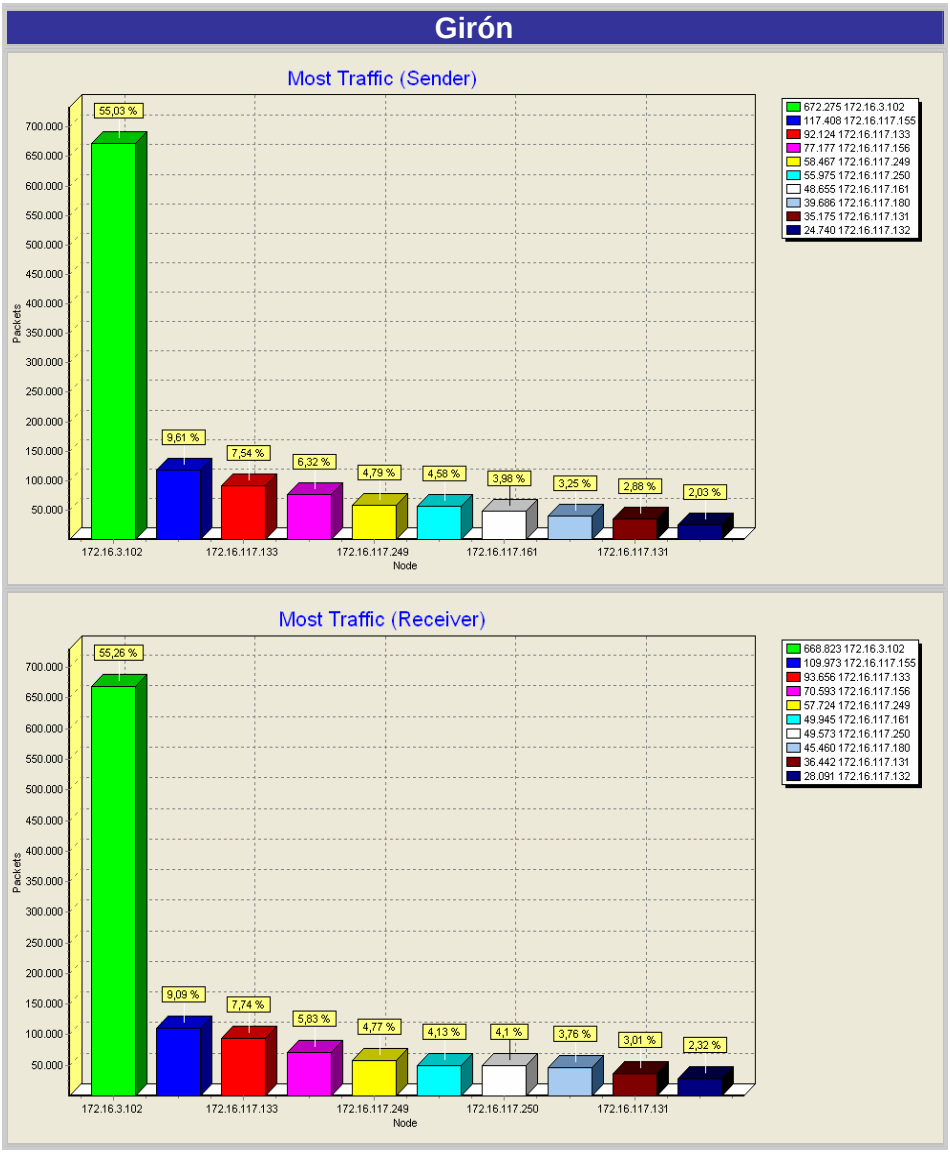


Figura 5.20. Nodos de Mayor Tráfico Enviado y Recibido – Sede Girón (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.117.155	No se dectetó
172.16.117.133	No se detectó
172.16.117.156	No se detectó
172.16.117.249	IS~MARICELA
172.16.117.250	CIPINTO

Tabla 5.13. Nombres de los Hosts de Mayor Tráfico - Sede Girón

[83] Ver Anexo B.2.4.6 Nodos de mayor tráfico enviado - Sede Girón y B.2.4.7 Nodos de mayor tráfico recibo – Sede Girón

5.3.7.4.5 Sede Barranca[84]

En esta red LAN no se encontraron peticiones hacia el servidor Proxy de la dirección general, por tanto el enlace carece de tráfico de Internet, lo que ya se había podido observar en las gráficas de distribución de protocolos, dada la ausencia del protocolo HTTP. Los servicios predominantes en esta sede son aplicaciones en línea y FTP, que se concentran en los siguientes Hosts.

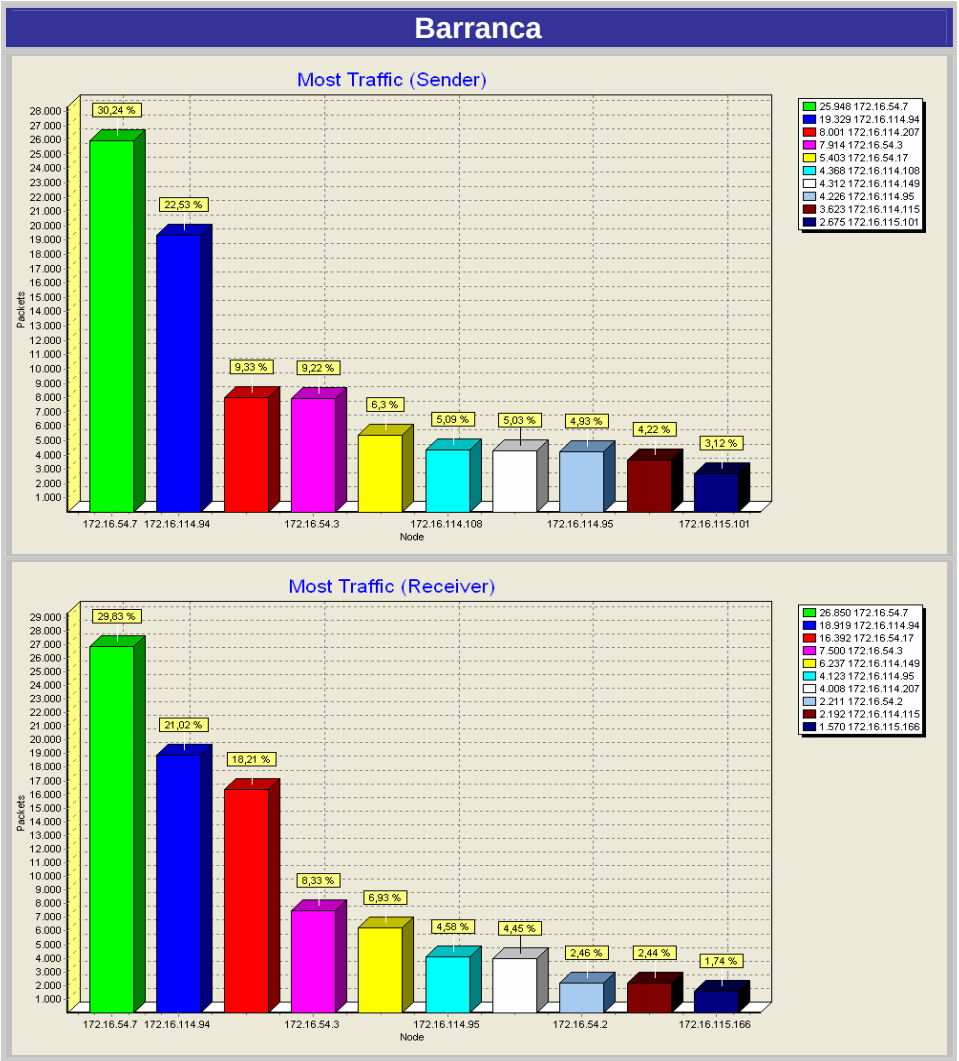


Figura 5.21. Nodos de Mayor Tráfico Enviado y Recibido – Sede Barranca (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.54.7	S_SAN_BUC_04_P
172.16.114.94	ACASTRILLON
172.16.54.17	dsanbucsisg001.sena.red
172.16.54.3	Servidor FTP
172.16.114.149	No se detectó

Tabla 5.14. Nombres de los Hosts de Mayor Tráfico - Sede Barranca

[84] Ver Anexo B.2.5.6 Nodos de mayor tráfico enviado - Sede Barranca y B.2.5.7 Nodos de mayor tráfico recibo – Sede Barranca

5.3.7.4.6 Sede Málaga[85]

En análisis anteriores, se encontró una alta utilización del servicio de FTP en la red LAN de este centro. Esto también es apreciable en las siguientes gráficas, en las que la dirección 172.16.55.3, que corresponde al Servidor FTP instalado en la Sede Administrativa tiene el mayor número de peticiones, seguido por el host que las efectuó.

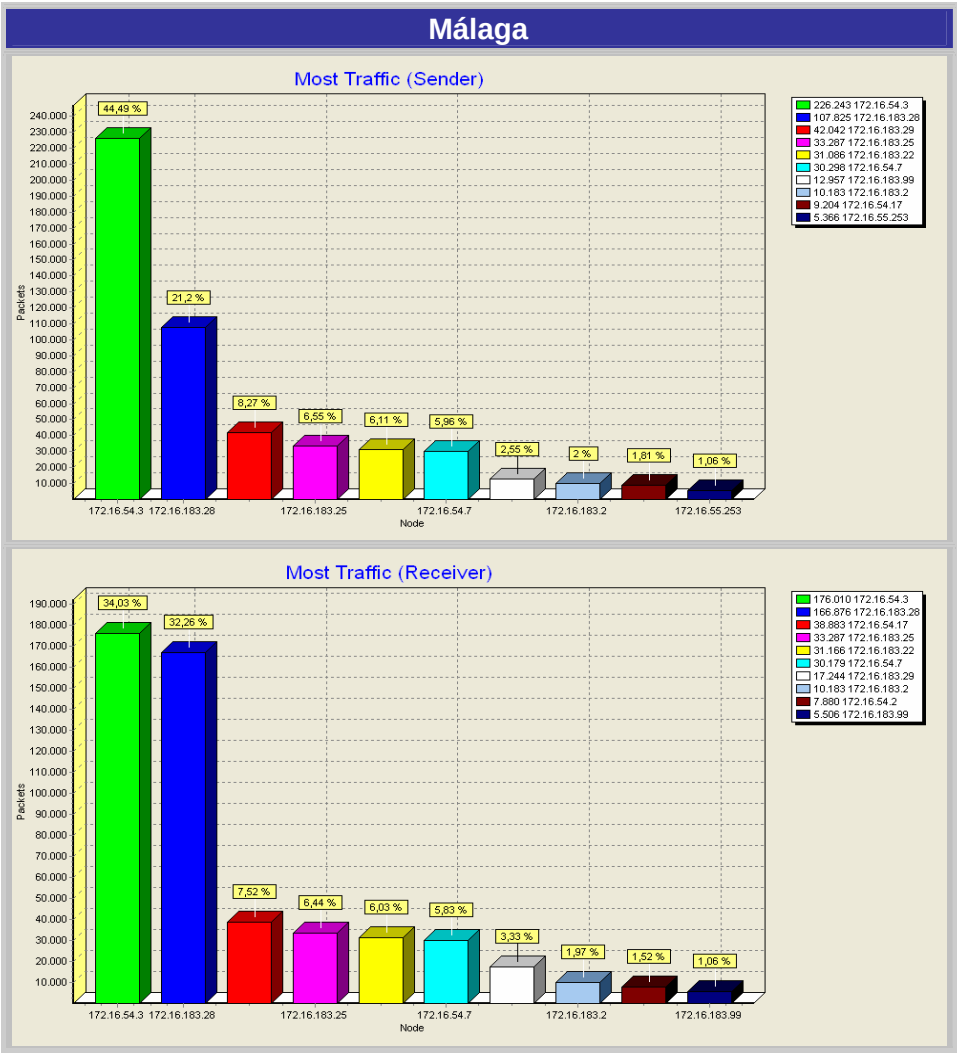


Figura 5.22. Nodos de Mayor Tráfico Enviado y Recibido – Sede Málaga (Fuente: Autores)

Los Host que presentan un alto índice de tráfico recibido y enviado son los siguientes:

Dirección IP	Nombre de Equipo
172.16.54.3	Servidor FTP
172.16.183.28	No se detectó
172.16.183.29	REGISTRO
172.16.183.22	No se detectó
172.16.183.25	COORDINACION

Tabla 5.15. Nombres de los Hosts de Mayor Tráfico - Sede Málaga

[85] Ver Anexo B.2.6.6 Nodos de mayor tráfico enviado - Sede Málaga y B.2.6.7 Nodos de mayor tráfico recibo – Sede Málaga

5.3.7.4.7 Sede Piedecuesta[86]

Se encontró que los Host que incluyen consumen una mayor porción del tráfico del enlace, se encuentran ejecutando aplicaciones en servidores de la Sede Administrativa y utilizando el servicio de FTP

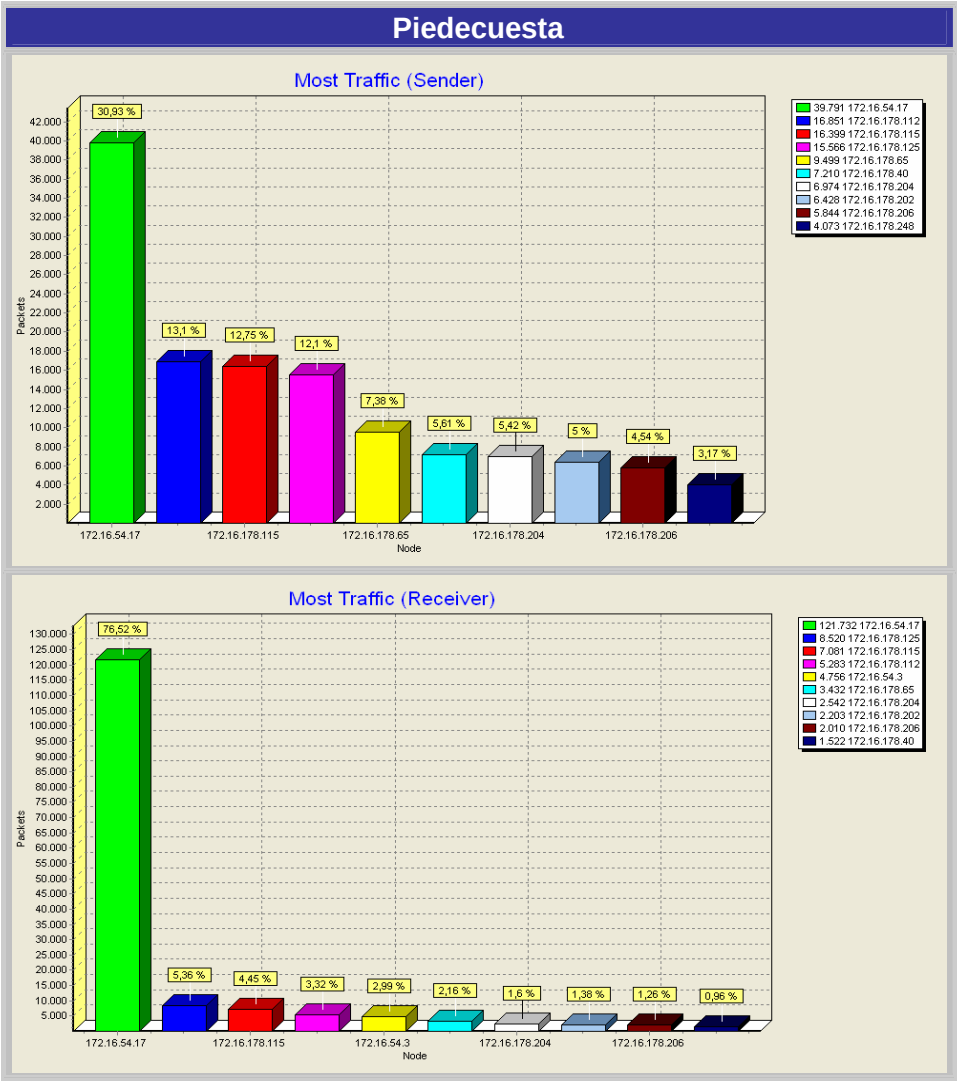


Figura 5.23. Nodos de Mayor Tráfico Enviado y Recibido – Sede Piedecuesta (Fuente: Autores)

Los Host que presentan un alto índice de tráfico recibido y enviado son los siguientes:

Dirección IP	Nombre de Equipo
172.16.54.17	dsanbucsisg001.sena.red
172.16.178.125	SGCCASA1
172.16. 178.115	CMOGOLLON
172.16. 178.112	SGC1
172.16.54.3	Servidor FTP

Tabla 5.16. Nombres de los Hosts de Mayor Tráfico - Sede Piedecuesta

[86] Ver Anexo B.2.7.6 Nodos de mayor tráfico enviado - Sede Piedecuesta y B.2.7.7 Nodos de mayor tráfico recibo – Sede Piedecuesta

5.3.7.4.8 Sede San Gil[87]

En la red LAN de San Gil se encontró un elevado índice de accesos a los servidores de la Sede Administrativa, en ejecución de aplicaciones del tipo cliente/servidor, como la de Gestión de Centros. También se detectó un acceso importante al servicio FTP.

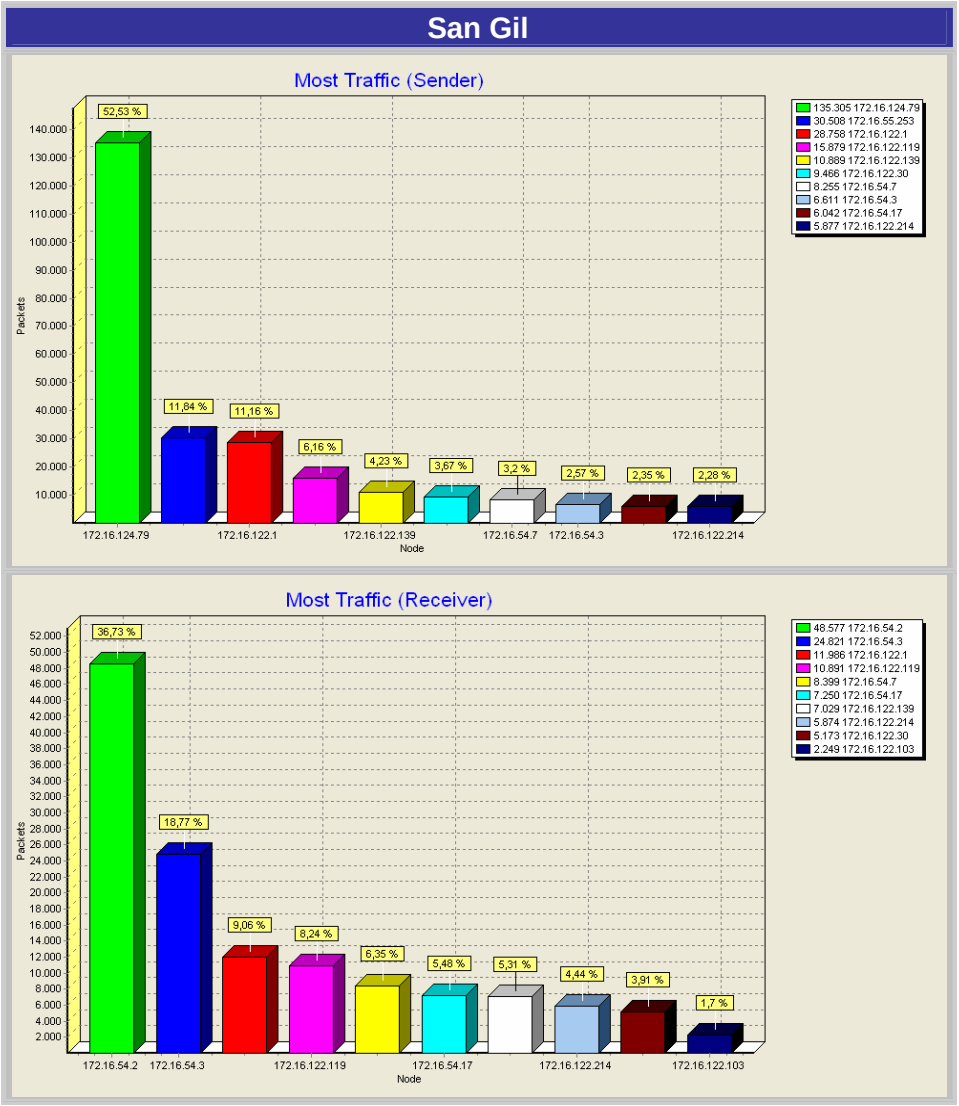


Figura 5.24. Nodos de Mayor Tráfico Enviado y Recibido – Sede San Gil (Fuente: Autores)

Los Host que presentan un alto índice de tráfico recibido y enviado son los siguientes:

Dirección IP	Nombre de Equipo
172.16.54.2	Servidor de la Sede Administrativa
172.16.54.3	Servidor FTP
172.16.122.1	SERVISANGIL
172.16.122.129	No se detectó
172.16.122.139	COORDISANGIL-2

Tabla 5.17. Nombres de los Hosts de Mayor Tráfico - Sede Gil

[87] Ver Anexo B.2.8.6 Nodos de mayor tráfico enviado - Sede San Gil y B.2.8.7 Nodos de mayor tráfico recibo – Sede San Gil

5.3.7.4.9 Sede Vélez[88]

Los resultados en la Sede Vélez hacen evidente la utilización de las aplicaciones en línea, dados los accesos a los servidores de la Sede administrativa, y del servicio de FTP que corresponde al servidor 172.16.54.3

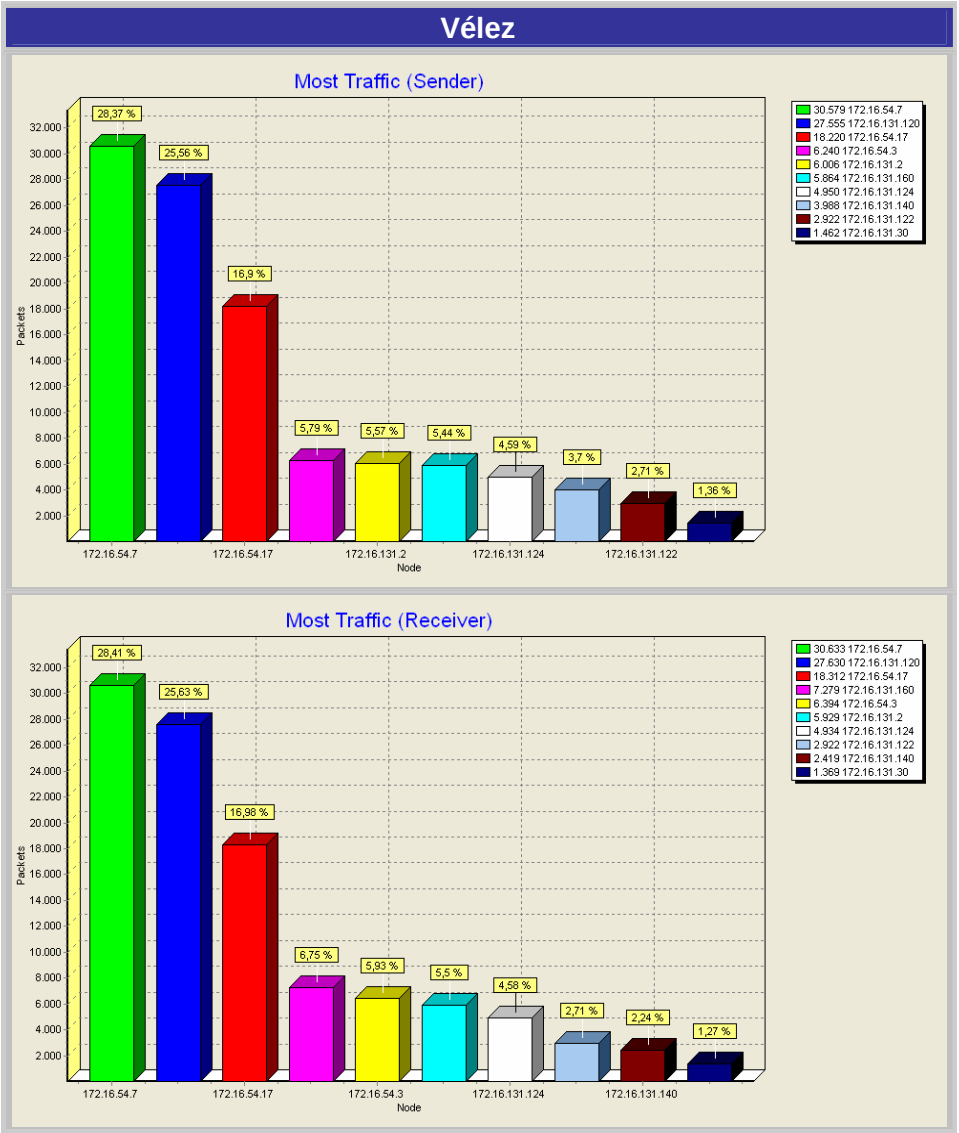


Figura 5.25. Nodos de Mayor Tráfico Enviado y Recibido – Sede Vélez (Fuente: Autores)

Los Host que presentan un alto índice de tráfico recibido y enviado son los siguientes:

Dirección IP	Nombre de Equipo
172.16.54.7	S_SAN_BUC_04_P
172.16.131.120	No se detectó
172.16.131.160	No se detectó
172.16.54.3	Servidor FTP
172.16.131.2	EQUIPO02

Tabla 5.18. Nombres de los Hosts de Mayor Tráfico - Sede Vélez

[88] Ver Anexo B.2.9.6 Nodos de mayor tráfico enviado - Sede Vélez y B.2.9.7 Nodos de mayor tráfico recibo – Sede Vélez

5.3.8 Capturas en el enlace del Router Cisco

De la misma manera que se presentó en el análisis del Router Huawei, a continuación se incluye una tabla con las cantidades diarias de tráfico aportadas por las redes LAN de cada una de las Sedes en el enlace del Router Cisco.

Recordemos que este Router maneja las subredes que se interconectan por RDSI y que corresponden a los centros de Girón y Florida.

Lunes

Sede	KBytes
Girón	146.681,128
Florida	62.826,223
Administración	4.967,488

Martes

Sede	KBytes
Girón	75.926,953
Florida	67.852,758
Administración	5.254,242

Miércoles

Sede	KBytes
Girón	108.700,261
Florida	59.269,760
Administración	5.225,495

Jueves

Sede	KBytes
Girón	123.744,325
Florida	51.017,344
Administración	4.365,461

Viernes

Sede	Bytes
Girón	88.448,662
Florida	55.382,727
Administración	6.314,776

Semana

Sede	Bytes
Girón	543.501,329
Florida	296.348,812
Administración	26.127,462

Tabla 5.19. KBytes transmitidos por cada una de las sedes del SENA Regional Santander en el enlade del Router Cisco

Si tenemos en cuenta las cantidades totales de datos correspondientes a las redes de Girón y Florida, y las comparamos con las manejadas por el Router Huawei de las mismas sedes que se presentan en la tabla 5.6[89], (544.429,708 KB para Girón y 310.543,869 KB en Florida) se encuentra que las cantidades son casi idénticas, demostrando que la mayoría de los paquetes de éstas dos sedes siguen hacia el router Huawei para salir a Internet. La diferencia de las dos cantidades corresponde a los paquetes que ingresan a la Sede Administrativa, la cual es una cantidad mínima.

[89] Ver la Tabla 5.6 KBytes transmitidos por cada una de las sedes del SENA Regional Santander en el enlace del Router Huawei

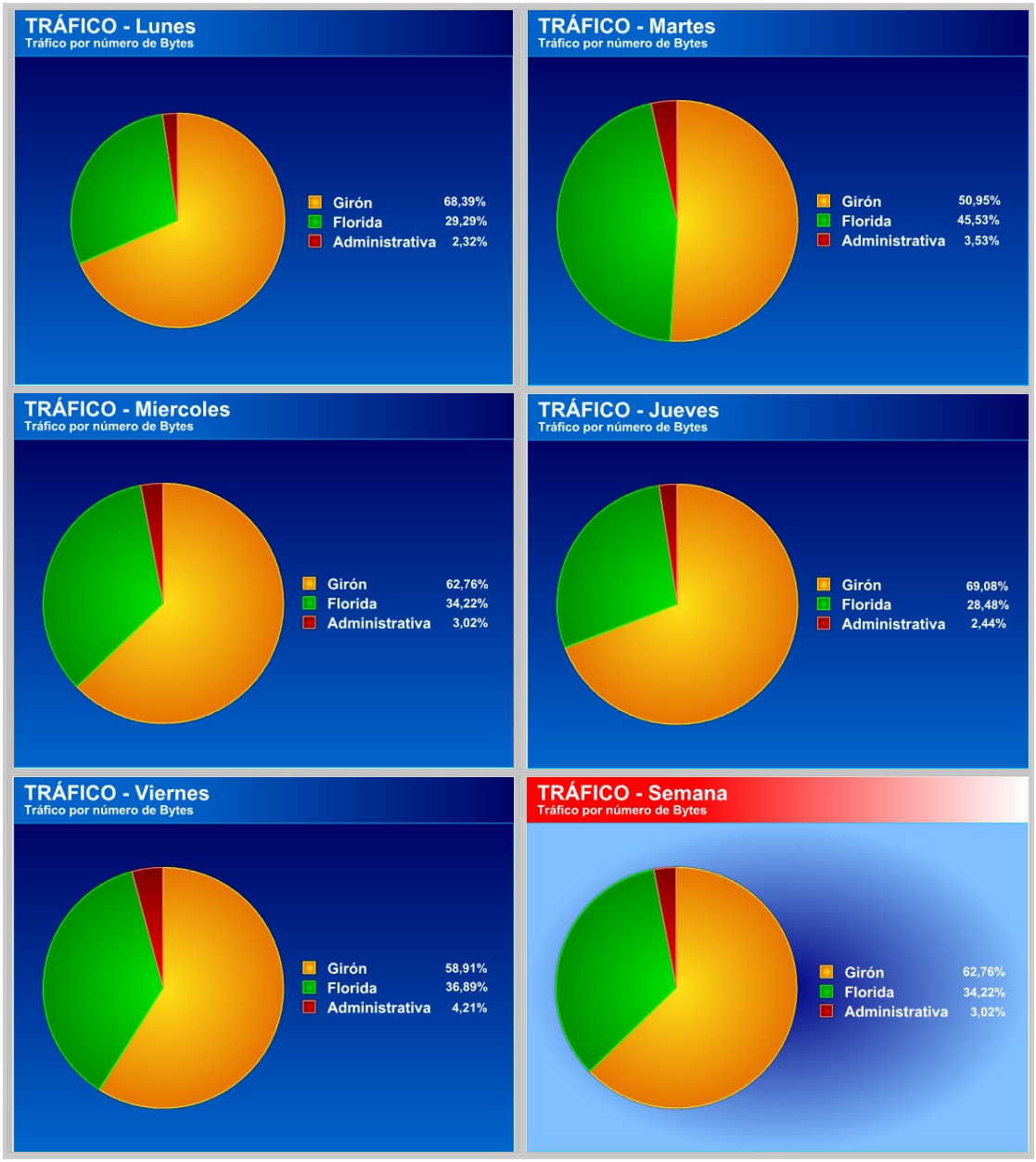


Figura 5.26. Porcentaje de utilización del enlace del Router Cisco por sede (Fuente: Autores)

Estas gráficas revelan que la red LAN que más aporta tráfico al enlace siempre es la del centro de Girón, seguida por la del Centro de Florida y por la Sede Administrativa. Esta última aporta una cantidad tan pequeña al enlace, que corresponde casi en su totalidad al tráfico broadcast que genera el Router Cisco.

5.3.8.1 Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast)[90]

A diferencia de lo presentado en el router Huawei, en el router cisco se advierte una gran cantidad de tráfico Broadcast y Multicast en comparación con el tráfico Unicast. Sin embargo, hay que anotar que este análisis se realizó tomando en cuenta solamente el tráfico de la Sede Administrativa en el enlace, el cual como se ve en la figura anterior, representa escasamente un 3% del tráfico total del enlace.

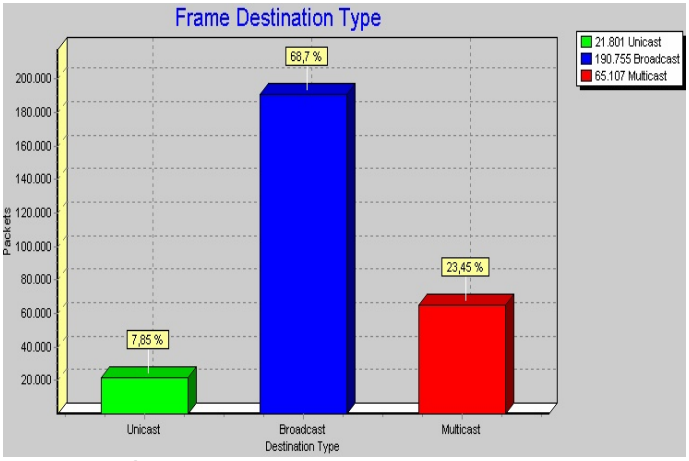


Figura 5.27. Tipo de tráfico en el Router Cisco – Sede Administrativa (Fuente: Autores)

5.3.8.2 Distribución de Tamaño de Paquetes

En la Sede Administrativa se observa un predominio total de paquetes pequeños, que según los resultados del estudio del tamaño promedio de los paquetes que maneja cada protocolo presentado en la figura 5.11, corresponden a ARP, ICMP y NBNS entre otros, que se caracterizan por operar en el nivel de red y por lo tanto forman parte del tráfico broadcast y multicast.

En las Sedes de Girón y Florida los tamaños de paquetes se encuentran en los rangos “<64” y “>1023”, lo que corresponde con lo encontrado en los paquetes provenientes de estas mismas sedes en enlace del router Huawei.[91]

[90] B.3.1.6 Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast) - Sede Administrativa
[91] Ver Figura 5.9. Distribución de Tamaño de Paquetes enlace Router Huawei

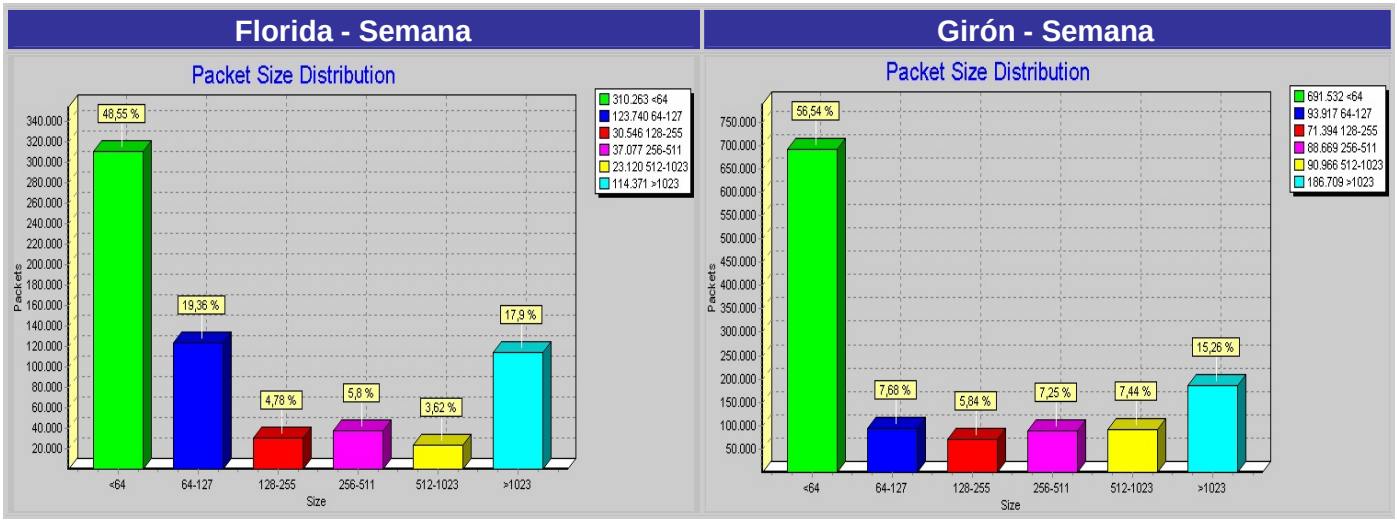


Figura 5.28. Distribución de Tamaño de Paquetes enlace Router Cisco (Fuente: Autores)

5.3.8.3. Distribución de Protocolos

En la Sede Administrativa, como era de esperarse debido a su bajo índice de tráfico, se encontró una gran cantidad de protocolos de red como ARP, NBNS, IPX, NBIPX, entre otros, que corresponden al tráfico broadcast y multicast que se observó en las gráficas anteriores. Sin embargo estas cantidades no son significativas debido a que el tráfico correspondiente a la Sede Administrativa que maneja este enlace es prácticamente nulo.

En las Sedes de Girón y Florida se observa un predominio de protocolos como HTTP y TCP, que consumen en los dos casos más del 80% del tráfico del enlace. También se destacan protocolos como el FTP-DATA que en la sede Florida alcanzó un 8% del enlace y el protocolo TNS que aunque con una presencia de tan sólo 2% en Florida y 0.5% en Girón, ocupa el tercer lugar, dado que corresponde a la utilización de las aplicaciones en línea basadas en Oracle.

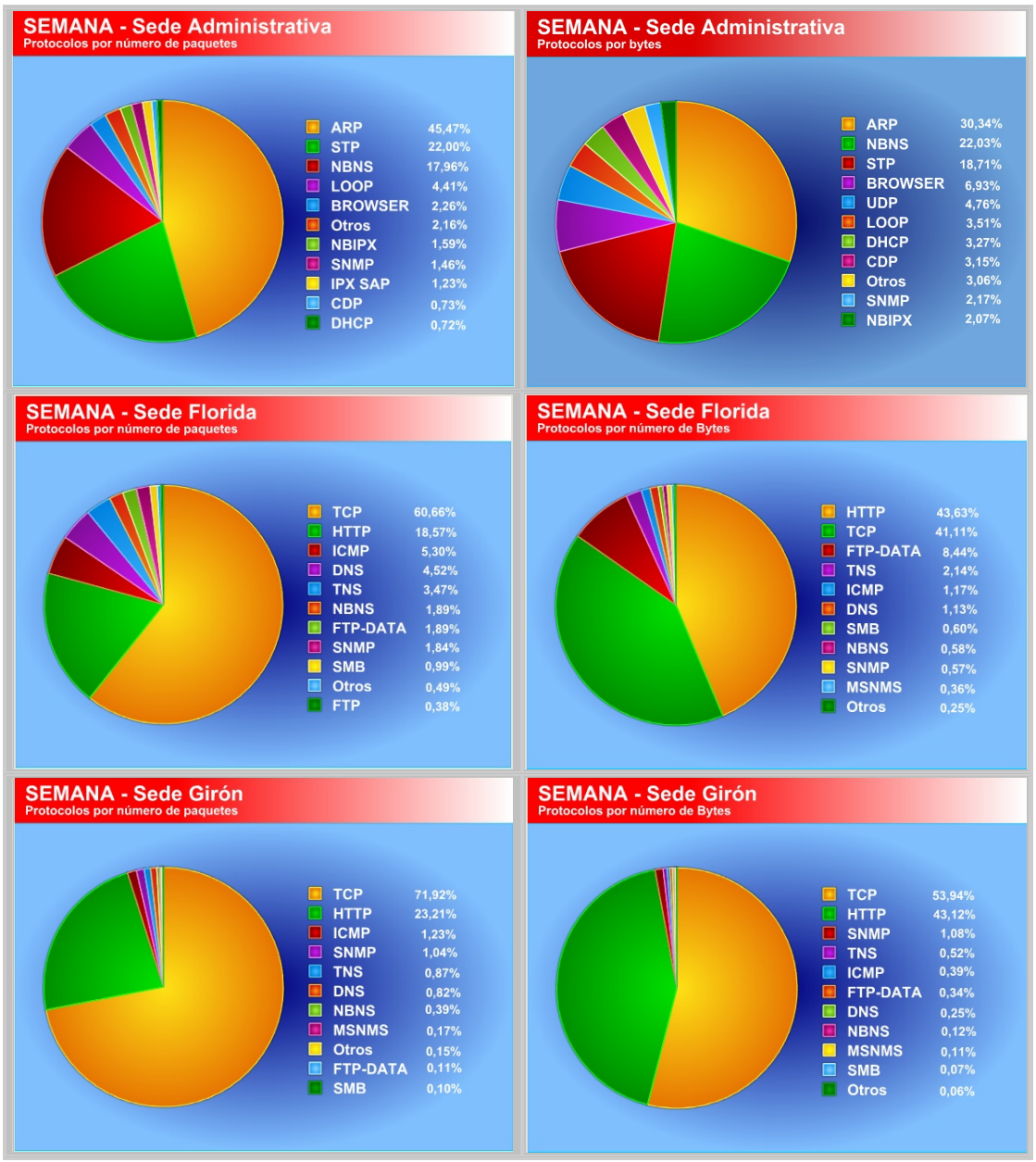


Figura 5.29. Distribución de protocolos durante la semana de la captura en cada una de las sedes (Fuente: Autores)

5.3.8.4 Nodos de mayor tráfico

A continuación, se presentan los resultados obtenidos en cuanto a los nodos de mayor tráfico en el enlace del router Cisco, para cada una de las sedes que interconecta.

5.3.8.4.1 Sede Administrativa

Como se ha venido observando en todas las gráficas que tienen que ver con la Sede Administrativa en el enlace del Router Cisco, el tráfico correspondiente a esta Sede es básicamente del tipo Broadcast y Multicast. Por lo tanto estas gráficas de orígenes y destinos de paquetes, determinan las fuentes que generan estos tipos de tráfico.

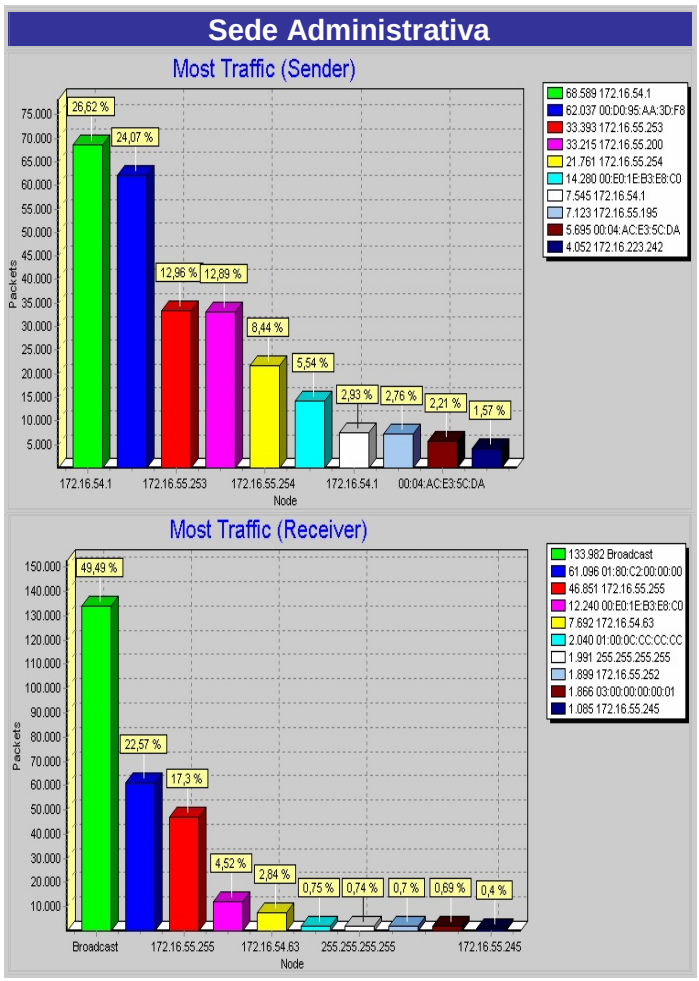


Figura 5.30. Nodos de Mayor Tráfico Enviado y Recibido – Sede Administrativa (Fuente: Autores)

5.3.8.4.2 Sede Florida[92]

Realizando una comparación entre las siguientes gráficas y las obtenidas en la sección 5.3.3.4.4[93] Las características observadas en la Red LAN de Florida que se encontraron en el enlace Cisco, son exactamente las mismas que se observaron con anterioridad en el análisis realizado en el Router Huawei.

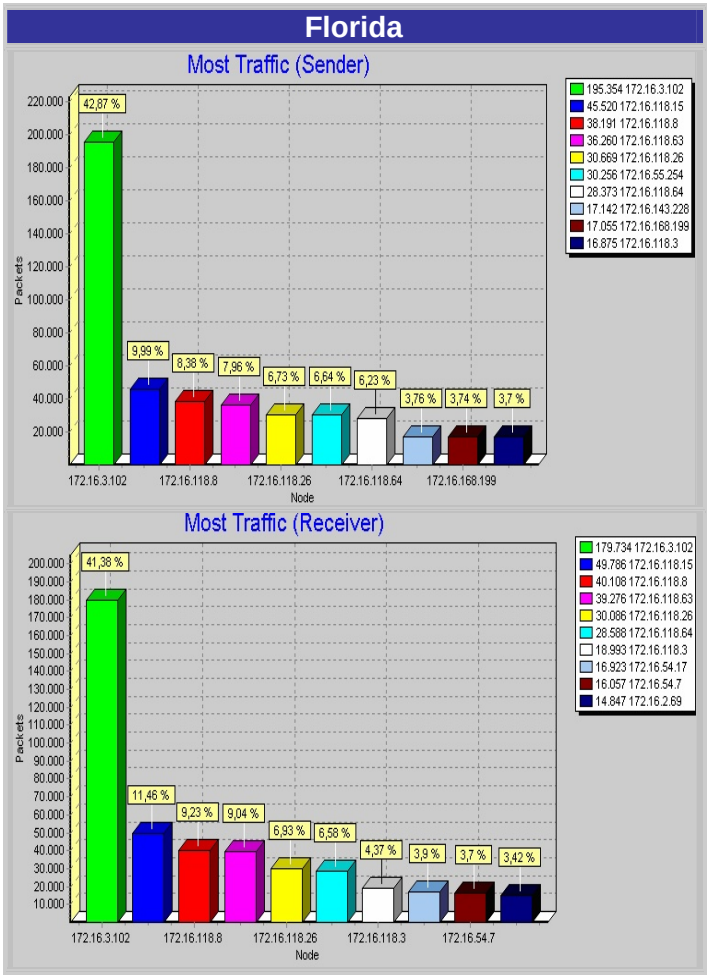


Figura 5.31. Nodos de Mayor Tráfico Enviado y Recibido – Sede Florida (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.118.15	EQUIPO15
172.16.118.8	FGOMEZ
172.16.118.63	EQUIPO9
172.16.118.64	BIBLIOTECA
172.16.118.26	SGCFLORIDA
172.16.118.3	EQUIPO3

Tabla 5.20. Nombres de los Servidores y de los Equipos de Mayor Tráfico - Sede Florida

[92] Ver Anexo B.3.2.6 Nodos de mayor tráfico enviado - Sede Florida y B.3.2.7 Nodos de mayor tráfico recibo – Sede Florida
[93] Ver Figura 5.16. Nodos de Mayor Tráfico Enviado y Recibido – Sede Florida

5.3.8.4.3 Sede Girón[94]

De la misma manera, el volumen del tráfico según el Host es prácticamente el mismo encontrado en el Router Huawei ya presentado en la sección 5.3.3.4.3

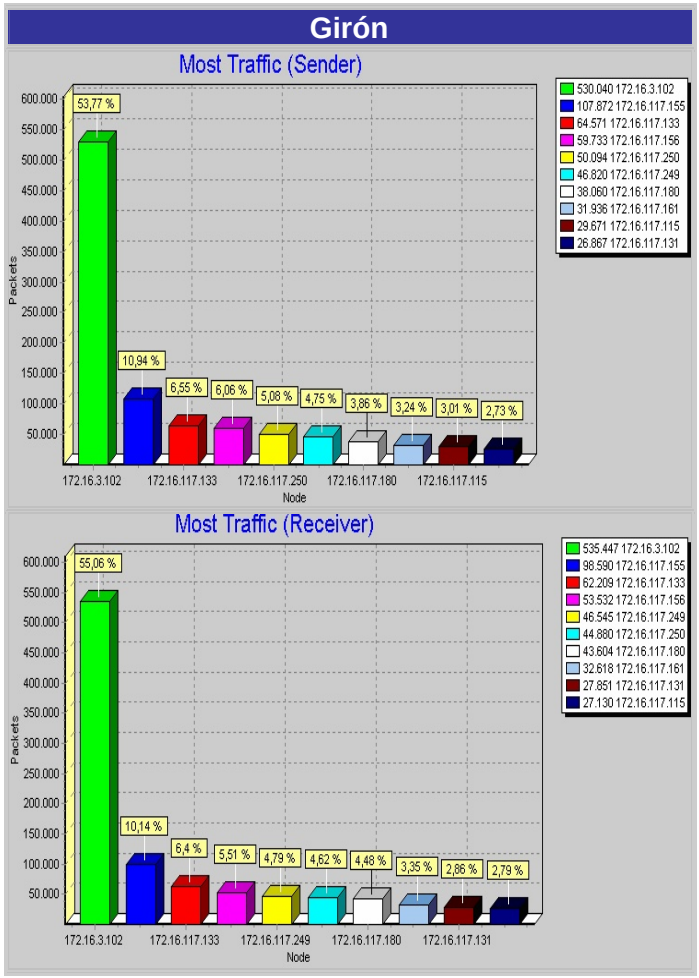


Figura 5.32. Nodos de Mayor Tráfico Enviado y Recibido – Sede Girón (Fuente: Autores)

Dirección IP	Nombre de Equipo
172.16.117.155	No se detectó
172.16.117.133	No se detectó
172.16.117.156	No se detectó
172.16.117.249	IS~MARICELA
172.16.117.250	CIPINTO

Tabla 5.21. Nombres de los Hosts de Mayor Tráfico - Sede Girón

[94] Ver Anexo B.3.3.6 Nodos de mayor tráfico enviado - Sede Girón y B.3.3.7 Nodos de mayor tráfico recibo – Sede Girón

5.3.9 Análisis TCP y UDP

Dado el alto índice de paquetes de la capa de transporte en las capturas, se decidió analizarlos detalladamente para determinar las razones por las cuales se presentan tan elevados índices de tráfico de éste tipo.

Este análisis se realizó escogiendo una muestra aleatoria de 10 minutos del tráfico de cada uno de los días, uniéndolas, filtrando los paquetes TCP y UDP respectivamente, y exportándolos a texto para su procesado. Posteriormente se realizó un análisis en Access para determinar los puertos asociados a estos paquetes (Fuente y Destino) con mayor tráfico.

El tamaño total de la muestra fue de 651’518.342 bytes de los cuales 261’220.242 bytes corresponden a tráfico TCP y 169’817.182 corresponden a tráfico UDP, lo que supone un total de 220’480.918 bytes de tráfico de otros protocolos diferentes a UDP y TCP, como se muestra en la gráfica a continuación:

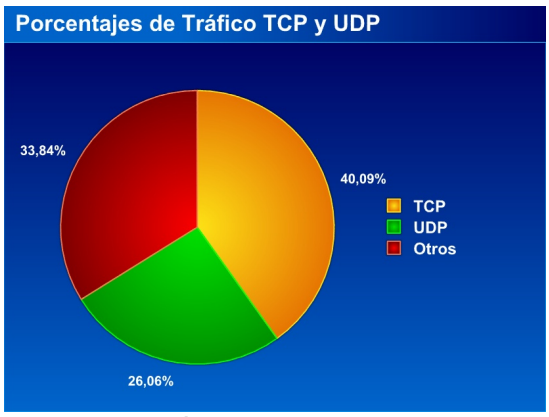


Figura 5.33. Porcentaje de tráfico TCP y UDP en el enlace (Fuente: Autores)

Como se esperaba, según lo observado en el análisis de protocolos de cada una de las sedes, el tráfico de capa de transporte corresponde a más del 60% del tráfico total del enlace, por lo tanto se hace necesario el estudio para determinar las razones por las cuales se presenta tan elevado porcentaje.

A continuación se presentan los resultados de dicho análisis:

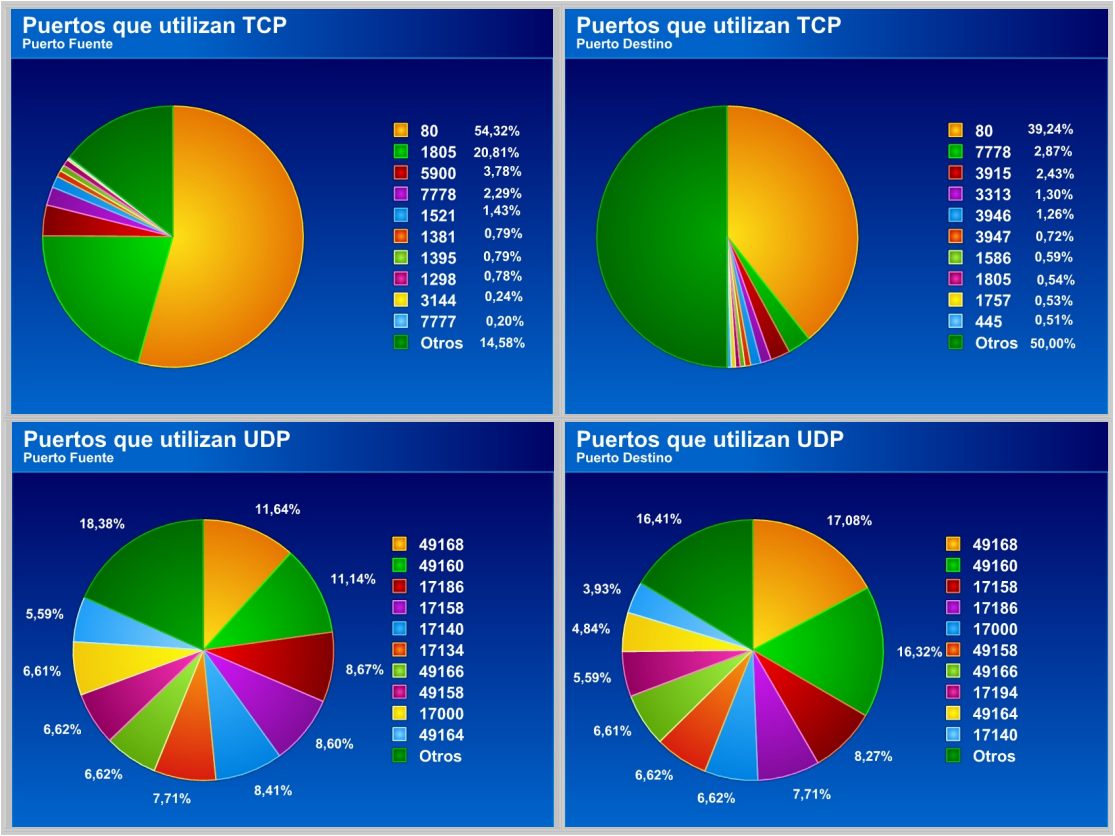


Figura 5.34. Distribución de puertos que utilizan los protocolos de capa de transporte TCP y UDP (Fuente: Autores)

Para poder realizar un correcto análisis de los resultados que se presentan en la figura anterior, se debe tener en cuenta la distribución de los puertos según la IANA[95], organismo responsable de asignar los puertos TCP y UDP para usos específicos, según la cual los números de puertos se dividen en tres grupos principales: Los conocidos, los registrados y los Dinámicos y/o privados.

Tipo de Puerto	Rango
Conocido	0-1023
Registrado	1024-49151
Dinámico o Privado	49152-65535

Tabla 5.22. Tipos de Puertos definidos por la IANA

En las gráficas del protocolo TCP, se observa que uno de los puertos fuente y destino que más que más aporta al tráfico TCP es el 80, que corresponde al servicio Web.

[95] IANA: Internet Assigned Numbres Authority

5.4 Gestión de Fallas (Monitoreo con OpManager)[96]

Uno de los principales logros de este proyecto fue proporcionar al SENA REGIONAL SANTANDER una documentación detallada de su red de datos. Sin embargo, dado el carácter dinámico de toda red, se hace necesaria la actualización periódica de esta información.

Para alcanzar este objetivo, se percibió la necesidad de encontrar una herramienta que permitiera monitorear en todo momento el desempeño de la red e informarle al administrador de la misma sobre cambios, estado de los enlaces o fallas en dispositivos.

Esta búsqueda tuvo como resultado la tercera herramienta de monitoreo que se manejó en la Red de Datos del SENA REGIONAL SANTANDER, el OpManager 6.0. Esta herramienta le permite al usuario caracterizar completamente una red, dado que integra funcionalidades como Gestión de Fallas, Gestión de Desempeño, Monitoreo de Redes, Monitoreo de Servidores, Monitoreo de Aplicaciones y Servicios, y Monitoreo de URL.[97]

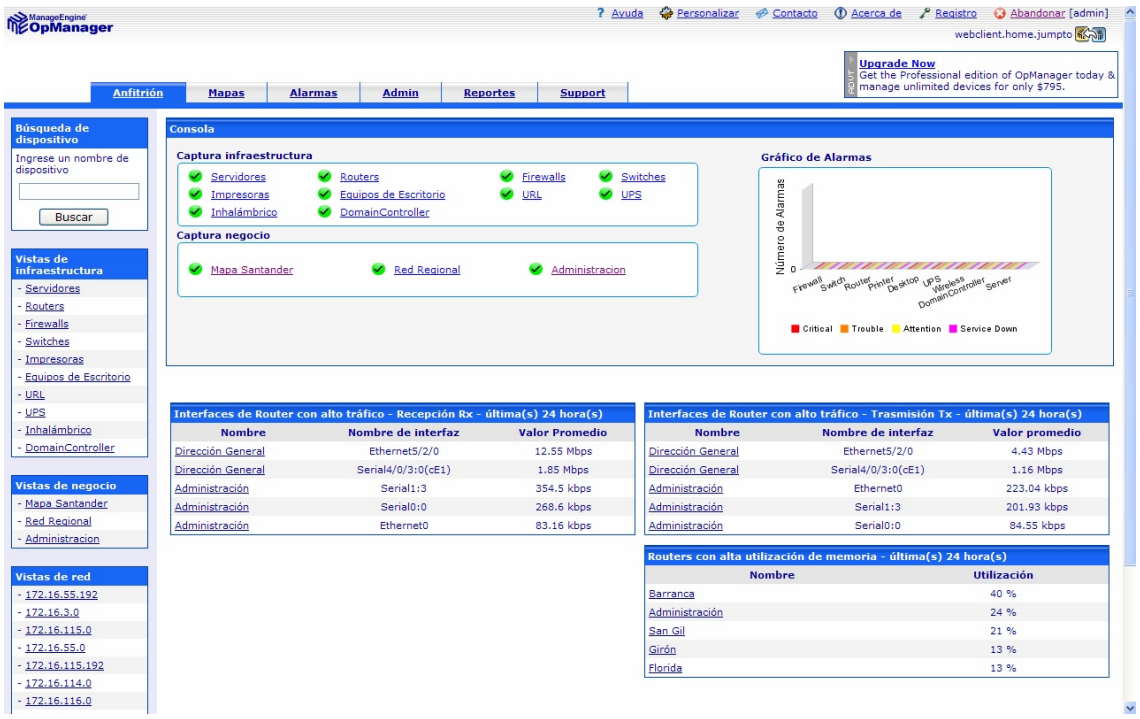


Figura 5.35. Interfaz Gráfica de OpManager 6.0 (Fuente: Autores)

[96] Ver Anexo D: Manual Básico de OpManager
[97] Ver Anexo D.1. Características

Esta herramienta permite además, hacer un descubrimiento de la red para detectar los dispositivos conectados a ella, monitorear sus interfaces, puertos y su desempeño en cuanto a la utilización de procesamiento que cada uno esté manejando en el momento del escaneo y el espacio de memoria y disco disponibles. Toda la información adquirida por el OpManager de cada uno de los dispositivos es manejada por medio de agentes SNMP y se actualiza en tiempo real.

Asimismo, el software cuenta con la capacidad de generar Alarmas de notificación al usuario sobre posibles fallas en la red y su localización específica. También permite crear reportes personalizados de cada dispositivo o interfaz.

Por último, una de las características más llamativas de este software, es la posibilidad de realizar una personalización total de la interfaz gráfica, adaptable a la red LAN de la empresa, creando diagramas de red inteligentes que le muestran al usuario en tiempo real el estado de los dispositivos y de los enlaces.

Este software se instaló en uno de los servidores principales de la red de datos del SENA REGIONAL SANTANDER (IP: 172.16.54.44), y dado que es un software basado completamente en Web, puede ser utilizado desde cualquier Host de la red, accediendo a esta dirección por medio del navegador de Internet e iniciando la sesión de usuario.

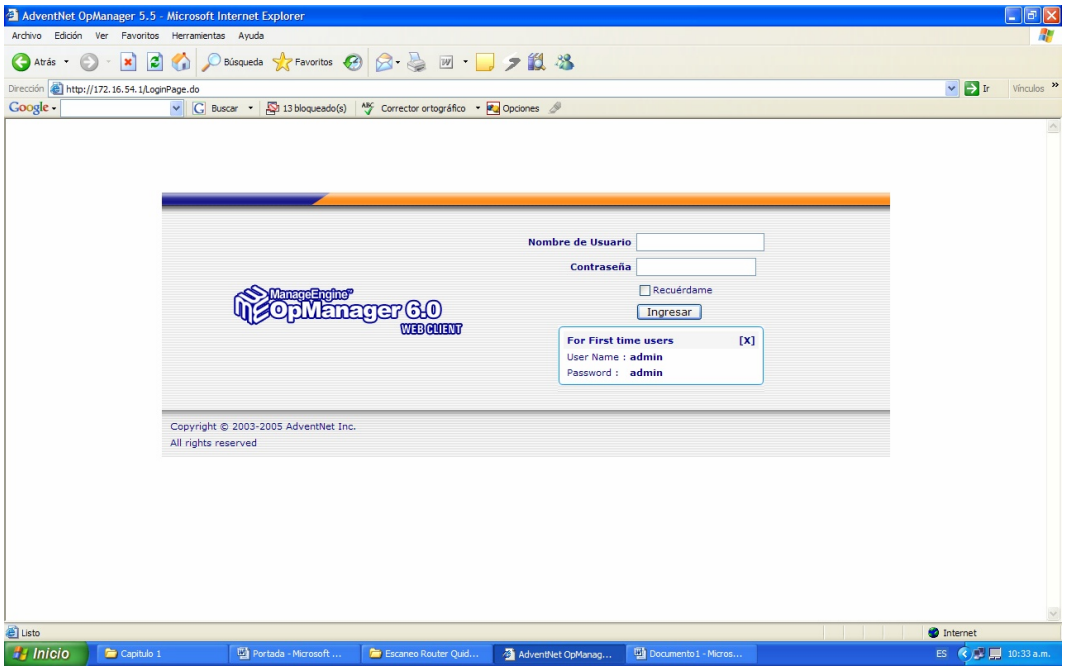


Figura 5.36. Ingreso al OpManager 6.0 por Internet Explorer (Fuente: Autores)

Dado que la versión gratuita del OpManager soporta solamente hasta 20 dispositivos para ser monitoreados, fue necesaria la identificación de los nodos críticos de la Red. Siendo así, se decidió agregar el router de cada Centro, los dos routers principales de la Sede Administrativa, el router principal en la Dirección General en Bogotá y los switches principales de la Sede Administrativa, como se observa en la siguiente tabla.

Nodo	Dispositivo	Sede	Dirección IP	Comunidad SNMP
1	Cisco 3640	Administración	172.16.55.247	Public
2	Huawei 3640	Administración	172.16.55.254	Senalcatel
3	Huawei NE-08	Dirección General	172.16.3.1	Senalcatel
4	Cisco 1750	Barranca	172.16.115.253	Senalcatel
5	Cisco 1750	Girón	172.16.117.254	Public
6	Cisco 1750	Florida	172.16.119.253	Public
7	Cisco 1720	San Gil	172.16.123.254	Public
8	Cisco 1720	Vélez	172.16.131.254	Senalcatel
9	Cisco 1720	Piedecuesta	172.16.178.254	Senalcatel
10	Cisco 1720	Málaga	172.16.183.254	Senalcatel
11	AlcatelOmniswitch 6624	Administración– Piso 5	172.16.55.253	Public
12	Alcatel Omnistack 6648	Administración– Piso 4	172.16.55.250	Public
13	Alcatel Omnistack 6648	Administración– Piso 3	172.16.55.249	Public
14	Alcatel Omnistack 6648	Administración - Piso 2	172.16.55.248	Public
15	Alcatel Omnistack 6648	Empleo	172.16.55.241	Public
16	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 2 Torre 1	172.16.55.251	Public
17	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 3 Torre 1	172.16.55.244	Public
18	Alcatel Omnistack 6624	Centro de Comercio y Servicios Apoyo	172.16.55.243	Public
19	Alcatel Omnistack 6648	Centro de Comercio y Servicios Inglés	172.16.55.245	Public
20	Alcatel Omnistack 6648	Centro de Comercio y Servicios Aulas	172.16.55.246	Public

Tabla 5.23. Dispositivos añadidos en el OpManager instalado en la Sede Administrativa del SENA Regional Santander

Estos dispositivos se agrupan en dos categorías o “Vistas de Infraestructura”, denominadas Switches y Routers. Cada una presenta el estado de los dispositivos y de las interfaces o puertos.

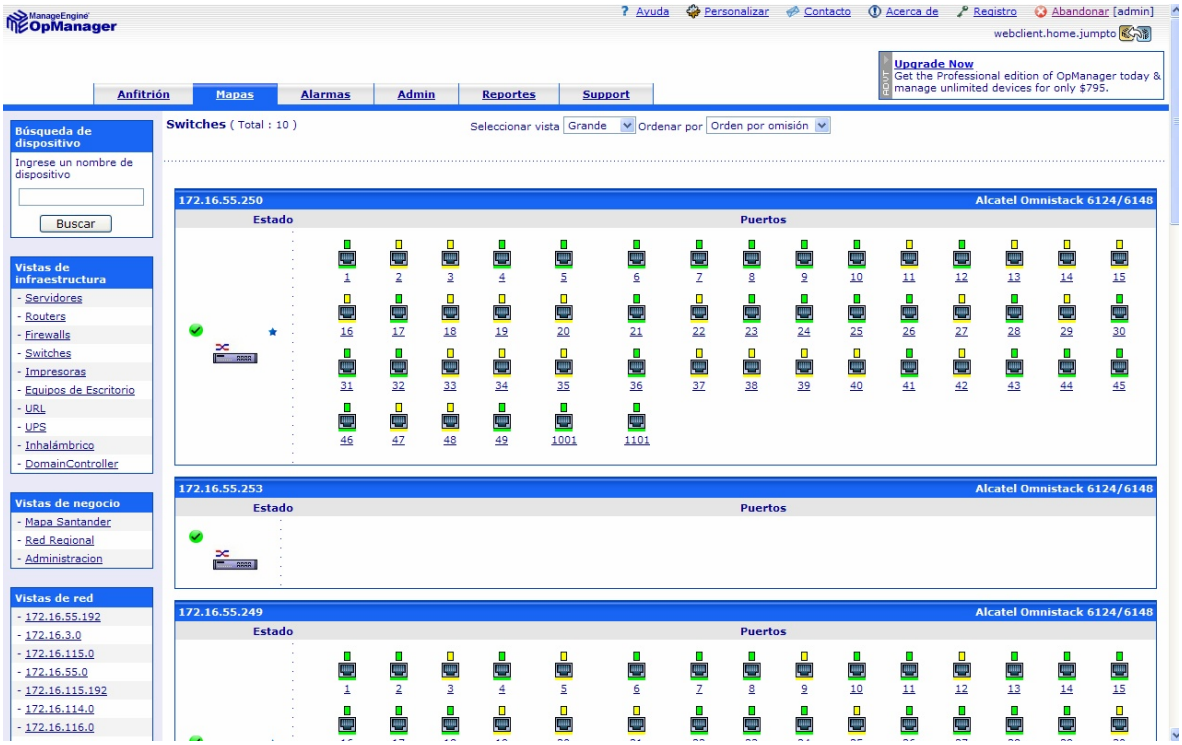


Figura 5.37. Vista de Infraestructura Switches (Fuente: Autores)

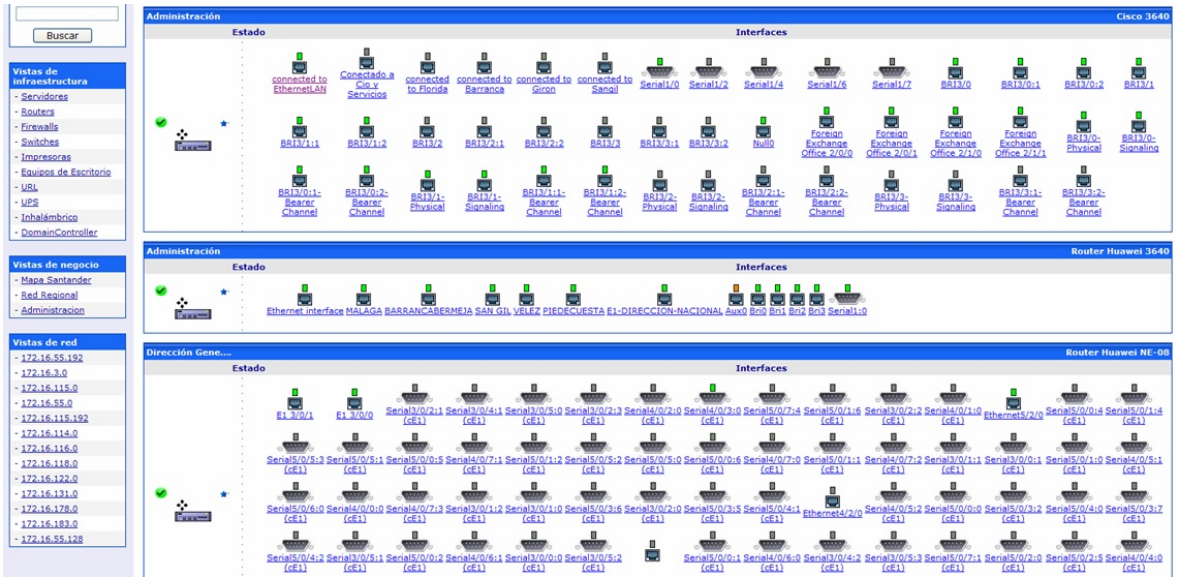


Figura 5.38. Vista de Infraestructura Routers (Fuente: Autores)

Posteriormente, se personalizó la interfaz gráfica del software, adaptándola a la Red de Datos del SENA REGIONAL SANTANDER y tomando como base la documentación realizada de la misma y los diagramas de interconexión elaborados. Estos diagramas personalizados se denominan “Vistas de Negocio”. De esta manera, se crearon las siguientes Vistas de Negocio:

- **Vista Mapa Santander:** Esta vista presenta la ubicación geográfica de todos los centros que conforman el SENA Regional Santander y el estado de sus respectivos enlaces de red según su color.

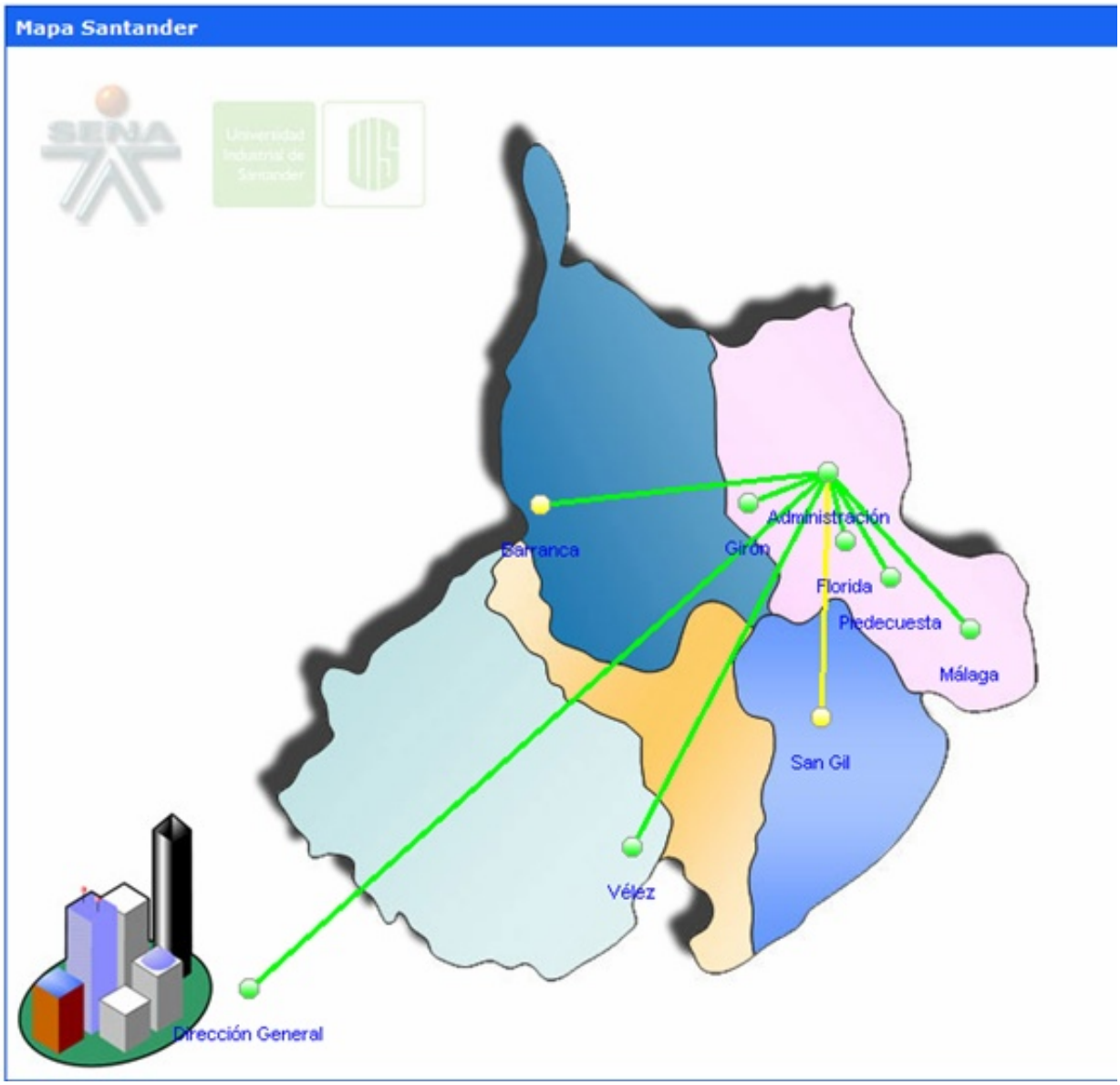


Figura 5.39. Vista de Negocios Mapa Santander (Fuente: Autores)

- **Vista Red Regional:** Esta vista presenta un esquema de toda la Red de Datos del SENA Regional Santander a manera de diagrama de red, con sus respectivos enlaces, routers y su estado

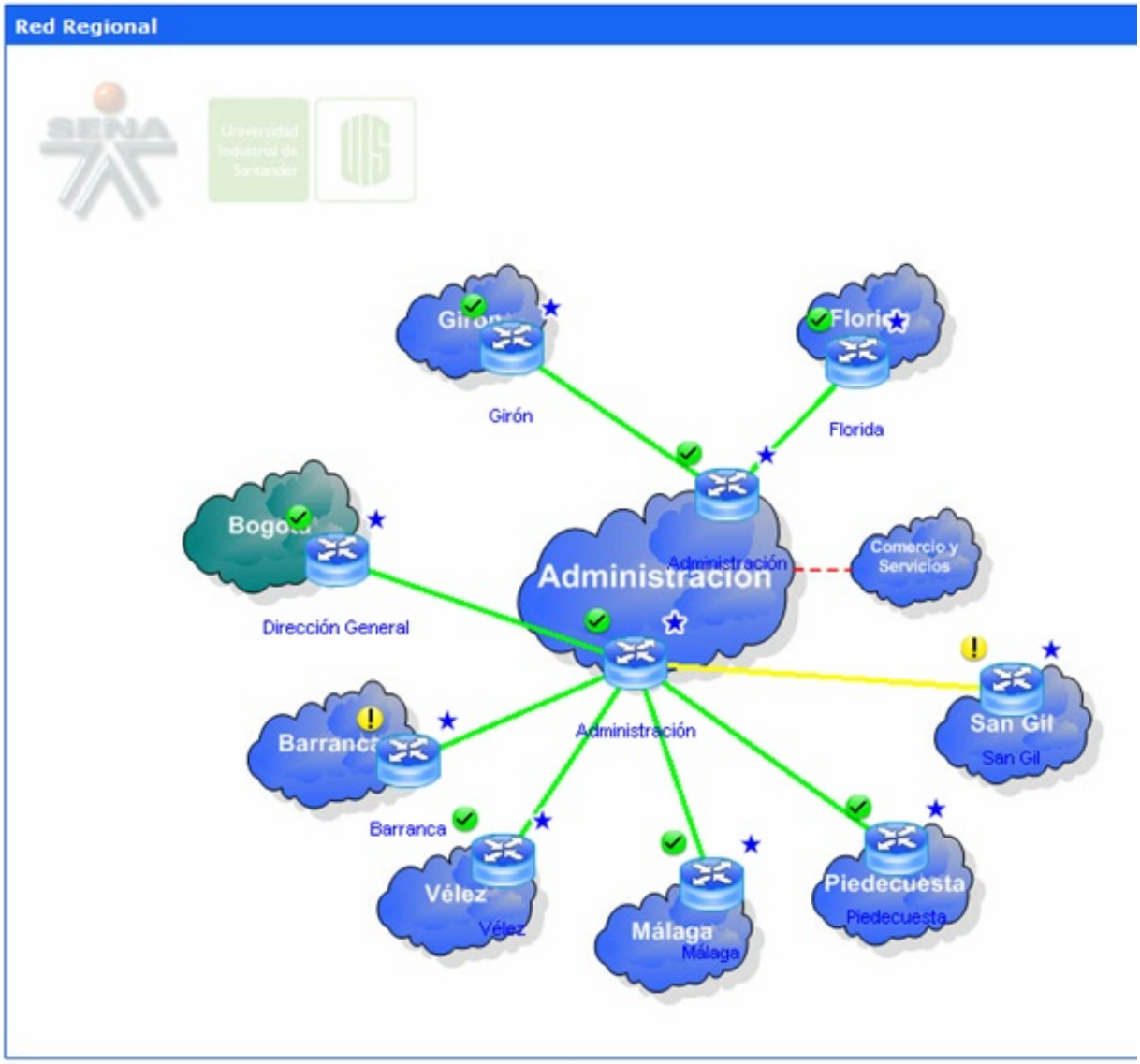


Figura 5.40. Vista de Negocios Red Regional (Fuente: Autores)

- **Vista Administración:** Esta vista, presenta un esquema de la red de datos de la Sede Administrativa del SENA Regional Santander, que incluye los dos routers principales y los swiches que se encuentran instalados en cada uno de los edificios.

Permite obtener información sobre los enlaces de los dispositivos y el estado de los mismos en cada una de las dependencias de la Sede Administrativa.

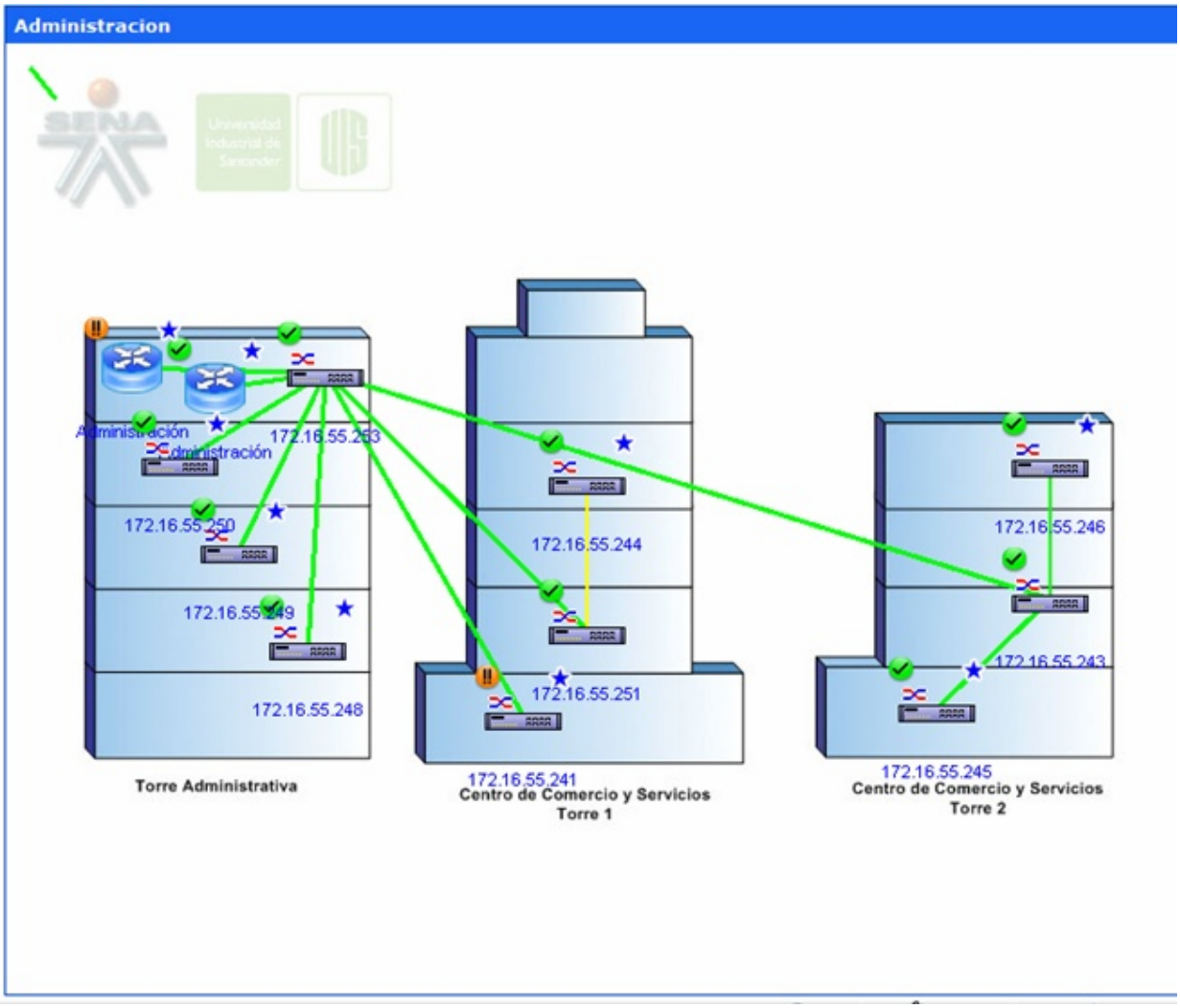


Figura 5.41. Vista de Negocios Administración (Fuente: Autores)

Para ilustrar el proceso de instalación, configuración, personalización y manejo de esta potente herramienta, se elaboró un manual básico, que se anexa al final de este libro.[98]

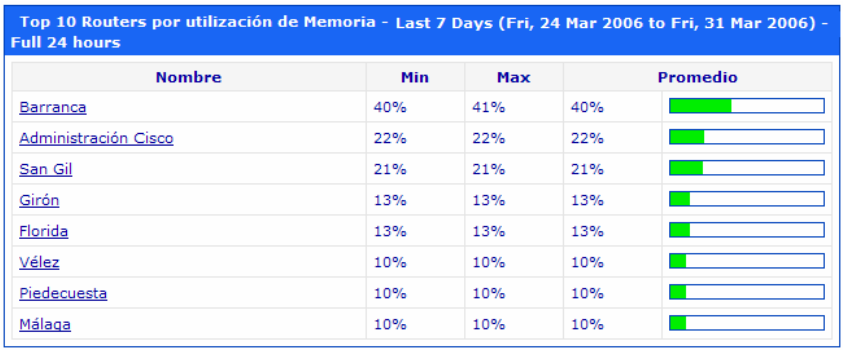
[98] Ver Anexo C: Manual Básico de OpManager 6.0

5.4.1 Resultados obtenidos con OpManager[99]

Los resultados que se presentan a continuación, corresponden a los reportes generados por el OpManager durante un mes (desde el 8 de abril al 8 de mayo de 2006). Estos reportes se anexan al final del presente documento.

5.4.1.1 Utilización de Memoria de los Routers

Durante el monitoreo se observó una alta utilización de memoria en el Router de la Sede de Barrancabermeja, superando incluso la utilización de memoria en el Router Cisco de la Sede Administrativa que maneja mucho más tráfico.



Top 10 Routers por utilización de Memoria - Last 7 Days (Fri, 24 Mar 2006 to Fri, 31 Mar 2006) - Full 24 hours

Nombre	Min	Max	Promedio
Barranca	40%	41%	40%
Administración Cisco	22%	22%	22%
San Gil	21%	21%	21%
Girón	13%	13%	13%
Florida	13%	13%	13%
Vélez	10%	10%	10%
Piedecuesta	10%	10%	10%
Málaga	10%	10%	10%

Figura 5.42. Utilización de Memoria en los Routers (Fuente: Autores)

5.4.1.2 Utilización de las Interfaces de los Routers

Como era de esperarse, las interfaces con una mayor tasa de transferencia y un mayor índice de utilización, son la interfaz Ethernet 5/2/0 del router Huawei NetEngine 08E que corresponde a la Red LAN de la Dirección General, la interfaz Serial 4/0/3:0 del mismo router, que corresponde al enlace E1 con la Sede Administrativa de la Regional Santander y la interfaz Serial 0:0 del router Huawei Quidway 3640 de la Sede Administrativa, que corresponde al mismo enlace E1 con la Dirección General.

También se observa un alto índice de tráfico en las interfaces del router de la Sede Málaga, que incluso llega a ser superior que en algunas de las interfaces de los routers de la Sede Administrativa.

5.4.1.3 Utilización de los puertos de los Switches

OpManager también permite elaborar reportes que incluyan los puertos de los switches de mayor tráfico. Se identificaron algunos puertos de alto índice de tráfico transmitido en los switches 172.16.55.245, 172.16.55.248 y 172.16.55.249.

[99] Ver Anexo D.15 Reportes Generados con OpManager en la Red de Datos del SENA REGIONAL SANTANDER

6. ESTUDIO DE COSTOS DE TELEFONIA

Con el fin de determinar el estado actual de telefonía en el Sena Regional Santander Sede Bucaramanga en cuanto a costos, se realizó un estudio de los costos de telefonía dirigido por el Ingeniero Humberto Luís Duran[100] A continuación, se analizarán sus resultados.

6.1 Estado Telefonía en Bucaramanga

El SENA REGIONAL SANTANDER en Bucaramanga está conformado por la Sede Administrativa, el Centro de Comercio y Servicios, el Servicio de Empleo y otras dependencias que laboran en la carrera 27 entre calles 15 y 16. Esta sede presenta un alto costo de telefonía tanto local, larga distancia y celulares. El análisis después de un mes[101] de seguimiento presentó los siguientes resultados:

Existen 79 líneas telefónicas en cobre proveídas por Telebucaramanga distribuidas así:

- PBX 6324828 con 22 líneas las cuales se utilizan exclusivamente de manera entrante.
- PBX 6356611 con 3 líneas también de forma entrante.
- Existen 3 líneas directas asignadas a faxes.
- Existen 2 líneas asignadas para conexiones ADSL.
- Existen 47 líneas aisladas como directos, los cuales en su mayoría se utilizan de forma entrante, ya sea porque la línea esta asignada a un funcionario y este no la usa o simplemente no sabe que la tiene. En algunos casos las líneas no están asignadas.

Asimismo, existe una línea E1 (6800600) con TELECOM, conformada por 30 líneas digitales para tráfico entrante y 30 líneas digitales para tráfico saliente. Además, se pagan mensualmente 8 pares aislados.

De esta manera, existen en total 147 líneas telefónicas soportando el tráfico de voz de la Sede de Bucaramanga.

[100] Tutor de la presente práctica en el SENA
[101] Este mes se refiere a Septiembre de 2005

6.2 Seguimiento del consumo en el mes de Septiembre:

Para revisar el consumo en el mes de Septiembre se utilizó un software[102] que permite capturar toda la información sobre el consumo saliente de la planta telefónica Lucent Definity con la que cuenta el SENA a nivel Bucaramanga. Este consumo saliente aplica tanto a llamadas de larga distancia, llamadas locales y llamadas a celulares. El software se ejecutó durante el mes de Septiembre, presentando los siguientes resultados.

6.2.1 Llamadas Locales:

Septiembre				
Valor Impulso (pesos)	**Llamadas**	**Impulsos**	**Valor (pesos)**	**Duración (Min)**
67 pesos	**36.474**	**38.575**	**2´583.266**	**90.652**

Tabla 6.1. Llamadas locales.

Se realizaron 36.474 llamadas a teléfonos locales en Bucaramanga, lo que significa un promedio diario de 1.658 llamadas/día hábil.

Estas llamadas generaron una impulsación telefónica de 38.575 que al precio actual[103] de $67 impulso dan un valor para el mes de $2´583.266

Todas las llamadas del mes duraron 90.652 minutos, lo cual corresponde a 2.35 minutos por impulso, aproximadamente.

6.2.2 Llamadas larga distancia y a celulares:

Septiembre				
Operador	**Valor Minuto**	**Llamadas**	**Minutos**	**Valor**
Ola	34,8	934	1.873	65.180
Movistar	301,6	2.123	3.227	973.263
Comcel	301,6	1.798	4.335	1.307.436
Dirección General (Ola)	301,6	1.130	3.945	1.189.812
Subtotal:		**5.985**	**13.380**	**3´535.692**
Orbitel (07)	290	36	121	35.090
Telecom (09)	200	1.292	3.984	796.800
TOTAL:		**7.313**	**17.485**	**4´332.492**

Tabla 6.2. Llamadas larga distancia y celulares.

[102] Este software fue diseñado por el Ingeniero Humberto Luis Duran.
[103] Se refiere al precio del impulso que aplica al mes de Septiembre del 2005.

Se realizaron 7.313 llamadas de larga distancia y a celulares con un promedio diario de 332 llamadas diarias para los 22 días hábiles del mes de Septiembre con un consumo de minutos de 17.485 minutos y un costo total de $4´332.492 discriminadas de la siguiente forma:

- 1.130 llamadas al conmutador de la Dirección General con una duración de 3.945 minutos las cuales salieron por los celufijos de OLA programados en la planta telefónica de esa forma y su costo asciende a $1´189.812 dado que el valor minuto es a $302
- Se efectuaron 1.328 llamadas de larga distancia a teléfonos diferentes al de la Dirección General del SENA.
- 934 llamadas a celulares OLA con un consumo de 1.874 minutos direccionados también a los celufijos; el costo de estas llamadas es de $65.180 dado que el valor minuto a OLA es de aproximadamente $35 por ser el Sena pionero en esta telefonía.
- 2.123 llamadas a MOVISTAR con un consumo de 3.227 minutos direccionados a los celufijos; el costo de estas llamadas es de $973.263 dado que el valor minuto por OLA a Movistar es de $302.
- 1.798 llamadas a COMCEL con un consumo de 4.335 minutos direccionados a los celufijos; el costo de estas llamadas es de $1.307.436 dado que el valor minuto por OLA a Comcel es de $302.

Se destaca la gran cantidad de llamadas a teléfonos celulares como se muestra en las siguientes figuras.

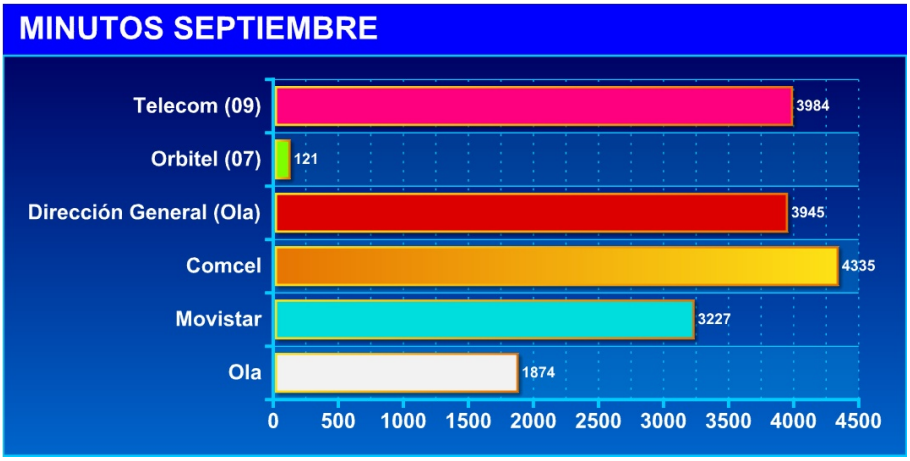


Figura 6.1. Llamadas celulares y sus operadores respectivos. (Fuente: Autores)

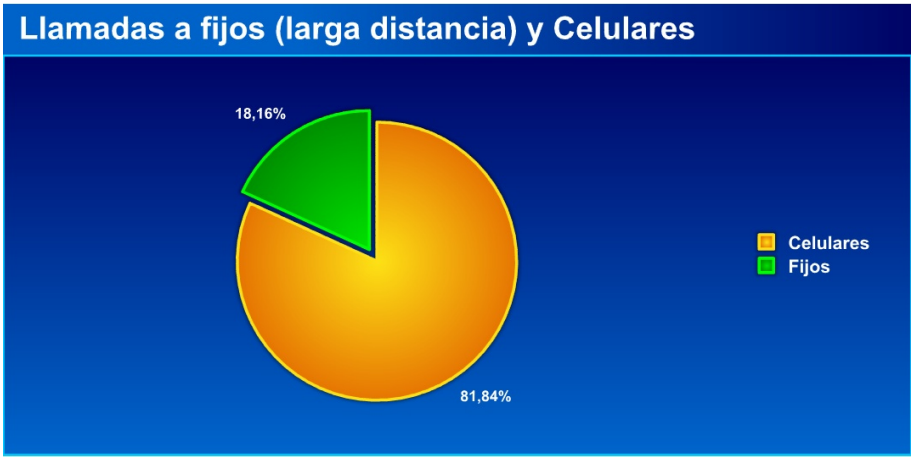


Figura 6.2 Llamadas a celulares y fijos larga distancia. (Fuente: Autores)

6.2.3 Análisis de resultados

Del total de llamadas realizadas durante el mes de Septiembre del 2005, se encontró que el 83.3% de llamadas correspondió a llamadas locales, el 13.67% a celulares y el 3.03% a llamadas de larga distancia. El consumo en impulsos de llamadas locales (promedio 1.658 llamadas diarias) es bastante alto[104], sin embargo como se puede apreciar en la Tabla 6.2, este no es el causante de los altos costos en la telefonía.

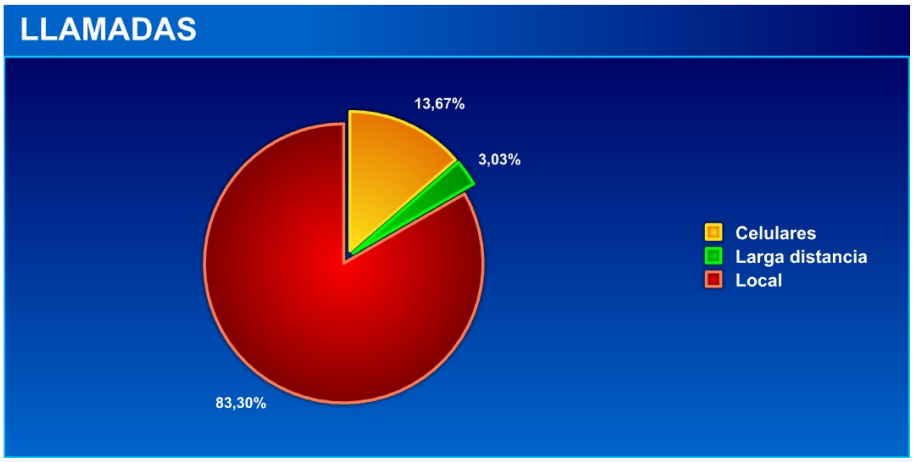


Figura 6.3. Total llamadas mes de Septiembre (Fuente: Autores)

El consumo de llamadas de celulares y larga distancia a pesar de ser mucho menor que el de llamadas locales es exagerado[105] (promedio diario de 332 llamadas) y corresponde a la principal causa de los altos costos de telefonía, teniendo en cuenta además, que las llamadas a celulares tienden a ser más que todo personales y no institucionales.

[104] Ver Figura 6.3: Total de llamadas mes de Septiembre
[105] Ver Figura 6.2: Llamadas a celulares y fijos larga distancia

Otra característica importante, que se puede apreciar en la figura 6.1, es la gran cantidad de llamadas hacia la Dirección General a través de los celufijos de Ola, lo cual representa un costo mensual de más de 1´000.000 de pesos. Lo que refleja la necesidad del SENA de mantener una comunicación constante con la Sede Bogotá.

Este costo podría ser disminuido significativamente si se implementase un sistema de Voz Sobre IP en el que la voz viaja sobre la red de datos ya existente en el SENA sobre el protocolo IP, sin necesidad de salir a la red pública PSTN[106]

6.3 Costos de telefonía Regional Santander

A continuación se presentan los gastos en telefonía para cada una de los Centros del SENA REGIONAL SANTANDER entre el mes de Enero y el mes de Agosto de 2005. Estos datos estan basados en la facturas de pago de telefonía de cada una de las sedes.

