FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

ESTUDIO E IMPLEMENTACIÓN DE UN SISTEMA DE VIGILANCIA Y MONITOREO IP SOBRE UNA INTRANET

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Tecnólogo en Redes y Telecomunicaciones

Profesor guía:

Ing. David González

Autor:

Santiago García Jaramillo

Año
2011

Anteproyecto:

I.- Parte Teórica

1. Enunciado del Proyecto:

ESTUDIO E IMPLEMENTACION DE UN SISTEMA DE VIGILANCIA Y MONITOREO IP SOBRE UNA INTRANET.

2. Justificación:

En la actualidad empresas e instituciones requieren contar con sistemas de vigilancia y monitoreo (los mismos que comúnmente son analógicos), sean estos orientados a control o seguridad en sus dependencias, pero uno de estos sistemas requieren de un cableado adicional, su calidad de imagen no es buena, no se puede transmitir el vídeo en vivo y para hacerlo se necesita de una gran inversión, entre otras limitaciones generadas por el tipo de tecnología.

Por otro lado actualmente la mayoría de empresas e instituciones cuentan con redes IP (Tecnología digital) en sus infraestructuras y tomando en cuenta la convergencia (capacidad de las redes IP de comunicar servicios multimedia como voz y video), podemos implementar sistemas de vigilancia y monitoreo IP obteniendo: mayor calidad de imagen en la transmisión y recepción de vídeo, facilidad en el almacenamiento de voz y vídeo, nos permite la transmisión del audio y vídeo en vivo desde varias localidades a través del Internet o de una Intranet (red privada que utiliza tecnología IP para compartir de forma segura cualquier información o programa).

Nos permite abaratar los costos de infraestructura, ya que utiliza la red previamente implementada, además nos brinda gestión, control y acceso remoto a la mayoría de elementos en la red IP, así como del sistema de vigilancia y monitoreo entre otros beneficios.

En base a estas consideraciones se implementará un Sistema de Vigilancia y Monitoreo IP, ofreciendo así una solución inteligente de tener bajo un mismo sistema de monitoreo todas las dependencias (seis en Pichincha y tres en Guayas) pertenecientes a un concesionario de automóviles.

Formulación del problema e hipótesis:

Implementar un Sistema de Vigilancia y Monitoreo IP, de manera que desde una central de monitoreo, se pueda gestionar y visualizar lo que sucede en las diferentes dependencias.

3. Preguntas y Objetivos del Proyecto:

4.1. Preguntas:

¿Dónde se implementará?

El proyecto será implementado en la Intranet de un concesionario de autos, que se compone de cinco dependencias conectadas a una oficina matriz en Quito y otras dos sucursales conectadas a otra oficina matriz en Guayaquil, cabe acotar que las oficinas matrices cuentan con un enlace de fibra óptica que las conecta entre si a altas velocidades.

¿Qué se necesita?

Anchos de banda en los se pueda transmitir el audio y video de las cámaras, cableado eléctrico para energizar las cámaras, cableado de red para conectar las cámaras a la red de datos, cámaras IP, NVR´s (Network Video Recorder: Grabador de vídeo en red), un equipo (PC) para la central de monitoreo, switches y elementos de la red IP en la que trabajaremos.

¿En cuanto tiempo se llevará a cabo?

El proyecto será planificado para implementarse en aproximadamente ocho semanas.

¿Cómo trabajará el sistema de vigilancia y monitoreo IP sobre la red?

E sistema de vigilancia y monitoreo IP trabajará con una o mas cámaras, dependiendo de cada sucursal o matriz, transmitirá vídeo en vivo desde las dependencias y matriz de Guayaquil a un centro de monitoreo en la matriz de Quito, contará con un NVR de pequeña capacidad de almacenaje que grabara los sucesos en cada dependencia y uno de gran capacidad en la central de monitoreo el cual gestionará los archivos deseados desde las dependencias según el administrador lo requiera.

4.2. Objetivo general:

"Implementar un Sistema de Vigilancia y Monitoreo IP sobre la Intranet de un Concesionario de Automóviles"

4.3. Objetivos específicos:

a. *Analizar y especificar los protocolos a utilizarse para la transmisión de voz y video sobre la red de datos.*

b. *Analizar las características de la Intranet del concesionario, paralelamente determinar los requerimientos para la transmisión y recepción de voz y video.*

c. *Diseñar un Sistema de Vigilancia y Monitoreo IP, y definir equipos a utilizarse.*

d. *Implementar y probar el Sistema de Vigilancia y Monitoreo IP.*

II.- Metodología

1. Metodología para el desarrollo del Plan de Trabajo de Titulación.

1.1. Características generales:

El análisis e implementación del proyecto se llevará a cabo en un concesionario de automóviles, se contará con la colaboración del personal encargado del área técnica para la especificación, análisis y reconocimiento de la estructura de la Intranet.

1.2. Metodología a utilizar:

En el desarrollo del proyecto se usará el método descriptivo mediante el cual se realizará un análisis detallado del como y que necesitamos para su implementación desde los análisis previos hasta las pruebas del mismo.