MES / SEDE	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO
Administrativa	5.489.570	14.617.640	12.029.950	6.671.740	8.977.989	3.587.900	12.176.490	9.048.190
Florida	1.266.240	1.157.930	1.157.930	502.216	1.358.380	1.434.010	659.964	1.656.100
Girón	750.950	940.090	1.124.596	1.088.118	865.880	1.054.260	1.607.768	1.548.150
Piedecuesta	454.400	1.441.280	821.034	1.278.116	515.040	445.590	770.838	382.250
San Gil	550.010	1.106.760	4.015.750	4.996.100	1.268.220	1.584.680	267.450	2.437.360
Barranca	2.242.790	8.095.690	1.979.900	1.683.570	10.046.230	2.108.690	2.231.100	2.548.990
Málaga	985.600	4.137.860	0	4.538.390	949.510	1.158.200	1.968.220	1.221.030
Vélez	784.430	2.910.960	2.514.510	2.551.400	572.660	1.109.550	1.766.760	832.170

Tabla 6.3. Costos telefonía[107] entre Enero y Agosto de 2005 por sedes.

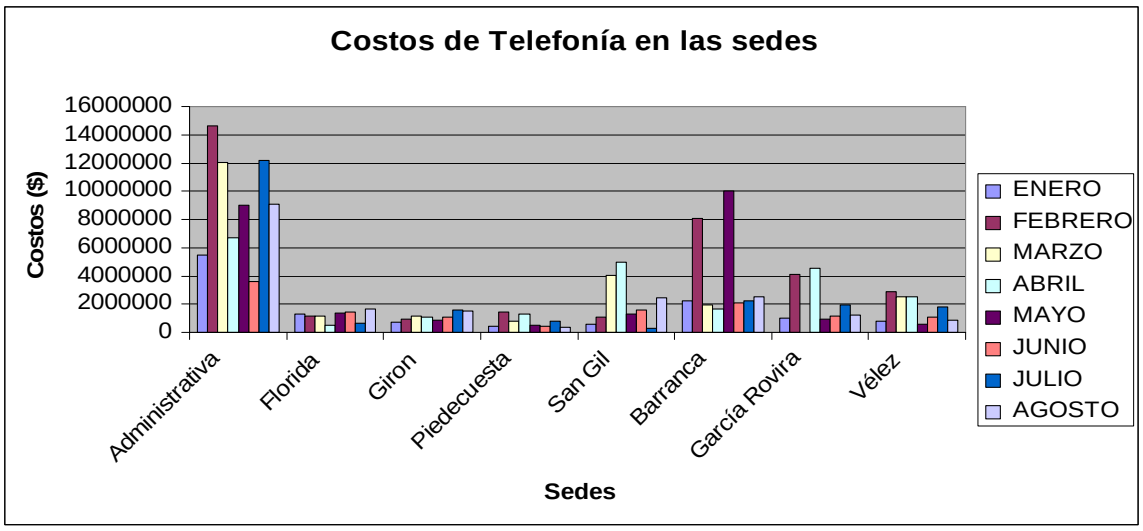


Figura 6.4. Costos de telefonía en las sedes. (Fuente: Autores)

[106] Public Switch Telephon Network
[107] Estas cantidades estan en pesos.

Esto corresponde a los siguientes totales mensuales en cuanto a gastos en telefonía, asumidos por la Sede Administrativa.

Mes	Pago ($)
ENERO	12.523.990
FEBRERO	34.408.210
MARZO	23.643.670
ABRIL	23.309.650
MAYO	24.553.909
JUNIO	12.482.880
JULIO	19.463.169
AGOSTO	19.674.240

Tabla 6.4. Costos totales de telefonía entre Enero y Agosto de 2005.

Como se hace evidente, los costos de telefonía, son bastante elevados, con un promedio por mes de $21'266.464 pesos, lo que sugiere buscar opciones que permitan minimizarlos. Una de estas opciones es la implementación de Canales de Voz sobre IP entre la Sede Administrativa y cada uno de sus Centros.

6.4 Ahorros mensuales de la implementación de VoIP

Según el anterior estudio de costos, una implementación de canales IP entre la planta telefónica de la Regional Santander y la planta telefónica de la Dirección General supone una reducción de mas de $1'000.000 mensuales en las facturas en concepto de telefonía a la Dirección General[108], dado que al viajar por la Red Interna de Datos del SENA, la voz no necesita salir hasta proveedores externos del servicio como Ola, ETB, Orbitel, etc, y por lo tanto el costo de las llamadas sería prácticamente $0.00

De esta manera, teniendo en cuenta que en la tabla 6.4 los costos totales de telefonía por mes como mínimo fueron de un poco más de $12'000.000, y considerando, siendo pesimistas, que por lo menos un 25% de ese total mensual corresponde a llamadas de carácter institucional, la implementación de un servicio de este tipo para todo el SENA REGIONAL SANTANDER, supone unos ahorros mensuales en telefonía de por lo menos $3´000.000

Sin embargo, hay que tener en cuenta que para implementar una posible solución completa de Voz sobre IP, es necesario realizar una inversión inicial en infraestructura

[108] Ver Tabla 6.2 Llamadas a Larga Distancia y Celulares

que permitan realizar un puente entre las redes IP y PSTN[109] e incrementar el ancho de banda de los enlaces según el número de líneas que se deseen instalar, que garantice la calidad en la transmisión de la voz y no consuma la porción del ancho de banda destinado al tráfico de datos. Teniendo en cuenta lo anterior, se realizaron los siguientes cálculos:

Inversión Inicial en equipos de voz IP[110]:

Concepto	Precio Unidad	Precio Total
7 gateways para cada uno de los centros	699 USD	4893 USD
1 gateway/gatekeeper para la Sede Administrativa	3600 USD	3600 USD
Total		8493 USD

Tabla 6.5. Inversión inicial en equipos de Voz IP.

Suponiendo una financiación a 36 meses y un cambio de $2500 pesos colombianos por dólar, tenemos aproximadamente un monto mensual de $600.000 pesos, correspondiente a la inversión inicial.

Los costos asociados al aumento en el ancho de banda de los enlaces son los siguientes, y se calcularon en base a los valores cotizados con Colombia Telecomunicaciones S.A ESP. (TELECOM) que se presentan en los anexos al final del libro.[111]. Asimismo, se tuvo en cuenta que un canal para voz IP consume aproximadamente 16 Kbps[112] del ancho de banda, por lo que los cálculos se realizaron pensando en la implementación de 30 líneas IP en la Sede Administrativa y 15 en cada uno de sus centros.

Sede	Ancho de Banda	Capacidad	Costo
Bucaramanga	512 Kbps	30 líneas	$ 1’575.000
Barranca	256 kbps	15 líneas	$ 975.000
Girón	256 kbps	15 líneas	$ 975.000
Florida	256 kbps	15 líneas	$ 975.000
San Gil	256 kbps	15 líneas	$ 975.000
Vélez	256 kbps	15 líneas	$ 975.000
Piedecuesta	256 kbps	15 líneas	$ 975.000
Málaga	256 kbps	15 líneas	$ 975.000
Total			$ 8’400.000

Tabla 6.6. Costos mensuales para aumentar los enlaces

[109] El dispositivo que se encarga de esta tarea se conoce como Gateway
[110] Ver Anexo C. Propuestas de Proveedores
[111] Ver Anexo C. Propuestas de Proveedores
[112] Ver 3.3.1 Voz Sobre IP y Telefonía IP

Para visualizar con mayor claridad los ahorros correspondientes a telefonía, de implementar una solución del tipo IP, elaboramos la siguiente gráfica.

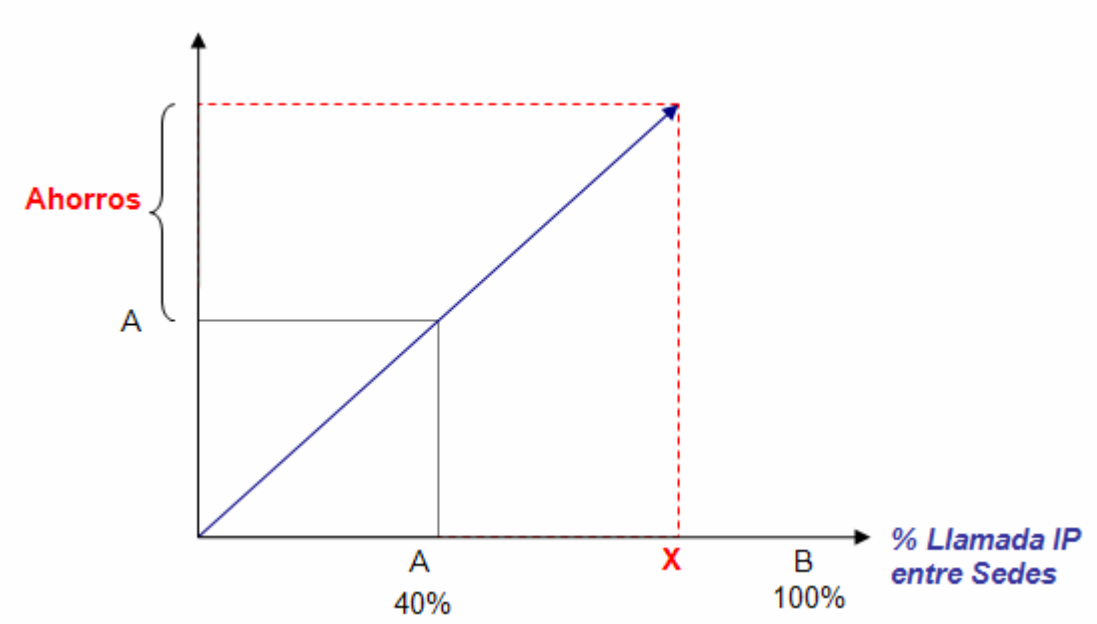


Figura 6.5. Ahorros mensuales en telefonía con la implementación de Voz IP. (Fuente: Autores)

El valor A, corresponde al costo mensual en el aumento del ancho de banda de los enlaces para que permitan una buena calidad en la comunicación de voz, más la inversión inicial en los equipos de voz IP o en su arrendamiento, según el proveedor de los servicios, lo que significa que A = 8´400.000 + 600.000 = $ 9’000.000 pesos.

Mientras tanto, el valor B, es el promedio pagado mensualmente por el SENA REGIONAL SANTANDER por conceptos de telefonía, es decir, B = $21’266.464 pesos, este valor corresponde al 100% de las llamadas.

Como se puede apreciar en la gráfica, el valor A, corresponde al 40% del valor B, lo cual quiere decir que solamente si el 40% o más del total de las llamadas entre las sedes se efectúan a través de la red IP, se percibirán ahorros significativos por conceptos de telefonía.

7. EVALUACION DE LA RED

Suponiendo que en cada sede la mitad de los usuarios se encuentran haciendo uso de la red en un momento determinado, se calculó la velocidad de acceso por host para cada una, según el ancho de banda designado actualmente en ellas.

Sede	Usuarios	Velocidad Actual	Vel. de acceso actual por host
B/manga sin videoconf. B/manga con videoconf.[113]	397	1152 kbps 640 kbps	5,76 Kbps 3,2 Kbps
Barrancabermeja	281	128 Kbps	0,9 Kbps
Girón	149	128 Kbps	1,8 Kbps
Floridablanca	138	128 Kbps	1,96 Kbps
San Gil	85	128 Kbps	3,2 Kbps
Vélez	82	128 Kbps	3,2 Kbps
Piedecuesta	42	128 Kbps	6,4 Kbps
Málaga	50	128 Kbps	5,12 Kbps
TOTAL	1224	2048 Kbps	

Tabla 7.1. Velocidades de acceso actuales por host

En general, se detectaron niveles muy bajos de acceso por host en todas las sedes, en especial en las de Barranca, Girón y Florida.

A continuación se incluyen los resultados de la evaluación de la situación actual de la Red de Datos del SENA REGIONAL SANTANDER y el servicio de telefonía.

7.1 Internet

Concepto	Acceso a Internet
Situación Actual	▪ Todas las sedes de la Regional Santander se conectan a Internet por medio del Servidor Proxy de la Dirección General, lo que adiciona mucho tráfico al enlace, relentizando aplicaciones o videoconferencias. ▪ En la Dirección General, el servidor Proxy es del tipo AnalogX, lo cual indica que no maneja caché, lo que induce a un congestionamiento del canal cuando se realizan peticiones simultáneas.

[113] Suponiendo que la videoconferencia consume un máximo de 512 kbps de ancho de banda total del enlace.

Como mejorar	▪ Utilizar un servidor Proxy alterno exclusivo para el acceso a Internet de los Centros y reservar el servidor Proxy de la Dirección General para el acceso a Internet de la Sede Administrativa. ▪ Utilizar servidores Proxy que manejen caché

Concepto	Uso de Internet
Situación Actual	▪ Se detectó un uso elevado del Internet de parte de los usuarios en las Sedes para fines no académicos, lo cual implica, además de una pérdida de tiempo y de un consumo apreciable del ancho de banda, un riesgo para los hosts en cuanto a posibles infecciones con Virus Informáticos.
Como mejorar	▪ Monitorear en todo instante el tráfico de la red en todas las sedes para detectar usuarios problema que estén generando un tráfico excesivo. ▪ Establecer unas políticas claras sobre el uso del Internet en la Red de Datos del SENA REGIONAL SANTANDER. ▪ Instalar en el Proxy de la Red Regional un Firewall que permita poner en funcionamiento estas políticas

Concepto	Velocidad de Conexión
Situación Actual	▪ Los Centros de la Regional Santander cuentan con velocidades de conexión a Internet muy bajas y que no dan abasto con la demanda de tráfico de los usuarios.
Como mejorar	▪ El aumento del ancho de banda en las conexiones entre los centros mejoraría notoriamente a la calidad del servicio ya que la demanda de aplicaciones y la educación virtual se han convertido en una prioridad para el SENA. Sin embargo, el aumento del la velocidad de conexión de los centros debe ir de la mano con la administración adecuada del ancho de banda para que el usuario no lo malgaste en tareas innecesarias.

7.2 Red Interna

Concepto	Hardware
Situación Actual	▪ Se cuenta con dos Router principales de gran capacidad de manejo de información pero con múltiples interfaces deshabilitadas. ▪ La infraestructura que enlaza a la Sede Administrativa con Telecom, a través del ODU Radio Sagem permite soportar hasta dos canales E1 más. ▪ En muchas de las Sedes aún se trabaja en base a Hubs, los cuales introducen colisiones en los enlaces, disminuyendo su rendimiento. ▪ Los switches principales que interconectan el backbone de la Red Interna de la Sede Administrativa, los Routers y el ODU Radio Sagem son administrados desde Bogotá, por lo tanto en caso de fallos, su tiempo de atención se incrementa.
Cómo mejorar	▪ Los dispositivos subutilizados se pueden aprovechar para incrementar la capacidad de conectividad de la red. ▪ Reemplazar los Hubs existentes en las sedes por switches administrables desde la Sede Administrativa. ▪ Administrar localmente los dispositivos principales de la Red, con la supervisión de personal capacitado.

Concepto	Software
Situación Actual	▪ Las aplicaciones cliente/servidor basadas en Oracle que se trabajan en el SENA son muy pesadas, poco amigables para el usuario y rígidas. Además, exigen una especial configuración de la estación cliente desde la cual se ejecuta la aplicación, lo cual incrementa los costos de soporte. ▪ Dado que las aplicaciones no están completamente terminadas, cada cierto periodo de tiempo se generan actualizaciones y su proceso de instalación en las estaciones cliente es complejo además de que se debe hacer estación por estación. ▪ El esquema cliente/servidor exige la adquisición de licencias de Oracle Client para cada estación donde se instalan las aplicaciones cliente, lo que incrementa los costos de licenciamiento. ▪ Asimismo, se cuenta con un equipo de videoconferencia, que requiere de una infraestructura adecuada para establecer una eficiente utilización de este recurso. El canal de videoconferencia se comparte con el del tráfico de Internet y todas las demás aplicaciones.
Cómo mejorar	▪ Realizar una migración de las aplicaciones a entornos Web, completamente compatibles sobre protocolos y estándares de Internet en los que las aplicaciones residan en un servidor central y estén disponibles para todos los usuarios de forma inmediata. ▪ Implementar un canal dedicado o una porción fija del canal, exclusivamente para videoconferencia, que garantice un ancho de banda y un retardo fijos

Concepto	Cableado
Situación Actual	▪ Las Sedes Administrativa, Barrancabermeja y San Gil cuentan con un backbone en fibra óptica y un cableado UTP Cat. 5e. Las demás sedes cuentan con cableados Cat.5 ▪ En la mayoría de los Sedes se cuenta con centros de cableado que permiten organizar los dispositivos y protegerlos.
Cómo mejorar	▪ Es necesario organizar los centros de cableado, documentarlos y etiquetarlos. ▪ Reemplazar el cableado Cat. 5 existente por Cat. 5e o superior.

Concepto	Conectividad
Situación Actual	▪ La interconexión de las redes LAN de Girón y Florida está implementada en RDSI, mientras que los demás centros cuentan con una línea dedicada, ambas soluciones a 128 Kbps. Sin embargo, según los resultados obtenidos en la etapa de monitoreo, se observó que las interconexiones por RDSI presentaron un menor rendimiento que las de línea dedicada.
Cómo mejorar	▪ Reemplazar las interconexiones RDSI existentes por enlaces dedicados y aumentar la velocidad de le conexión según se requiera en cada centro

Concepto	Asistencia Técnica
Situación Actual	▪ La División de Sistemas de la Regional Santander tiene línea directa con la Dirección General en Bogota para cualquier deficiencia o falla en los enlaces de la Red. Sin embargo, una atención de fallas remota no es tan ágil como se necesita por lo que los tiempos de inactividad de la red en estos casos se incrementan.
Como mejorar	▪ Configurar una herramienta software para la detección de fallas en tiempo real como el OpManager, que permita disminuir los tiempos de atención y resolución de las mismas. ▪ Solicitar la administración local de los dispositivos y la capacitación adecuada para la atención de fallos desde la Sede Administrativa.

7.3 Telefonía

Concepto	Telefonía
Situación Actual	▪ Los costos de telefonía son exagerados. ▪ No existe un control apropiado del uso de las líneas institucionales debido a que la planta telefónica no cuenta con un software que permita hacer seguimiento a las llamadas desde estas líneas. ▪ Se requiere una comunicación telefónica constante de la Sede Administrativa con todos sus Centros y con la Dirección General. ▪ El Sena cuenta con demasiadas líneas telefónicas en la Sede Administrativa.
Cómo mejorar	▪ Implementar un software que permita hacer un seguimiento a las llamadas de los usuarios, así sería posible identificar que funcionarios dan mal uso del servicio de Telefonía. ▪ Implementar una solución del tipo IP para las comunicaciones de voz en la que las llamadas institucionales viajen por la red IP y no requieran salir hasta la red PSTN.

8. REQUERIMIENTOS TECNICOS

Teniendo en cuenta que la velocidad por host mínima que garantiza una tasa de transferencia ágil para los usuarios es de aproximadamente 5 kbps, se determinó que para cada sede las velocidades de acceso deberían incrementarse a las siguientes cantidades. Este cálculo se realizó suponiendo que en cada sede la mitad de los usuarios se encontraban haciendo uso de la red en un momento determinado.

Sede	Usuarios	Velocidad	Vel. de Acceso por host
B/manga sin videoconf. B/manga con videoconf.[114]	397	2048 kbps 1536 kbps	10,24 Kbps 7,68 Kbps
Barrancabermeja	281	1024 Kbps	7,31 Kbps
Girón	149	512 Kbps	7,21 Kbps
Floridablanca	138	512 Kbps	7,87 Kbps
San Gil	85	256 Kbps	6,4 Kbps
Vélez	82	256 Kbps	6,4 Kbps
Piedecuesta	42	256 Kbps	12,8 Kbps
Málaga	50	256 Kbps	5,12 Kbps
TOTAL	1224	4864 Kbps	10,24 Kbps

Tabla 8.1. Velocidades de acceso ideales por host

De acuerdo a lo analizado anteriormente, se procede a describir los requerimientos mínimos necesarios para responder a la demanda de servicios de red a corto plazo, que presenta el SENA REGIONAL SANTANDER.

8.1 Internet[115]

Teniendo en cuenta la cantidad de estaciones de trabajo de las sedes que se incluyen en la tabla 4.2, la cantidad de tráfico y las tasas de transferencia manejadas en cada una, que se presentan en la tabla 5.3, se plantearon los siguientes cambios en el ancho de banda de los enlaces que permitan dar soporte a la demanda de los usuarios.

[114] Suponiendo que la videoconferencia consume un máximo de 512 kbps de ancho de banda total del enlace.
[115] Ver Anexo C. Propuestas de Proveedores

- **Salida a Internet:**

Debe existir independencia en la salida a Internet de cada Sede con el ancho de banda correspondiente a cada una de ellas y descrito en la siguiente tabla:

Sede	Velocidad de Acceso
Bucaramanga y Centro de comercio y Servicios	1024Kbps
Floridablanca	512 Kbps
Girón	512 Kbps
Piedecuesta	256 Kbps
Vélez	256 Kbps
Barrancabermeja	1024 Kbps
Málaga	256 Kbps
San Gil	256 Kbps
TOTAL	3,584 MB

Tabla 8.2 Ancho de banda requerido salida Internet Sedes SENA REGIONAL SANTANDER

- **Ultimo Kilómetro de Interconexión con las Sedes:**

Al implementarse una conexión de tipo Clear Channel o enlace dedicado esta se sujeta a la propuesta del operador del servicio, seria apropiado que fuera fibra óptica.

- **Equipos de interconexión:**

Los equipos de interconexión deben tener algunas características mínimas que permitan manejar QoS[116], independencia de los canales, manejo del ancho de banda solicitado en estos términos de referencia y administración remota con una herramienta software de gestión de redes.

- **Disponibilidad:**

La disponibilidad de los canales entre las Sedes e Internet debe ser del 99.96% mensual por lo menos, garantizando un nivel óptimo de servicio. El no cumplimiento de esto acarreará unas multas que se cobrara como descuentos por motivos de indisponibilidad del canal de interconexión con las Sedes y la salida a Internet.

- **Soporte telefónico:**

Soporte telefónico todos los días del año las 24 horas del día (7 x 24 x 365). Se debe ofrecer un número telefónico de soporte de los ingenieros responsables del servicio, los cuales deben atender las solicitudes de soporte técnico de forma inmediata.

[116] Quality of Service (Calidad de Servicio), es una cualidad que permite programar en el dispositivo la cantidad de ancho de banda máximo y mínimo que utilizarán las aplicaciones IP que se transportarán sobre esta infraestructura de telecomunicaciones.

8.2. Red Interna

Se plantearon los siguientes requerimientos para la red interna, teniendo en cuenta la cantidad de estaciones de trabajo de las sedes que se incluyen en la tabla 4.2, la cantidad de tráfico y las tasas de transferencia manejadas en cada una, que se presentan en la tabla 5.3. También se tuvo en cuenta el requerimiento de ancho de banda que supone implementar una línea de voz IP entre cada una de las sedes y la Sede Administrativa.

- **Canales de interconexión con las sedes:**

Origen	Destino	Velocidad de Acceso
Floridablanca	Bucaramanga	512 Kbps
Girón	Bucaramanga	512 Kbps
Piedecuesta	Bucaramanga	256 Kbps
El Playón	Bucaramanga	128 Kbps
Vélez	Bucaramanga	256 Kbps
Barrancabermeja	Bucaramanga	1024 Kbps
Málaga	Bucaramanga	256 Kbps
San Gil	Bucaramanga	256 Kbps

Tabla 8.3 Ancho de banda requerido canales Sedes regional Santander

  - Canales Clear Channel
  - Todos los canales con Reuso 1:1

- **Optimización de recursos:**

Revisar los distintos dispositivos que pueden estar utilizándose de forma inapropiada, reevaluar sus funciones y con un conocimiento apropiado de su estructura y configuración, sacar un mejor provecho de ellos. Los elementos que no están cumpliendo su labor o no son útiles para una determinada función, deben ser descartados, agrupados e inventariados para que el SENA decida que hacer con ellos. (Podrían dedicarse para fines educativos en los cursos que los requieran)

- **Gestión de red:**

Se recomienda incluir herramientas que faciliten la administración de la red, basadas en tecnología Web o aplicaciones de administración centralizada, que permitan llevar a cabo el monitoreo, la detección de fallas y la configuración/operación de la infraestructura de red.

Estas aplicaciones deben ser instaladas en un PC dedicado exclusivamente a esta función proporcionado por el SENA y deben entregar como mínimo la siguiente información:

- Estadísticas del consumo de ancho de banda por cada Sede
- Estadísticas de la utilización del ancho de banda por tipo de aplicación
- Estadísticas en tiempo real de la disponibilidad del enlace Notificación en tiempo real de fallas y/o caídas en los enlaces vía correo electrónico
- Registro de los sucesos relacionados con loa disponibilidad de los enlaces

Además se debe permitir una administración local de la red, esto es, una capacitación de los funcionarios encargados del departamento de sistemas sobre como están configurados los dispositivos activos de la red y así tener acceso a ellos.

- **Actualización de aplicaciones:**

Acoplar las aplicaciones actuales a entornos Web, contratando una empresa para esta tarea, para correrlas desde un solo servidor central y tener acceso inmediato desde los centros.

- **Administración ancho de banda:**

Configurar un administrador de ancho de banda que permita restringir el ancho de banda reservado para distintos tipos de usuarios y distintos tipos de aplicativos que demanden recursos de red.

- **Cableado:**

Reemplazar el cableado UTP que se encuentre en las sedes por uno de mayor soporte como es el de cable UTP categoría 5e o categoría 6. Además de reorganizar los centros de cableado y los puntos de red; documentarlos y etiquetarlos.

8.3. Telefonía IP[117]

A corto plazo, se plantea implementar a modo de prueba un solo canal de voz sobre IP entre las sedes del SENA REGIONAL SANTANDER y la Sede Administrativa, para determinar la viabilidad de una migración total a este tipo de tecnología.

La solución a largo plazo debe permitir una comunicación telefónica (Teléfono a Teléfono) de doble vía entre todas las Sedes del SENA REGIONAL SANTANDER a través de la red IP interna del SENA y sin necesidad de salir a la Red PSTN, utilizando la tecnología Voz sobre IP.

Los retardos típicos en una red PSTN en llamadas nacionales se sitúan alrededor de los 50 a 70 milisegundos, mientras que en las internacionales, estos pueden llegar a elevarse hasta los 150-500 milisegundos. El oído humano comienza a percibir tales retrasos cuando estos son mayores de más o menos 250 milisegundos (umbral de percepción) [28], por lo tanto se requieren unos retardos que no superen este umbral. Las llamadas a través de Internet presentan retrasos que pueden ir desde los 400 ms hasta los 2 segundos.

La solución debe manejarse sobre plataformas Cisco por ser estos dispositivos con los que cuenta la Regional Santander y los que mejor manejan políticas de servicio (QoS)

Además, se requiere un registro detallado de llamadas que grabe detalles adicionales de todas las fases de las llamadas, duraciones e intervalos de llamadas entrantes, salientes, internas y encaminamiento de llamadas para todos los usuarios. Asimismo, se requiere plantear políticas para el control de las llamadas en la Sede Administrativa de la Regional Santander que es donde se presenta mayor número de llamadas innecesarias.

8.4 Planteamiento Topológico Final

A continuación se presenta el esquema básico de conectividad planteado como resultado de la documentación y evaluación de la red de datos del SENA REGIONAL SANTANDER, que pretende ser una guía para su mejoramiento progresivo según las prioridades de la Institución.

[117] Ver Anexo C. Propuestas de Proveedores

Se incluye la integración de los servicios de voz con los de datos por medio de la implementación de la tecnología Voz sobre IP entre la Sede Administrativa, los Centros y la Dirección General, la cual se vislumbra como una solución a largo plazo, que por lo tanto deberá tener en cuenta los lineamientos planteados por el Ministerio de Comunicaciones[118] que para la fecha de su implementación se encuentren vigentes en cuanto a telefonía IP se refiere.

Este sistema requiere de un aumento significativo del ancho de banda en los enlaces, que se debe tener en cuenta al momento de implementar la solución.

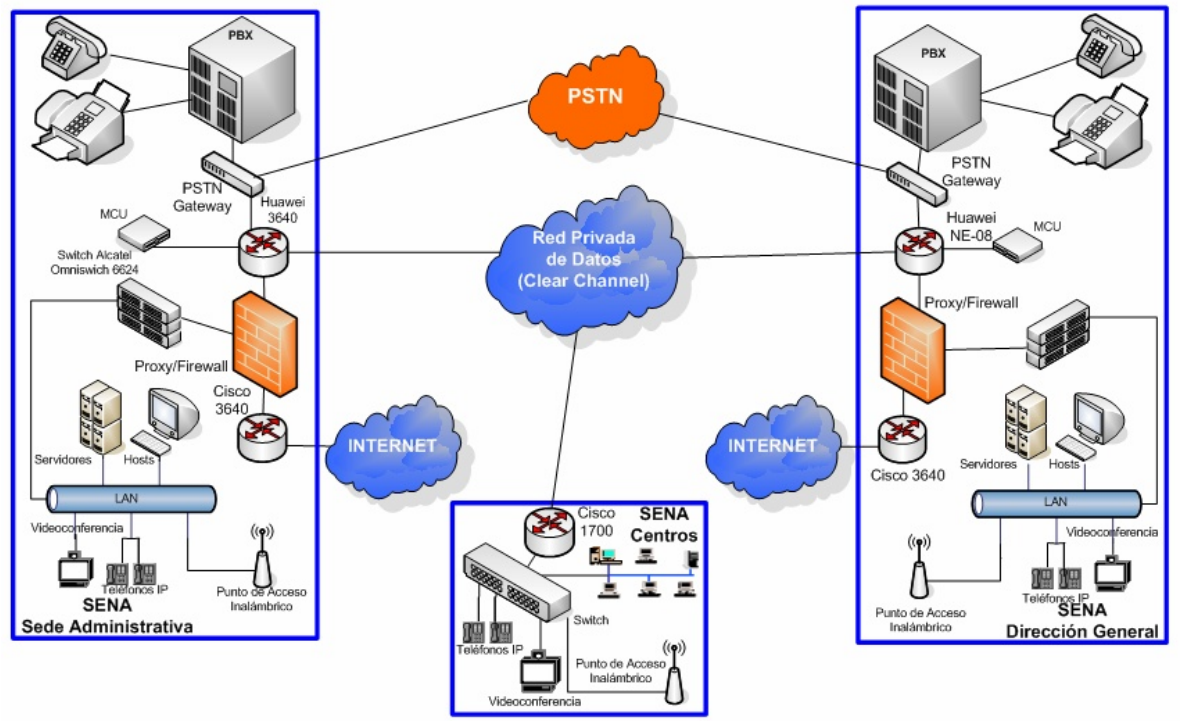


Figura 8.4 Esquema de la Red de Datos del SENA REGIONAL SANTANDER a largo plazo (Fuente: Autores)

[118] La política regulatoria del sector de las telecomunicaciones en Colombia tiene por directriz regular por servicios mas no por tecnología. En este orden de ideas, y en la medida en que VoIP es una tecnología que permite la comunicación de voz a través de una red basada en protocolo IP, no existe en Colombia regulación alguna al respecto, y no se ha proyectado emitirla. El servicio de comunicación de voz, independientemente de la red que se emplee para su prestación, está regulado por las normas previstas para cada servicio, y por lo tanto los interesados en prestar un determinado servicio empleando tecnología IP deberán obtener la respectiva licencia por medio de la cual se autoriza la prestación del servicio.

9. RECOMENDACIONES

Como resultado de la evaluación de la Red de Datos del SENA REGIONAL SANTANDER, se plantean las siguientes recomendaciones para el mejoramiento de su conectividad y la elaboración de próximos estudios.

Se estableció el siguiente orden de prioridades:

Prioriodad	Significado
1	Implementación necesaria a término de máximo 6 meses
2	Implementación necesaria a término de 1 año
3	Implementación necesaria a término de 1 año y medio
4	Implementación necesaria a término de 2 años
5	Implementación necesaria a término de 2 años y medio

Red Interna

	Recomendación	Prioridad
Red Interna	Se propone interconectar todas las Sedes por medio de Líneas Dedicadas, reemplazando los dos enlaces RDSI existentes en el momento entre Girón y Florida e incrementar el ancho de banda de cada enlace de 128 Kbps a por lo menos 256 Kbps en los centros de Málaga, Piedecuesta y Vélez, y a 512 Kbps en los Centros de Barrancabermeja, Floridablanca, Girón y San Gil.	1
	Manejar todas las Sedes en un solo router y reservar el otro solamente para el enlace con Internet.	1
	Implementar una herramienta de Gestión de Redes como el OpManager en la red de datos regional para minimizar los tiempos de detección, atención y corrección de fallos	1
	Realizar una evaluación sobre la posibilidad de implementa soluciones de conectividad del tipo Wireless en cada una de las Sedes, iniciando en la Sede Administrativa.	1
	Realizar estudios sobre la migración de las aplicaciones en línea tipo cliente/servidor a aplicaciones basadas completamente en Web, que no requieran ser actualizadas en las estaciones cliente.	1
	Administrar todos los dispositivos desde la Sede Administrativa, para reducir los tiempos de atención y solución de fallos en caso de que se presenten.	4

	Recomendación	Prioridad
Red Interna	Reemplazar todos los Hubs por Switches que puedan ser administrables desde la Sede Administrativa y que no introduzcan colisiones al tráfico de la Red Interna en cada una de las Sedes.	5
	Reemplazar todo el cableado UTP Cat.5 existente por Cat.5e o superior, o por Fibra Optica, según evaluaciones técnicas detalladas de cada una de las Sedes.	5
	Administrar correctamente el ancho de banda por medio de un dispositivo diseñado para tal fin, que permita dedicar y priorizar ciertos usos de la red como la videoconferencia, la Voz sobre IP y los aplicativos en línea.	3

Internet

	Recomendación	Prioridad
Internet	Reorganizar el servicio de Internet de los Centros de tal forma que se libere este tipo de tráfico del enlace con la Dirección General y se desvíe por medio de un servidor Proxy a un ISP local.	1
	Reservar el enlace con la Dirección General solamente para el tráfico de Aplicativos en línea, Videoconferencia y tráfico de Internet de las Redes LAN de la Sede Administrativa y el Centro de Comercio y Servicios.	2
	Monitorear en tiempo real el tráfico de Internet para identificar si se le está dando el uso adecuado, identificando los protocolos más utilizados y los nodos de mayor tráfico enviado y recibido.	3
	Adquirir un dispositivo de administración de ancho de banda que a su vez actúe como Firewall y permita fragmentar el canal asignándole una porción fija al tráfico de Internet, para que en caso de presentarse picos, no se disminuya el rendimiento en otras aplicaciones críticas como Videoconferencia y aplicaciones Cliente/Servidor. De nada sirve aumentar el ancho de banda si no se administra.	5
	Posibilidad de ofrecer servicios de Videoconferencias en todas las sedes.	5

Voz sobre IP

	Recomendación	Prioridad
VoIP	Instalar por lo menos un teléfono IP en cada una de las Sedes, que permita evaluar la calidad del servicio de la comunicación y tomar decisiones al respecto sobre la migración a este tipo de tecnología.	3
	Migrar completamente a esta tecnología para llamadas SENA-SENA, que no requieran salir a la red PSTN	4
	Implementar una solución de VoIP con la asesoría de una empresa prestadora de este tipo de servicios, que incluya un enlace con la Red PSTN y permita direccionar las llamadas de teléfonos convencionales hacia la red IP teniendo en cuenta los lineamientos planteados a la fecha por el Ministerio de Comunicaciones[119].	5

[119] Al no existir regulación específica para la prestación de VoIP, la prestación de este tipo de comunicaciones por redes IP deberá hacerse mediante la obtención de una licencia que habilite al operador para prestar servicios de telefonía a terceros, la cual la expide el Ministerio de Comunicaciones, de acuerdo con las normas vigentes (Ley 142 de 1994 y Res. CRT 087 de 1997). Diferente es el caso del establecimiento de redes privadas de telecomunicaciones, para lo cual se deberá tener en cuenta lo previsto en el Decreto 930 de 2992, en la medida en que no se presta servicio a terceros a través de este tipo de redes. [22], [23]

CONCLUSIONES

Teniendo en cuenta la gestión realizada en el SENA REGIONAL SANTANDER durante el desarrollo de la presente práctica empresarial y una vez cumplidos todos los objetivos planteados de la misma, es posible concluir lo siguiente:

Respecto a la Red Interna

La Red Interna del SENA REGIONAL SANTANDER requiere especial atención y una reestructuración inmediata que supla la demanda de velocidad de transmisión y de confiabilidad por parte de los usuarios, especialmente en cuanto a los nodos correspondientes a los Centros de Girón y Florida, que a pesar de ser de los más importantes en cuanto a cantidad de usuarios, cuentan con una estructura de red deficiente.

Respecto a Internet

La salida a Internet asignada sobre el canal E1, que enlaza la Sede Administrativa con la Dirección General no es suficiente para atender los requerimientos de conectividad de todos los Centros, por lo tanto se requiere solicitar la asignación de ancho de banda extra de parte de la Dirección General para tal fin o la contratación alterna de una solución a nivel Regional. Esta solución descongestionaría el enlace E1 reservándolo exclusivamente para el tráfico correspondiente a las aplicaciones administrativas y a videoconferencias.

Sin embargo, de nada sirve aumentar el ancho de banda de los enlaces si no se establece un control sobre su utilización, como se desarrolló en el presente estudio y específicamente remitiéndose a los monitoreos realizados, que comprobaron que en gran medida la utilización de los enlaces de la Red de Datos del SENA REGIONAL SANTANDER está orientada a las consultas en Internet.

Respecto a Telefonía IP

La implementación de una solución del tipo IP para atender todo el tráfico de voz del SENA REGIONAL SANTANDER resulta muy atractiva, pero no precisamente debido a la innovación tecnológica que esta supone, si no más que todo, a los ahorros en conceptos de telefonía tradicional que representa. No obstante, hay que tener en cuenta que para que sea realmente viable su implementación en cuanto a costos, se requiere que una gran porción de las llamadas viajen a través de la red IP.

Es importante que el SENA REGIONAL SANTANDER incursione en este tipo de tecnología progresivamente y tenga en cuenta que los ahorros en conceptos de telefonía siempre van a ir ligados a un gasto significativo en el aumento del ancho de banda y de la infraestructura adecuada para soportar el tráfico de voz. Sólo si se logra un equilibrio entre los dos, es viable implementar la solución.

Aportes a la institución

Dentro de los aportes otorgados al SENA REGIONAL SANTANDER una vez finalizado el trabajo en sus instalaciones, se cuenta con:

- Una documentación detallada de toda su Red de Datos, que incluye los diagramas de interconexión y de cableado, de todos sus Centros con la Sede Administrativa y de esta con la Dirección General en la ciudad de Bogotá. Esta documentación es de gran importancia para el mejoramiento de la red ya que sin un verdadero conocimiento del funcionamiento de la misma y de los dispositivos involucrados no se pueden tomar medidas correctivas, localizar fallas y atender problemas que se presenten.

- Se implemento y se configuró la herramienta de gestión OpManager 6.0 en su versión gratuita, la cual es una herramienta invaluable para el administrador de la red, por su capacidad para detectar fallas, manejar alarmas, monitorear enlaces y su estado, monitorear los dispositivos y sus interfaces, presentar reportes de utilización y minimizar con esto los tiempos de inoperatividad de la red. Además, se elaboró un manual básico para la utilización de esta potente herramienta de Gestión de Red.

- Se realizó un monitoreo detallado del tráfico en los enlaces más importantes de la Red de Datos en cuanto a tasas de transferencia de todas las subredes, tamaño de

paquetes, tipo de tráfico, nodos de mayor tráfico enviado y recibido y análisis de protocolos. Es importante realizar este tipo de monitoreos con cierta frecuencia para determinar posibles usos inapropiados en la red. Sería ideal implementar alguna herramienta software/hardware que permita realizarlo en tiempo real pero esto implica cierta inversión de recursos. Sin embargo, se comprobó que la utilización del método de Hub para realizar el monitoreo no afecta significativamente el desempeño de la red una vez insertado en el enlace y por lo tanto, se podría implementar este tipo de solución.

- Se planteó una propuesta topológica de reestructuración de la Red de Datos como modelo para una futura implementación, teniendo en cuenta los dispositivos actuales con los que cuenta el SENA REGIONAL SANTANDER y contemplando la posibilidad de adecuar un sistema de Voz IP.

- Se presentó una propuesta económica para el acceso a Internet de TELECOM siendo esta la que mejor se ajustaba a los requerimientos mínimos planteados a razón del estudio hecho en esta práctica y la que contaba con un mejor portafolio de servicios.

BIBLIOGRAFIA

Libros

[1] DAVIDSON, Jhonatan; PETERS, James. Voice over IP Fundamentals, Cisco Systems. 2000

[2] GARCIA, Alberto León. Communication Networks, McGraw Hill, 2003

[3] OREBAUGH, Angela. Syngress Publishing. 2004, 468 p. Ethereal Packet Sniffing Manual Ethereal

[4] TANENBAUM, Andrew S. Computer Networks, Prentice Hall, 2003

[5] WALLINGFORD, Theodore. Switching to VoIP, O'Reilly, 2005

[6] WERNER, Feibel. Encyclopedia of Networking, Network Press, 2005

Documentos

[7] Documento CONPES 3072: Ministerio de Comunicaciones, Agenda de Conectividad. República de Colombia, Departamento Nacional de Planeación, Santa Fe De Bogotá, 9 de Febrero de 2000, DNP: UINFE-DITEL

[8] Solución de Incidencias en Entornos Conmutados, Fluke Networks. 2005

[9] CANO M Jeimy J, YAYA NARVAEZ León David. Consideraciones legales y comerciales sobre VoIP en Colombia. Revista Derecho Informático No. 092, Marzo de 2006. Alfa-Redi. ISSN 1681-5726

[10] GUZMAN, Andrés Alberto. Aspectos legales sobre Voz sobre IP en Colombia. Revista Derecho Informático No. 069, Abril de 2006. Alfa-Redi. ISSN 1681-5726

[11] FERREIRA Adriana, PEPE Marcelo, LOPEZ Fernando, GUANI Julio. VoIP en Redes Corporativas.

Trabajos de grado

[12] ACEVEDO SILVA, Héctor Alfonso; VERGEL ZAPATA Ronald Martín. Caracterización del Tráfico del Backbone de la Universidad Industrial de Santander, 2005. 138 p. Trabajo de investigación presentado como requisito para optar al título de Ingeniero Electrónico. Universidad Industrial de Santander. Facultad de Ciencias Físico-mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones.

[13] DELGADO ALBA, Jesús Antonio. Desarrollo e implementación de herramientas de conectividad para el Sena Regional Santander, 2005. 85 p. Trabajo de grado (Especialización en Telecomunicaciones). Universidad Industrial de Santander. Facultad de Ciencias Físico-mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones

[14] GAMBOA GAMBOA, Armando; VIDAL HERNANDEZ, Jorge Iván. Análisis de Tráfico en el Enlace Externo de la Red de Datos de la Universidad Industrial de Santander, 2005. 112 p. Trabajo de investigación presentado como requisito para optar al título de Ingeniero Electrónico. Universidad Industrial de Santander. Facultad de Ciencias Físico-mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones.

[15] GUZMAN CASTILLO, Paola Fernanda. Análisis de Gestión de los dispositivos administrables en la red de datos institucional, 2005. 259 p. Trabajo de investigación presentado como requisito para optar al título de Magíster en Ingeniería. Universidad Industrial de Santander. Facultad de Ciencias Físico-mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones

Manuales

[16] CISCO. Manuales del Router Cisco 3640

[17] HUAWEI. Manuales de Huawei Quidwai 3640

[18] ALCATEL. Manuales del Switch Alcatel OmniSwitch 6624

Otras fuentes

[19] RFC´S 1157 (A Simple Network Management Protocol), 1212 (Concise MIB definitions), 1918 (Address Allocation for Private Internets).

[20] Portal principal de Cisco®. Se puede acceder mediante en enlace <http://ww.cisco.com>

[21] Portal principal de la Agenda de Conectividad. Se puede acceder mediante el enlace <http://ww.agenda.gov.co>

[22] Portal principal de la Comisión Reguladora de Telecomunicaciones República de Colombia. Se puede acceder mediante el enlace <http://ww.crt.gov.co>

[23] Portal principal del Ministerio de Comunicaciones de la República de Colombia. Se puede acceder mediante el enlace <http://ww.mincomunicaciones.gov.co>

[24] Portal principal del Sena Regional Santander. Se puede acceder mediante el enlace <http://ww.senasantander.org>

[25] Portal principal del Sena. Se puede acceder mediante el enlace <http://ww.sena.edu.co>

[26] U.S. Department of Transportation, Federal Highway Administration. Fundamentals Of Telecommunications. Chapter 2. Pág 3. <http://ops.fhwa.dot.gov/publications/telecomm_handbook/chapter2_03.htm>

[27] ARAUJO CARDENAS, Alfonso. Redes y sus topologías. 2004
<http://mx.geocities.com/alfonsoaraujocardenas/topologias.html>

[28] JALIFE, Salma. Voz sobre IP y temas afines. Comisión Federal de Telecomunicaciones. México.
<http://www.cft.gob.mx/wb2/COFETEL/COFE_Voz_sobre_IP>

Software

[29] PRTG Traffic Grapher. Paessler
<http://www.paessler.com>

[30] ManageEngine OpManager 6.0. Adventnet
<http://www.opmanager.com>

[31] Ethereal 0.10.14
<http://www.ethereal.com>

[32] Solarwinds 8.0.17
<http://www.solarwinds.net>

[33] Dice Packet Decoder 2.9.9
<http://www.ngthomas.co.uk>

ANEXO A.
Documentación de la Red

A.1 Rangos de direcciones IP asignadas por la Dirección General

A.2 Interfaces y Tablas de Rutas de los Routers

A.3 Diagramas de Interconexión

A.4 Diagramas de Cableado

A.5 Conexiones en el rack principal

DOCUMENTACION DE LA RED DE DATOS
SENA REGIONAL SANTANDER
2006

Elaborado por:
JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNÁNDEZ CELIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERIAS ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2006

A.1 Rangos de direcciones IP asignadas por la Dirección General

En este anexo se presenta la tabla de los rangos de direcciones IP asignados por la Oficina de Sistemas de la Dirección General, a nivel nacional.

Dirección IP de red: 172.16.0.0			
Mascara de red (para todas las redes): 255.255.254.0			
Dirección de Broadcast (para todas las redes): 172.16.255.255			
Rangos de IP Nacionales Asignados			
Subred	**Host Range**	**Regional**	**Gateway (Router)**
0	172.16.0.1 - 172.16.1.254	Reservado Para Red	
1	172.16.2.1 - 172.16.3.254	Dirección General	172.16.3.254
2	172.16.4.1 - 172.16.5.254	Antioquia – Sede Central	172.16.5.254
3	172.16.6.1 - 172.16.7.254	Antioquia – Complejo Norte	172.16.7.254
4	172.16.8.1 - 172.16.9.254	Antioquia – Complejo Sur	172.16.9.254
5	172.16.10.1 - 172.16.11.254	Atlántico – Sede Central	172.16.11.254
6	172.16.12.1 - 172.16.13.254	Atlántico – Complejo Industrial	172.16.13.254
7	172.16.14.1 - 172.16.15.254	Bogotá – Sede Central	172.16.15.254
8	172.16.16.1 - 172.16.17.254	Bogotá – Paloquemao	172.16.17.254
9	172.16.18.1 - 172.16.19.254	Bogotá – Sur	172.16.19.254
10	172.16.20.1 - 172.16.21.254	Bolívar – Comercio	172.16.21.254
11	172.16.22.1 - 172.16.23.254	Boyacá – Belencito	172.16.23.254
12	172.16.24.1 - 172.16.25.254	Caldas – Enea	172.16.25.254
13	172.16.26.1 - 172.16.27.254	Caquetá – Florencia	172.16.27.254
14	172.16.28.1 - 172.16.29.254	Cauca – Sede Central	172.16.29.254
15	172.16.30.1 - 172.16.31.254	Cesar – Multisectorial V/dupar	172.16.31.254
16	172.16.32.1 - 172.16.33.254	Choco – Multisectorial	172.16.33.254
17	172.16.34.1 - 172.16.35.254	Córdoba – Multisectorial	172.16.35.254
18	172.16.36.1 - 172.16.37.254	Guajira – Sede Central	172.16.37.254
19	172.16.38.1 - 172.16.39.254	Huila – Sede Central	172.16.39.254
20	172.16.40.1 - 172.16.41.254	Magdalena – Multisectorial	172.16.41.254
21	172.16.42.1 - 172.16.43.254	Meta – Multisectorial	172.16.43.254
22	172.16.44.1 - 172.16.45.254	Nariño – Multisectorial Lope	172.16.45.254
23	172.16.46.1 - 172.16.47.254	Norte Santander – Pescadero	172.16.47.254
24	172.16.48.1 - 172.16.49.254	Quindío – Agroindustrial	172.16.49.254
25	172.16.50.1 - 172.16.51.254	Risaralda – Sede Central	172.16.51.254
26	172.16.52.1 - 172.16.53.254	San Andrés – Multisectorial	172.16.53.254
27	172.16.54.1 - 172.16.55.254	Santander – Sede Central	172.16.55.254
28	172.16.56.1 - 172.16.57.254	Sucre – Multisectorial	172.16.57.254
29	172.16.58.1 - 172.16.59.254	Tolima – sede Central	172.16.59.254
30	172.16.60.1 - 172.16.61.254	Valle – Salomia	172.16.61.254
31	172.16.62.1 - 172.16.63.254	Antioquia – La salada	172.16.63.254
32	172.16.64.1 - 172.16.65.254	Antioquia – Rionegro	172.16.65.254
33	172.16.66.1 - 172.16.67.254	Antioquia – Apartado	172.16.67.254
34	172.16.68.1 - 172.16.69.254	Antioquia – Caucacia	172.16.69.254
35	172.16.70.1 - 172.16.71.254	Antioquia – Puerto Berrio	172.16.71.254
36	172.16.72.1 - 172.16.73.254	Antioquia – Santafe	172.16.73.254
37	172.16.74.1 - 172.16.75.254	Antioquia – Cisnero	172.16.75.254
38	172.16.76.1 - 172.16.77.254	Antioquia – Santa Rosa	172.16.77.254

39	172.16.78.1 - 172.16.79.254	Antioquia – Venesia	172.16.79.254
40	172.16.80.1 - 172.16.81.254	Antioquia – Sede Central (Adic.)	172.16.81.254
41	172.16.82.1 - 172.16.83.254	Boyacá – Morca	172.16.83.254
42	172.16.84.1 – 172.16.85.254	Bogotá – Centros	172.16.85.254
43	172.16.86.1 – 172.16.87.254	Bogotá – Centros	172.16.87.254
44	172.16.88.1 – 172.16.89.254	Bogotá – Centros	172.16.89.254
45	172.16.90.1 – 172.16.91.254	Bogotá – Centros	172.16.91.254
46	172.16.92.1 – 172.16.93.254	Bogotá – Centros	172.16.93.254
47	172.16.94.1 – 172.16.95.254	Bogotá – Centros	172.16.95.254
48	172.16.96.1 – 172.16.97.254	Bogotá – Centros	172.16.97.254
49	172.16.98.1 – 172.16.99.254	Bogotá – Centros	172.16.99.254
50	172.16.100.1 – 172.16.101.254	Bogotá – Centros	172.16.101.254
51	172.16.102.1 – 172.16.103.254	Bogotá – Centros	172.16.103.254
52	172.16.104.1 – 172.16.105.254	Bogotá – Centros	172.16.105.254
53	172.16.106.1 – 172.16.107.254	Bogotá – Centros	172.16.107.254
54	172.16.108.1 – 172.16.109.254	Bogotá – Centros	172.16.109.254
55	172.16.110.1 – 172.16.111.254	Bogotá – Centros	172.16.111.254
56	172.16.112.1 – 172.16.113.254	Bogotá – Centros	172.16.113.254
57	172.16.114.1 – 172.16.115.254	Santander – Barranca	172.16.115.254
58	172.16.116.1 – 172.16.117.254	Santander – Girón	172.16.117.254
59	172.16.118.1 – 172.16.119.254	Santander – Florida	172.16.119.254
60	172.16.120.1 – 172.16.121.254	Casanare	172.16.121.254

Tabla A.1.1 Rangos de Direcciones IP de las Regionales del SENA a nivel Nacional[120]

[120] De acuerdo con las necesidades de interconexión, las regionales podrán solicitar a la División de Organización y Sistemas de la Dirección General la asignación de nuevos rangos de direcciones IP para centros que se integren a la red regional. Las direcciones correspondientes a los enrutadores ya fueron programadas y son las que se muestran en la tabla anterior. Santafé de Bogotá, Febrero de 1999

A.2 Interfaces y Tablas de Rutas de los Routers

A.2.1 Router Cisco 3640 – Sede Administrativa (IP: 172.16.55.247)

Interfaces:

Nombre	Dirección IP	Máscara de Red	Descripción	Ancho de Banda	Estado
Ethernet0/0	172.16.55.247	255.255.254.0	Ethernet	10 Mbps	Habilitado
Serial 1/0					Deshabilitado
Serial 1/1	173.65.1.1	255.255.255.252	Barranca		Deshabilitado
Serial 1/2					Deshabilitado
Serial 1/3	173.69.1.1	255.255.255.252	Com. y Serv.	768 kbps	Habilitado
Serial 1/4					Deshabilitado
Serial 1/5	173.68.1.1	255.255.255.252	Sangil		Deshabilitado
Serial 1/6					Deshabilitado
Serial 1/7					Deshabilitado
BRI3/0			Girón	16 Kbps	Habilitado
BRI3/1			Floridablanca	16 Kbps	Habilitado
BR3/2					Deshabilitado
BR3/3					Deshabilitado
Dialer 1	173.66.1.1	255.255.255.252	Girón (6769050)	56 kbps	Habilitado
Dialer2	173.67.1.1	255.255.255.252	Florida (6796080)	56 kbps	Habilitado

Tabla A.2.1.1 Interfaces Router Cisco 3640

Tabla de Rutas:

Dirección de Red	Mascara de Red	Interfaz
0.0.0.0	0.0.0.0	172.16.55.254 (Ethernet 0/0)
172.16.116.0 (Sede Girón)	255.255.254.0	173.66.1.2 (Dialer 1)
172.16.118.0 (Sede Florida)	255.255.254.0	173.67.1.2 (Dialer 2)
172.16.122.0 (Sede Sangil)	255.255.254.0	173.68.1.2 (Serial1/5 - Sangil)
172.16.124.0 (Sede Com. y Serv.)	255.255.254.0	173.69.1.2 (Serial1/3 - Com. y Serv.)
173.65.1.0 (Serial 1/1 - Barranca)	255.255.255.252	172.16.55.254 (Ethernet0/0 -)
173.66.1.0 (Dialer 1 - Girón)	255.255.255.252	173.66.1.2 (Dialer1 - Girón)
173.67.1.0 (Dialer 2 - Florida)	255.255.255.252	173.67.1.2 (Dialer2 - Florida)
173.68.1.0 (Serial 1/5 - San Gil)	255.255.255.252	172.16.55.254 (Ethernet0/0 -)
173.69.1.0 (Serial 1/3 - Com. Y Serv.)	255.255.255.252	172.16.55.254 (Ethernet0/0 -)

Tabla A.2.1.2 Tabla de rutas Router Cisco 3640

A.2.2 Router Quidway 3640 – Sede Administrativa (IP: 172.16.55.254)

Interfaces:

Nombre	Dirección IP	Máscara de Red	Descripción	Ancho de Banda	Estado
Ethernet0	172.16.55.254	255.255.254.0	Ethernet		E
Serial 0/0	192.168.220.2	255.255.255.252	Dirección General (Bogotá)	256 kbps	E
Serial 1/1	192.168.220.29	255.255.255.252	Piedecuesta	128 kbps	E
Serial 1/2	192.168.220.21	255.255.255.252	Velez	128 kbps	E
Serial 1/3	192.168.220.17	255.255.255.252	Sangil	128 kbps	E
Serial 1/4	192.168.220.5	255.255.255.252	Barrancabermeja	128 kbps	E
Serial 1/5	192.168.220.25	255.255.255.252	Malaga	128 kbps	E

Tabla A.2.2.1 Interfaces Router Huawei 3640

Tabla de Rutas:

Dirección de Red	Mascara de Red	Interfaz
0.0.0.0	0.0.0.0	192.168.220.1 (Serial 0/0 - Bogotá)
172.16.114.0 (Sede Barranca)	255.255.254.0	192.168.220.6 (Serial 1/4 - Barranca)
172.16.116.0 (Sede Girón)	255.255.254.0	172.16.55.247 (Ethernet0 -)
172.16.118.0 (Sede Florida)	255.255.254.0	172.16.55.247 (Ethernet0 -)
172.16.122.0 (Sede San Gil)	255.255.254.0	192.168.220.18 (Serial 1/3 - Sangil)
172.16.124.0 (Sede Com. y Serv.)	255.255.254.0	172.16.55.247 (Ethernet0 -)
172.16.131.0 (Sede Velez)	255.255.255.0	192.168.220.22 (Serial 1/2 - Velez)
172.16.178.0 (Sede Piedecuesta)	255.255.255.0	192.168.220.30 (Serial 1/1 - Piedecuesta)
172.16.183.0 (Sede Málaga)	255.255.255.0	192.168.220.26 (Serial 1/5 - Malaga)

Tabla A.2.2.2 Tabla de rutas Router Huawei 3640

A.2.3 Huawei NetEngine-08 - Router Principal Dirección General (IP:172.16.3.1)

Interfaces:

Nombre	Descripción	Ancho de Banda	Tipo	Admin Status	Operacional Status
Serial3/0/0:0	REGIONAL-NEIVA	1.02 Mbps	sdlc	enable	up
Serial3/0/0:1	REGIONAL-RIOACHA	960 Kbps	sdlc	enable	up
Serial3/0/1:0	REGIONAL-POPAYAN	896 Kbps	sdlc	enable	up
Serial3/0/1:1	ARAUCA	512 Kbps	sdlc	enable	up
Serial3/0/1:2	REGIONAL-YOPAL	512 Kbps	sdlc	enable	up
Serial3/0/2:0	REGIONAL-SANTAMARTA	640 Kbps	sdlc	enable	up
Serial3/0/2:1	REGIONAL-LETICIA	512 Kbps	sdlc	enable	up
Serial3/0/2:3	CONEXION MEISSEN	256 Kbps	sdlc	enable	up
Serial3/0/2:2	REGIONAL-PEREIRA	512 Kbps	sdlc	enable	up
8390 E1 3/0/3	HUAWEI, Quidway Series, E1 3/0/3	2.05 Mbps	E1	enable	down
8518 E1 3/0/4	HUAWEI, Quidway Series, E1 3/0/4	2.05 Mbps	E1	enable	up
Serial3/0/4:1	LOS NARANJOS-META	128 Kbps	sdlc	enable	up
8774 E1 3/0/5	HUAWEI, Quidway Series, E1 3/0/5	2.05 Mbps	E1	enable	up
Serial3/0/5:0	REGIONAL-PASTO	1.02 Mbps	sdlc	enable	up
Serial3/0/5:2	CHIA	256 Kbps	sdlc	enable	up
9158 E1 3/0/6	HUAWEI, Quidway Series, E1 3/0/6	2.05 Mbps	E1	enable	down
9286 E1 3/0/7	HUAWEI, Quidway Series, E1 3/0/7	2.05 Mbps	E1	enable	down
410 Ethernet3/2/0	Ethernet3/2/0	100 Mbps	ethernet csmacd	enable	down
Serial3/0/5:1	SOACHA	128 Kbps	sdlc	enable	down
Serial3/0/5:3	BUS-ITINERANTE-2	128 Kbps	sdlc	enable	down
5718 E1 4/0/0	E1-CALI-REGIONAL	2.05 Mbps	E1	enable	up
Serial4/0/0:0	E1-CALI-REGIONAL	1.98 Mbps	sdlc	enable	up
E1 4/0/1	E1-MEDELLIN-REGIONAL	2.05 Mbps	E1	enable	up
Serial4/0/1:0	E1-MEDELLIN-REGIONAL	1.98 Mbps	sdlc	enable	up
6230 E1 4/0/2	E1-BARRANQUILLA-REGIONAL	2.05 Mbps	E1	enable	up
Serial4/0/2:0	E1-BARRANQUILLA-REGIONAL	1.98 Mbps	sdlc	enable	up
6486 E1 4/0/3	E1-BUCARAMANGA-REGIONAL	2.05 Mbps	E1	enable	up
Serial4/0/3:0	E1-BUCARAMANGA-REGIONAL	1.98 Mbps	sdlc	enable	up
6742 E1 4/0/4	E1-SOGAMOSO-REGIONAL	2.05 Mbps	E1	enable	up
6998 E1 4/0/5	E1-BOGOTA1-REGIONALES-	2,05 Mbps	E1	enable	up

	NOCII-A3-4				
Serial4/0/5:0	ITAGUI	256 Kbps	sdlc	enable	up
Serial4/0/5:1	PEDREGAL	256 Kbps	sdlc	enable	up
Serial4/0/5:2	REGIONAL-CARTAGENA	1.02 Mbps	sdlc	enable	up
7510 E1 4/0/6	E1-BOGOTA2-REGIONALES-NOCII-B1-A	2.05 Mbps	E1	enable	up
Serial4/0/6:0	REGIONAL-IBAGUE	1.02 Mbps	sdlc	enable	up
Serial4/0/6:1	REGIONAL-MANIZALES	960 Kbps	sdlc	enable	up
7894 E1 4/0/7	E1-BOGOTA3-REGIONALES-NOCII-B1-B	2.05 Mbps	E1	enable	up
Serial4/0/7:0	DOSQUEBRADAS	1.02 Mbps	sdlc	enable	up
Serial4/0/7:1	PUERTO ASIS	256 Kbps	sdlc	enable	up
Serial4/0/7:2	VICHADA-PtoCarreño	256 Kbps	sdlc	enable	up
Serial4/0/7:3	GAIRA-STMARTA	256 Kbps	sdlc	enable	up
530 Ethernet4/1/0	HUAWEI, Quidway Series, Ethernet4/1/0	100 Mbps	ethernet csmacd	disable	down
658 Ethernet4/2/0	CONEXION-TELMEX-BOGOTA (10.10.87.58)	100 Mbps	ethernet csmacd	enable	up
4582 E1 5/0/0	E1-BOGOTA4-REGIONALES-NOCII-A3-8	2.05 Mbps	E1	enable	up
Serial5/0/0:0	REGIONAL-VILAVICENCIO	384 Kbps	sdlc	enable	up
Serial5/0/0:1	REGIONAL-MONTERIA	384 Kbps	sdlc	enable	up
Serial5/0/0:2	REGIONAL-ARMENIA	384 Kbps	sdlc	enable	up
Serial5/0/0:4	REGIONAL-VALLEDUPAR	640 Kbps	sdlc	enable	up
Serial5/0/0:6	PTO-CARRENO 2	128 Kbps	Frame Relay	enable	up
Serial5/0/0:5	CONEXION USME	64 Kbps	sdlc	enable	down
5478 E1 5/0/1	TUMACO	2.05 Mbps	E1	enable	up
Serial5/0/1:0	SAN-JOSE-GUAVIARE	256 Kbps	sdlc	enable	up
Serial5/0/1:1	REGIONAL-FLORENCIA	384 Kbps	sdlc	enable	up
Serial5/0/1:2	REGIONAL-SINCELEJO	640 Kbps	sdlc	enable	up
Serial5/0/1:4	MITU	256 Kbps	Frame Relay	enable	up
Serial5/0/1:6	PTO-INIRIDA	256 Kbps	Frame Relay	enable	up
6246 E1 5/0/2	E1-BOGOTA5-REGIONALES-NOCI-B7-2	2.05 Mbps	E1	enable	up
Serial5/0/2:0	REGIONAL-CUCUTA	1.02 Mbps	sdlc	enable	up
Serial5/0/2:1	BAQUILLA-INDUSTRIAL	768 Kbps	sdlc	enable	up
Serial5/0/2:5	CONEXION SUBA	64 Kbps	sdlc	enable	up
6758 E1 5/0/3	E1-BOGOTA-REGIONALES-AUTOPISTA-P1-9-8	2.05 Mbps	ethernet csmacd	enable	up
Serial5/0/3:1	C-AGROPECUARIO	128 Kbps	sdlc	enable	up
Serial5/0/3:2	REGIONAL-QUIBDO	512 Kbps	sdlc	enable	up
Serial5/0/3:5	VILLETA	384 Kbps	sdlc	enable	up
Serial5/0/3:6	CALLE 34	128 Kbps	sdlc	enable	up
Serial5/0/3:7	GIRARDOT	512 Kbps	sdlc	enable	up
7526 E1 5/0/4	E1-BOGOTA-REGIONALES-AUTOPISTA-P1-10-6	2.05 Mbps	E1	enable	up

Serial5/0/4:0	PALOQUEMAO	1.02 Mbps	sdlc	enable	up
Serial5/0/4:1	MOSQUERA	512 Kbps	sdlc	enable	up
Serial5/0/4:2	FUSAGASUGA	384 Kbps	sdlc	enable	up
8038 E1 5/0/5	E1 DE TELMEX	2.05 Mbps	E1	enable	up
Serial5/0/5:0	COMPLEJO-SUR	1.02 Mbps	sdlc	enable	up
Serial5/0/5:1	CONEXION USAQUEN	192 Kbps	sdlc	enable	up
Serial5/0/5:2	CONEXION FONTIBON	192 Kbps	sdlc	enable	up
Serial5/0/5:3	CONEXION ONASSIS	64 Kbps	sdlc	enable	down
8678 E1 5/0/6	REGIONAL-CUNDINAMARCA	2.05 Mbps	E1	enable	up
Serial5/0/6:0	REGIONAL-CUNDINAMARCA	1.98Mbps	sdlc	enable	up
8934 E1 5/0/7	CONEXION NEWBRIDGE A ROUTER HUAWEI	2.05 Mbps	E1	enable	up
Serial5/0/7:1	REGIONAL-SAN-ANDRES	448 Kbps	sdlc	enable	up
Serial5/0/7:2	ENLACE-EBDCLL100-SENACLL57	512 Kbps	sdlc	enable	up
Serial5/0/7:4	EDIFICIO-CALLE-52	512 Kbps	sdlc	enable	up
442 Ethernet5/1/0	HUAWEI, Quidway Series, Ethernet5/1/0	100Mbps	ethernet csmacd	enable	down
570 Ethernet5/2/0	CONEXION_LAN (172.16.3.1)	100 Mbps	ethernet csmacd	enable	up

Tabla A.2.3.1 Interfaces Router Huawei NetEngine 08E

A.3 Diagramas de Interconexión

A continuación se presentan los diagramas detallados de interconexión entre la Sede Administrativa del SENA y cada uno de sus centros. Se incluyen detalles como el rango de direcciones IP de cada subred y los dispositivos asociados a la misma con sus respectivas interfaces.

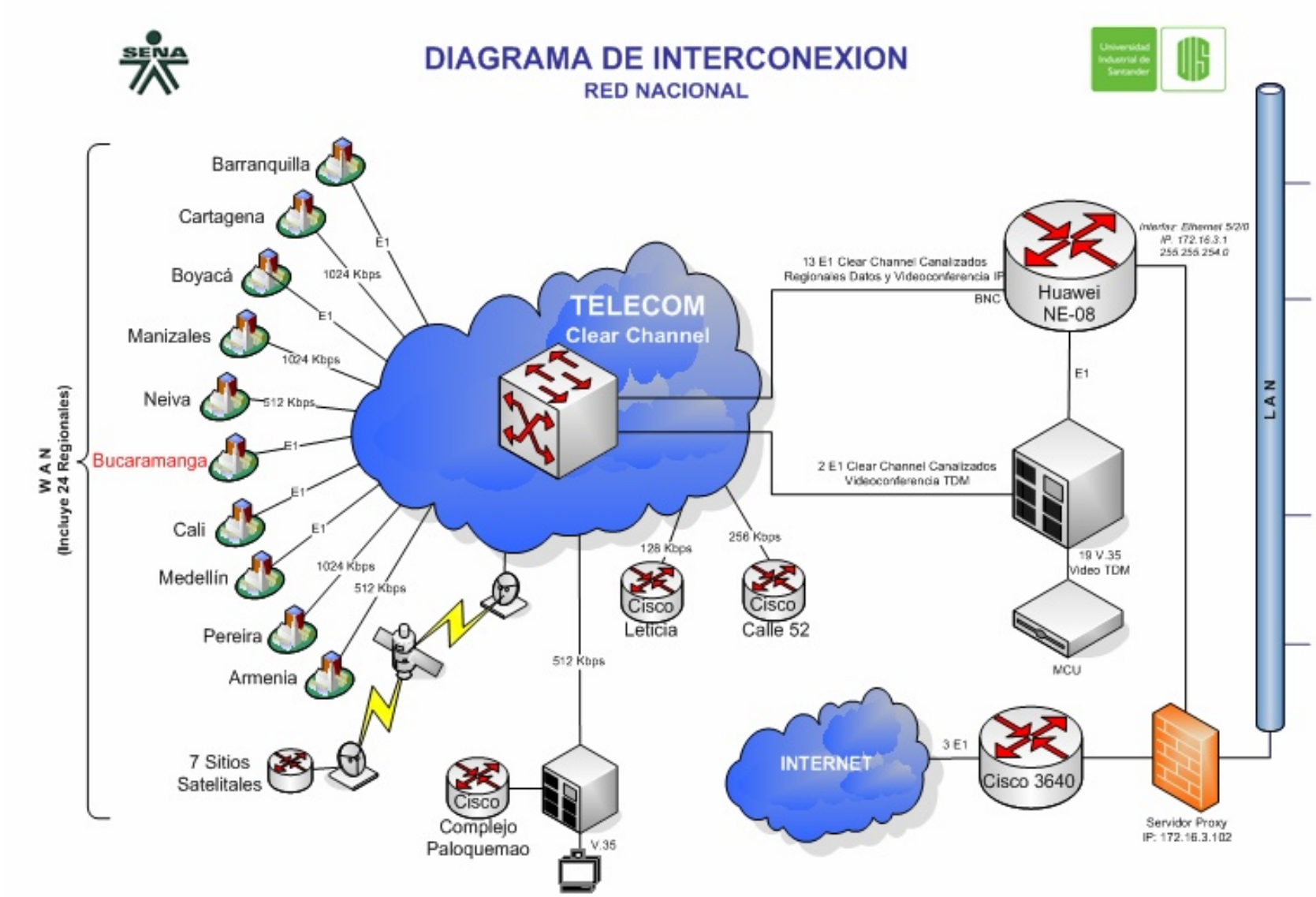


Figura A.3.1. Estructura de la Red WAN Nacional del SENA

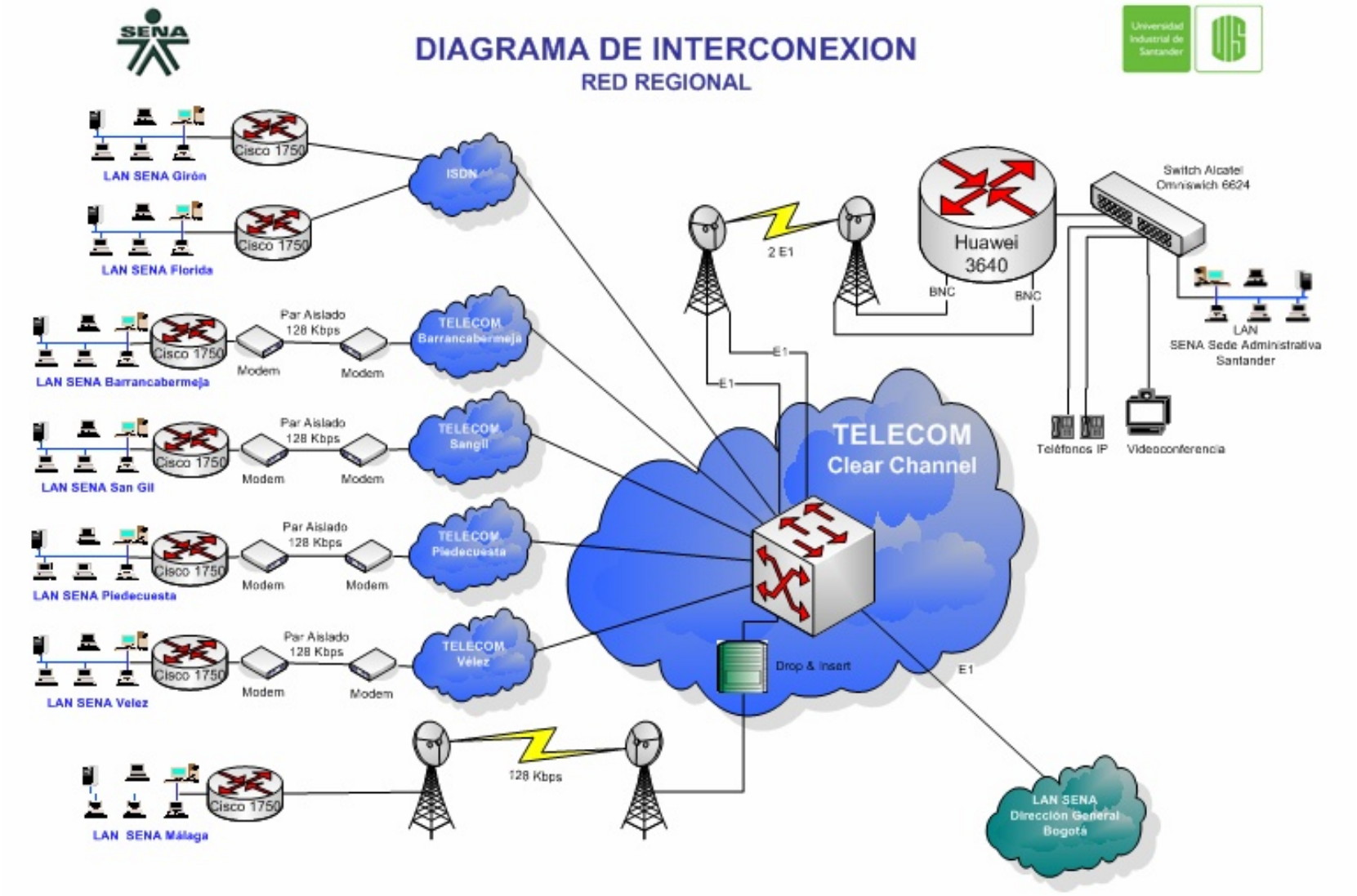


Figura A.3.2. Estructura de la Red Regional del SENA

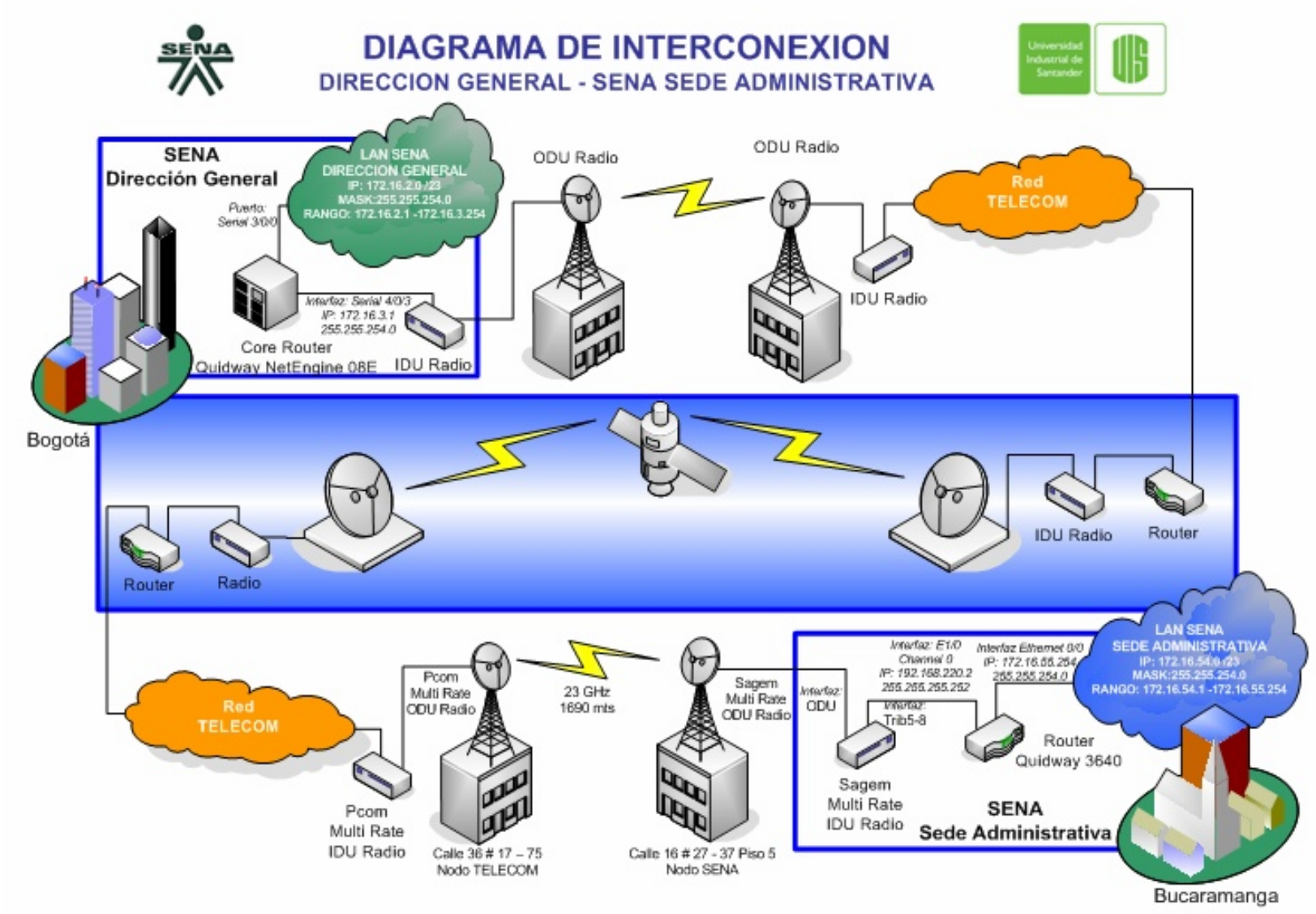
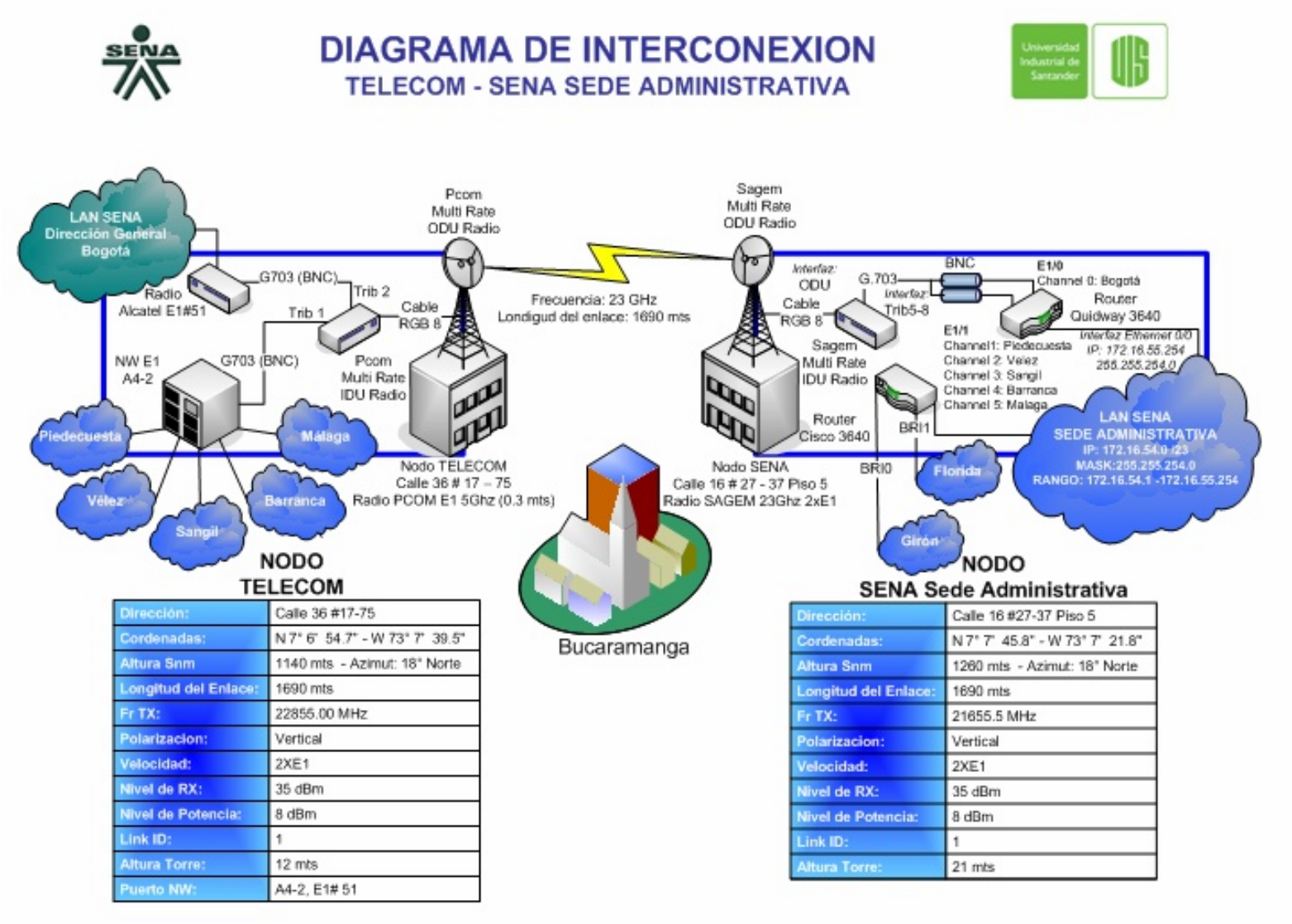


Figura A.3.3. Interconexión Sede Administrativa – Dirección General



Dirección:	Calle 36 #17-75
Cordenadas:	N 7° 6' 54.7" - W 73° 7' 39.5"
Altura Snm	1140 mts - Azimut: 18° Norte
Longitud del Enlace:	1690 mts
Fr TX:	22855.00 MHz
Polarizacion:	Vertical
Velocidad:	2XE1
Nivel de RX:	35 dBm
Nivel de Potencia:	8 dBm
Link ID:	1
Altura Torre:	12 mts
Puerto NW:	A4-2, E1# 51

Dirección:	Calle 16 #27-37 Piso 5
Cordenadas:	N 7° 7' 45.8" - W 73° 7' 21.8"
Altura Snm	1260 mts - Azimut: 18° Norte
Longitud del Enlace:	1690 mts
Fr TX:	21655.5 MHz
Polarizacion:	Vertical
Velocidad:	2XE1
Nivel de RX:	35 dBm
Nivel de Potencia:	8 dBm
Link ID:	1
Altura Torre:	21 mts

Figura A.3.4. Interconexión Sede Administrativa - TELECOM

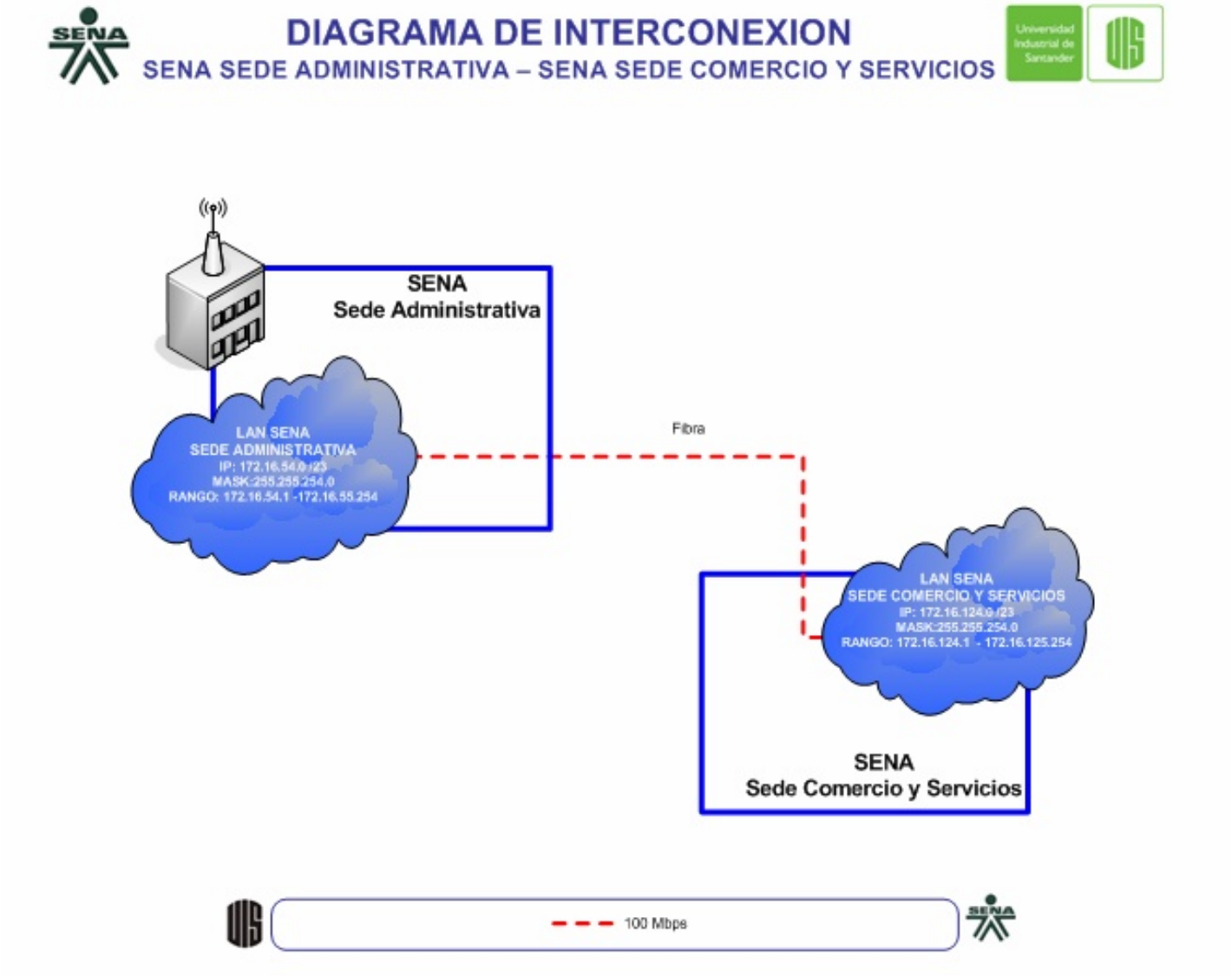


Figura A.3.5. Interconexión Sede Administrativa – Sede Comercio y Servicios

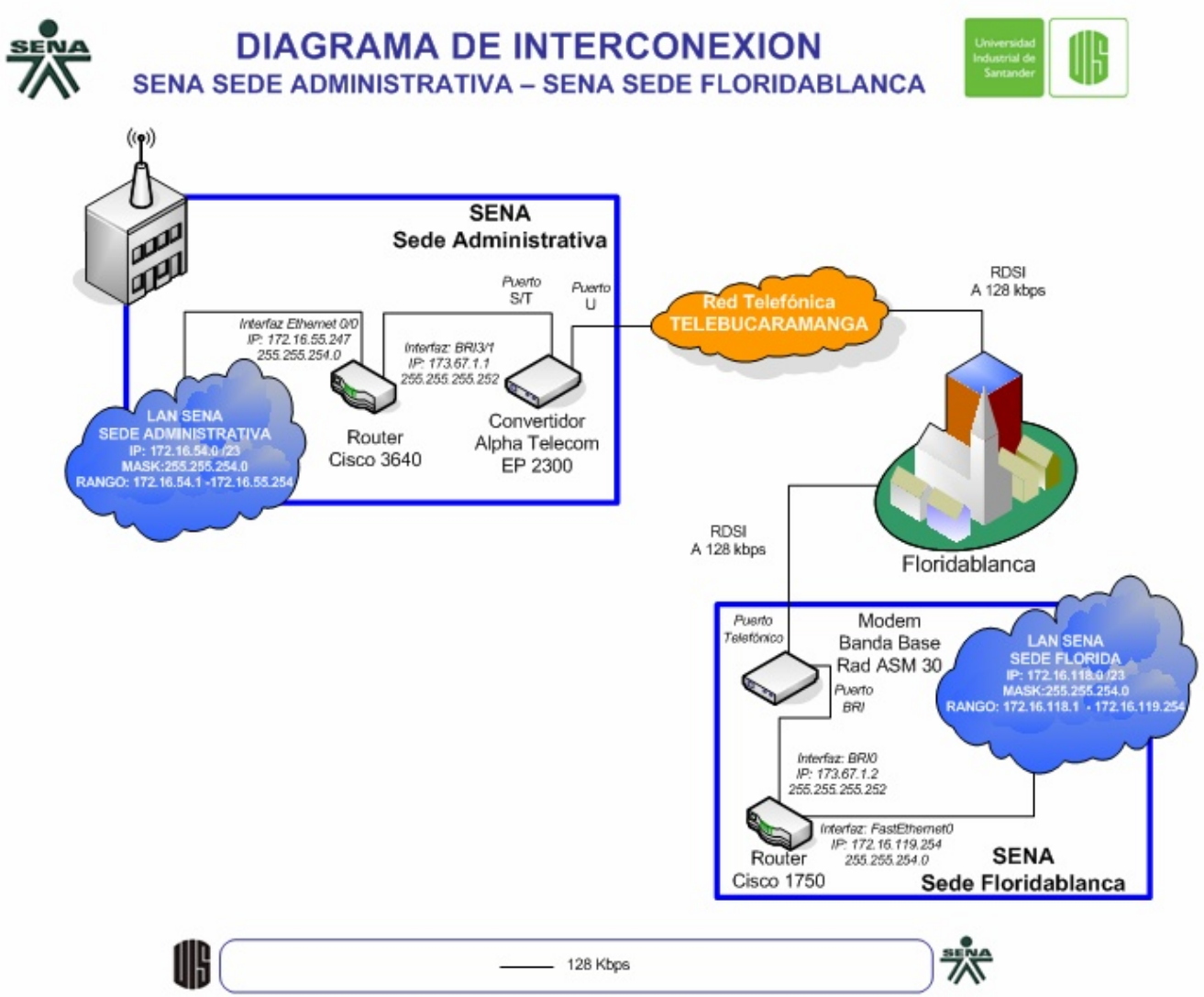


Figura A.3.6. Interconexión Sede Administrativa – Sede Floridablanca

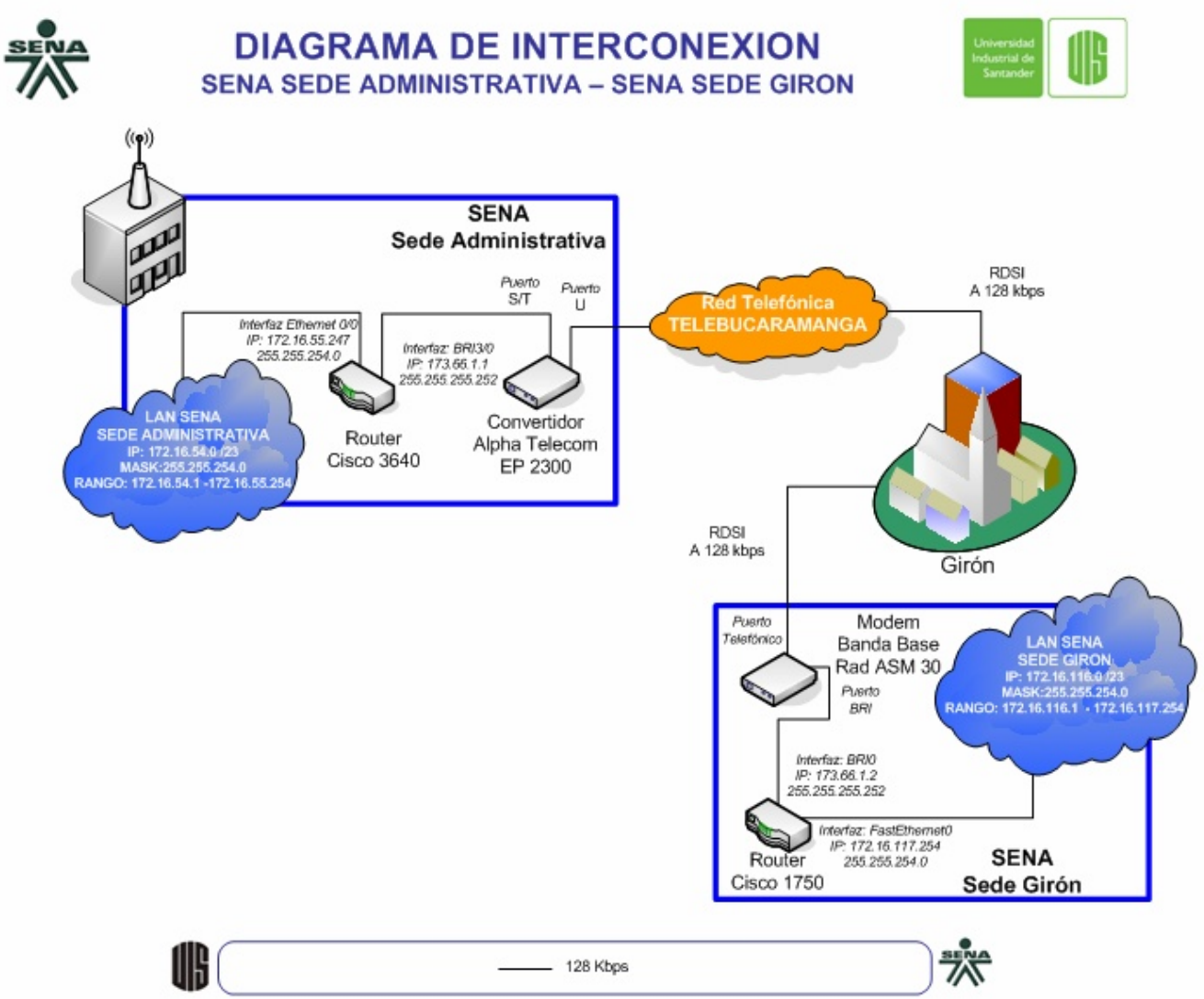


Figura A.3.7. Interconexión Sede Administrativa – Sede Girón

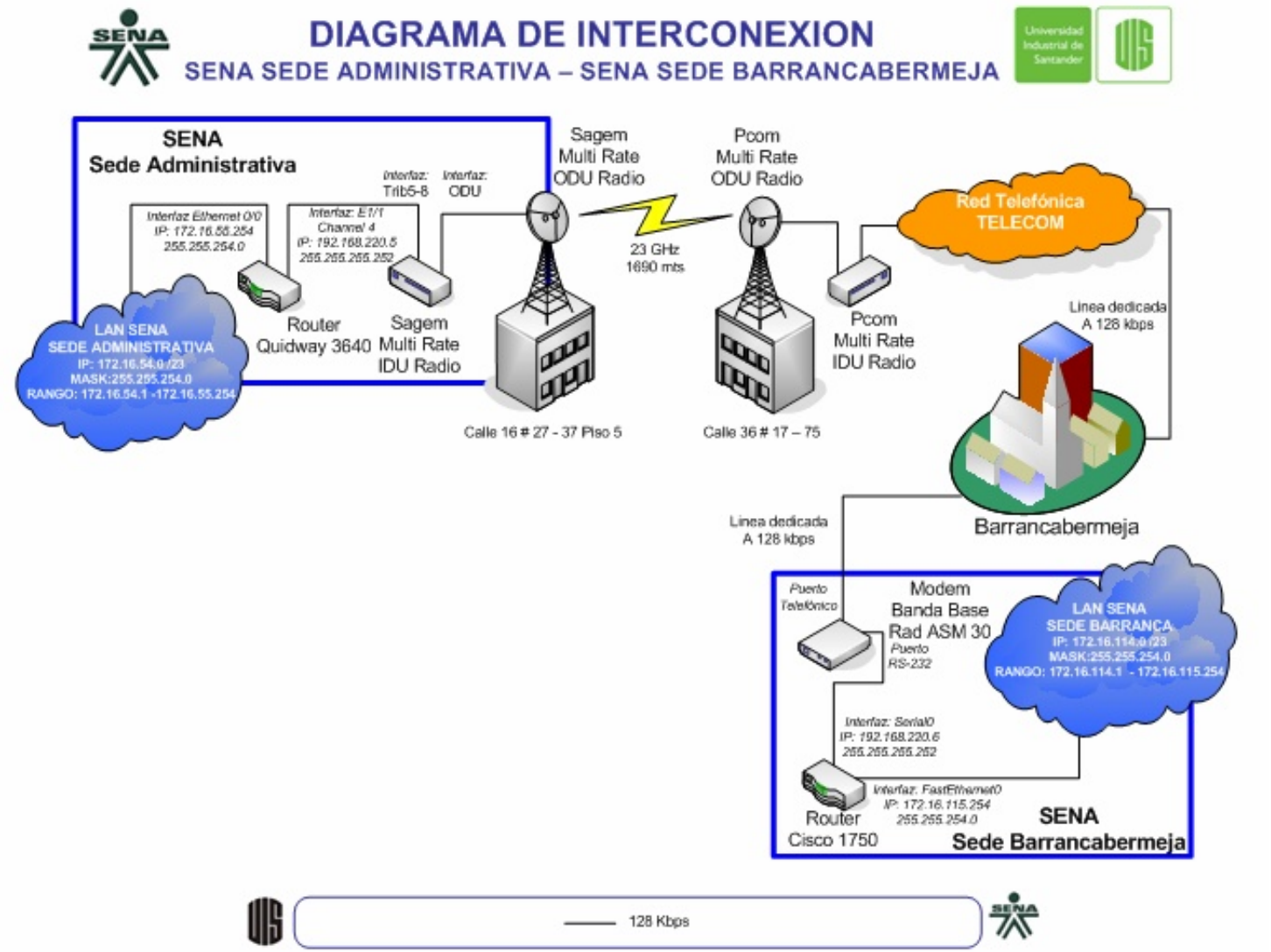


Figura A.3.8. Interconexión Sede Administrativa – Sede Barrancabermeja

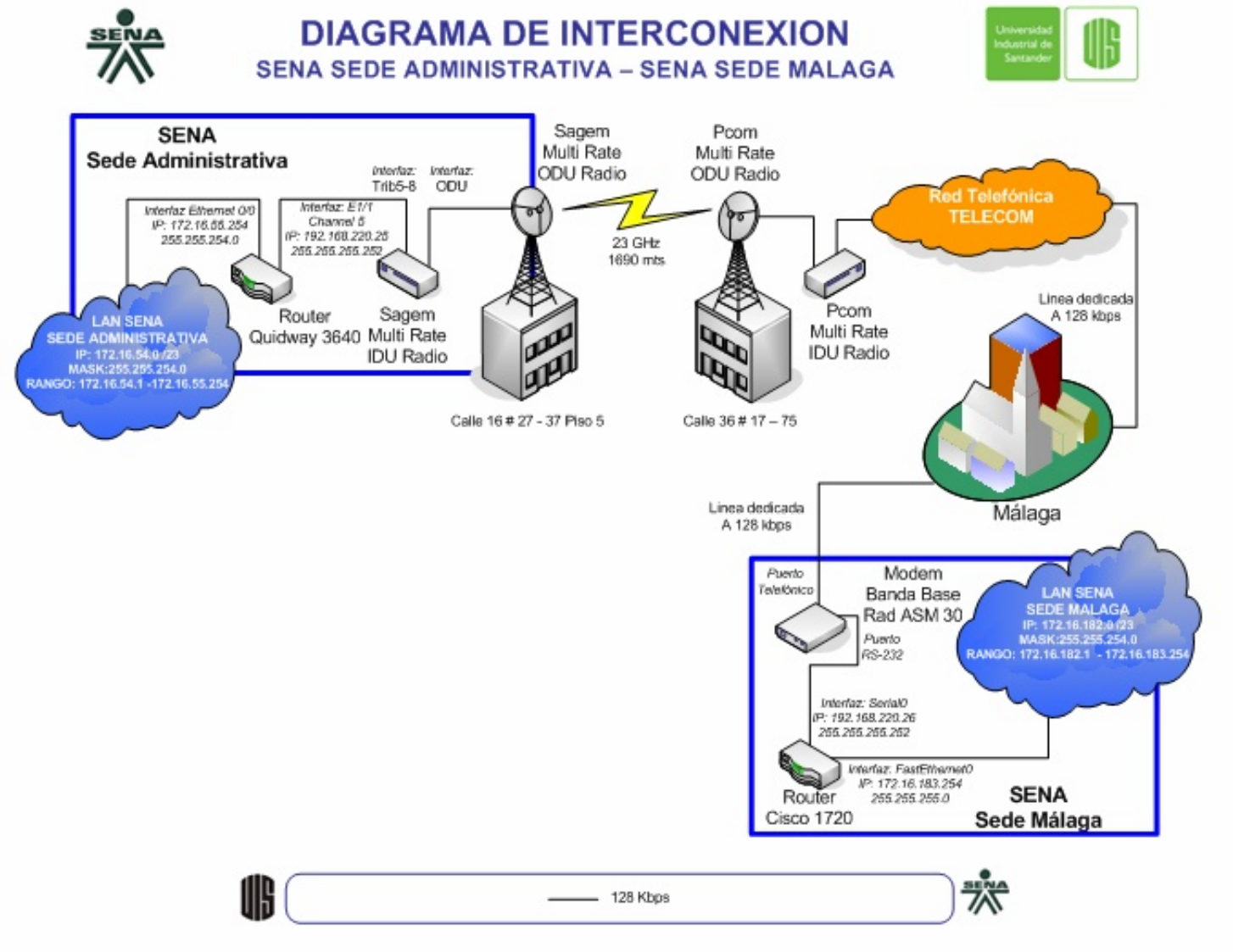


Figura A.3.9. Interconexión Sede Administrativa – Sede Málaga

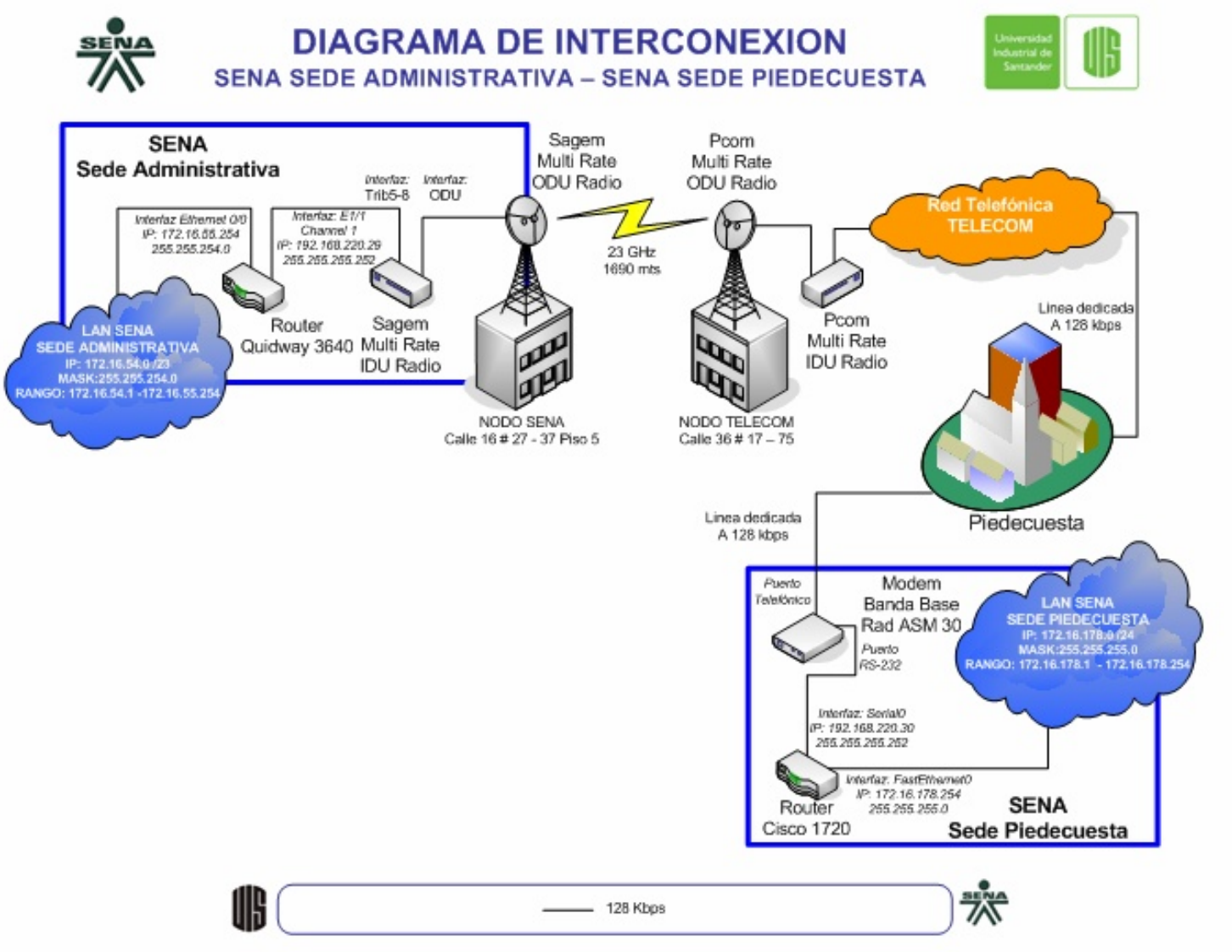


Figura A.3.10. Interconexión Sede Administrativa – Sede Piedecuesta

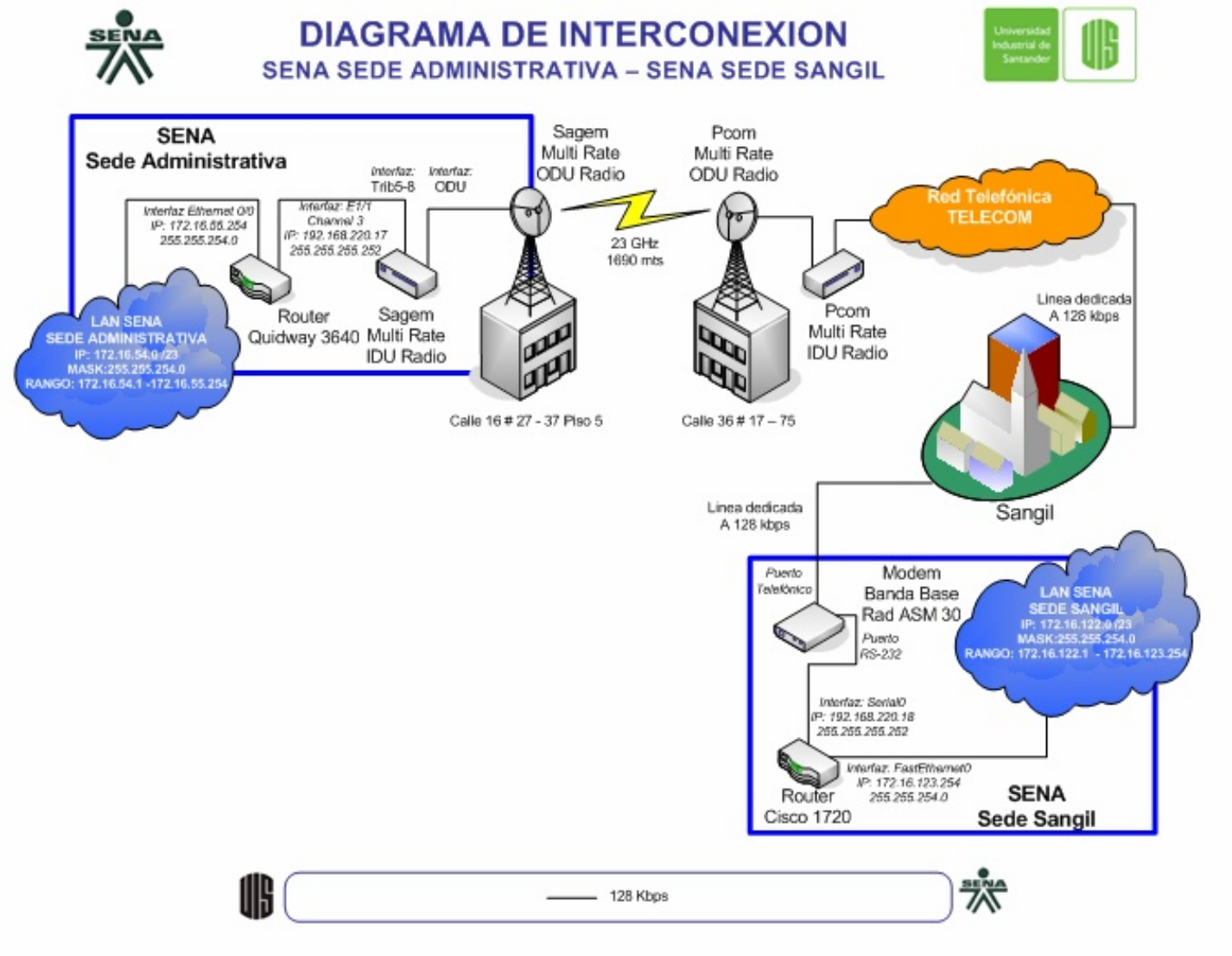


Figura A.3.11. Interconexión Sede Administrativa – Sede San Gil

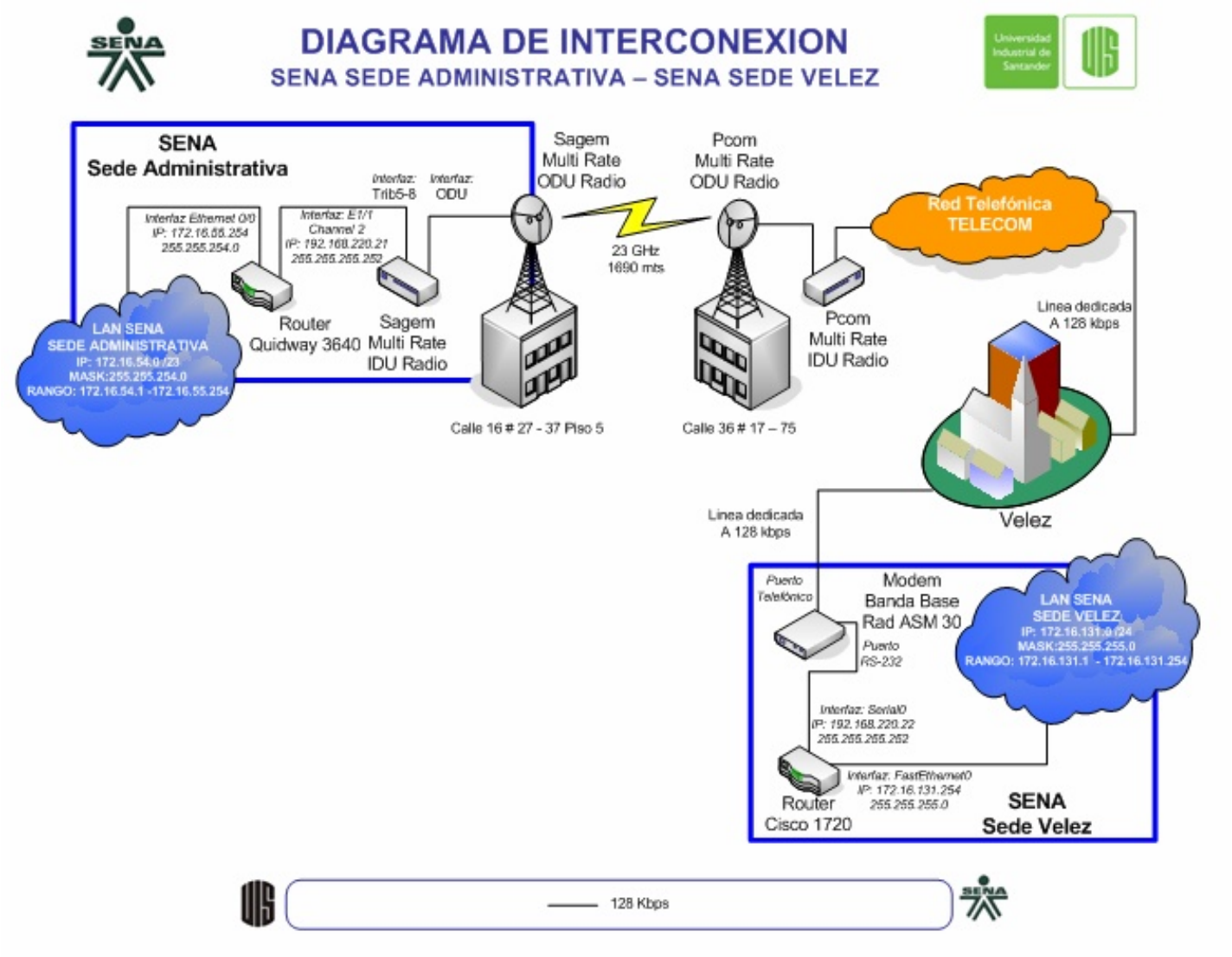


Figura A.3.12. Interconexión Sede Administrativa – Sede Vélez

A.4 Diagramas de Cableado

Los Diagramas de Cableado que se presentan a continuación constituyen un esquema básico del cableado de la red de datos de cada una de las Sedes del SENA REGIONAL SANTANDER y de su tipo (Cable UTP Cat. 5, Cat 5e o F.O.). Se incluyen los dispositivos activos más importantes de la Red que se encuentran en funcionamiento.

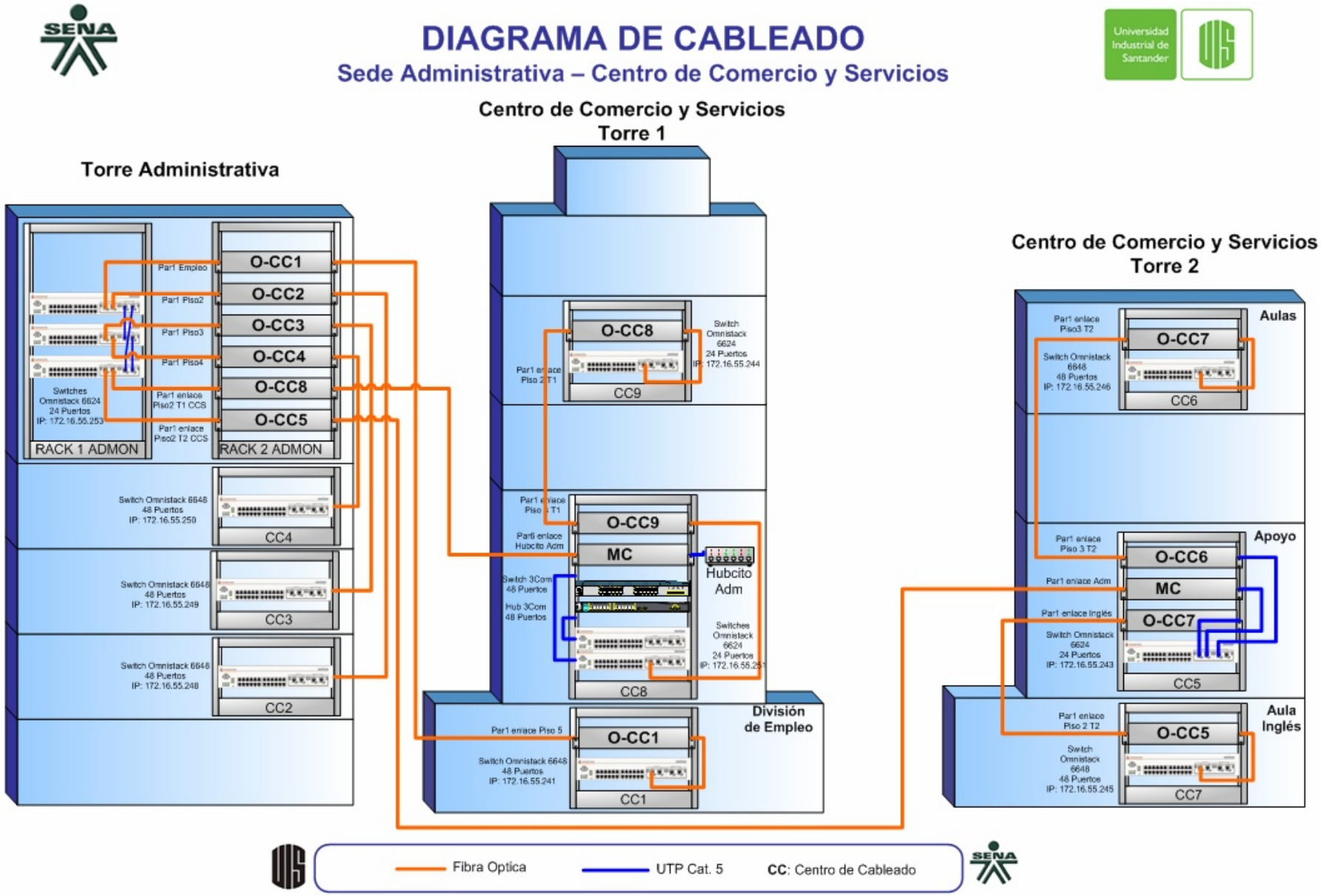


Figura A.4.1. Diagrama de Cableado Sede Administrativa – Sede Comercio y Servicios

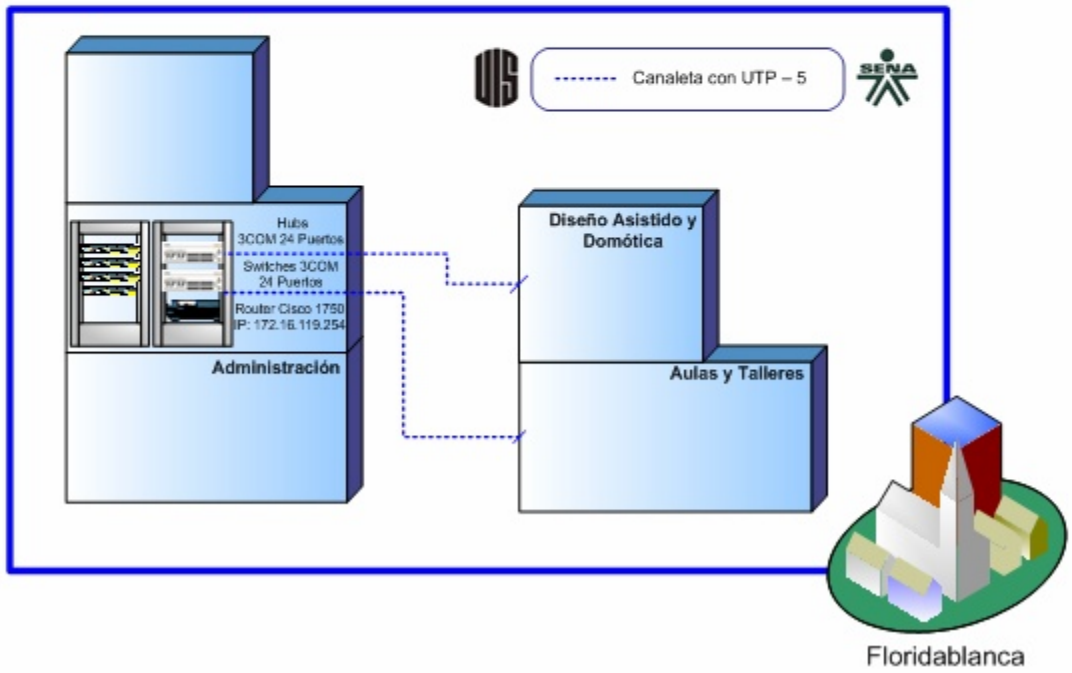


Figura A.4.2. Diagrama de Cableado Sede Floridablanca

DIAGRAMA DE CABLEADO
SENA SEDE GIRON

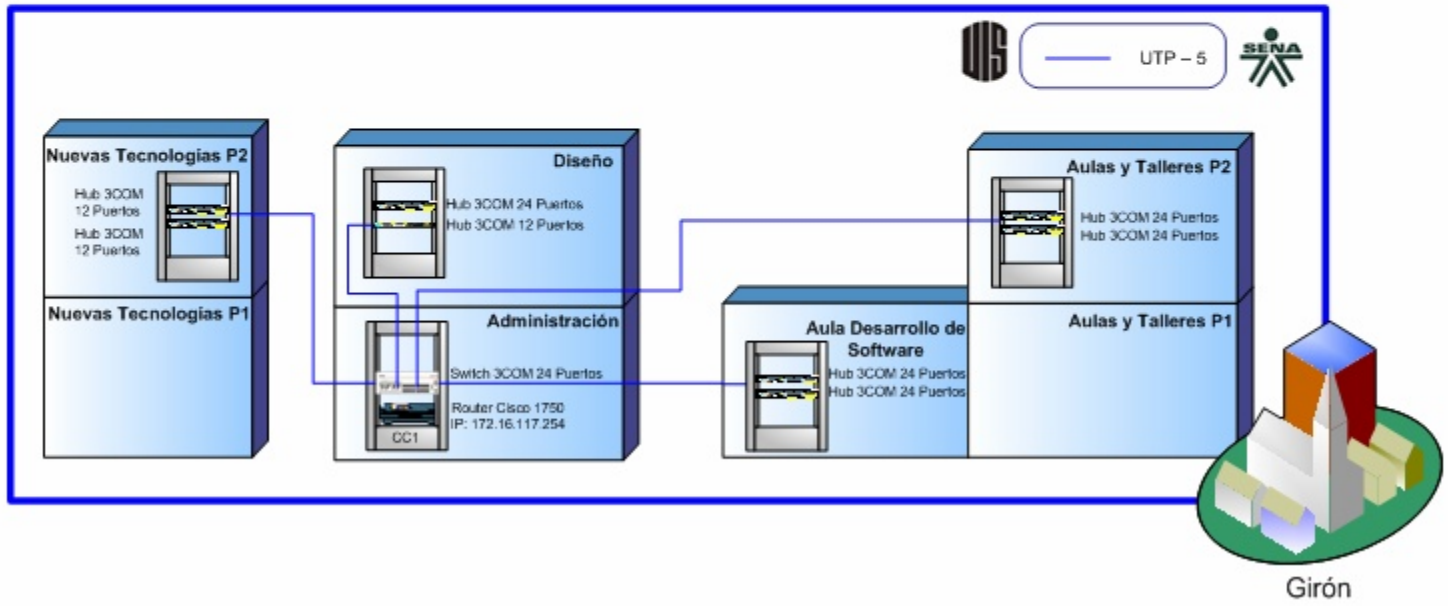


Figura A.4.3. Diagrama de Cableado Sede Girón

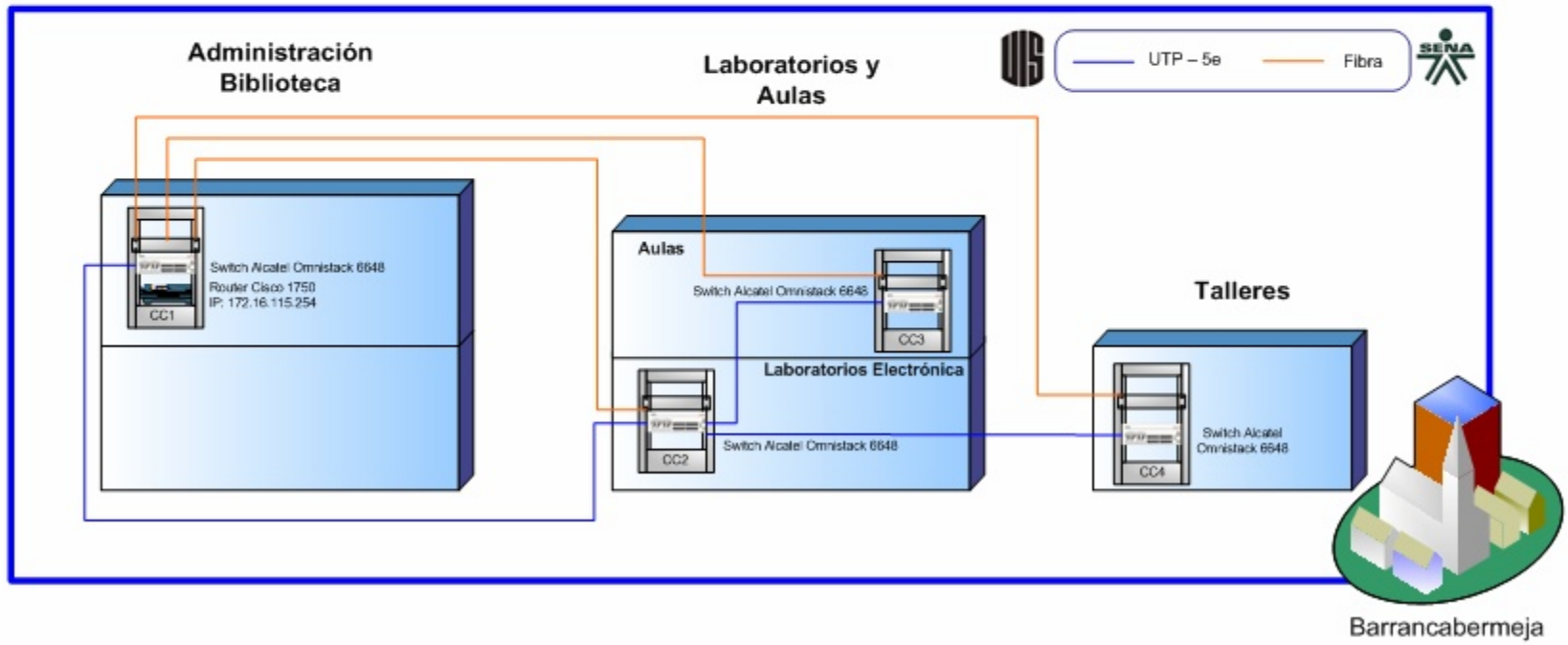


Figura A.4.4. Diagrama de Cableado Sede Barrancabermeja

DIAGRAMA DE CABLEADO
SENA SEDE MALAGA

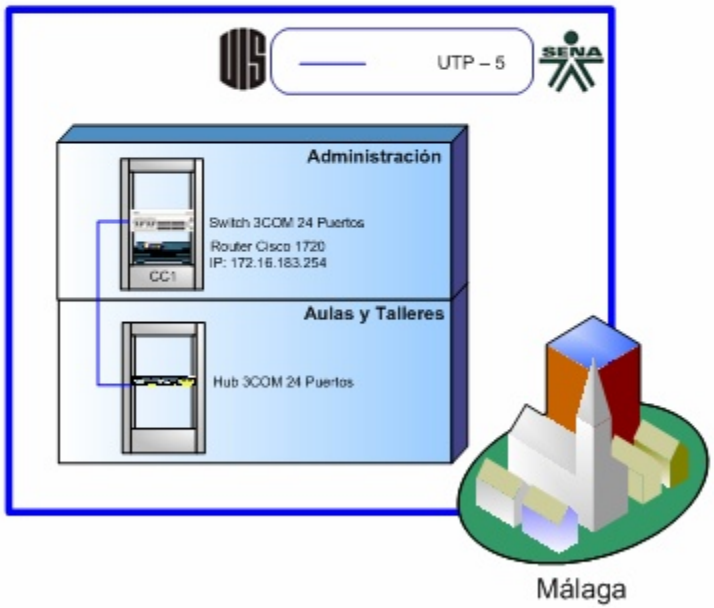


Figura A.4.5. Diagrama de Cableado Sede Málaga

DIAGRAMA DE CABLEADO
SENA SEDE PIEDECUESTA

Figura A.4.6. Diagrama de Cableado Sede Piedecuesta

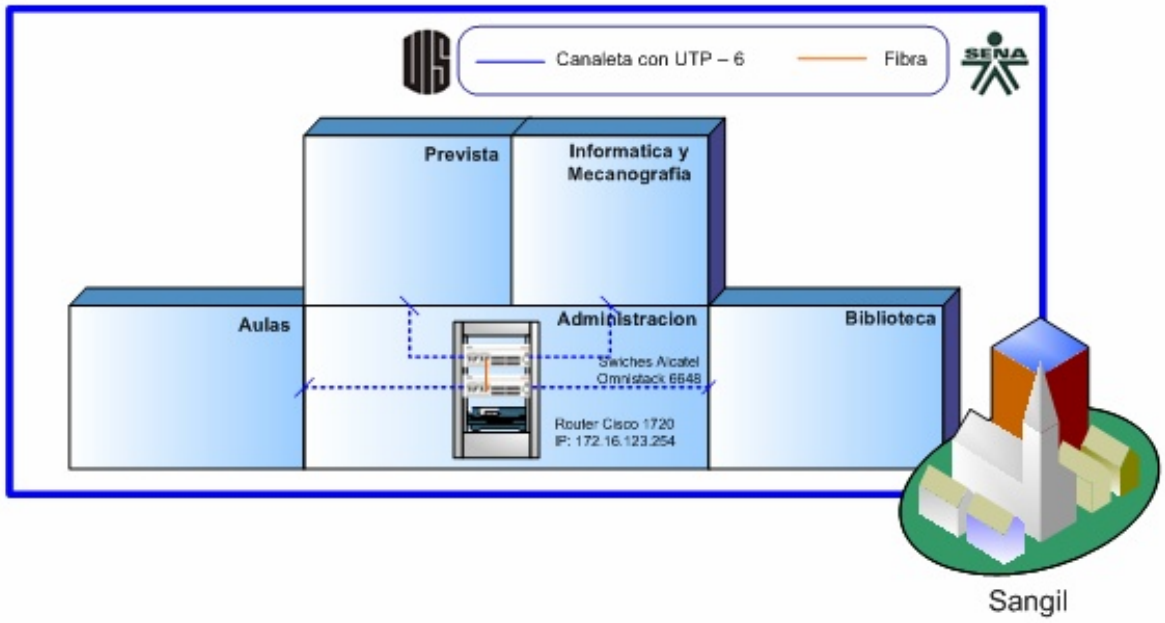


Figura A.4.7. Diagrama de Cableado Sede San Gil

DIAGRAMA DE CABLEADO
SENA SEDE VELEZ

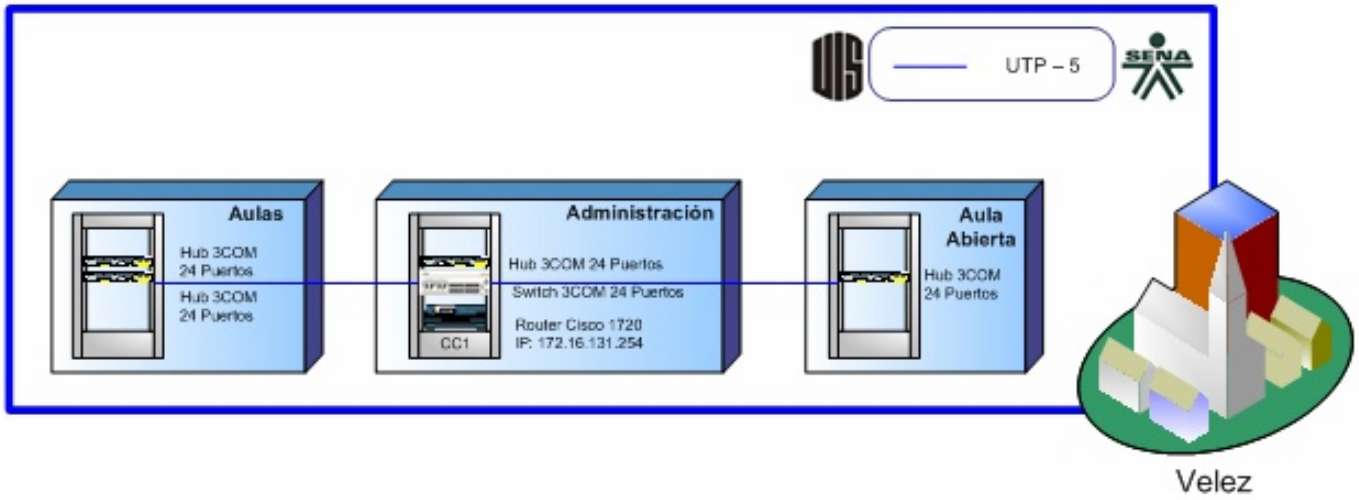


Figura A.4.8. Diagrama de Cableado Sede Vélez

A.5 Conexiones en el Rack Principal

Este esquema corresponde a la forma en la que están interconectados todos los dispositivos activos que se encuentran ubicados en el rack principal de la Red LAN del SENA REGIONAL SANTANDER al momento en el que se realizó el presente estudio.

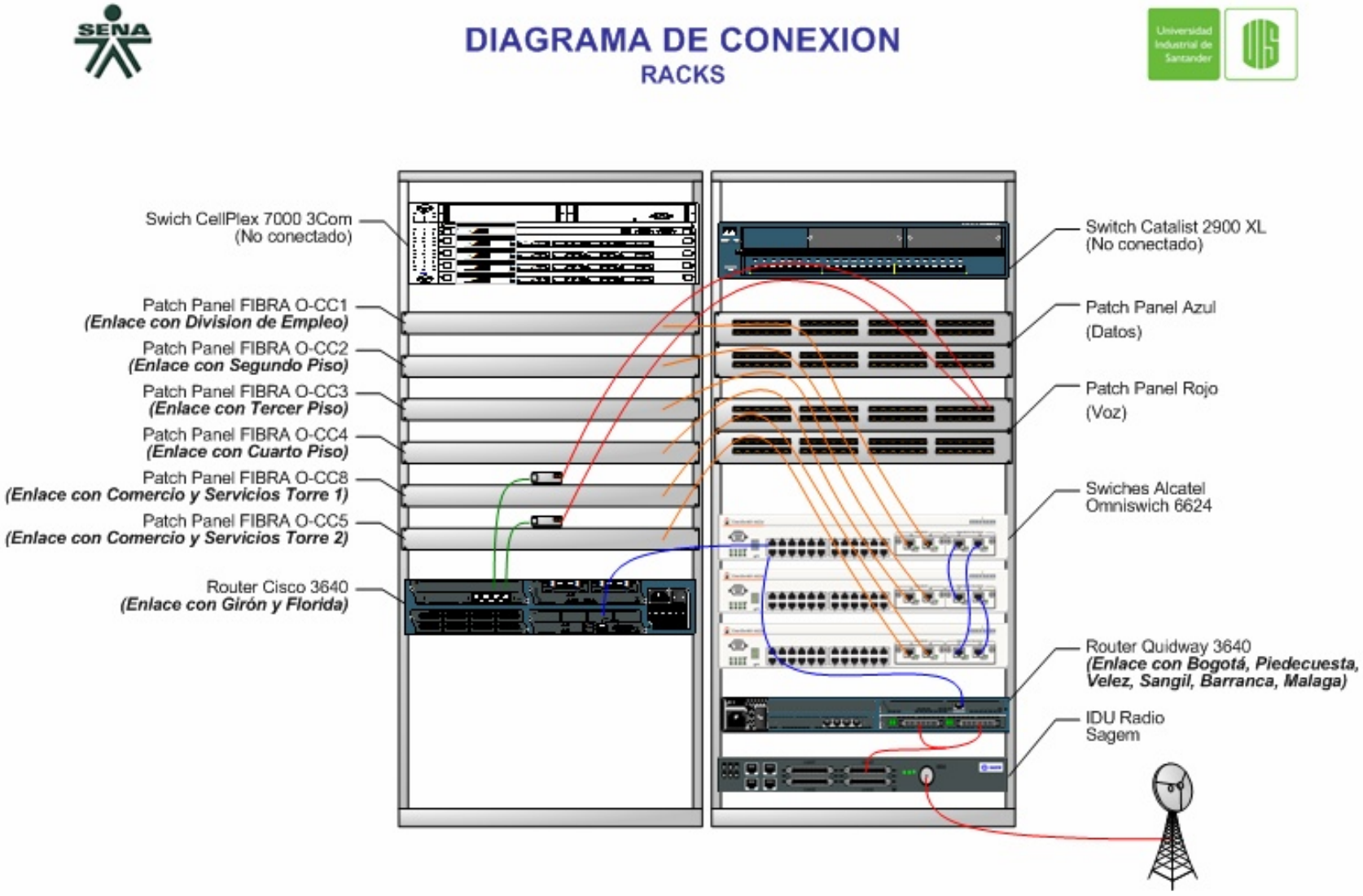


Figura A.5.1. Diagrama de Conexiones actuales en el rack principal

A.6 Inventario de Dispositivos Activos

Para generar este inventario, se contrastó la información suministrada por la Oficina de Sistemas del SENA REGIONAL SANTANDER, con los resultados de los escanéos realizados con la herramienta SNMP Browser de Solarwinds que permite descubrir dispositivos conectados a la red que soporten SNMP y sus características, introduciendo la dirección de red y la comunidad SNMP del dispositivo.

A.6.1 Dispositivos Sede Administrativa

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Piso 5	172.16.55.247	Cisco	Cisco 3640	Habilitado
	Piso 5	172.16.55.254	Huawei	Quidway 3640	Habilitado
Switches	Empleo	172.16.55.241	3COM	SuperStack	Habilitado
	Empleo	172.16.55.241	ALCATEL	OmniStack 6148	Habilitado
	Piso 2	172.16.55.248	3COM	SuperStack 6148	Habilitado
	Piso 2	172.16.55.248	3COM	SuperStack 6148	Habilitado
	Piso 2	172.16.55.248	ALCATEL	OmniStack	Habilitado
	Piso 3	172.16.55.249	3COM	SuperStack	Habilitado
	Piso 3	172.16.55.249	ALCATEL	OmniStack 6148	Habilitado
	Piso 4	172.16.55.250	3COM	SuperStack	Habilitado
	Piso 4	172.16.55.250	3COM	SuperStack	Habilitado
	Piso 4	172.16.55.250	ALCATEL	OmniStack 6148	Habilitado
	Piso 4	172.16.55.250	ALCATEL	OmniSwitch 6148	Habilitado
	Piso 5	172.16.55.253	ALCATEL	OmniSwitch 6148	Habilitado
	Piso 5	172.16.55.253	ALCATEL	OmniSwitch 6148	Habilitado
	Piso 5	172.16.55.253	ALCATEL	OmniSwitch 6148	Habilitado
	Piso 5		3COM	SuperStack	Deshabilitado
	Piso 5		3COM	Cellplex 700	Deshabilitado
	Piso 5		Cisco	Catalyst 2900	Deshabilitado
Servers	Piso 5	172.16.54.7	IBM	Net Finity 5500	Habilitado
	Piso 5	172.16.54.17	DELL	Power Edge 6400	Habilitado
	Piso 5	172.16.54.62	Compaq	Proliant	Habilitado
Tel. IP	Piso 5	172.16.55.239	Alcatel	Premium reflexes	Habilitado
	Piso 5	172.16.55.240	Alcatel	Premiun refrexes	Habilitado
Videoconf.	Piso 5	172.16.55.252	Policom	VSX7000	Habilitado

Tabla A.6.1. Dispositivos Sede Administrativa

A.6.2 Dispositivos Sede Comercio y Servicios

	Localización	Dirección IP	Marca	Referencia	Estado
Switches	Empleo	172.16.55.241	3COM	Superstack	Habilitado
	Empleo	172.16.55.241	ALCATEL	OmniStack 6148	Habilitado
	Piso 2	172.16.55.248	3COM	Superstack 6148	Habilitado
	Piso 2	172.16.55.248	3COM	Superstack 6148	Habilitado
	Piso 2	172.16.55.248	ALCATEL	OmniStack	Habilitado
	Piso 3	172.16.55.249	3COM	Superstack	Habilitado
	Piso 3	172.16.55.249	ALCATEL	OmniStack 6148	Habilitado

Tabla A.6.2. Dispositivos Sede Comercio y Servicios

A.6.3 Dispositivos Sede Florida

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Piso 2 Administración	172.16.119.254	Cisco	Cisco 1750	Habilitado
Switches	Piso 2 Administración		3COM	4226T SuperStack 24 ptos	Habilitado
	Piso 2 Administración		3COM	4226T SuperStack 24 ptos	Habilitado
Hub	Piso 2 Administración		3COM	SuperStack Hub 40	Habilitado
Módem	Piso 2 Administración		RAD	ASM-31	Habilitado

Tabla A.6.3. Dispositivos Sede Florida

A.6.4 Dispositivos Sede Girón

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.117.254	Cisco	Cisco 1750	Habilitado
Switches	Administración		3COM	4226T SuperStack 24 ptos	Habilitado
	Administración		3COM	4226T SuperStack 24 ptos	Habilitado
Hub	Piso 2 Nuevas Tecnologías		3COM	SuperStack Hub 10 (12 puertos)	Habilitado
	Piso 2 Nuevas Tecnologías		3COM	SuperStack Hub 10 (12 puertos)	Habilitado
	Diseño		3COM	SuperStack Hub 10 (12 puertos)	Habilitado
	Diseño		3COM	SuperStack Hub 40 (24 puertos)	Habilitado
	Aula Desarrollo de Software		3COM	SuperStack Hub 40 (24 puertos)	Habilitado
	Aula Desarrollo de Software		3COM	SuperStack Hub 40 (24 puertos)	Habilitado
	Piso 2 Aulas y Talleres		3COM	SuperStack Hub 40 (24 puertos)	Habilitado
	Piso 2 Aulas y Talleres		3COM	SuperStack Hub 40 (24 puertos)	Habilitado
Módem	Administración		RAD	ASM-31	Habilitado

Tabla A.6.4. Dispositivos Sede Girón

A.6.5 Dispositivos Sede Barranca

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.115.253	Cisco	Cisco 1750	Habilitado
Switches	Administración		ALCATEL	OmniStack 6648	Habilitado
	Aulas		ALCATEL	OmniStack 6648	Habilitado
	Laboratorio de Electrónica		ALCATEL	OmniStack 6648	Habilitado
	Talleres		ALCATEL	OmniStack 6648	Habilitado
Hub					
Módem	Administración		RAD	ASM-31	Habilitado

Tabla A.6.5. Dispositivos Sede Barranca

A.6.6 Dispositivos Sede Málaga

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.183.254	Cisco	Cisco 1750	Habilitado
Switches	Administración		3 COM	4226T SuperStack 24 ptos	Habilitado
Hub	Aulas y Talleres		3 COM	SuperStack Hub 40 (24 puertos)	Habilitado
Módem	Administración		RAD	ASM-31	Habilitado

Tabla A.6.6. Dispositivos Sede Málaga

A.6.7. Dispositivos Sede Piedecuesta

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.178.254	Cisco	Cisco 1750	Habilitado
Switches	Administración		3 COM	4226T SuperStack 24 ptos	Deshabilitado
Hub	Aula y Talleres		3 COM	SuperStack Hub 40 (24 puertos)	Habilitado
Módem	Administración		RAD	ASM-31	Habilitado

Tabla A.6.7. Dispositivos Sede Piedecuesta

A.6.8 Dispositivos Sede San Gil

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.123.254	Cisco	Cisco 1750	Habilitado
Switches	Administración		ALCATEL	OmniStack 6648	Habilitado
Hub	Administración		3 COM	SuperStack Hub 40 (24 puertos)	Deshabilitado
Módem	Administración		RAD	ASM-31	Habilitado

Tabla A.6.8. Dispositivos Sede San Gil

A.6.9. Dispositivos Sede Vélez

	Localización	Dirección IP	Marca	Referencia	Estado
Routers	Administración	172.16.131.254	Cisco	Cisco 1750	Habilitado
Switches	Administración		Encore	ENH956P NWY 16 ptos	Deshabilitado
	Administración		TrendNet	TE100 – SE16E Plus 18 ptos	Deshabilitado
	Administración		3 COM	4226T SuperStack 24 ptos	Habilitado
Hub	Administración		3COM	Superstack Hub 40 (24 puertos)	Habilitado
	Aulas		3COM	Superstack Hub 40 (24 puertos)	Habilitado
	Aulas		3COM	Superstack Hub 40 (24 puertos)	Habilitado
	Aula abierta		3COM	Superstack Hub 40 (24 puertos)	Habilitado
Módem			RAD	ASM-31	Habilitado

Tabla A.6.9. Dispositivos Sede Vélez

ANEXO B.
Monitoreo de la Red

B.1. Resultados Gráficos de la Utilización de los Enlaces

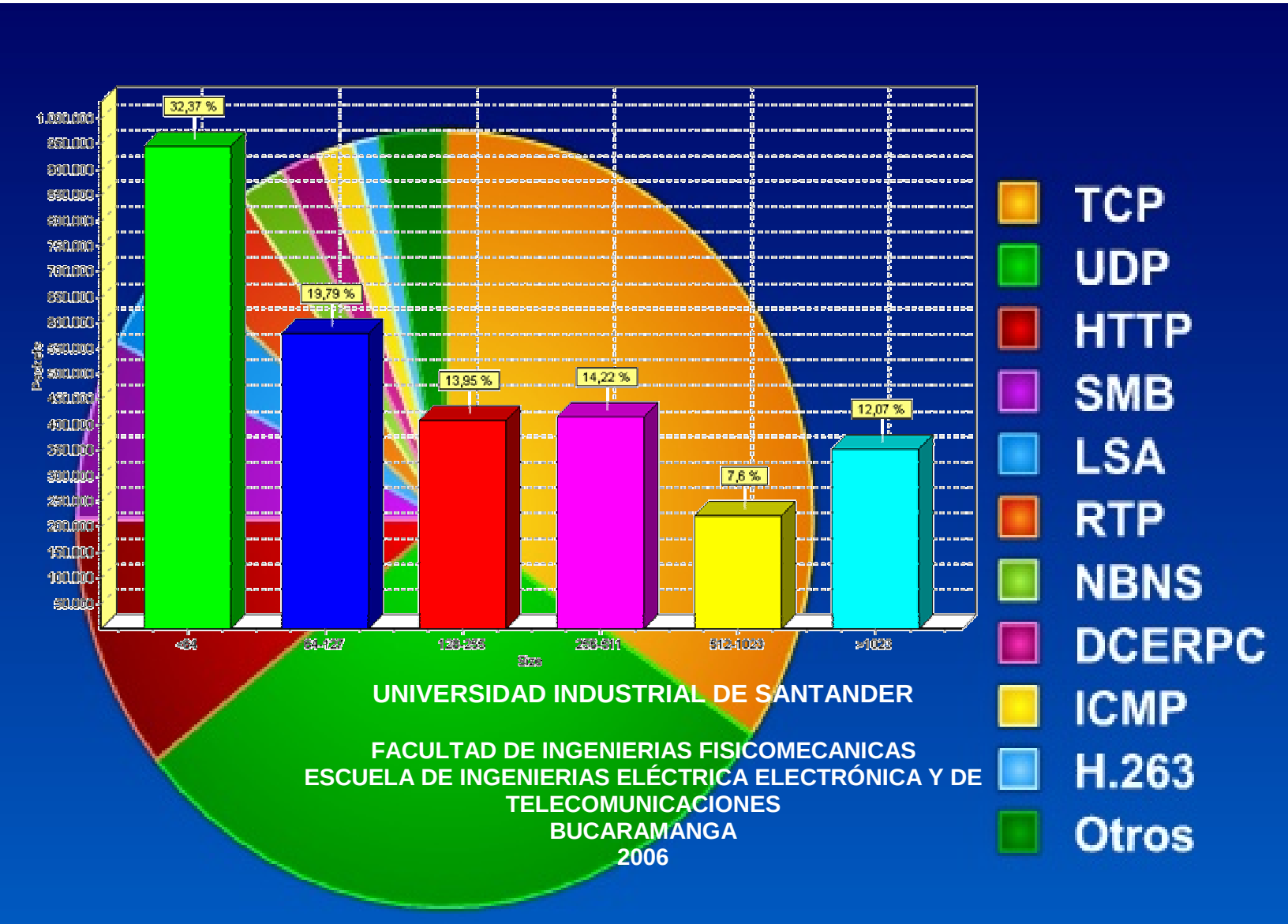
B.2. Resultados Gráficos de la Caracterización del Tráfico – Router Huawei 3640

B.3. Resultados Gráficos de la Caracterización del Tráfico – Router Cisco 3640

B.4. Configuración de un puerto espejo en un switch Alcatel Omniswitch 6624

MONITOREO DE LA RED DE DATOS
SENA REGIONAL SANTANDER
2006

Elaborado por:
JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNÁNDEZ CELIS



UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERIAS ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA

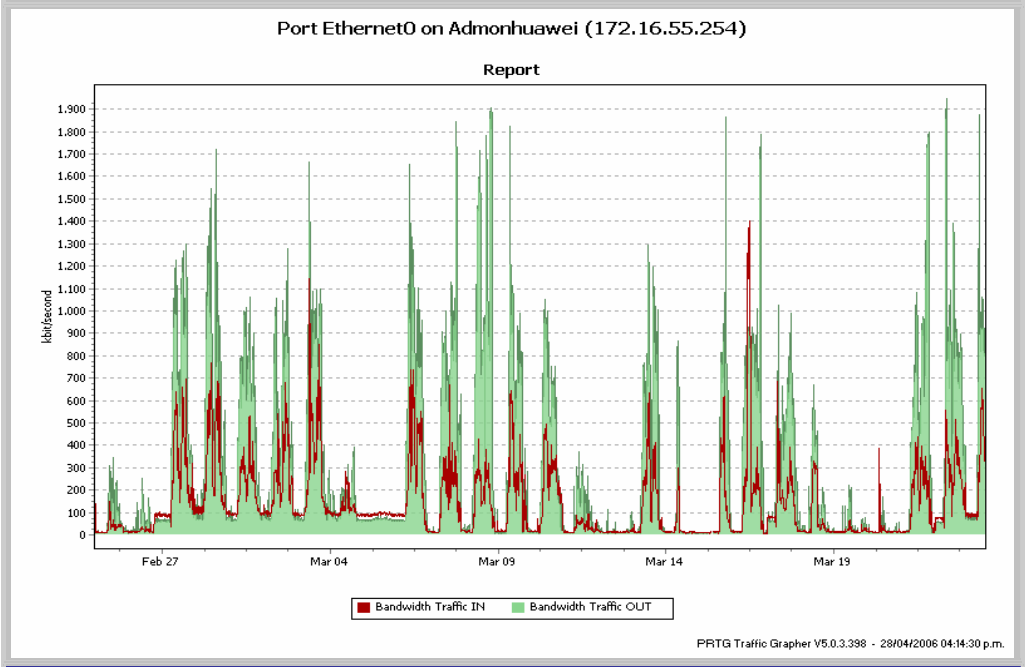
2006

B.1. Resultados Gráficos de la Utilización de los Enlaces

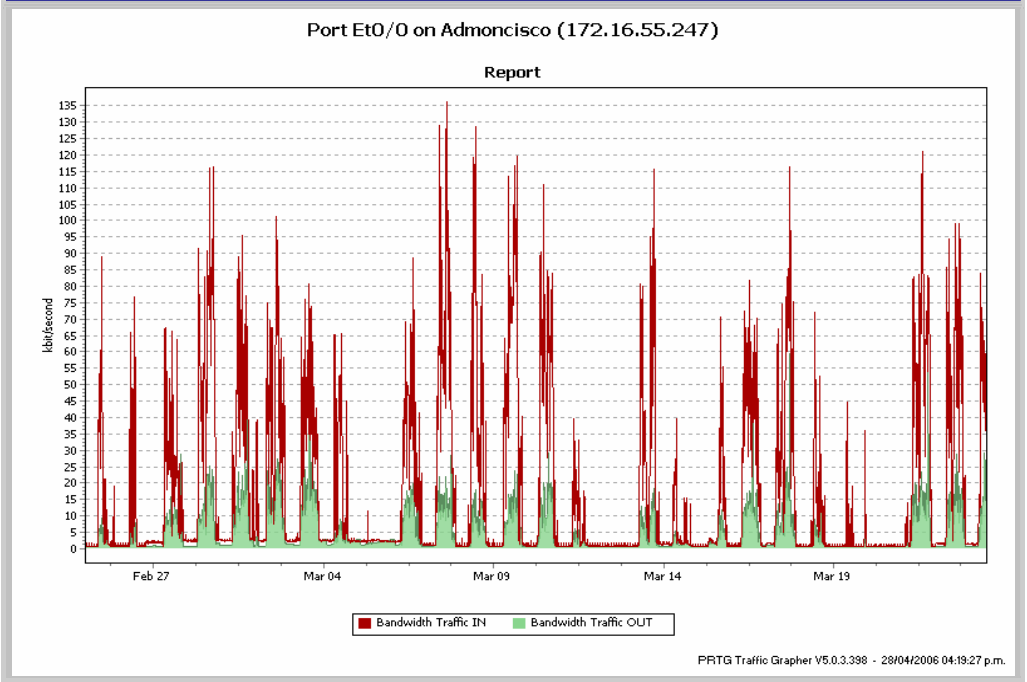
A continuación se presentan los resultados gráficos del monitoreo de los enlaces críticos de la Red de datos del SENA REGIONAL SANTANDER realizados con la herramienta PRTG Traffic Grapher durante los 30 días comprendidos entre el 25 de Febrero y el 26 de Marzo de 2006 y durante el día 28 de febrero del 2006.

B.1.1 Monitoreo de los enlaces entre el 25 de febrero y el 26 de marzo de 2006

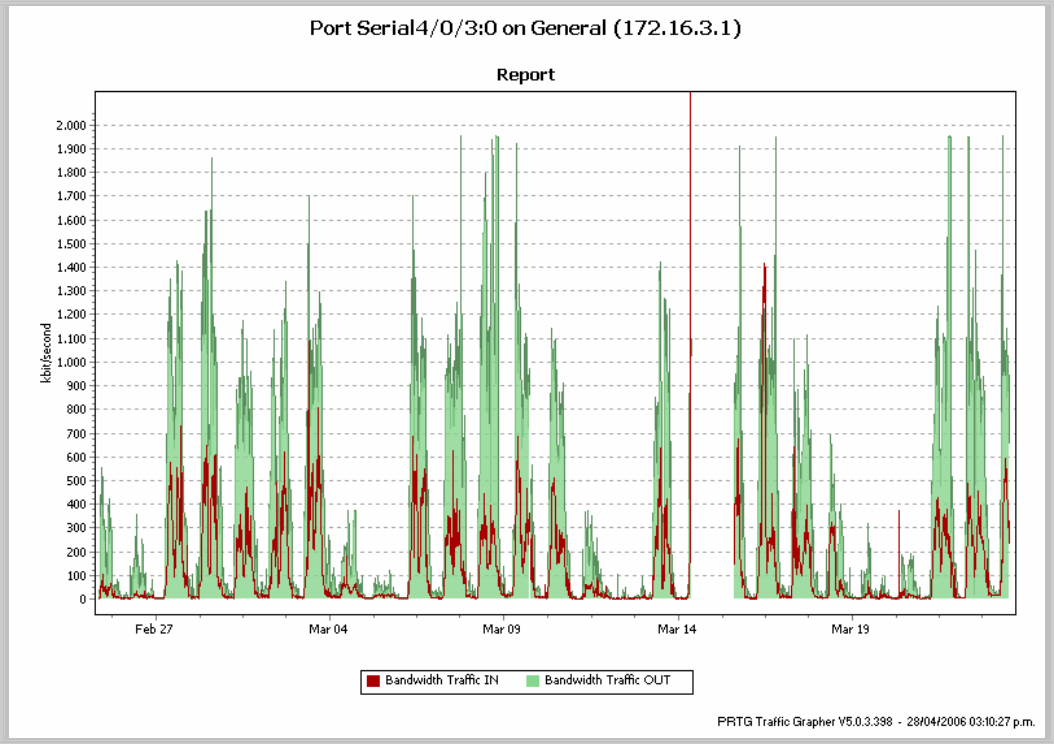
Puerto Ethernet Huawei – 30 días



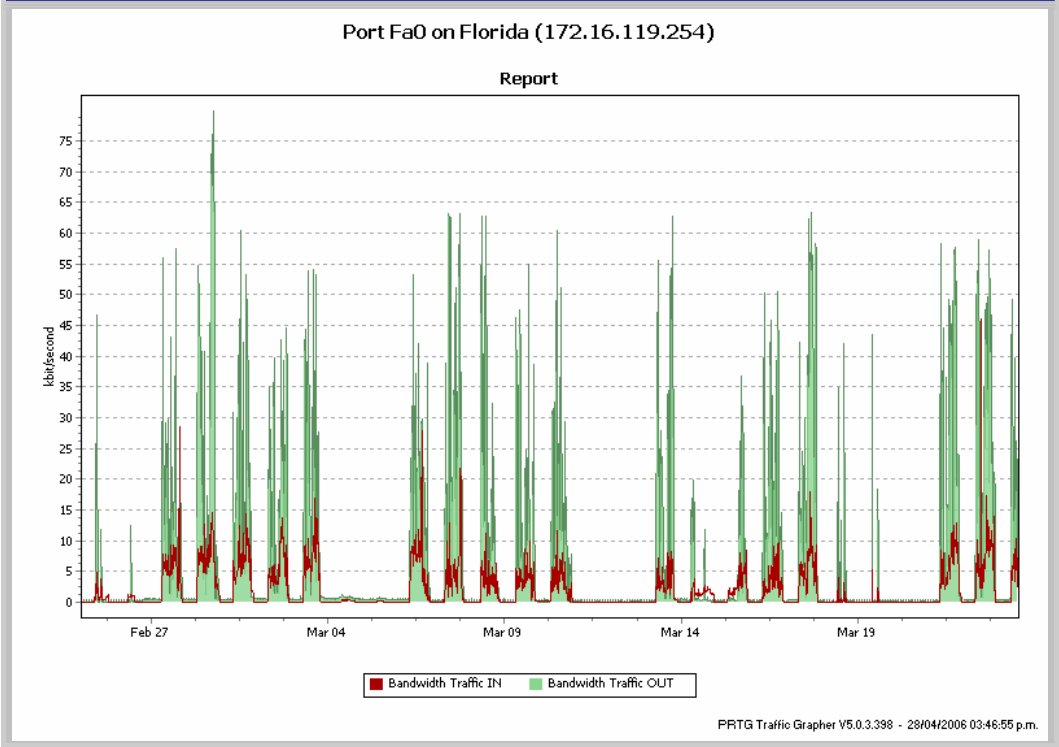
Puerto Ethernet Cisco – 30 días



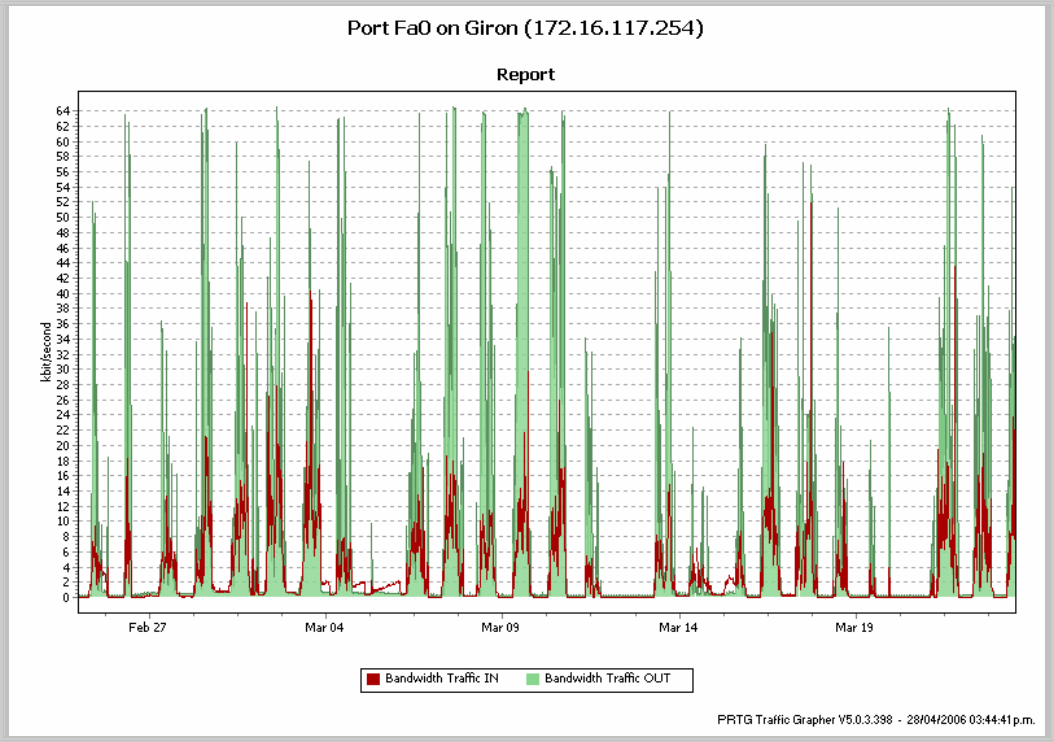
Enlace con la dirección General – 30 días



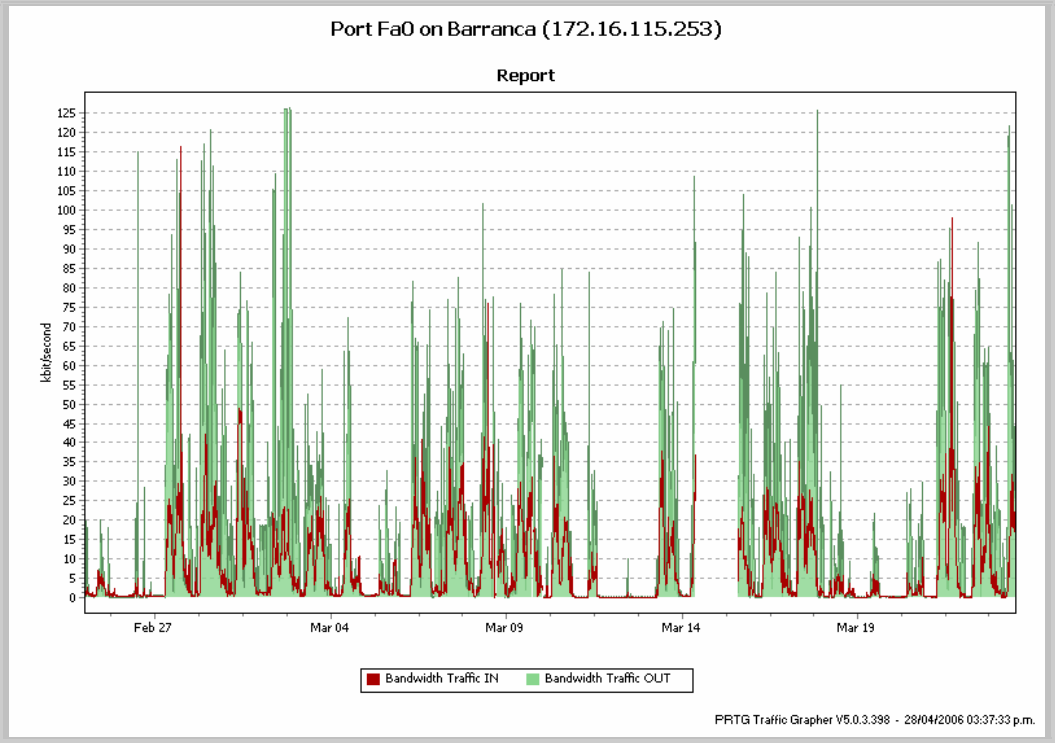
Enlace con Floridablanca – 30 días



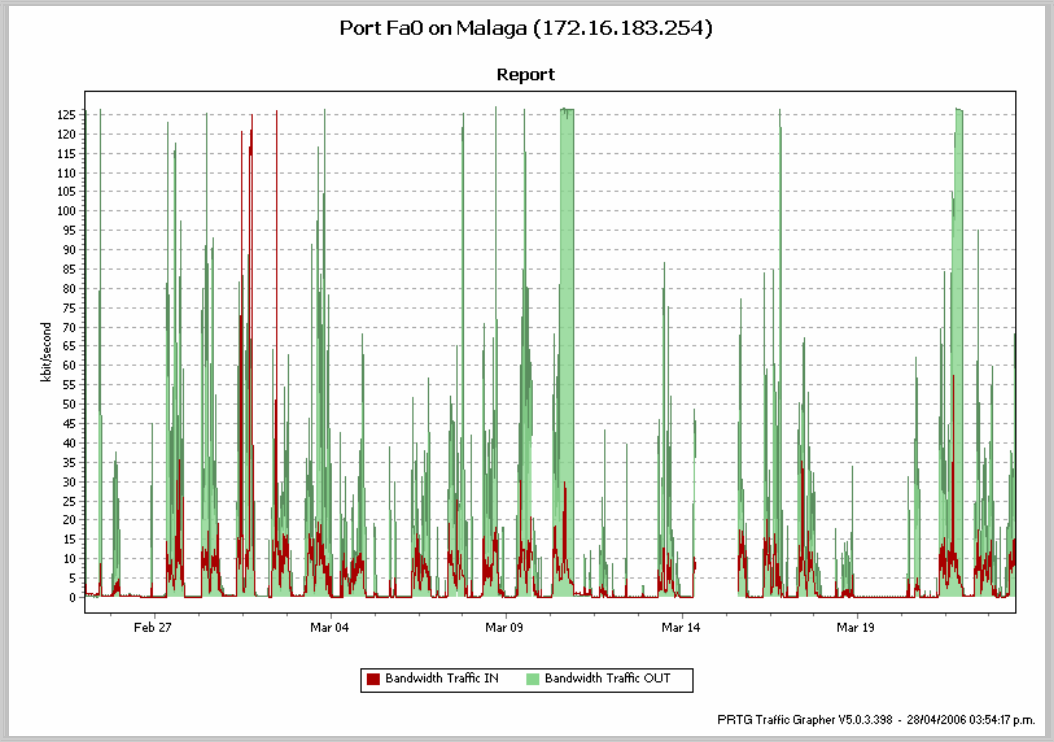
Enlace con Girón – 30 días



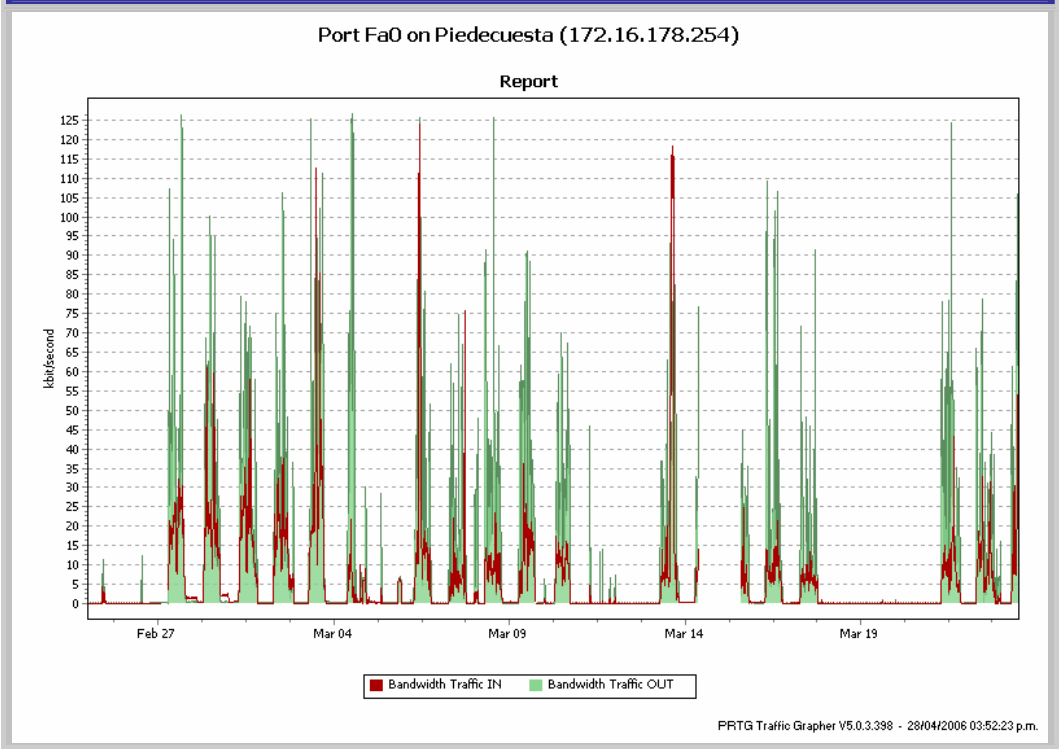
Enlace con Barrancabermeja – 30 días



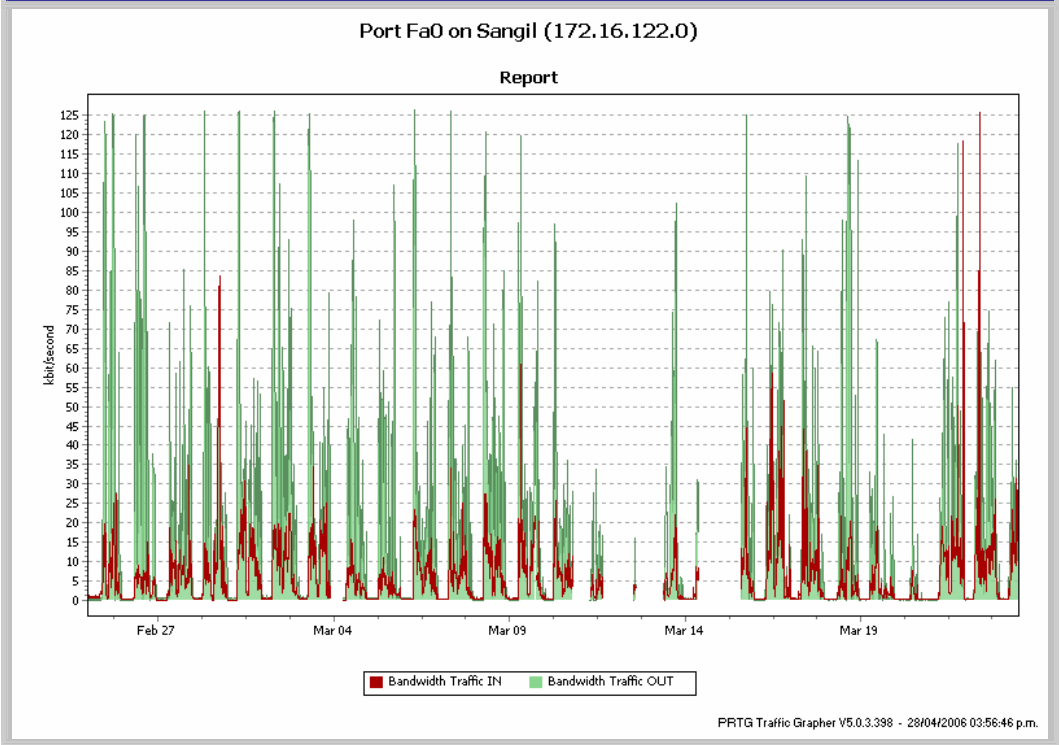
Enlace con Málaga – 30 días



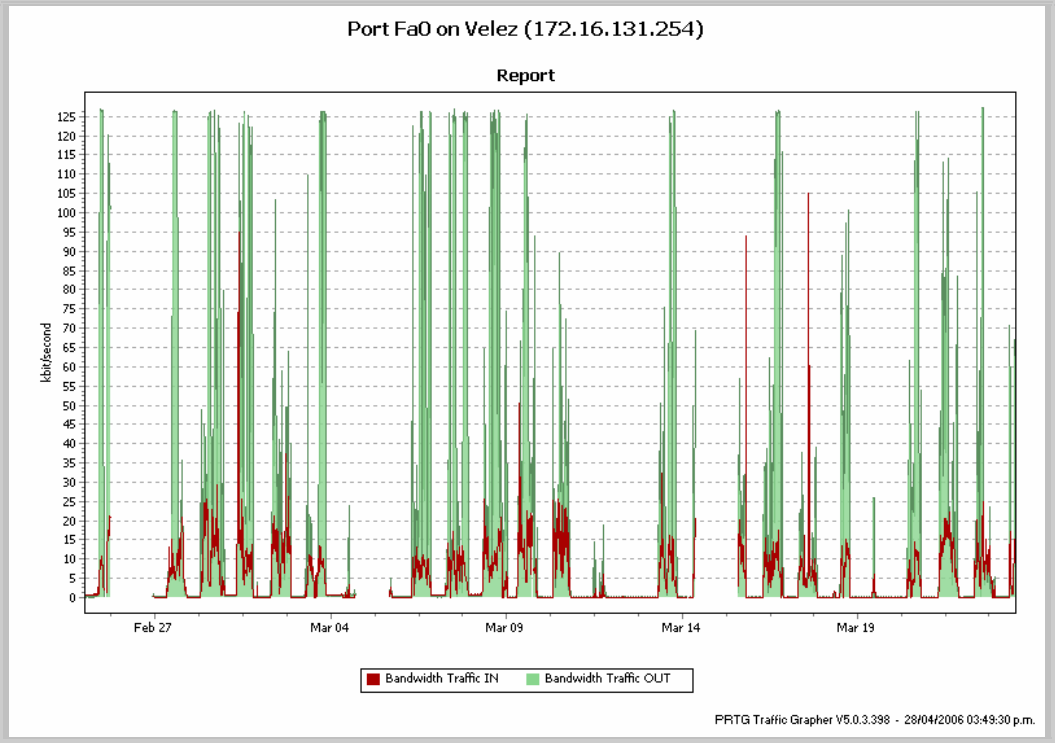
Enlace con Piedecuesta – 30 días



Enlace con San Gil – 30 días

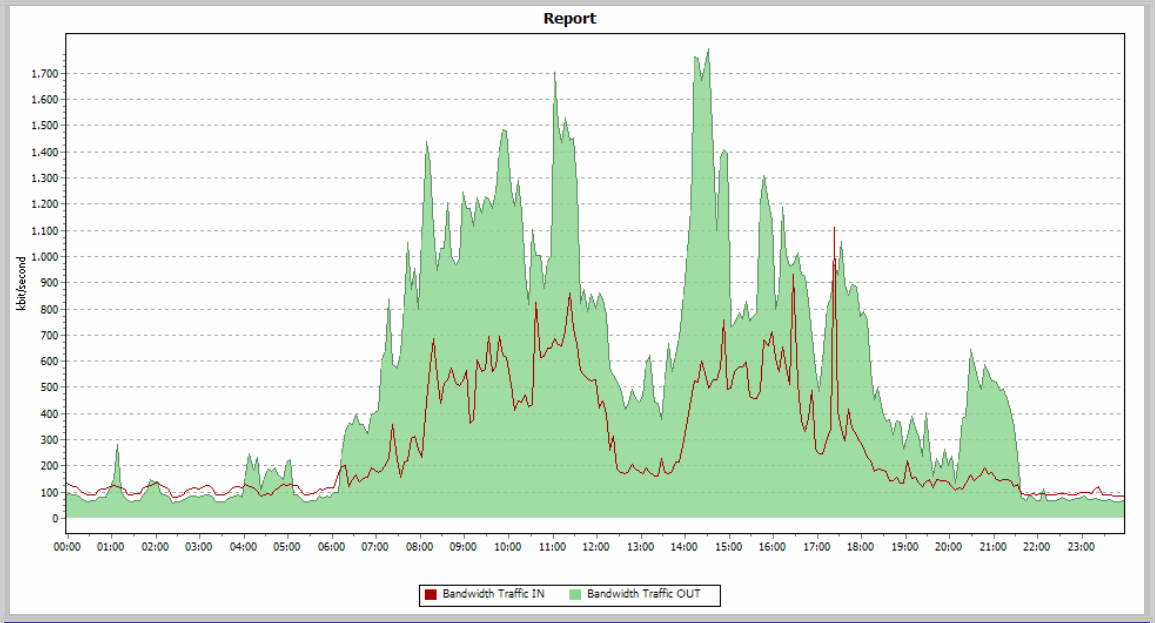


Enlace con Vélez – 30 días

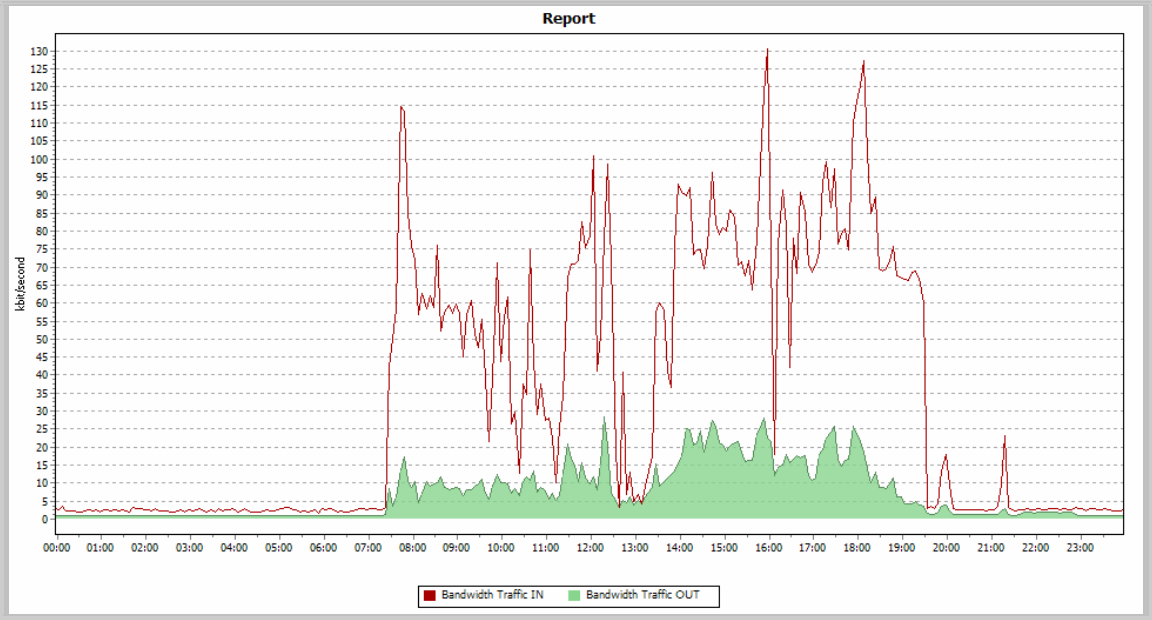


B.1.2 Monitoreo de los enlaces durante el 28 de febrero de 2006

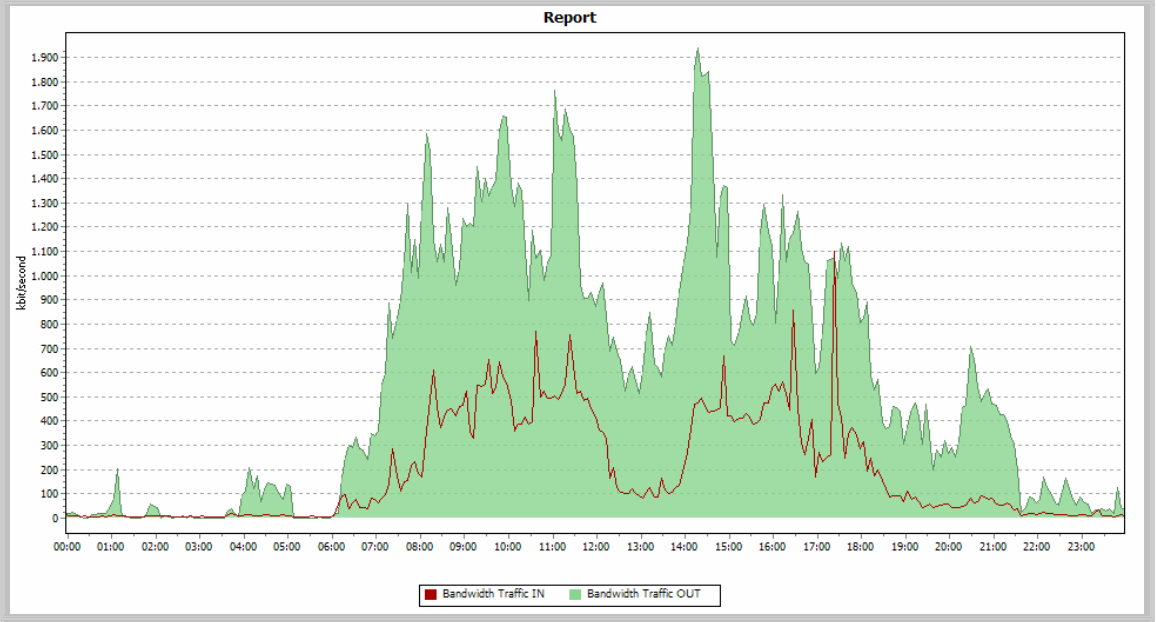
Puerto Ethernet Huawei – 1 día



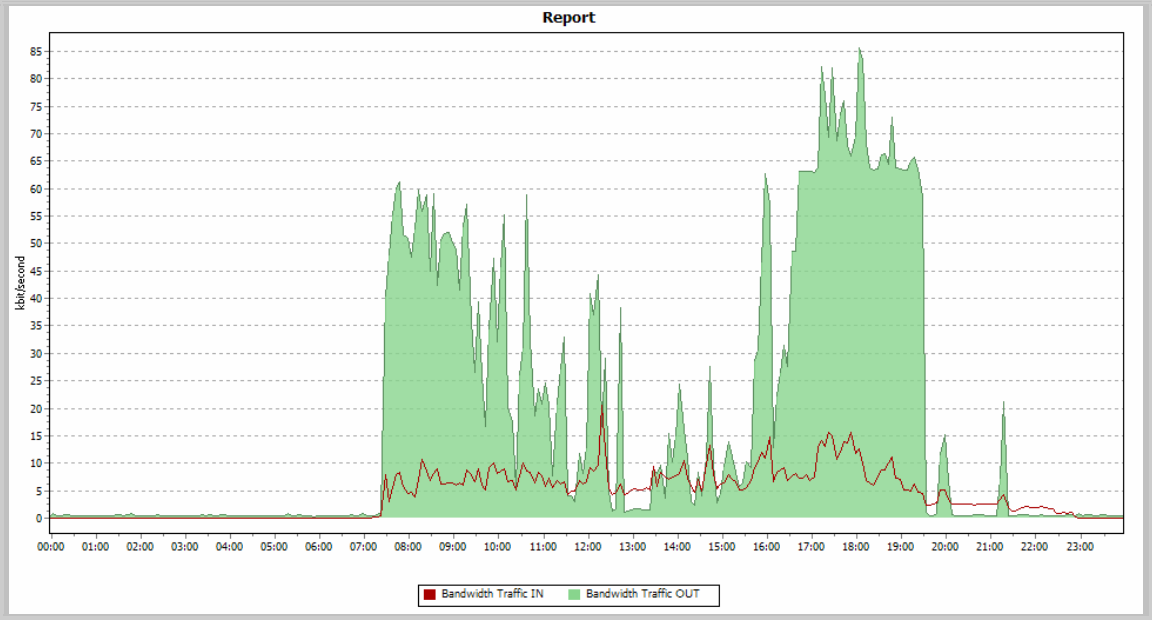
Puerto Ethernet Cisco– 1 día



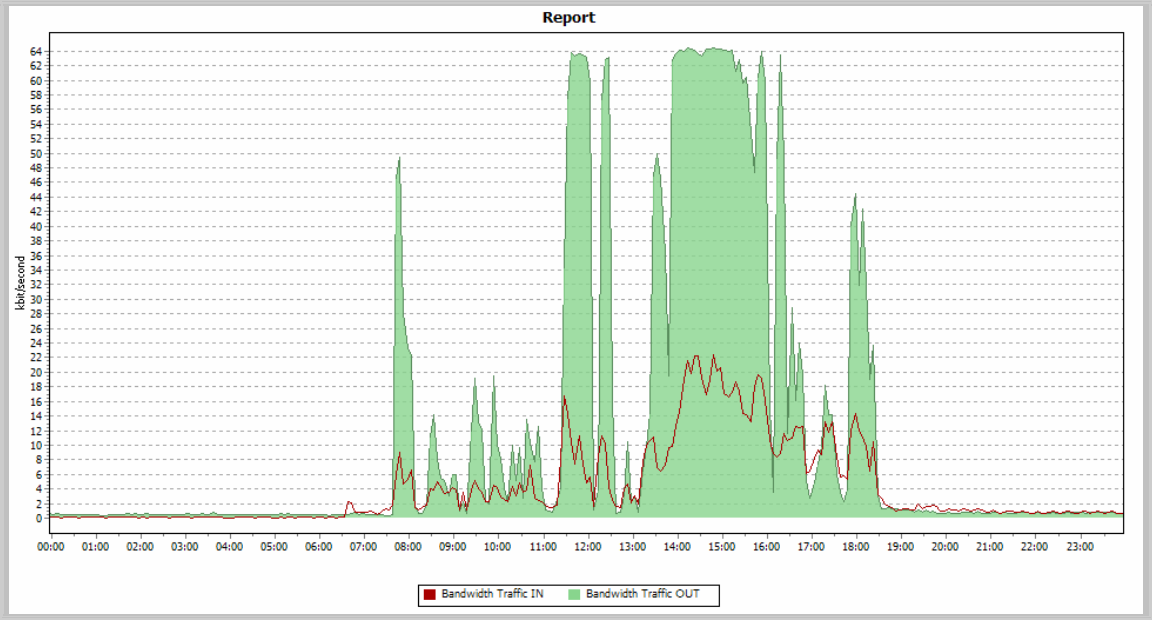
Enlace con la dirección General – 1 día



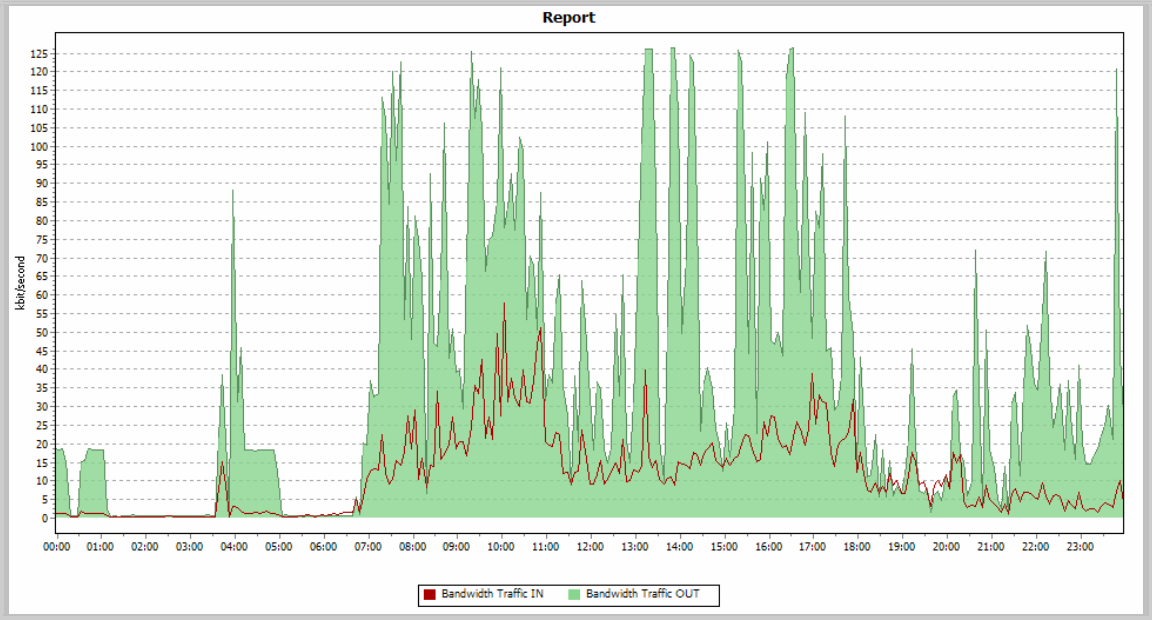
Enlace con Floridablanca – 1 día



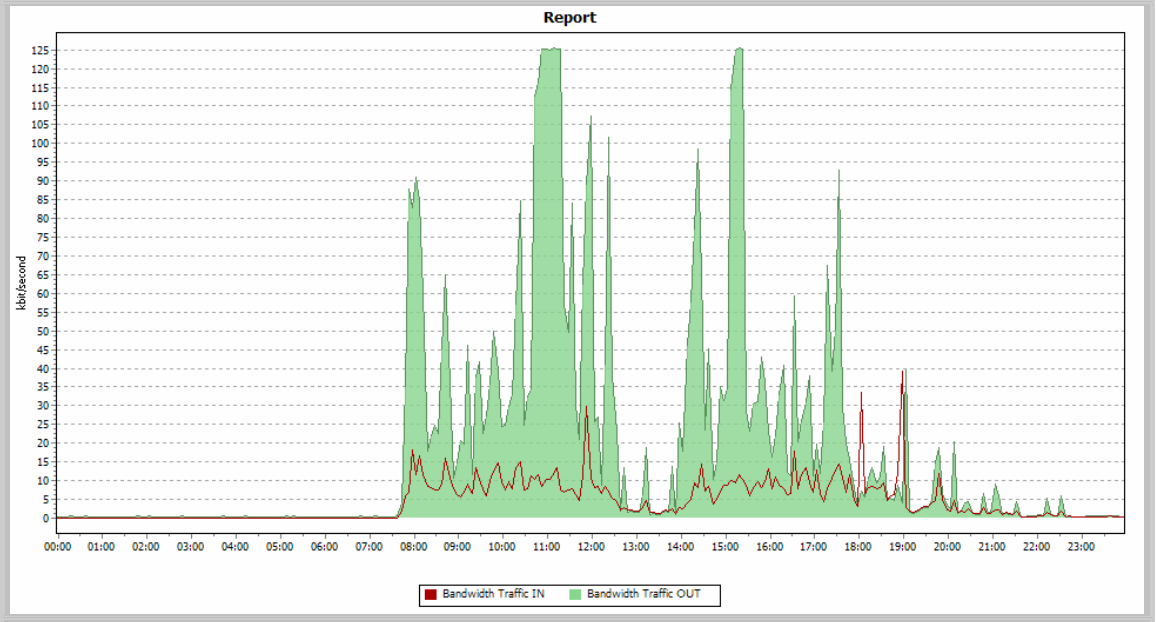
Enlace con Girón – 1 día



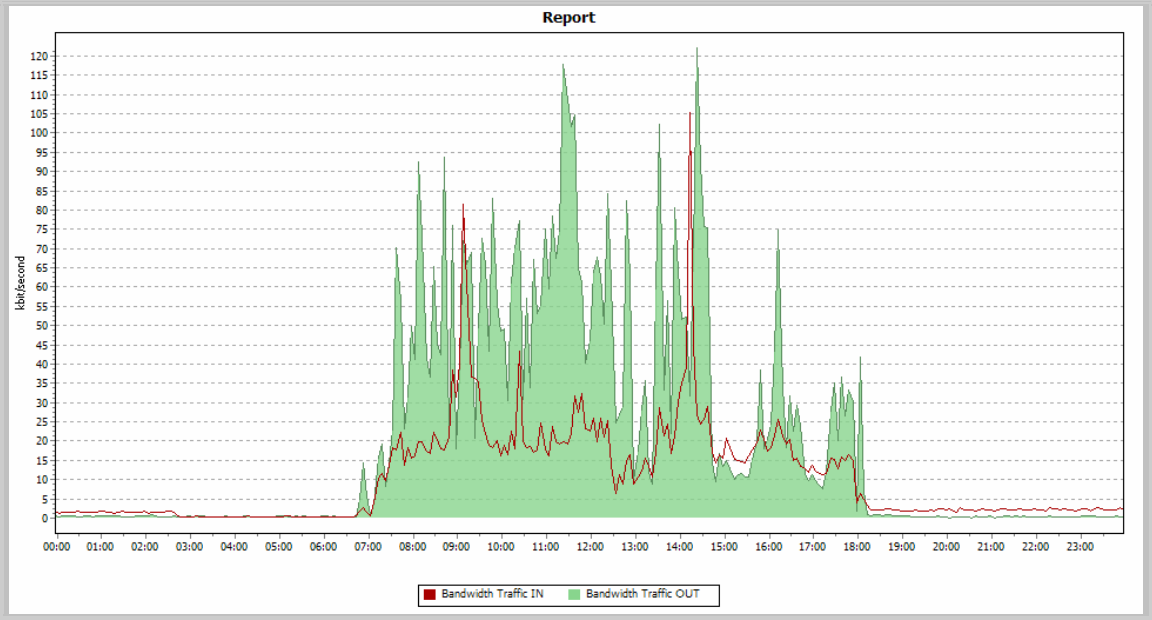
Enlace con Barrancabermeja – 1 día



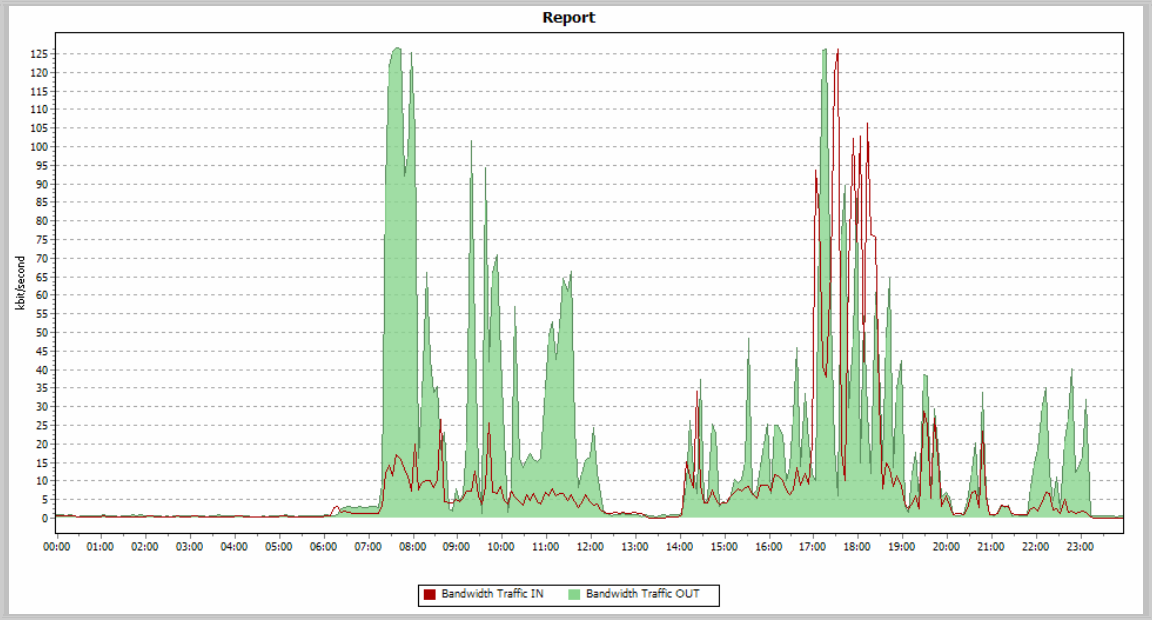
Enlace con Málaga – 1 día



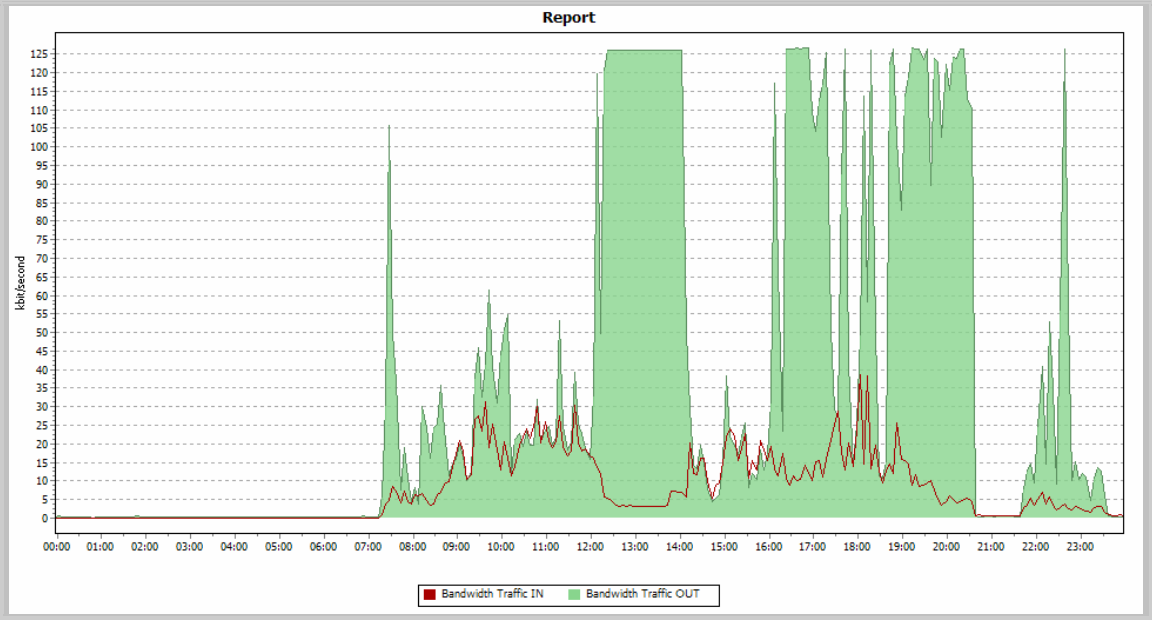
Enlace con Piedecuesta – 1 día



Enlace con San Gil – 1 día



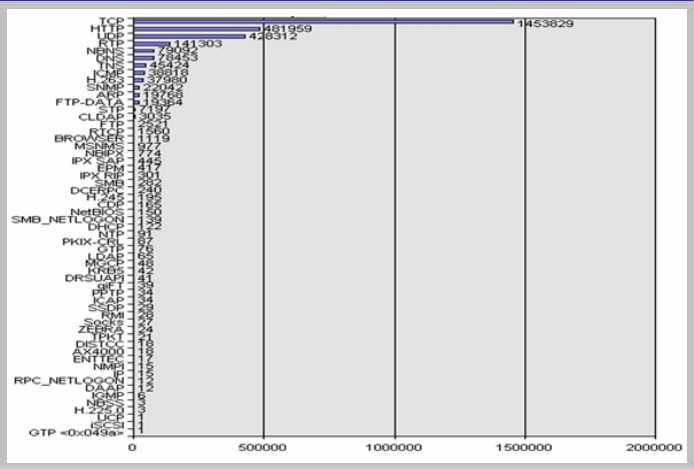
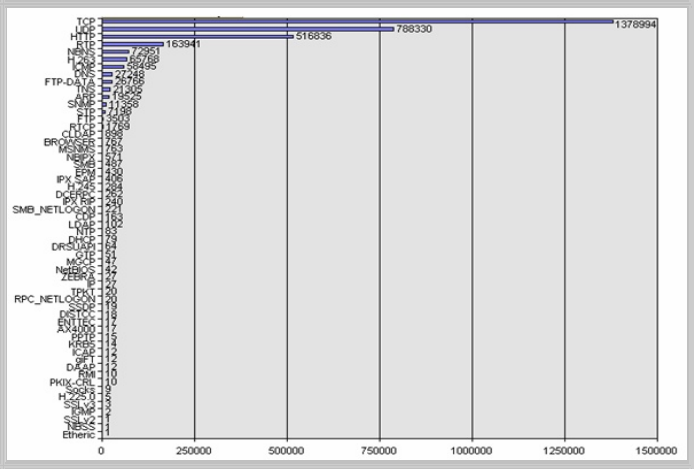
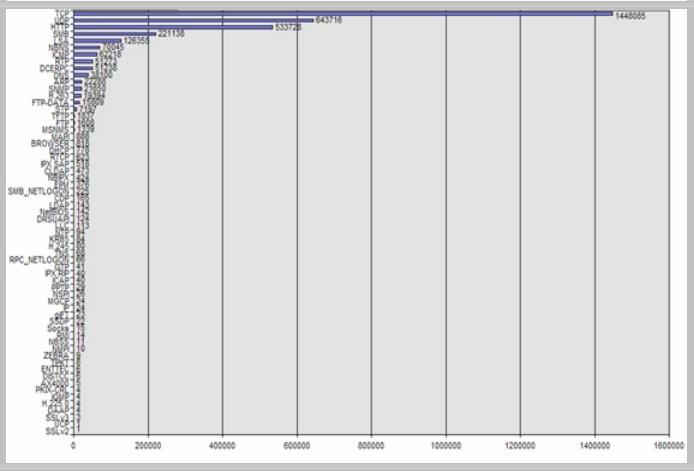
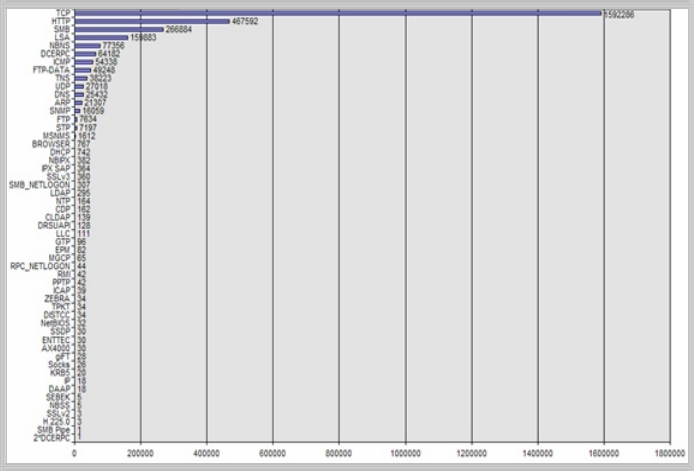
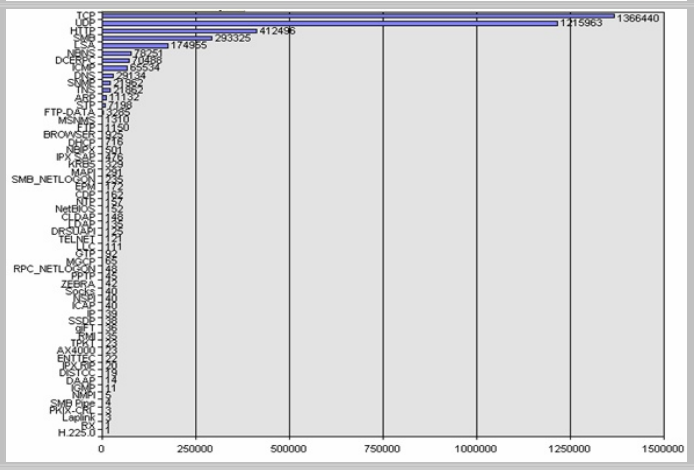
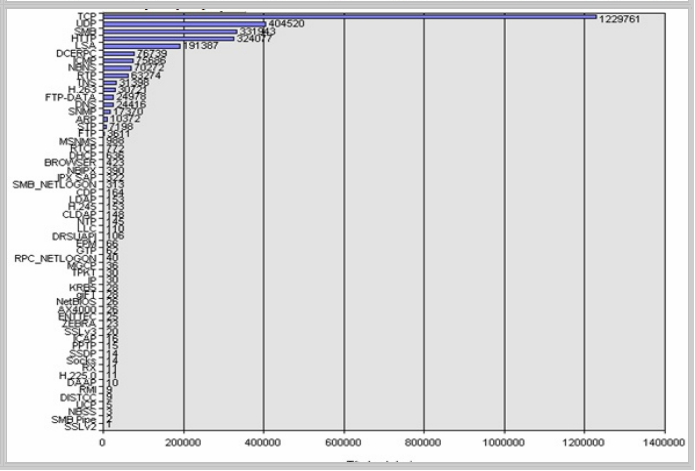
Enlace con Vélez – 1 día