1.3. Ámbito del Proyecto:

Se estima conseguir con el proyecto el centralizar un Sistema de Vigilancia y Monitoreo IP, para que sea la "Central de Monitoreo" la que reciba las transmisiones de todas las sucursales; que será gestionada por una sola persona, la cual controlara todas las cámaras, tendrá acceso a todos los NVR´s y podrá gestionar toda la información que se genere en el sistema de vigilancia y monitoreo, además podrá transmitir

el vídeo a una empresa de seguridad pagada, según el administrador lo requiera

1.4. Métodos y técnicas a utilizar:

a. *Se recopilará la información por medio del personal del área técnica, la misma que se complementará con visitas, en las que se realizarán análisis de la Intranet y conjuntamente se ejecutarán reconocimientos de las dependencias para el diseño del sistema.*

b. *Se determinará los requerimientos de la Red IP Metropolitana, para la implementación de protocolos de transmisión, recepción de voz y vídeo ip, mediante la investigación de estándares internacionales para aplicaciones multimedia sobre IP, de igual forma en base a estándares de funcionamiento y características de los equipos a implementar (servido, switches, cámaras IP y NVR´s).*

c. *Se detallará que elementos compondrán el Sistema de Vigilancia y Monitoreo IP, además se diseñara la distribución de los mismos en base a: información recopilada de esquemas, estudios, visitas realizadas, y al respectivo análisis de costo – beneficio.*

d. *Se implementará, en base al diseño; realizando trabajos adicionales como: cableado para energizar las cámaras IP, cableado de red para conectarlas a la Red Ip Metropolitana y otros trabajos según se requieran al momento de la implementación.*

2. Temario Inicial del Trabajo

Introducción

Capitulo I

IMPLEMENTACION DE UN SISTEMA DE VIGILANCIA Y MONITOREO IP

1.1.- Contextualización.

1.2.- Formulación del Problema.

1.3.- Delimitación.

1.4.- Interrogantes.

1.5.- Objetivos.

1.6.- Justificación.

Capítulo II

2.1.- Mapa de Inclusión.

2.2.- Constelación de Ideas.

2.3.- Metodología del Proyecto.

2.3.- Recursos del Sistema de Vigilancia y Monitoreo IP.

2.4.- Presupuesto.

2.4.- Cronograma de Actividades.

Capítulo III

3.1.- Redes Convergentes.

3.2.- Análisis de la Intranet del Concesionario.

3.2.1.- Características de la Intranet del Concesionario.

3.3.- Análisis de Protocolos (VoIP, Vídeo IP).

3.3.1.- Características y Requerimientos.

3.4.- Estudio de Factibilidad para la Implementación.

Capitulo IV

4.1.- Diseño del Sistema de Vigilancia y Monitoreo IP.

4.2.- Selección de Equipos.

4.2.1.- Características.

4.2.2.- Parámetros Generales de Configuración.

Capitulo V

Ingeniería del Proyecto

5.1.- Instalación y Configuración de Equipos.

5.2.- Pruebas del Sistema de Vigilancia y Monitoreo IP.

5.3.- Ventajas y Desventajas de la Solución.

Capitulo VI

6.1.- Conclusiones.

6.2.- Recomendaciones.

Bibliografía

Anexos.

3. Recursos del Proyecto.

3.1. Recursos Humanos:

Nombres	**Personal**
David González	Coordinador del Proyecto
Michael Salinas	Coordinador del Proyecto por parte del concesionario.
Santiago García	Técnico 1
Franklin Quiroz	Técnico 2
Nelson Tutillo	Técnico 3

3.2. Recursos Materiales:

Tipo de Material	**Modelo**	**Cantidad**
Cámara IP tipo domo a color	FD7131	17
Cámara IP tipo tubo exterior	IP7330	5
Disco Duro (HDD) SATA 1TB	WD10EACS	8
NVR 4 canales, 1 HDD	QN-NVR-104V	6
NVR 20 canales, 5 HDD	QN-VS-5020	1

3.3. Recursos Financieros:

Concepto de gasto	**Presupuesto**

Transporte	85 USD
Viáticos	95 USD
Imprevistos	50 USD

4. Bibliografía Básica:

- 3cx Voip (25 Febrero 2010) Disponible en: www.3cx.es.
- Anibal R, Figueiras. Madrid 2002. Una Panorámica de las telecomunicaciones Convergencia IP pág. 93,94.
- Ateinco Redes Diseño de Red Convergencia de Redes ip.

  (24 Febrero 2010). Disponible en: www.ateinco.com.
- GUSTAVO CABRERA - DIRECTOR ICONO Capital Consulting and Traiding Nuevos Sistemas de Vigilancia Camaras IP (25 Febrero 2010).

  Disponible en: www.cap-consulting.com.
- IP.TV inicio Que es (26 Febrero 2010).

  Disponible en: www.ip.tv/iptv_site/esp/htm/plataforma.html.
- Iain E.G. Richardson Inglaterra 2003. H.264 and MPEG-4. pág. 5, 6,7.
- Mitecnologico Main RedesConvergentes (24 Febrero 2010).

  Disponible en: www.mitecnologico.com.
- Rob Koenen Overview of the MPEG-4 Standard March 2002.

  Disponible en: mpeg.chiariglione.org/standards/mpeg-4/mpeg-4.htm.
- Tecnologia Media Solutions Video Digital (25 Febrero 2010).

  Disponible en: media-solutions.buscamix.com.
- Voip-voice-over-ip VoIp Standards y Protocols (25 Febrero 2010).

  Disponible en: www.voip-voice-over-ip.com.