B.2 Resultados Gráficos de la Caracterización del Tráfico Router Huawei

B.2.1 Sede Administrativa

B.2.1.1 Distribución de protocolos por número de paquetes (Cantidades) – Sede Administrativa

	Mañana	Tarde
Lunes		
Martes		
Miércoles		

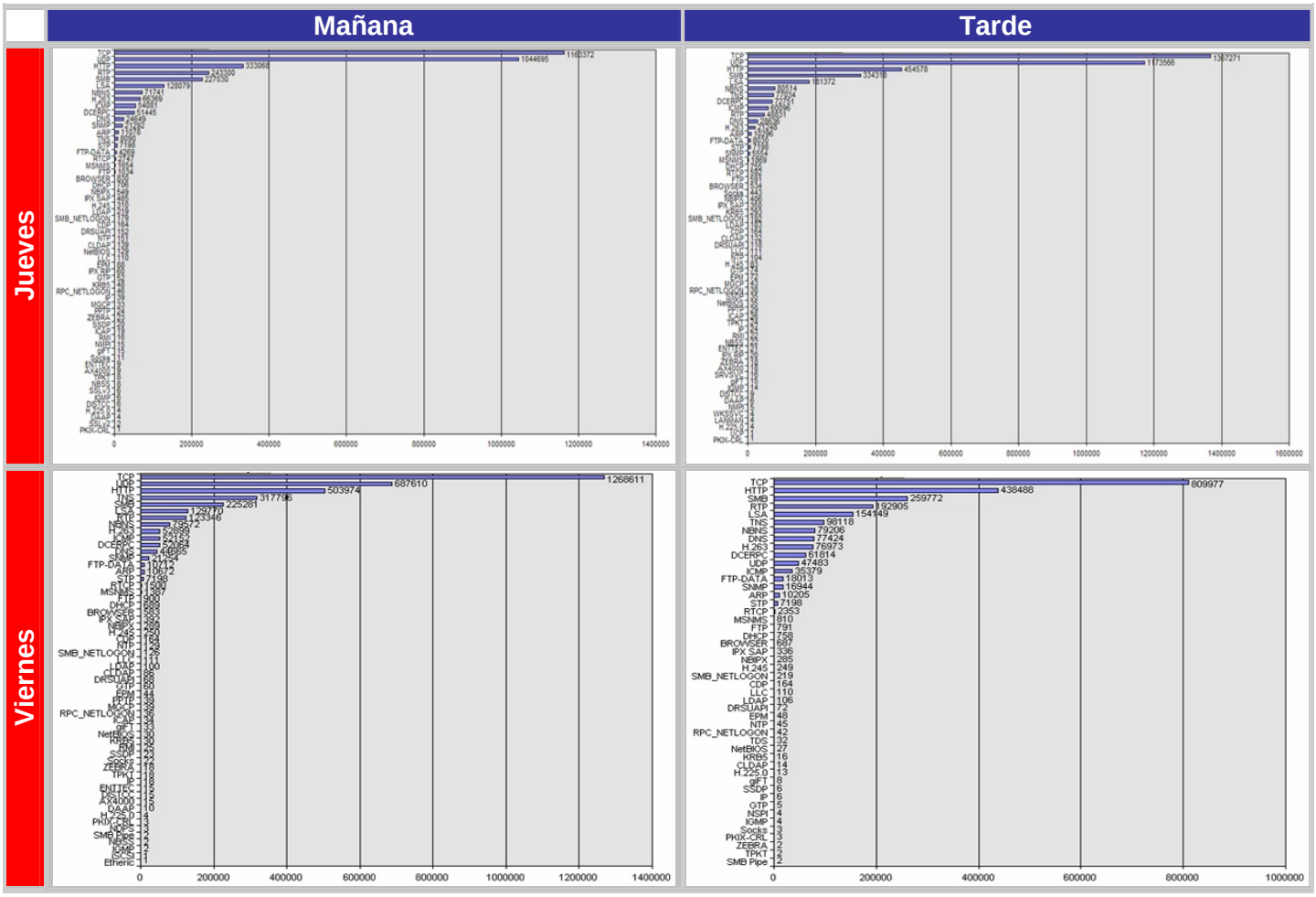


Figura B.2.1.1. Distribución de protocolos por número de paquetes (Cantidades) – Sede Administrativa

B.2.1.2 Distribución de protocolos por número de paquetes (Porcentajes) – Sede Administrativa

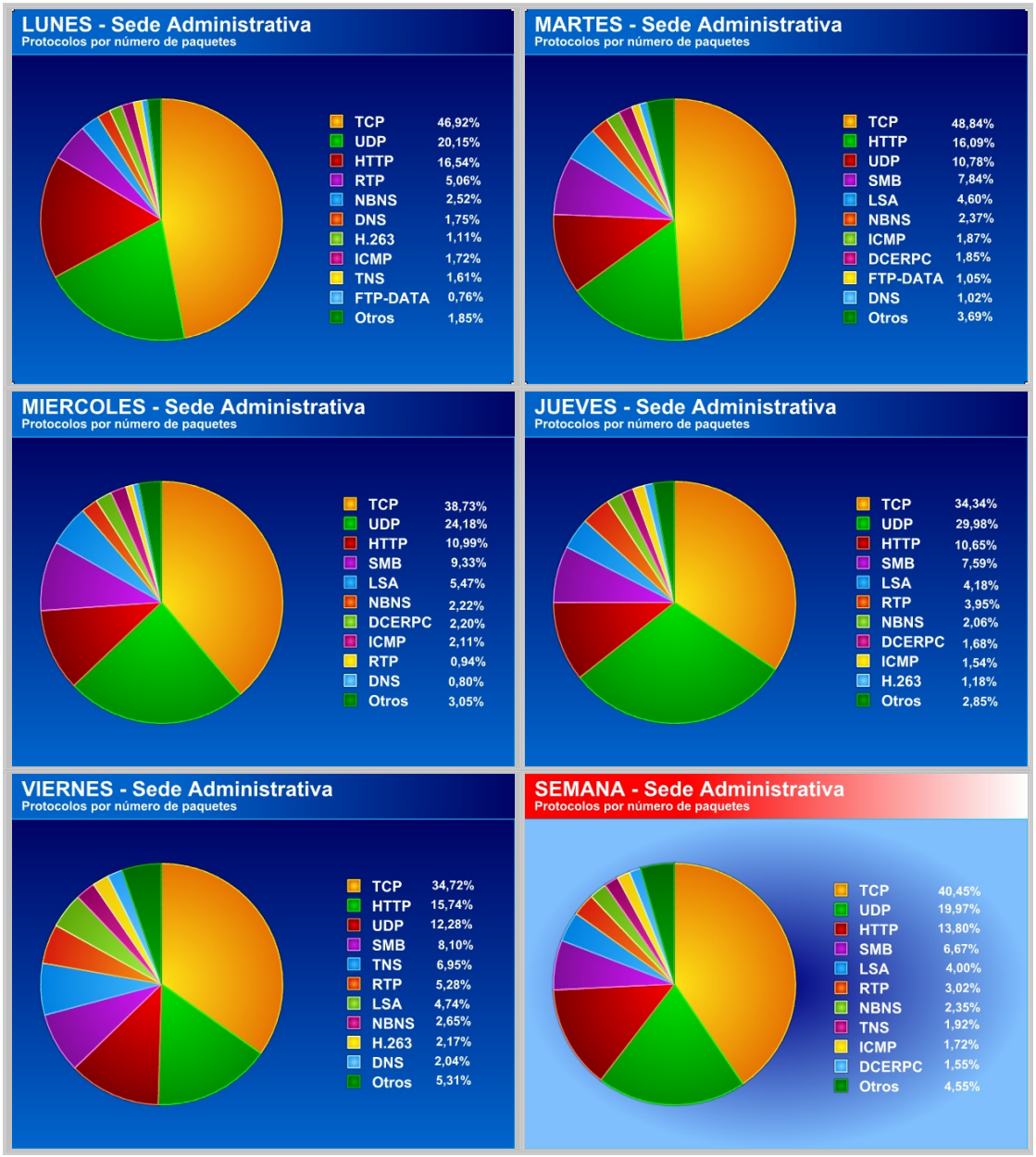
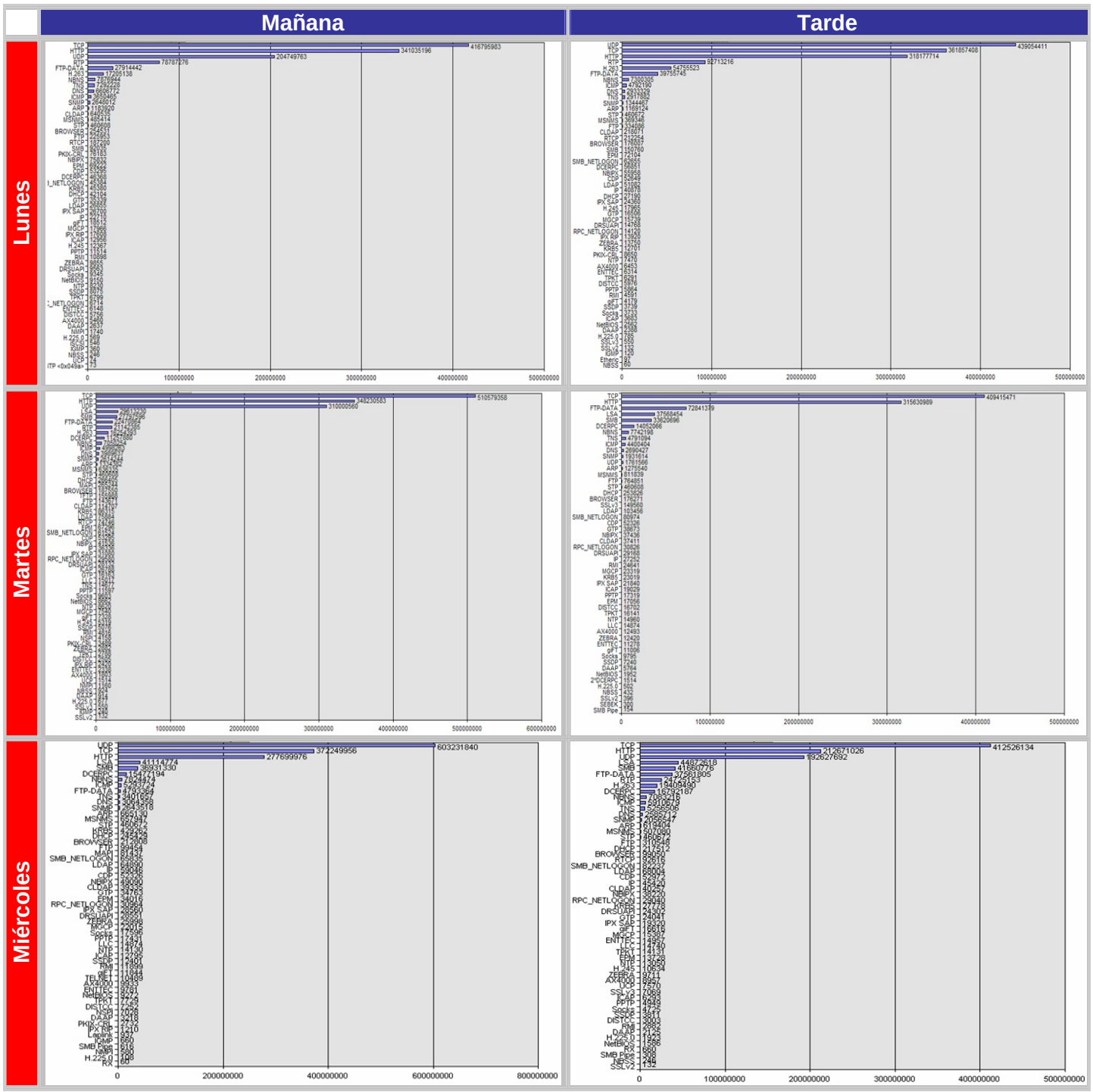


Figura B.2.1.2. Distribución de protocolos por número de paquetes (Porcentajes) Sede Administrativa

B.2.1.3 Distribución de protocolos por bytes (Cantidades) - Sede Administrativa



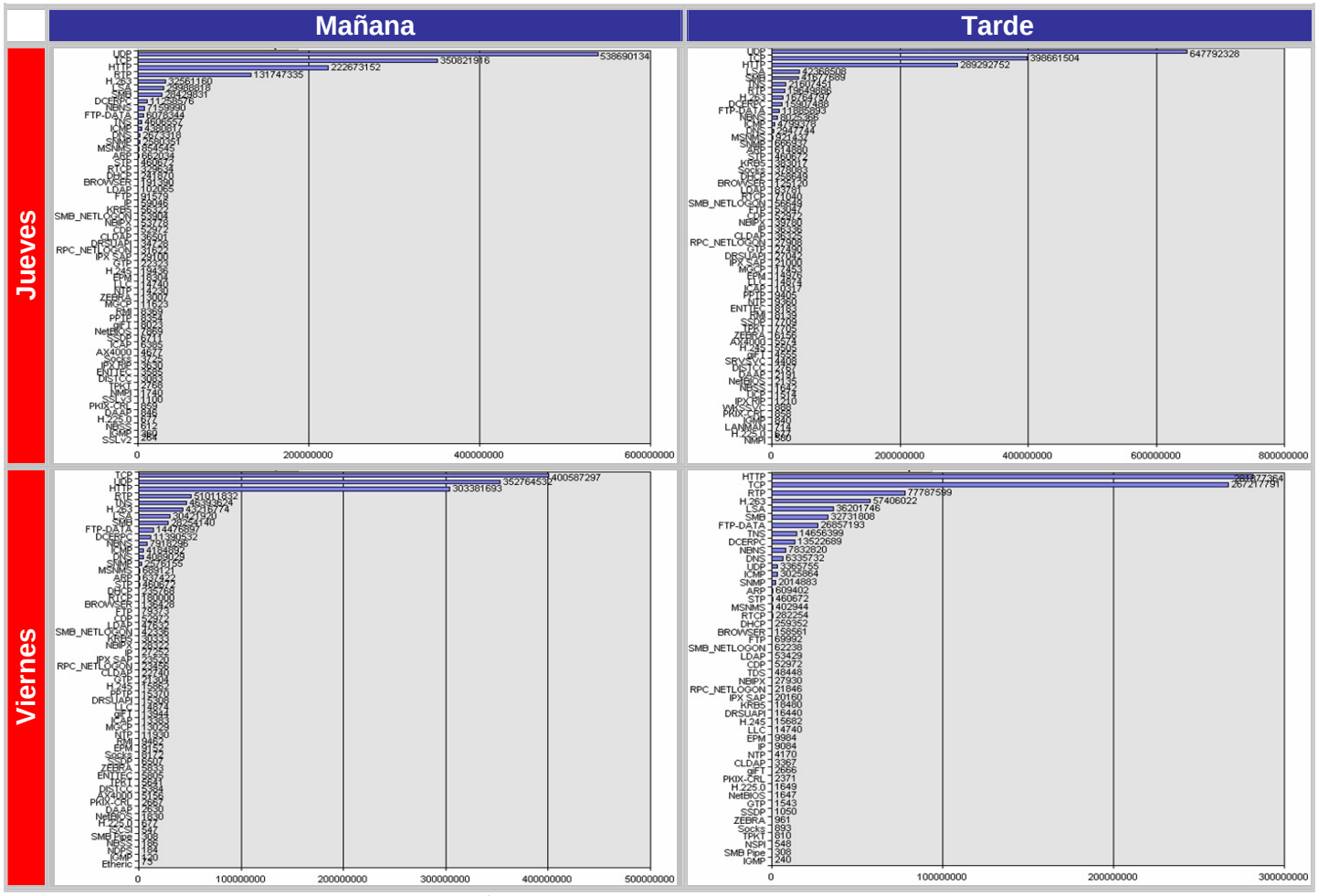


Figura B.2.1.3 Distribución de protocolos por bytes (Cantidades) - Sede Administrativa

B.2.1.4 Distribución de protocolos por bytes (Porcentajes) - Sede Administrativa

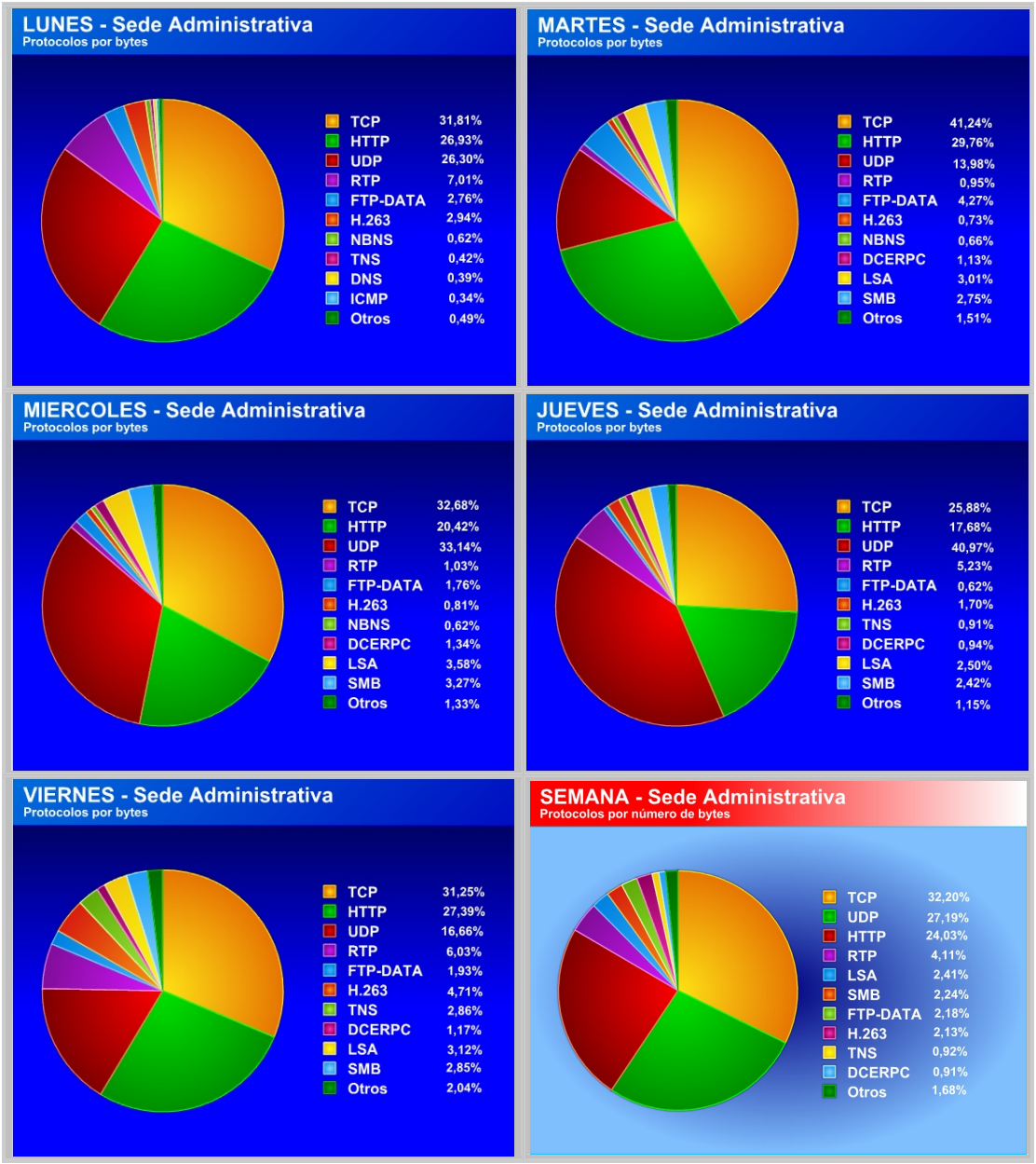
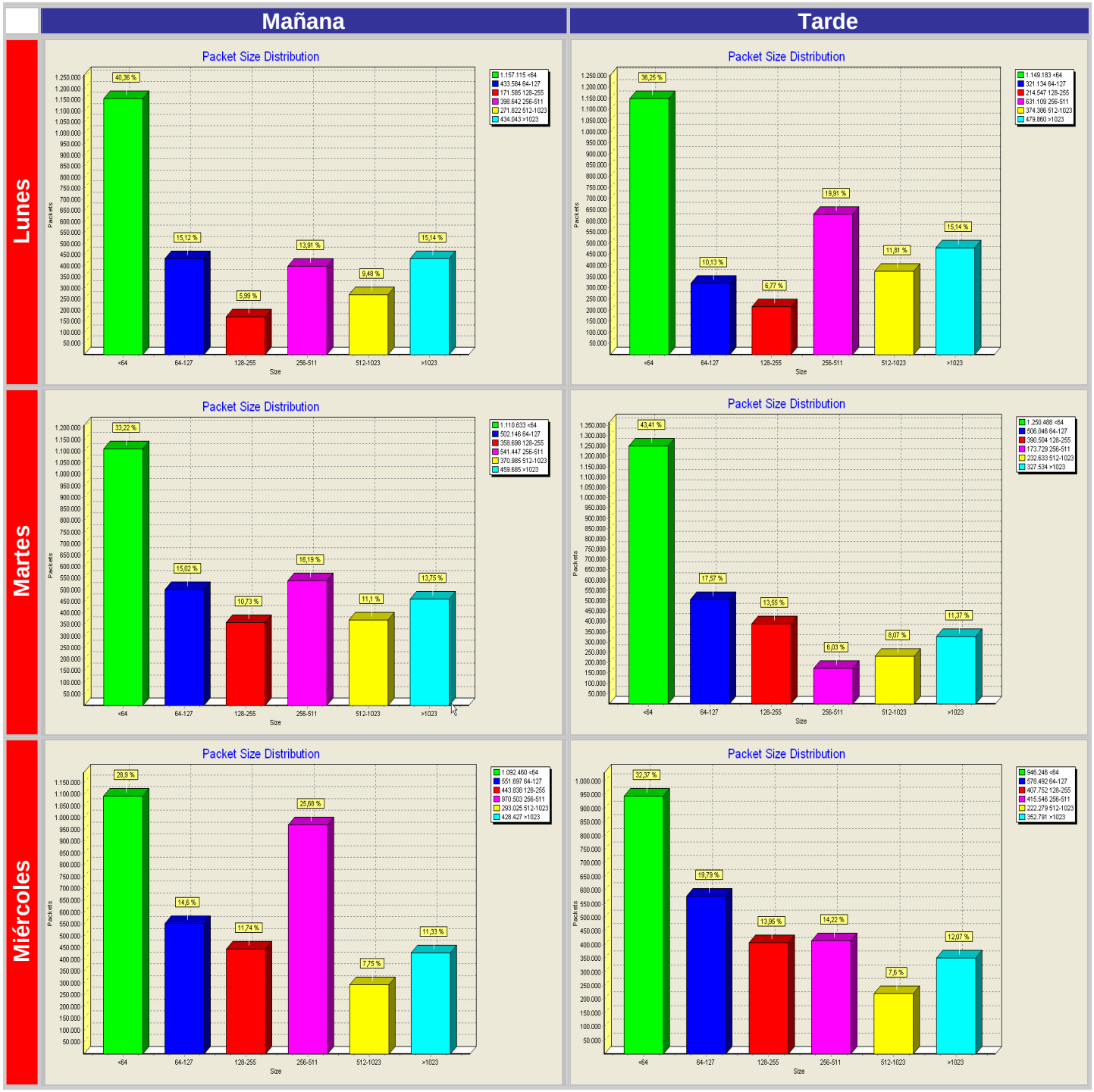


Figura B.2.1.4. Distribución de protocolos por bytes (Porcentajes) - Sede Administrativa

B.2.1.5 Distribución de tamaño de paquetes - Sede Administrativa



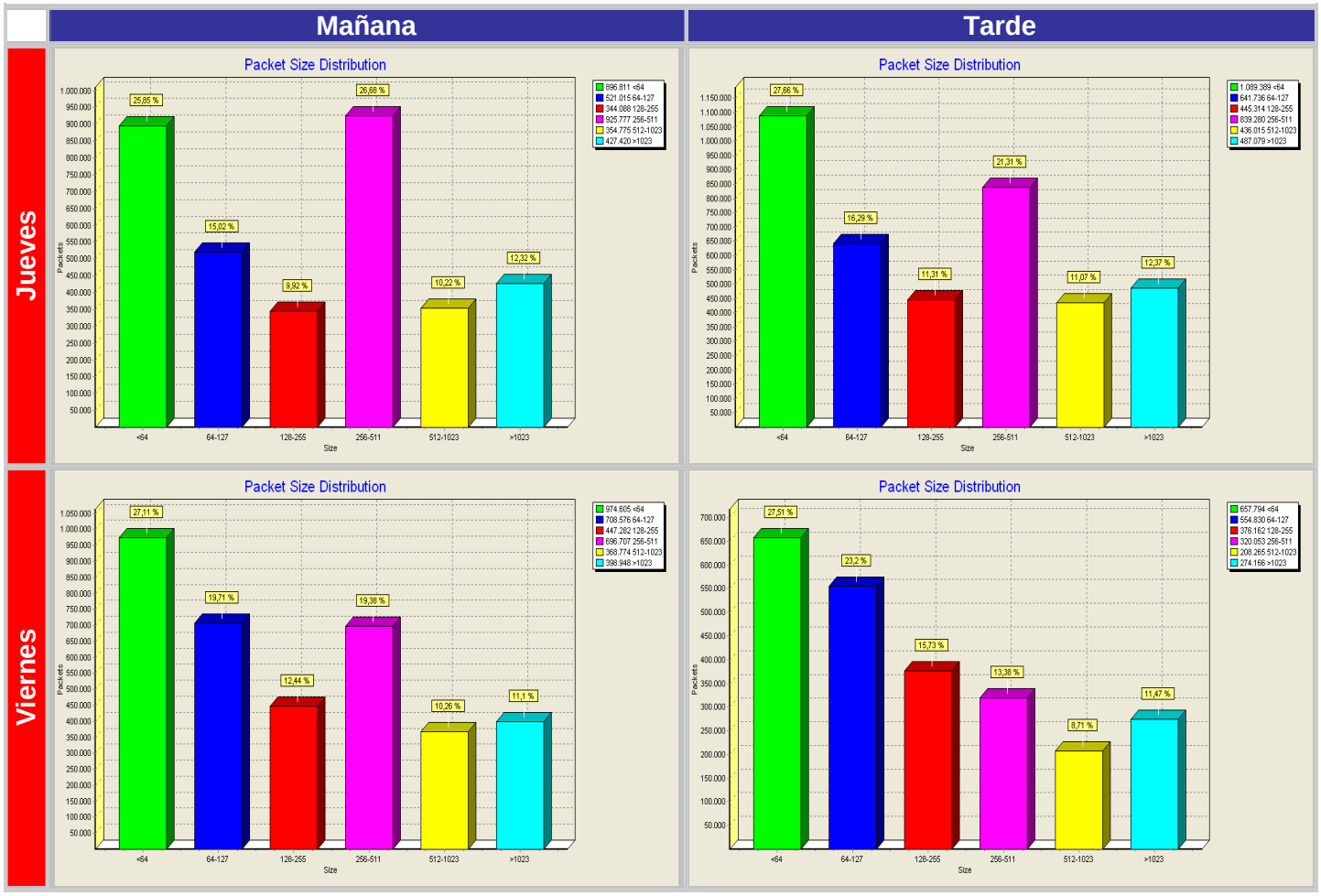
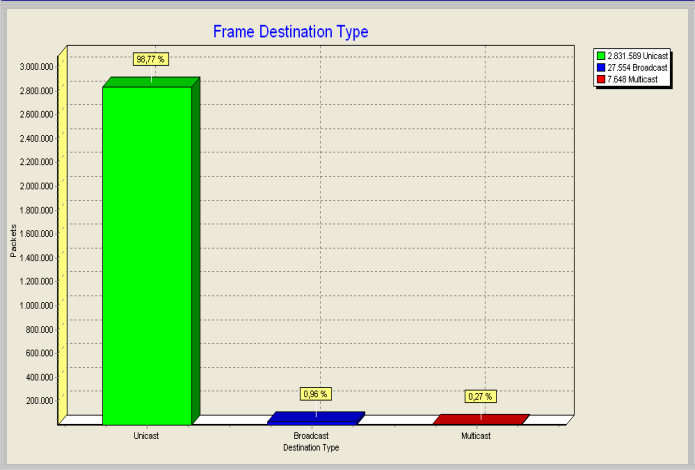
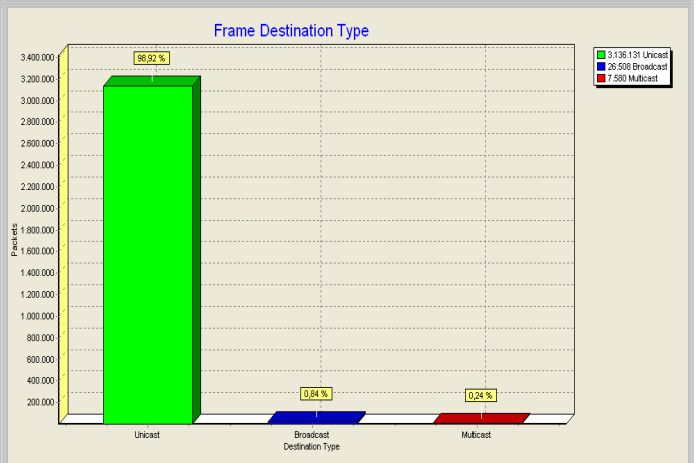
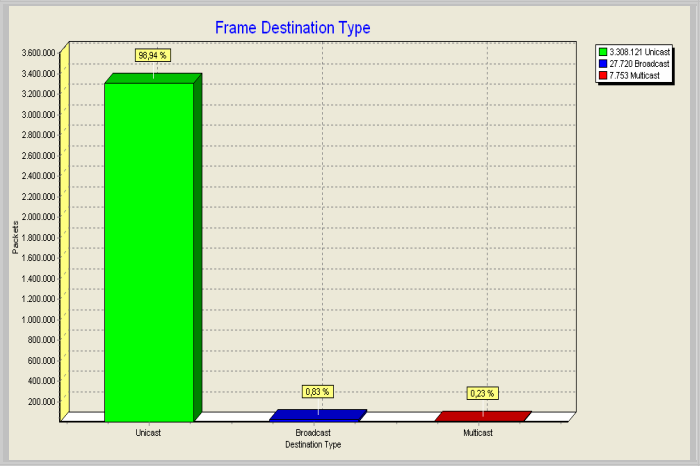
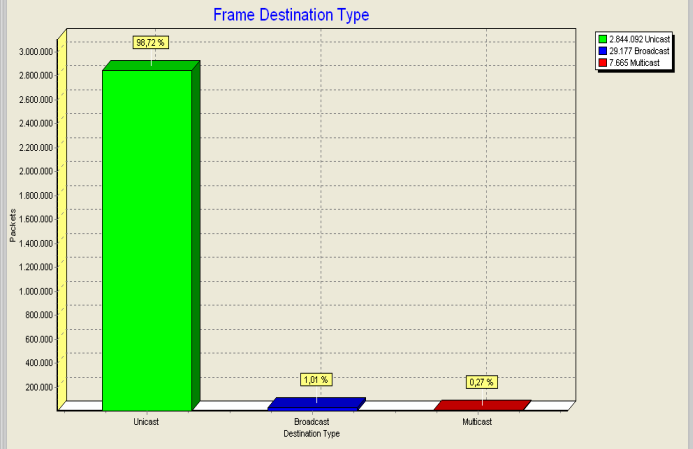
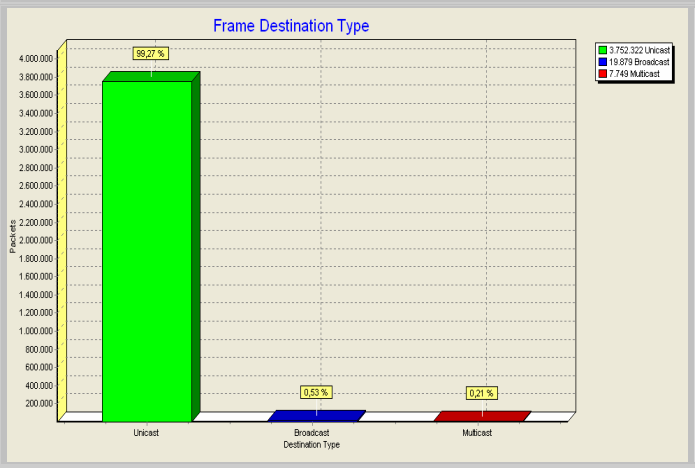
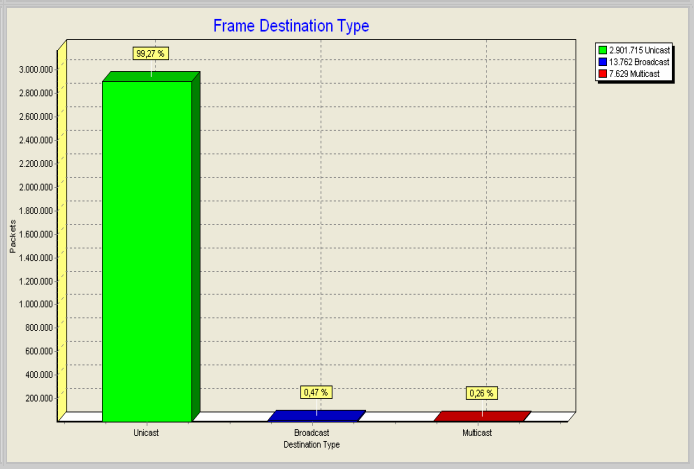


Figura B.2.1.5. Distribución de tamaño de paquetes - Sede Administrativa

B.2.1.6 Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast) - Sede Administrativa

	Mañana	Tarde
Lunes		
Martes		
Miércoles		

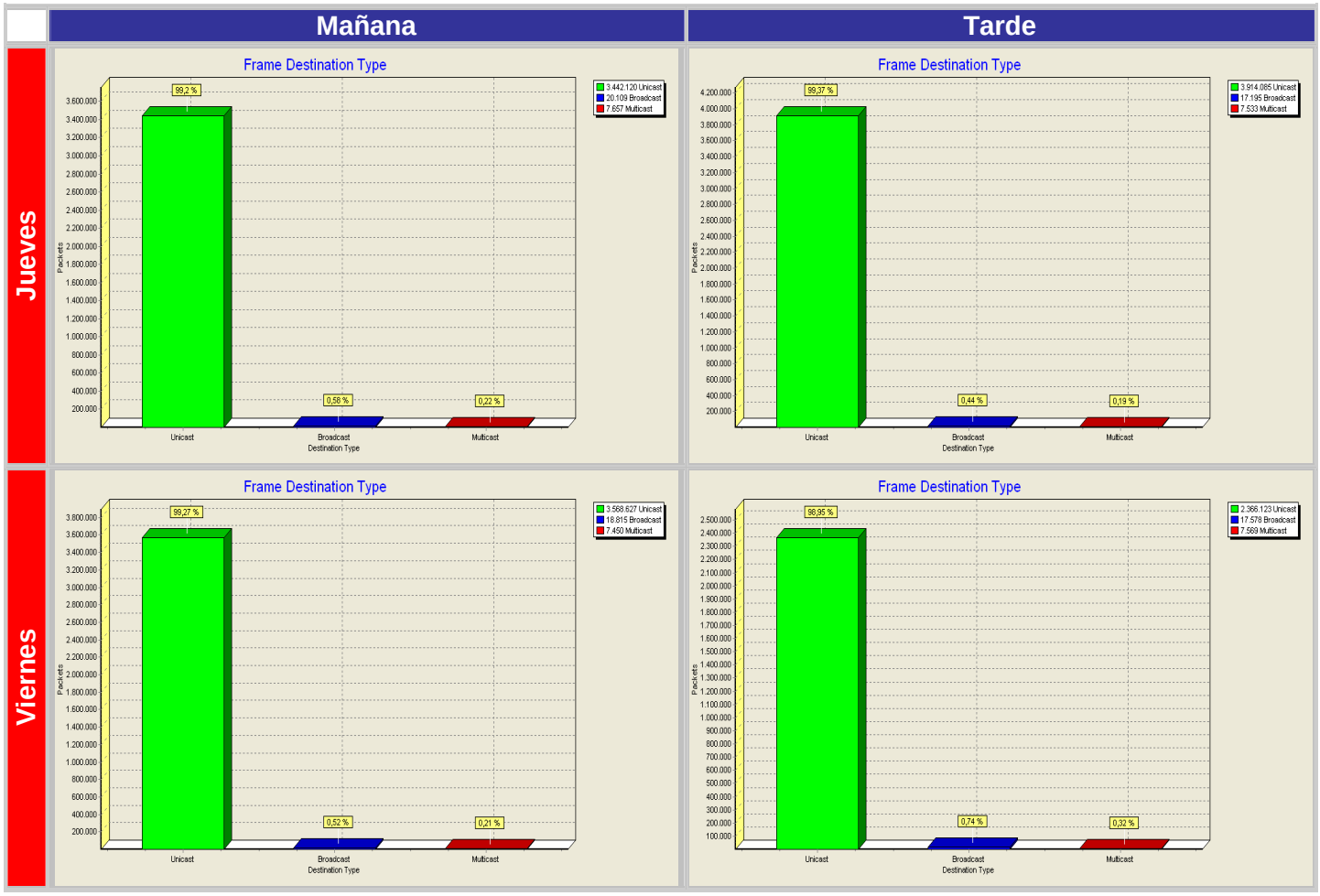
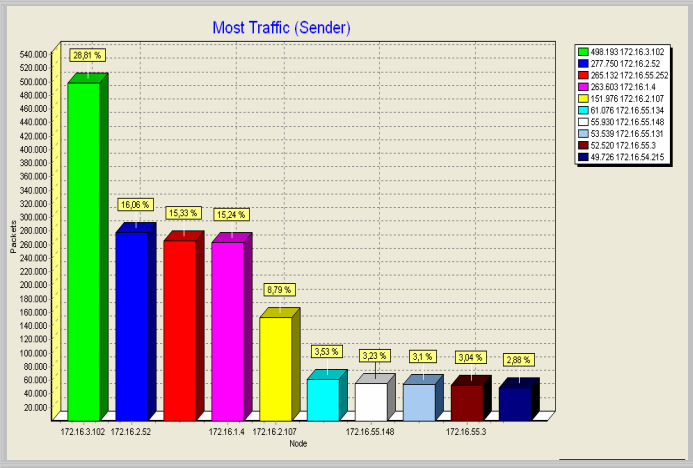
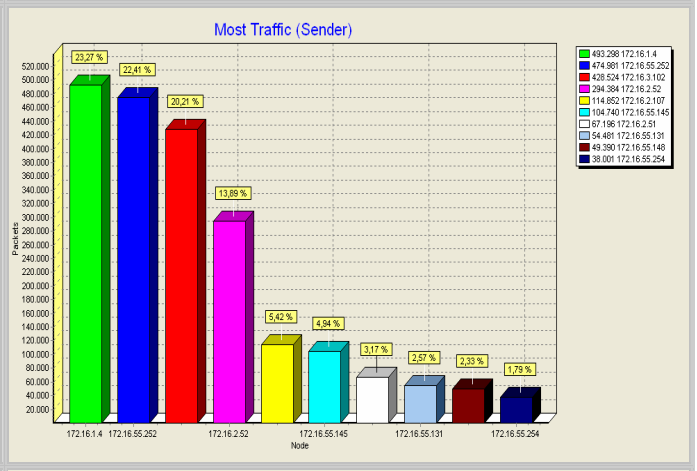
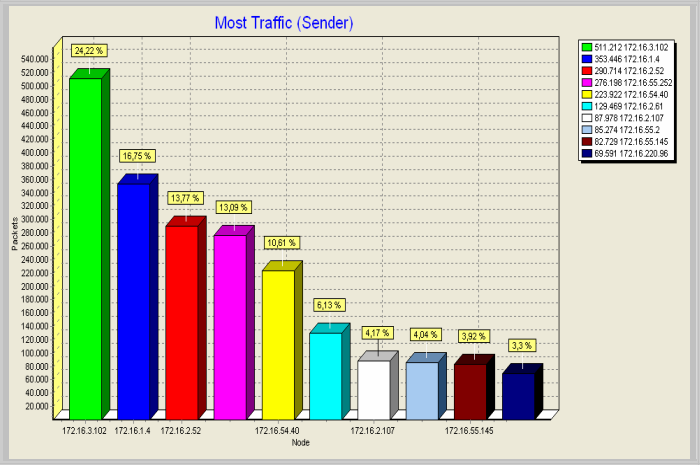
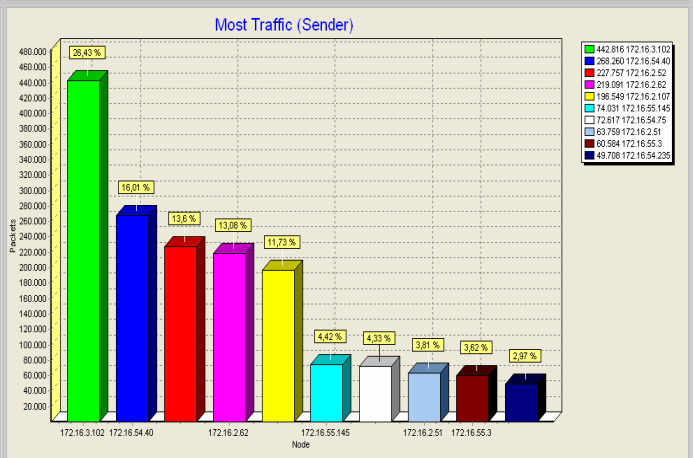
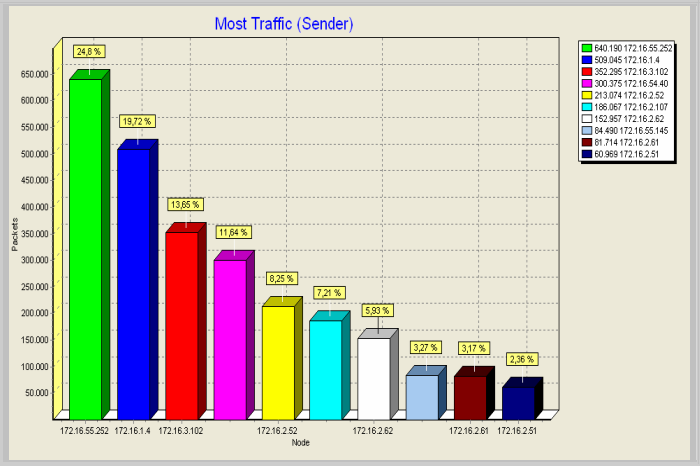
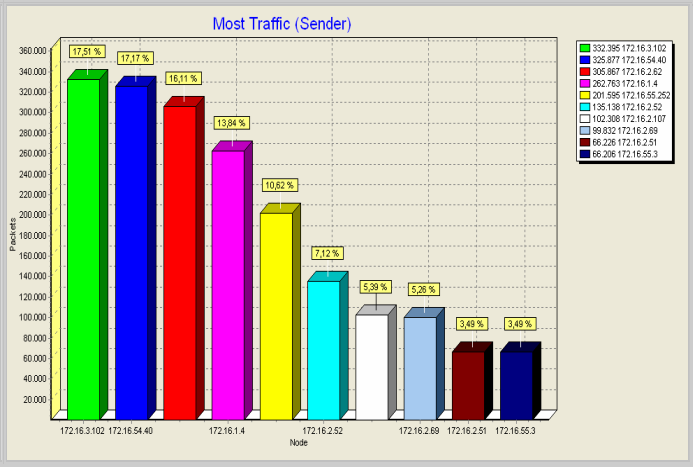


Figura B.2.1.6. Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast) - Sede Administrativa

B.2.1.7 Nodos de mayor tráfico enviado - Sede Administrativa

	Mañana	Tarde
Lunes		
Martes		
Miércoles		

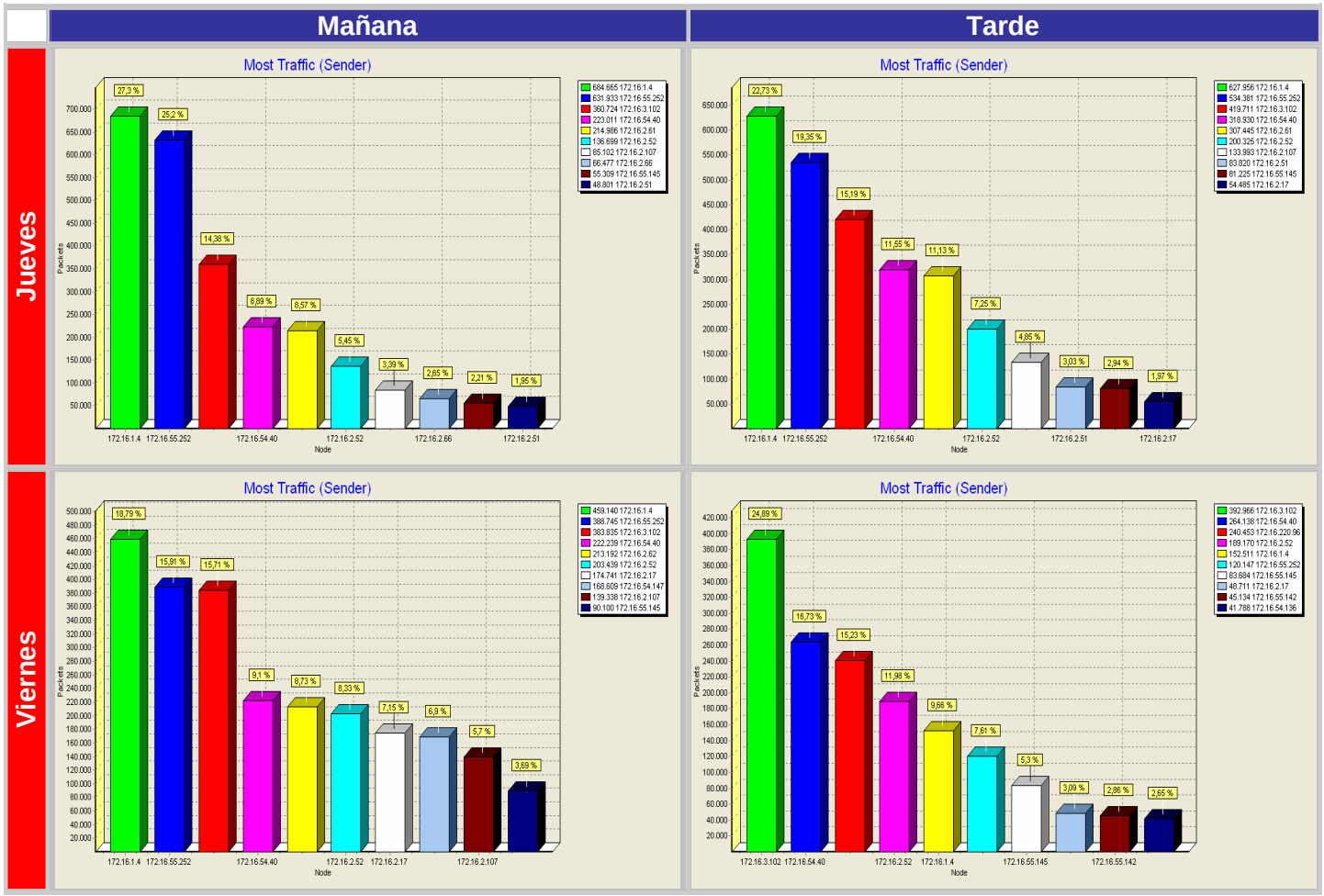
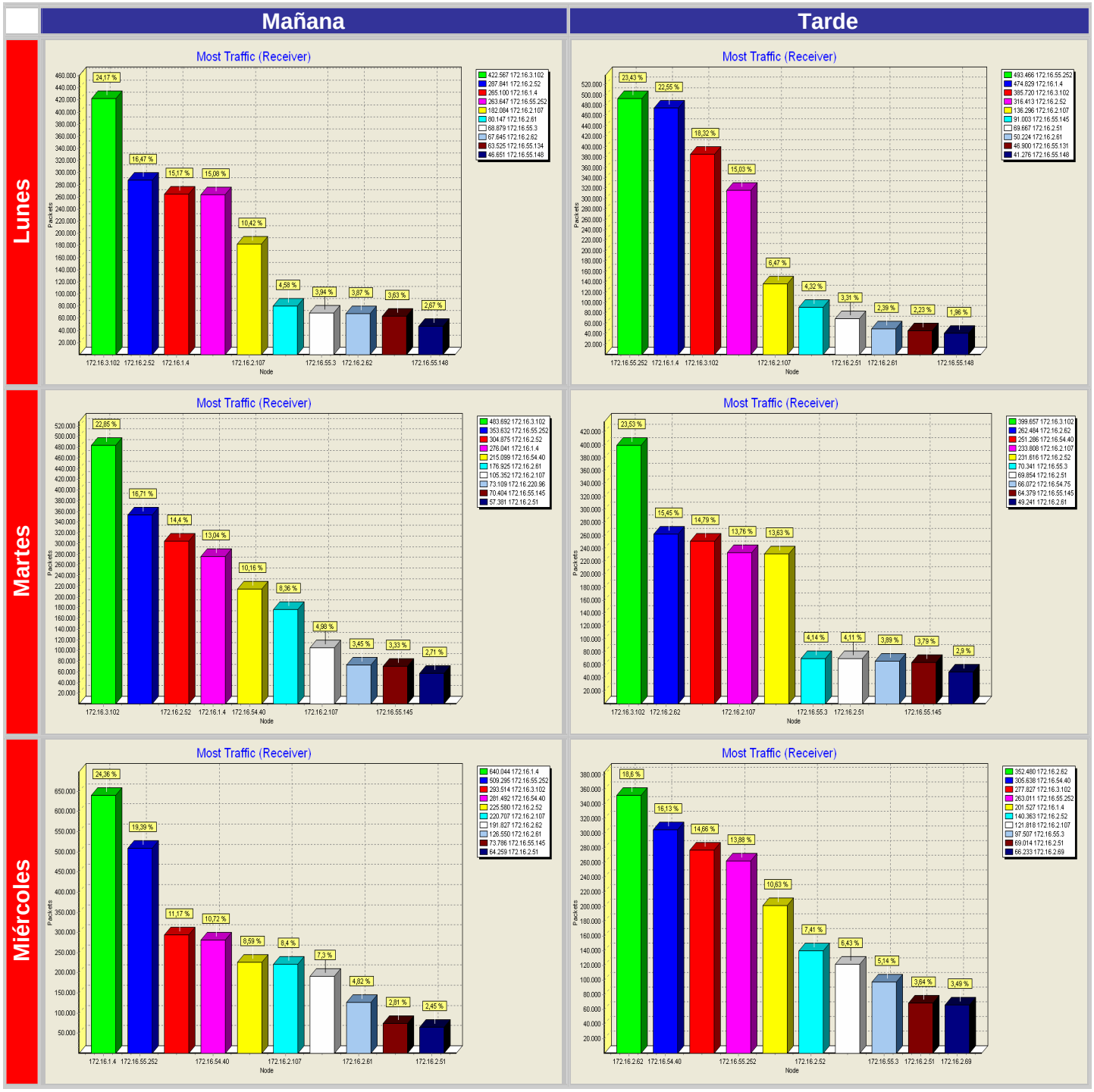


Figura B.2.1.7. Nodos de mayor tráfico enviado - Sede Administrativa

B.2.1.8 Nodos de mayor tráfico recibido - Sede Administrativa



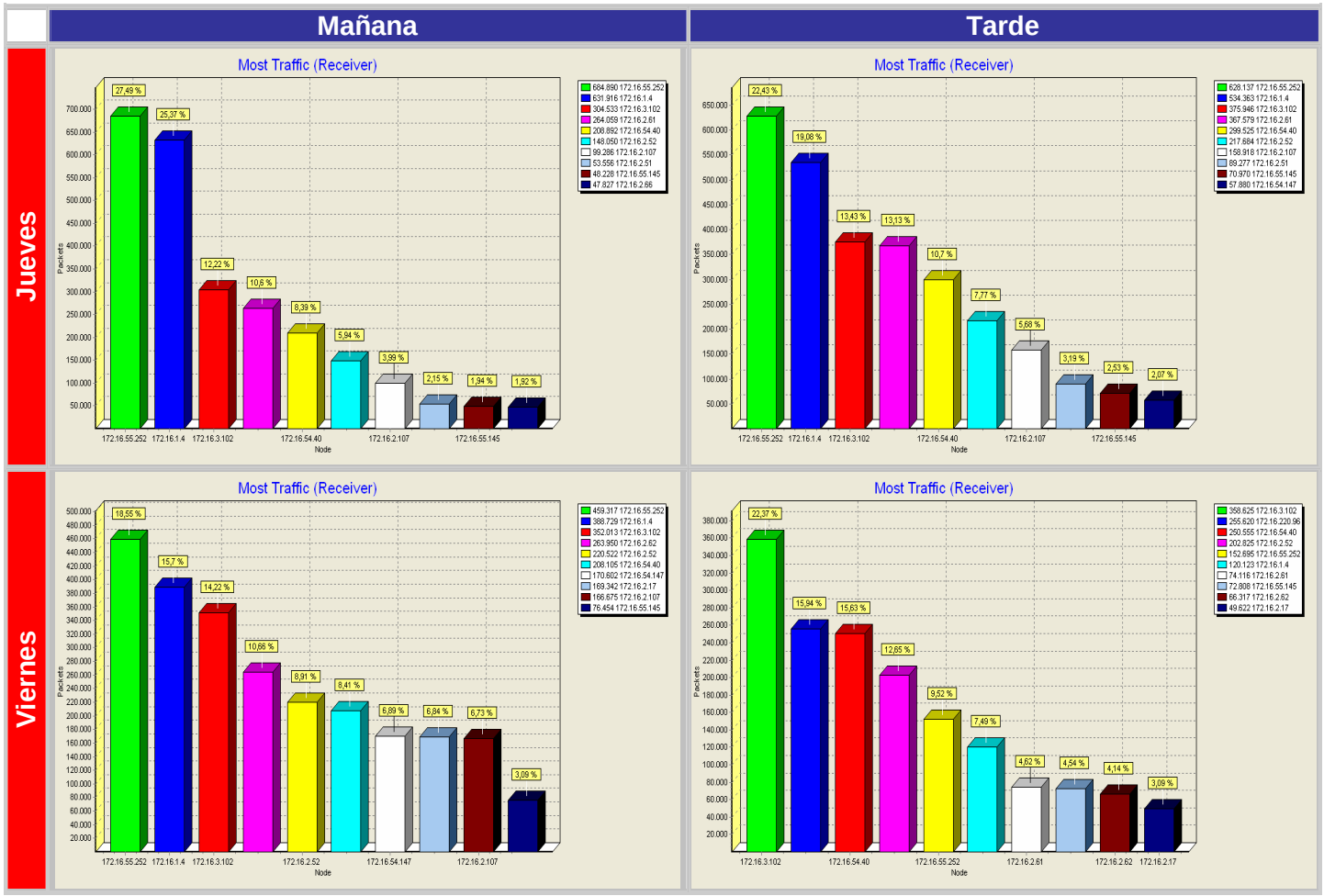


Figura B.2.1.8. Nodos de mayor tráfico recibido - Sede Administrativa

B.2.2 Sede Comercio y Servicios

B.2.2.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Comercio y Servicios

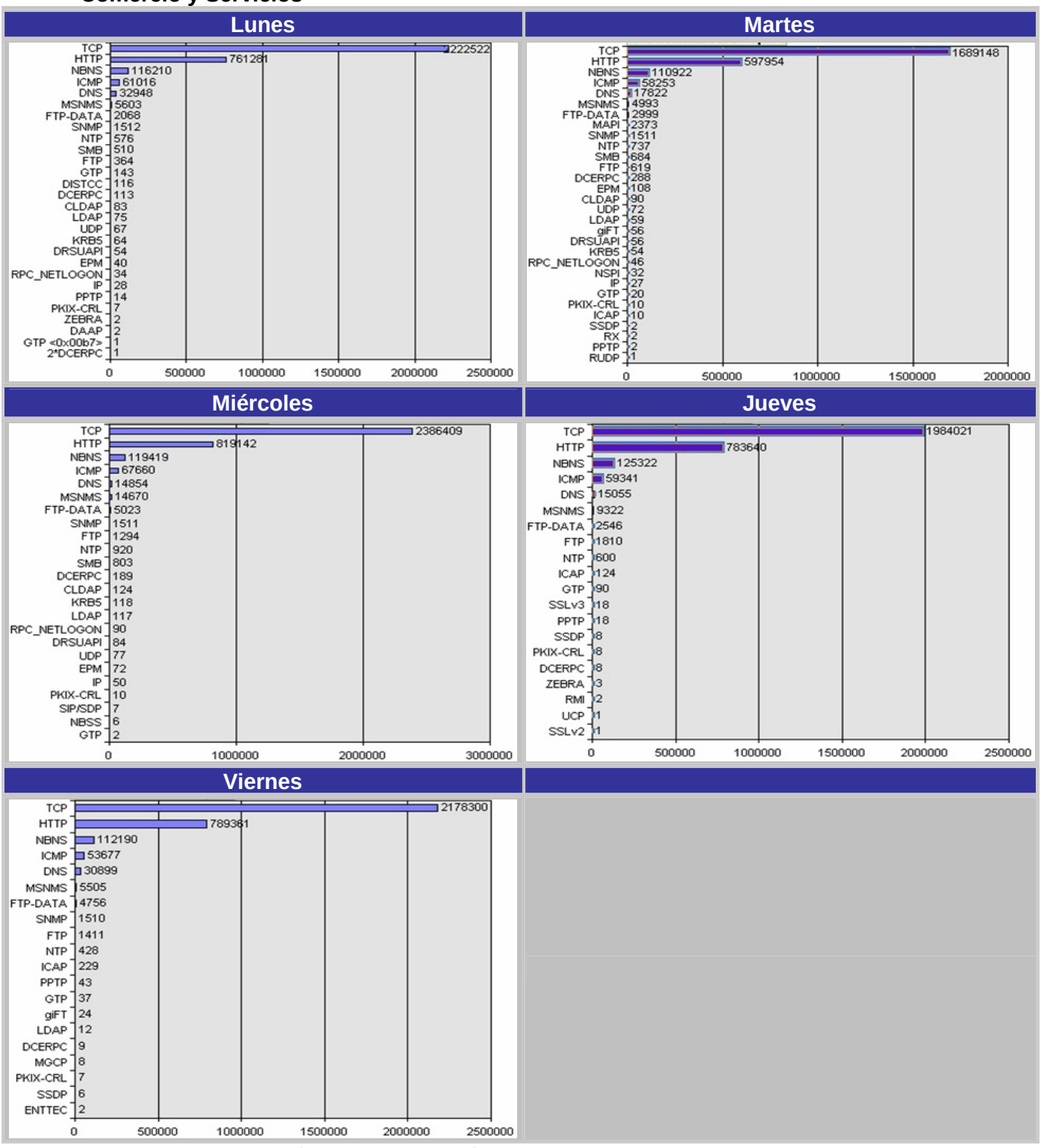


Figura B.2.2.1. Distribución de protocolos por número de paquetes (cantidades) - Sede Comercio y Servicios

B.2.2.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Comercio y Servicios

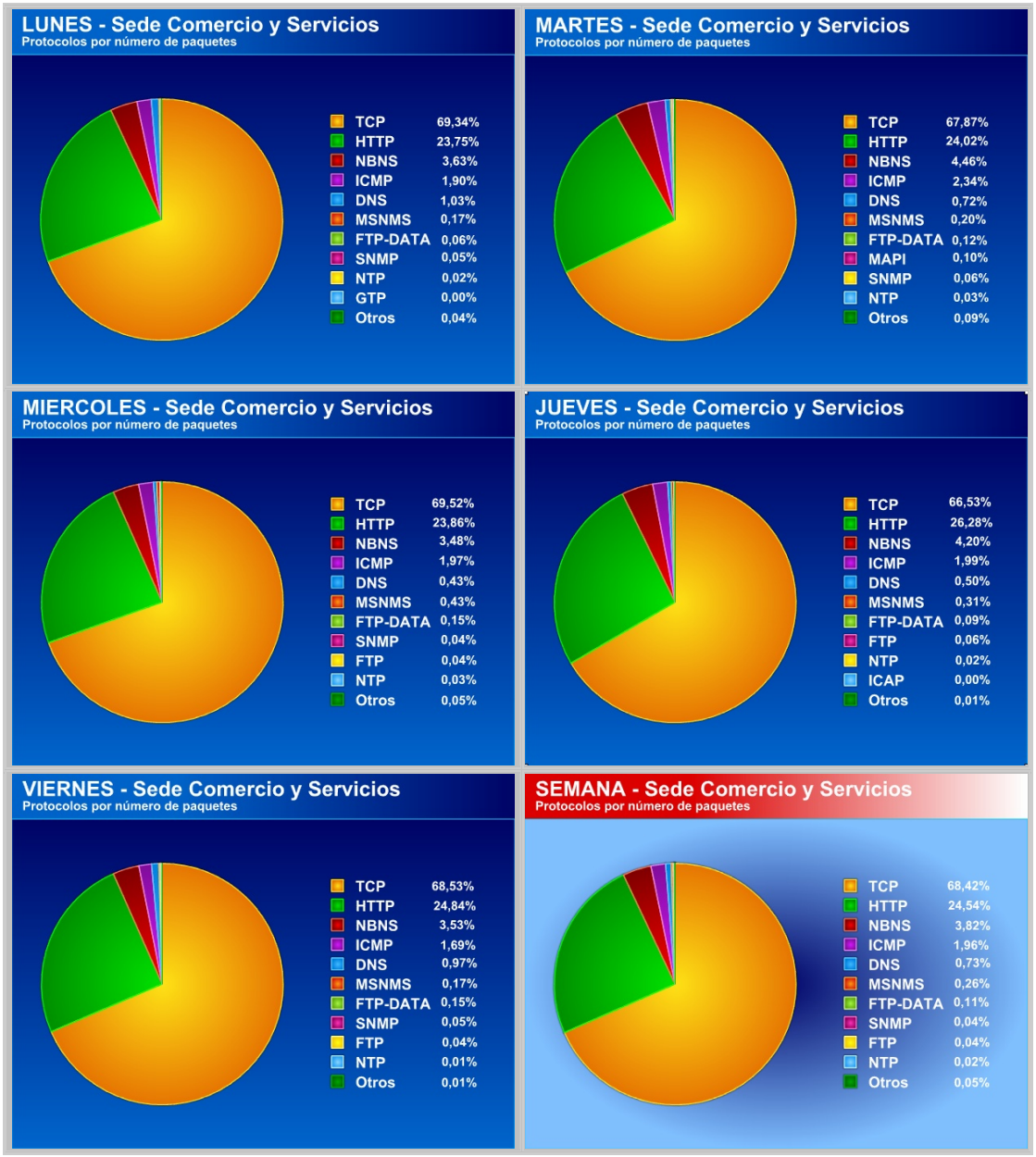


Figura B.2.2.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Comercio y Servicios

B.2.2.3 Distribución de protocolos por bytes (Cantidades) - Sede Comercio y Servicios

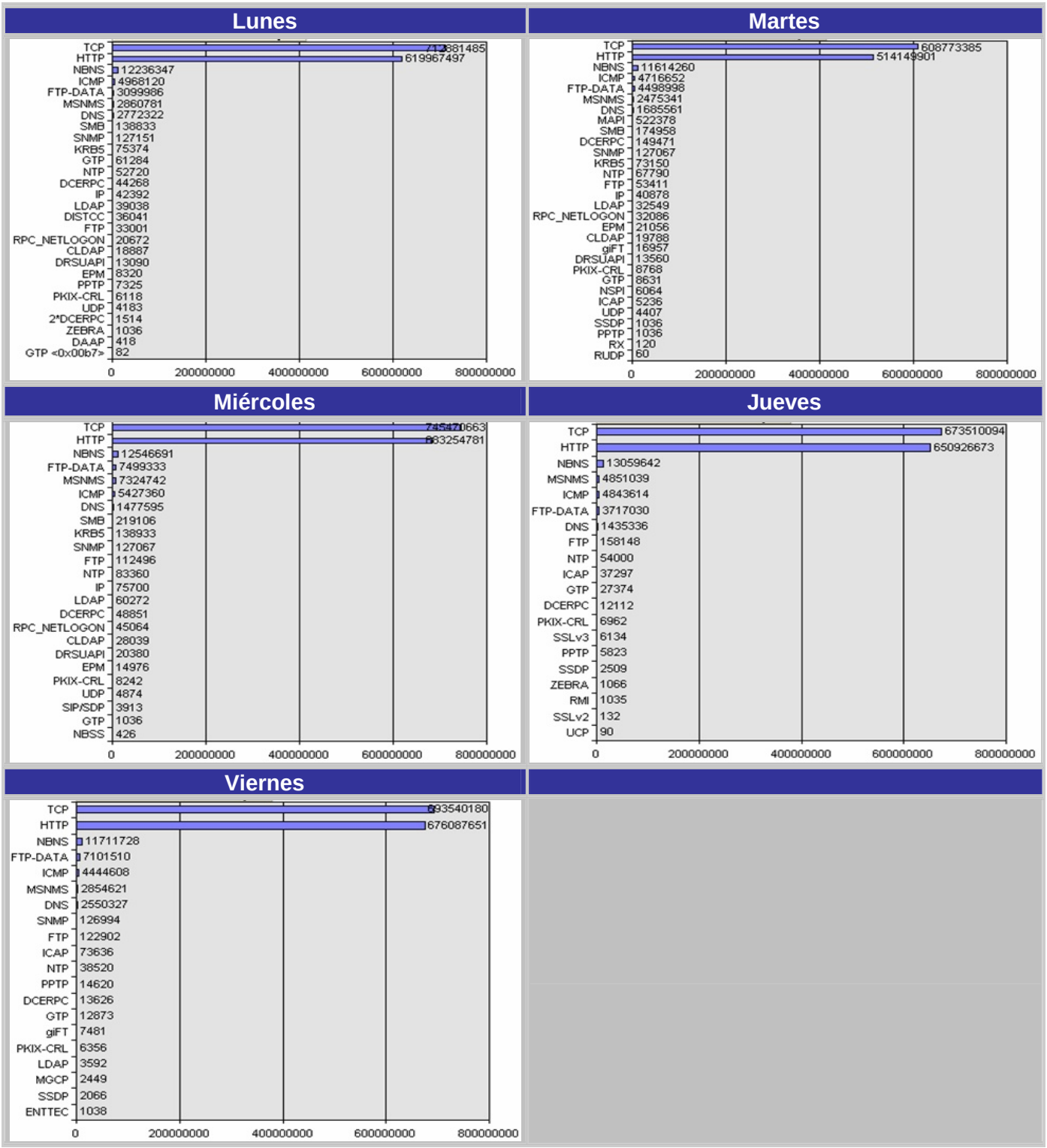


Figura B.2.2.3. Distribución de protocolos por bytes (Cantidades) - Sede Comercio y Servicios

B.2.2.4 Distribución de protocolos por bytes (Porcentajes) - Sede Comercio y Servicios

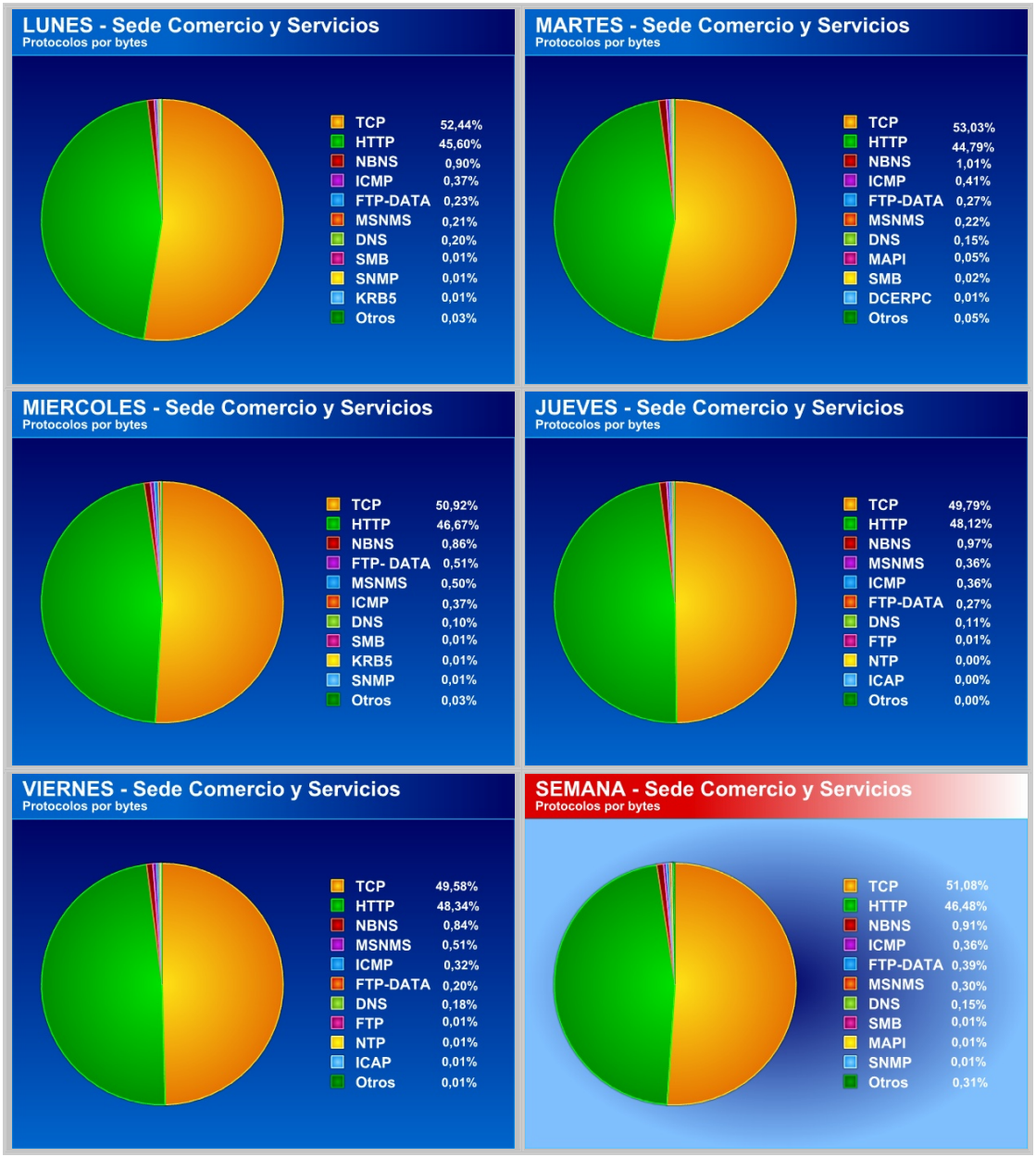


Figura B.2.2.4. Distribución de protocolos por bytes (Porcentajes) - Sede Comercio y Servicios

B.2.2.5 Distribución de tamaño de paquetes - Sede Comercio y Servicios

Figura B.2.2.5. Distribución de tamaño de paquetes - Sede Comercio y Servicios

B.2.2.6 Nodos de mayor tráfico enviado - Sede Comercio y Servicios

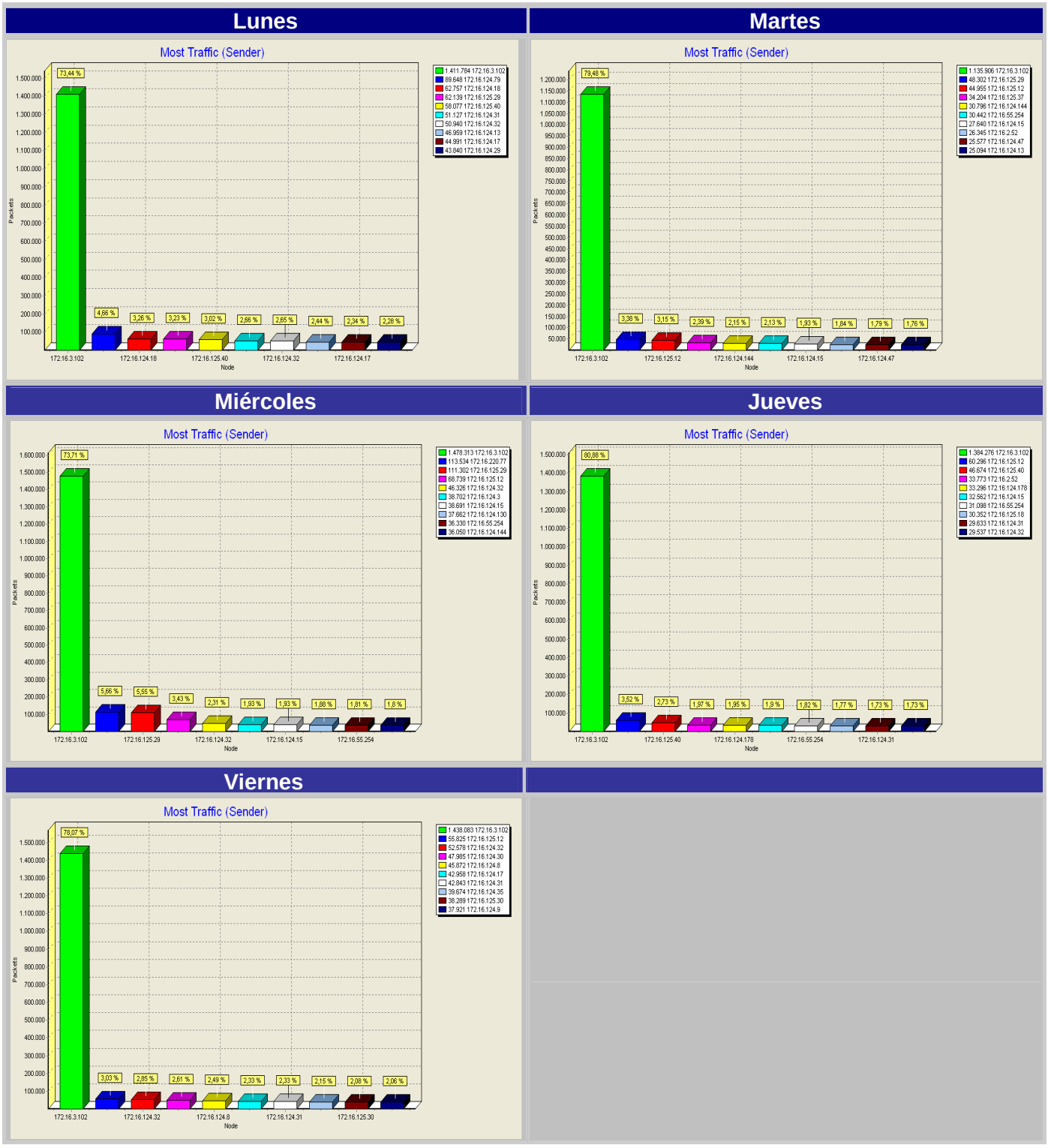


Figura B.2.2.6. Nodos de mayor tráfico enviado - Sede Comercio y Servicios

B.2.2.7 Nodos de mayor tráfico recibido - Sede Comercio y Servicios

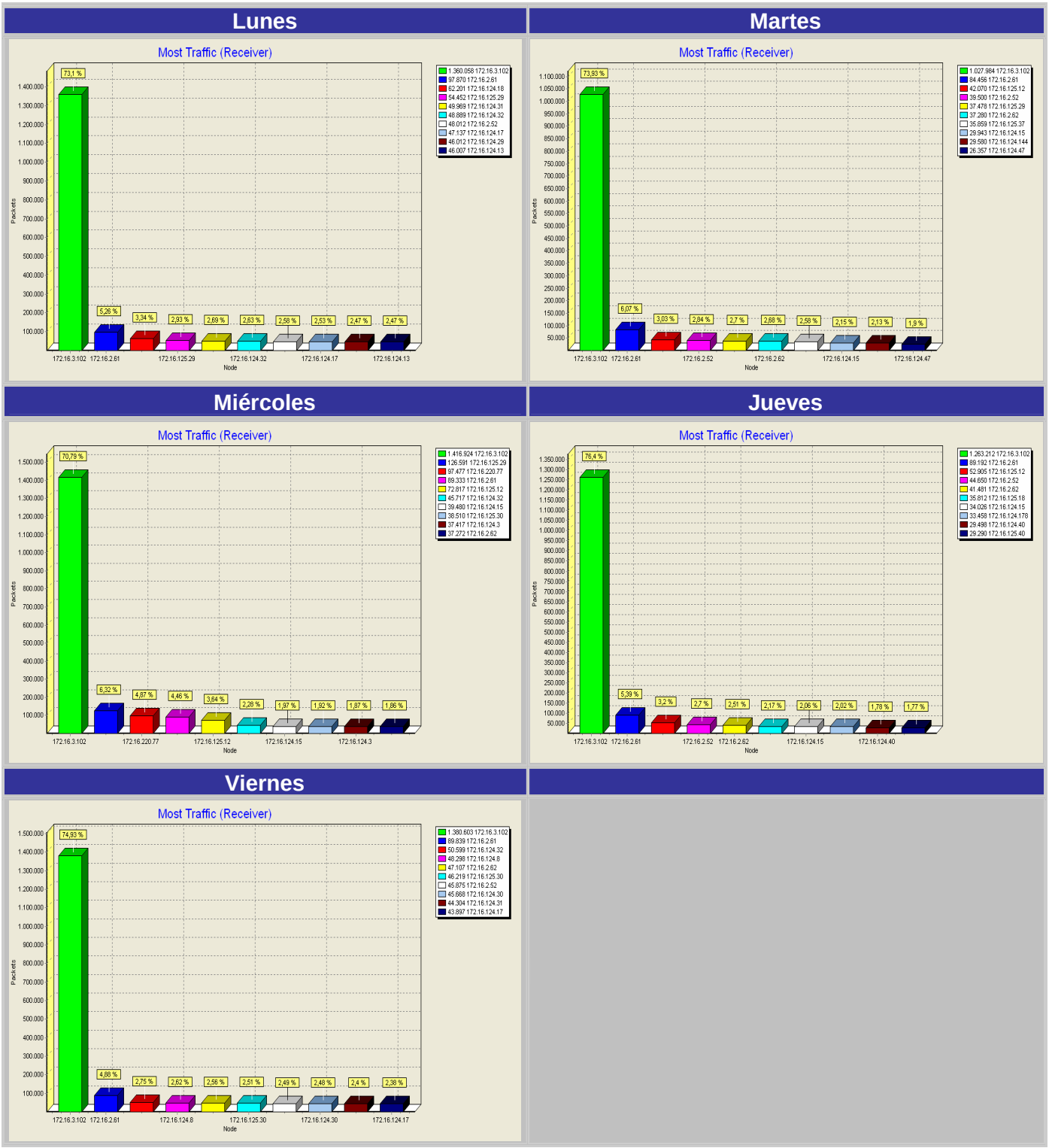


Figura B.2.2.7. Nodos de mayor tráfico recibido - Sede Comercio y Servicios

B.2.3 Sede Floridablanca

B.2.3.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Floridablanca

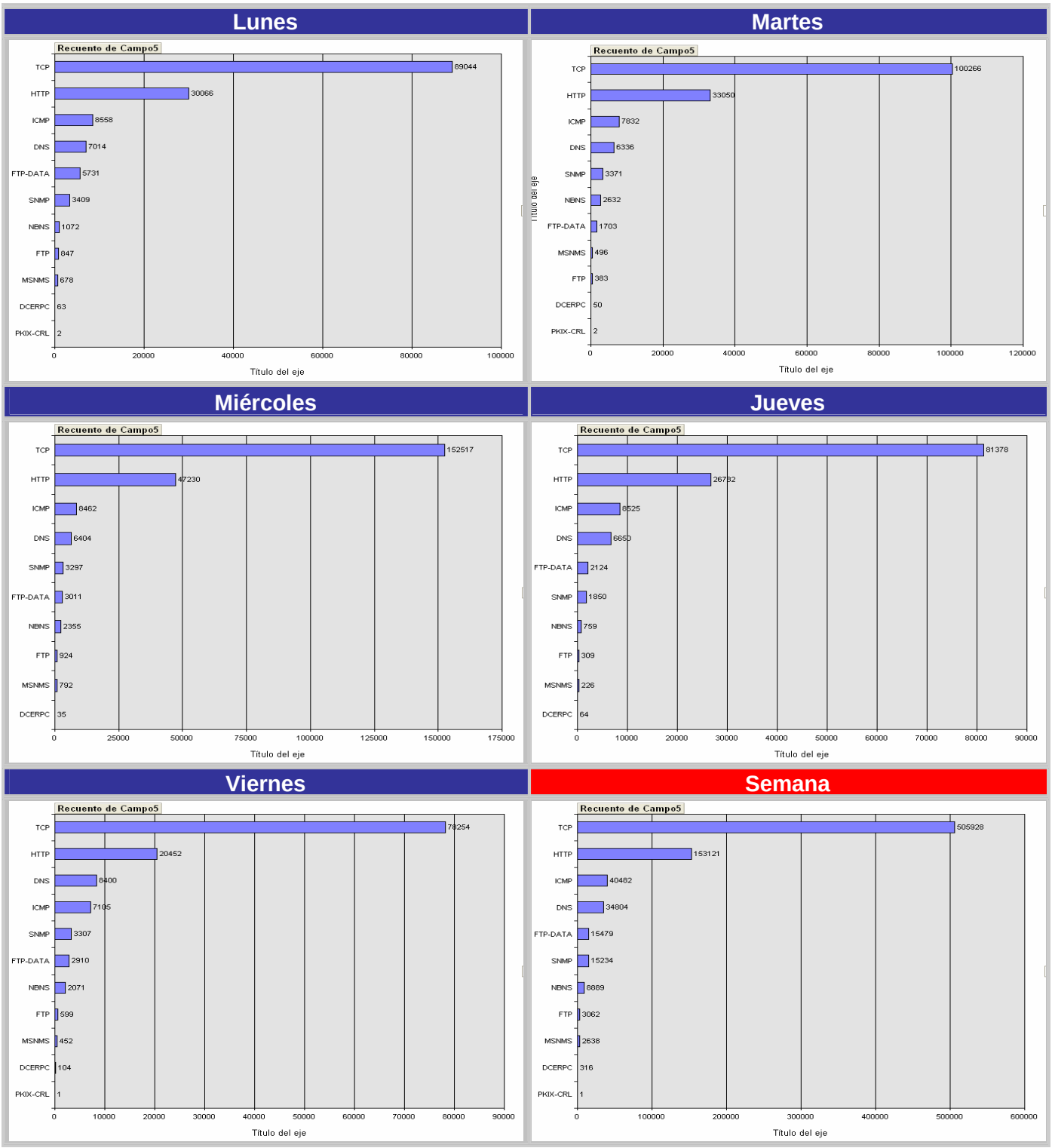


Figura B.2.3.1. Distribución de protocolos por número de paquetes (Cantidades) - Sede Floridablanca

B.2.3.2 Distribución de protocolos por número de paquetes (Porcentajes) - Sede Floridablanca

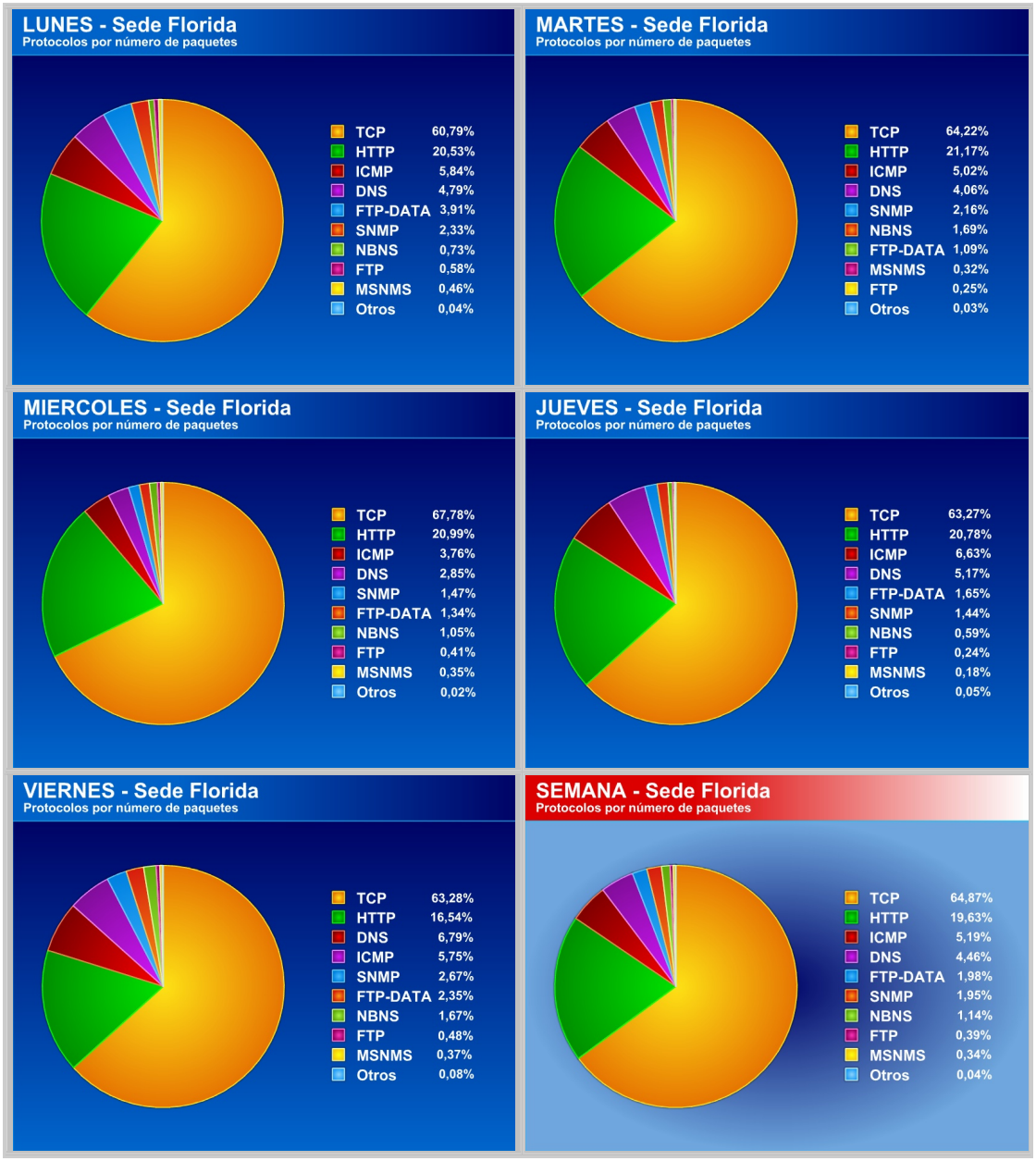


Figura B.2.3.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Floridablanca

B.2.3.3 Distribución de protocolos por bytes (Cantidades) - Sede Floridablanca

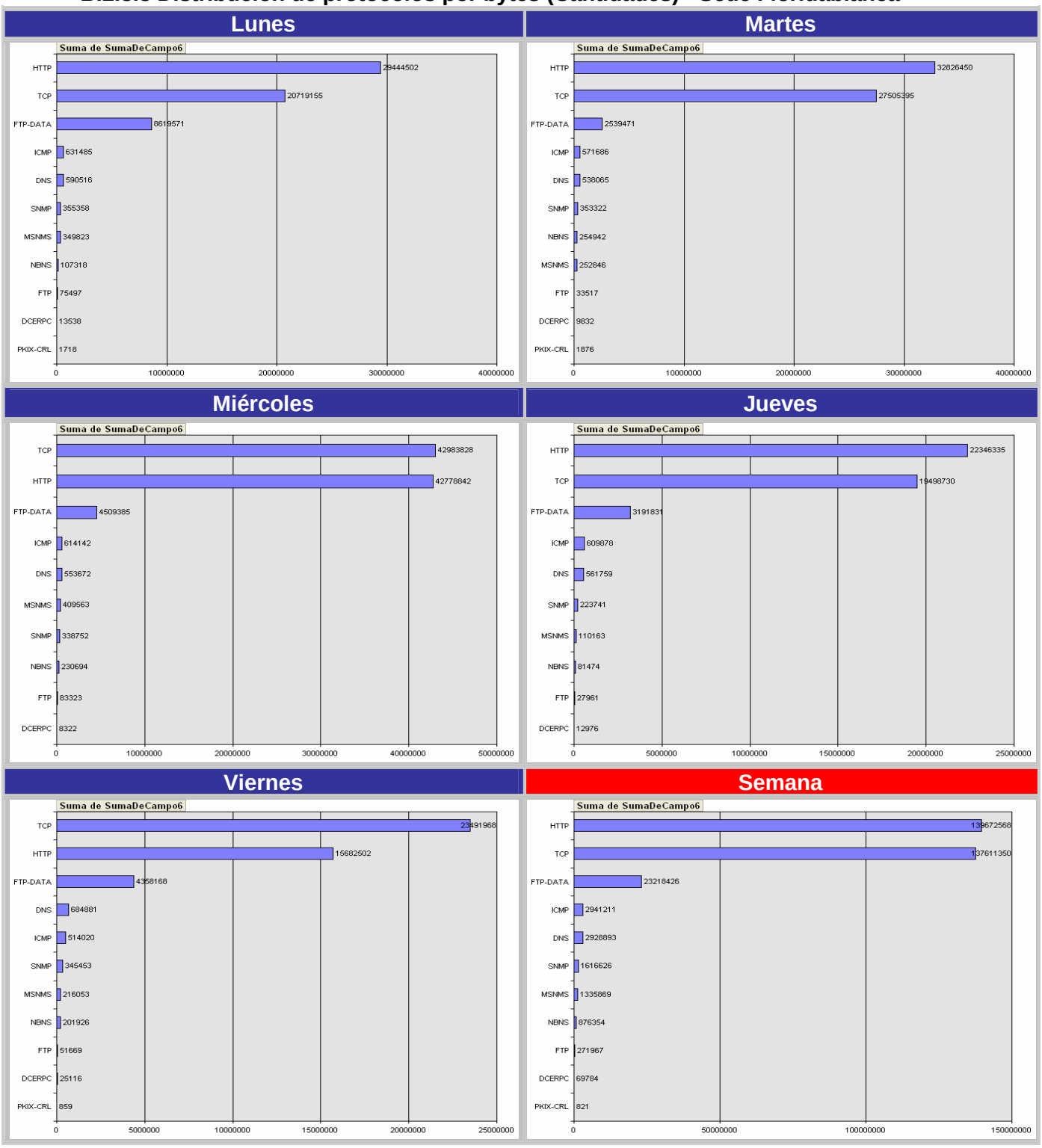


Figura B.2.3.3. Distribución de protocolos por bytes (Cantidades) - Sede Floridablanca