5. Cronograma de Actividades:

Actividades	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8
Análisis de la red								
Análisis de protocolos y requerimientos								
Diseño del sistema								
Selección de equipos, análisis de costos								
Implementación del proyecto								
Pruebas y evaluación del proyecto								
Capítulo 1								
Capítulo 2								
Capítulo 3								
Capítulo 4								
Capítulo 5								
Entrega de Informe								

_____
_____

Alumno: Santiago García Tutor: David González

INTRODUCCIÓN

El hablar de convergencia no es nuevo, ya en diciembre de 1997 la Comisión Europea publicaba el “Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus consecuencia para la reglamentación”.

El documento, a modo de resumen, dice que la convergencia existe a nivel tecnológico, es decir, que gracias a la tecnología digital los servicios de comunicación pueden ser dados por una misma red en vez de redes diferenciadas para voz, datos y video. Las operadoras afectadas por la convergencia están intentando aprovechar las oportunidades que les ofrece el progreso tecnológico para mejorar sus servicios tradicionales e irrumpir en actividades nuevas. Como ejemplo más representativo de nuevos servicios son todos los que se dan por Internet.

Como bien dice el documento citado, la convergencia no es un concepto aplicable solamente a la tecnología sino que significa también nuevos servicios y nuevas formas de actividad empresarial. Uno de los factores más importantes es el uso creciente de las mismas tecnologías en distintos sectores, en particular en los de telecomunicaciones, medios de comunicación y tecnología de la información.

Como se citó anteriormente, es Internet la que ha propagado y puesto en marcha nuevos servicios que han calado muy bien en la gente joven y que después son solicitados en el mundo laboral.

Este documento pretende informar de los nuevos servicios de comunicación personales, la tendencia por parte de los dos mundos convergentes, informática y comunicaciones, y lo que se considera puede ser la solución ofertada por las operadoras tradicionales de comunicaciones.

Por último, y como parte más importante de este documento, se manifiesta la problemática que se puede vivir por el hecho de la separación del mundo de la voz y los datos.

EVOLUCIÓN HISTÓRICA DE LAS COMUNICACIONES PERSONALES/ EMPRESARIALES

Situándonos a finales del siglo IXX podemos ver que el primer servicio de comunicaciones personales/empresariales de forma electrónica fue el telégrafo y la red que lo sustenta que es la red telex. A finales del mismo siglo y principios del XX es el servicio telefónico y la red telefónica. Ambas redes tiene cobertura mundial y han sido las redes básicas de comunicaciones personales/empresariales electrónicas durante los 80 primeros años del siglo XX.

A principio de los 80 surge el correo electrónico, al principio muy asociado al mundo académico y después popularizado por ser uno de los servicios más utilizados en el mundo Internet.

Pero las comunicaciones personales no acaban con el correo electrónico, los nuevos servicios de mensajería electrónica, telefonía IP y videoconferencia son muy comunes en Internet con aplicaciones/servicios como Messenger de Microsoft y Skype. Como se puede ver la gran diferencia entre las redes de los años 80 a la actual es que para las comunicaciones actuales se utiliza únicamente una sola red, Internet.

NUEVOS SERVICIOS DE COMUNICACINES PERSONALES-EMPRESARIALES

Como se citó anteriormente y surgiendo desde el mundo Internet han aparecido los servicios de tiempo real:

- Servicio de directorio.
- Presencia.
- Mensajería instantánea.
- Telefonía IP (ToIP).
- Videoconferencia.
- Compartición de documentos/colaboración.

y otros servicios consolidados casi tiempo real:

- E-mail.
- SMS

SERVICIO DE PRESENCIA – MENSAJERÍA INSTÁNTANEA (IM)

Según muchos expertos, la presencia tiene todo el potencial para convertirse en la "killer application" que revolucionará el modo en que las empresas se comunican y colaboran entre sí. Los usuarios de mensajería instantánea (IM) ya sacan buen partido de ella, como se comentó anteriormente, pero estas tecnologías poco a poco van dejando de estar asociadas exclusivamente a entornos lúdicos juveniles y convirtiéndose en un servicio de red utilizado también por las aplicaciones y comunicaciones de empresa, incluida la telefonía. Como afirma la consultora Nemertes Research, en el futuro, la presencia será la capacidad de red subyacente, e IM será solo una de las muchas aplicaciones que se beneficien de sus beneficios.

En pocas palabras, la detección de presencias en la red o, más abreviadamente, de presencia, se puede definir como la tecnología de mensajería que permite a los usuarios y dispositivos encontrarse y, en consecuencia, contactarse rápidamente, con independencia de la localización física. Para ello, un servidor o servidores centrales hacen el seguimiento de los usuarios en función de cuando entran y salen de la red. Este es un punto muy importante la red nos tiene que ver siempre como una persona, hablamos de comunicaciones personales independientes de ubicación y eso exige sistemas centralizados capaces de identificar a la persona y al dispositivo con el que se ha identificado en la red. El valor del audio, el vídeo y la conferencia Web aumenta cuando estos servicios se enriquecen con capacidades de presencia y se integran con el sistema IM de la empresa.

TELEFONÍA IP (ToIP)

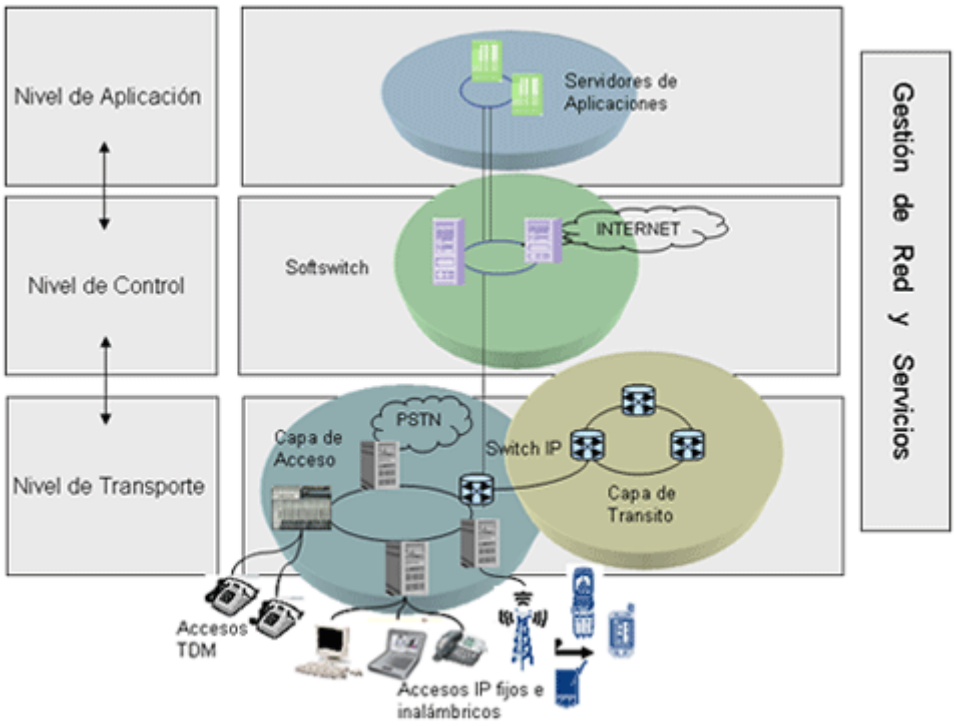
Sin duda, si se pregunta ahora cual son las tres "killers applications" (aplicaciones principales/matadoras) nos pueden contestar, la voz, la voz, la voz. La red telefónica básica por su fiabilidad, la red de móviles por su independencia de la ubicación física y

la propia voz como medio de comunicación han hecho que esta sea la aplicación/servicio más valorado por los usuarios para las comunicaciones personales.

Hasta el principio del siglo XXI la red telefónica básica de todas las operadoras y de las empresas era totalmente independiente de la llamada red de datos. Doble cableado, de voz y de datos, dos redes WAN (Wide Area Network) independientes, pero la tendencia actual de considerar la voz como una aplicación más de datos y la realidad del mercado, hace que no sea sostenible durante mucho tiempo dos redes independientes. Esto que es cierto y que sin duda acontecerá, por ejemplo BT, considera que para el 2010 tendrá la mayoría de sus usuarios/clientes migrados a la nueva red convergente NGN (Next Generation Network- red de Nueva Generación), llamada 21st Century Network (21CN), lo que permitirá la convergencia de servicios, aplicaciones y dispositivos.

NGN (NEXT GENERATION NETWORK) RED DE NUEVA GENERACIÓN

Aunque no es objeto de este documento extenderse en lo que puede ser la NGN si se quiere dejar constancia de su estructura ya que permite tener una visión de la arquitectura que emplearán las operadoras públicas para dar los servicios mencionados.



Del gráfico se puede observar un nivel de acceso que abarca todas las modalidades que se pueden considerar, desde las tradicionales TDM (Time Division Multiplexing), accesos IP fijos o inalámbricos WIFI (WIreless FIdelity) hasta tecnologías radio UMTS (Universal Mobile Telecommunications System). Lo que si acontecerá es que los accesos analógicos, TDM y las centrales de conmutación PSTN (Public Switched Telephone Network) migrarán a tecnología Ethernet o xDSL en el bucle y Ethernet y MPLS (Multiprotocol Label Switching) en el transporte y servidores de llamadas como centrales de conmutación.

Es muy importante subrayar la importancia del nivel de control y dentro de este nivel se encuentra el IMS (IP Multimedia Subsystem) que es la base de la pretendida flexibilidad para dar nuevos servicios y la convergencia fijo-móvil.

La estructura del IMS es:

PLATAFORMAS ACTUALES PARA ESTOS NUEVOS SERVICIOS

Como se citó anteriormente, muchos de estos nuevos servicios son ofrecidos por empresas focalizadas en el mundo Internet y usando de transporte la red Internet. Incluso este tipo de servicios son utilizados en las empresas pero lo que si es cierto que el mundo Internet no es el más seguro y hay otras opciones que trasladan los

servicio citados a la propia organización. Es aquí en este mundo de la convergencia de las comunicaciones y de las TI (Tecnologías de la Información) donde se presenta la batalla. Por un lado los dominadores de las TI , Microsoft, IBM, Oracle e incluso SAP por otro lado los fabricantes tradicionales de equipos de comunicaciones, Nortel, Siemens, Avaya, Alcatel y el dominador del mundo de los datos, que es Cisco. Cada uno con sus fortalezas, el tiempo real, voz y video para los tradicionales de comunicaciones y el resto para los TI.