B.2.3.4 Distribución de protocolos por bytes (Porcentajes) - Sede Floridablanca

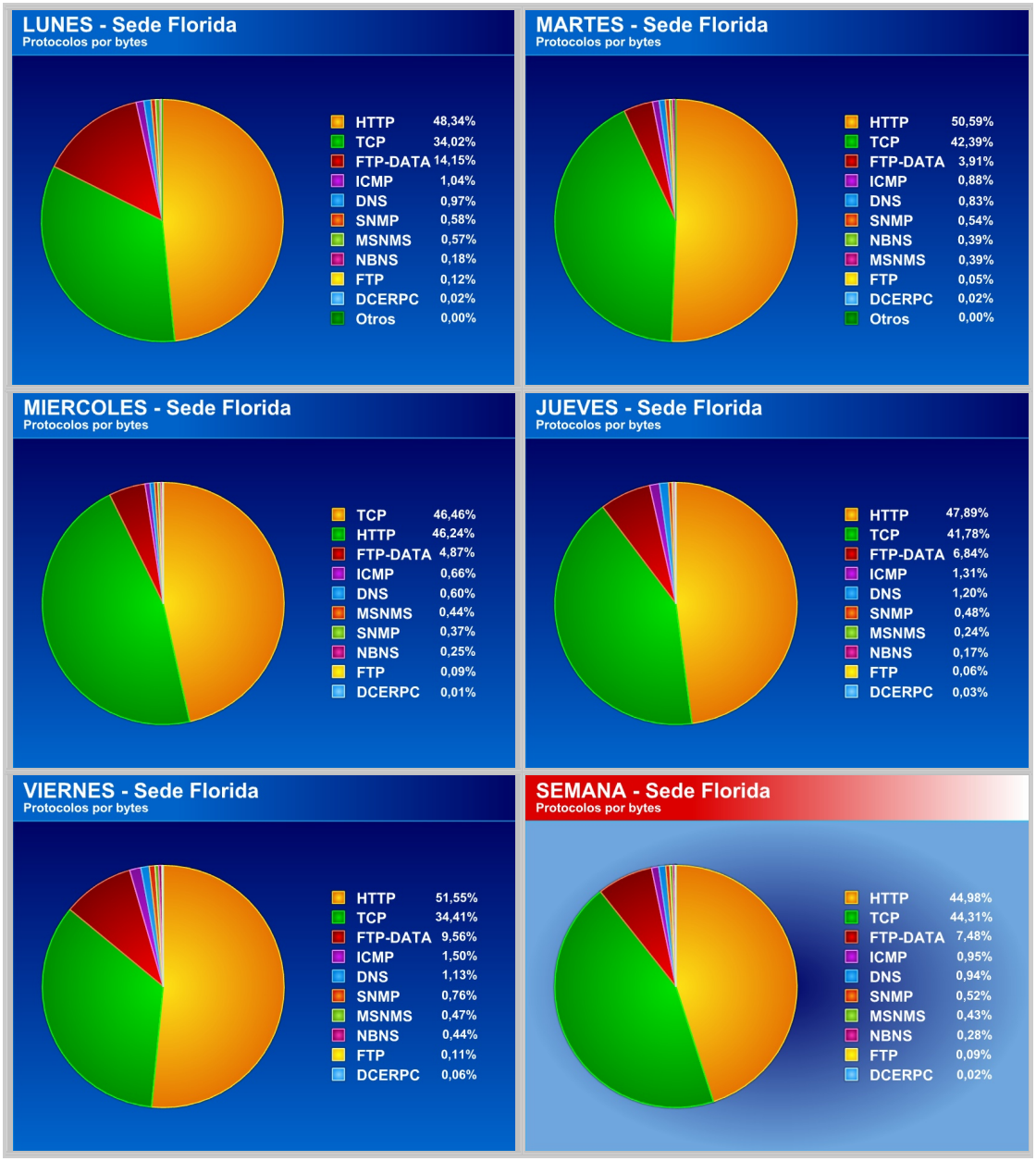


Figura B.2.3.4. Distribución de protocolos por bytes (Porcentajes) - Sede Floridablanca

B.2.3.5 Distribución de tamaño de paquetes -Sede Floridablanca

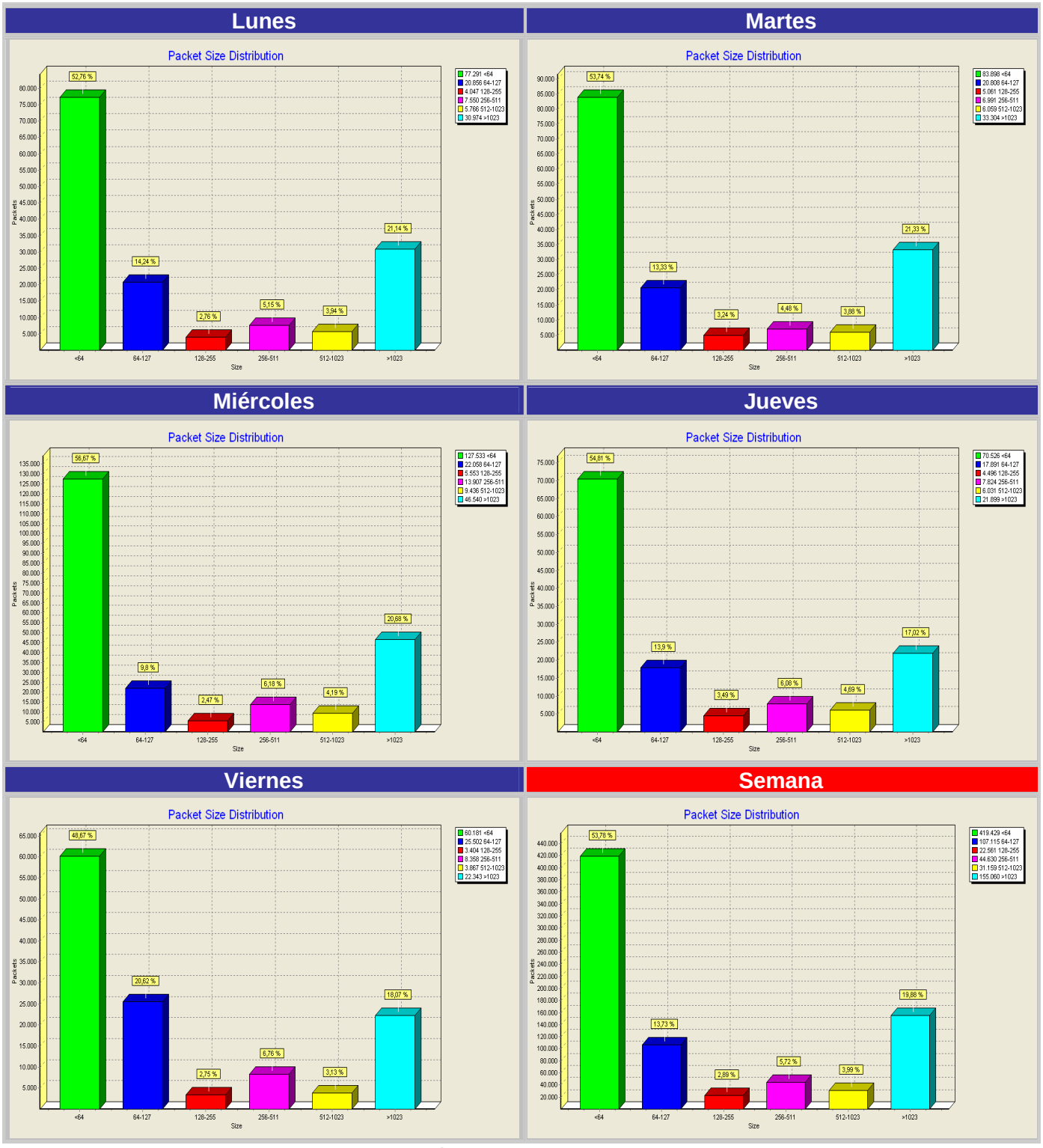


Figura B.2.3.5. Distribución de tamaño de paquetes -Sede Floridablanca

B.2.3.6 Nodos de mayor tráfico enviado - Sede Floridablanca

Figura B.2.3.6. Nodos de mayor tráfico enviado - Sede Floridablanca

B.2.3.7 Nodos de mayor tráfico recibido - Sede Floridablanca

Figura B.2.3.7. Nodos de mayor tráfico recibido - Sede Floridablanca

B.2.4 Sede Girón

B.2.4.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Girón

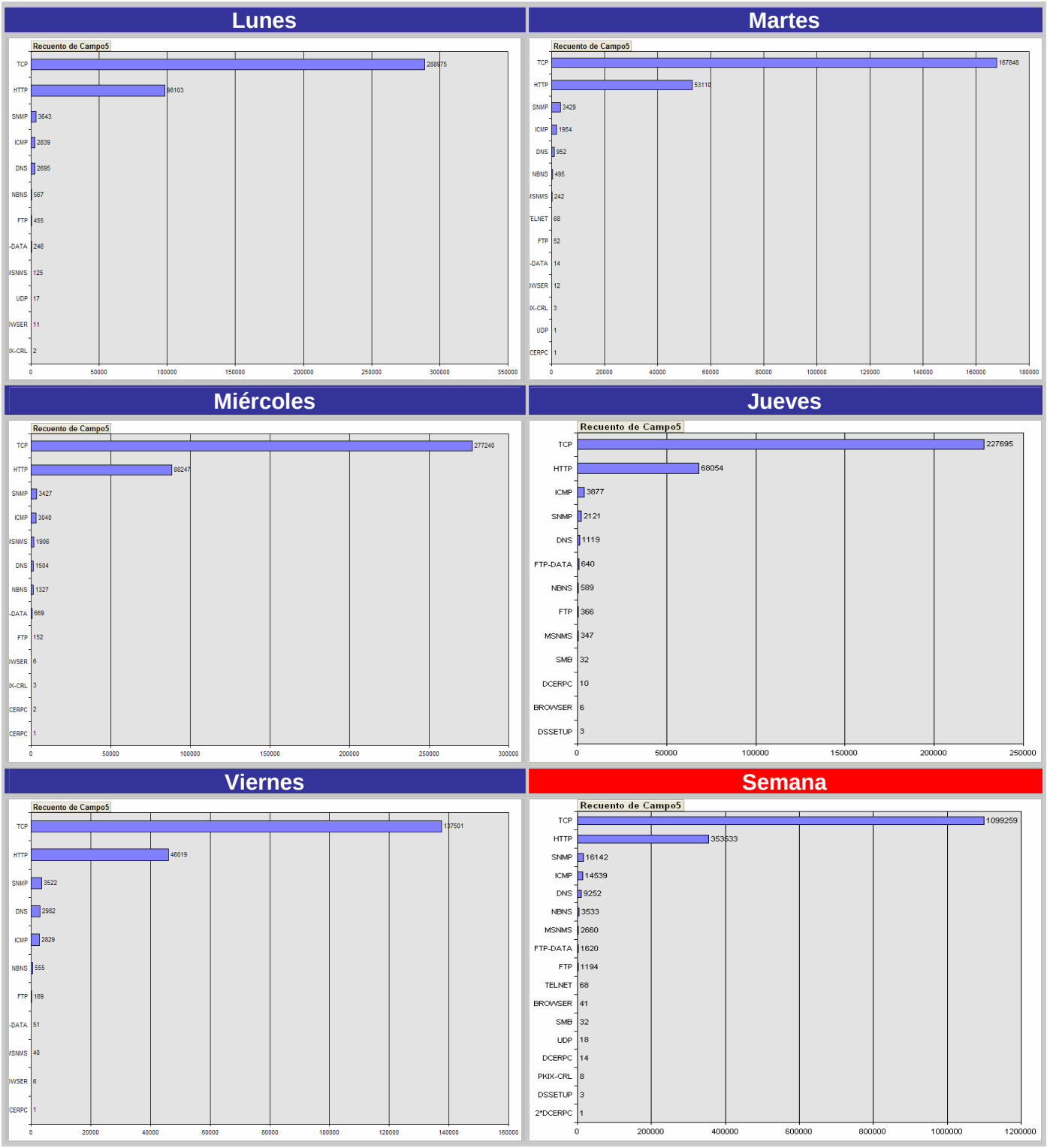


Figura B.2.4.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Girón

B.2.4.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Girón

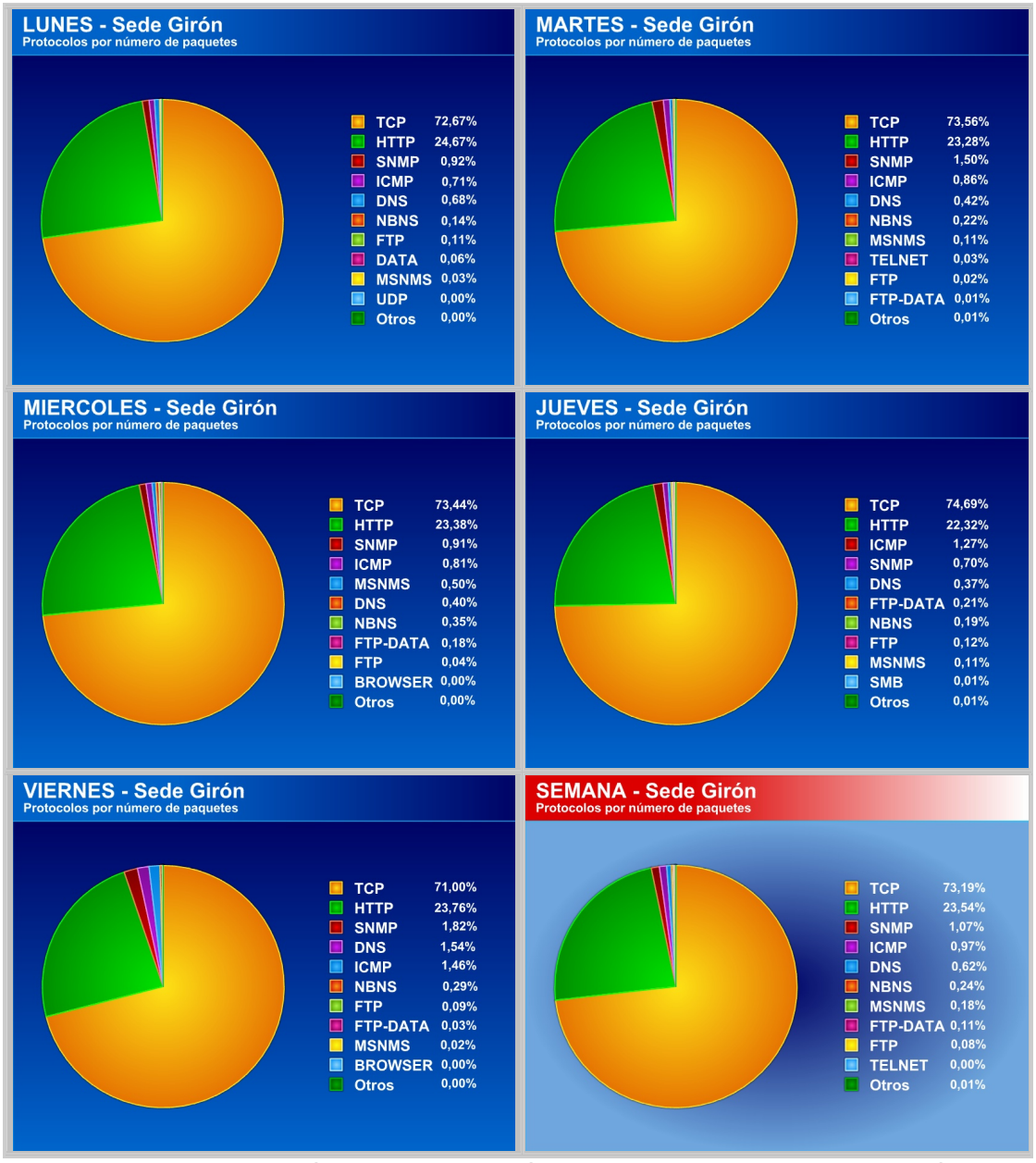


Figura B.2.4.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Girón

B.2.4.3 Distribución de protocolos por bytes (Cantidades) - Sede Girón

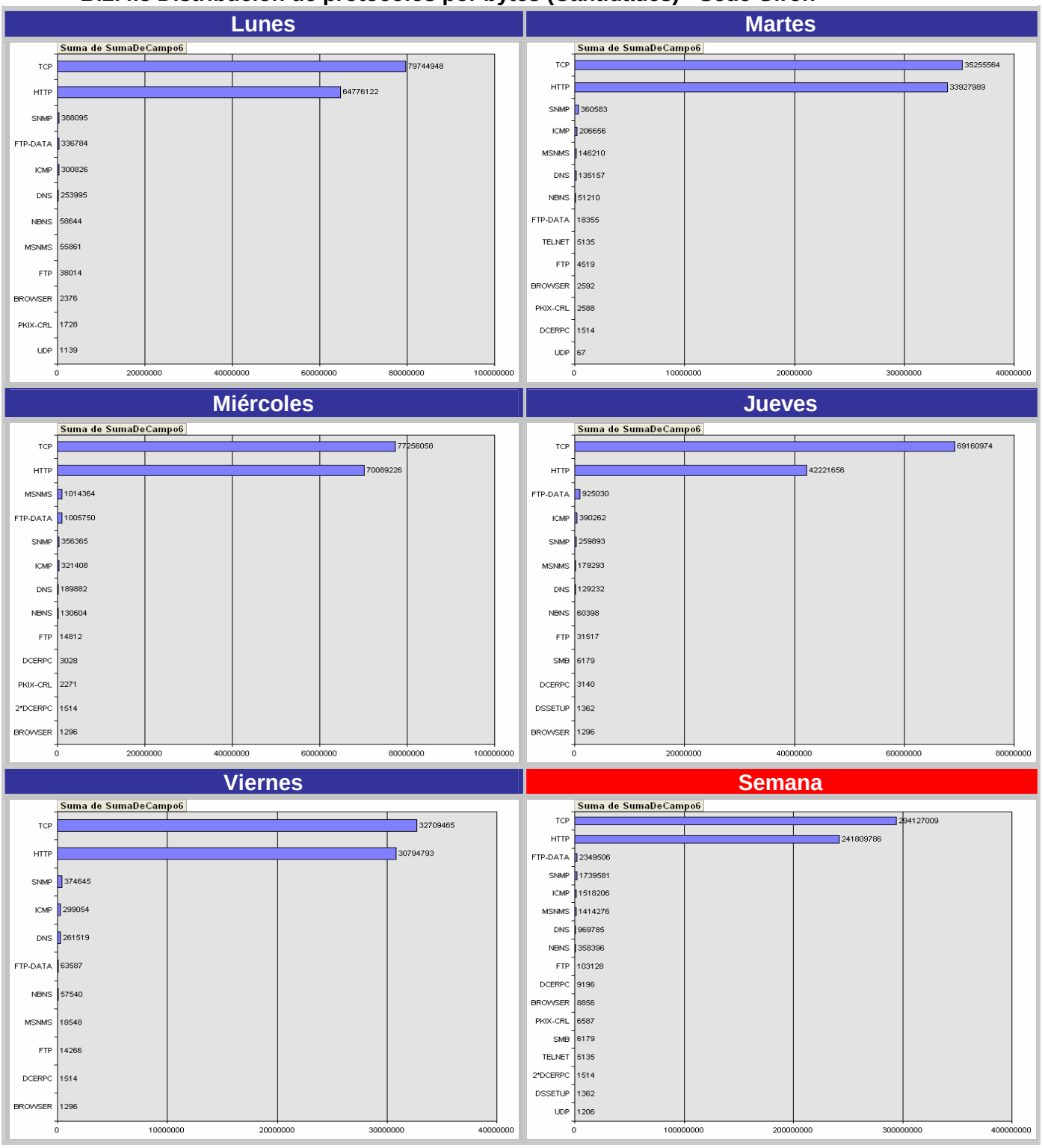


Figura B.2.4.3 Distribución de protocolos por bytes (Cantidades) - Sede Girón

B.2.4.4 Distribución de protocolos por bytes (Porcentajes) - Sede Girón

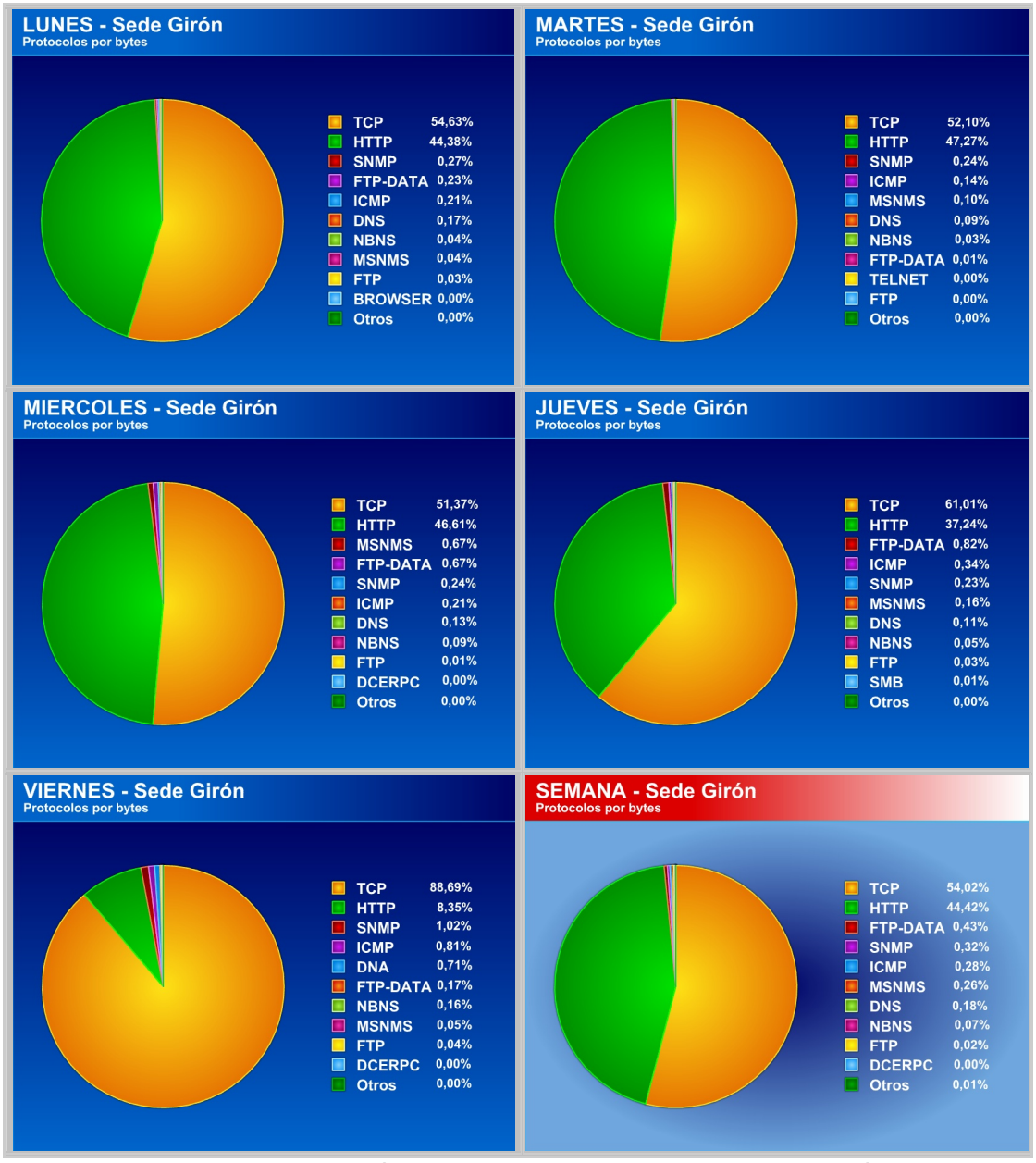


Figura B.2.4.4 Distribución de protocolos por bytes (Porcentajes) - Sede Girón

B.2.4.5 Distribución de tamaño de paquetes - Sede Girón

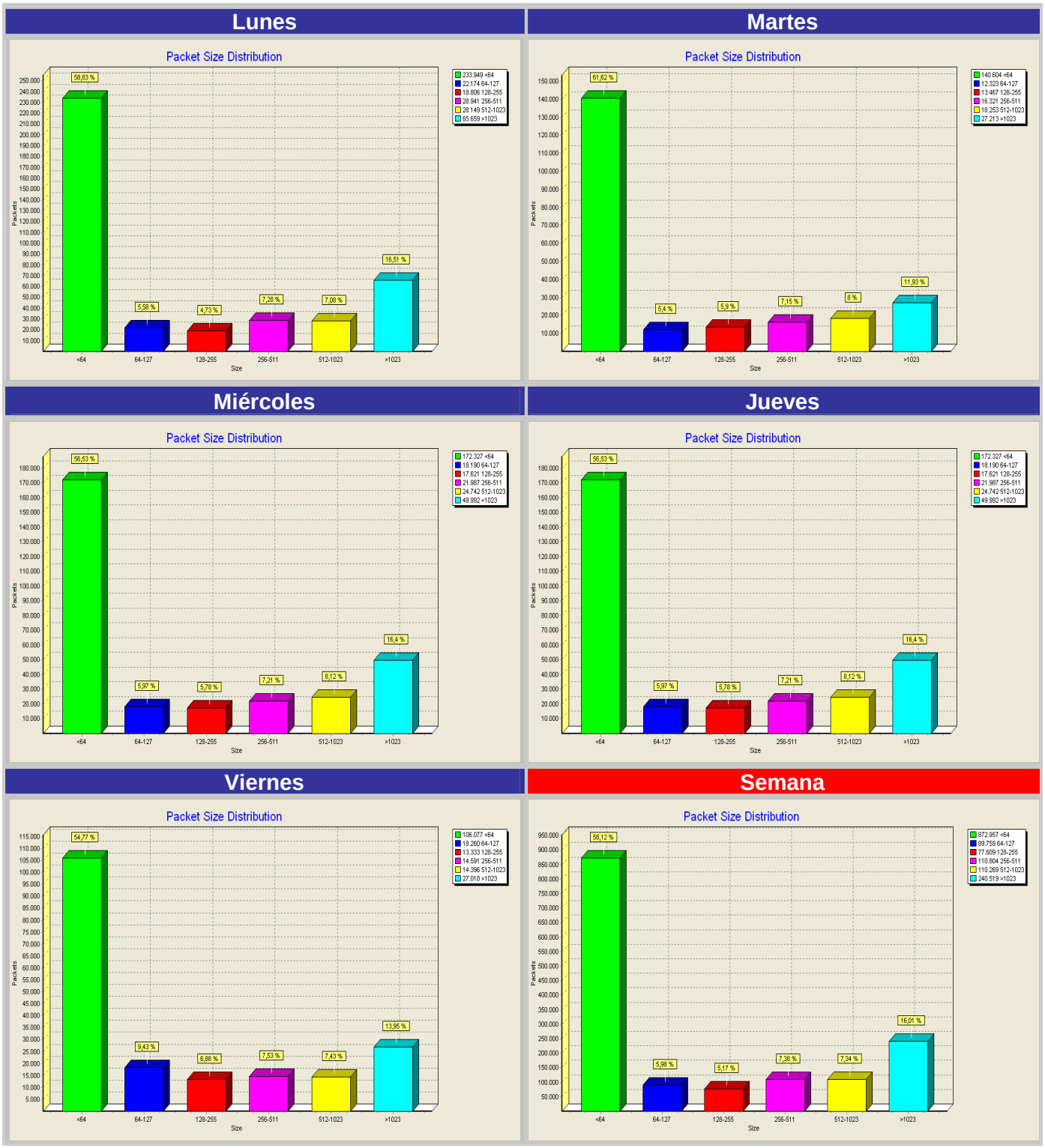


Figura B.2.4.5 Distribución de tamaño de paquetes - Sede Girón

B.2.4.6 Nodos de mayor tráfico enviado - Sede Girón

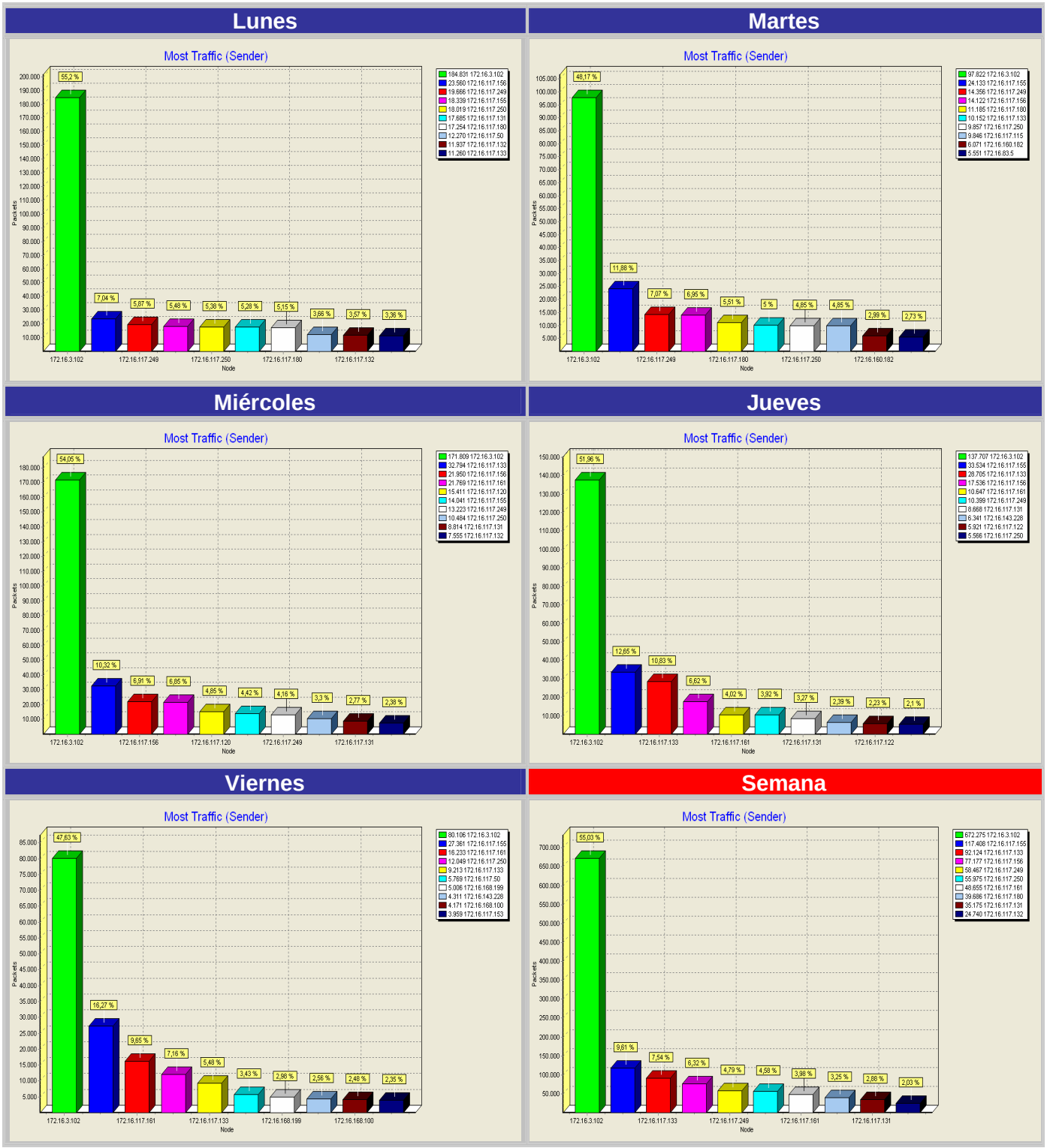


Figura B.2.4.6 Nodos de mayor tráfico enviado - Sede Girón

B.2.4.7 Nodos de mayor tráfico recibido - Sede Girón

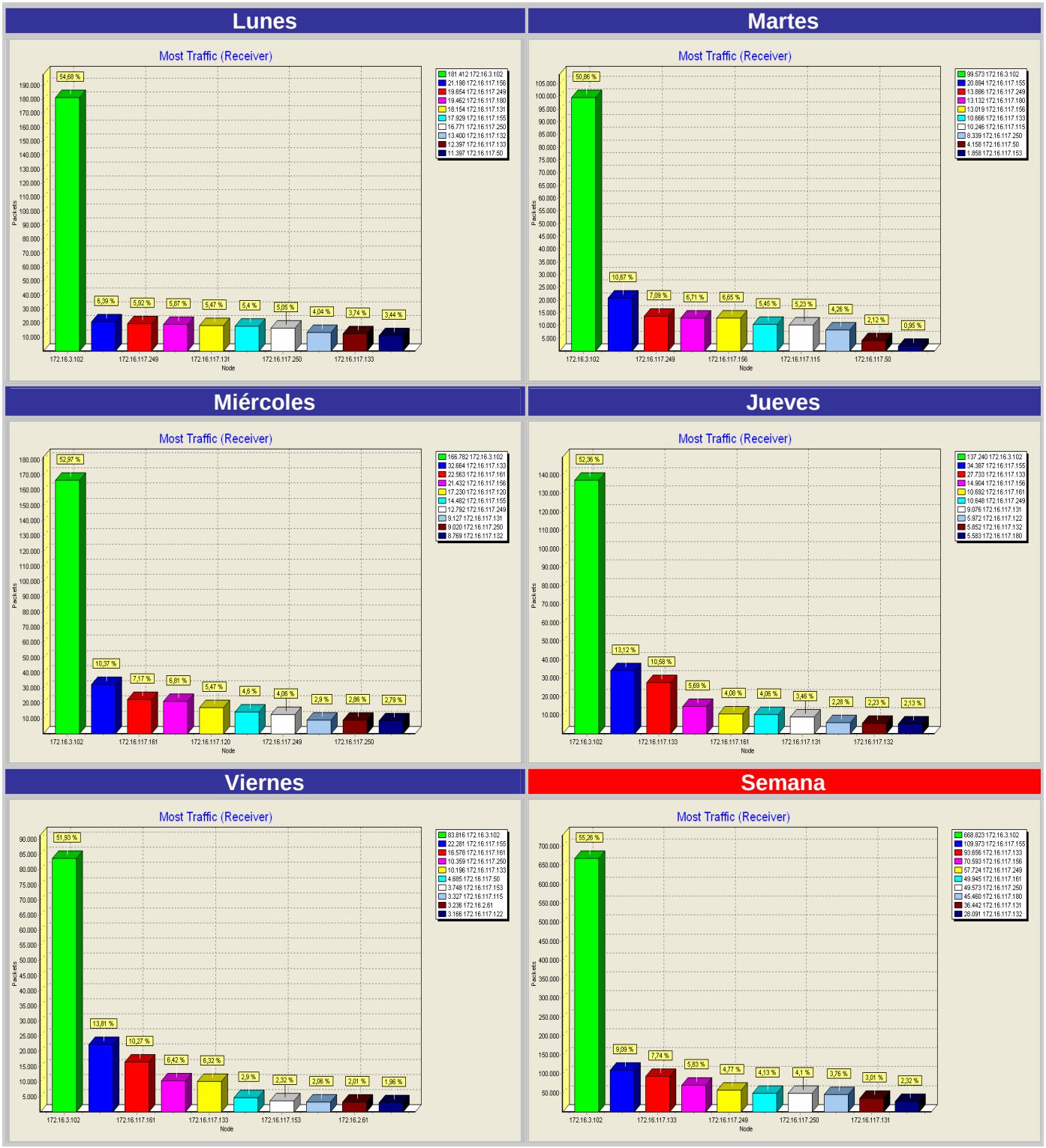


Figura B.2.4.7 Nodos de mayor tráfico recibido - Sede Girón

B.2.5 Sede Barrancabermeja

B.2.5.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Barrancabermeja

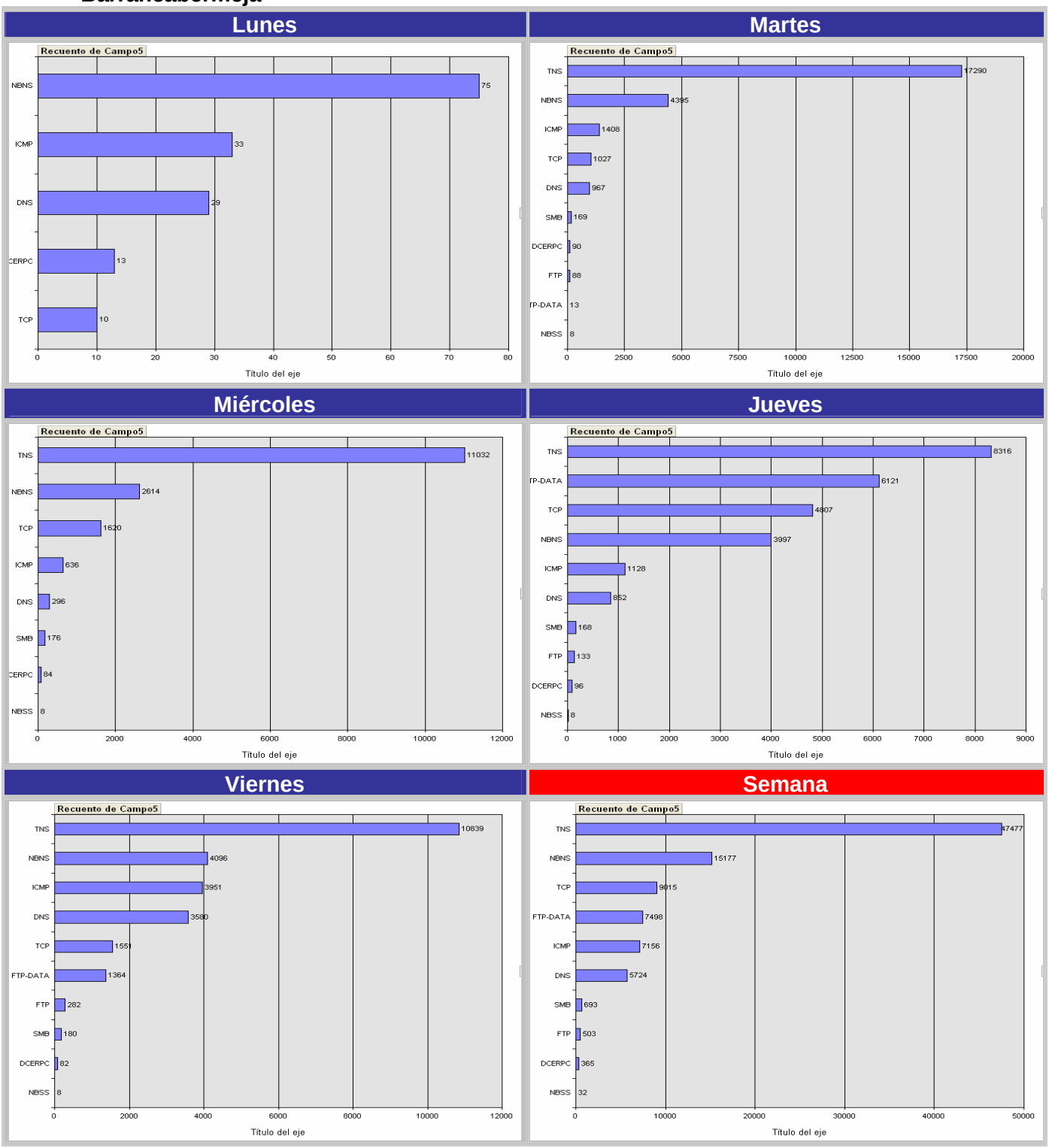


Figura B.2.5.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Barrancabermeja

B.2.5.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Barrancabermeja

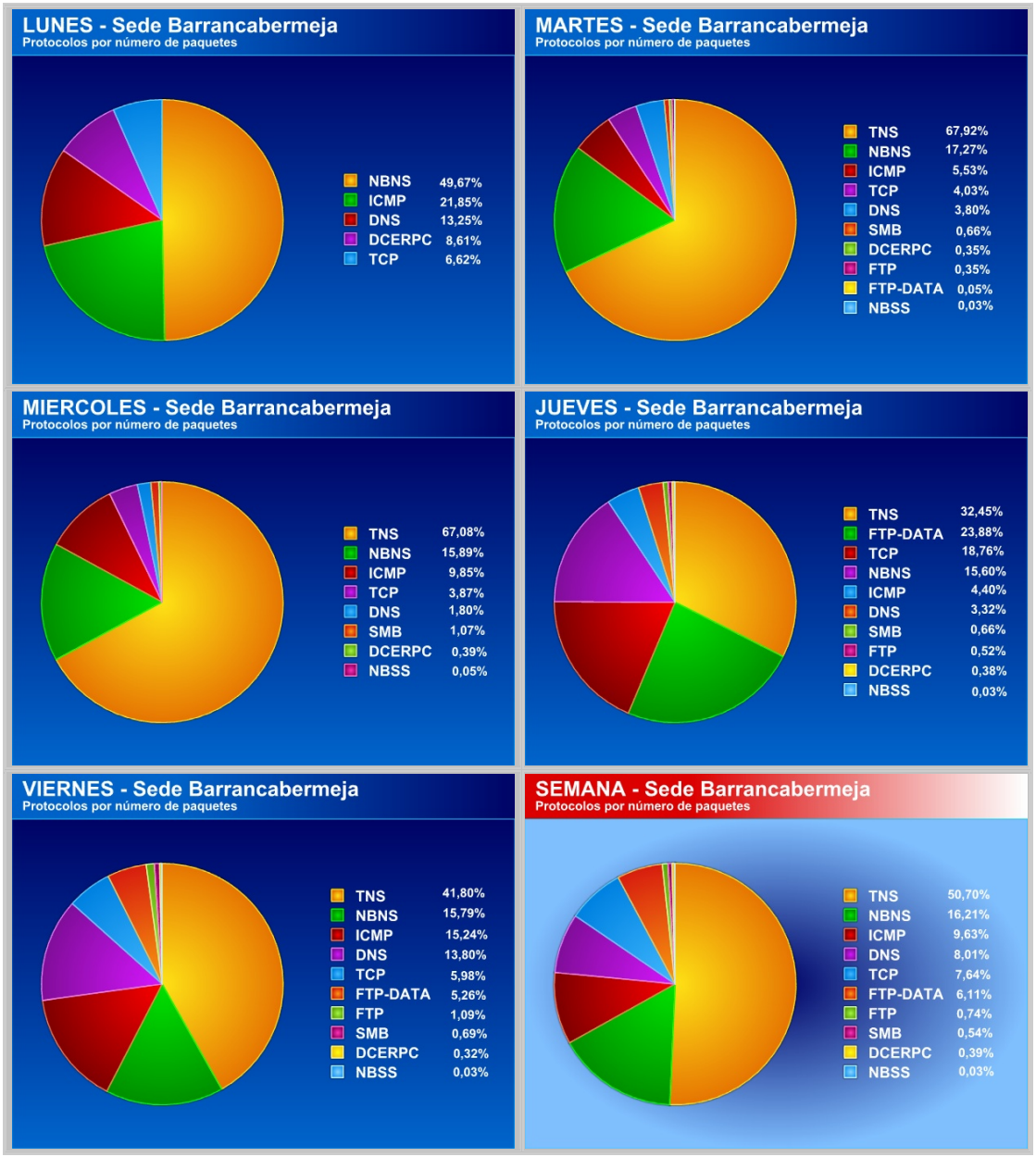


Figura B.2.5.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Barrancabermeja

B.2.5.3 Distribución de protocolos por bytes (Cantidades) - Sede Barrancabermeja

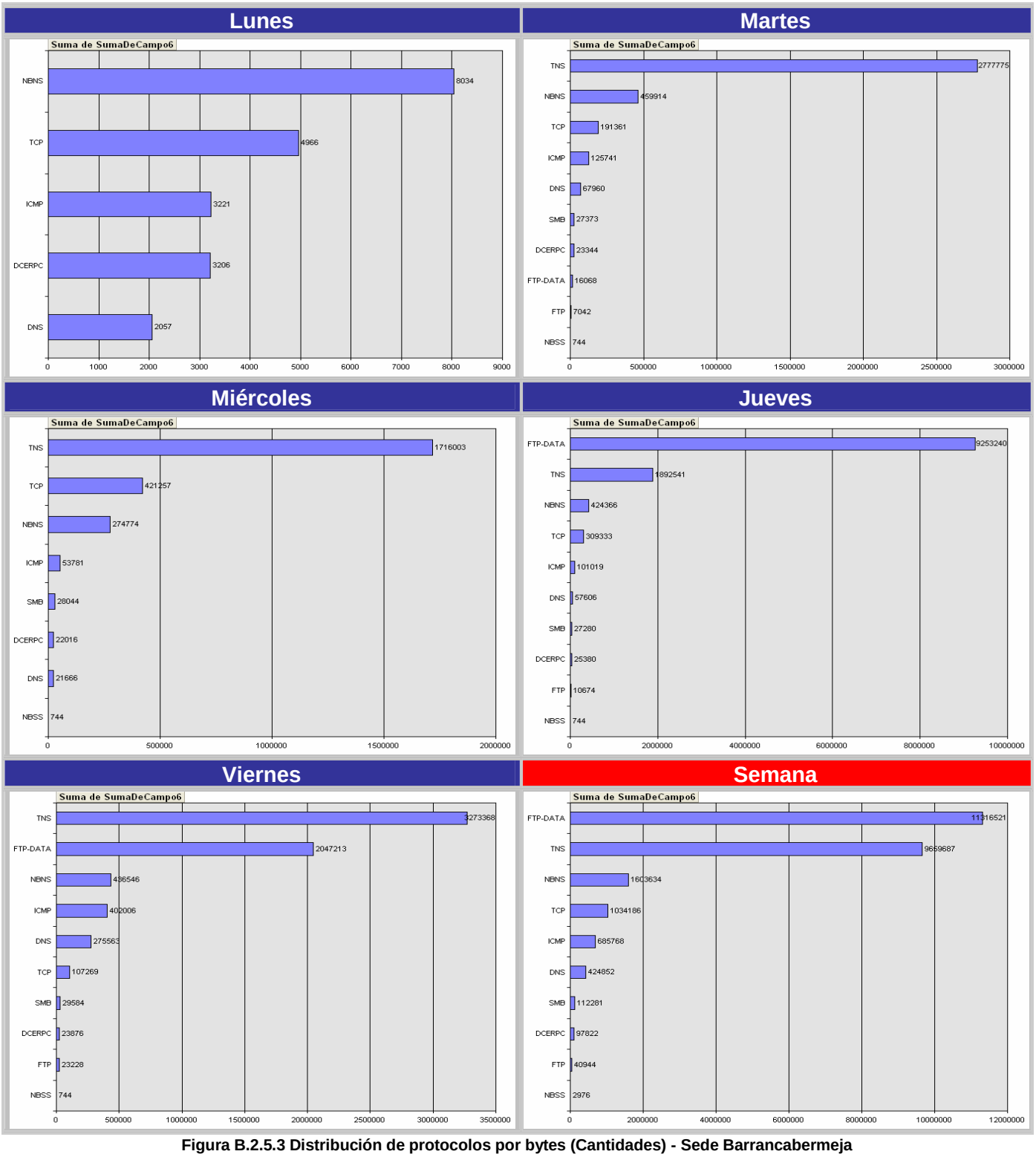


Figura B.2.5.3 Distribución de protocolos por bytes (Cantidades) - Sede Barrancabermeja

B.2.5.4 Distribución de protocolos por bytes (Porcentajes) - Sede Barrancabermeja

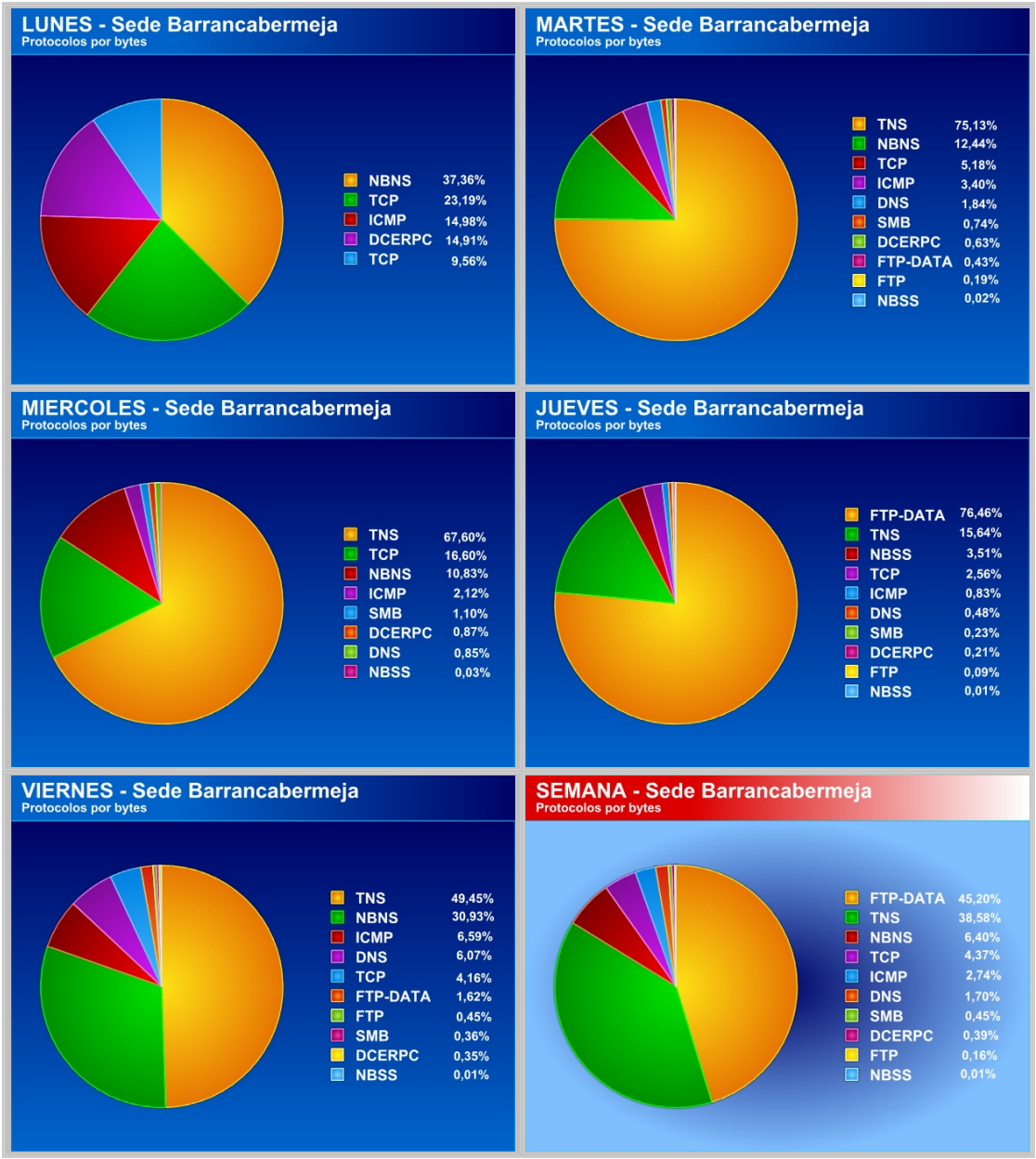


Figura B.2.5.4 Distribución de protocolos por bytes (Porcentajes) - Sede Barrancabermeja

B.2.5.5 Distribución de tamaño de paquetes - Sede Barrancabermeja

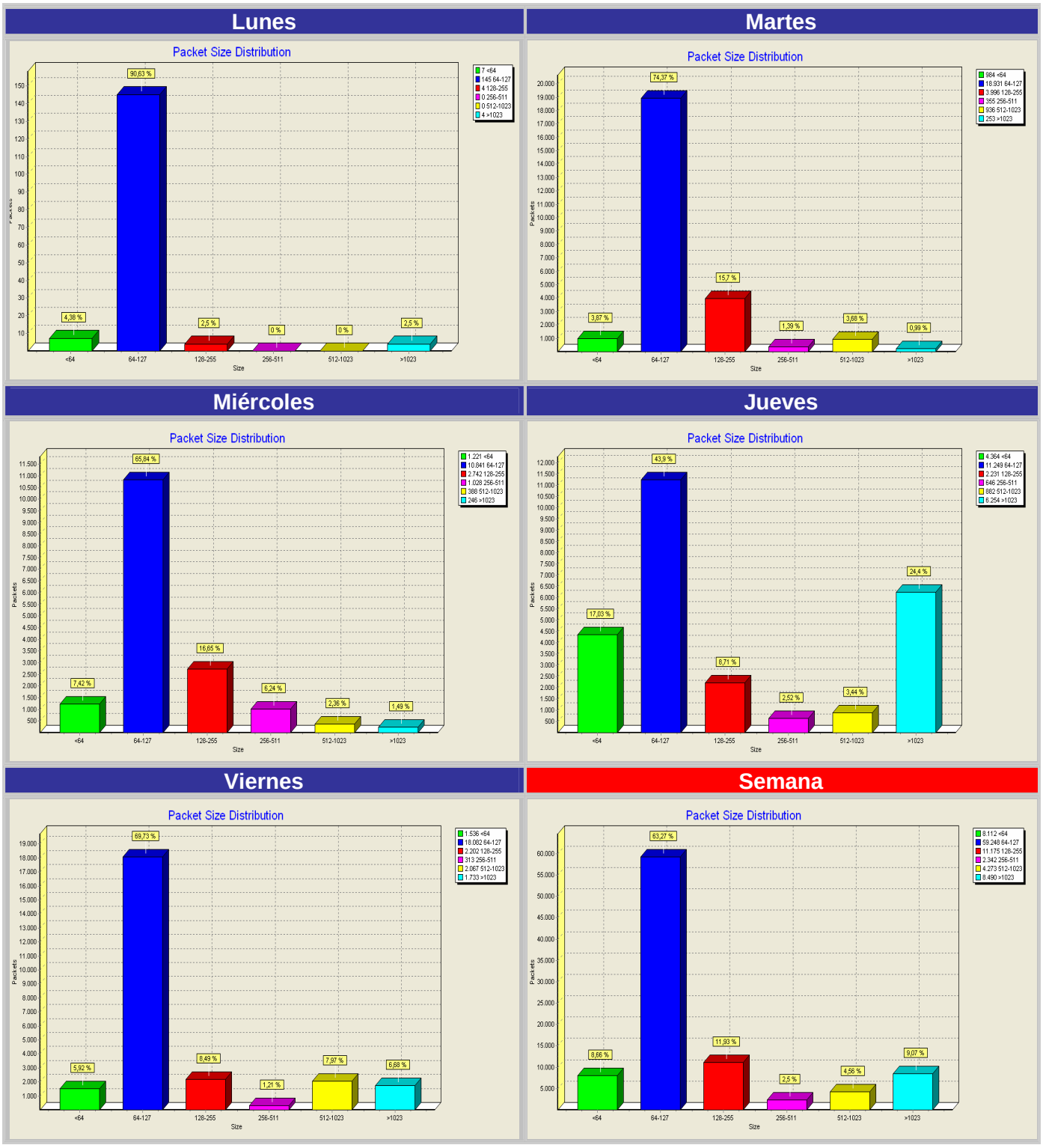


Figura B.2.5.5 Distribución de tamaño de paquetes - Sede Barrancabermeja

B.2.5.6 Nodos de mayor tráfico enviado - Sede Barrancabermeja

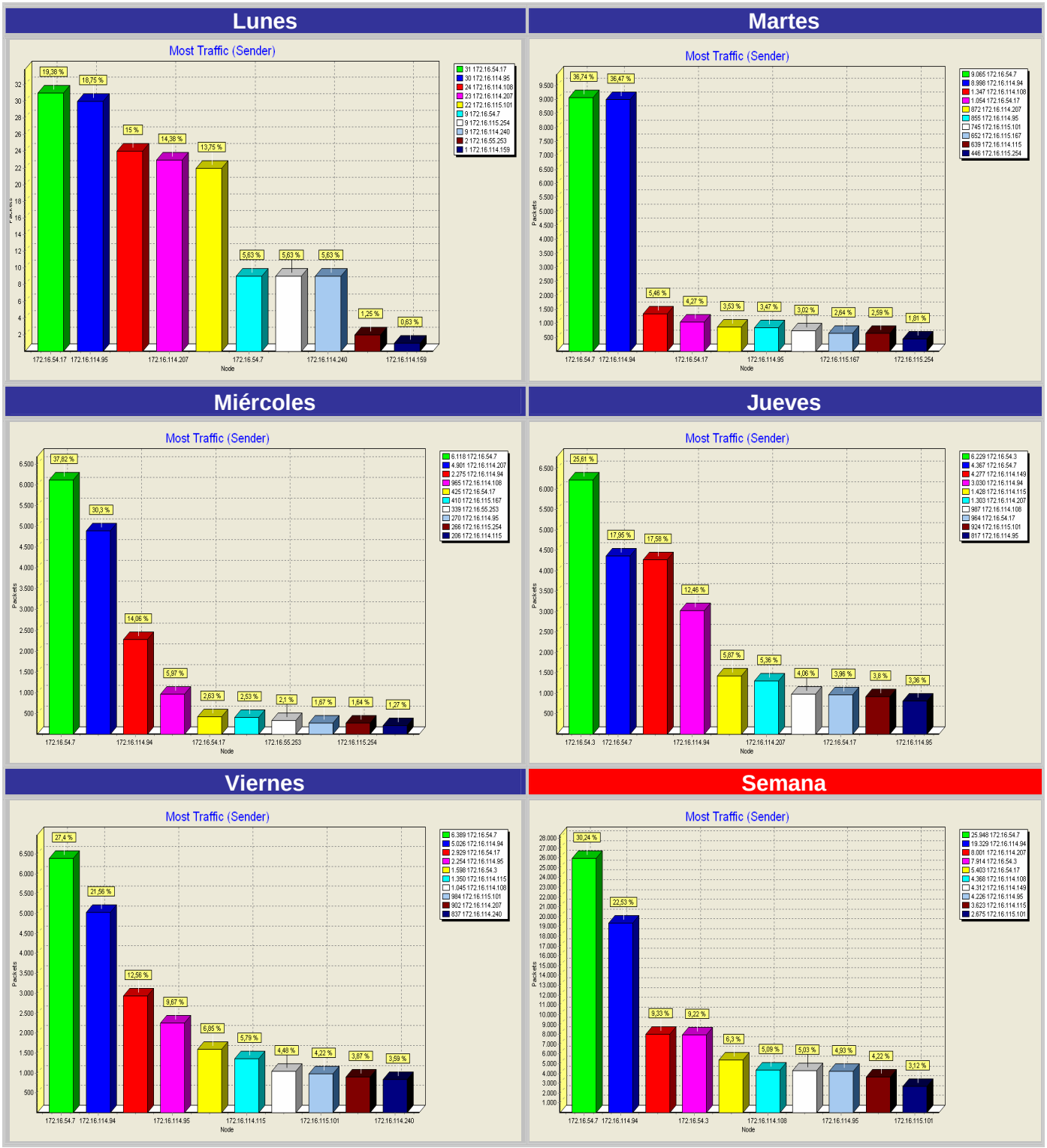


Figura B.2.5.6 Nodos de mayor tráfico enviado - Sede Barrancabermeja

B.2.5.7 Nodos de mayor tráfico recibido - Sede Barrancabermeja

Figura B.2.5.7 Nodos de mayor tráfico recibido - Sede Barrancabermeja

B.2.6 Sede Málaga

B.2.6.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Málaga

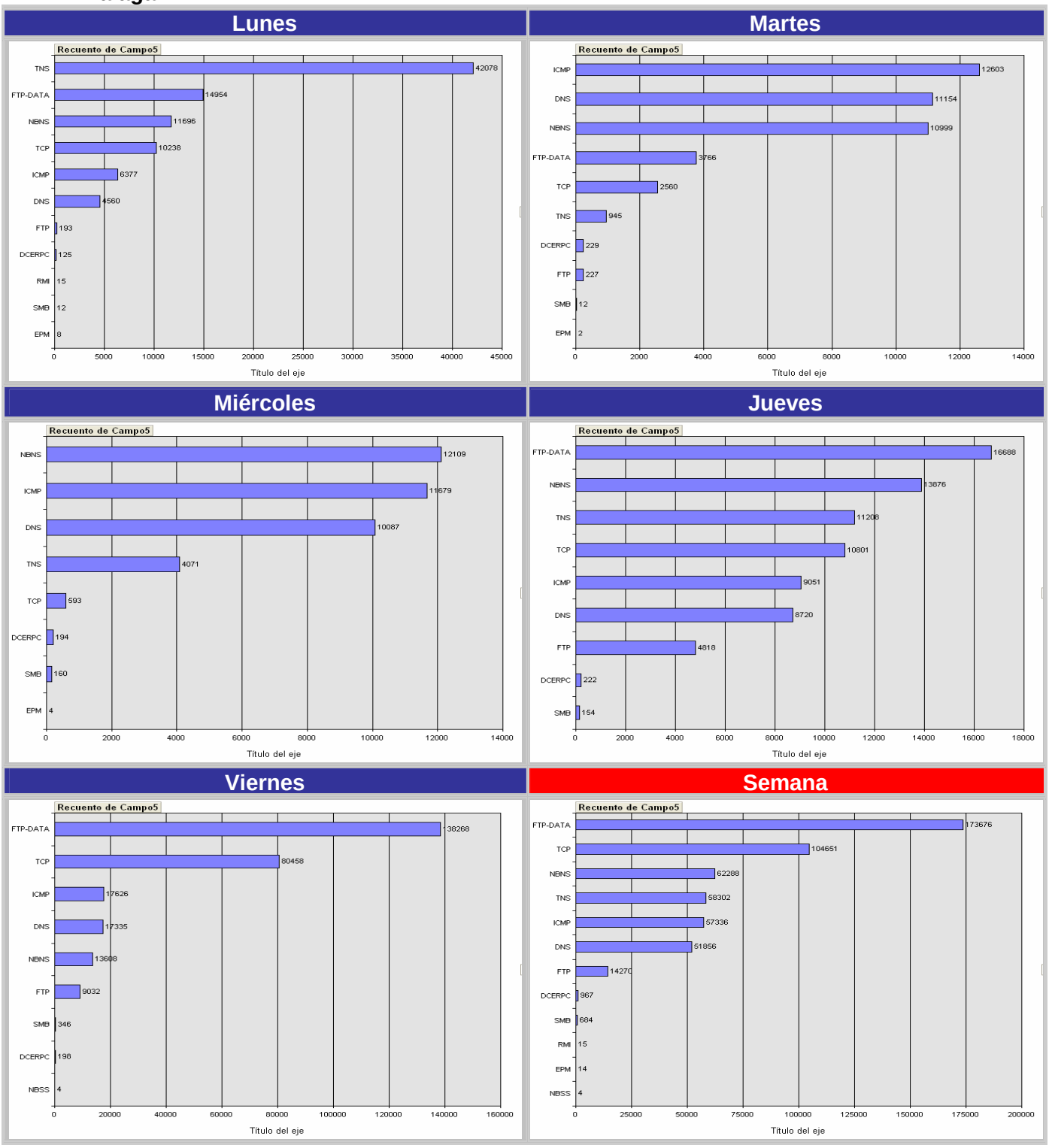


Figura B.2.6.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Málaga

B.2.6.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Málaga

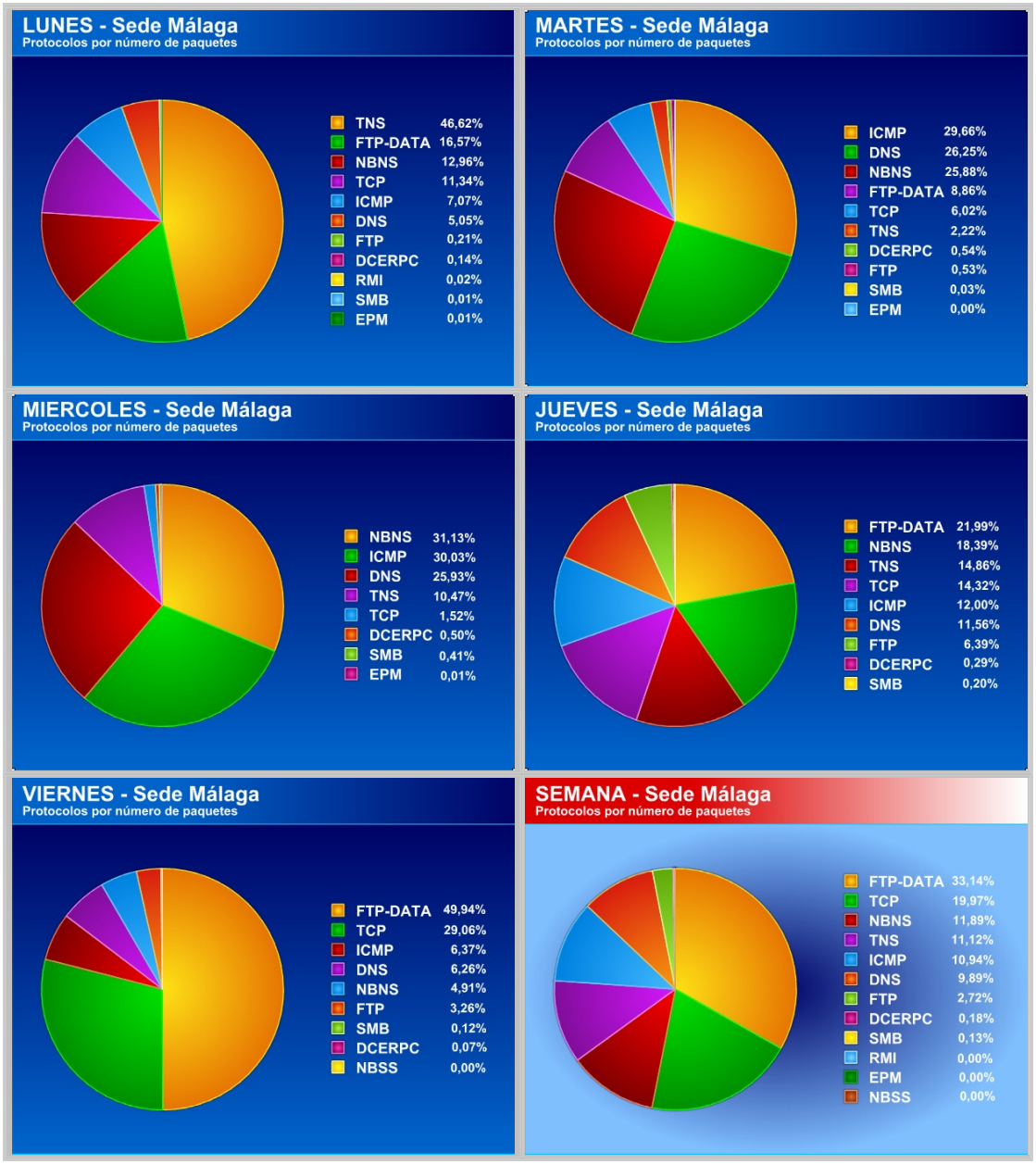


Figura B.2.6.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Málaga

B.2.6.3 Distribución de protocolos por bytes (Cantidades) - Sede Málaga

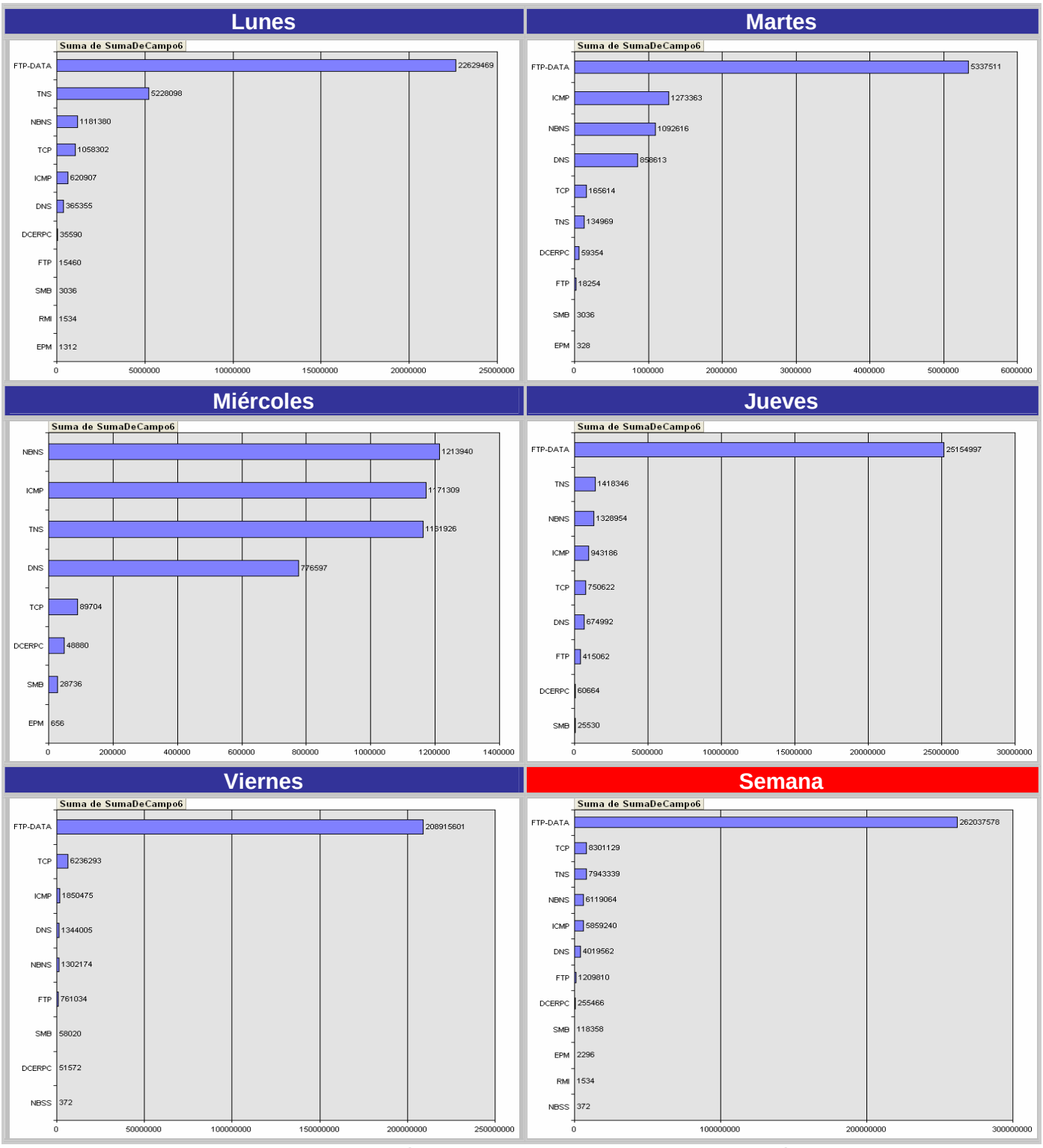


Figura B.2.6.3 Distribución de protocolos por bytes (Cantidades) - Sede Málaga

B.2.6.4 Distribución de protocolos por bytes (Porcentajes) - Sede Málaga

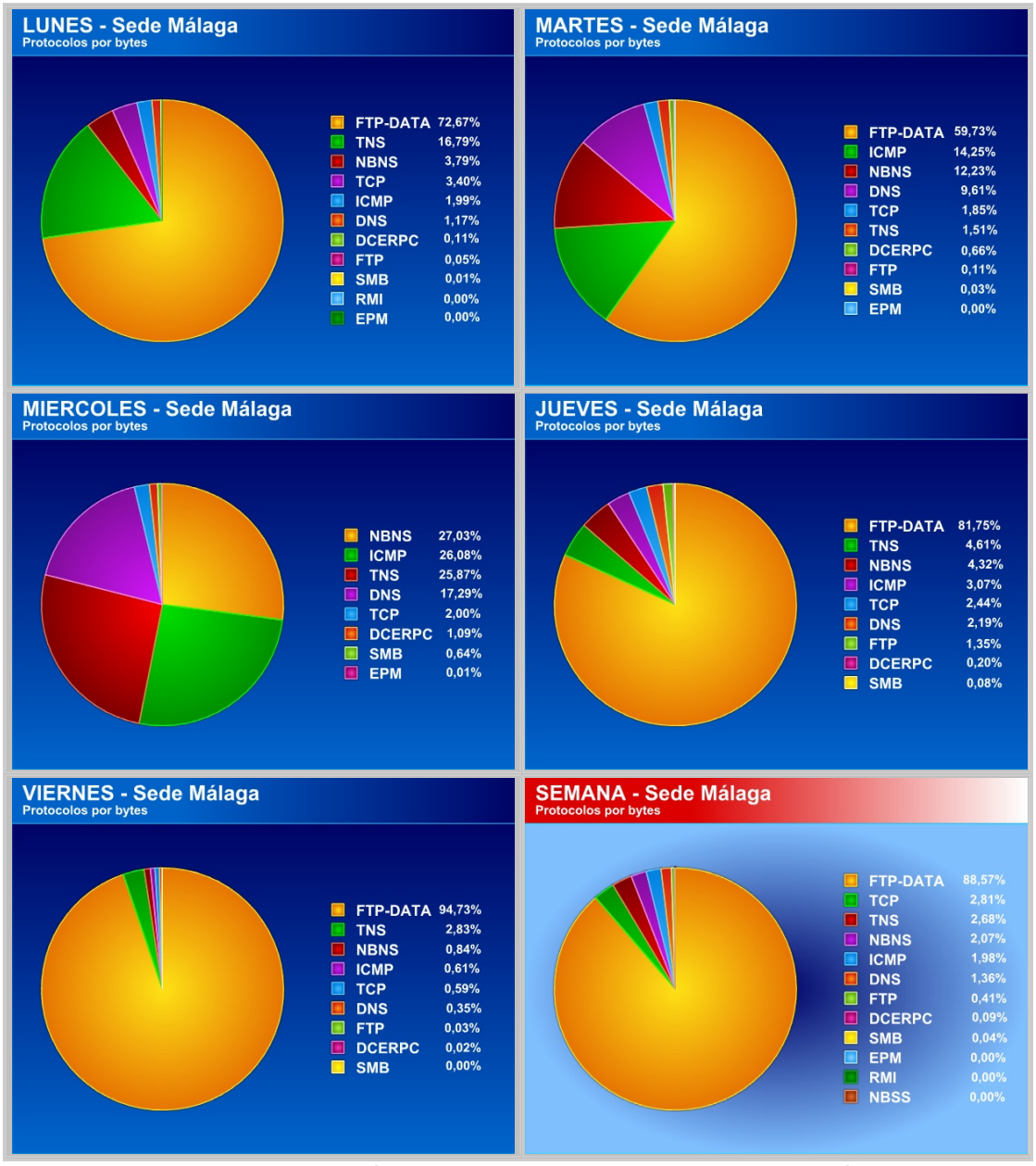


Figura B.2.6.4 Distribución de protocolos por bytes (Porcentajes) - Sede Málaga

B.2.6.5 Distribución de tamaño de paquetes - Sede Málaga

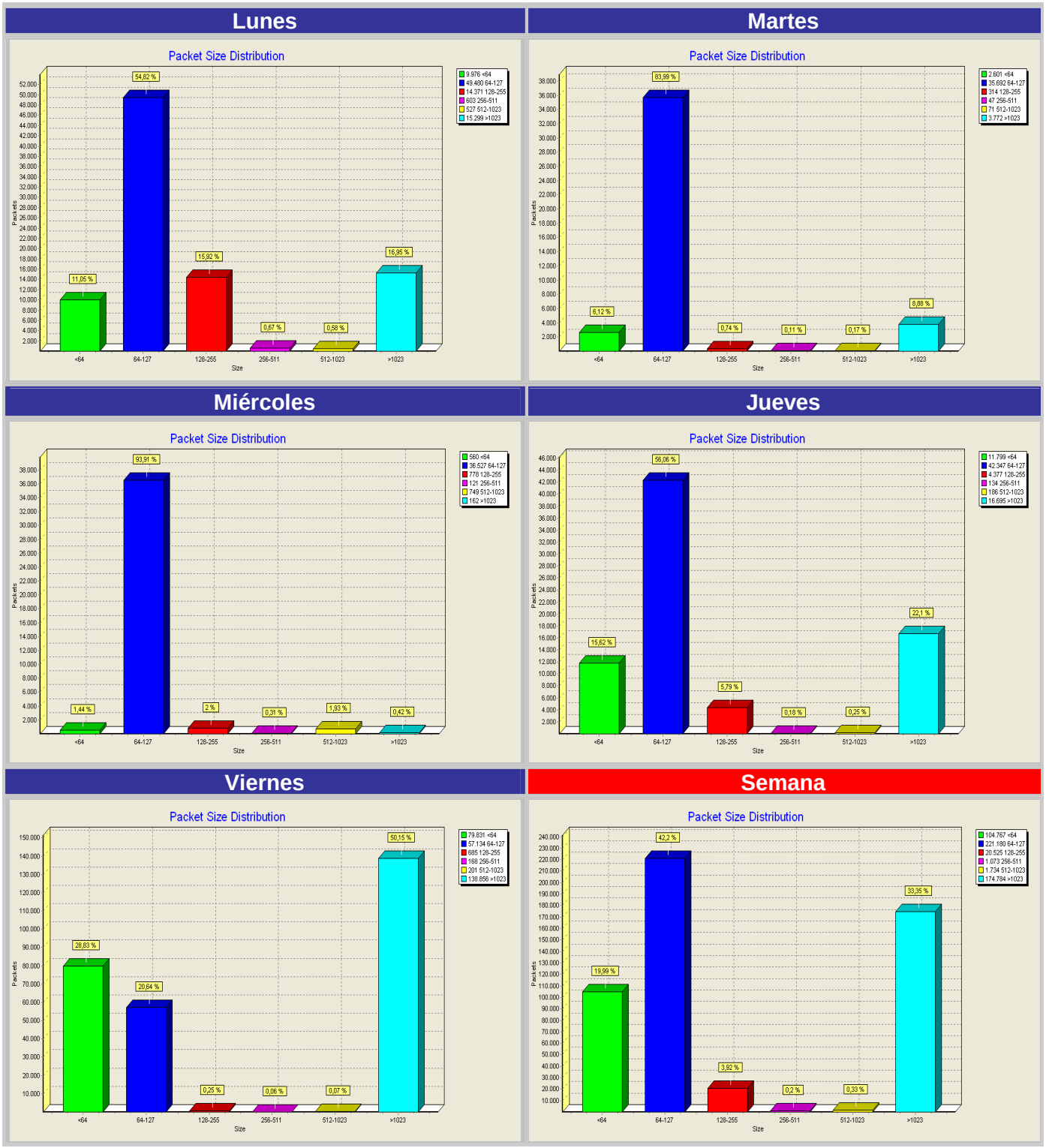


Figura B.2.6.5 Distribución de tamaño de paquetes - Sede Málaga

B.2.6.6 Nodos de mayor tráfico enviado - Sede Málaga

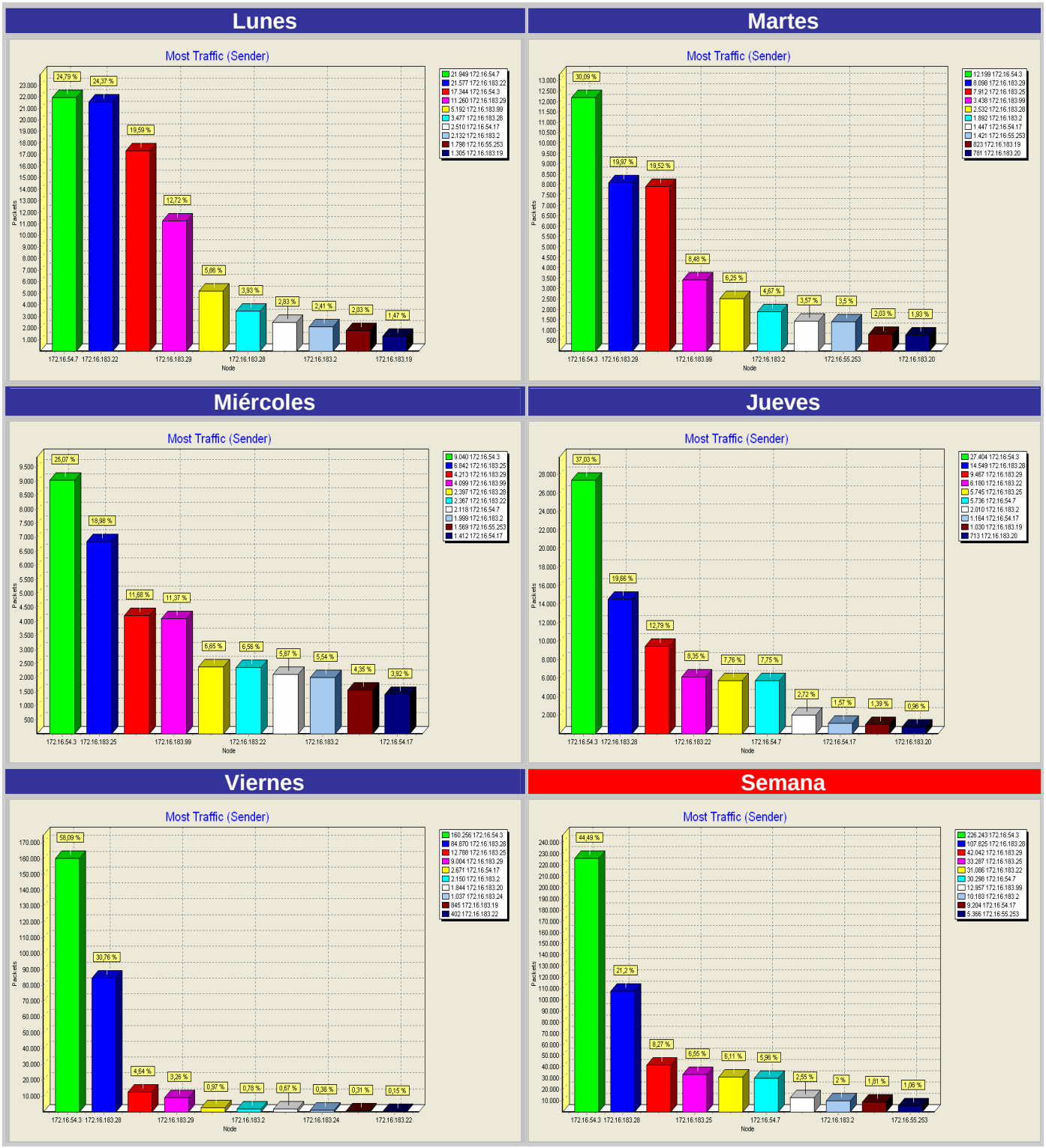


Figura B.2.6.6 Nodos de mayor tráfico enviado - Sede Málaga

B.2.6.7 Nodos de mayor tráfico recibido - Sede Málaga

Figura B.2.6.7 Nodos de mayor tráfico recibido - Sede Málaga

B.2.7 Sede Piedecuesta

B.2.7.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Piedecuesta

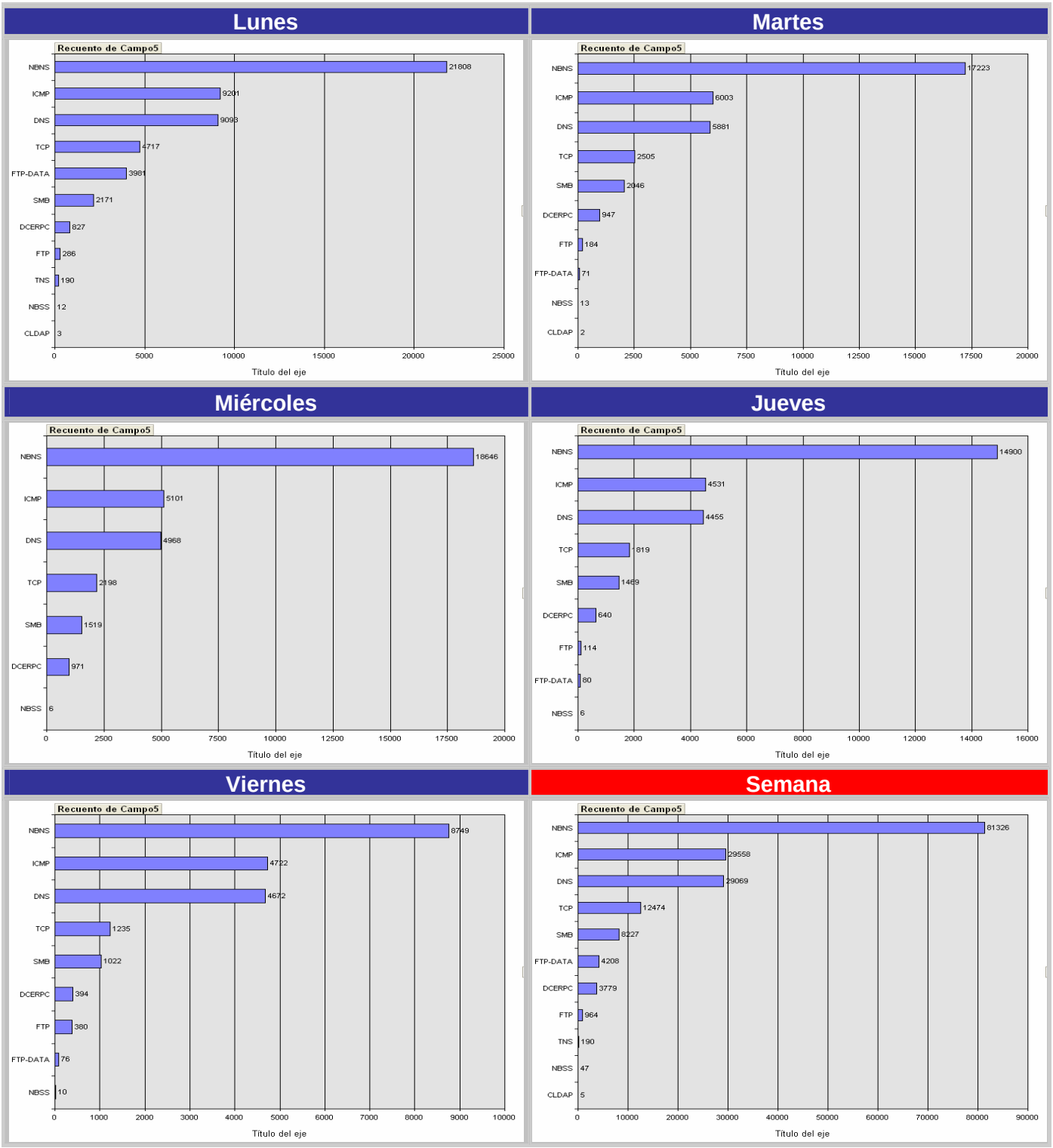


Figura B.2.7.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Piedecuesta

B.2.7.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Piedecuesta

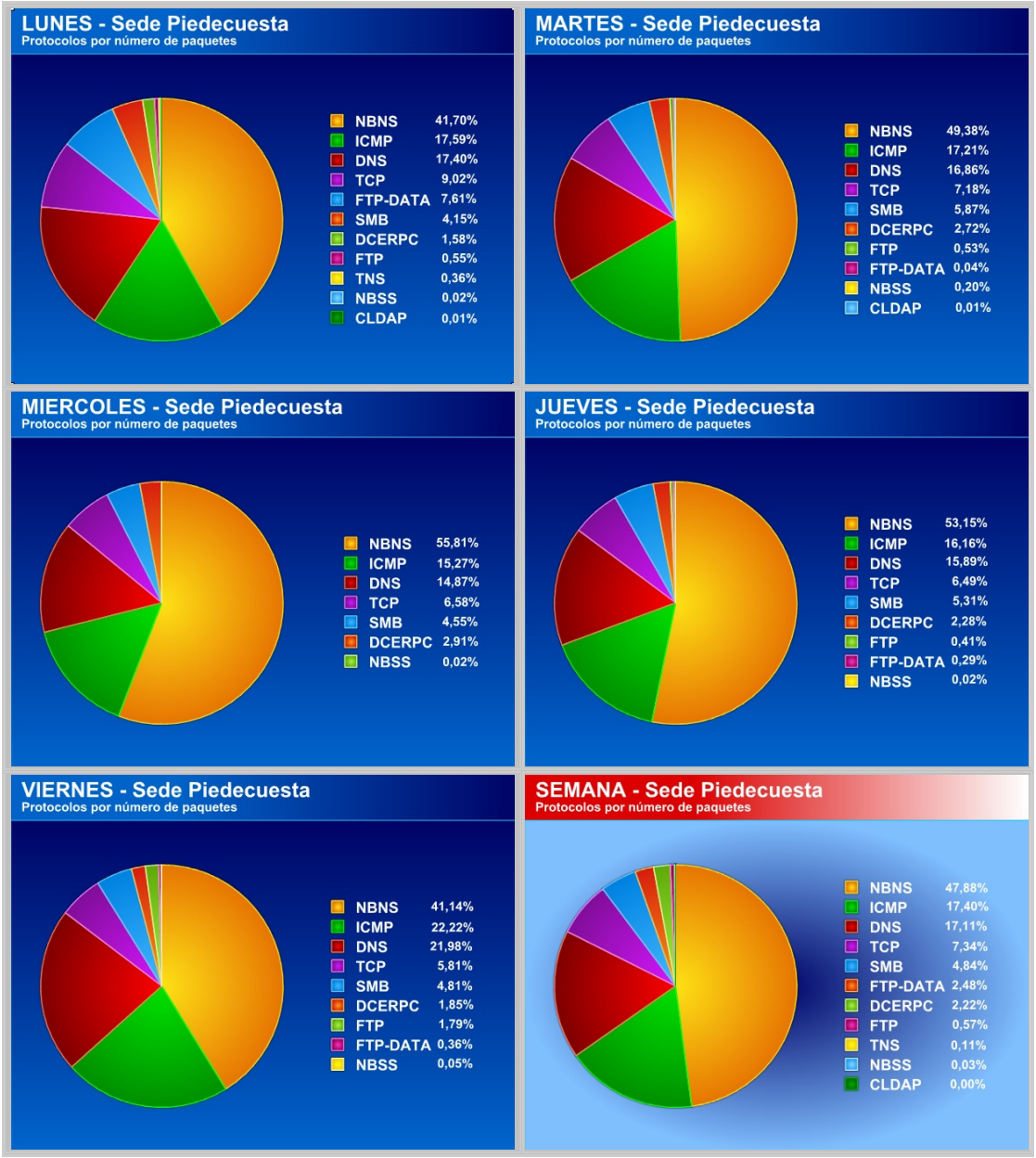


Figura B.2.7.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Piedecuesta

B.2.7.3 Distribución de protocolos por bytes (Cantidades) - Sede Piedecuesta

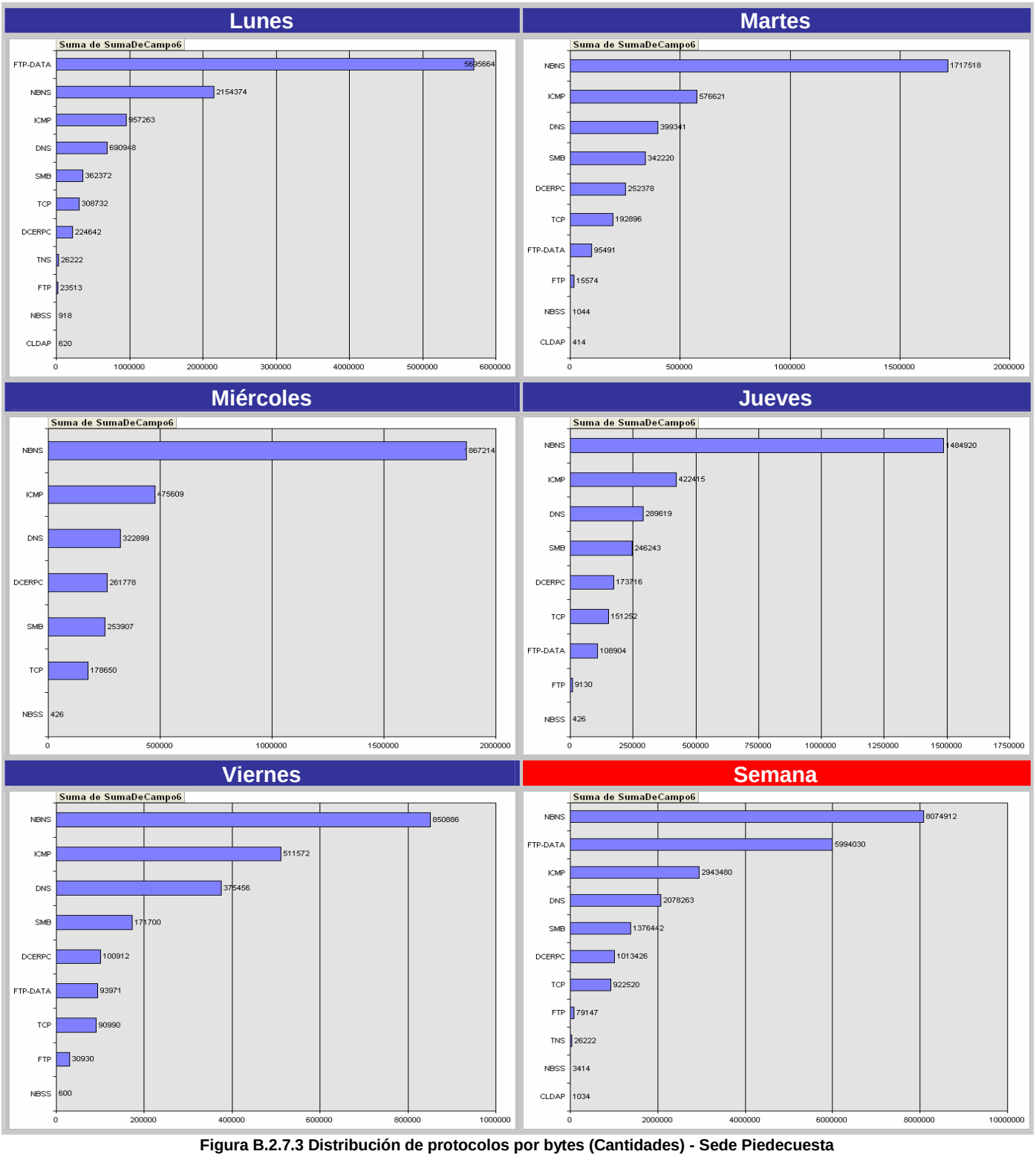


Figura B.2.7.3 Distribución de protocolos por bytes (Cantidades) - Sede Piedecuesta