A la hora de elegir la plataforma esto es un dilema y por eso las propias alianzas entre los dos mundos Microsoft/Nortel, IBM/¿Avaya, Cisco? Pero ¿es la mejor solución adquirir, mantener y gestionar plataformas propietarias?, veamos otras alternativas

PLATAFORMAS DE COMUNICACIONES PERSONALES-EMPRESARIALES SUMINISTRADAS COMO SERVICIO POR OPERADORAS DE COMUNICACIONES

Después de haber visto la plataforma de la red NGN se ve como esta cuadra perfectamente en el concepto de los nuevos servicios de comunicaciones personales y además ofrece lo que una plataforma propietaria lo tiene más difícil, la integración fijo móvil. Se estaría hablando de una plataforma individual o compartida que reside en la operadora y que es capaz de ofrecer servicios de directorio, presencia, mensajería instantánea, voz, video, colaboración, etc, es decir, se está trasladando los servicios/aplicaciones que se encuentran en el mundo Internet a una red que asegure la calidad de los servicios y además tenga capacidad de gestionar y mantener las infraestructuras.

Esto, que visto sobre el papel cuadra bien, tiene la desventaja de que las operadoras son menos ágiles que las empresas del mundo Internet pero por el contrario tienen la ventaja de que estas operadoras vienen de las redes clásicas de conmutación de circuitos cuya disponibilidad es los cinco nueves (99,999%) y tienen a gala asegurar la calidad del servicio y deben seguir dando esa calidad con la nueva red. Por lo dicho anteriormente y por la posible canibalización de los servicios actuales la implantación de la NGN es lenta y si el modelo inglés de BT pretende estar totalmente operativo para el 2010., se considera que en España puede rondar el 2012/15, pero eso no es obstáculo en el mundo empresarial y sobre todo con las redes del tamaño grande como pueden ser la redes administrativas de la Comunidades Autónomas.

DILEMA DE LA SOLUCIÓN PARA COMUNICACIONES CONVERGENTES EMPRESARIALES

Como se ha comentando anteriormente existen dos soluciones para disponer de todos los servicios citados, modelo de inversión o modelo de servicio de operadora, pero si es cierto que solamente la solución de tener una plataforma propia lo permite en la actualidad. Si nos situamos en el tiempo todavía los nuevos servicios, presencia, mensajería, videoconferencia no son muy demandados pero lo que si es obligado es el servicio de voz y es en el servicio de voz donde nos centraremos.

SERVICIOS DE VOZ

Sin duda la voz es el servicio básico indispensable y que en la actualidad presenta un importante dilema. Ya se ha comentado la verticalización servicio/red que existía pero los nuevos servicios convergentes facilitados por el protocolo IP y la tendencia de todos los fabricantes hace insostenible a presente/futuro el mantenimiento de redes separadas. Esto que dicho así queda bien y es cierto trae aparejado la problemática de la adquisición, mantenimiento, y administración de los elementos comunes cuando sobre ellos circulan aplicaciones propias de TI y aplicaciones de voz. Esta situación se da por historia en muchas organizaciones, la voz depende de áreas asociadas al mantenimiento y los datos son propios de los departamentos de informática.

PROBLEMÁTICA DE LAS RESPONABILIDADES DIVIDAS

Con dos redes totalmente separadas de voz y de datos no hay ningún problema ya que toda la infraestructura es independiente desde cableados interiores hasta las salidas a red pública, la problemática radica en el momento de la compartición de infraestructuras tanto para su inversión, mantenimiento y administración/gestión.

Dentro de las infraestructuras comunes se pueden citar:

- Cableado estructurado al puesto del usuario.
- Elemento de electrónica de red (switch).
- Router.
- Red WAN (Wide Area Network).

Este informe pretende dejar constancia que la convergencia de infraestructuras, servicios/aplicaciones es inevitable y se apuntan los pasos que se deben dar para lograr unas inversiones con futuro.

ESTRATEGIA PARA LA CONVERGENCIA DE ENTORNOS

Después de analizar los nuevos servicios de comunicaciones personales y pensando siempre en esos nuevos servicios, soluciones integradas y convergencia fijo-móvil se dispone de tres formas para darlos:

- Todos los servicios con plataforma propia (inversión) y contratando las salidas/entradas a la red pública de las operadoras.
- Todos los servicios ofrecidos por las operadoras desde plataformas centrales de las mismas.
- Un modelo mixto en el que predomina el servicio y solamente la inversión en los elementos locales a nivel de edificio para ubicaciones críticas.

MODELO MIXTO INVERSIÓN LOCAL-SERVICIO CENTRALIZADO

El modelo mixto lo que pretende es tener la inmediatez de servicio necesaria para los centros que son nuevos o que deben ser renovados y además asegurar la inversión para lo que se considera a que es el modelo de futuro inmediato, que no es otro, que contratar a modo de servicio todos los servicios que se homologuen.

El anterior párrafo llevado a la realidad se traduce en las distintas soluciones según el entorno y las posibles servidumbres heredadas.

ESTRATEGIA DE LA NUEVA RED

La estrategia es disponer de una red convergente que facilite los servicios de voz y que asegure la calidad de servicio de la red actual. Para ello de momento en los centros críticos, su salida a la red pública será por tecnología tradicional, primarios RDSI y su marcación corporativa por tecnología IP. Se distinguen tres entornos:

- Edificios sin cableado estructurado.
- Edificios con cableado estructurado.
- Centros pequeños de salud no críticos.

EDIFICIOS SIN CABLEADO ESTRUCTURADO

Se pretende la renovación de los equipamientos de conmutación de circuitos (centralitas).

En un entorno muy crítico, siempre es aconsejable que haya equipamiento de emergencia (backup) y además en muchos casos es preciso mantener el cableado actual a dos hilos. Como solución estratégica se sugiere equipamiento local capaz de trabajar con enlaces TDM y tener salida/entrada a una plataforma IP centralizada Q.SIP (Session Initation Protocol). Así mismo la centralita admitirá extensiones IP/SIP. Este tipo de infraestructura permite que Telefónica avance en su infraestructura central y deja abierta todas las posibilidades a una telefonía todo IP actuando la centralita de Media GateWay (MGW) en caso de fallo de la red o plataforma IP.

EDIFICIOS CON CABLEADO ESTRUCTURADO

Dado que se dispone de cableado estructurado se ha diseñado la solución con tecnología IP hacia las extensiones con la condición de utilizar el protocolo SIP en las extensiones y que el terminal no supere los 60€. Sus interfaces hacia red pública y privada (corporativa) son las mismas que para los edificios sin cableado estructurado.

NUEVOS CENTROS PEQUEÑOS

En los centros pequeños y no críticos no se justifica una infraestructura de backup (MGW) y es en este tipo de centros donde se debe trabajar con celeridad para que se pueda contratar la telefonía convergente como un servio completo. Existen varios obstáculos que hay que ir superando para llegar a lo que se considera la solución óptima:

- Solución por parte de Telefónica de la plataforma central SIP capaz de dar soporte a los más de 300 centros.
- Contrato como servicio y no inversión.
- Se debe incluir para contratarlo como servicio completo los conmutadores.