B.2.7.4 Distribución de protocolos por bytes (Porcentajes) - Sede Piedecuesta

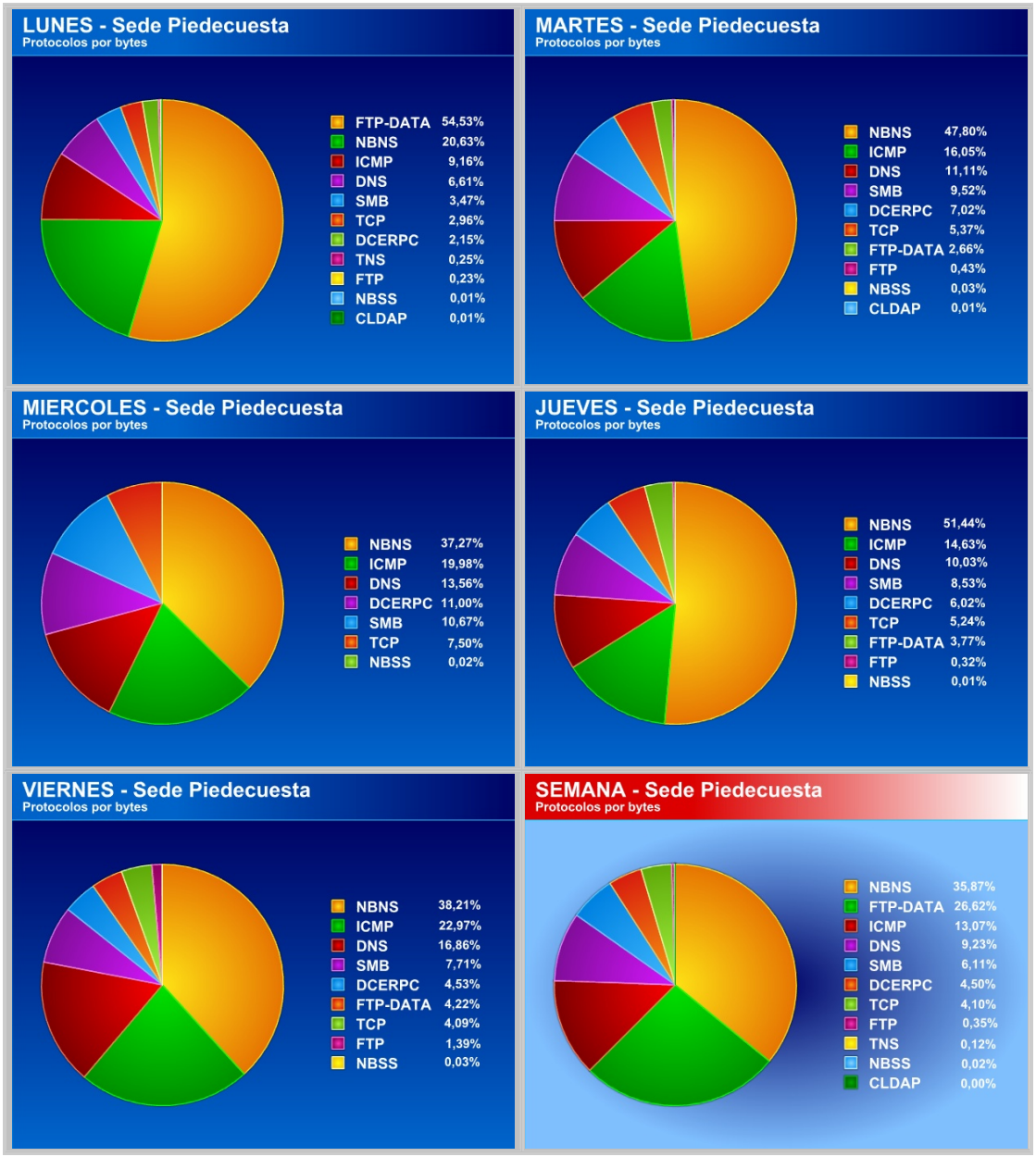


Figura B.2.7.4 Distribución de protocolos por bytes (Porcentajes) - Sede Piedecuesta

B.2.7.5 Distribución de tamaño de paquetes - Sede Piedecuesta

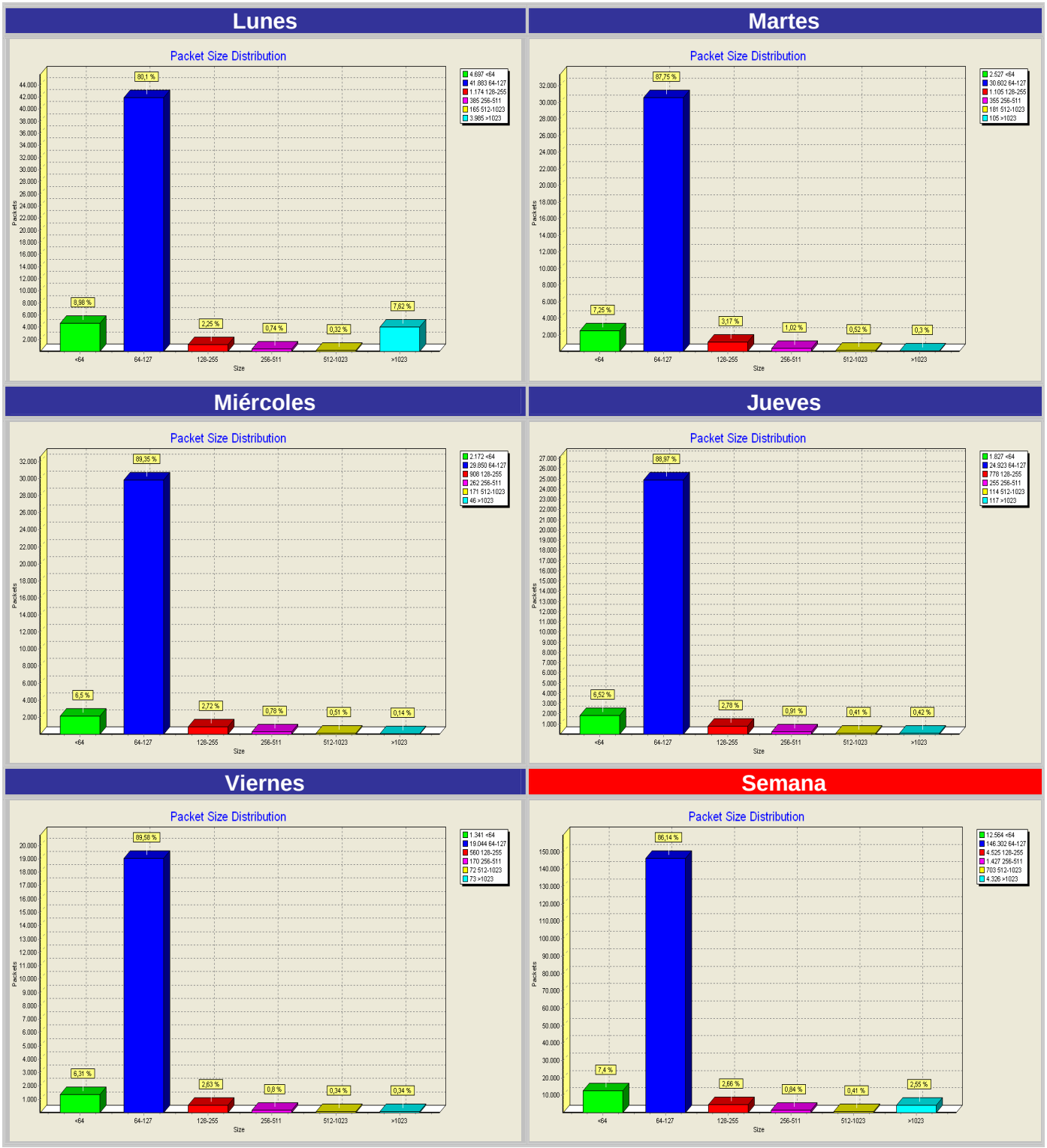


Figura B.2.7.5 Distribución de tamaño de paquetes - Sede Piedecuesta

B.2.7.6 Nodos de mayor tráfico enviado - Sede Piedecuesta

Figura B.2.7.6 Nodos de mayor tráfico enviado - Sede Piedecuesta

B.2.7.7 Nodos de mayor tráfico recibido - Sede Piedecuesta

Figura B.2.7.7 Nodos de mayor tráfico recibido - Sede Piedecuesta

B.2.8 Sede San Gil

B.2.8.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede San Gil

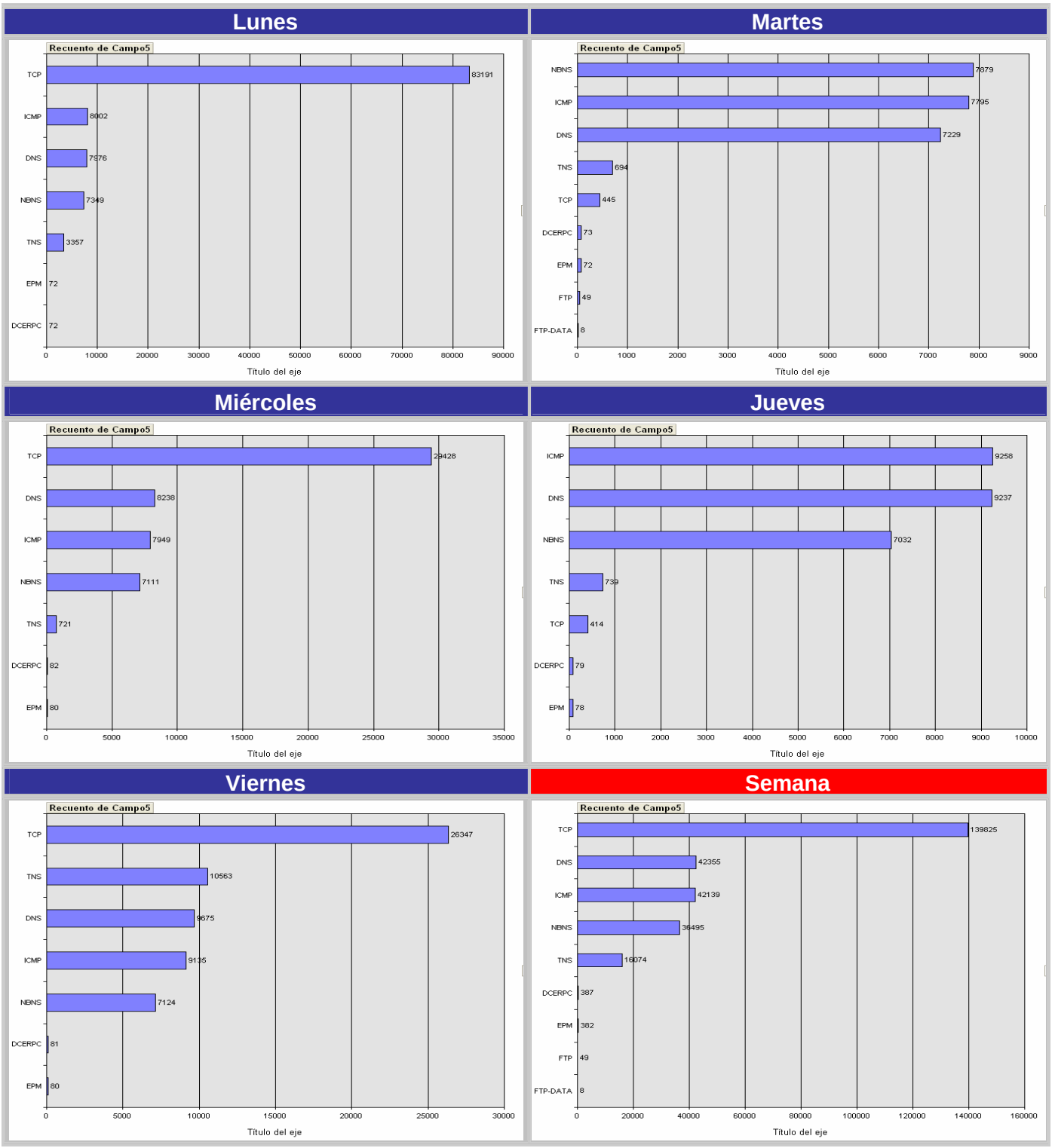


Figura B.2.8.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede San Gil

B.2.8.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede San Gil

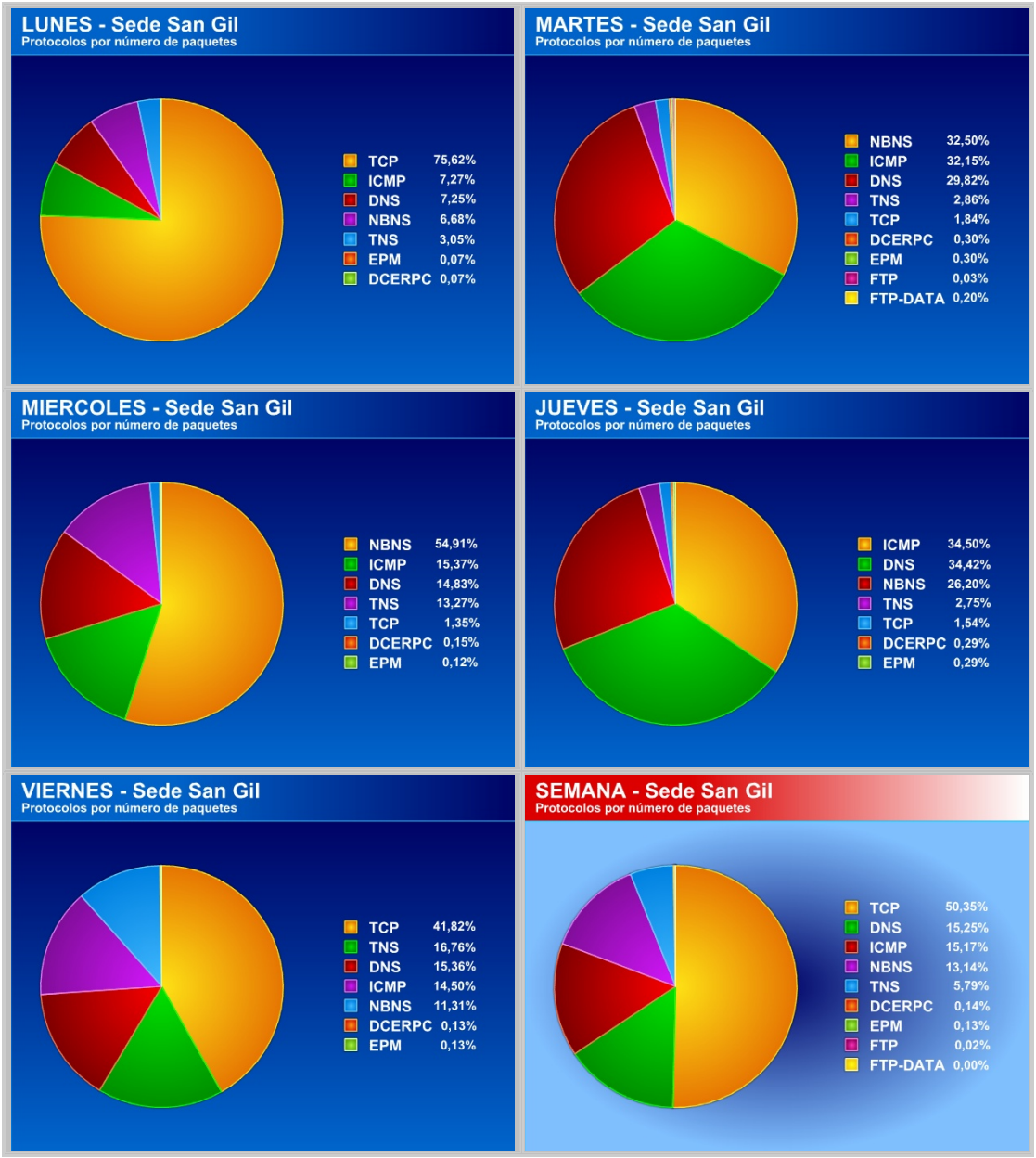


Figura B.2.8.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede San Gil

B.2.8.3 Distribución de protocolos por bytes (Cantidades) - Sede San Gil

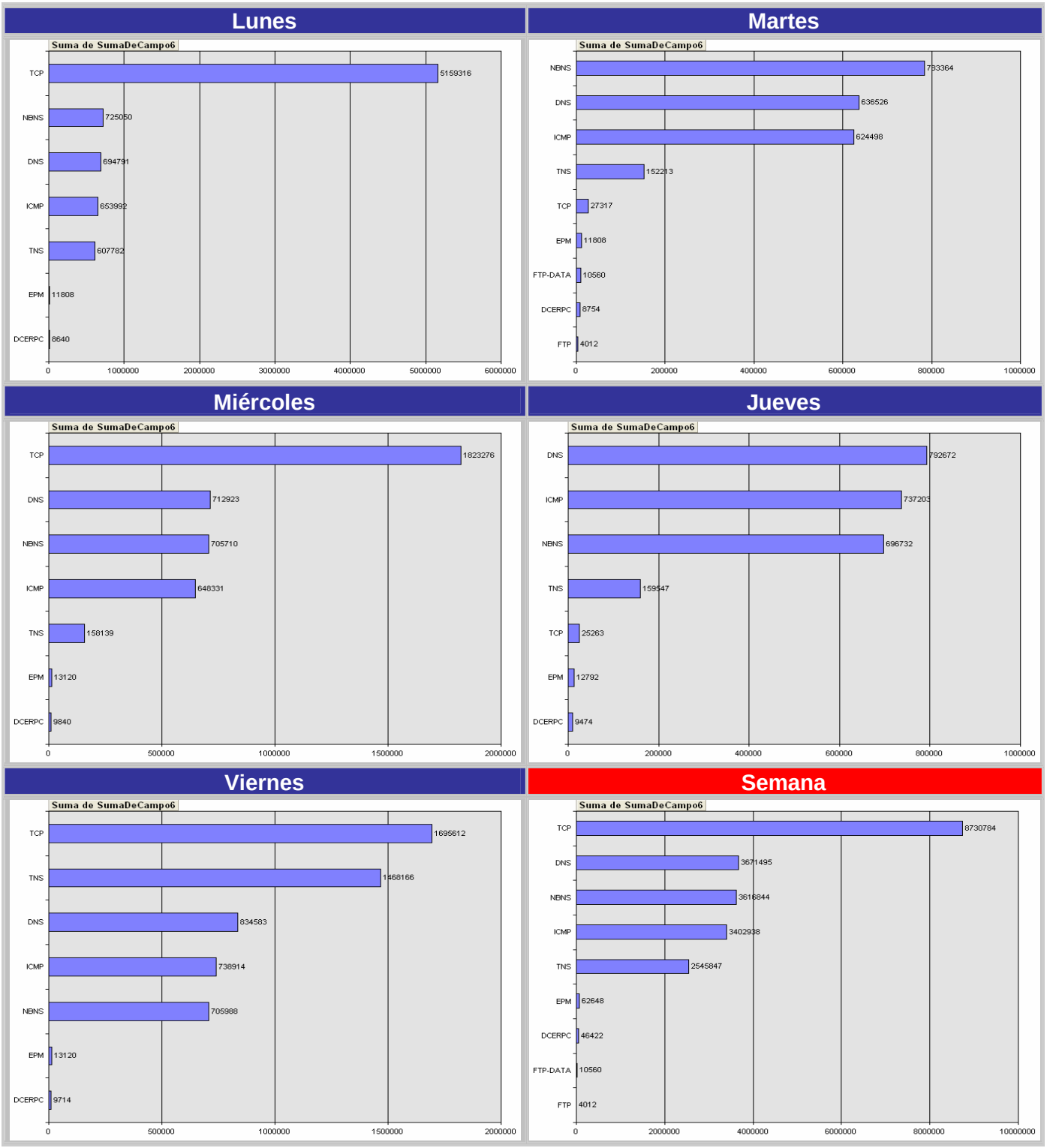


Figura B.2.8.3 Distribución de protocolos por bytes (Cantidades) - Sede San Gil

B.2.8.4 Distribución de protocolos por bytes (Porcentajes) - Sede San Gil

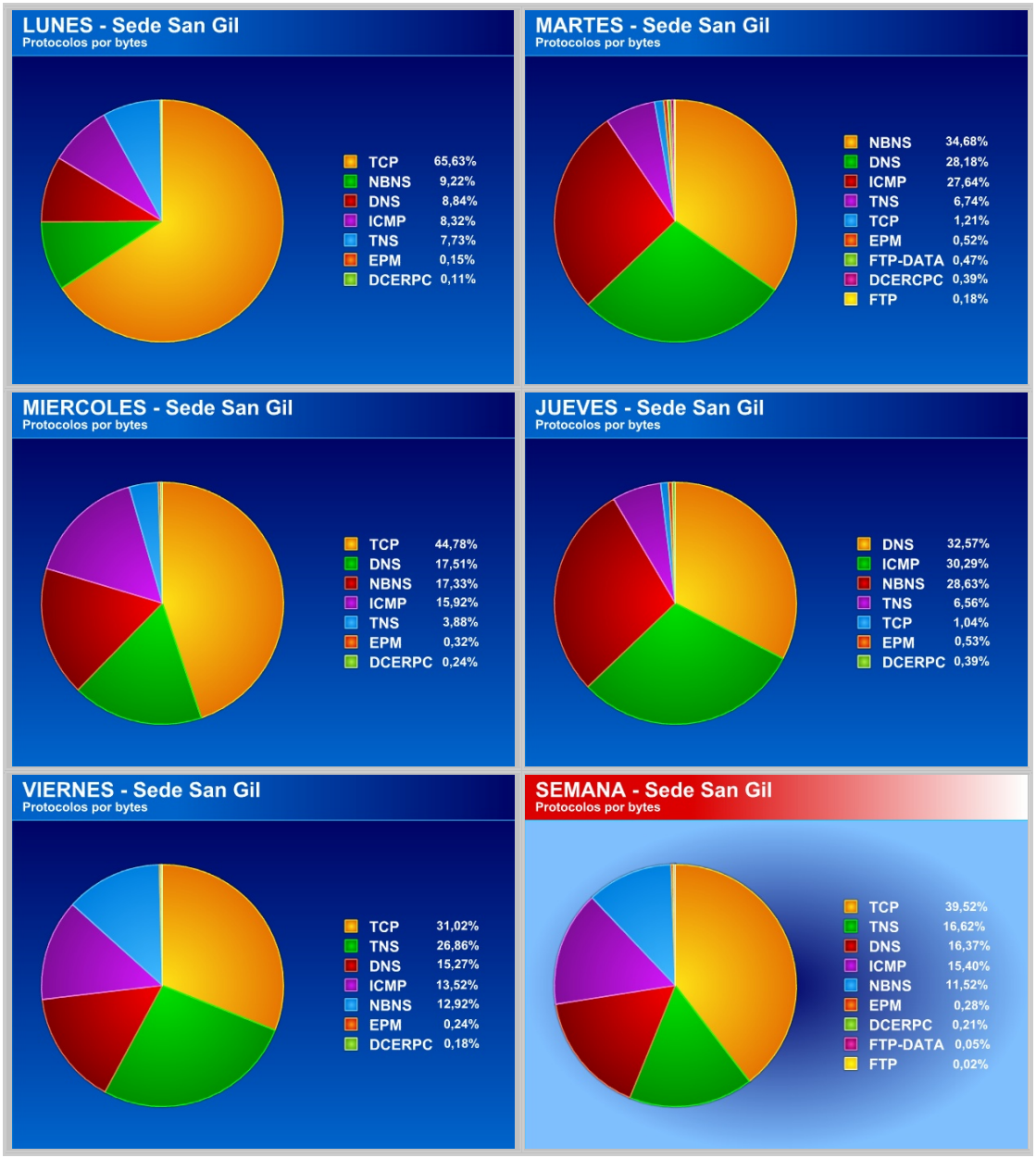


Figura B.2.8.4 Distribución de protocolos por bytes (Porcentajes) - Sede San Gil

B.2.8.5 Distribución de tamaño de paquetes - Sede San Gil

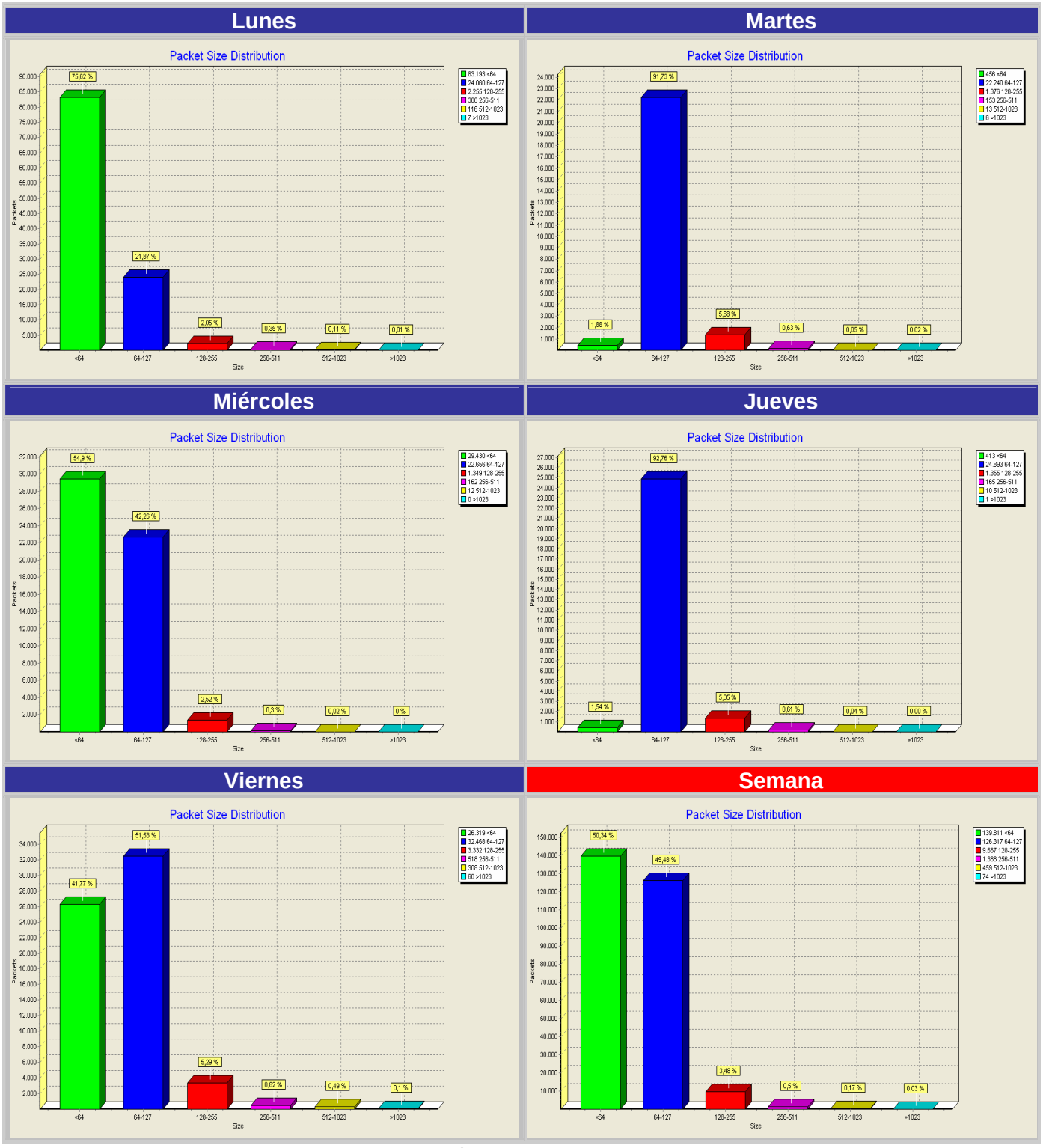


Figura B.2.8.5 Distribución de tamaño de paquetes - Sede San Gil

B.2.8.6 Nodos de mayor tráfico enviado - Sede San Gil

Figura B.2.8.6 Nodos de mayor tráfico enviado - Sede San Gil

B.2.8.7 Nodos de mayor tráfico recibido - Sede San Gil

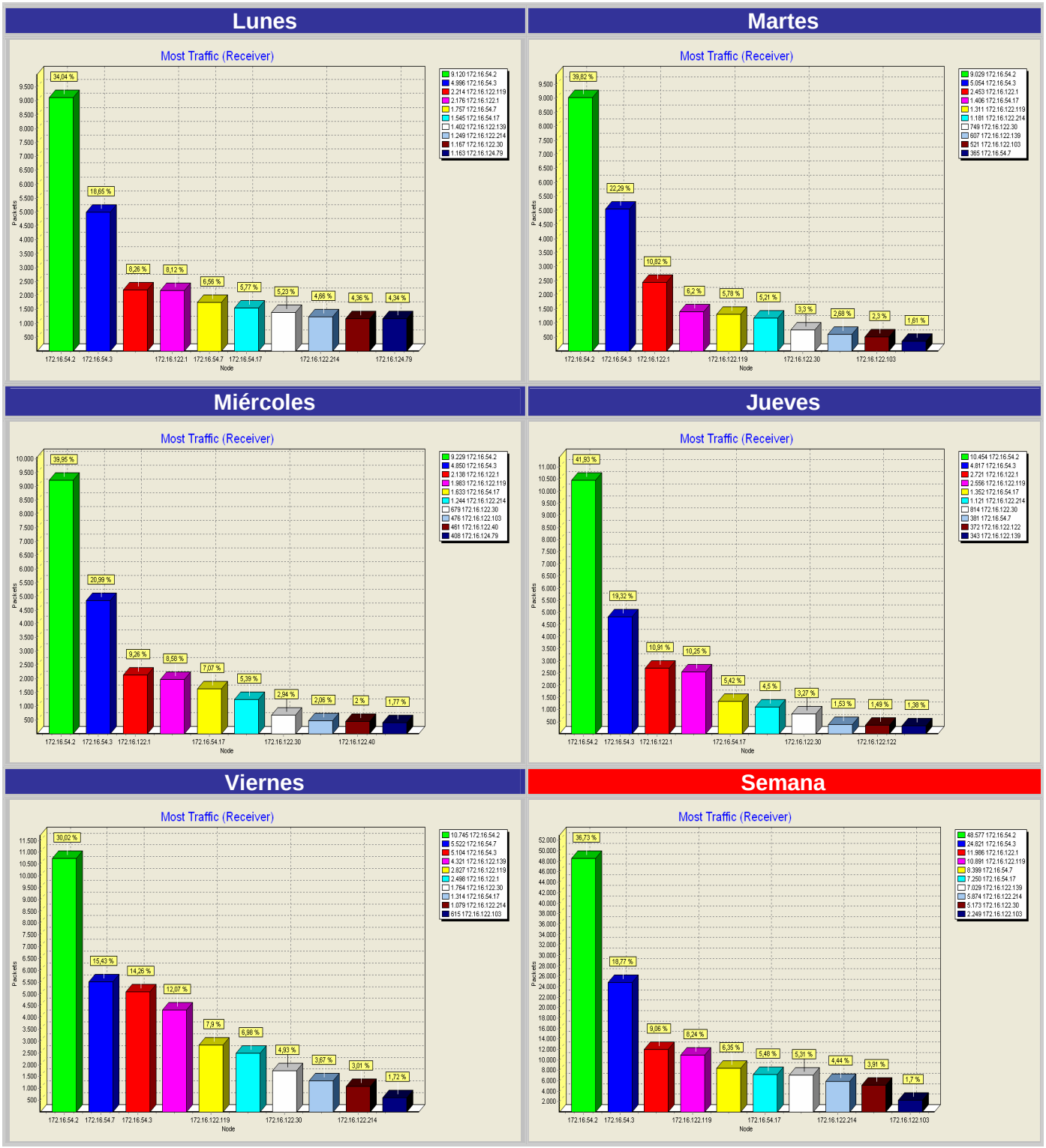


Figura B.2.8.7 Nodos de mayor tráfico recibido - Sede San Gil

B.2.9 Sede Vélez

B.2.9.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Vélez

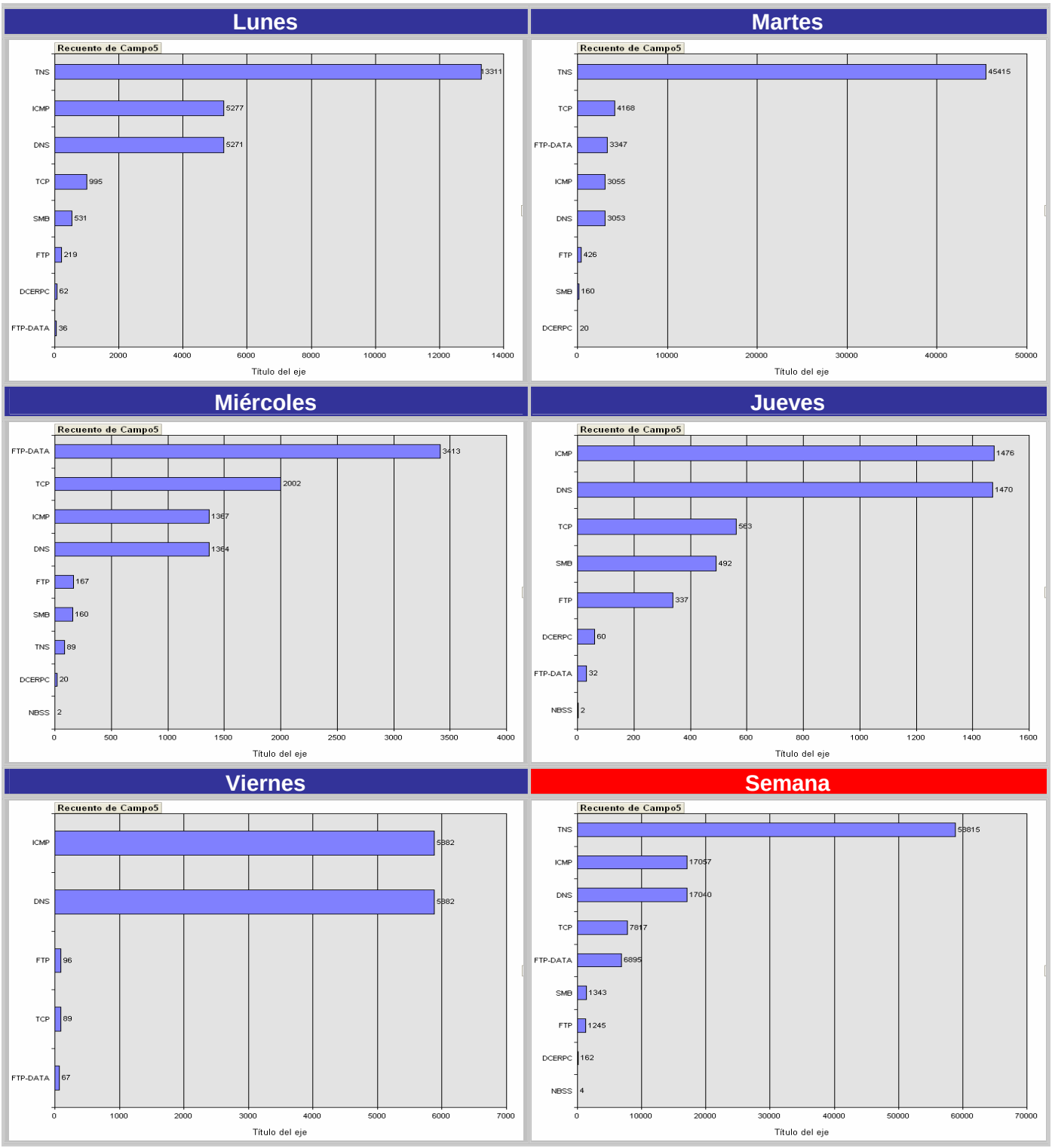


Figura B.2.9.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Vélez

B.2.9.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Vélez

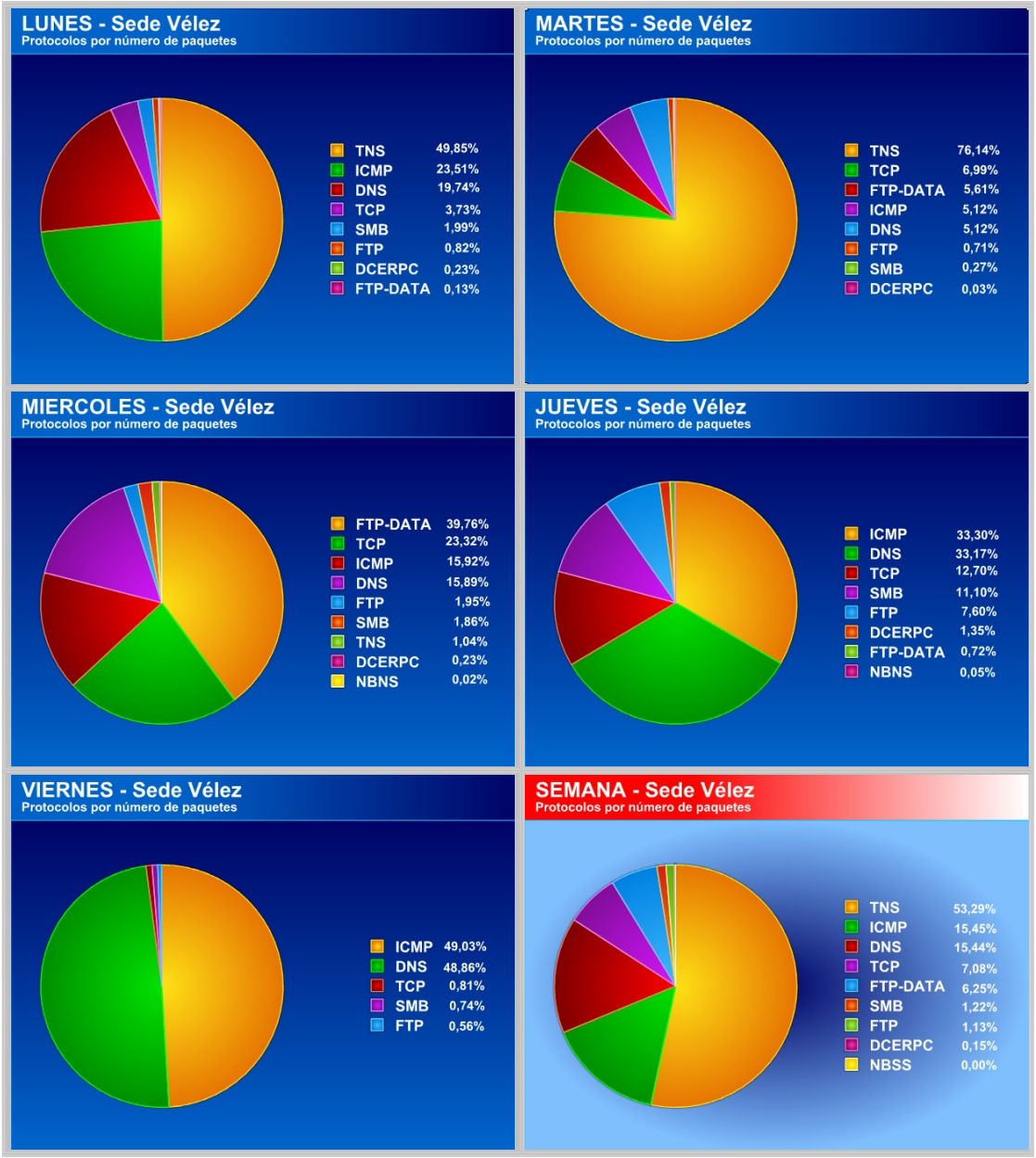


Figura B.2.9.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Vélez

B.2.9.3 Distribución de protocolos por bytes (Cantidades) - Sede Vélez

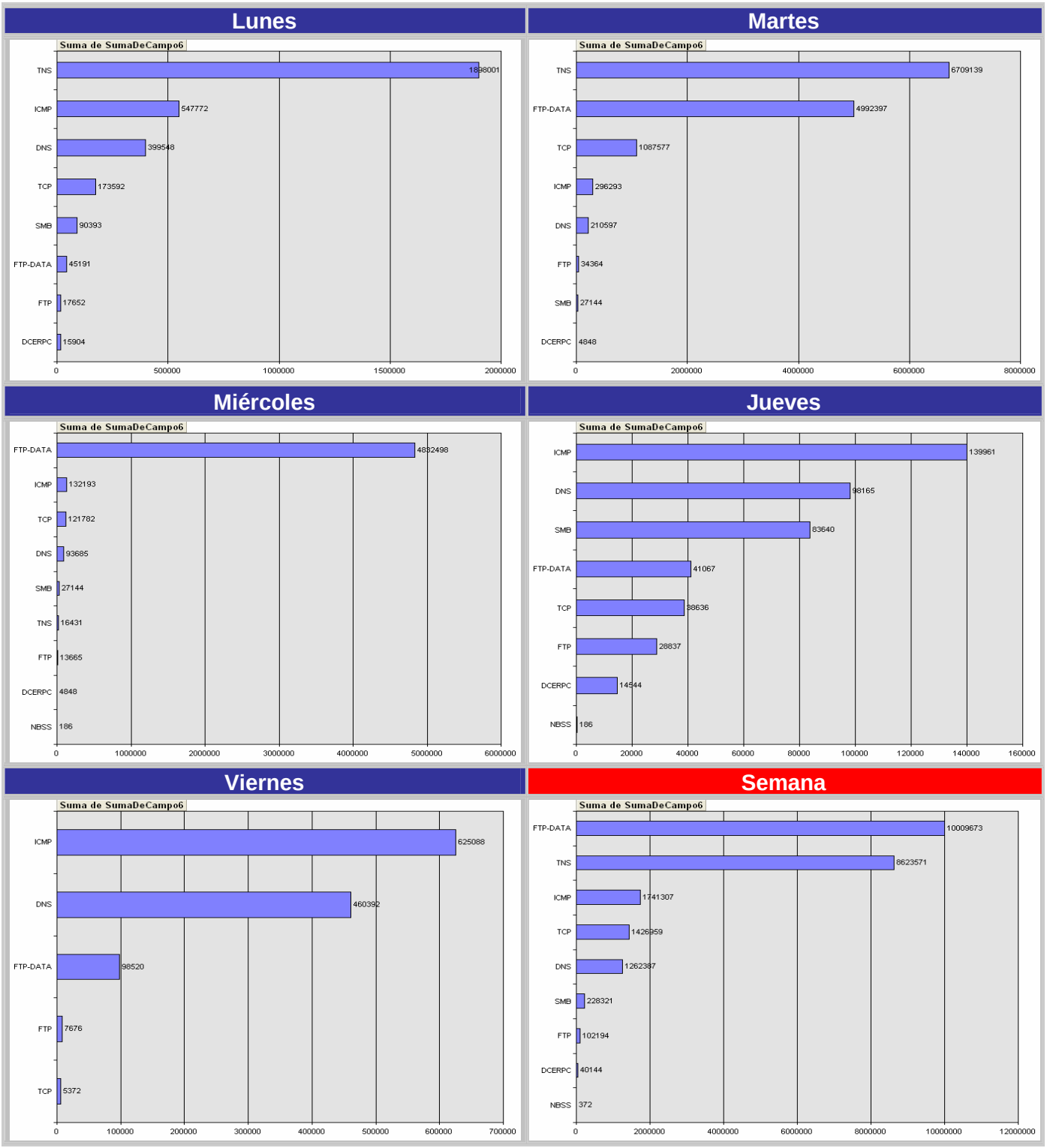


Figura B.2.9.3 Distribución de protocolos por bytes (Cantidades) - Sede Vélez

B.2.9.4 Distribución de protocolos por bytes (Porcentajes) - Sede Vélez

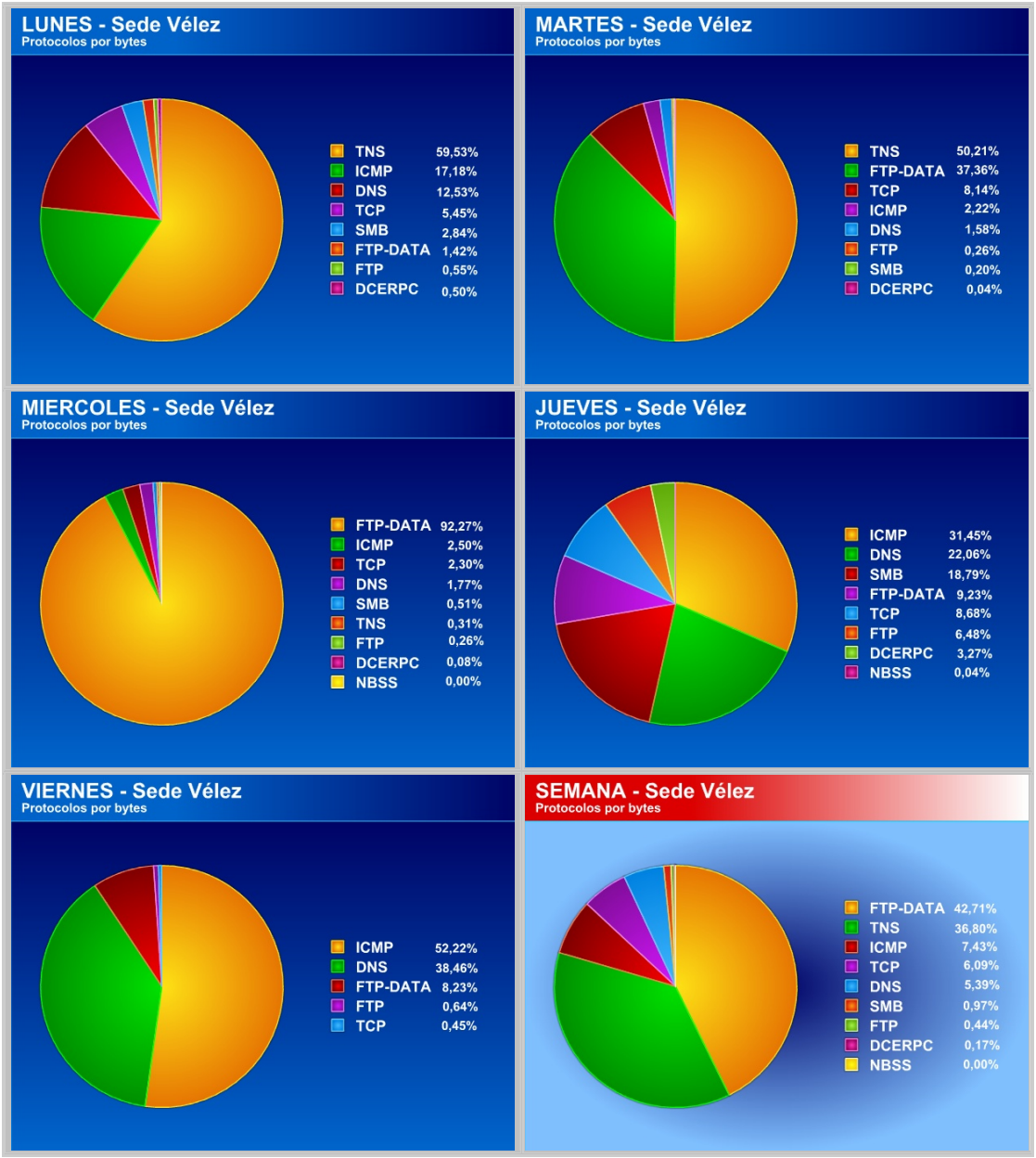


Figura B.2.9.4 Distribución de protocolos por bytes (Porcentajes) - Sede Vélez

B.2.9.5 Distribución de tamaño de paquetes - Sede Vélez

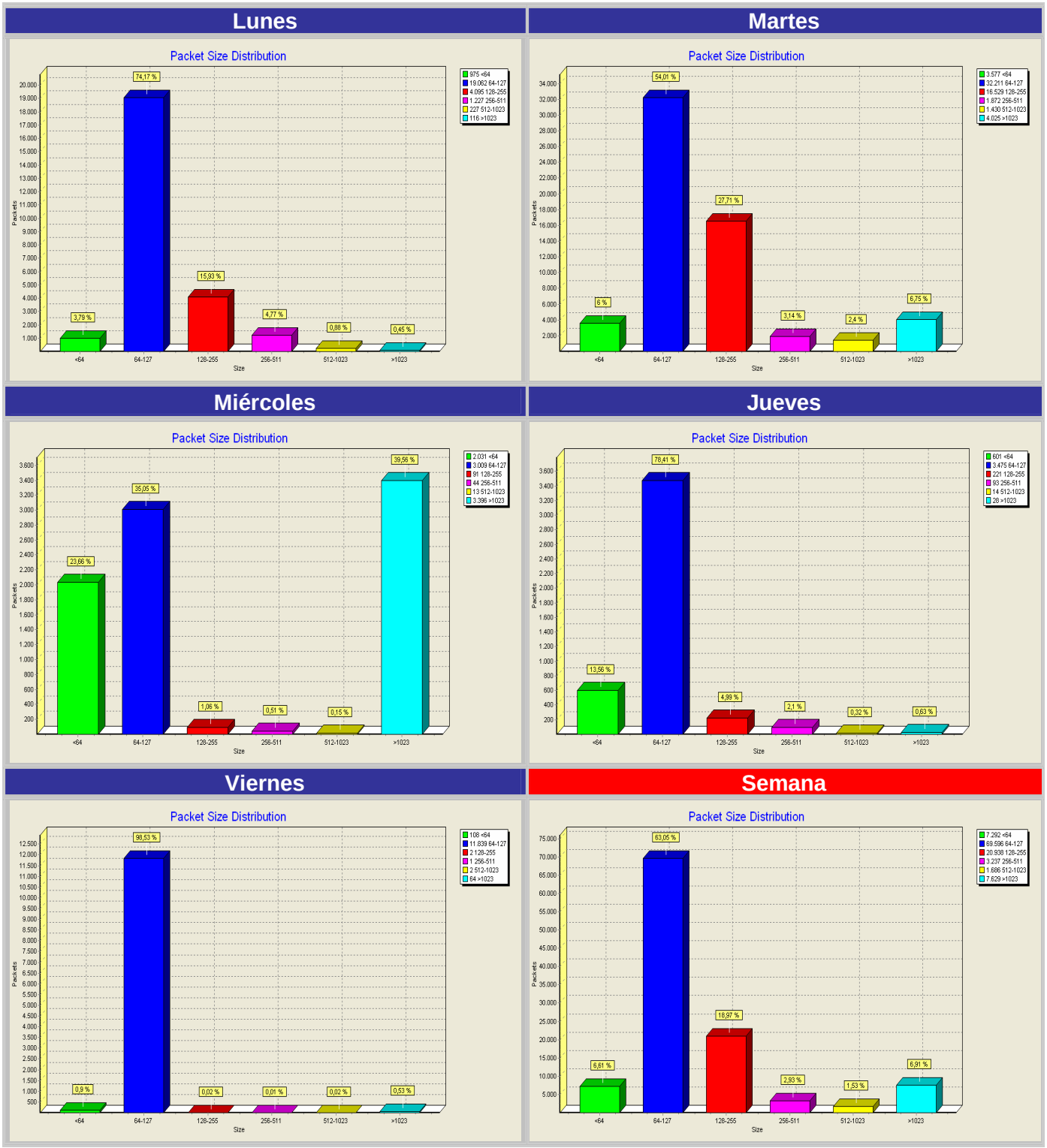


Figura B.2.9.5 Distribución de tamaño de paquetes - Sede Vélez

B.2.9.6 Nodos de mayor tráfico enviado - Sede Vélez

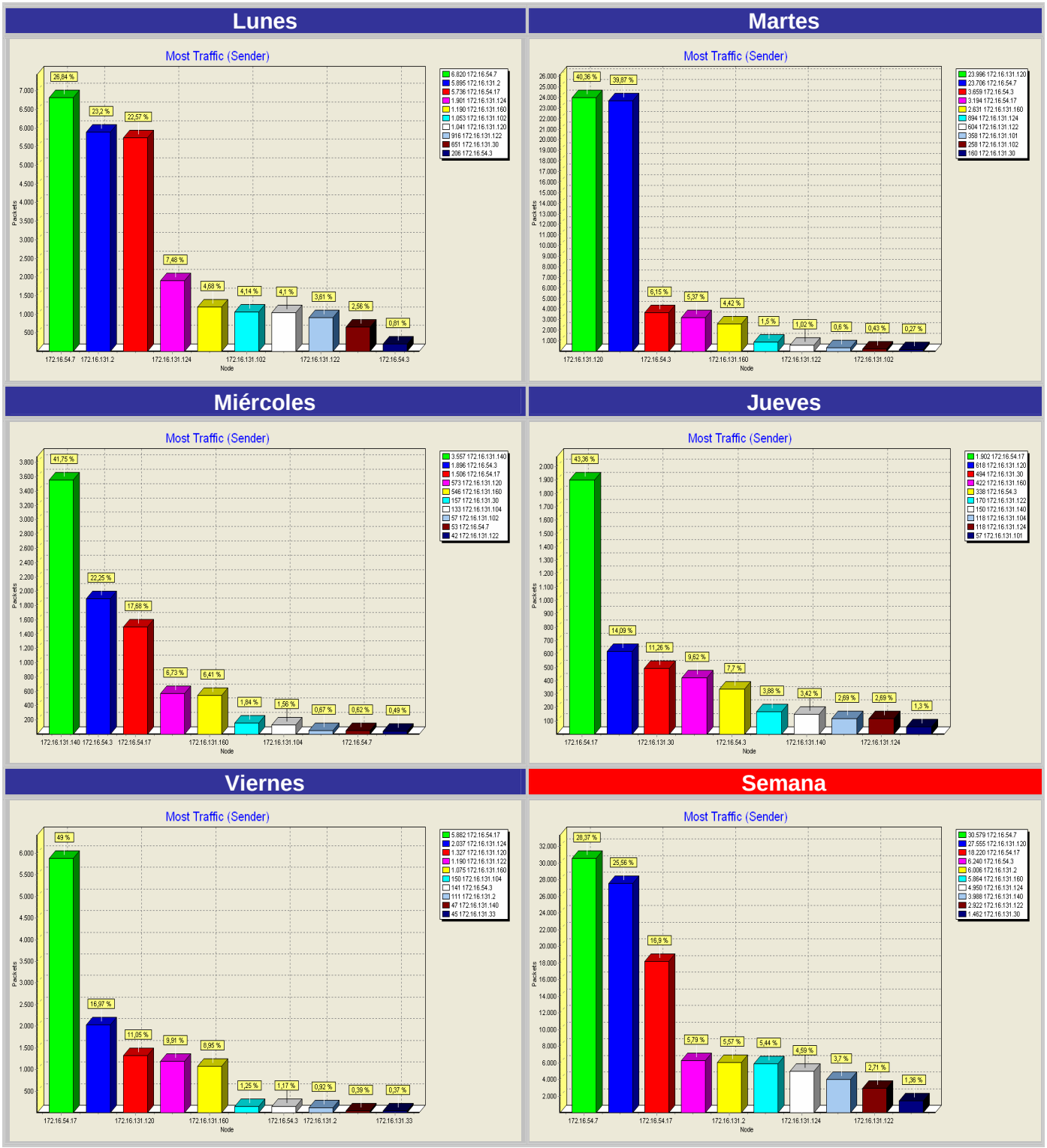


Figura B.2.9.6 Nodos de mayor tráfico enviado - Sede Vélez

B.2.9.7 Nodos de mayor tráfico recibido - Sede Vélez

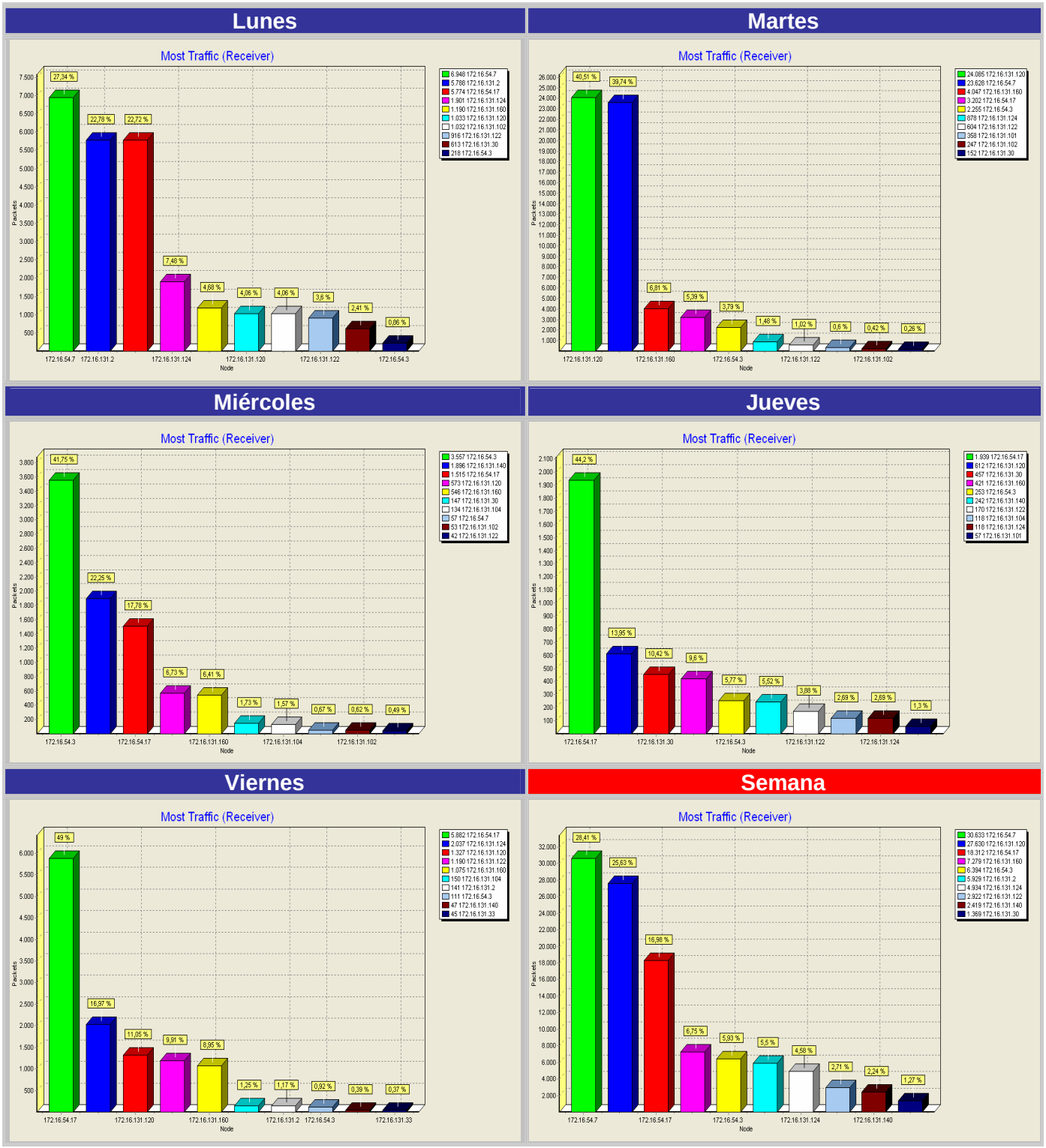


Figura B.2.9.7 Nodos de mayor tráfico recibido - Sede Vélez

B.3 Resultados Gráficos de la Caracterización del Tráfico Router Cisco

B.3.1 Sede Administrativa

B.3.1.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Sede Administrativa

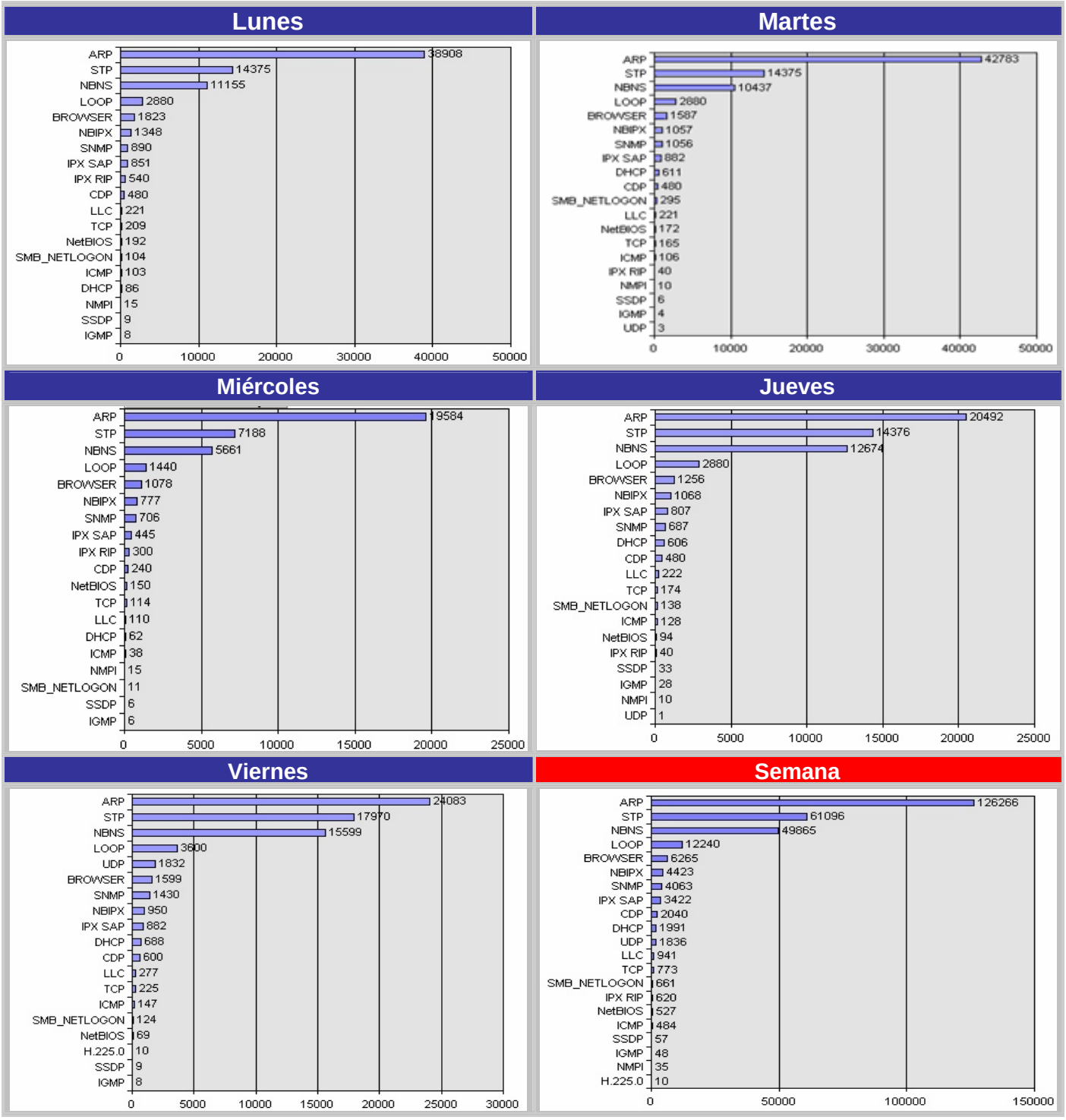


Figura B.3.1.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Sede Administrativa

B.3.1.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Sede Administrativa

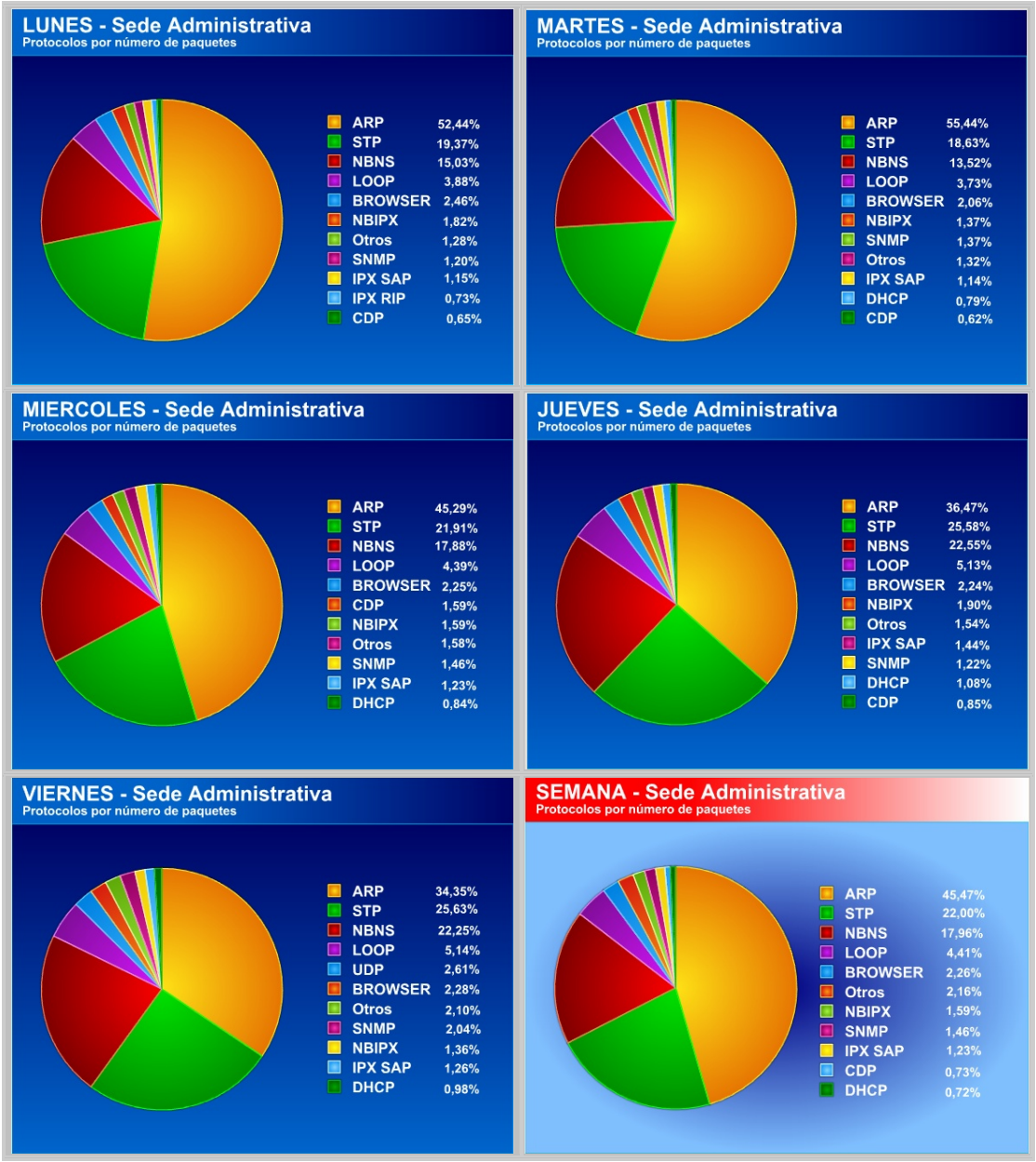


Figura B.3.1.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Sede Administrativa

B.3.1.3 Distribución de protocolos por bytes (Cantidades) - Sede Sede Administrativa

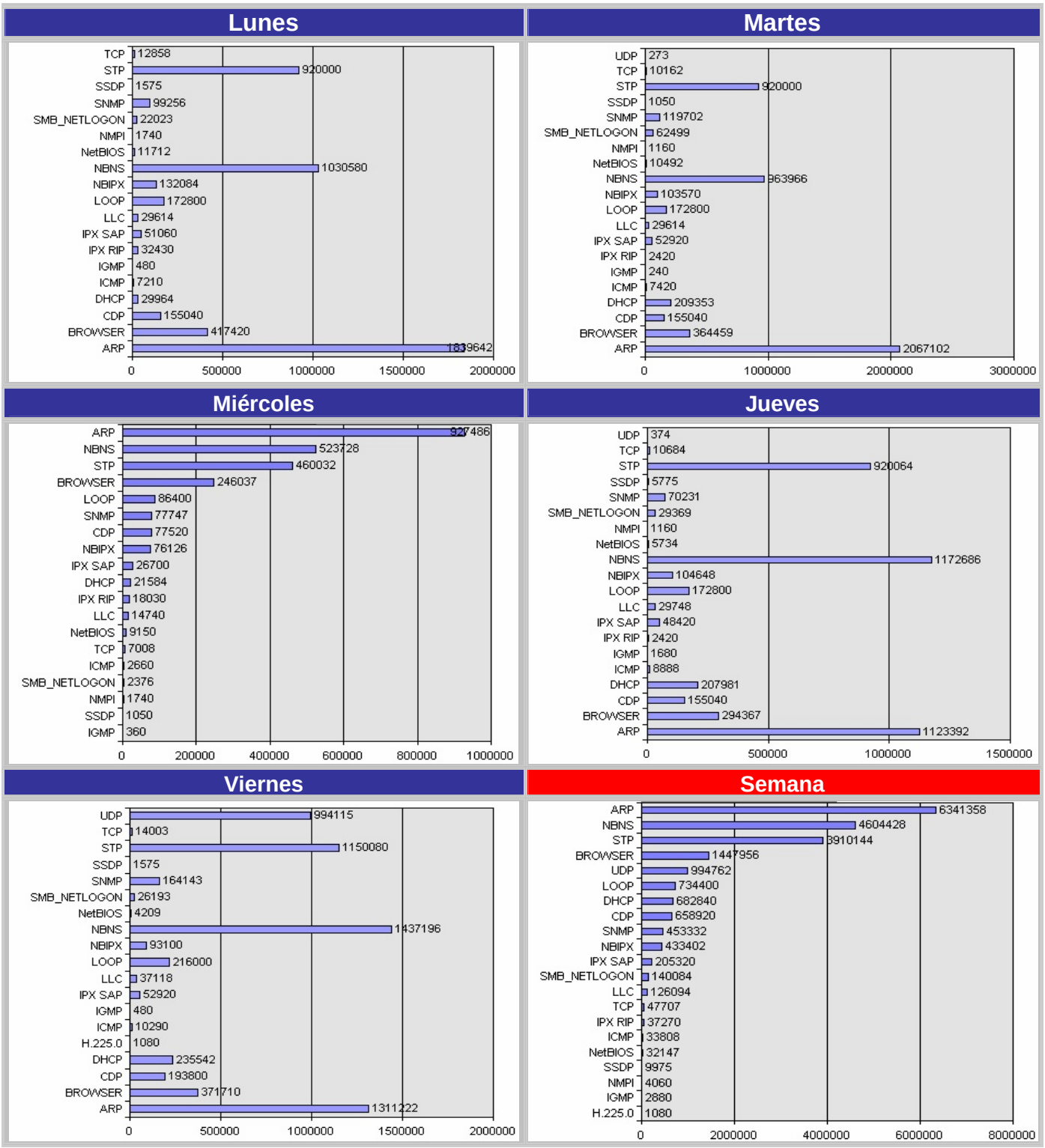


Figura B.3.1.3 Distribución de protocolos por bytes (Cantidades) - Sede Sede Administrativa

B.3.1.4 Distribución de protocolos por bytes (Porcentajes) - Sede Sede Administrativa

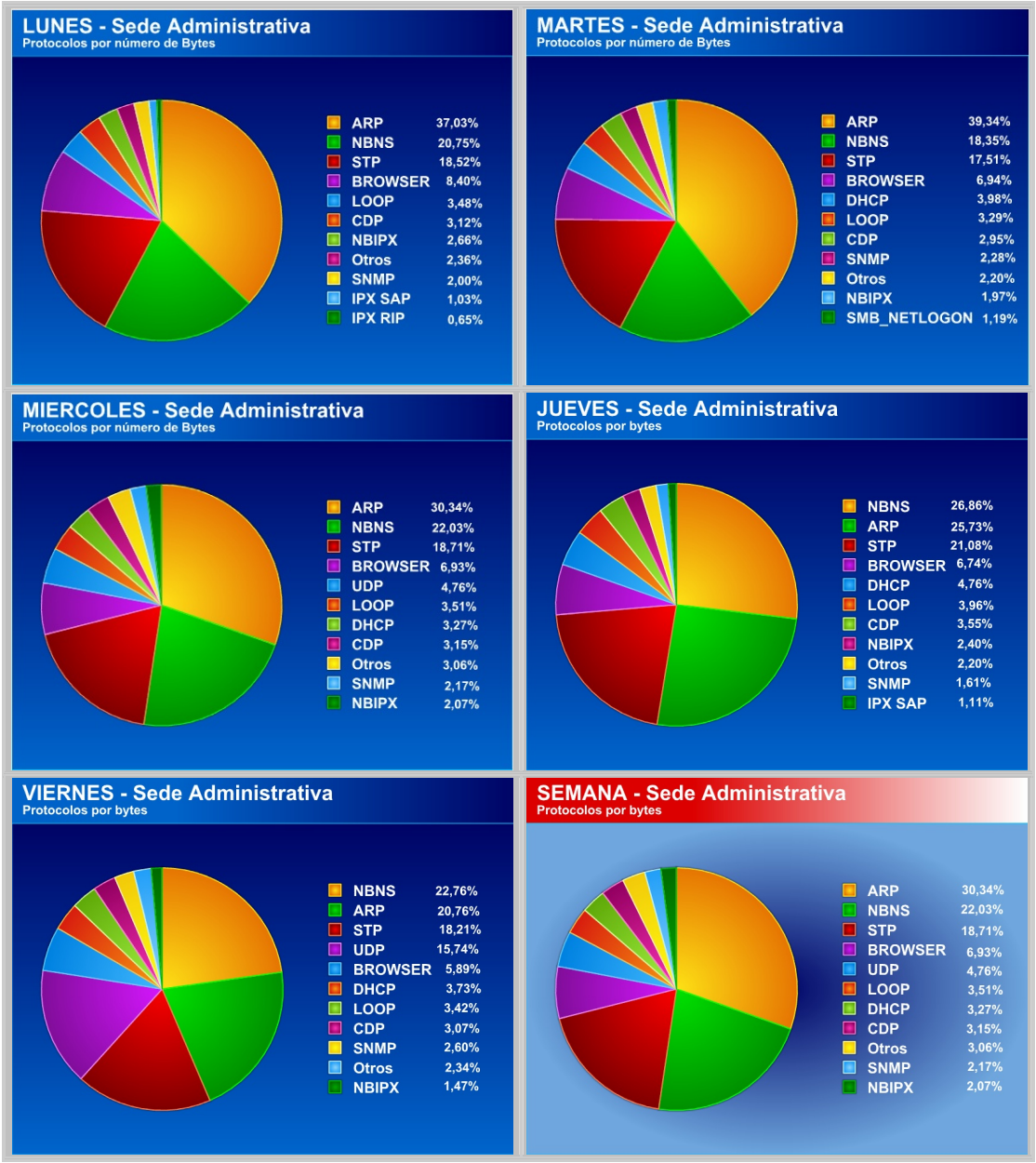


Figura B.3.1.4 Distribución de protocolos por bytes (Porcentajes) - Sede Sede Administrativa

B.3.1.5 Distribución de tamaño de paquetes - Sede Sede Administrativa

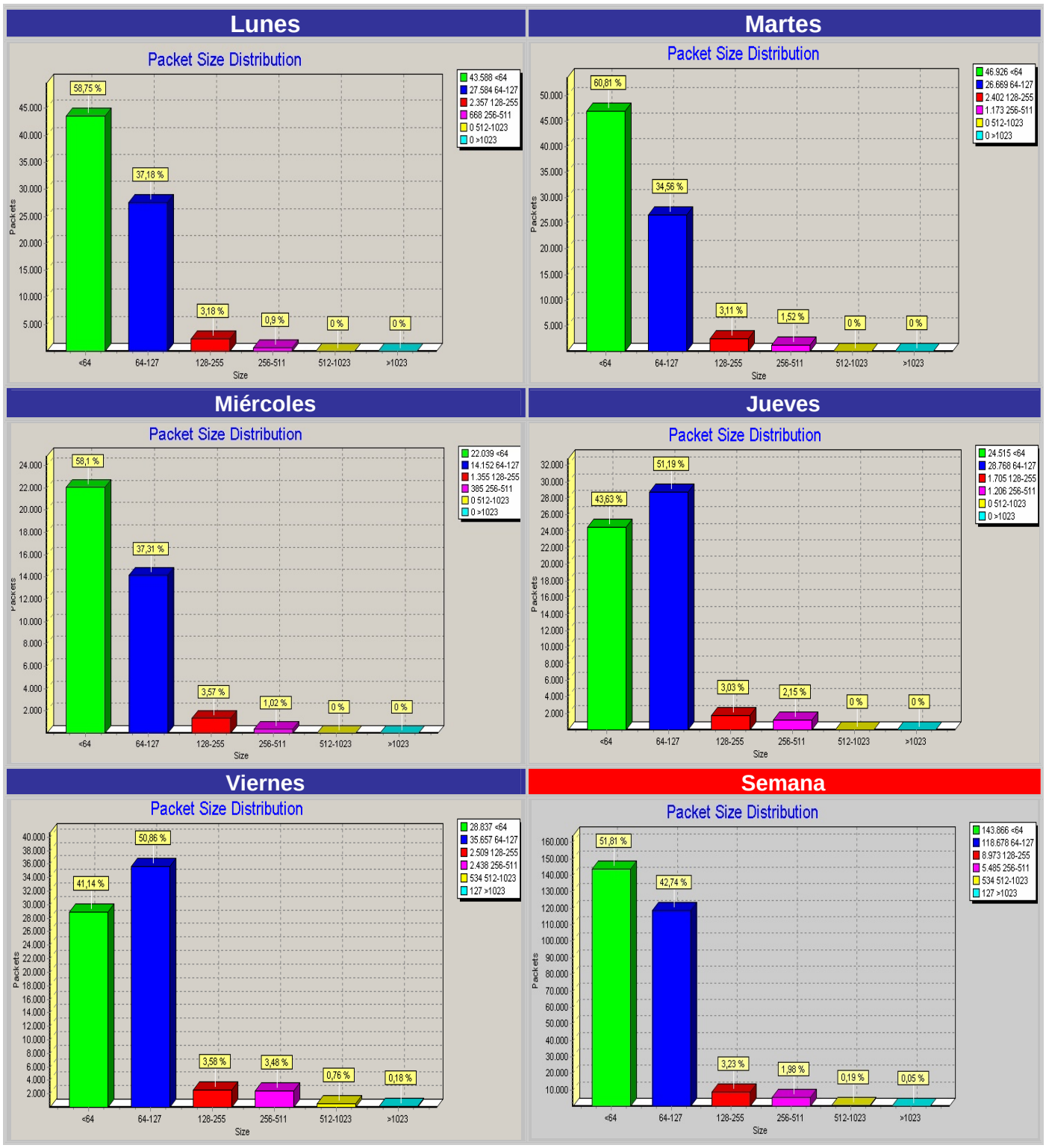


Figura B.3.1.5 Distribución de tamaño de paquetes - Sede Sede Administrativa

B.3.1.6. Distribución de modos de direccionamiento (Unicast, Multicast y Broadcast) - Sede Administrativa

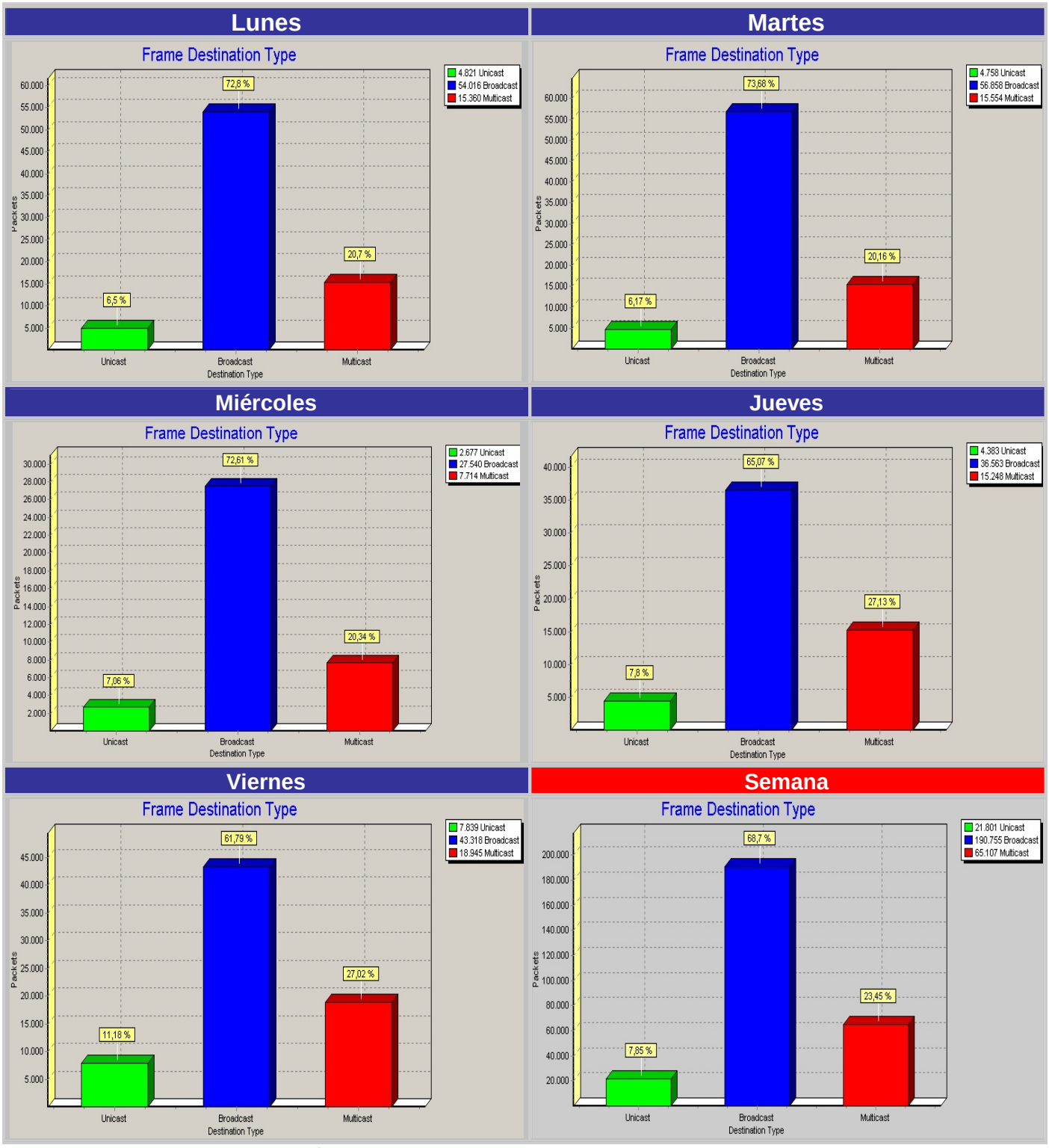


Figura B.3.1.6 Distribución de modos de direccionamiento- (Unicast, Multicast y Broadcast) - Sede Sede Administrativa