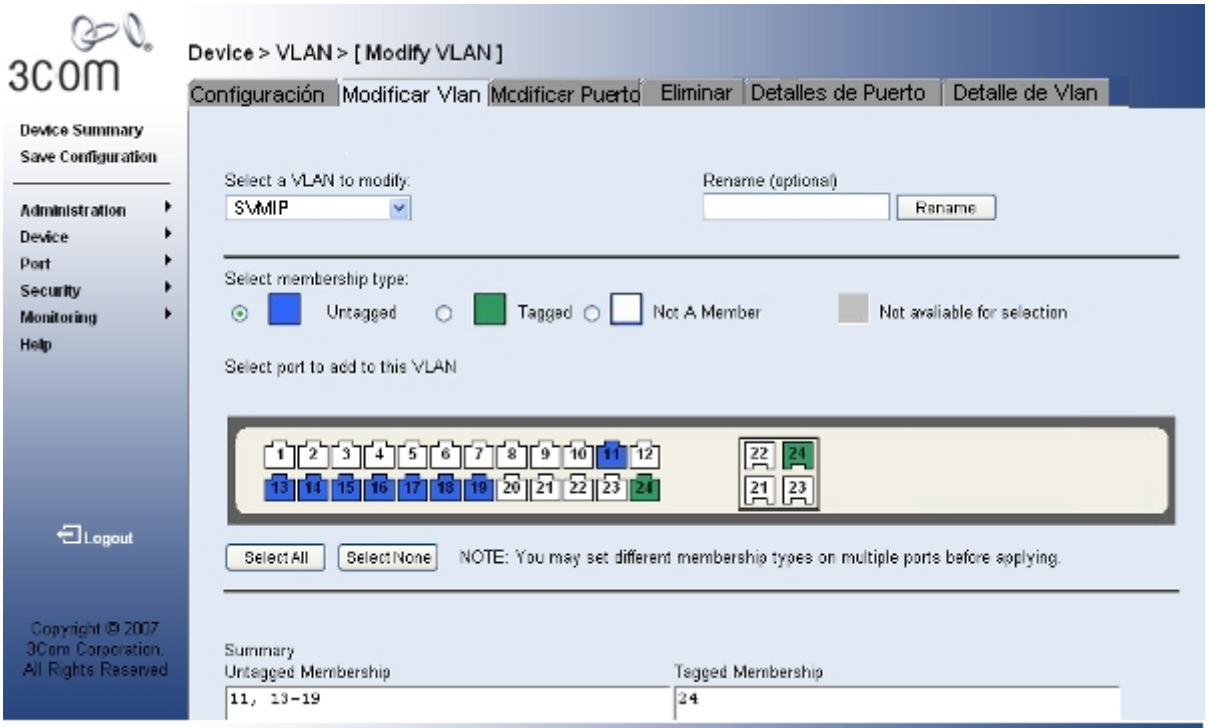
CONCLUSIONES

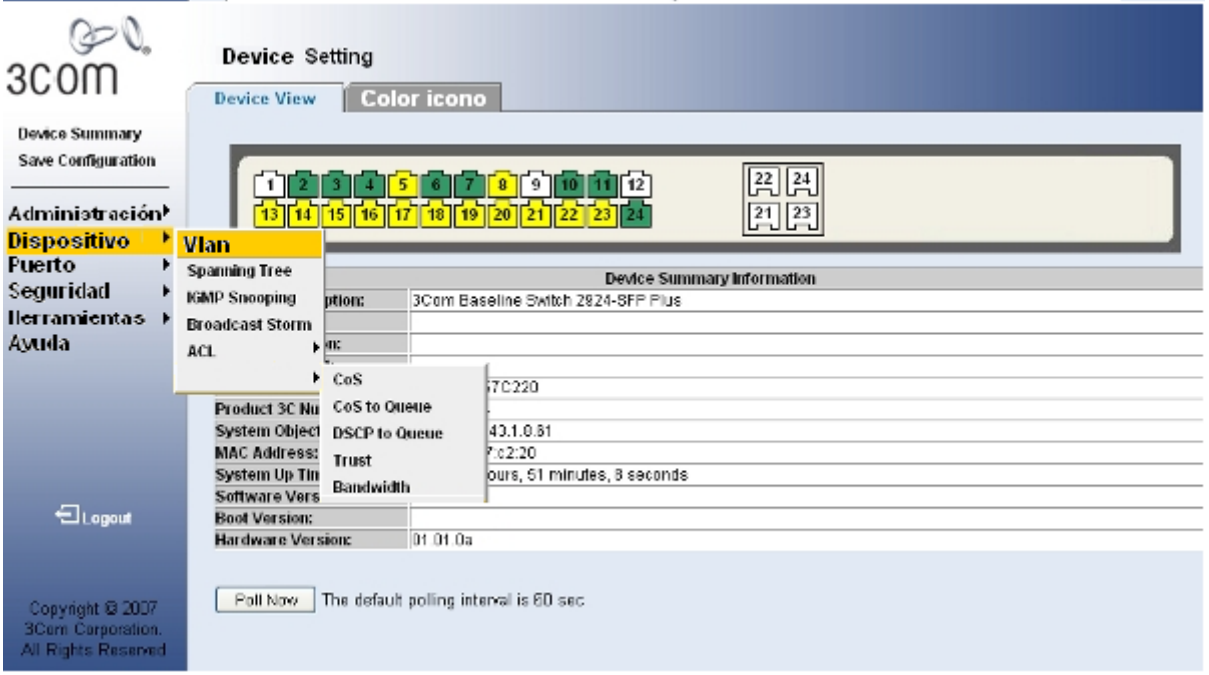
Este documento ha pretendido definir el presente, ToIP (Telefonía IP) y el futuro inmediato de las comunicaciones personales. Como se puede leer todo pasa por la convergencia, convergencia de infraestructuras, convergencia de servicios y convergencia de comunicaciones y TI.

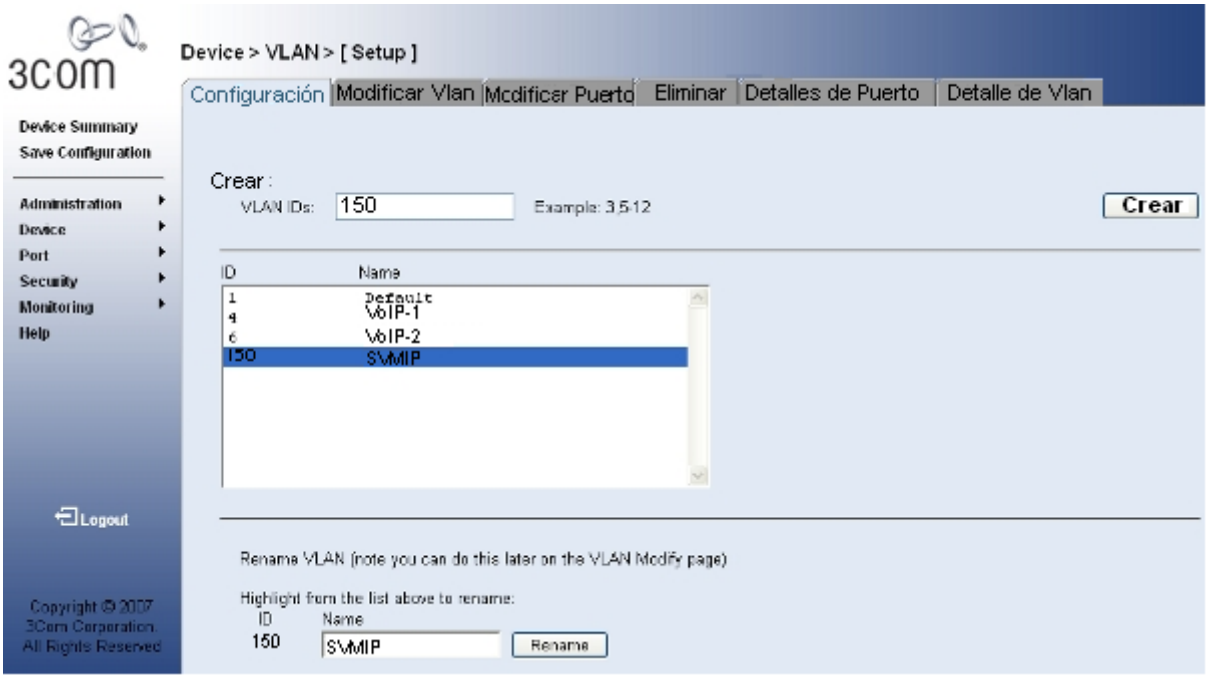
Se considera que entre una opción de inversión en adquisición de infraestructuras o un modelo de servicio ofertado por las operadoras de comunicaciones se debe optar por esta segunda opción excepto en las ubicaciones que por su criticidad deban estar soportadas en caso de emergencia por equipamiento en el propio edificio.

Dado que se apuesta por servicios, debemos mirar a los servicios actuales de comunicaciones personales que se ofrecen desde la red Internet. Todos los servicios están soportados por infraestructuras centrales y esta es la misma política que se debe considerar pero cambiando la red de transporte, se cambiaría la red Internet por una red de transporte IP con calidad controlada y las plataformas centrales serían de uso exclusivo a compartido dependiendo de la criticidad y volumetría radicadas en la operadora.