B.3.1.7 Nodos de mayor tráfico enviado - Sede Sede Administrativa

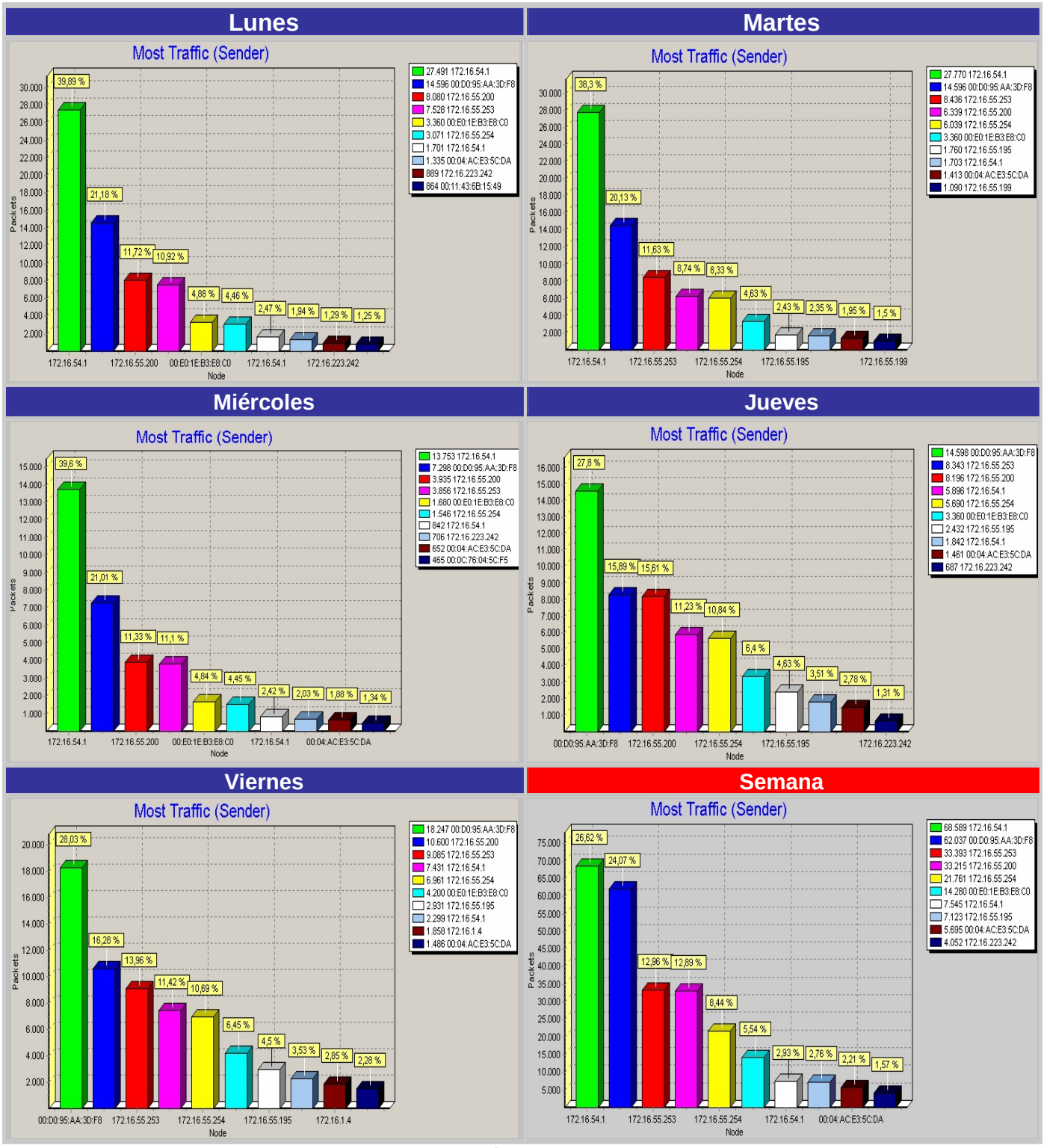


Figura B.3.1.7 Nodos de mayor tráfico enviado - Sede Sede Administrativa

B.3.1.8 Nodos de mayor tráfico recibido - Sede Sede Administrativa

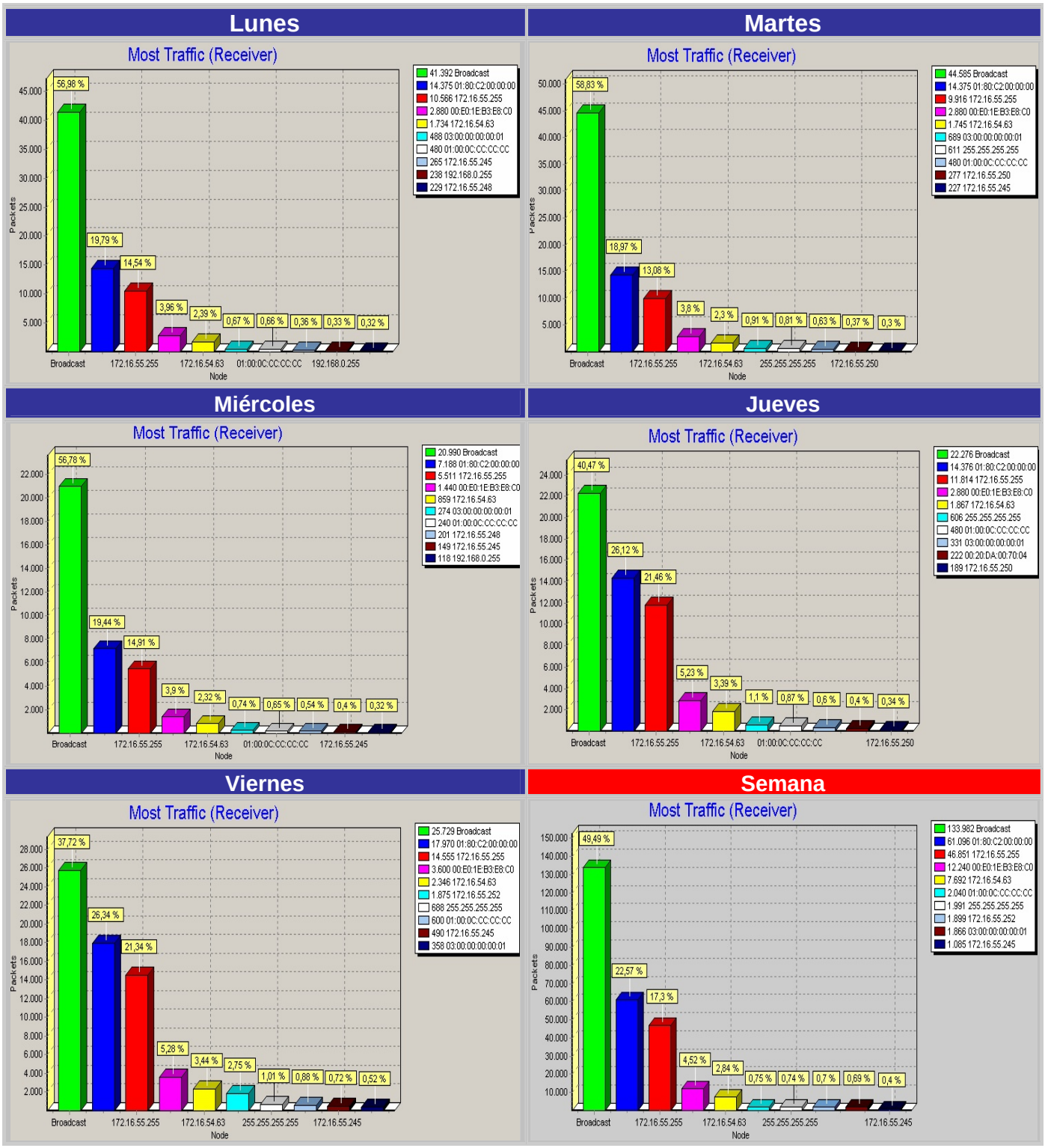


Figura B.3.1.8 Nodos de mayor tráfico recibido - Sede Sede Administrativa

B.3.2 Sede Florida

B.3.2.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Florida

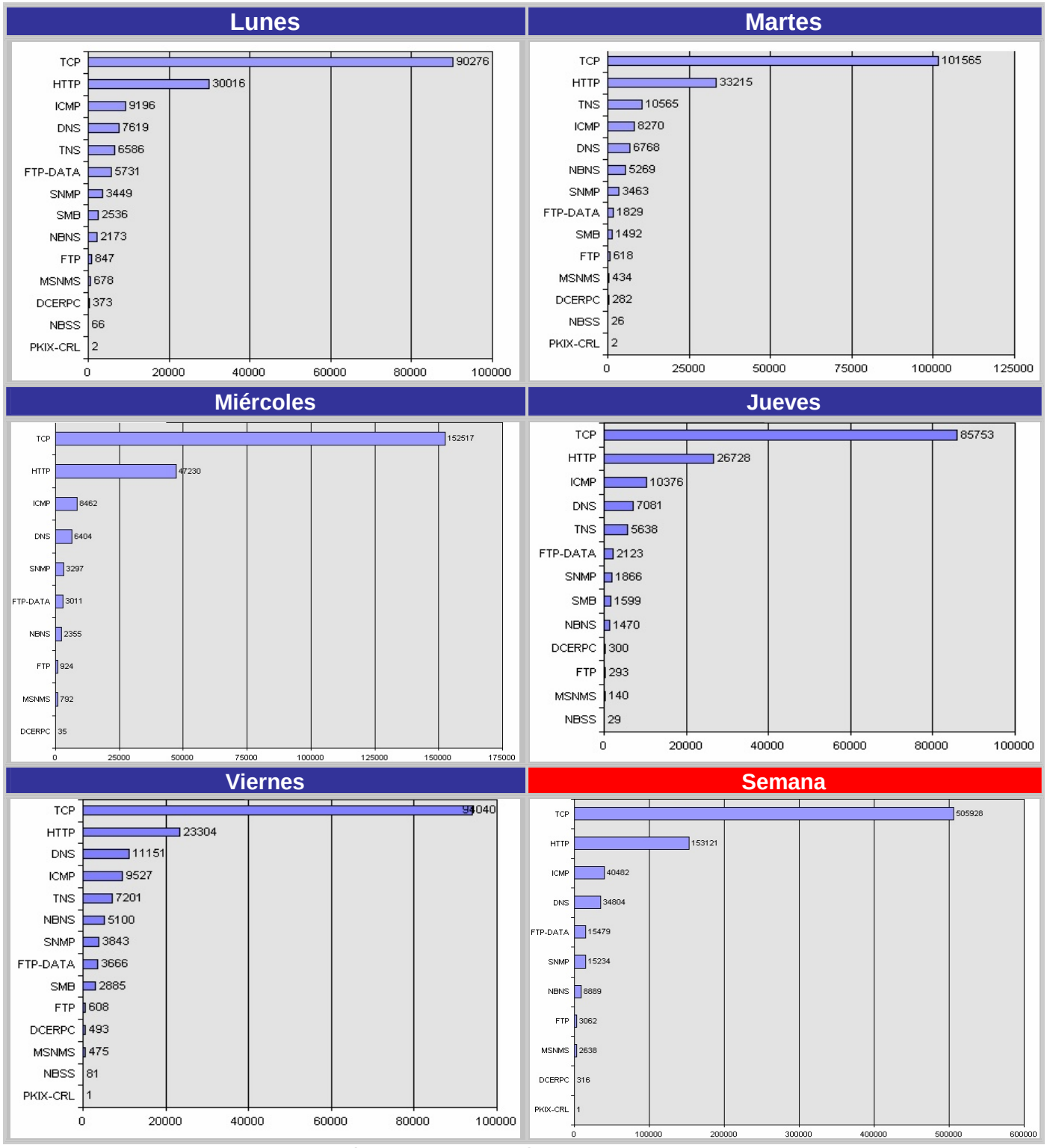


Figura B.3.2.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Florida

B.3.2.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Florida

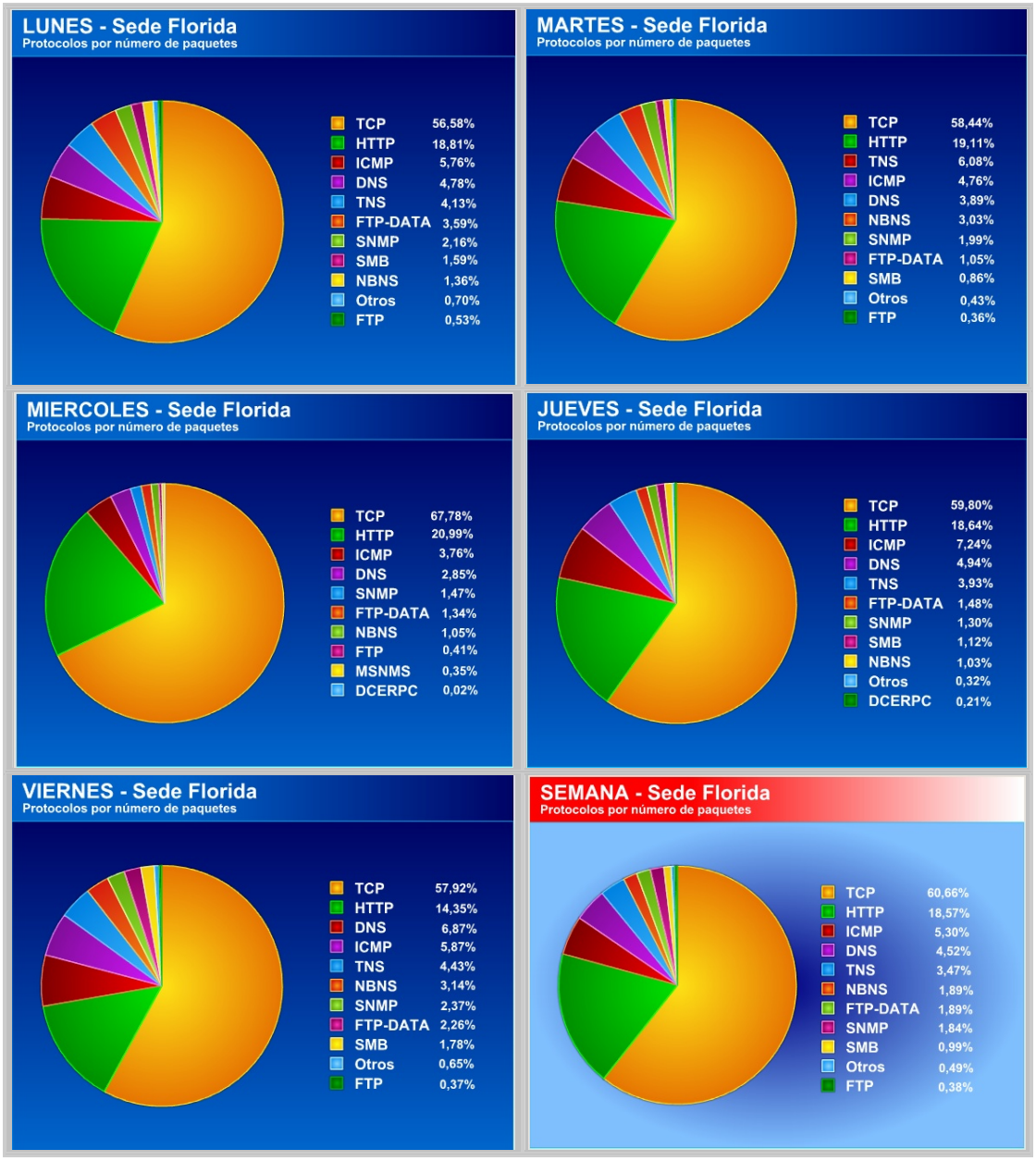


Figura B.3.2.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Florida

B.3.2.3 Distribución de protocolos por bytes (Cantidades) - Sede Florida

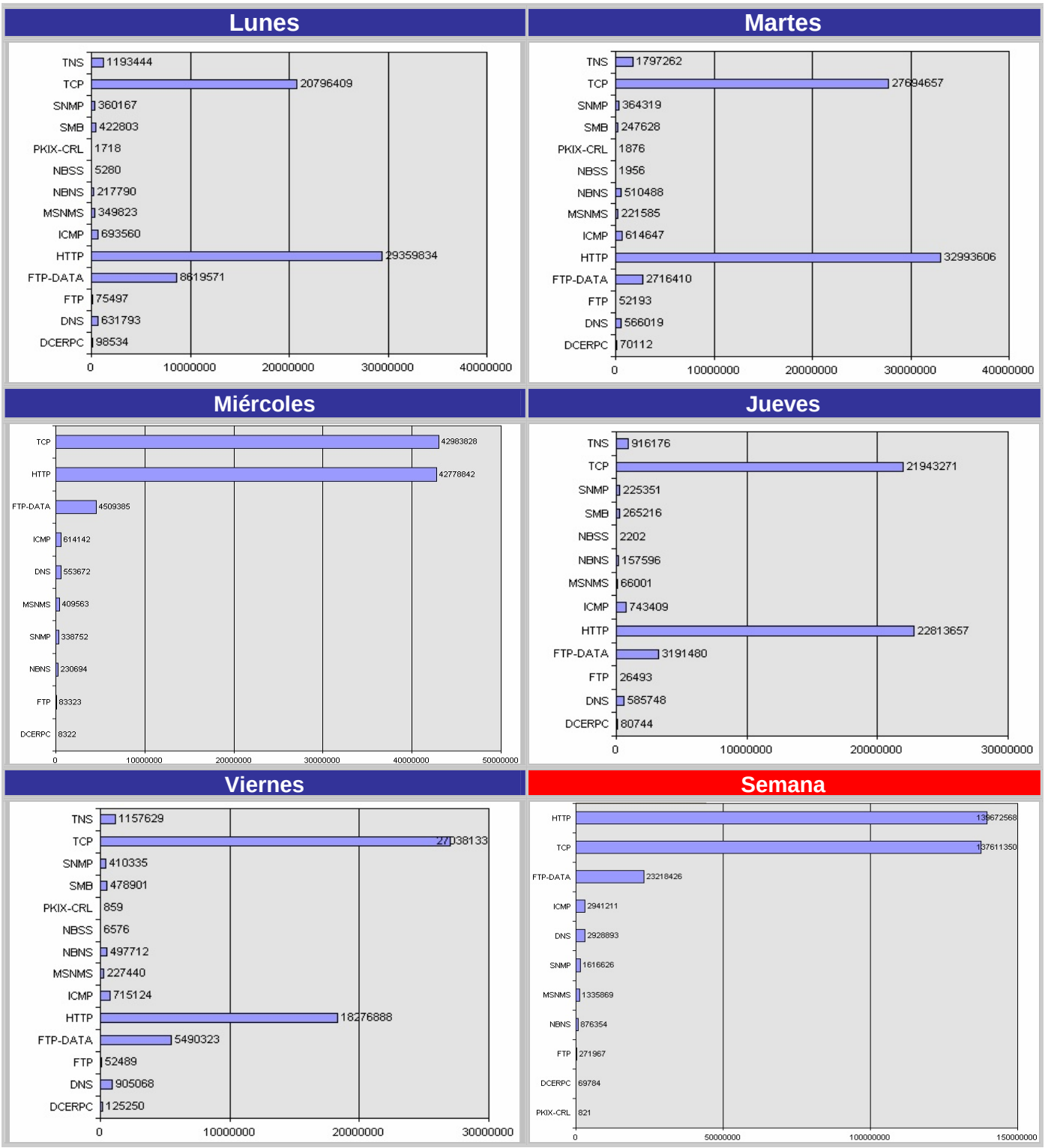


Figura B.3.2.3 Distribución de protocolos por bytes (Cantidades) - Sede Florida

B.3.2.4 Distribución de protocolos por bytes (Porcentajes) - Sede Florida

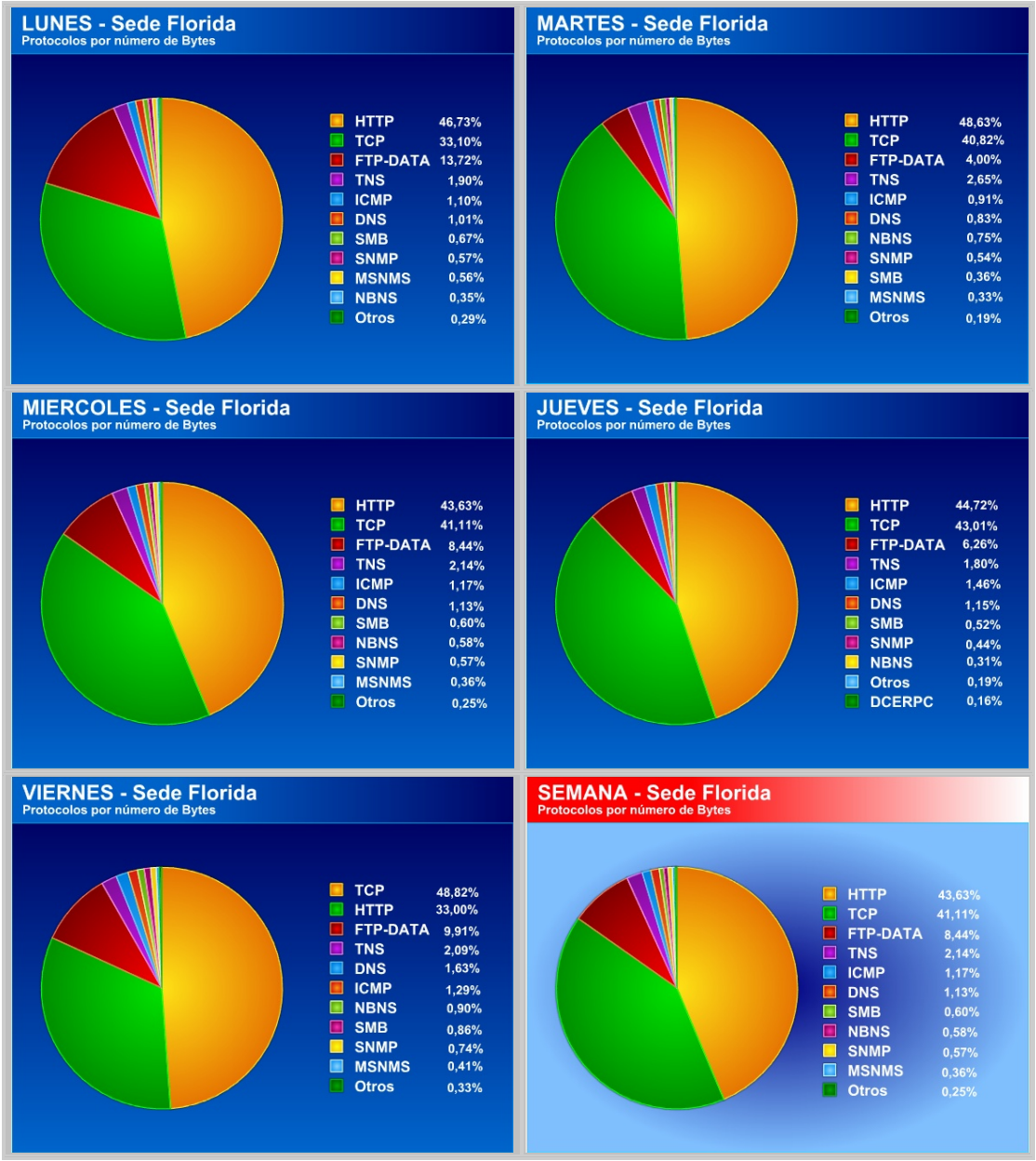


Figura B.3.2.4 Distribución de protocolos por bytes (Porcentajes) - Sede Florida

B.3.2.5 Distribución de tamaño de paquetes - Sede Florida

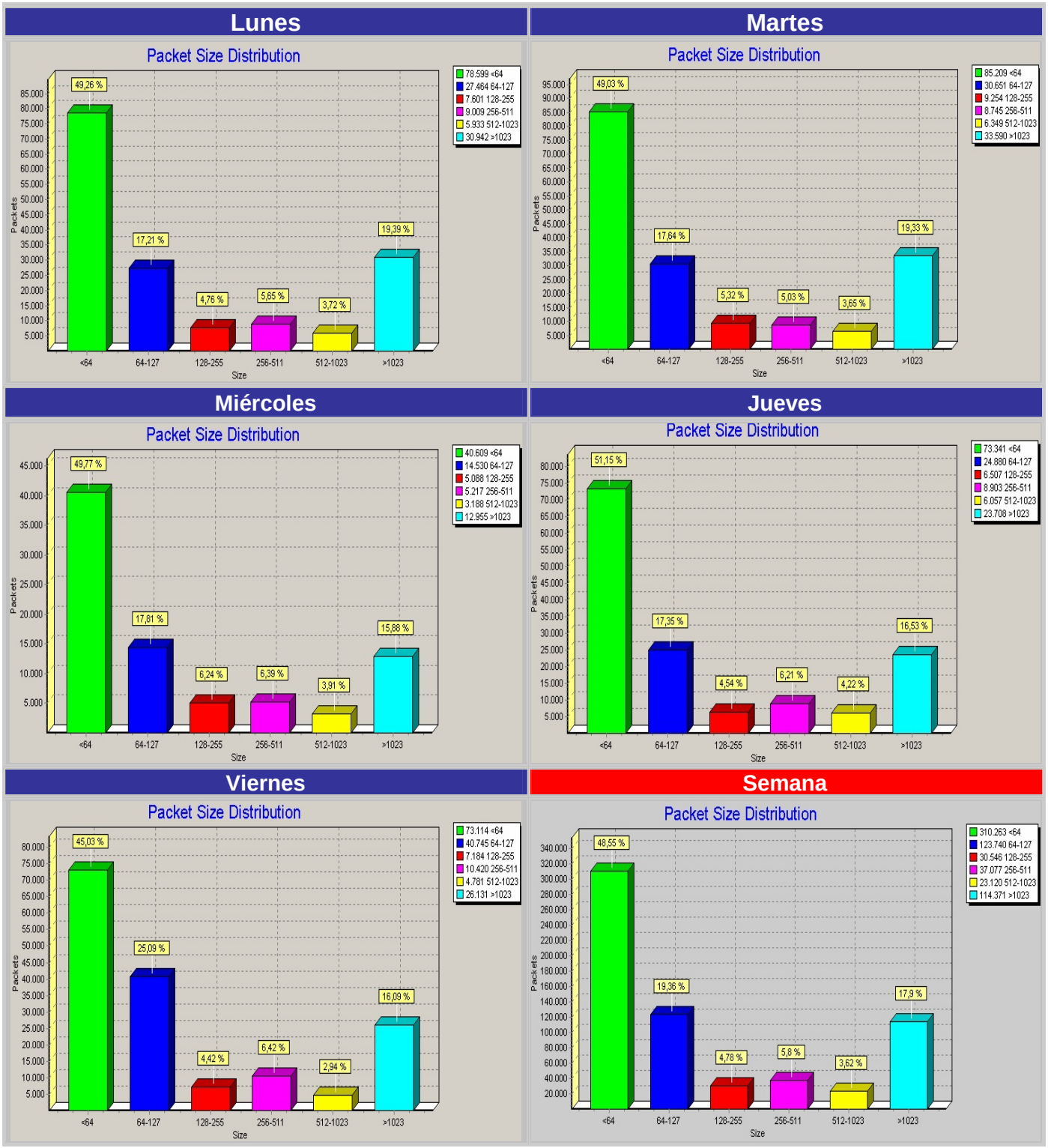


Figura B.3.2.5 Distribución de tamaño de paquetes - Sede Florida

B.3.2.6 Nodos de mayor tráfico enviado - Sede Florida

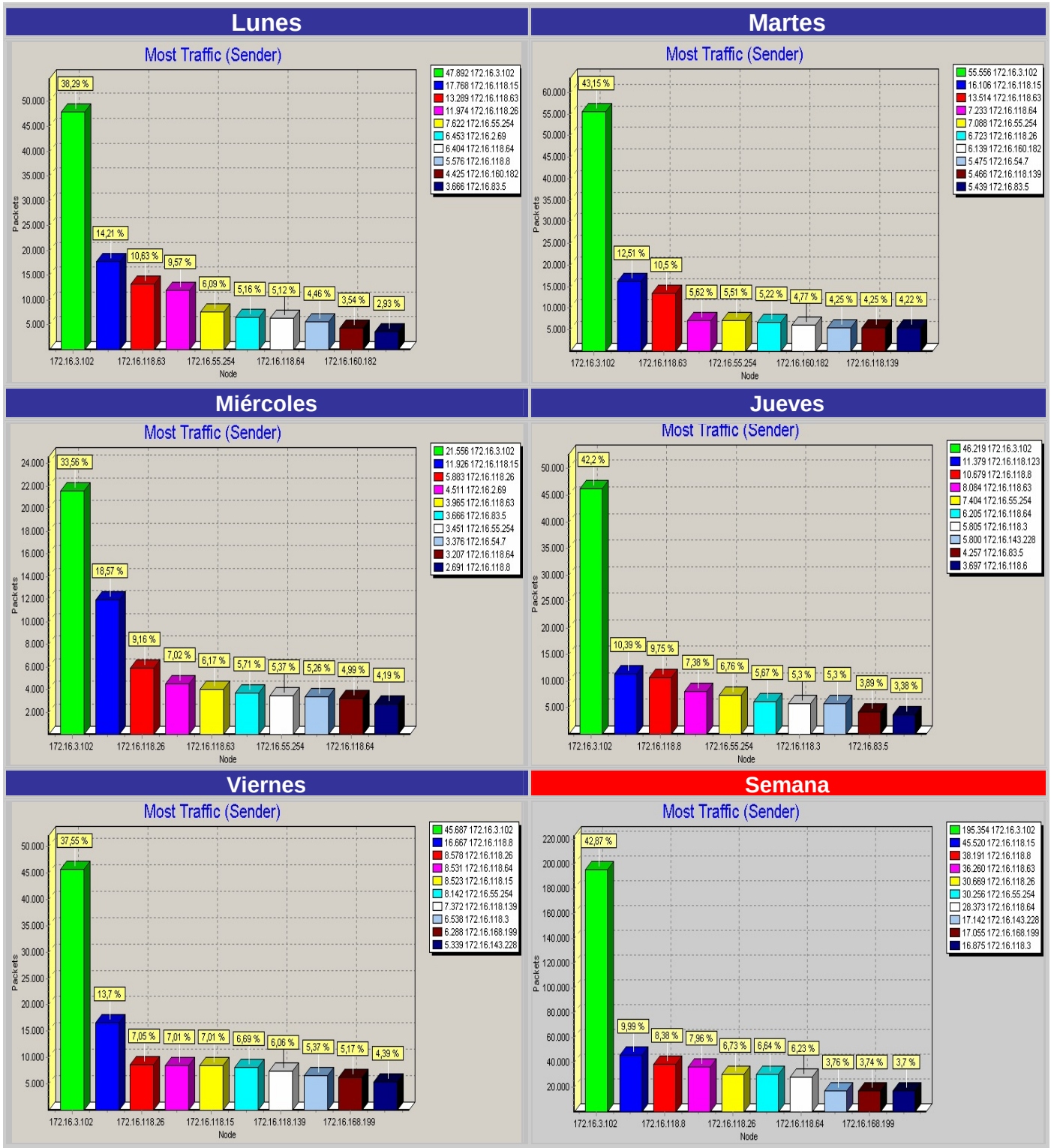


Figura B.3.2.6 Nodos de mayor tráfico enviado - Sede Florida

B.3.2.7 Nodos de mayor tráfico recibido - Sede Florida

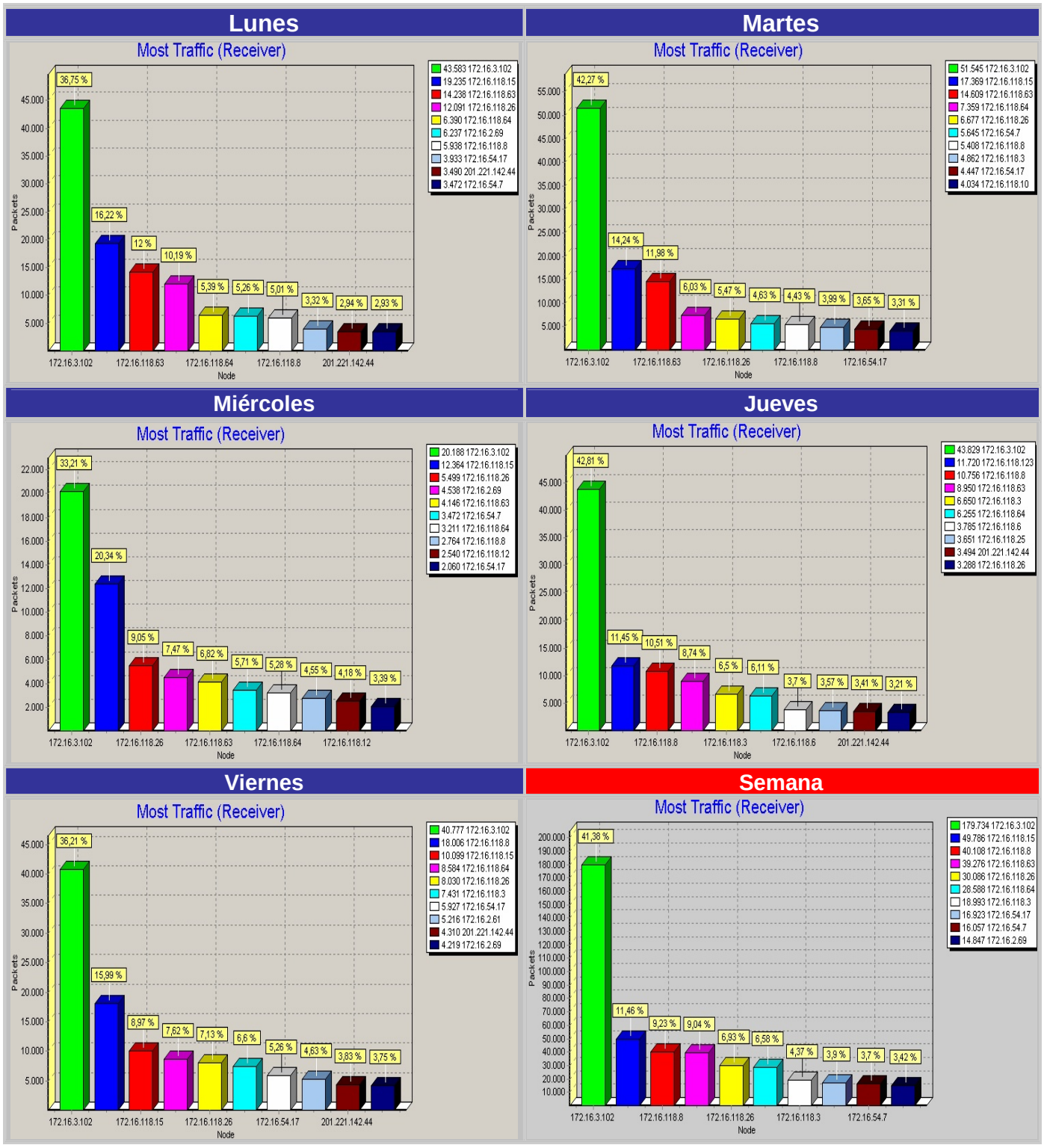


Figura B.3.2.7 Nodos de mayor tráfico recibido - Sede Florida

B.3.3 Sede Girón

B.3.3.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Girón

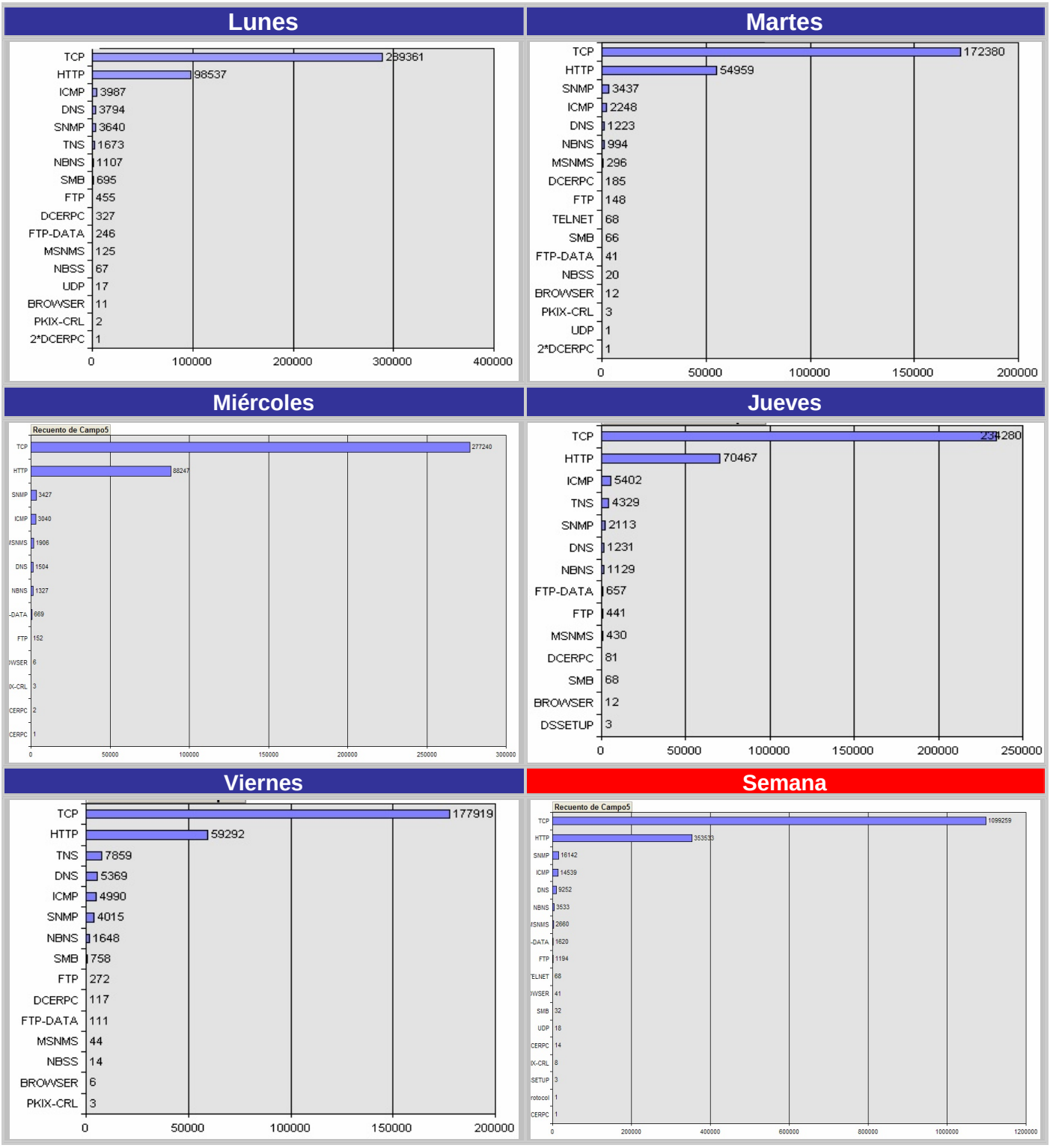


Figura B.3.3.1 Distribución de protocolos por número de paquetes (Cantidades) - Sede Girón

B.3.3.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Girón

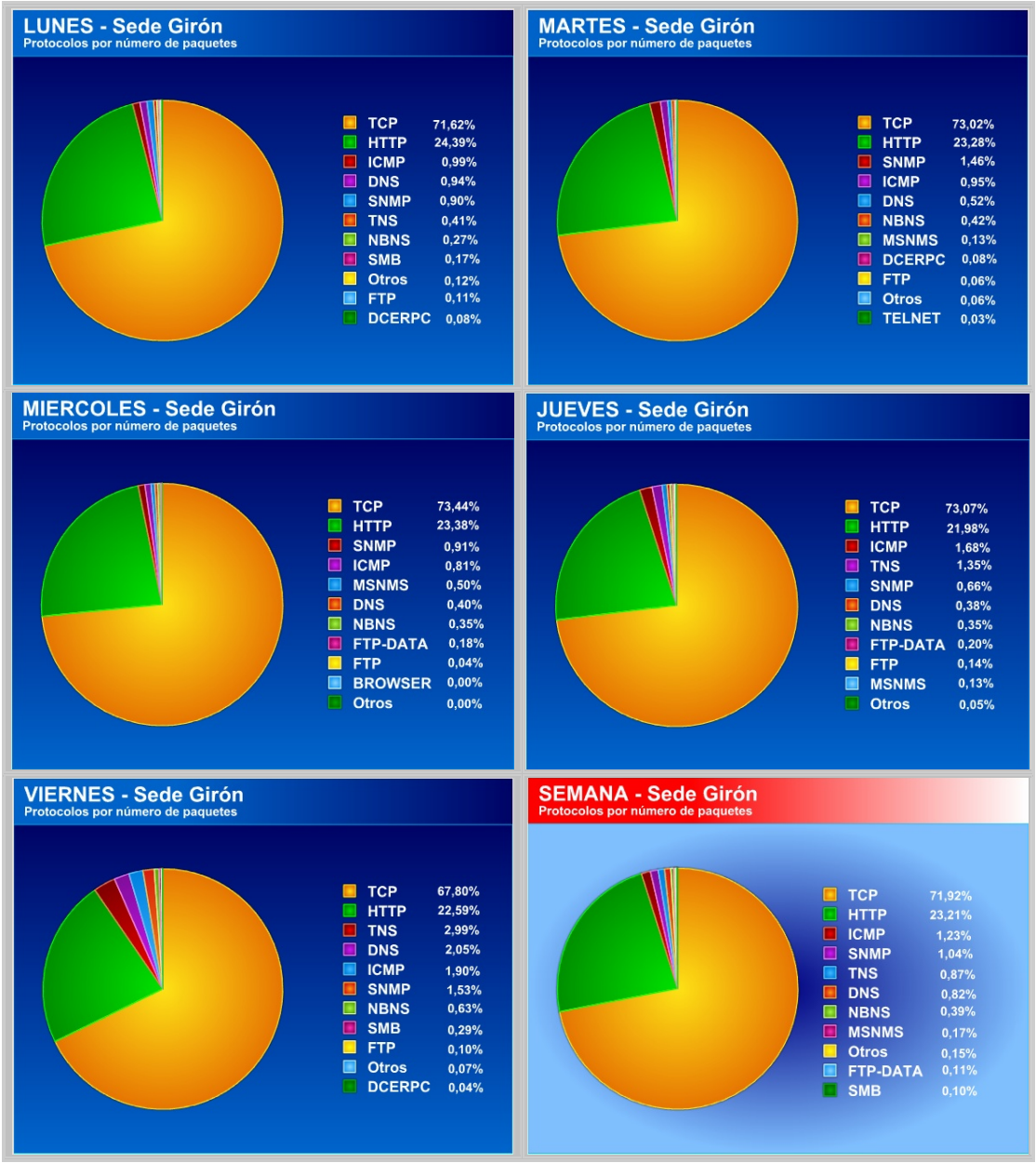


Figura B.3.3.2. Distribución de protocolos por número de paquetes (Porcentajes) - Sede Girón

B.3.3.3 Distribución de protocolos por bytes (Cantidades) - Sede Girón

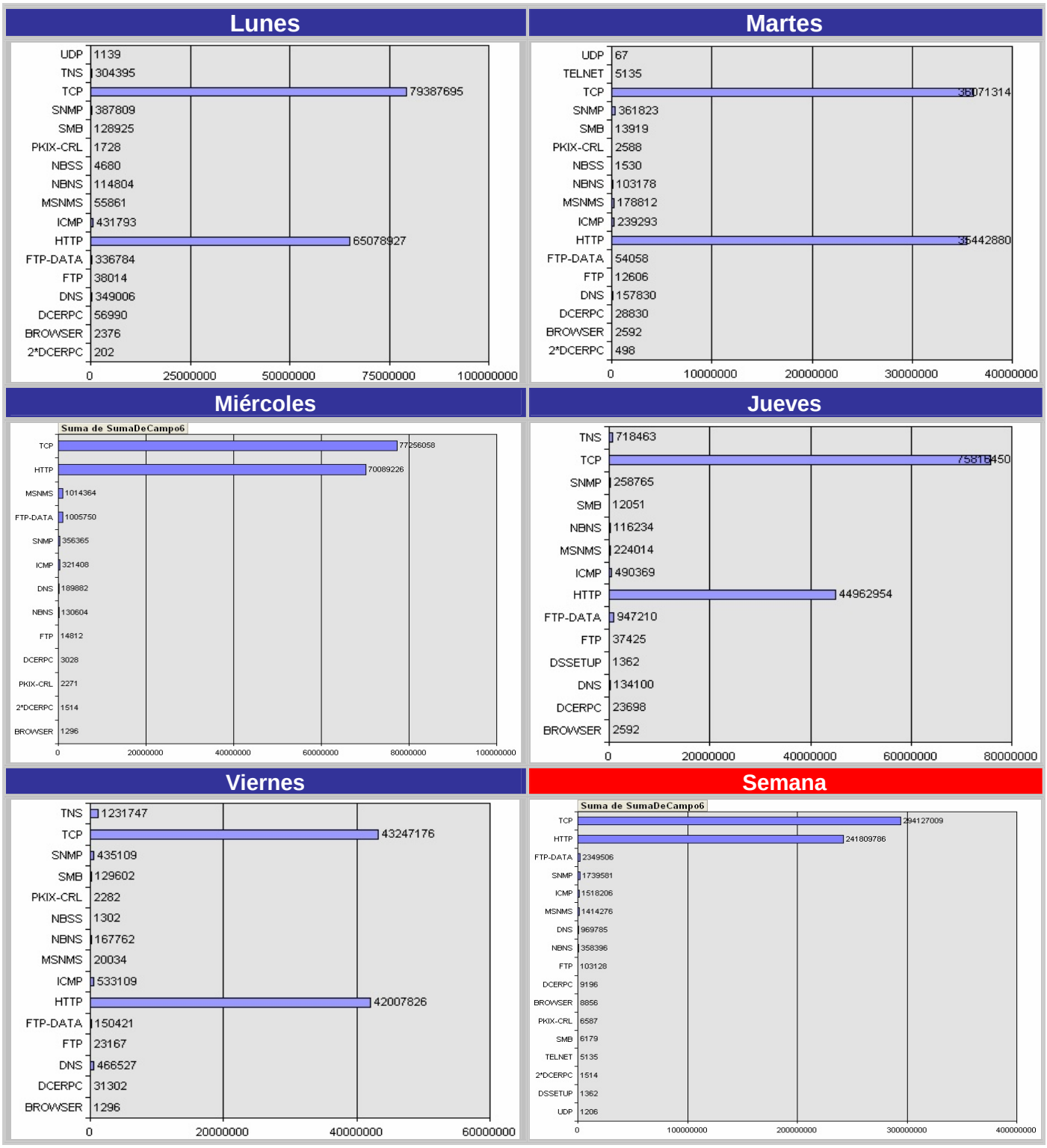


Figura B.3.3.3 Distribución de protocolos por bytes (Cantidades) - Sede Girón

B.3.3.4 Distribución de protocolos por bytes (Porcentajes) - Sede Girón

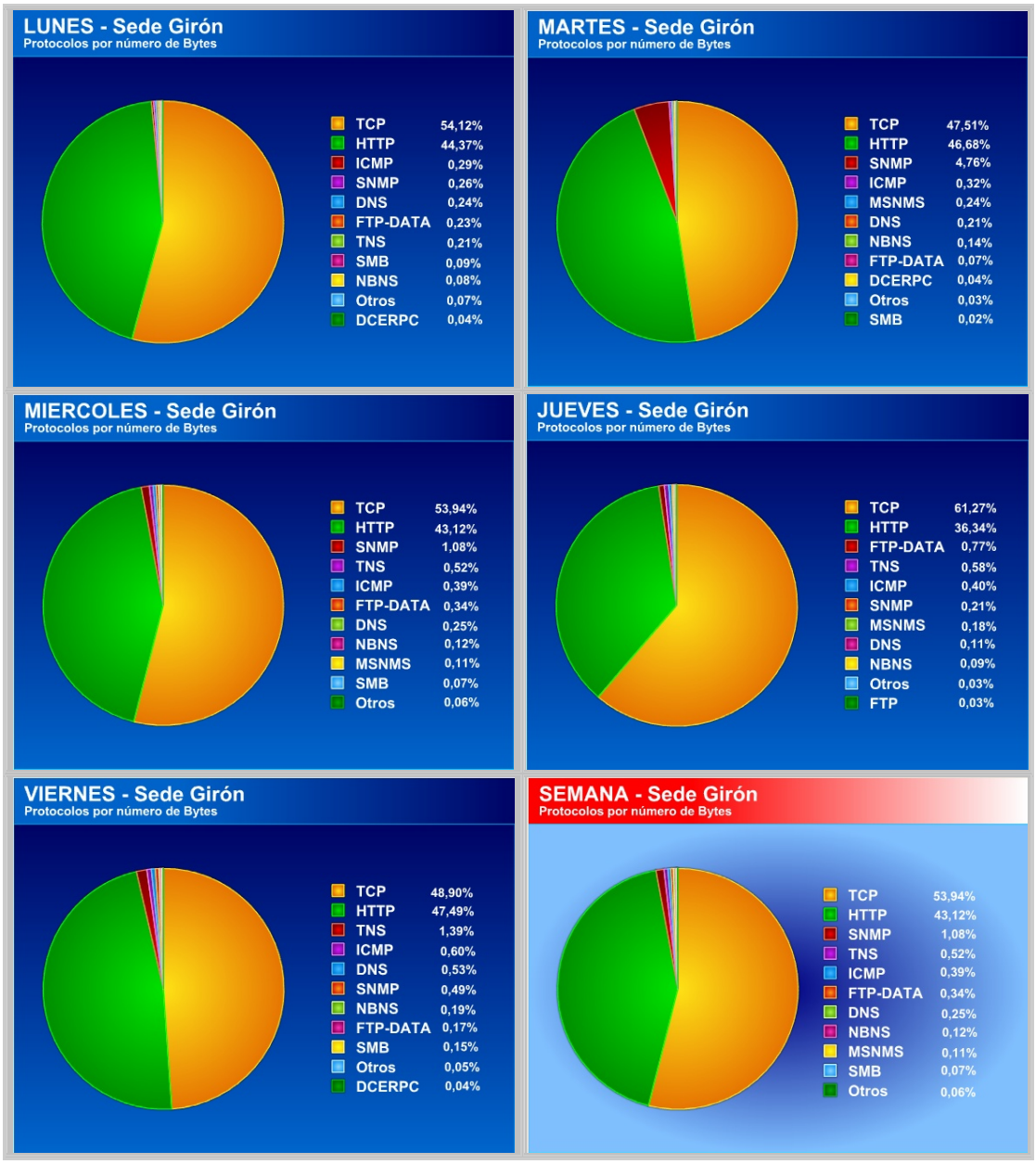


Figura B.3.3.4 Distribución de protocolos por bytes (Porcentajes) - Sede Girón

B.3.3.5 Distribución de tamaño de paquetes - Sede Girón

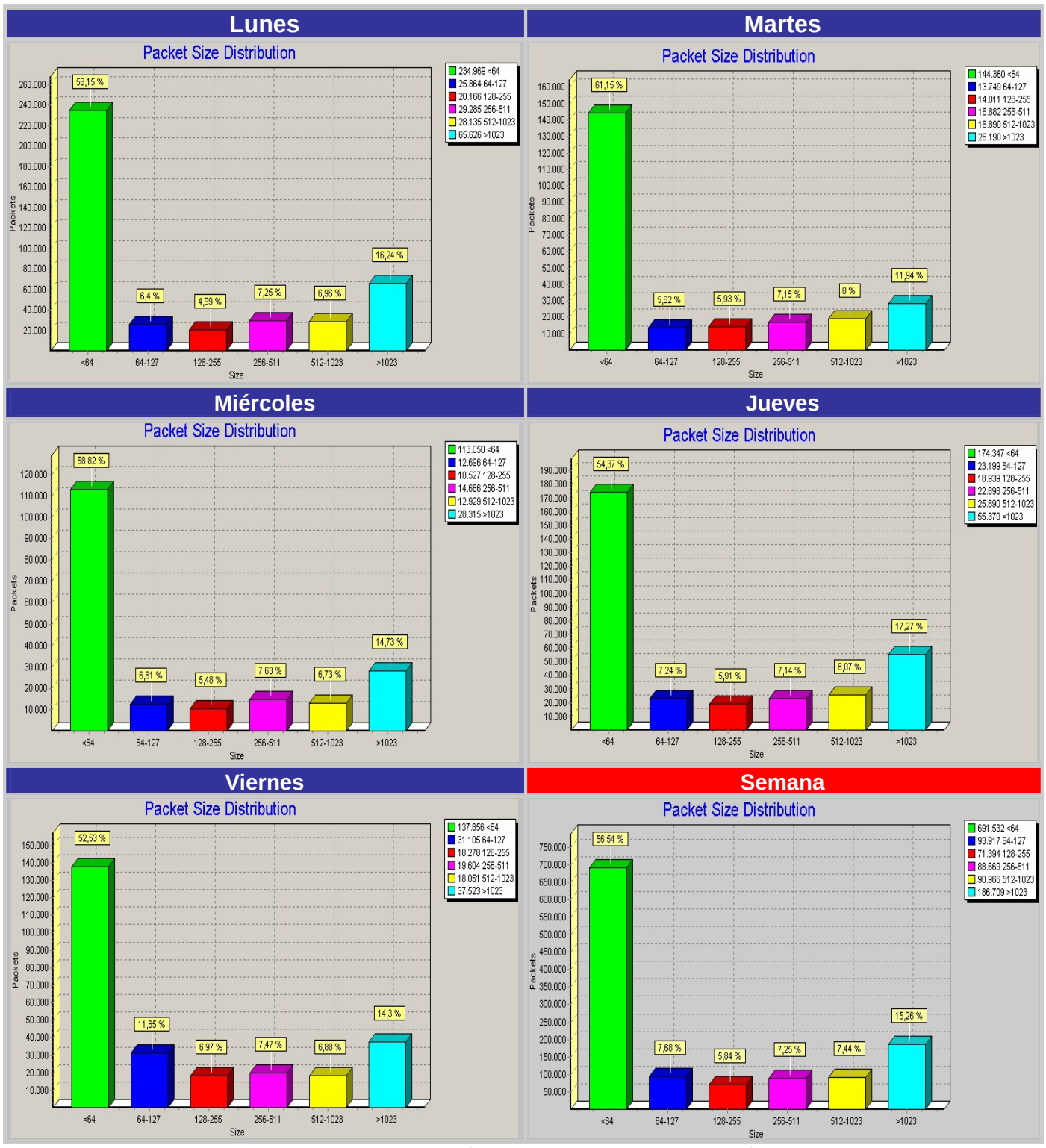


Figura B.3.3.5 Distribución de tamaño de paquetes - Sede Girón

B.3.3.6 Nodos de mayor tráfico enviado - Sede Girón

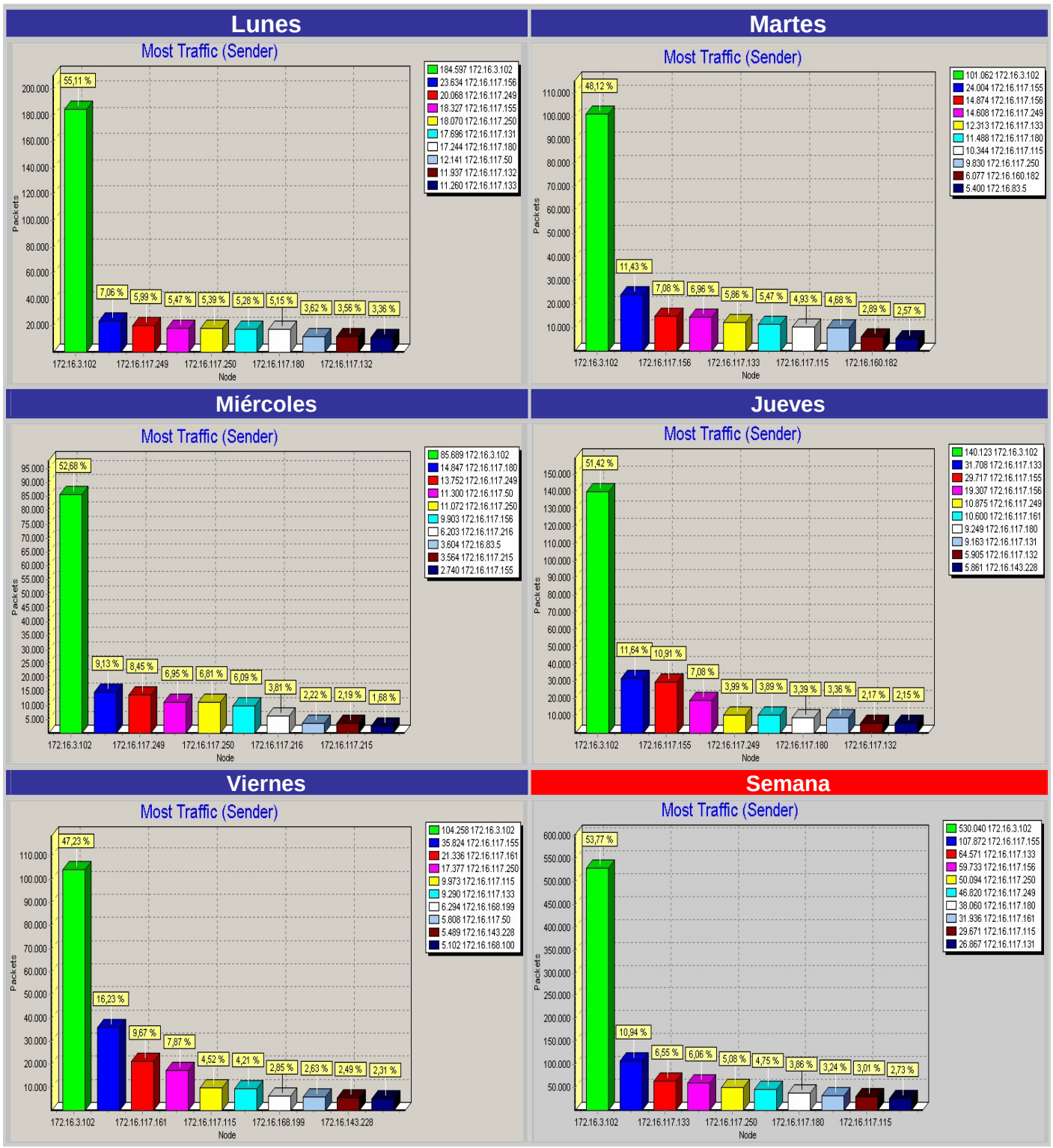


Figura B.3.3.6 Nodos de mayor tráfico enviado - Sede Girón

B.3.3.7 Nodos de mayor tráfico recibido - Sede Girón

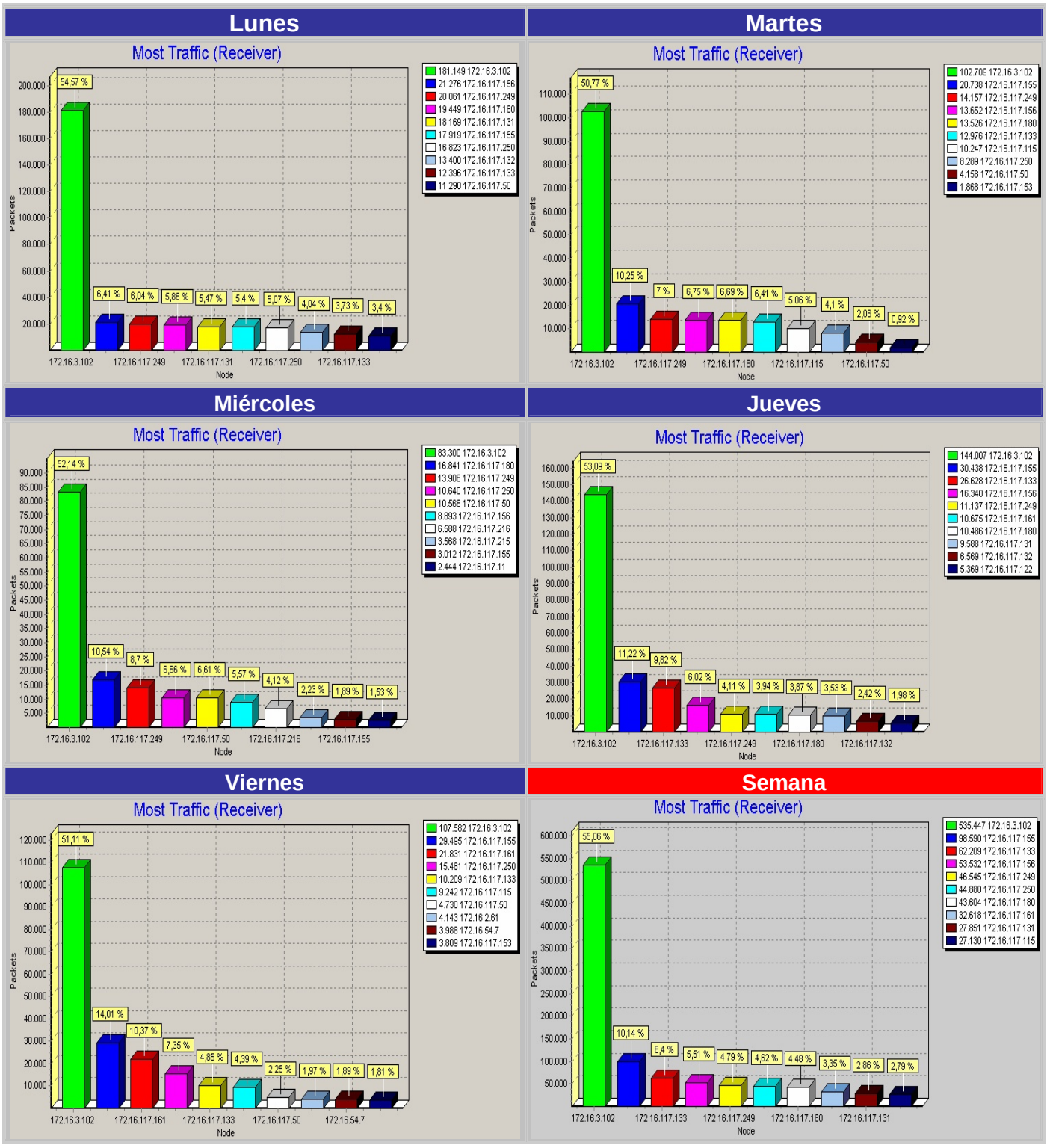


Figura B.3.3.7 Nodos de mayor tráfico recibido - Sede Girón

B.4. Configuración de un puerto espejo en un switch Alcatel Omniswitch 6624

La función de puerto espejo, permite remitir todas las transmisiones de un puerto a otro, permitiendo el análisis de todas las tramas entrantes o salientes por medio de un sofware especializado de captura de paquetes que permita visualizarlas y analizarlas.

Se seleccionará un puerto fuente, que en este caso será el puerto 1 y 2 del switch alcatel, dado que a estos están conectados los puertos Ethernet de los dos routers principales con los que cuenta la red de datos del SENA Regional Santander.

Es posible configurar puertos espejos entre cualquier par de puertos Ethernet del mismo switch. Entre los puertos Ethernet que soportan port mirroriring están: 10BaseT/100BaseTX (RJ-45) y 1000BaseLX(LC) conectores MiniGBIC.

Cuando el port mirroring está activo, el puerto fuente (mirrored) transmite y recibe todo el tráfico de la red normalmente mientras que el puerto destino (mirroring), recibe una copia de todo este tráfico.

Se puede conectar un RMON probe o directamente un analizador de red al puerto destino (mirroring), para observar la replica exacta del tráfico presente en el puerto fuente (mirrored) sin interrumpir, ni afectar el tráfico entrante y saliente en este puerto.

Especificaciones

Puertos Soportados	Ethernet (10 Mbps)/Fast Ethernet (100 Mbps)/ Gigabit Ethernet (1 Gb/1000 Mbps)
Sesiones de Port Mirroring soportadas	OmniSwitch 6624, OmniSwitch 6600-U24, OmniSwitch 6600-P24, y OmniSwitch 6602-24 —1 sesion por switche en stack. Por ejemplo, un stack de 4 OmniSwitch 6624 puede soportar 4 sesiones port mirror. OmniSwitch 6648 y OmniSwitch 6602-48 — 2 sesiones por switche en stack. Por ejemplo, un stack of de OmniSwitch 6648 puede soportar 8 sesiones port mirror.
Capacidad en los puertos	El puerto fuente *(mirrored)* y el puerto destino *(mirroring)* deben ser de la misma capacidad (ambos deben soportar por lo menos las mismas tasas de transferencia) o el puerto espejo debe ser de más capacidad que el puerto fuente.

Parámetros por defecto

Parámetro	Comando CLI	Valor por defecto
Creación de una sesión mirror	**port mirroring source destination**	Ninguna sesión mirror configurada
Protección contra Spanning Tree (Spanning Tree Deshabilitado)	**port mirroring source destination**	Spanning Tree Habilitado
Estado de la sesión mirror	**port mirroring source destination**	Desabilitado
Dirección del Puerto Mirror	**port mirroring source destination**	Bidireccional
Configuración de la sesión mirror	**port mirroring**	Desabilitado

Pasos para configurar un Puerto Espejo

1. Crear una sesión mirror, especificando el ID de la sesión, el puerto fuente (mirrored), el puerto destino (mirroring). Además, se puede agregar un comando opcional para desbloquear la VLAN y proteger la sesión mirror de cambios en el Spanning Tree en caso de que se quiera monitorear en este puerto el tráffico perteneciente a otra VLAN)

   > port mirroring [session ID] source [slot/port] destination [slot/port] unblocked [VLAN ID]

   Por Ejemplo:
   > port mirroring 6 source 2/3 destination 2/4 unblocked 7

2. Habilitar la sesión mirror

   > port mirroring [session ID] enable

   Por Ejemplo:
   > port mirroring 6 enable

3. Comprobar la configuración de la sesión mirror

   > show port mirroring status [session ID]

   Por Ejemplo:
   Para revisar la configuración de la sesión anterior, se teclea:
   > show port mirroring status 5

```
Session   Mirrored    Mirroring      Mirror      Mirroring  Mirroring
          slot/port   slot/port      Direction      Vlan     Status
----------+----------+----------+--------------+----------+----------
6.          2/3         6/4          bidirectional  7         ON
```

Procedimiento para la configuración del Puerto Espejo en los switches principales del SENA REGIONAL SANTANDER

En el caso particular del SENA, se cuenta con 3 switches principales, de marca Alcatel y con referencia Omniswitch 6624, apilados o configurados en stack.

Se propone crear dos sesiones mirror, la primera para el puerto 1/1 que corresponde al puerto Ethernet del Router Cisco 3640 y la segunda para el puerto 1/2 que corresponde al puerto Ethernet del Router Heawei 3640, y remitirlas al mismo puerto, para poder realizar una monitorización detallada de todo el tráfico entrante y saliente de la red de datos.

A continuación se describen los pasos a seguir para conseguirlo:

1. Como primera medida, se debe ingresar por telnet al snack de swiches, que tiene dirección IP: 172.16.55.253

2. Revisar la configuración actual de las sesiones mirror
   >show port mirroring status

3. Revisar la configuración actual de las VLAN
   >show vlan

4. Crear las 2 sesiones mirror
   >port mirroring 6 source 1/1 destination 3/20
   >port mirroring 6 source 1/2 destination 3/20

5. Habilitar las 2 sesiones mirror
   >port mirroring 1
   >port mirroring 2

6. Revisar la configuración de las dos sesiones mirror
   >show port mirroring status 1
   >show port mirroring status 2

ANEXO C.
Propuestas de Proveedores

C.1 Propuesta de TELECOM para Red Interna e Internet

C.2 Cotización de dispositivos para Voz sobre IP

C.1 Propuesta de TELECOM para Red Interna e Internet

A continuación se presenta la descripción de la propuesta de conectividad de Colombia Telecomunicaciones (TELECOM) al SENA REGIONAL SANTANDER, teniendo en cuenta los requerimientos planteados anteriormente en cuanto a Internet y Red Interna.

C.1.1 Descripción de conectividad del servicio Internet

Colombia Telecomunicaciones S.A. ESP cuenta con un Backbone IP Nacional de un STM-1 (155 Mbps) soportado sobre el anillo de fibra óptica con cobertura para las siete ciudades más importantes de Colombia: Bogotá, Cali, Pereira, Medellín, Barranquilla, Bucaramanga y Cúcuta[121]; a su vez, a estas ciudades se conectan más de 30 ciudades de Colombia logrando una gran cobertura nacional de Internet a nivel nacional.[122]

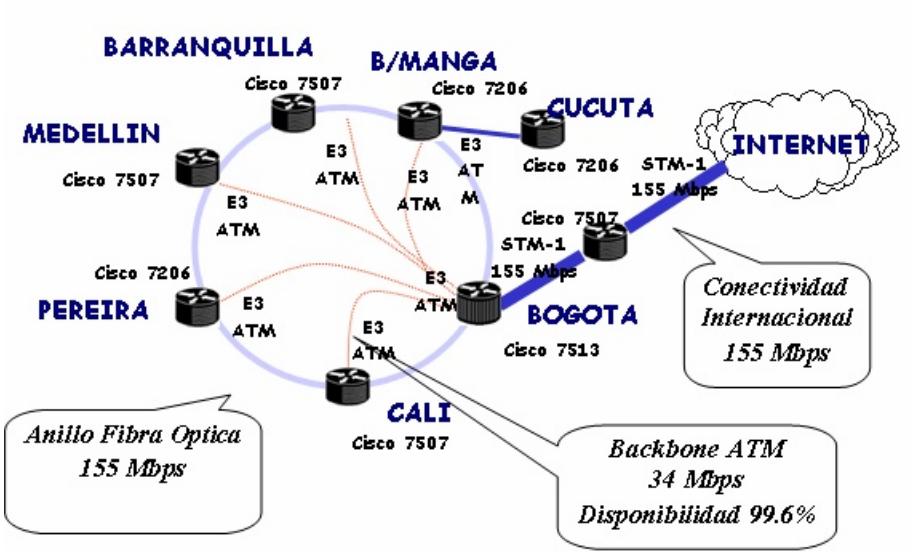


Figura C.1 Topología de Backbone Internet Telecom

[121] Ver Figura C.1 Topología de Backbone Internet TELECOM
[122] Ver Figura C.2 Servicio de Internet TELECOM

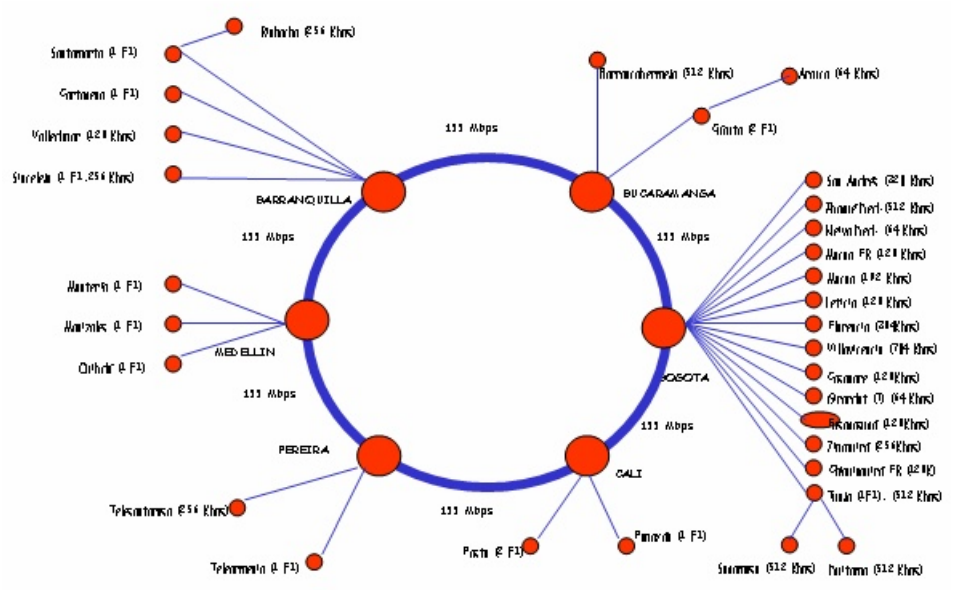


Figura C.2 Servicio de Internet TELECOM

Así mismo, el backbone nacional está conectado al NAP Colombia directamente. A nivel Internacional, para acceso a la red Mundial Internet se tiene una capacidad contratada de un STM-1 (155 Mbps) con el proveedor SPRINT a través del cable Maya y una capacidad de respaldo de 17 E1s a través de los cables Panamericano y Americas II.[123]

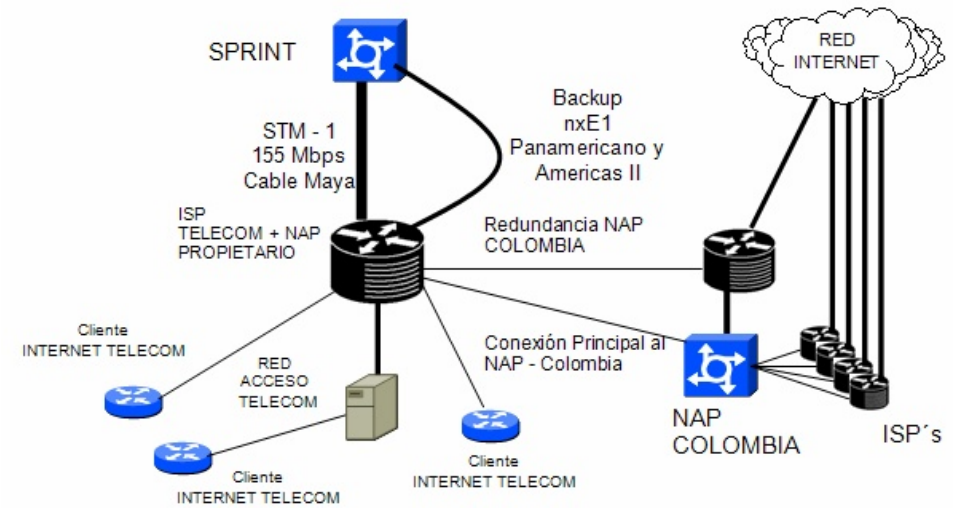


Figura C.3 Topología de Red Internet TELECOM

La red de Internet de COLOMBIA TELECOMUNICACIONES S.A. ESP cuenta con un Firewall Checkpoint sobre appliance NOKIA el cual tiene las siguientes características:

[123] Ver Figura C.3 Topología de Red Internet Telecom

- Permite la implementación de hasta 500 políticas de seguridad.
- Soporta protocolos estándar ARP, TCP/IP, UDP, ICMP, HTTP, Radius, LDAP, TFTP, SNMP y PpoE.
- Permite la implementación de NAT y políticas de seguridad sobre NAT,
- Filtrado por direcciones IP.
- La caracterización de URL como maliciosos y la protección contra ataque en: Inundación ICMP/UDP, Ping of death, Exploración de puerto, Ataque tipo LAND, Ataque “SYN”, Tear drop, IP address sweep, WinNuke y Java/ActiveX/Zip.

COTIZACION TELECOM

	PUNTA								ACCESO				CATEGORIA			TOTAL SOLUCION		DURACION EN MESES	VALOR DEL SERVICIO
	UK (incluído equipo terminal)				EQUIPO CLIENTE														
Enlace	Ciudad	Proveedor Uk	Tipo de UK	BW (Kbps)	Tipo	Marca	Modelo	Proveedor	BW R 1:1	BW R 1:2	BW R 1:3	BW R 1:4	DEDICADO	ADSL	SATELITAL	Cargo conexión	Cargo fijo mes	*Tiempo de duración de la orden de servicio)*	*Formula: Cargo de conexión+cargo fijo mes*duración en meses)*
1	BUCARAMANGA	TELECOM	COBRE - MODEM	1024	ROUTER	CISCO	1721	TELECOM	X				X			$ 2.385.000	$ 2.298.871	12	$ 29.971.452
					MODEM	ADTRAN	6540	TELECOM											
2	FLORIDABLANCA	TELECOM	COBRE - MODEM	512	ROUTER	CISCO	1721	TELECOM	X				X			$ 1.503.000	$ 1.575.125	12	$ 20.404.500
					MODEM	ADTRAN	6540	TELECOM											
3	GIRON	TELECOM	COBRE - MODEM	512	ROUTER	CISCO	1721	TELECOM	X				X			$ 1.503.000	$ 1.575.125	12	$ 20.404.500
					MODEM	ADTRAN	6540	TELECOM											
4	PIEDECUESTA	TELECOM	COBRE - MODEM	256	ROUTER	CISCO	805	TELECOM	X				X			$ 1.303.000	$ 975.125	12	$ 13.004.500
					MODEM	ADTRAN	6540	TELECOM											
5	El Playón	TELECOM	SATELITAL	128	ANTENA	VSAT		TELECOM				X			X	$ 2.030.000	$ 1.180.000	12	$ 16.190.000
					ODU	VSAT		TELECOM											
					IDU	VSAT		TELECOM											
6	VELEZ	TELECOM	COBRE - MODEM	256	ROUTER	CISCO	805	TELECOM	X							$ 1.303.000	$ 975.125	12	$ 13.004.500
					MODEM	ADTRAN	6540	TELECOM											
7	BARRANCABERMEJA	TELECOM	COBRE - MODEM	512	ROUTER	CISCO	1721	TELECOM	X				X			$ 1.503.000	$ 1.575.125	12	$ 20.404.500
					MODEM	ADTRAN	6540	TELECOM											
8	MALAGA	TELECOM	COBRE - MODEM	256	ROUTER	CISCO	805	TELECOM	X				X			$ 1.303.000	$ 975.125	12	$ 13.004.500
					MODEM	ADTRAN	6540	TELECOM											
9	San Gil	TELECOM	COBRE - MODEM	256	ROUTER	CISCO	805	TELECOM	X				X			$ 1.303.000	$ 975.125	12	$ 13.004.500
					MODEM	ADTRAN	6540	TELECOM											

PORCENTAJES DE DESCUENTOS POR INDISPONIBLIDAD DEL SERVICIO

% disponiblidad		total max	% de
Desde	Hasta	horas/mes	descuento
100	99,6	2,9	0%
99,59	99	7,2	4%
98,9	98	14,4	5%
97,9	96	28,8	7%
95,9	92	57,6	12%
91,9	86	100,8	20%
85,9	76	172,8	30%
75,9	50	360,0	45%
50	0	720,0	100%

Notas aclaratorias:	
UK:	*Ultimo kilómetro*
BW:	*Ancho de Banda*
R:	*Reuso*

Tabla C.1 Cotización Telecom

Propuesta TELECOM para proveer Internet							
	Ancho de Banda Clear Channel	Reuso	Conexión	Valor Instalación	Descuento al 2do Año	Valor Mensual Con Descuentos	Valor Anual
Administración y Centro de Comercio y Servicios	1024K	1:1	Clear Channel	2.385.000	2.385.000	2.268.871	27.226.452
Centro Industrial de Floridablanca	512K	1:1	Clear Channel	1.503.000	1.503.000	1.545.125	18.541.500
Centro Industrial de Girón	512K	1:1	Clear Channel	1.503.000	1.503.000	1.545.125	18.541.500
CASA Guatiguará	256K	1:1	Clear Channel	1.303.000	1.303.000	945.125	11.341.500
CASA Aguas Calientes (satelital)	256K	1:1	Satelital	1.798.000			
Centro Mult. de Vélez	256K	1:1	Clear Channel	1.303.000	1.303.000	945.125	11.341.500
Centro Mult. de Barranca	512K	1:1	Clear Channel	1.503.000	1.503.000	1.545.125	18.541.500
Centro Mult. de García Rovira	256K	1:1	Clear Channel	1.303.000	1.303.000	945.125	11.341.500
Centro Mult. de Guanentina Comunera	512K	1:1	Clear Channel	1.503.000	1.503.000	1.545.125	18.541.500
TOTALES:						11.284.746	135.416.952

Tabla C.2 Propuesta Telecom para proveer Internet

C.2 Cotización de dispositivos para Voz sobre IP

Dispositivo	Especificaciones
 **Tipo:** Gateway PSTN ***Referencia:*** *D-Link SIP Analog Trunk Gateway DVG-3004S* **Precio:** USD $699.00 **Distribuidor:** http://www.expansys.com.mx	**Protocolos que soporta:** • SIP (RFC3261) Compliance • DTMP Dialing/Detection • Fix IP and DHCP • PSTN Polarity Reversal Detection **Caracteristicas red:** • LAN Port: 10Mb Base-T Ethernet • PSTN Port: 4 Analog FXO Ports • COM Port: RS-232 Console Port (DB9) • Support Static IP and DHCP • QoS by ToS (Type of Service) • SNTP (Simple Network Time Protocol) **Caracteristicas de telefono:** • Peer-to-Peer Mode • Support Auto-Attendant (2nd Dial Tone/Voice Greeting) • Line Hunting • E.164 (Telephone Number Plan) • DTMF Dialing • DTMF Detection/Generation • VAD (Voice Activity Detection) • CNG (Comfort Noise Generate) • Dynamic Jitter Buffer • Bad Frame Interpolation • Completed Voice Band Signaling Support • Receive Caller ID (DTMF of FSK) From PSTN • Provide Inbound and Outbound DTMF Generation/Detection between LAN and PSTN Interface • Gain/Attenuation Settings • G.168.1 Echo Cancellation

Tipo : Gateway PSTN

Referencia: Quintum Tenor DX

Precio: USD $3.600

Distribuidor: www.corpdata.com.ve

Especificaciones de teléfono
• Voice algorithms: G.723.a and G.729ab, G.711
• Auto codec negotiation
• Fax support: Industry standard T.38 and Group III at 2.4, 4.8, 7.2, 9.6, 14.4 Kbps
• Modem over IP
• Choice of 2, 4, 6, or 8 T1/E1/PRI Spans
• Standard RJ-45 Connectors
• Coding: A-law, µ-law
• Enhanced (Carrier Grade) Echo Cancellation: ITU Rec. G 168, up to 128 msec tailsize
• PRI Signaling Protocols: National ISDN-2, Euro ISDN NET5, Japan INS-NET1500, KDD, 4ESS, 5ESS, DMS100
• T1 CAS (E&M, Loop Start, Feature Group-D, DTMF, MF)
• E1 CAS (R2 MF)
• DASS2
• Tandem/TDM switching
• Maximum Call Rate: 7,200 calls/hour
• VoIP to circuit, and circuit to circuit (Tandem/TDM) switching

Especificaciones de red
• LAN Interface: Fast Ethernet port (10/100 Base-T)
• Standard RJ-45 Interface (IEEE 802.3) for 10 Base-T or 100 Base-T connections
• QoS Support: IP TOS, DiffServ

Especificaciones Voip
• H.323 v.3 Gateway and Integrated Gatekeeper
• SIP User Agent (RFC3261 compliant endpoint)
• SIP Back-to-Back User Agent (B2BUA)**
• SIP RFC2833 In-band DTMF signaling
• SIP Refer Method Support
• IVR/RADIUS server support for AAA with integrated multilingual IVR
• Adaptive Voice Activity Detection (VAD) with Comfort Noise Generation (CNG)
• Adaptive Jitter Buffer
• Packet Loss Compensation
• NATAccess™
• Security: IP Filtering
• Up to 120 simultaneous VoIP calls

Tipo: Videoconferencia MCU

Referencia: Cisco IP/VC 3510 MCU

Precio: USD $999.99

Distribuidor: http://www.cibercorp.com.mx

Caracteristicas:

- Hace posible establecer conversaciones “cara a cara” entre participantes que se encuentren en diferentes ubicaciones.
- Conecta tres o más puntos finales de videoconferencia H.323 en una sola sesión integrada para varios participantes.
- Combina flujos de vídeo, audio y datos de varios puntos finales de la conferencia en una sesión interactiva de varias ubicaciones.

Cuando se utiliza en combinación con equipos selectores de videoconferencia IP/VC 3520 y 3525, la MCU IP/VC 3510 puede también introducir en la conferencia uno o más puntos finales H.320.

Tipo: Videoconferencia

Referencia: Polycom VSX 7000s

Precio: USD $4.275,00

Distribuidor: http://www.visualcom.com.co

Características:

- Ofrece un video verdaderamente excepcional con H.264 y Pro-Motion con calidad tipo televisión
- Una interfaz de usuario hecha a la medida y fácil de usar
- Codificación criptográfica de software con norma AES
- Capacidades de integración con pantallas touch-screen y capacidades para añadir llamadas de voz.
- Para integrar aplicaciones especiales, cualquiera de los productos de la serie VSX 7000 puede añadirse al Polycom Media Center para obtener una solución completa de rack y monitor.

Tipo: Telefono IP

Referencia: *Alcatel Premium Reflexes*

Precio: $508.292

Distribuidor: Alcatel de Colombia S.A.
Avda. 19 No. 36-28 3240000 - FAX 3240030
Bogotá

- **Conexión 10BT/100BT:**
half/full duplex con negociación automática

- **VoIP estándar**:
Compatibles H323, RTP, RTCP

- **Protocolos de compresión de voz estándar:**
G711, G723.1, G729a

- **Conectividad**:
Conector RJ45 Ethernet para redes LAN.
Conector RJ45 Ethernet> Toma de alimentación

- **Calidad de servicio:**
Conmutador Ethernet integrado para QOS
TOS diffserv
802.1p/q

- **Configuración de la dirección IP:**
Los parámetros IP se pueden configurar de forma estática o dinámica. Los terminales incluyen un cliente DHCP.

- **Fuente de alimentación:**
Compatible tanto con alimentación LAN como local.

Tabla C.3 Cotización de dispositivos para Voz sobre IP

ANEXO D.
Manual Básico de OpManager 6.0

MANUAL BÁSICO DE OPMANAGER 6
SENA REGIONAL SANTANDER
2006

Elaborado por:
JORGE ORLANDO CIFUENTES CIFUENTES
HELBER ANTONIO HERNÁNDEZ CELIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERIAS ELÉCTRICA ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2006

CONTENIDO

Tablas y figuras

1. Características

OpManager es una herramienta de monitoreo que ofrece al administrador de la red una consola integrada de visualización y gestión de red, permitiéndole detectar a tiempo problemas en el rendimiento de la red que supongan costosos tiempos de inactividad. Además, automatiza diversas tareas de monitoreo de la red y elimina la complejidad asociada a su administración

La consola de OpManager permite monitorear y gestionar routers, switches, servidores, firewalls, impresoras y todo tipo de dispositivos que se encuentren conectados a la red generando gráficas y reportes que darán una idea acertada de su desempeño.

El OpManager es un software basado completamente en Web, por lo tanto cuenta con dos partes esenciales, el “OpManager Server” y el “OpManager Web Client”. Esta característica posibilita su utilización desde cualquier punto de la red, simplemente conociendo la dirección IP del servidor en el que se encuentre ejecutándose y los datos de usuario para iniciar la sesión.

Algunas de las funcionalidades del OpManager son las siguientes:

1.1 Gestión de Fallas:

OpManager sondea periódicamente la red en busca de fallas y genera alarmas de aviso para el administrador.

1.2 Gestión de Desempeño:

OpManager mide el desempeño del hardware y el software de la red, generando gráficas y reportes periódicos de ancho de banda, memoria, utilización de disco y CPU, tiempo de respuesta de los servicios, etc.

1.3 Monitoreo de Redes:

OpManager permite realizar una optimización en la asignación de ancho de banda al presentar información precisa sobre el tráfico de los enlaces, su porcentaje de utilización y los errores de la red WAN.

Igualmente se puede monitorear el estado de todos los dispositivos conectados a la red (routers, switches, servidores, firewalls, etc) y sus interfaces, visualizando todas las variables críticas de su rendimiento, como estadísticas de utilización de CPU, utilización de memoria, errores y descartes, etc.

Con la función de "Autodiscovery", OpManager puede descubrir switches, routers y firewalls conectados a la red automáticamente y puede monitorear sus parámetros críticos, como la taza de transferencia, la taza de errores y los bits perdidos en el buffer entre otros.

Además, OpManager permite generar un reporte de la disponibilidad de cada puerto o interfaz y de los dispositivos y usando la función "Switch Port Mapper" se puede obtener un listado de los dispositivos conectados a cada puerto de un switche. [Ver la sección: "Monitoreo de Routers" y Monitoreo de Swiches"]

1.4 Monitoreo de Servidores:

Con OpManager es posible distinguir entre los servidores y las estaciones de trabajo o hosts. Proporciona gráficos detallados e informes de disponibilidad diaria, semanal, mensual y trimestral de sus servidores y además, también permite monitorear la utilización de aplicaciones que se ejecuten en los servidores.

El administrador puede obtener informes automáticos para identificar los servidores sobrecargados y ocupados en términos de utilización de la CPU y la memoria. [Ver la sección: "Monitoreo de Servidores"]

1.5 Monitoreo de Aplicaciones y Servicios:

OpManager descubre y monitorea la disponibilidad y el tiempo de respuesta de todos los servicios que se ejecuten en los servidores como Web, HTTPS, FTP, IMAP, LDAP, Telnet, SMTP, POP3, WebLogic, etc y aplicaciones como MSSQL, MS Exchange, Oracle y Lotus. Además, se puede configurar OpManager para que monitoree otros servicios críticos que se tengan instalados en los servidores. [Ver la sección: "Monitoreo de Servicios de Windows"]

1.6 Monitoreo de URL:

OpManager permite monitorear en tiempo real la disponibilidad de los sitios web o sitios de intranet de una red y verificar si se encuentran funcionales.

1.7 Versión de Prueba

La versión de prueba del OpManager se puede descargar de la siguiente dirección: http://manageengine.com/products/opmanager/download.html

Esta versión cuenta con todas las funcionalidades de la versión completa, sin embargo, está limitada a 30 días, al término de los cuales la versión cambia a su modo “Freeware”, en el cual permite monitorear por tiempo indefinido solamente 20 dispositivos de red.

2. Requerimientos

2.1 Hardware

CPU	Pentium III 800 MHz
RAM	512 MB
Disk Space	200 MB
Display	High color

Tabla 1: Requerimientos de Hardware

2.2 Sistemas Operativos

- Windows 2000
- Windows 2003
- Windows XP
- Red Hat Linux 7.2 y posteriores

2.3 Requerimientos para el Web Client

El cliente HTML requiere por lo menos uno de los siguientes navegadores:

- Netscape 4.2 o posterior
- IE 5.0 o posterior

3. Instalación

Para instalar el OpManager en los equipos con Windows, siga los siguientes pasos:

1. Ejecutar AdventNet_ManageEngine_OpManager_5.exe

	**Nota:** Si no se cuenta con el archivo de instalación, puede ser descargado desde la siguiente dirección: http://manageengine.com/products/opmanager/download.html

2. Hacer click en "**Next**" para comenzar el proceso de instalación

3. Leer el "**License Agreement**" y hacer clic en "**Yes**"

4. Escoger el tipo de instalación (**30 days Trial Version**) o (**Free Edition**).

   La primera cuenta con todas las funcionalidades de la versión completa pero está limitada a un mes de prueba, mientras que la segunda no está limitada en tiempo, pero permite añadir solamente 20 nodos para monitorearlos.

	**Nota:** Se recomienda seleccionar la opción gratuita si se quiere dejar instalado el programa durante largo tiempo e identificar los 20 nodos críticos de la red que requieran ser monitoreados.

   En el caso del SENA, se determinó que estos nodos serían todos los routers principales y los swiches Alcatel de la Sede Administrativa como se muestra a continuación:

Nodo	Dispositivo	Sede	Dirección IP	Comunidad SNMP
1	Cisco 3640	Administrativa	172.16.55.247	Public
2	Huawei 3640	Administrativa	172.16.55.254	Senalcatel
3	Huawei NE-08	Dirección General	172.16.3.1	Senalcatel
4	Cisco 1750	Barrancabermeja	172.16.115.253	Senalcatel
5	Cisco 1750	Girón	172.16.117.254	Public
6	Cisco 1750	Floridablanca	172.16.119.253	Public
7	Cisco 1720	San Gil	172.16.123.254	Public
8	Cisco 1720	Vélez	172.16.131.254	Senalcatel
9	Cisco 1720	Piedecuesta	172.16.178.254	Senalcatel
10	Cisco 1720	Málaga	172.16.183.254	Senalcatel
11	AlcatelOmniswitch 6624	Administración– Piso 5	172.16.55.253	Public
12	Alcatel Omnistack 6648	Administración– Piso 4	172.16.55.250	Public
13	Alcatel Omnistack 6648	Administración– Piso 3	172.16.55.249	Public
14	Alcatel Omnistack 6648	Administración - Piso 2	172.16.55.248	Public
15	Alcatel Omnistack 6648	Empleo	172.16.55.241	Public
16	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 2 Torre 1	172.16.55.251	Public
17	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 3 Torre 1	172.16.55.244	Public
18	Alcatel Omnistack 6624	Centro de Comercio y Servicios Apoyo	172.16.55.243	Public
19	Alcatel Omnistack 6648	Centro de Comercio y Servicios Inglés	172.16.55.245	Public
20	Alcatel Omnistack 6648	Centro de Comercio y Servicios Aulas	172.16.55.246	Public

Tabla 2: Dispositivos añadidos en el OpManager instalado en la Sede Administrativa del SENA Regional Santander

5. Escoger el idioma de la instalación (El software se puede instalar en español, inglés, chino o japonés) y dar click en "**Next**"

6. En este paso se determina la carpeta de instalación, si la que aparece es la deseada, dar clic en "**Next**"

7. Se verifica que el acceso directo al programa sea el deseado (Inicio>Todos los programas>ManageEngine OpManager) y se da click en "**Next**"

8. Se escoge el puerto en el que va a correr el "**OpManager Server**", por defecto está el **puerto 80**, se recomienda no cambiarlo.

9. Se abrirá una ventaja opcional para servicio técnico. Dar click en "**Next**"

10. Verificar los detalles de la instalación en la siguiente ventana y dar click en "**Next**". El programa comenzará a instalarse.

11. Hacer click en "**Next**" para completar el proceso de instalación

Nota:

- Un acceso directo para abrir el OpManager Server se creará en el escritorio y otro en el menú:

  Inicio> Todos los Programas> ManageEngine OpManager

- Después de terminar la instalación, si se ha hecho correctamente, el OpManager Server se iniciará automáticamente y el Web client se abrirá.

- Dado que el programa se instala en Windows como un servicio, cada vez que se inicie el equipo el servidor y el cliente también se iniciarán, lo que lo harán un poco más lento al iniciar. Por esta razón, se recomienda instalar el OpManager solamente en servidores.

3.1 Desinstalación

Click en: Inicio > Programas > ManageEngine OpManager > Uninstall OpManager y seguir los pasos indicados por el asistente de desinstalación.

4. OpManager Server

Luego de la instalación, todos los archivos del OpManager quedarán disponibles en el directorio que se haya escogido, que en adelante será el directorio de trabajo de la herramienta.

Para iniciar el OpManager Server en Windows:

Dado que por defecto el programa se instala como un servicio de Windows, una vez se termine de instalar el programa, automáticamente se iniciará el servidor:

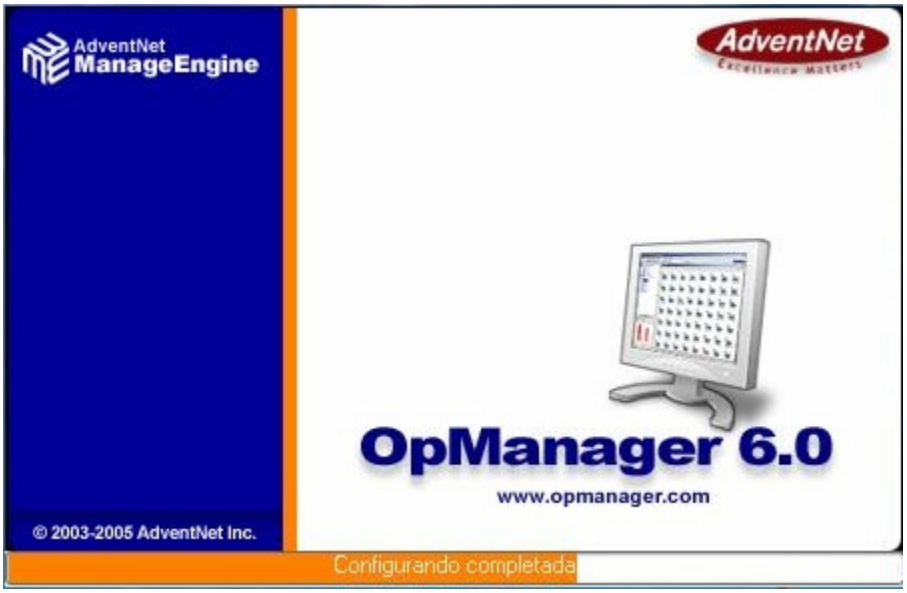


Figura 1: Ventana indicadora de inicio del servidor de OpManager

Cuando el servidor está encendido, se despliega en la parte inferior derecha de la pantalla el icono del mismo, que pasa de color gris a color verde.

Figura 2: Indicador de servidor encendido

Para verificar el estado del servidor y su configuración, podemos hacer click derecho sobre el icono y entrar a "**Estado de OpManager**"

Se desplegará la siguiente ventana, con el nombre del servidor, su dirección IP y el puerto que está utilizando.

Figura 3: Estado del servidor de OpManager

Para apagar el servidor, hacemos click derecho sobre su icono y seleccionamos la opción "**apagar servidor**", se desplegarán las siguientes ventanas:

Figura 4: Apagado del servidor

5. Web Client

Una vez iniciado el servidor, se abrirá automáticamente el Web Client en el navegador de Internet que se tenga instalado y le solicitará al usuario los datos para el inicio de la sesión.

Figura 5: Inicio de sesión de OpManager

Los datos de la cuenta de inicio no serán modificados, por lo tanto serán los mismos que el programa trae configurados por defecto:

Nombre de Usuario:	admin
Password:	admin

5.1 Ayudante para el descubrimiento de Red

Cuando se inicie por primera vez sesión en Web Client, se abrirá automáticamente el ayudante de descubrimiento de red.

	**Nota**: Sin embargo, recomendamos no utilizarlo y dar click en “Cancel” para salir del asistente, dado que la versión instalada es la gratuita y sólo permite el monitoreo de 20 nodos críticos que pueden ser añadidos uno a uno posteriormente.

5.2 Iniciando el Web Client desde cualquier host de la red

1. Abrir el navegador de Internet

	**Nota**: El navegador de Internet debe tener “Java” habilitado.

2. En la barra de direcciones teclear:

http://<host_name>:<puerto>

Donde <**host_name>** es el nombre de la máquina o la dirección IP del servidor en el que se encuentra corriendo el OpManager Server.

En el SENA se instaló el OpManager en la máquina: 172.16.54.44, por lo tanto la sintaxis para ingresar al Web Client desde cualquier punto de la red, sería: http://172.16.54.44:80 o simplemente http://172.16.54.44 dado que el puerto 80 es el puerto configurado por defecto en el navegador para acceder a Internet.

3. Ingresar los datos correspondientes de usuario para iniciar la sesión

Nombre de Usuario: admin

Password: admin

	**Nota:** También se puede iniciar el Web Client en el servidor donde se tenga instalado usando la ruta de menú: **Inicio>Programas> ManageEngine OpManager > OpManager Web Client**

6. Personalización

El Web Client permite ser personalizado por el usuario según sus preferencias de la siguiente manera:

6.1 Superficie

Se puede escoger entre 8 superficies de trabajo diferentes:

1. Dar click en la pestaña "**Personalizar**" que se encuentra en la parte superior derecha del Web Client

2. En la ventana que se abre, seleccionar selector de superficie y escoger el que más se acomode al gusto del usuario
3. Dar click en "**Aplicar**" para guardar los cambios

6.2 Cambiar Contraseña

De nuevo en el menú "Personalizar" hacemos click en la pestaña "**Cambiar contraseña**". Ingresamos la contraseña anterior y la nueva y damos click en aplicar para guardar los cambios.

6.3 Tiempo de espera de sesión

En "**Personalizar**" hacer click en la pestaña de "**Refresco Automático**" y configurar el tiempo de sesión según se desee. Por defecto la sesión nunca expirará

6.4 Añadir una nueva cuenta de usuario

El administrador puede crear en OpManager usuarios con los privilegios que se deseen. Para crear una nueva cuenta de usuario, hacemos lo siguiente:

1. Dar click en la pestaña "**Admin**"
2. En el menú "**Definiciones Globales**" dar click en el ícono "**Usuarios** 

3. En el menú "**Acciones**" de la derecha, dar click en "**Agregar Usuarios**". Sin embargo, la versión de prueba sólo permite configurar una cuenta de usuario.

7. Interfaz de usuario

La Interfaz de usuario del OpManager Web Client está organizada en 6 pestañas: Anfitrión, Mapas, Alarmas, Admin, Reportes y Support.

Figura 6: Pestañas del Web Client

7.1 Pestaña Anfitrión

Es la pestaña principal que se presenta al usuario una vez iniciada la sesión en el Web Client. Está dividida en la sección "Consola", que agrupa la "**Captura de Infraestructura**", la "**Captura de Negocios**" y los "**Gráficos de Alarma**", que pretenden suministrar una información ágil al administrador sobre el estado de la red.

En la parte inferior, se presentan informes sobre interfaces críticas con mucho tráfico o con alta utilización de memoria.

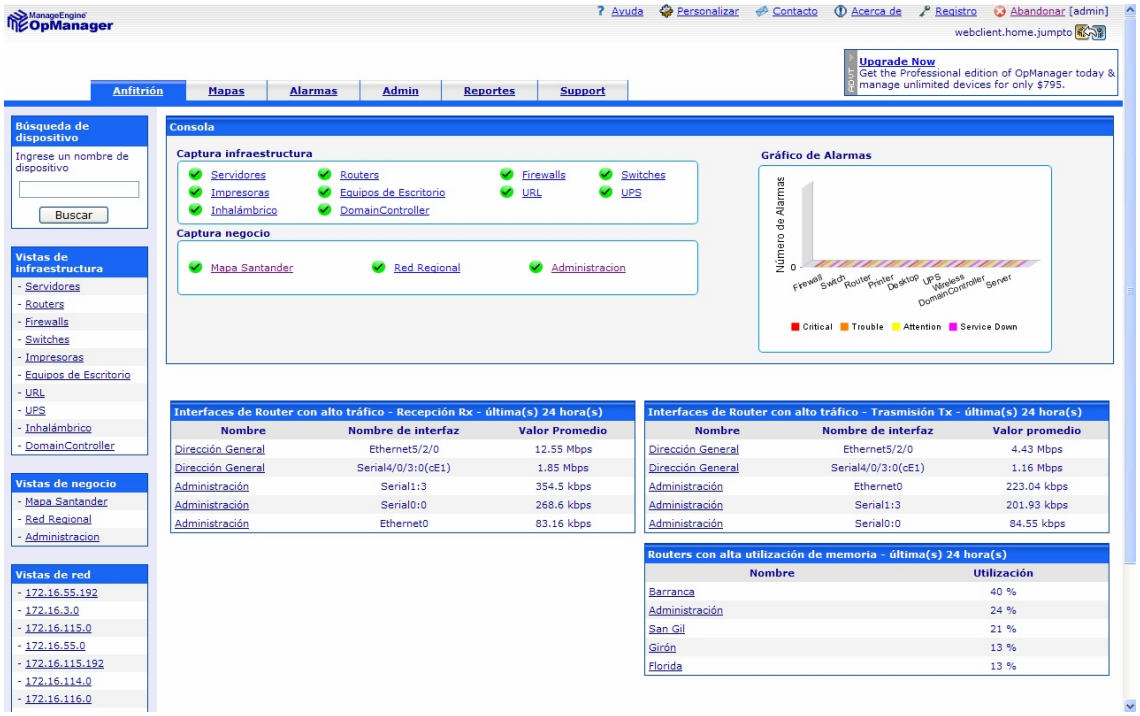


Figura 7: Pestaña inicial

Como se puede apreciar en la figura anterior, toda la información sobre el estado de la red que se presenta está codificada con colores según su importancia o grado de riesgo, lo que permite al administrador decidir sobre el orden en el que debe atenderlas.

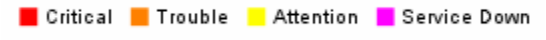


Figura 8: Código de colores

Adicionalmente, el color verde se presenta para dispositivos y enlaces que están funcionando correctamente, por ejemplo en la siguiente figura:

Figura 9: Ejemplo código de colores

Se indica que todos los dispositivos de la red detectados o añadidos se encuentran funcionando correctamente y que el administrador de la red puede descansar tranquilo.

7.2 Pestaña Mapas

En esta pestaña se muestran los detalles sobre los dispositivos detectados o agregados, dependiendo del nodo seleccionado en la sección "**Vistas de Infraestructura**".

Figura 10: Vistas de Infraestructura

Cuando se abre la pestaña “**Mapas**” se carga por defecto la vista “**Servidores**”, sin embargo, en el programa instalado en el SENA no se mostrará ninguna información, debido a que no se añadió ninguno.

Al contrario, al dar click en la vista “**Routers**”, se presentará un mapa de todos los Routers que conforman la Red Regional, su estado y sus interfaces. De la misma manera ocurre con los switches.

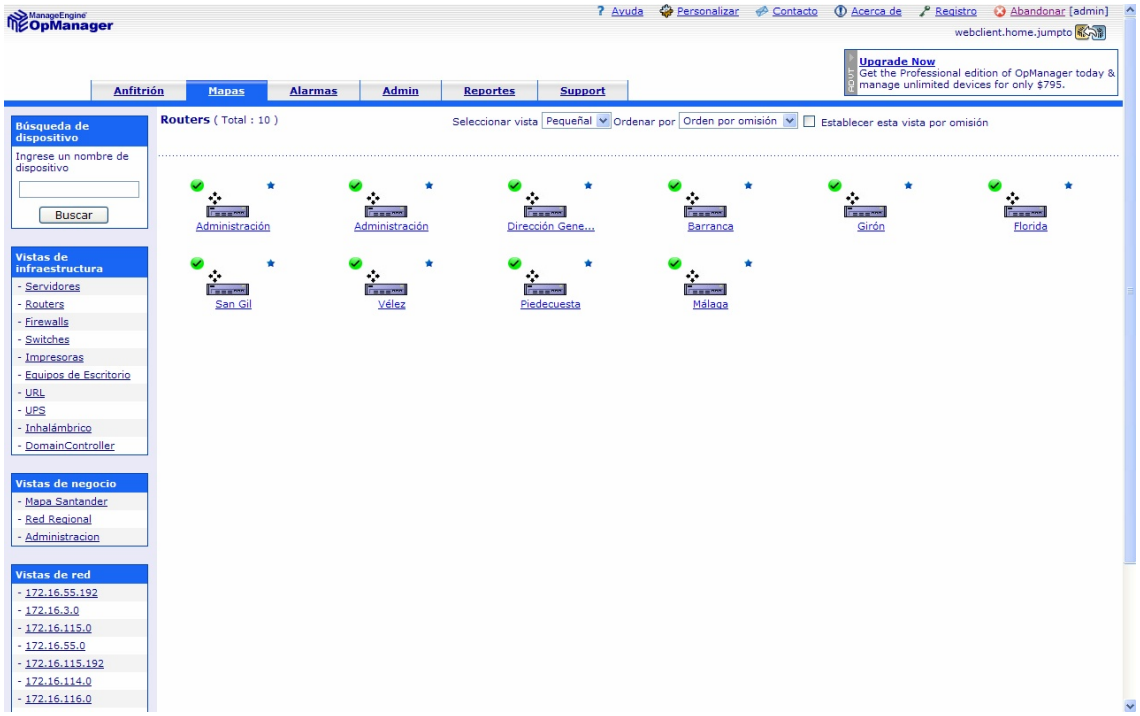


Figura 11: Pestaña Mapas

Asimismo, en la lista desplegable de la parte superior, se puede ordenar la lista de los dispositivos como se desee y seleccionar el tipo de vista (Grande, Pequeña o Detalles).

La vista grande está seleccionada por defecto y muestra gráficamente el estado de todos los puertos de los dispositivos.

Figura 12: Vista grande

La vista pequeña genera un mapa de todos los dispositivos, proporcionando una idea general de su estado y de si son administrables bajo SNMP (estrella azul al lado del icono).

Figura 13: Vista pequeña

La vista detalles genera un listado de todas las interfaces de los dispositivos que incluye su identificación, velocidad, estado, porcentaje de utilización y tráfico.

Routers Detalles

Nombre	Nombre de Interfaz	Desplegar Nombre	Velocidad (Mbps)	Estado	Utilización de Recepción - Rx (%)	Utilización de Transmisión - Tx (%)	Tráfico Recepción - Rx (Kbps)	Tráfico Transmisión - Tx (Kbps)	Errores (paquetes)
	Serial0/0	connected to I...	2		2	1	33	26	0
63.168.113.1	FastEthernet0/0	connected to F...	100		0	0	27	33	0
	Null0	IF-63.168.113....	4295		0	0	0	0	0

Figura 14: Vista detalles

Más adelante se entrará en detalle sobre cómo leer la información que se presenta en esta pestaña. [Ver: Monitoreo de Routers, Monitoreo de Switches].

7.3 Pestaña Alarmas

Esta pestaña le presenta al usuario una vista más detallada de todas las alarmas de los dispositivos y su importancia, clasificándolas en: critical (), trouble () , attention (), service down () y clear ().

7.3.1 Niveles de alerta

A continuación, se muestran los iconos de niveles de alerta presentados por OpManager y su significado. Estos iconos son desplegados junto a los dispositivos para indicar su estado de operación de una manera sencilla.

Icono	Alerta	Significado
	Critical	▪ Sin respuesta en los últimos 5 sondeos ▪ Trap recibida (dependiendo de la configuración seleccionada) ▪ Umbral superado (dependiendo de la configuración seleccionada)
	Trouble	▪ Sin respuesta en los últimos 3 sondeos. ▪ Problemas de impresión (Toner vacío, sin papel, etc) ▪ Puerto de swiche bloqueado ▪ Trap recibida (dependiendo de la configuración seleccionada) ▪ Umbral superado (dependiendo de la configuración seleccionada)
	Attention	▪ Sin respuesta en el último sondeo ▪ Trap recibida (dependiendo de la configuración seleccionada) ▪ Umbral superado (dependiendo de la configuración seleccionada)
	Service Down	Servicio caído
	Clear	▪ Servicio normal ▪ El dispositivo respondió al ultimo sondeo ▪ Trap recibida (dependiendo de la configuración seleccionada) ▪ Umbral no superado (Dependiendo de la configuración seleccionada)

Tabla 3: Niveles de alerta

A continuación se presenta la pestaña "**Alarmas**", en este caso muestra dos alertas críticas que indican que el dispositivo está caído y no puede ser monitoreado por el OpManager.

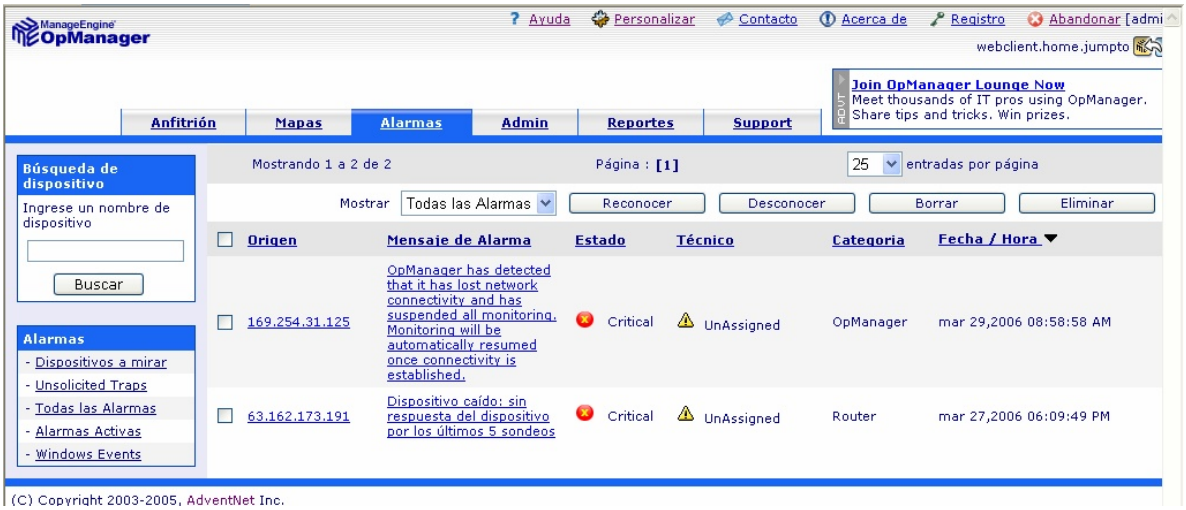


Figura 15: Pestaña Alarmas

Para conocer más detalles sobre el trabajo con alarmas, [Ver la sección "Alarmas"].

7.4 Pestaña Admin

Esta pestaña le permite al administrador configurar el OpManager según lo requiera. Cuenta con una sección de "**Descubrimiento**" con asistentes para el descubrimiento de red, agregar dispositivos, configurar servicios y parámetros SNMP.

La sección "**Definiciones Globales**", permite establecer el tiempo del intervalo de monitoreo, agregar nuevos tipos de dispositivos, agregar cuentas de usuario, configurar el Proxy, etc.

En "**Monitors**", es posible hacer un manejo detallado de todos los monitores que soporta la herramienta, adaptándolos a las necesidades del administrador.

La sección "**Tools**", ofrece al usuario inexperto una manera sencilla de configurar el software según sus requerimientos con el "**Asistente para configuración rápida**". También incluye un mapeador de puertos en el switch y un navegador MIB.

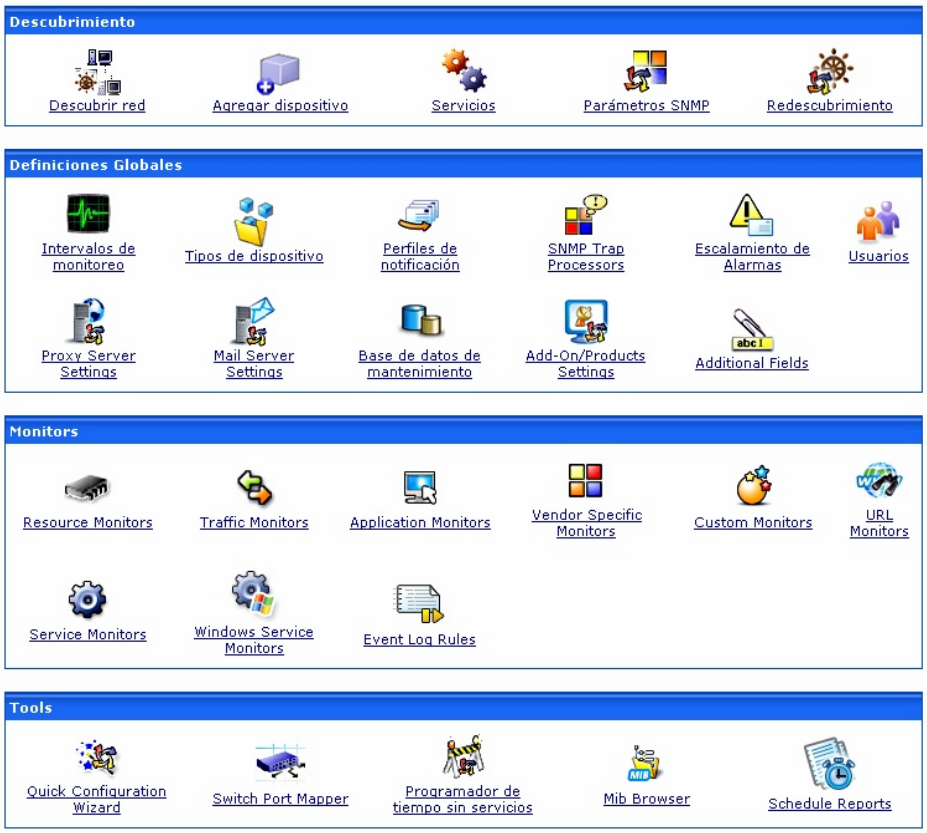


Figura 16: Pestaña Admin

7.5 Pestaña Reportes

En esta pestaña se presentan todos los posibles reportes que la herramienta tiene configurados para cada sección de dispositivos. Se incluyen reportes de Utilización de Memoria, Tráfico Tx y Rx, disponibilidad, errores y muchos más que pueden ser útiles para el administrador de la red. Estos reportes pueden ser exportados a formato “pdf” para su fácil manejo.

También se pueden configurar reportes personalizados y filtrarlos según la preferencia del administrador.

Figura 17: Pestaña Reportes

Para más detalles sobre el trabajo de reportes, [Ver la sección: “Reportes”]

7.6 Pestaña Support

En esta pestaña la compañía desarrolladora del software le ofrece al administrador todo el soporte necesario para garantizar un aprovechamiento total de la herramienta.

Figura 15: Pestaña Support

8. Dispositivos

8.1 Dispositivos soportados

OpManager puede descubrir más de 100 tipos de dispositivos, identificándolos como Routers, Switches, Firewalls, Impresoras, Servidores, Hosts de Escritorio, UPS, Gíreles, etc.

Para verificar los dispositivos soportados por OpManager:

1. Seleccionar la pestaña "**Admin**"
2. Hacer click en "**Tipos de Dispositivos**" en la sección "**Definiciones Globales**".

Inmediatamente se desplegará una lista con todos los dispositivos incluidos por defecto en la librería del OpManager, con su respectiva imagen asociada, su descripción y su OID de descripción del sistema.

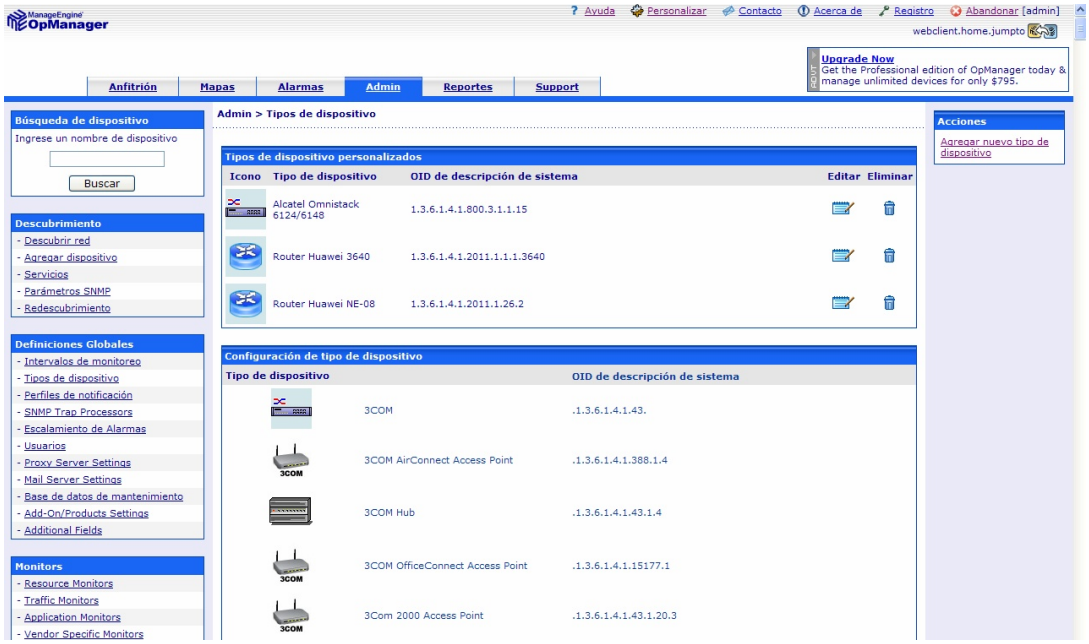


Figura 16: Dispositivos soportados

Los dispositivos no incluidos en esta lista, pueden ser creados manualmente. [Ver: Añadir un nuevo tipo de dispositivo]

Nota:
Cuando el tipo de un dispositivo no sea reconocido por OpManager le asignará el valor "Unknown" en el campo "Tipo de dispositivo"

8.2 Añadir dispositivos

Recordemos que en la versión gratuita, tenemos la posibilidad de agregar hasta 20 dispositivos, por lo tanto tenemos que identificar los dispositivos críticos de la red, que requieran ser monitoreados. En el caso del SENA, se añadieron todos los routers a nivel regional y los switches de la Sede Administrativa.

Las características de estos dispositivos son las siguientes, es importante tenerlas a mano a la hora de añadirlos.

Nodo	Dispositivo	Sede	Dirección IP	Comunidad SNMP
1	Cisco 3640	Administración	172.16.55.247	Public
2	Huawei 3640	Administración	172.16.55.254	Senalcatel
3	Huawei NE-08	Dirección General	172.16.3.1	Senalcatel
4	Cisco 1750	Barranca	172.16.115.253	Senalcatel
5	Cisco 1750	Girón	172.16.117.254	Public
6	Cisco 1750	Florida	172.16.119.253	Public
7	Cisco 1720	San Gil	172.16.123.254	Public
8	Cisco 1720	Vélez	172.16.131.254	Senalcatel
9	Cisco 1720	Piedecuesta	172.16.178.254	Senalcatel
10	Cisco 1720	Málaga	172.16.183.254	Senalcatel
11	AlcatelOmniswitch 6624	Administración– Piso 5	172.16.55.253	Public
12	Alcatel Omnistack 6648	Administración– Piso 4	172.16.55.250	Public
13	Alcatel Omnistack 6648	Administración– Piso 3	172.16.55.249	Public
14	Alcatel Omnistack 6648	Administración - Piso 2	172.16.55.248	Public
15	Alcatel Omnistack 6648	Empleo	172.16.55.241	Public
16	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 2 Torre 1	172.16.55.251	Public
17	Alcatel Omnistack 6624	Centro de Comercio y Servicios Piso 3 Torre 1	172.16.55.244	Public
18	Alcatel Omnistack 6624	Centro de Comercio y Servicios Apoyo	172.16.55.243	Public
19	Alcatel Omnistack 6648	Centro de Comercio y Servicios Inglés	172.16.55.245	Public
20	Alcatel Omnistack 6648	Centro de Comercio y Servicios Aulas	172.16.55.246	Public

Tabla 4: Dispositivos añadidos en el OpManager instalado en la Sede Administrativa del SENA Regional Santander

Para agregar un nuevo dispositivo en OpManager hacemos lo siguiente:

1. Seleccionar la pestaña "**Admin**"
2. Hacer click en "**Agregar Dispositivos**" en la sección "**Descubrimiento**"

Se abrirá la ventana para agregar dispositivos:

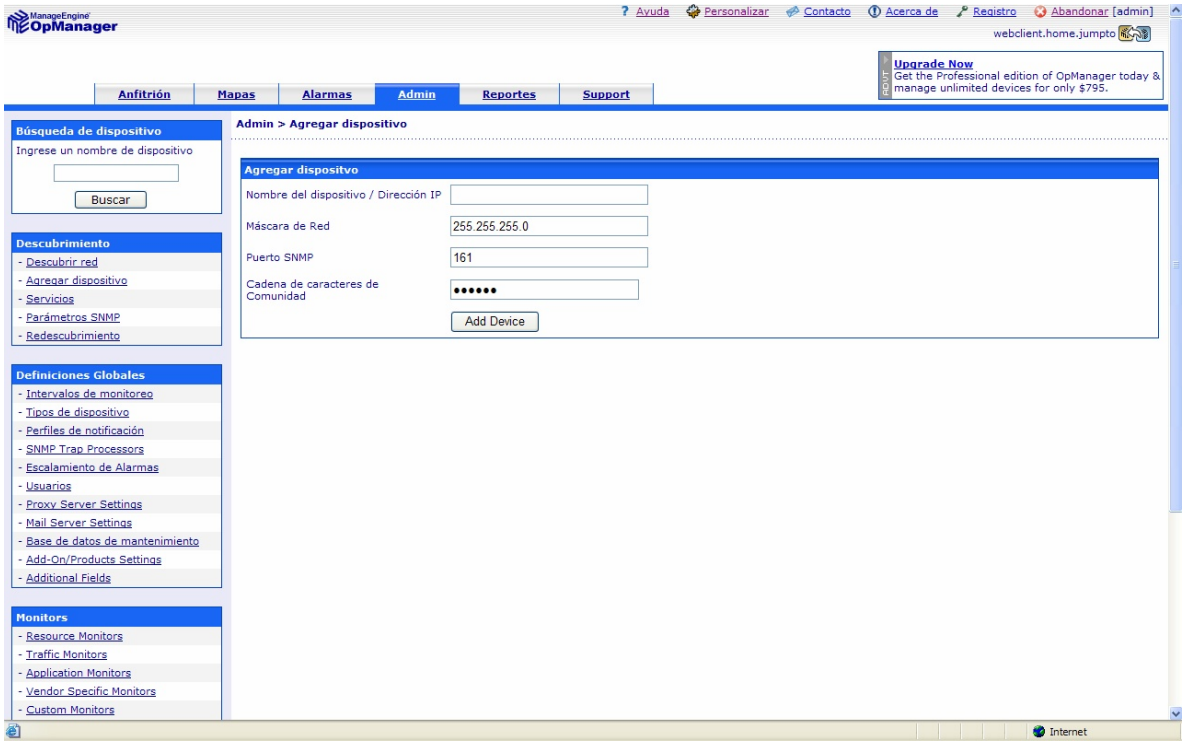


Figura 17: Agregar dispositivo

3. Ingresar los datos correspondientes del dispositivo: Dirección IP, Máscara de Red, Puerto SNMP y comunidad string. Estos datos pueden ser consultados en la tabla anterior.

Nota:

No se debe cambiar el puerto SNMP (161 por defecto)

4. Dar click en "**Add Device**" para agregar el dispositivo. El programa puede tardar cierto tiempo en añadirlo, dependiendo de la congestión de la red en ese momento y del número de puertos que tenga. Al finalizar de añadirlo, se desplegará un mensaje de confirmación.

8.3 Clasificación de dispositivos

El OpManager agrupa los dispositivos detectados o añadidos en la red en las siguientes categorías:

Servidores (), Routers (), Firewalls (), Switches (), Impresoras (),

Escritorio (), URL, UPS (), Inalámbrico () y Domain Controler ()

Una vez clasificados los dispositivos, el programa los agrupa en mapas diferentes bajo ese mismo nombre, para facilitar su administración.

Si OpManager, por alguna razón, no logra descifrar la categoría de algún dispositivo, lo incluye en la lista de **Equipos de Escritorio**, por lo tanto se recomienda, una vez añadidos todos los dispositivos, revisar esta categoría para verificar si se identificaron dispositivos erróneamente y si es el caso, proceder a cambiarla. [Ver cambiar la categoría de dispositivos]

	**Nota:** Para una correcta identificación el dispositivo debe soportar y tener activo el protocolo SNMP.

8.3.1 Cambiar la categoría

Para cambiar la categoría de un dispositivo, seguimos los siguientes pasos:

1. Identificar el dispositivo en la pestaña "**Mapas**" y hacer click sobre su símbolo para acceder a su ventana de detalles

2. En la sección "**Detalles del Dispositivo**", hacer click en "**Edit**" frente a "**Categoría**"

Figura 18: Detalles del Dispositivo

3. Se desplegará la ventana "**Propiedades de Dispositivo**", donde podremos escoger la categoría correcta en la lista desplegable "**Categoría**", como se ve a continuación

Figura 19: Ventana Propiedades del Dispositivo

4. Dar click en "**Guardar**" para cargar los cambios.

8.3.2 Cambiar el tipo

Como se aprecia en la **Figura 18**, otra de los detalles que presenta el OpManager, además de la categoría, es el **tipo de dispositivo**. Si el administrador detecta que un dispositivo está mal clasificado o ha sido identificado como "**Unknown**", es necesario cambiar el tipo de la siguiente manera:

1. Identificar el dispositivo en la pestaña "**Mapas**" y hacer click sobre su símbolo para acceder a su ventana de detalles

2. En la sección "**Configurar**", ubicada en el extremo derecho de la pantalla, hacer click en "**Tipo de Dispositivo**"

Figura 20: Configurar dispositivo

3. Se abrirá la ventana "**Configuración del tipo de dispositivo**", donde podremos seleccionar el tipo adecuado del dispositivo en la lista desplegable.

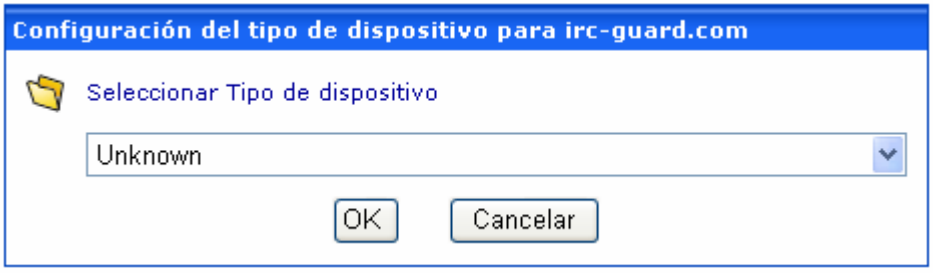


Figura 21: Tipo de dispositivo

4. Dar click en "**Ok**" para guardar los cambios.

8.3.2.1 Añadir un nuevo tipo de dispositivo

Sin embargo, no todas las veces será posible encontrar a nuestro dispositivo en la lista que OpManager ofrece, por lo tanto, se hace necesario agregar un nuevo Tipo de Dispositivo. Para agregar un nuevo dispositivo en OpManager se realiza lo siguiente:

1. Seleccionar la pestaña "**Admin**"
2. Hacer click en "**Tipos de Dispositivos**" en la sección "**Definiciones Globales**".

3. En la sección "**Acciones**" a la derecha de la pantalla, hacer click en "**Agregar nuevo tipo de dispositivo**"

Figura 22: Acciones

4. Se abrirá la ventana "**Agregar nuevo tipo de dispositivo**", en la que podremos incluir el nombre de nuestro dispositivo, el número de identificación OID y la imagen que queremos asociarle.

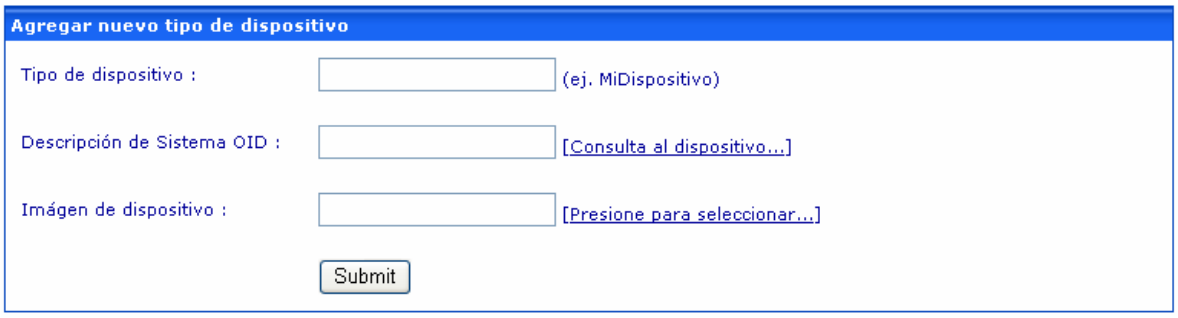


Figura 23: Agregar nuevo tipo de dispositivo

5. Dar click en "**Submit**" para guardar el nuevo dispositivo.

Hay que tener en cuenta que el nombre que se incluya en "**Tipo de Dispositivo**" debe ser único y no repetirse.

También es importante incluir el número de identificación OID para que si se agregan más dispositivos similares, el OpManager los pueda reconocer automáticamente.

Por ejemplo, dentro de los 20 dispositivos agregados en la red del SENA no se reconocieron los switches de marca Alcatel, ni los routers Huawei (administración y Dirección General), por lo tanto se hizo necesario seguir este proceso para identificarlos.

Los OID de estos dispositivos son los siguientes:

Dispositivo	Ubicación	Cantidad	OID
Omnistack 6624	Sede Administrativa	10	1.3.6.1.4.1.800.3.1.1.15
Huawei Quidway 3640	Sede Administrativa	1	1.3.6.1.4.1.2011.1.1.1.3640
Huawei NetEngine 08	Dirección General	1	1.3.6.1.4.1.2011.1.26.2

Tabla 5: OID de los dispositivos no reconocidos por el OpManager en la red de datos del SENA Regional Santander

Para asociar una imagen con un dispositivo, es suficiente con ingresar solamente su nombre, sin necesidad de incluir la ruta. (Ej: router.png, switch.png, etc)

Las imágenes que se pueden asociar están en la carpeta:
C:\Archivos de programa\AdventNet\ME\OpManager, por tanto, si se desea incluir una imagen personalizada debe copiarse a esta carpeta.

Se puede verificar que los dispositivos si fueron añadidos en la sección "**Tipos de dispositivos personalizados**", donde además, se permite editarlos o eliminarlos.

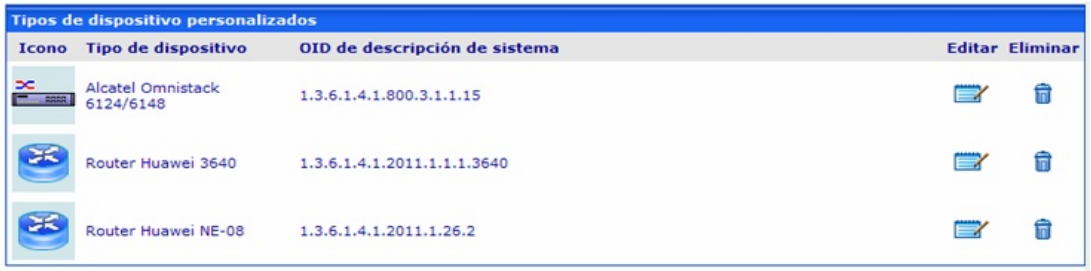


Figura 24: Tipos de dispositivos personalizados

Nota:
Si no se conoce el OID de un dispositivo, se debe hacer click en "Consulta al dispositivo" y escribir en los campos su dirección IP, el puerto y la comunidad SNMP. Luego de hacer click en "Ok" y esperar unos segundos, el OID del dispositivo debe mostrarse.

9. Monitoreo

9.1 Que se puede monitorear?

El monitoreo de red es una herramienta importante para obtener una idea en tiempo real del estado de la red. Sin embargo, un monitoreo frecuente introduce cierto tráfico que puede cargar los recursos de la red, especialmente si esta es de gran tamaño. Por esta razón, es recomendable monitorear, solamente los dispositivos críticos de la red.

Los siguientes componentes se consideran críticos:

- Infraestructura WAN: Routers, Switches, Firewall, etc.
- Infraestructura LAN: Switches, Hubs, Impresoras
- Servidores, Servicios y Aplicaciones: Servidores de aplicaciones, Servidores de Base de datos, Servidores Web, Servidores de Correo, etc.
- Recursos del Host: CPU, Memoria y utilización de disco de dispositivos críticos.
- Host Críticos y estaciones de trabajo.

En la Red de Datos del SENA Regional Santander, se identificaron 20 dispositivos críticos, que incluyen todos los routers de la Sede Administrativa y sus centros, el Router de la Dirección General en Bogotá y todos los Switches de la Sede Administrativa. [Ver Tabla 2]

9.2 Intervalo de Monitoreo

La norma general es monitorear los dispositivos críticos con más frecuencia que los que no son tan críticos.

A continuación presentamos los tiempos de monitoreo recomendados para cada dispositivo:

Dispositivo	Intervalo
Routers y Servidores Críticos	5 – 10 minutos
Switches, Hubs e Impresoras	10 – 20 minutos
Host y Estaciones de Trabajo	1 hora (para reducir la cantidad de tráfico generado por OpManager)

Tabla 6: Intervalos de monitoreo recomendados

Para configurar un intervalo de monitoreo en cada categoría de dispositivos, hacemos lo siguiente:

1. Hacer click en la pestaña "**Admin**"
2. En "**Definiciones Globales**", hacer click en "**Intervalos de Monitoreo**"
3. Para habilitar el monitoreo para una categoría, seleccionar la casilla de verificación y teclear el intervalo de monitoreo en minutos en el campo correspondiente.
4. Hacer click en "**Guardar**"

9.3 Monitoreando dispositivos

OpManager permite monitorear diversos dispositivos por medio del menú de dispositivo, que muestra la información sobre el hardware y el software del dispositivo. Dentro de los dispositivos que se pueden monitorear están: Router, Switches, UPS, Servidores Exchange, Servicios de Windows, Proxies, URL.

9.3.1 Indicadores

Al abrir el mapa de los dispositivos, se tendrá una idea de cuál es el estado de cada uno observando sus indicadores.

Dispositivo	Indicadores
Routers	
Switches	
UPS	
Servidores	

Tabla 7: Indicadores

El Indicado estado ( ), da una idea del funcionamiento global del router, y su color corresponde a los niveles de alerta. [Ver Tabla 3].

Por su parte, el indicador SNMP ( ), aparece cuando el dispositivo soporta este tipo de agente para su gestión.

El indicador Tipo, da una idea de la categoría a la cual pertenece el dispositivo y por lo tanto es diferente para cada una.

En los servidores se presentan también indicadores de los servicios que se encuentran instalados y del Sistema Operativo que los soporta.

9.3.2 Menú de dispositivos

Para ver el menú de dispositivos, hacer click en el nombre del mismo en la pestaña "**Mapas**". A continuación se abrirá el menú de dispositivo

Este menú tiene varias secciones:

9.3.2.1 Detalles del dispositivo:

Muestra detalles del sistema, como su nombre, su estado, su dirección IP, su máscara de red y su descripción, entre otras.

Detalles del Dispositivo	
Nombre	**Administración Huawei**
Estado	**Trouble**
Dirección IP	172.16.55.254
Máscara de Red	255.255.255.192
Categoria	**Router** [Edit]
Tipo	**Router Huawei 3640**
Desc. Sistema	Quidway Router R3640E Huawei Versatile Routing Platform Software VRP (R) software, Version 1.74 Release 0105
Ultima Alarma	Interface IF-172.16.55...
Ultima Obtención en	Mar 31,2006 12:12:01 PM
Próxima Obtención en	Mar 31,2006 12:17:04 PM
	[Add More Details]

Figura 25: Detalles del dispositivo

9.3.2.2 Disponibilidad actual:

Muestra la disponibilidad diaria del dispositivo en forma gráfica. Al hacer click en "**7**" o en "**30**", se puede obtener el reporte de disponibilidad en la última semana o en el último mes, según se requiera.

Figura 26: Disponibilidad actual

9.3.2.3 Tiempo de Respuesta:

Muestra el tiempo de respuesta del dispositivo en milisegundos. Al hacer click en "**7**" o en "**30**", se pueden obtener detalles del tiempo de respuesta en la última semana o en el último mes, según se requiera.

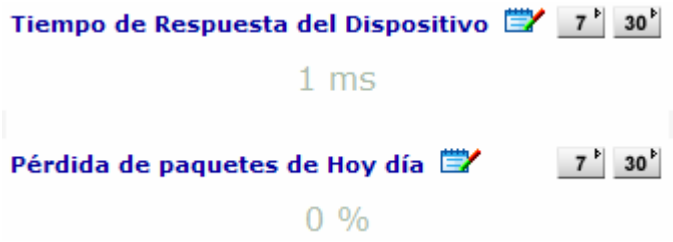


Figura 27: Tiempo de respuesta

9.3.2.4 Utilización de CPU:

Muestra la actual carga de trabajo del procesador principal del dispositivo. Al hacer click en la gráfica, se puede observar el gráfico de tendencia de la carga de CPU.

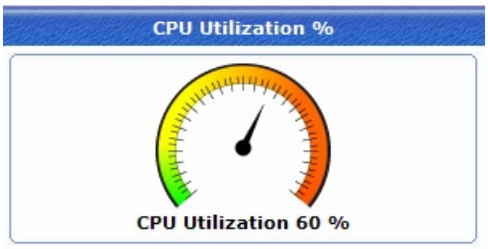


Figura 28: Utilización de CPU

9.3.2.5 Utilización de memoria:

Muestra la memoria que en ese instante se esté utilizando en el dispositivo.

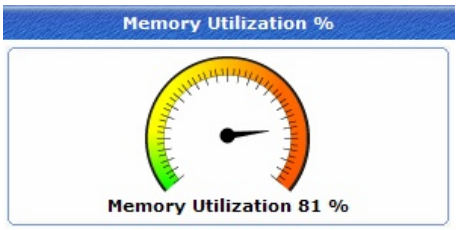


Figura 29: Utilización de memoria

9.3.2.6 Utilización de disco:

Muestra el espacio utilizado y disponible en el disco del dispositivo lo que puede ser de gran utilidad especialmente en el manejo de servidores.

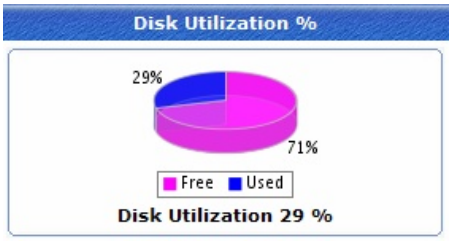


Figura 30: Utilización de disco

9.3.2.7 Monitores:

Presenta un listado de todos los monitores que OpManager puede asociar a los dispositivos. Se encuentran subdivididos en: Resourse Monitores, Traffic Monitores, Aplication Monitores, Vendor Specific Monitores, Custom Monitores. Para ver los monitores que se encuentran configurados se puede dar click en en "**Show**". Si se quieren agregar más monitores, se puede dar click en "**Add Monitor**" en cada una de las categorías.

Figura 31: Monitores

9.3.2.8 Interfaces:

Muestra un listado de todas las interfaces del dispositivo seleccionado, junto a su estado y otras características como: Utilización de Rx, Utilización de Tx, Tráfico Rx, Tráfico Tx y errores. Al hacer click sobre una interfaz, se despliegarán las gráficas de disponibilidad, tráfico y ancho de banda.

Interfaces

Indice	Descripción	Velocidad (Mbps)	Estado	Desplegar Nombre	Utilización de Recepción - Rx (%)	Utilización de Transmisión - Tx (%)	Tráfico Recepción - Rx (Kbps)	Tráfico Transmisión - Tx (Kbps)	Errores (paquetes)
1	Aux0	0		IF-172.16.55.2...	0	0	0	0	0
2	Bri0	0		IF-172.16.55.2...	0	0	0	0	0
3	Bri1	0		IF-172.16.55.2...	0	0	0	0	0
4	Bri2	0		IF-172.16.55.2...	0	0	0	0	0
5	Bri3	0		IF-172.16.55.2...	0	0	0	0	0
6	Ethernet0	100		Ethernet inter...	3	8	392	897	0
8	Serial0:0	2		E1-DIRECCION-N...	50	23	1008	459	0
9	Serial1:0	0		IF-172.16.55.2...	0	0	0	0	0
10	Serial1:1	0		PIEDECUESTA	48	37	63	47	0
11	Serial1:2	0		VELEZ	12	14	15	19	0
12	Serial1:3	0		SAN GIL	2	9	3	12	0
13	Serial1:4	0		BARRANCABERMEJA	7	23	10	30	0
14	Serial1:5	0		MALAGA	6	25	8	33	0

Figura 32: Interfaces

9.3.2.9 Acciones:

Presenta un listado de las acciones que se pueden hacer en el dispositivo. Se incluyen: Actualización de estado, Redescubrir ahora, Ping, Trazar ruta, Mostrar Alarmas, Eliminar, Desadministrar y Reporte personalizado

Figura 33: Acciones

9.3.2.10 Configurar:

Presenta un listado de las características que se pueden configurar en el dispositivo, según se requiera. Se incluyen: Propiedades del dispositivo, Monitoreo, Tipo de dispositivo, Dependencia y Configurar Interfaces.

Figura 34: Configurar

9.3.2.11 Información del dispositivo:

Permite obtener ciertas características propias del dispositivo, como por ejemplo su tabla de rutas y su tabla de direcciones si es un router.

Figura 35: Información del dispositivo

Nota:

En cualquier caso, es indispensable tener apropiadamente configurados los parámetros SNMP del dispositivo, para poder acceder a todas las opciones de monitoreo que se incluyen en el menú del dispositivo. [Ver Modificar los parámetros SNMP de un dispositivo]

9.3.3 Modificar los parámetros SNMP de un dispositivo

En ocasiones se requiere modificar los parámetros SNMP de un dispositivo en caso de que el puerto o su comunidad hayan sido cambiadas o no sean las especificadas por defecto.

Para modificar las características SNMP, seguimos los siguientes pasos:

1. Abril el menú de dispositivo
2. En la sección "**Configurar**", seleccionar "**Passwords**"
3. Modificar los valores del puerto del protocolo SNMP y la comunidad string, que se desplegarán.
4. Hacer click en "**Aceptar**" para cargar los cambios.
5. Hacer click en "**Redescubrir Ahora**" en la sección "**Acciones**" para descubrir el dispositivo nuevamente pero con los parámetros modificados

	**Advertencia**: Cuando un dispositivo es redescubierto, los datos obtenidos anteriormente de disponibilidad y tiempo de respuesta, se perderán.

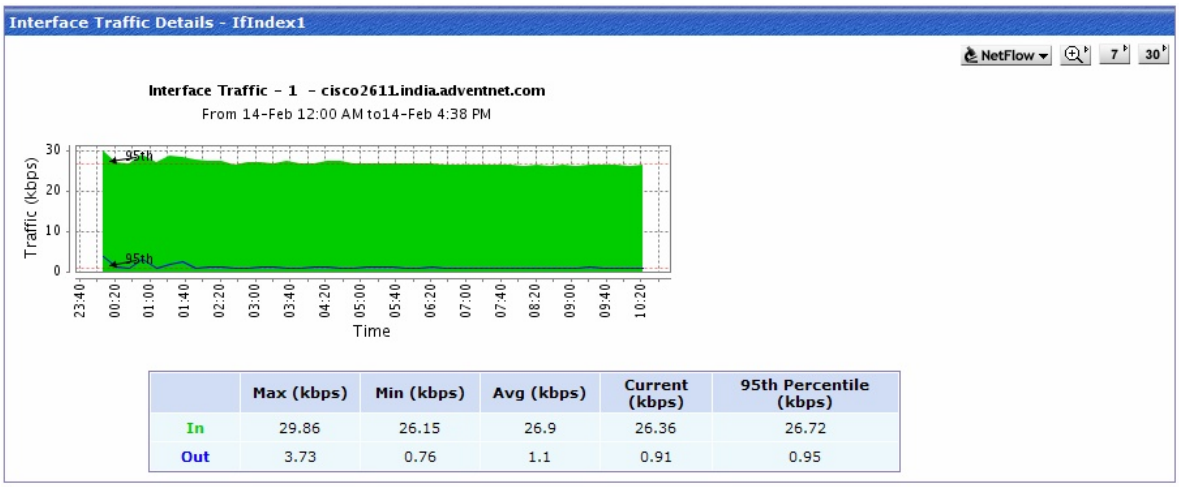
9.3.4 Gráficas

OpManager, permite visualizar una gran variedad de parámetros de manera gráfica, lo cual facilita al administrador determinar el estado de los dispositivos que conforman la red. Además, es posible configurar gráficas personalizadas de cualquier variable SNMP soportada por estos dispositivos.

Para acceder a las gráficas se debe hacer click sobre el parámetro deseado en el menú del dispositivo; inmediatamente se abrirá la gráfica en una nueva ventana.

A continuación se presenta la gráfica del tráfico Tx de una interfaz de un router, como se puede apreciar, además de la gráfica, OpManager también genera una tabla de valores cada cierto tiempo, lo cual puede resultar útil para el administrador.

Los botones  son utilizados para hacerle un zoom a la gráfica, para graficar el comportamiento de los últimos 7 días o de los últimos 30 días, respectivamente.



	Max (kbps)	Min (kbps)	Avg (kbps)	Current (kbps)	95th Percentile (kbps)
In	29.86	26.15	26.9	26.36	26.72
Out	3.73	0.76	1.1	0.91	0.95

Figura 36: Gráficas de OpManager

Algunas de las gráficas generadas por OpManager son las siguientes:

9.3.4.1 Gráficas de Recursos de Host

Perfiles para recolectar datos sobre utilización de CPU, memoria y disco para dispositivos con SNMP habilitado. Son comunes para sistemas Windows, Linux y Solaris.

9.3.4.2 Tráfico Rx y tráfico Tx de la interfaz

Genera la gráfica del número de paquetes recibidos y transmitidos por la interfaz. Por defecto, los datos graficados en esta gráfica son recolectados por OpManager cada 10 minutos. Esta gráfica sólo está disponible para dispositivos que soporten SNMP.

9.3.4.3 Utilización Rx y utilización Tx de la interfaz

Genera la gráfica del porcentaje de utilización de ancho de banda mientras se reciben o se transmiten paquetes, teniendo en cuenta una o más interfaces del dispositivo. El porcentaje de utilización se calcula utilizando las siguientes fórmulas:

Utilización Rx: (2.2.1.10*8*100)/((2.2.1.5)*(intervalo de muestreo en segundos)

Utilización Tx: (2.2.1.16*8*100)/((2.2.1.5)*(intervalo de muestreo en segundos)

Por defecto, los datos a graficar se obtienen de los dispositivos cada 10 minutos. Esta gráfica sólo está disponible para dispositivos que soporten SNMP.

9.3.4.4 Errores y descartes de la interfaz

Muestra la gráfica de los errores y los paquetes descartados de la interfaz. Esta gráfica sólo está disponible para dispositivos que soporten SNMP.

9.3.4.5 Tiempo de respuesta

Muestra la gráfica del tiempo de respuesta del dispositivo al hacerle un escaneo de su estado. Si el dispositivo tiene servicios corriendo en él, OpManager, también grafica el tiempo de respuesta de los servicios. Esta gráfica sólo está disponible para dispositivos que soporten SNMP.

9.3.5 Monitoreo de Routers

Para iniciar el monitoreo de un router y sus respectivas interfaces:

1. Entrar a su respectivo menú, haciendo click en la pestaña Mapas y luego en Routers.
2. Se abrirá el mapa de todos los routers que se están monitoreando con sus respectivas interfaces y su estado.
3. Dar click en el router que se desee monitorear

9.3.5.1 Administrar y desadministrar interfaces

1. Una vez en el menú del dispositivo, para administrar una interfaz que no se encuentre activa, hacer click en "**Configurar Interfaces**" dentro de la sección "**Configurar**".
2. Se abrirá una nueva ventana que mostrará las interfaces del router con una casilla de verificación para habilitar o deshabilitar su administración.
3. Si se requiere en esa ventana también se puede modificar el nombre que muestra la interfaz

Nota:

En caso de que se quiera desadministrar alguna interfaz, se debe deseleccionar la casilla de verificación correspondiente.

9.3.5.2 Cambiar el nombre del router

1. Abrir el menú del router
2. Hacer click en "**Propiedades del dispositivo**" en la sección "**Configuración**"
3. Incluir el nombre que se desee en la casilla y dar click en "**Aceptar**" para guardar los cambios.

9.3.5.3 Ver la tabla de rutas

1. Abrir el menú del router
2. Hacer click en "**Tabla de rute IP**" en la sección "**Información del dispositivo**"

9.3.5.4 Ver la tabla de direcciones IP

1. Abrir el menú del router
2. Hacer click en "**Tabla de direcciones IP**" en la sección "**Información del dispositivo**"

9.3.6 Monitoreo de Switches

Para iniciar el monitoreo de un switch y sus respectivos puertos:

1. Entrar a su respectivo menú, haciendo click en la pestaña Mapas y luego en Switches.
2. Se abrirá el mapa de todos los switches que se están monitoreando con sus puertos y su estado.
3. Dar click en el switch que se desee monitorear

9.3.6.1 Administrar y desadministrar puertos

1. Una vez en el menú del dispositivo, para administrar una interfaz que no se encuentre activa, hacer click en "**Configurar Interfaces**" dentro de la sección "**Configurar**".
2. Se abrirá una nueva ventana que mostrará todos los puertos del switch con una casilla de verificación para habilitar o deshabilitar su administración.
3. Si se requiere en esa ventana también se puede modificar el nombre que muestra el puerto.

Nota:

En caso de que se quiera desadministrar algún puerto, se debe deseleccionar la casilla de verificación correspondiente.

9.3.6.2 Switch Port Mapper

OpManager, permite mostrar la conectividad entre un switch y otros dispositivos conectados a la red, mediante la herramienta “Switch Port Mapper”. Se pueden obtener detalles como la dirección MAC, la dirección IP y los DNS de los dispositivos conectados al switche.

Para utilizar el Port Mapper, hacemos:

1. Abrir el menú del router
2. Hacer click en “**Switch Port Mapper**” en la sección “**Información del Dispositivo**”
3. Ingresar los detalles del switch, como su dirección IP y su comunidad SNMP.
4. Hacer click en “**Mostrar Mapa**” para ver los detalles

9.3.7 Monitoreo de UPS

Los recursos de una UPS conectada en red que se pueden monitorear son: carga, voltaje de salida, corriente de salida, porcentaje de carga de la batería y vida útil de la batería.

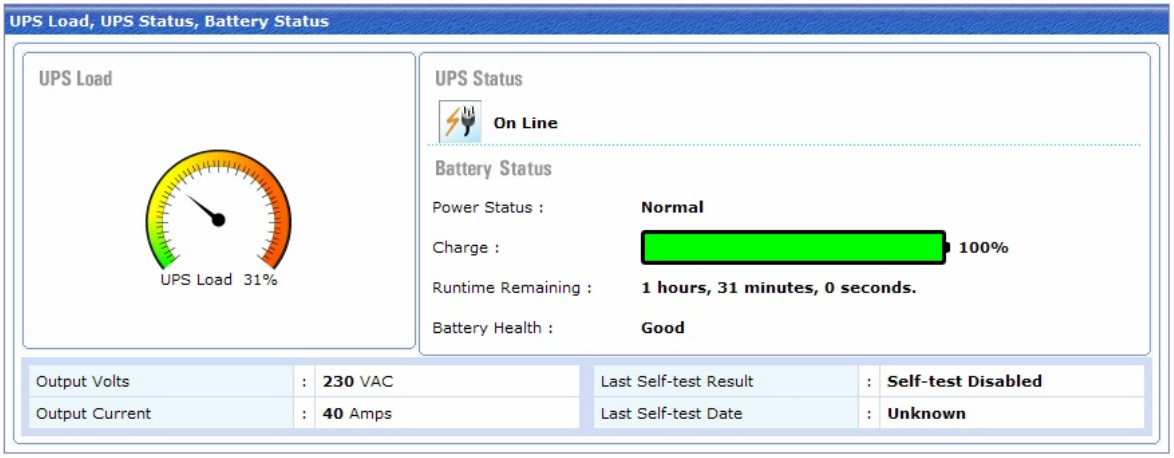


Figura 37: Monitoreo de una UPS

Para monitorear estos recursos, debemos seguir los siguientes pasos:

1. En el menú de la UPS, ubicar la sección “**Vendor Specific Monitors**” y dar click en “**Add Monitors**”
2. Hacer click en APC para que se despliegue la lista de los recursos que pueden ser monitoreados
3. Seleccionar los recursos que se requieran y dar click en “**Aceptar**” para añadirlos.

9.3.8 Monitoreo de Servidores Exchange

OpManager permite monitorear parámetros y servicios críticos de servidores MSExchange 2000/2003 tales como:

Servicios:

- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendent
- Routing Engine
- Event Service

Parámetros:

- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

Para configurar servicios Exchange para ser monitoreados, hacemos lo siguiente:

1. Ir al menú del dispositivo en el que se encuentra corriendo el Servicio Exchange.
2. Hacer click en la opción “Add Monitor” dentro de la sección “**Aplication Monitors**”.
3. Hacer click en “**MSExchange 2000/2003 Monitos (WMI Based)”**
4. Seleccionar los servicios requeridos y hacer click en “**Aceptar**” para añadirlos.

9.3.9 Monitoreo de Servicios de Windows

Ciertas aplicaciones de Windows se instalan como servicios en la red. OpManager permite monitorear su estado.

Algunos de los servicios de Windows monitoreados por OpManager son:

- Alerter
- DHCP Server
- DNS Server
- Disk Manager
- Event Log
- FTP
- IAS
- IIS
- Messenger
- MySQL
- Net Logon
- Print Spooler
- RPC
- Telephony
- Telnet

Para añadir un monitor de Servicio de Windows, seguir los siguientes pasos:

1. En la pestaña "**Admin**", hacer click en "**Windows Service Monitors**"
2. En "**Acciones**" hacer click en "**Add New Service**"
3. Escribir el nombre del servicio en el campo "**Service Name**"
4. Escribir el nombre a desplegar para este servicio en el campo "**Name**"
5. Hacer click en "**Add Service**" para añadir el servicio.
6. Posteriormente usar el link "**Asóciate to devices**" en la sección "**Acciones**" para asociar este servicio a los servidores que se desee.

10. Alarmas

OpManager, facilita la identificación rápida de fallos en la red o en dispositivos por medio de las alarmas. Para entrar a la sección Alarmas, hacemos click en la pestaña con el mismo nombre.

También se presentarán las alarmas activas en la pantalla de inicio del OpManager Client, y una gráfica de las mismas con su estado asociado a un color, según los Niveles de Alerta presentados en la sección 7.3.1 [Ver Tabla 3], facilitando su atención para el usuario.

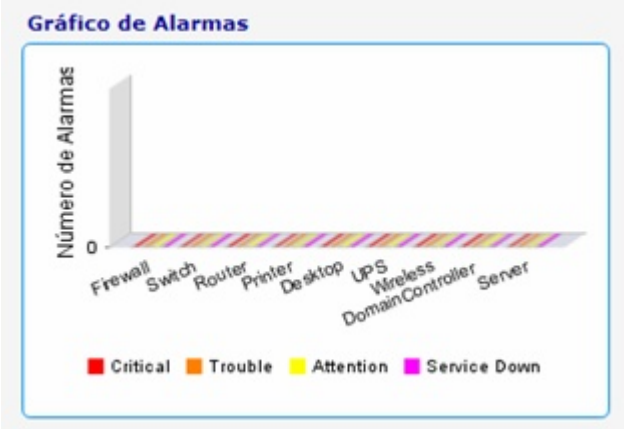


Figura 38: Gráfico de Alarmas Inicial

10.1 Configuración

OpManager permite configurar las alarmas para que estén activas sólo por cierto tiempo y posteriormente se eliminen automáticamente:

1. Hacer click en la pestaña "**Admin**"
2. En "**Definiciones Globales**" hacer click en "**Mantenimiento de la Base de Datos**"
3. En la casilla "**Mantener ____ alarmas recientes en la base de datos**", escribir el número de alarmas recientes que se desea mantener siempre. El valor por defecto es 10000.
4. En la casilla "**Borrar eventos antiguos cada ____ día**s", escribir el número de días durante los que se quieran guardar los eventos. Por defecto el número de días es 30, a partir del día en que se generó.
5. Hacer click en "**Salvar**" para guardar los cambios.

10.2 Manejo de Alarmas

Las alarmas están agrupadas en la pestaña "**Alarmas**" y para su administración, el usuario cuenta con las siguientes opciones:

10.2.1 Reconocer alarmas

Se utiliza para marcar las alarmas que ya se hayan atendido.

1. Hacer click en el icono (Atención) en la sección "**Acciones**", de la alarma correspondiente.
2. El icono cambiará a (Reconocida)

Nota:

- Si se hace click sobre el estado de la alarma volverá a (Atención)
- Es posible reconocer varias alarmas al mismo tiempo, seleccionándolas y posteriormente haciendo click en "Reconocer"

10.2.2 Añadir notas

Se utiliza para añadir notas a la alarma, que expliquen los pasos a seguir para corregir la falla si esta se llegase a presentar.

1. Hacer click en la pestaña "**Alarmas**"
2. Hacer click sobre la alarma a la que se le quiere añadir la nota
3. Hacer click en (Añadir Nota)
4. Escribir la nota en la ventana que se abre y dar click en "**Añadir**"

10.2.3 Limpiar y Borrar alarmas

Algunas alarmas generadas por OpManager, no se limpian automáticamente aún si ya se han corregido en el dispositivo, por lo tanto es necesario limpiarlas manualmente.

Para limpiar las alarmas deseadas, simplemente la seleccionamos y damos click en "**Clear**".

Además, todas las alarmas que se generan, quedan grabadas en la lista de alarmas, hasta que sean borradas automáticamente por OpManager cuando excedan el límite o manualmente por el usuario de la siguiente manera:

1. Seleccionar la alarma deseada
2. Hacer click en "**Delete**" y luego en "**Aceptar**" para confirmar.

11. Reportes

El trabajo con reportes le permite al administrador obtener la información que necesita para conocer el desempeño de toda la red y de cada uno de los dispositivos que la conforman.

En la ventana inicial del Web Client, se presentan varios reportes críticos, como vemos a continuación: Las 5 interfaces de routers con mayor tráfico Rx y Tx y los 5 routers con más alta utilización de memoria.

Interfaces de Router con alto tráfico - Recepción Rx - última(s) 24 hora(s)

Nombre	Nombre de interfaz	Valor Promedio
Dirección General	Ethernet5/2/0	12.55 Mbps
Dirección General	Serial4/0/3:0(cE1)	1.85 Mbps
Administración	Serial1:3	354.5 kbps
Administración	Serial0:0	268.6 kbps
Administración	Ethernet0	83.16 kbps

Figura 39: Interfaces de Router con alto tráfico recibido

Interfaces de Router con alto tráfico - Trasmisión Tx - última(s) 24 hora(s)

Nombre	Nombre de interfaz	Valor promedio
Dirección General	Ethernet5/2/0	4.43 Mbps
Dirección General	Serial4/0/3:0(cE1)	1.16 Mbps
Administración	Ethernet0	223.04 kbps
Administración	Serial1:3	201.93 kbps
Administración	Serial0:0	84.55 kbps

Figura 40: Interfaces de Router con alto tráfico transmitido

Routers con alta utilización de memoria - última(s) 24 hora(s)

Nombre	Utilización
Barranca	40 %
Administración	24 %
San Gil	21 %
Girón	13 %
Florida	13 %

Figura 41: Routers con alta utilización de memoria

Además, en la pestaña "**Reportes**" se pueden generar otros reportes diferentes de cada uno de los dispositivos que se agrupan en las siguientes categorías:

11.1 Reportes de Servidores

Utilización de CPU, utilización de memoria, espacio en disco, tráfico de la interfaz y utilización, disponibilidad del servidor.

Servidores	
Nombre del reporte	**Descripción**
10 principales reportes	
Servidores por utilización de CPU	Identifique servidores ocupados, con alta utilización de CPU
Servidores por utilización de memoria	Identifique servidores sobrecargados con alta utilización de memoria
Servidores por utilización de disco	Identificar servidores sobrecargados con alta utilización de disco
Servidores por tráfico Rx	Identifica servidores con tráfico entrante recargado
Servidores por tráfico Tx	Identifica servidores con tráfico de salida recargado
Servidores por Utilización Rx	Identificar servidores con utilización de tráfico entrante recargado
Servidores por utilización Tx	Identificar servidores con utilización de tráfico de salida recargado
Volúmenes con mínimo espacio libre	Identificar particiones de disco con menor cantidad de espacio libre disponible
Volúmenes con mayor espacio libre	Identificar particiones de disco con mayor espacio libre disponible
Reportes detallados	
Reporte de utilización de disco para todos los servidores	Obtener reporte actualizado de utilización de disco para todos los servidores
Reporte de disponibilidad - Todos los servidores	Obtener reporte de disponibilidad para todos los servidores

Figura 42: Principales reportes de servidores

11.2 Reportes de Routers

Utilización de CPU, utilización de memoria, espacio en disco, tráfico de la interfaz y utilización, disponibilidad de las interfaces.

Routers	
Nombre del reporte	**Descripción**
10 Principales Reportes	
Routers por utilización de CPU	Identificar routers ocupados con alta utilización de CPU
Routers por utilización de Memoria	Identificar routers sobrecargados con alta utilización de memoria
Interfaces por Tráfico Rx	Identificar interfaces con tráfico entrante muy pesado
Interfaces por tráfico Tx	Identificar interfaces con tráfico saliente muy pesado
Interfaces por errores Rx	Identificar interfaces con alta cantidad de errores entrantes
Interfaces por errores Tx	Identificar interfaces con alta cantidad de errores de salida
Interfaces por utilización Rx	Identificar interfaces con alto porcentaje de utilización - Recepción
Interfaces por utilización Tx	Identificar interfaces con alto porcentaje de utilización - Transmisión
Reportes detallados	
Reporte de disponibilidad - Todas las interfaces	Obtener reporte de disponibilidad para todas las interfaces

Figura 43: Principales reportes de routers

11.3 Reportes de Switches

Tráfico de puertos, porcentaje de utilización de puertos, errores en puertos.

Switches	
Nombre del reporte	**Descripción**
10 reportes principales	
Puertos por tráfico Rx	Identificar puertos con tráfico entrante muy pesado
Puertos por tráfico Tx	Identificar puertos con tráfico saliente muy pesado
Puertos por errores Rx	Identificar puertos con mayor cantidad de errores de recepción
Puertos por errores Tx	Identificar puertos con mayor cantidad de errores de transmisión
Puertos por utilización Rx	Identificar puertos con alto porcentaje de utilización - Recepción
Puertos por utilización Tx	Identificar puertos con alto porcentaje de utilización - Transmisión

Figura 44: Principales reportes de switches

11.4 Reportes de Aplicaciones

Tiempo de respuesta para HTTP, SMTP y aplicaciones MySQL.

Aplicaciones	
Nombre del reporte	**Descripción**
10 Principales reportes	
Servidores HTTP por tiempo de respuesta	Identificar servidores web con alto tiempo de respuesta
Servidores SMTP por tiempo de respuesta	Identificar servidores SMTP con alto tiempo de respuesta
Servidores MySQL por tiempo de respuesta	Identificar servidores MySQL con alto tiempo de respuesta
Servidores FTP por tiempo de respuesta	Identificar servidores FTP con alto tiempo de respuesta
Servidores Telnet por tiempo de respuesta	Identificar servidores Telnet con alto tiempo de respuesta

Figura 45: Principales reportes de aplicaciones

11.5 Reportes de Todos los dispositivos

Utilización de CPU, utilización de memoria, espacio en disco, tráfico de la interfaz y utilización.

Todos los dispositivos	
Nombre del reporte	**Descripción**
10 Principales reportes	
Todos los dispositivos por utilización de CPU	Identificar dispositivos ocupados con alta utilización de CPU
Todos los dispositivos por utilización de memoria	Identificar dispositivos sobrecargados con alta utilización de memoria
Dispositivos por utilización de disco	Identificar dispositivos sobrecargados con alta utilización de disco
Interfaces por tráfico Rx	Identificar dispositivos con tráfico entrante muy pesado
Interfaces por tráfico Tx	Identificar dispositivos con tráfico saliente muy pesado
Interfaces por errores Rx	Identificar interfaces con alta cantidad de errores entrantes
Interfaces por errores Tx	Identificar interfaces con alta cantidad de errores de salida
Interfaces por utilización Rx	Identificar dispositivos con utilización de tráfico entrante muy pesada
Interfaces por utilización Tx	Identificar dispositivos con utilización de tráfico saliente muy pesada
Reporte de disponibilidad - Todos los dispositivos	Obtener reporte de disponibilidad para todos los dispositivos

Figura 46: Principales reportes de todos los dispositivos

11.6 Inventario

Realiza un inventario de todos los dispositivos añadidos al OpManager.

Inventory Reports	
Nombre del reporte	**Descripción**
Inventory Reports	
Servidores	Reporte de inventario de Servidores
Equipos de escritorio	Reporte de Inventario de Equipos de Escritorio
Todos los Dispositivos	Reporte de Inventario - Todos los dispositivos
Dispositivos habilitados con SNMP	Reporte de Inventario SNMP
Dispositivos no habilitados con SNMP	Reporte de Inventario no SNMP

Figura 47: Principales reportes de inventario

11.7 Reportes personalizados

Es posible ver al mismo tiempo varias gráficas del mismo dispositivo y obtener una versión impresa del mismo usando la utilidad de reportes personalizados.

Para obtener un reporte personalizado de un dispositivo, seguimos los siguientes pasos:

1. En la pestaña "**Reportes**" dar click en "**Ejecutar reporte personalizado**"
2. Escribir el nombre del dispositivo o usar "**Seleccionar dispositivo**" para añadirlo por medio de una lista.
3. Seleccionar las gráficas que se quieren ver y hacer click en "**Mostrar Reporte**"

11.8 Ver reportes

1. Hacer click en la pestaña "**Reportes**". Se abrirá una ventana con todos la lista de todos los reportes disponibles para cada uno de los dispositivos con una breve descripción.
2. Hacer click en el reporte que se quiera ver.

Nota:

- Por defecto los reportes que se muestran son para el mismo día de la consulta. Sin embargo, se puede ver el reporte de un periodo específico de tiempo seleccionándolo de la lista de "Ventana de Tiempo".
- Para cambiar el periodo del reporte al día anterior, a los últimos 7 días, a los últimos 30 días, etc. Usar la lista desplegable "Periodo"
- Para ver el reporte en cualquier otro intervalo de tiempo, usar las casillas "Start Time" y "End Time".

11.9 Salvar e imprimir reportes

1. Abrir la pestaña “**Reportes**”
2. Seleccionar el reporte que se quiera ver
3. Para salvar el reporte en formato PDF, hacer click en “**Exportar a PDF**”
4. Para imprimir el reporte, hacer click en “**Vista de Impresión**” y luego en “**Print**”

12. MIB Browser

La herramienta MIB Browser permite cargar y explorar los MIBs para manejar todas las operaciones SNMP relacionadas.

Las características del MIB Browser incluyen:

- Guardar las opciones del MIB
- Cargar y ver los módulos en el árbol MIB
- Explorar el árbol MIB para ver las definiciones de cada uno de los nodos
- Ejecutar las operaciones básicas de SNMP como GET, GETNEXT, GETBULK y SET
- Graficar en tiempo real los datos SNMP
- Vista en forma de tabla de los datos SNMP

12.1 Interfaz MIB Browser

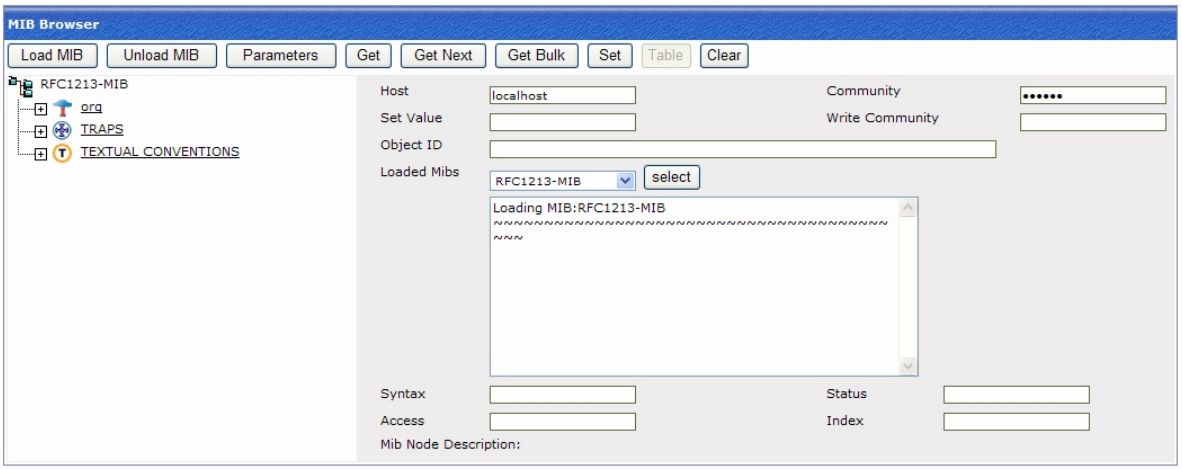


Figura 48: MIB Browser

Barra de menú:

Contiene los comandos para realizar todas las operaciones administrativas

Toolbar:

Facilita el acceso a los comandos más utilizados agrupándolos en una barra de herramientas

MIB Tree:

Muestra toda las MIBs cargadas permitiendo explorar el árbol y ver la definición de cada uno de los nodos

Configuración SNMP:

Muestra la configuración SNMP del nodo seleccionado

Area de despliegue de resultados:

Muestra los resultados de las operaciones SNMP

Atributos de objetos:

Muestra los atributos del nodo seleccionado

12.2 Abrir el MIB Browser

1. Hacer click en la pestaña "**Admin**"
2. Hacer click en "**MIB Browser**" en la sección "**Tools**"

12.3 Cargar MIBs

1. Abrir el MIB Browser
2. Hacer click en "**Load MIB**"
3. Seleccionar el archivo MIB a cargar
4. Hacer click en "**Load**"

13. Business Views

Además de las "**Vistas de Infraestructur**a" y las "**Vistas de Red**", que se presentan en la pantalla inicial del Web Client, OpManager permite crear vistas personalizadas o "Vistas de Negocio" que se adapten a las necesidades de la red.

Estas vistas le permiten al usuario, agrupar dispositivos de su interés según su ubicación geográfica y manejarlos desde una misma ventana o añadir nuevas categorías de dispositivos si estos no se pueden clasificar entre las que aparecen en las "**Vistas de Infraestructura**".

En las "Vistas de Negocio", es posible añadir enlaces entre los dispositivos que le indiquen al administrador de una manera gráfica cuál es la topología de la red y si el enlace se encuentra funcionando correctamente o presenta dificultades en la recepción o la transmisión de datos.

Por último, para completar la personalización de las vistas de negocio, también se puede añadir una imagen de fondo que presente la distribución de los dispositivos, por ejemplo en un edificio o en una región determinada.

13.1 Vistas de Negocio de la Red del SENA

Para manejar la Red de Datos de la Regional Santander del SENA, se crearon en total 3 vistas de negocio: La vista "Mapa Santander", la vista "Red Regional" y la vista "Administración", como se muestra a continuación.

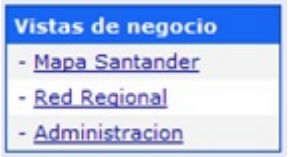


Figura 49: Vistas de Negocio SENA

13.1.1 Vista Mapa Santander

Esta vista presenta la ubicación geográfica de todos los centros que conforman el SENA Regional Santander y el estado de sus respectivos enlaces de red según su color.

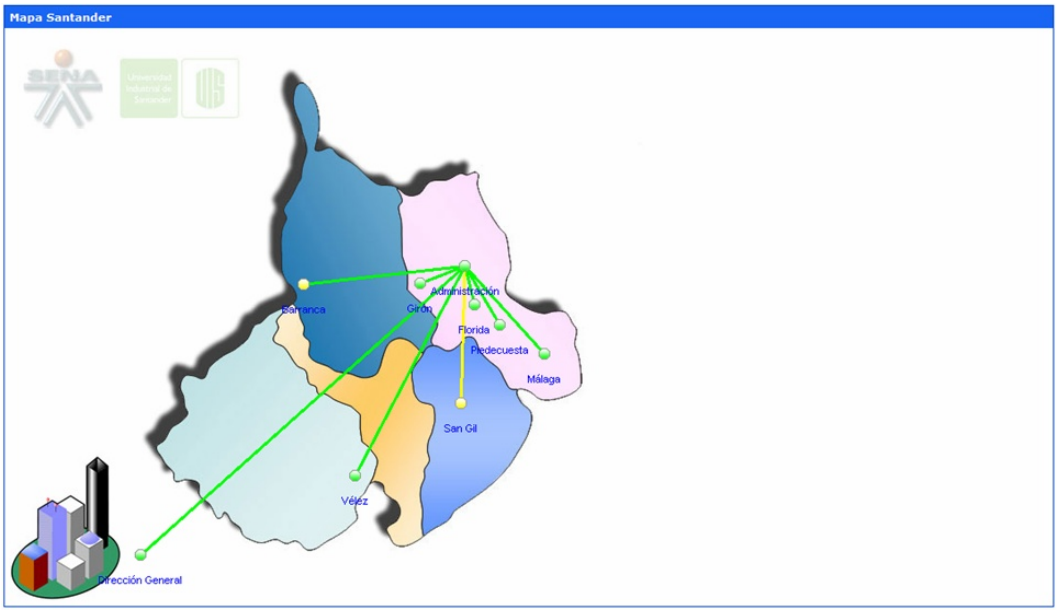


Figura 50: Vista Mapa Santander

13.1.2 Vista Red Regional

Esta vista presenta un esquema de toda la Red de Datos del SENA Regional Santander a manera de diagrama de red, con sus respectivos enlaces, routers y su estado.

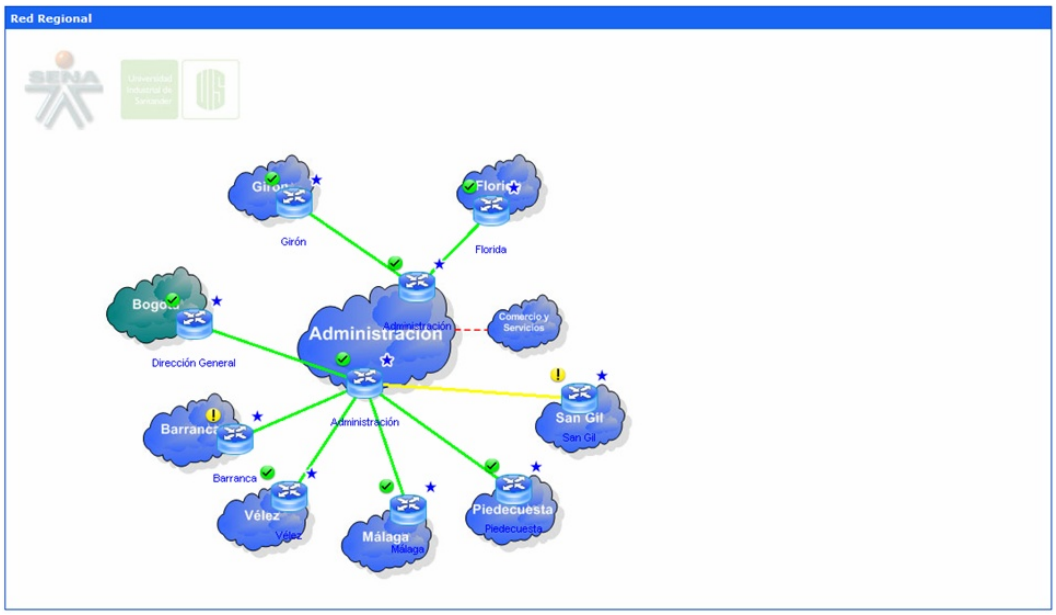


Figura 51: Vista Red Regional

13.1.3 Vista Administración

Esta vista, presenta un esquema de la red de datos de la Sede Administrativa del SENA Regional Santander, que incluye los dos routers principales y los swiches que se encuentran instalados en cada uno de los edificios.

Permite obtener información sobre los enlaces de los dispositivos y el estado de los mismos en cada una de las dependencias de la Sede Administrativa.

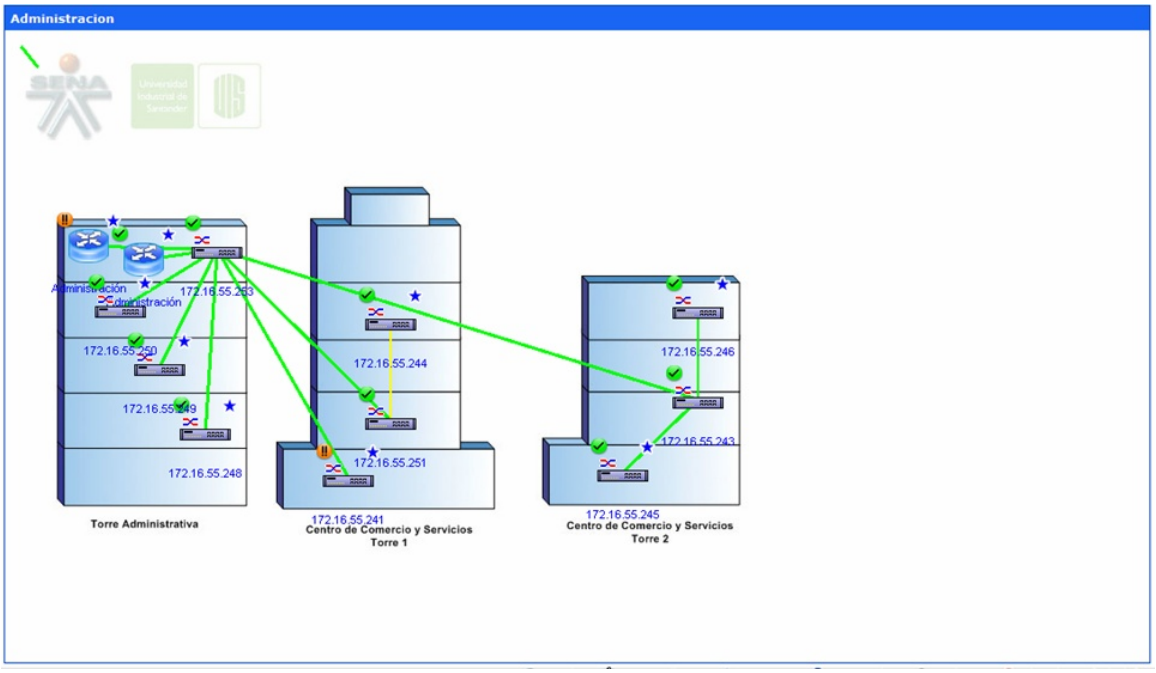


Figura 52: Vista Administración

13.2 Añadir una Vista de Negocios

1. Abrir el OpManager MapMaker haciendo click en:

   Inicio>Programas> ManageEngine OpManager > OpManager MapMaker

2. Hacer click en el botón "**Add Business View**"  Se abrirá la ventana de propiedades de la vista

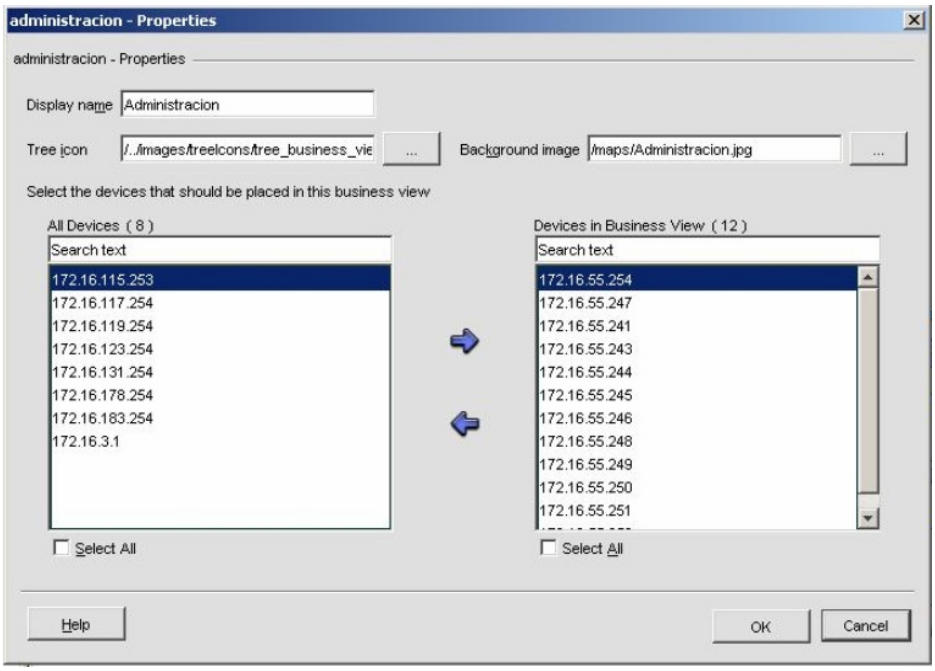


Figura 53: OpManager MapMaker

3. Introducir en el campo "**Display Name**" el nombre de la vista
4. Seleccionar el icono del la vista en el campo "**Tree Icon**"
5. Seleccionar una imagen de fondo en el campo "**Background image**"
6. Seleccionar los dispositivos que van a ser agrupados en la Vista de Negocios
7. Hacer click en "**Ok**" para guardar los cambios. Se abrirá la Vista de Negocios con los dispositivos añadidos
8. Arrastrar los dispositivos hasta la posición deseada
9. Hacer click en "**Save Business View**" para guardar la nueva vista de negocios

13.3 Modificar una Vista de Negocios

Una vez añadida la vista, es posible modificar su icono, su imagen de fondo y los dispositivos añadidos a la misma.

1. Una vez en el **Opmanager MapMaker**, seleccionar la vista que se quiere modificar
2. Hacer click en "**Modify Business View**" Se abrirá la ventana de propiedades de la vista de negocios
3. Realizar los cambios requeridos y hacer click en "**Ok**"
4. Hacer click en "**Save Business View**" para guardar la nueva vista de negocios

13.4 Añadir un enlace entre dispositivos

Para representar un diagrama de red en las Vistas de Negocio, OpManager permite dibujar enlaces entre los dispositivos, asignándole su respectivo nombre y configurándolo para que cambie de color según su estado.

Para agregar un enlace entre dos dispositivos, debemos seguir los siguientes pasos:

1. Seleccionar con un click los dos dispositivos que van a ser enlazados teniendo presionada la tecla CTRL
2. Hacer click en "**Add link between devices** 
3. Escribir el nombre del enlace en el campo "**Display Name**"
4. Usar el botón "**…**" del campo "**Get status from**" para seleccionar la interfaz de cualquiera de los dos dispositivos que va a determinar el estado del enlace.
5. Seleccionar el ancho de la líne del enlace en el campo "**Thickness**"
6. Hacer click en "**Ok**"

14. Reinstalación

En caso de que se requiera reinstalar el OpManager por un cambio de servidor o por cualquier otra razón, es importante realizar previamente un Backup de toda la información que éste contiene para que no se pierdan los dispositivos que ya se han añadido, ni las Vistas de Negocio configuradas.

14.1 Backup

Para realizar el backup de los datos y de la configuración del OpManager, hacer lo siguiente:

1. Ir al directorio principal de OpManager, normalmente en:
   C:\Archivos de programa\AdventNet\ME\OpManager\bin\backup
2. Ejecutar BackupDB.bat/sh para empezar a hacer el backup

Una vez el backup termine, se creará el directorio “backup” en el directorio raíz de OpManager (C:\Archivos de programa\AdventNet\ME\OpManager) y dentro de este directorio, el archivo de backup con extención .dat

El nombre del archivo de backup contiene la fecha y la hora a la cual se realizó el backup, por ejemplo: BackUp_APR16_2006_12_59.data

14.2 Restauración

Para restaurar los datos guardados en un archivo de backup, seguir los siguientes pasos:

1. Ir al directorio principal de OpManager, normalmente en:
   C:\Archivos de programa\AdventNet\ME\OpManager\bin\backup
2. Ejecutar RestoreDB.bat/sh con el nombre del archivo de backup que se quiera restaurar como argumento, por ejemplo:
   C:\Archivos de programa\AdventNet\ME\OpManager\bin\backup\RestoreDB.bat BackUp_APR16_2006_12_59.data

15. Reportes generados con OpManager en la Red de Datos del SENA REGIONAL SANTANDER

A continuación se presentan los reportes más importantes que se generaron con el OpManager 6.0 en la Red de Datos del SENA REGIONAL SANTANDER entre los 30 días comprendidos desde el 8 de abril y el 8 de mayo de 2006.

Se incluyen:

- Reporte de Inventario, en el que se muestran los 20 dispositivos añadidos y si son administrables o no por medio de agentes SNMP.
- Reporte de tráfico Tx y Rx de las interfaces de los routers
- Reporte de errores en las interfaces de los routers
- Reportes de disponibilidad de las interfaces de los routers
- Reportes de utilización de las interfaces de los routers
- Reportes de tráfico Tx y Rx por los puertos de los switches

ManageEngine OpManager

Reporte de Inventario - Todos los dispositivos

Name	IP Adress	OS	RAM(in MB)	Disk(in GB)
172.16.55.241	172.16.55.241	Alcatel Omnistack 6124/6148	0	0
172.16.55.243	172.16.55.243	Alcatel Omnistack 6124/6148	0	0
172.16.55.244	172.16.55.244	Alcatel Omnistack 6124/6148	0	0
172.16.55.245	172.16.55.245	Alcatel Omnistack 6124/6148	0	0
172.16.55.246	172.16.55.246	Alcatel Omnistack 6124/6148	0	0
172.16.55.248	172.16.55.248	Alcatel Omnistack 6124/6148	0	0
172.16.55.249	172.16.55.249	Alcatel Omnistack 6124/6148	0	0
172.16.55.250	172.16.55.250	Alcatel Omnistack 6124/6148	0	0
172.16.55.251	172.16.55.251	Alcatel Omnistack 6124/6148	0	0
172.16.55.253	172.16.55.253	Alcatel Omnistack 6124/6148	0	0
Administración Cisco	172.16.55.247	Cisco 3640	0	0
Administración Huawei	172.16.55.254	Router Huawei 3640	0	0
Barranca	172.16.115.253	Cisco 1700 Series	0	0
Dirección General	172.16.3.1	Router Huawei NE-08	0	0
Florida	172.16.119.254	Cisco 1700 Series	0	0
Girón	172.16.117.254	Cisco 1700 Series	0	0
Málaga	172.16.183.254	Cisco 1700 Series	0	0
Piedecuesta	172.16.178.254	Cisco 1700 Series	0	0
San Gil	172.16.123.254	Cisco 1700 Series	0	0
Vélez	172.16.131.254	Cisco 1700 Series	0	0

ManageEngine OpManager

Routers por tráfico Rx

Top 25 Routers por tráfico Rx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
Dirección General	Ethernet5/2/0	8.98 kbps	37.6 Mbps	5.97 Mbps
Administración Huawei	Serial0:0	491.0 bps	1.75 Mbps	303.04 kbps
San Gil	FastEthernet0	0.0 bps	38.17 Mbps	296.67 kbps
San Gil	Serial0	5.0 bps	38.18 Mbps	258.81 kbps
Dirección General	Serial4/0/3:0(cE1)	230.0 bps	1.22 Mbps	123.17 kbps
Administración Huawei	Ethernet0	214.0 bps	1.07 Mbps	105.44 kbps
Málaga	FastEthernet0	0.0 bps	35.95 Mbps	78.04 kbps
Málaga	Serial0	9.0 bps	32.39 Mbps	76.84 kbps
Barranca	FastEthernet0	13.0 bps	31.42 Mbps	64.29 kbps
Piedecuesta	FastEthernet0	0.0 bps	31.13 Mbps	59.73 kbps
Barranca	Serial0	18.0 bps	24.53 Mbps	59.27 kbps
Piedecuesta	Serial0	35.0 bps	18.62 Mbps	43.36 kbps
Vélez	Serial0	21.0 bps	187.43 kbps	11.35 kbps
Administración Cisco	Ethernet0/0	32.0 bps	101.06 kbps	11.24 kbps
Administración Huawei	Serial1:4	8.0 bps	70.37 kbps	5.86 kbps
Vélez	FastEthernet0	0.0 bps	375.17 kbps	5.05 kbps
Girón	BRI0:1	6.0 bps	60.69 kbps	4.92 kbps
Administración Huawei	Serial1:2	7.0 bps	30.77 kbps	3.37 kbps
Administración Huawei	Serial1:3	0.0 bps	52.06 kbps	3.18 kbps
Administración Huawei	Serial1:5	0.0 bps	56.68 kbps	2.76 kbps
Administración Huawei	Serial1:1	1.0 bps	38.19 kbps	2.76 kbps
Girón	FastEthernet0	0.0 bps	56.9 kbps	2.46 kbps
Florida	FastEthernet0	0.0 bps	14.47 kbps	1.46 kbps
Administración Cisco	BRI3/0:2	0.0 bps	54.65 kbps	1.17 kbps
Administración Cisco	BRI3/0:1	0.0 bps	16.33 kbps	1.16 kbps

ManageEngine OpManager

Routers por tráfico Tx

Top 25 Routers por tráfico Tx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
Dirección General	Ethernet5/2/0	3.18 kbps	21.28 Mbps	2.13 Mbps
Dirección General	Serial4/0/3:0(cE1)	552.0 bps	2.36 Mbps	317.84 kbps
San Gil	Serial0	3.0 bps	38.17 Mbps	302.27 kbps
Administración Huawei	Ethernet0	460.0 bps	1.63 Mbps	261.71 kbps
San Gil	FastEthernet0	5.0 bps	38.18 Mbps	257.88 kbps
Administración Huawei	Serial0:0	201.0 bps	1.08 Mbps	109.34 kbps
Málaga	Serial0	3.0 bps	36.18 Mbps	78.2 kbps
Málaga	FastEthernet0	9.0 bps	32.22 Mbps	76.74 kbps
Barranca	Serial0	8.0 bps	33.35 Mbps	66.35 kbps
Piedecuesta	Serial0	78.0 bps	32.09 Mbps	61.07 kbps
Barranca	FastEthernet0	19.0 bps	24.16 Mbps	59.54 kbps
Piedecuesta	FastEthernet0	47.0 bps	18.08 Mbps	42.52 kbps
Administración Huawei	Serial1:4	17.0 bps	125.29 kbps	14.59 kbps
Vélez	FastEthernet0	22.0 bps	126.84 kbps	11.3 kbps
Administración Huawei	Serial1:2	20.0 bps	125.25 kbps	11.13 kbps
Administración Huawei	Serial1:3	5.0 bps	125.53 kbps	9.77 kbps
Administración Huawei	Serial1:5	7.0 bps	103.24 kbps	8.92 kbps
Administración Huawei	Serial1:1	15.0 bps	125.32 kbps	8.75 kbps
Florida	FastEthernet0	25.0 bps	84.79 kbps	6.06 kbps
Administración Cisco	BRI3/0:1	0.0 bps	62.86 kbps	5.34 kbps
Girón	FastEthernet0	6.0 bps	61.63 kbps	5.04 kbps
Vélez	Serial0	8.0 bps	31.37 kbps	3.35 kbps
Administración Cisco	Ethernet0/0	1.0 bps	63.03 kbps	3.14 kbps
Administración Cisco	BRI3/0:2	0.0 bps	55.29 kbps	2.83 kbps
Administración Cisco	BRI3/1:1	0.0 bps	48.33 kbps	2.54 kbps

ManageEngine OpManager

Routers por errores Rx

Top 10 Routers por errores Rx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
Málaga	Serial0	0 packets	1193046 packets	12427 packets
Piedecuesta	Serial0	0 packets	1193045 packets	9468 packets
Barranca	Serial0	0 packets	1193377 packets	8647 packets
Vélez	FastEthernet0	0 packets	105 packets	0 packets
Barranca	FastEthernet0	0 packets	0 packets	0 packets
Barranca	Null0	0 packets	0 packets	0 packets
Girón	FastEthernet0	0 packets	0 packets	0 packets
Girón	BRI0	0 packets	0 packets	0 packets
Girón	BRI0:1	0 packets	0 packets	0 packets
Girón	BRI0:2	0 packets	0 packets	0 packets

ManageEngine OpManager

Routers por errores Tx

Top 10 Routers por errores Tx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
Barranca	FastEthernet0	0 packets	1193377 packets	8647 packets
Barranca	Serial0	0 packets	0 packets	0 packets
Barranca	Null0	0 packets	0 packets	0 packets
Girón	FastEthernet0	0 packets	0 packets	0 packets
Girón	BRI0	0 packets	0 packets	0 packets
Girón	BRI0:1	0 packets	0 packets	0 packets
Girón	BRI0:2	0 packets	0 packets	0 packets
Girón	Null0	0 packets	0 packets	0 packets
Girón	BRI0-Signaling	0 packets	0 packets	0 packets
Florida	FastEthernet0	0 packets	0 packets	0 packets

ManageEngine OpManager

Reporte de disponibilidad - Todas las Interfaces - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Router Name	Interface Name	Description	Total Down Time	MTTR	MTBF	UpTime Percentage
Barranca	connected to EthernetLAN	FastEthernet0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Barranca	IF-172.16.115.253-3	Null0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Barranca	IF-192.168.220.6	Serial0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Girón	IF-172.16.117.254-1	BRI0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Girón	IF-172.16.117.254-7	BRI0-Physical	4 Mins 55 Secs	4 Mins 55 Secs	359 Hrs 57 Mins	99.99%
Girón	IF-172.16.117.254-8	BRI0-Signaling	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Girón	IF-172.16.117.254-2	BRI0:1	4 Mins 55 Secs	4 Mins 55 Secs	359 Hrs 57 Mins	99.99%
Girón	IF-172.16.117.254-9	BRI0:1-Bearer Channel	4 Mins 55 Secs	4 Mins 55 Secs	359 Hrs 57 Mins	99.99%
Girón	IF-172.16.117.254-3	BRI0:2	46 Hrs 29 Mins	46 Hrs 29 Mins	336 Hrs 45 Mins	93.54%
Girón	IF-172.16.117.254-10	BRI0:2-Bearer Channel	51 Hrs 35 Mins	51 Hrs 35 Mins	334 Hrs 12 Mins	92.83%
Girón	connected to EthernetLAN_3	FastEthernet0	4 Mins 55 Secs	4 Mins 55 Secs	359 Hrs 57 Mins	99.99%
Girón	IF-172.16.117.254-5	Null0	4 Mins 55 Secs	4 Mins 55 Secs	359 Hrs 57 Mins	99.99%
Florida	IF-172.16.119.254	FastEthernet0	4 Mins 57 Secs	4 Mins 57 Secs	359 Hrs 57 Mins	99.99%
San Gil	connected to EthernetLAN_2	FastEthernet0	10 Hrs 51 Mins	10 Hrs 51 Mins	354 Hrs 34 Mins	98.49%
San Gil	IF-172.16.123.254-3	Null0	10 Hrs 51 Mins	10 Hrs 51 Mins	354 Hrs 34 Mins	98.49%

ManageEngine OpManager

Router Name	Interface Name	Description	Total Down Time	MTTR	MTBF	UpTime Percentage
San Gil	connected to Cisco3640	Serial0	10 Hrs 51 Mins	10 Hrs 51 Mins	354 Hrs 34 Mins	98.49%
San Gil	IF-172.16.123.254-5	Virtual-Access1	10 Hrs 51 Mins	10 Hrs 51 Mins	354 Hrs 34 Mins	98.49%
Vélez	IF-172.16.131.254	FastEthernet0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Vélez	IF-172.16.131.254-3	Null0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Vélez	IF-192.168.220.22	Serial0	4 Mins 52 Secs	4 Mins 52 Secs	359 Hrs 57 Mins	99.99%
Piedecuesta	IF-172.16.178.254	FastEthernet0	4 Mins 50 Secs	4 Mins 50 Secs	359 Hrs 57 Mins	99.99%
Piedecuesta	IF-172.16.178.254-3	Null0	4 Mins 50 Secs	4 Mins 50 Secs	359 Hrs 57 Mins	99.99%
Piedecuesta	IF-192.168.220.30	Serial0	4 Mins 50 Secs	4 Mins 50 Secs	359 Hrs 57 Mins	99.99%
Málaga	IF-172.16.183.254	FastEthernet0	4 Mins 51 Secs	4 Mins 51 Secs	359 Hrs 57 Mins	99.99%
Málaga	IF-172.16.183.254-3	Null0	4 Mins 51 Secs	4 Mins 51 Secs	359 Hrs 57 Mins	99.99%
Málaga	IF-192.168.220.26	Serial0	4 Mins 51 Secs	4 Mins 51 Secs	359 Hrs 57 Mins	99.99%
Dirección General	IF-172.16.3.1-201326854	E1 3/0/0	5 Mins 0 Secs	5 Mins 0 Secs	359 Hrs 57 Mins	99.99%
Dirección General	IF-172.16.3.1-201327238	E1 3/0/1	5 Mins 0 Secs	5 Mins 0 Secs	359 Hrs 57 Mins	99.99%
Dirección General	IF-172.16.3.1	Ethernet5/2/0	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Dirección General	IF-192.168.220.1	Serial4/0/3:0(cE1)	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-10	BRI3/0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-37	BRI3/0-Physical	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%

ManageEngine OpManager

Router Name	Interface Name	Description	Total Down Time	MTTR	MTBF	UpTime Percentage
Administración Cisco	IF-172.16.55.247-38	BRI3/0-Signaling	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-11	BRI3/0:1	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-39	BRI3/0:1-Bearer Channel	4 Mins 59 Secs	4 Mins 59 Secs	359 Hrs 57 Mins	99.99%
Administración Cisco	IF-172.16.55.247-12	BRI3/0:2	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-40	BRI3/0:2-Bearer Channel	4 Mins 58 Secs	4 Mins 58 Secs	359 Hrs 57 Mins	99.99%
Administración Cisco	IF-172.16.55.247-13	BRI3/1	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-41	BRI3/1-Physical	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-42	BRI3/1-Signaling	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-14	BRI3/1:1	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-43	BRI3/1:1-Bearer Channel	24 Hrs 50 Mins	24 Hrs 50 Mins	347 Hrs 34 Mins	96.55%
Administración Cisco	IF-172.16.55.247-15	BRI3/1:2	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-44	BRI3/1:2-Bearer Channel	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	connected to EthernetLAN	Ethernet0/0	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-31	Foreign Exchange Office 2/0/0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-32	Foreign Exchange Office 2/0/1	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-33	Foreign Exchange Office 2/1/0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Cisco	IF-172.16.55.247-34	Foreign Exchange Office 2/1/1	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%

Router Name	Interface Name	Description	Total Down Time	MTTR	MTBF	UpTime Percentage
Administración Cisco	IF-172.16.55.247-22	Null0	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Cisco	IF-172.16.55.247-2	Serial1/0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	IF-172.16.55.254-1	Aux0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	IF-172.16.55.254-2	Bri0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	IF-172.16.55.254-3	Bri1	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	IF-172.16.55.254-4	Bri2	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	IF-172.16.55.254-5	Bri3	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	Ethernet interface	Ethernet0	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	E1-DIRECCION-NACIONAL	Serial0:0	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	IF-172.16.55.254-9	Serial1:0	720 Hrs 0 Mins	720 Hrs 0 Mins	0 Mins 0 Secs	0.0%
Administración Huawei	PIEDECUESTA	Serial1:1	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	VELEZ	Serial1:2	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	SAN GIL	Serial1:3	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	BARRANCABERMEJA	Serial1:4	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%
Administración Huawei	MALAGA	Serial1:5	0 Mins	0 Mins	720 Hrs 0 Mins	100.0%

ManageEngine OpManager

Routers por utilización Rx

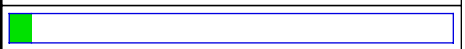
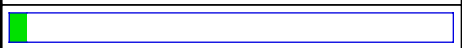
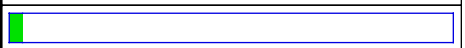
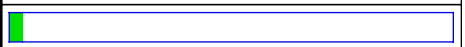
Top 10 Routers por utilización Rx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/ Port	Min	Max	Avg	
Administración Huawei	Serial0:0	0 %	88 %	14 %	
Girón	BRI0:1	0 %	94 %	6 %	
Dirección General	Ethernet5/2/0	0 %	36 %	5 %	
Dirección General	Serial4/0/3:0(cE1)	0 %	56 %	4 %	
Administración Huawei	Serial1:4	0 %	54 %	3 %	
Administración Huawei	Serial1:2	0 %	24 %	2 %	
Administración Huawei	Serial1:5	0 %	44 %	1 %	
Administración Huawei	Serial1:3	0 %	40 %	1 %	
Administración Cisco	BRI3/0:1	0 %	25 %	1 %	
Administración Cisco	BRI3/0:2	0 %	85 %	1 %	

ManageEngine OpManager

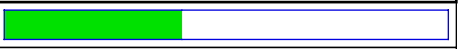
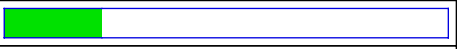
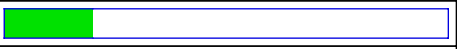
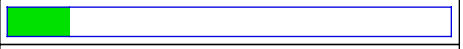
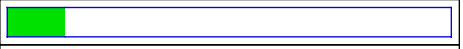
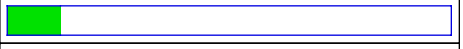
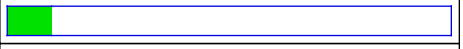
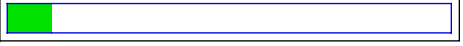
Routers por utilización Tx

Top 10 Routers por utilización Tx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/ Port	Min	Max	Avg	
Dirección General	Serial4/0/3:0(cE1)	0 %	100 %	15 %	
Administración Huawei	Serial1:4	0 %	97 %	10 %	
Administración Huawei	Serial1:2	0 %	97 %	7 %	
Administración Cisco	BRI3/0:1	0 %	98 %	7 %	
Administración Huawei	Serial1:3	0 %	98 %	6 %	
Administración Huawei	Serial1:5	0 %	80 %	6 %	
Administración Huawei	Serial1:1	0 %	97 %	5 %	
Administración Huawei	Serial0:0	0 %	54 %	4 %	
Administración Cisco	BRI3/0:2	0 %	86 %	3 %	
Administración Cisco	BRI3/1:1	0 %	75 %	3 %	

Routers por utilización de Memoria

Top 10 Routers por utilización de Memoria - Today (Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Min	Max	Avg	
Barranca	40	41	40	
Administración Cisco	22	22	22	
San Gil	20	21	20	
Girón	14	14	14	
Florida	13	13	13	
Vélez	12	12	12	
Piedecuesta	10	10	10	
Málaga	10	10	10	

ManageEngine OpManager

Puertos de Switch por tráfico Rx

Top 25 Puertos de Switch por tráfico Rx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
172.16.55.245	Port - 36	0.0 bps	5.74 Mbps	221.41 kbps
172.16.55.248	Port - 15	132.0 bps	610.47 kbps	150.89 kbps
172.16.55.248	Port - 11	62.0 bps	372.36 kbps	135.22 kbps
172.16.55.249	Port - 13	0.0 bps	14.15 Mbps	131.94 kbps
172.16.55.248	Port - 49	25.0 bps	17.92 Mbps	110.94 kbps
172.16.55.249	Port - 49	44.0 bps	7.95 Mbps	110.18 kbps
172.16.55.245	Port - 49	62.0 bps	2.0 Mbps	97.26 kbps
172.16.55.248	Port - 28	0.0 bps	17.5 Mbps	67.5 kbps
172.16.55.241	Port - 49	75.0 bps	399.1 kbps	40.75 kbps
172.16.55.245	Port - 15	0.0 bps	4.3 Mbps	39.83 kbps
172.16.55.248	Port - 5	0.0 bps	244.96 kbps	25.29 kbps
172.16.55.246	Port - 49	15.0 bps	400.1 kbps	24.49 kbps
172.16.55.250	Port - 49	11.0 bps	681.8 kbps	18.12 kbps
172.16.55.248	Port - 18	0.0 bps	4.17 Mbps	12.36 kbps
172.16.55.244	Port - 25	13.0 bps	96.26 kbps	11.14 kbps
172.16.55.245	Port - 24	0.0 bps	173.62 kbps	9.13 kbps
172.16.55.250	Port - 10	0.0 bps	1.97 Mbps	7.69 kbps
172.16.55.249	Port - 23	0.0 bps	410.74 kbps	4.37 kbps
172.16.55.248	Port - 1	0.0 bps	1.32 Mbps	4.33 kbps
172.16.55.246	Port - 2	0.0 bps	64.41 kbps	2.96 kbps
172.16.55.245	Port - 28	0.0 bps	784.89 kbps	2.55 kbps
172.16.55.241	Port - 6	0.0 bps	53.68 kbps	2.37 kbps
172.16.55.249	Port - 47	0.0 bps	365.01 kbps	2.25 kbps
172.16.55.249	Port - 35	0.0 bps	90.63 kbps	2.12 kbps
172.16.55.248	Port - 24	0.0 bps	656.84 kbps	1.63 kbps

ManageEngine OpManager

Puertos de Switch por tráfico Tx

Top 25 Puertos de Switch por tráfico Tx - Last 30 Days (Sat, 8 Apr 2006 to Mon, 8 May 2006) - Ventana de Tiempo - Full 24 hours

Device Name	Interface/Port	Min	Max	Avg
172.16.55.248	Port - 15	66.0 bps	455.23 kbps	162.87 kbps
172.16.55.249	Port - 23	4.0 bps	14.15 Mbps	116.51 kbps
172.16.55.248	Port - 11	105.0 bps	611.14 kbps	111.59 kbps
172.16.55.248	Port - 49	4.0 bps	17.58 Mbps	86.49 kbps
172.16.55.245	Port - 24	45.0 bps	4.72 Mbps	86.21 kbps
172.16.55.248	Port - 18	0.0 bps	17.77 Mbps	68.2 kbps
172.16.55.249	Port - 35	0.0 bps	3.53 Mbps	46.86 kbps
172.16.55.248	Port - 5	17.0 bps	413.74 kbps	36.54 kbps
172.16.55.245	Port - 16	0.0 bps	665.95 kbps	23.99 kbps
172.16.55.245	Port - 9	0.0 bps	806.19 kbps	21.25 kbps
172.16.55.245	Port - 8	0.0 bps	658.4 kbps	20.99 kbps
172.16.55.245	Port - 38	0.0 bps	796.09 kbps	20.75 kbps
172.16.55.245	Port - 12	0.0 bps	1.03 Mbps	19.88 kbps
172.16.55.245	Port - 49	13.0 bps	344.2 kbps	19.76 kbps
172.16.55.245	Port - 44	0.0 bps	741.51 kbps	19.24 kbps
172.16.55.245	Port - 32	0.0 bps	693.81 kbps	18.75 kbps
172.16.55.245	Port - 39	0.0 bps	901.71 kbps	18.49 kbps
172.16.55.245	Port - 7	0.0 bps	982.59 kbps	16.11 kbps
172.16.55.249	Port - 39	0.0 bps	4.95 Mbps	14.48 kbps
172.16.55.245	Port - 42	1.0 bps	3.6 Mbps	14.43 kbps
172.16.55.245	Port - 31	0.0 bps	2.49 Mbps	14.28 kbps
172.16.55.249	Port - 34	0.0 bps	4.18 Mbps	14.21 kbps
172.16.55.249	Port - 49	10.0 bps	417.26 kbps	13.58 kbps
172.16.55.248	Port - 32	1.0 bps	744.09 kbps	13.07 kbps
172.16.55.241	Port - 49	30.0 bps	154.18 kbps	12.94 kbps