Y por último, y como parte más importante del documento se manifiesta la imposibilidad de disponer de servicios convergentes con infraestructuras de red independientes, una de voz y otra de datos. Como planificación en el tiempo lo primero es tener clara la solución que presenten las operadoras y muy en especial Telefónica.


Device > VLAN > [Modify VLAN]
Configuración
Modificar Vlan
Mcdificar Puerto
Eliminar
Detalles de Puerto
Detalle de Vlan
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Copyright © 2007 3Com Corporation. All Rights Reserved
Select a VLAN to modify:
SVMIP
Rename (optional)
Rename
Select membership type:
Untagged
Tagged
Not A Member
Not available for selection
Select port to add to this VLAN
Select All
Select None
NOTE: You may set different membership types on multiple ports before applying.
Summary
Untagged Membership
11, 13-19
Tagged Membership
24


Device Setting
Device View
Color icono
Device Summary
Save Configuration
Administración
Dispositivo
Puerto
Seguridad
Herramientas
Ayuda
Vlan
Spanning Tree
IGMP Snooping
Broadcast Storm
ACL
CoS
CoS to Queue
DSCP to Queue
Trust
Bandwidth
Logout
Copyright © 2007 3Com Corporation. All Rights Reserved
Device Summary Information
3Com Baseline Switch 2824-SFP Plus
Poll Now
The default polling interval is 60 sec

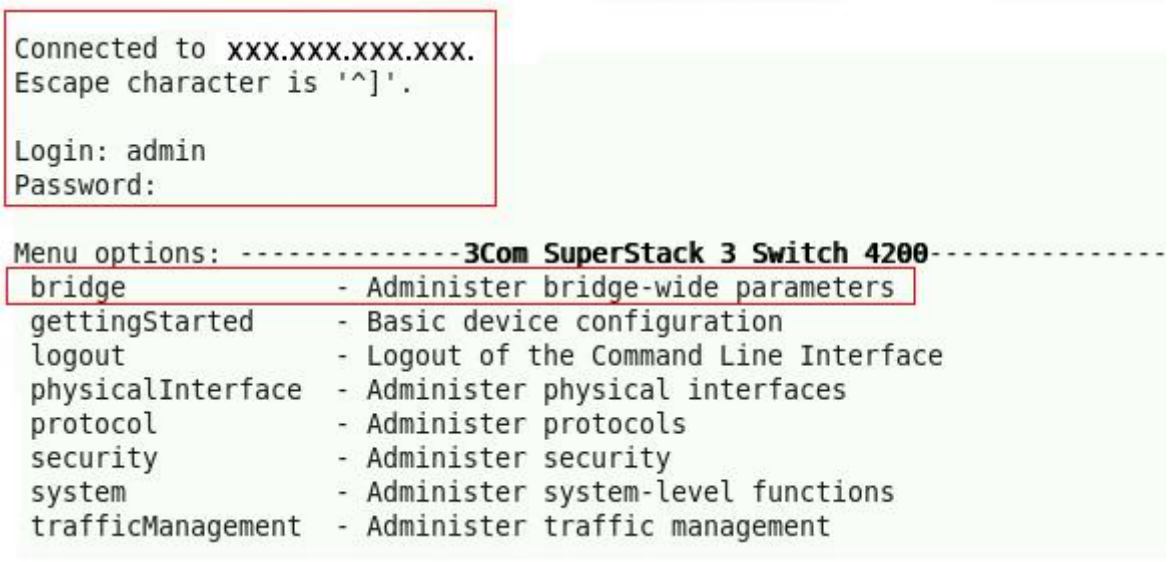

3com
Device > VLAN > [Setup]
Configuración
Modificar Vlan
Mcdificar Puerto
Eliminar
Detalles de Puerto
Detalle de Vlan
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Copyright © 2007
3Com Corporation.
All Rights Reserved
Crear :
VLAN IDs:
150
Example: 3,5-12
Crear
ID
Name
1
Default
4
VoIP-1
6
VoIP-2
150
SVMIP
Rename VLAN (note you can do this later on the VLAN Modify page)
Highlight from the list above to rename:
ID
Name
150
SVMIP
Rename

```
Select menu option (bridge/vlan/modify): quit

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 create             - Create a VLAN
 delete             - Delete a VLAN
 detail             - Display detailed information
 modify             - Modify a VLAN
 summary            - Display summary information

Type "quit" to return to the previous menu or  ? for help
---------------------------------------- (1)----------------------------
Select menu option (bridge/vlan): detail
Select VLAN ID (1-2)[1]: 150

VLAN ID: 150     Name: aula

Unit              Untagged Member Ports      Tagged Member Ports
----------------- ------------------------------------------------------
1                 6-25                       none
Aggregated Links  none                       none

Select menu option (bridge/vlan): logout
```

```
Select menu option (bridge/vlan): create
Select VLAN ID (1-4094)[2]: 150
Enter VLAN Name [VLAN 2]: SMVIP

Select menu option (bridge/vlan): modify

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 addPort             - Add a port to a VLAN
 name                - Name a VLAN
 removePort          - Remove a port from a VLAN

Type "quit" to return to the previous menu or  ? for help
---------------------------------------- (1)----------------------------
Select menu option (bridge/vlan/modify): addport
Select VLAN ID (1-2)[1]: 150
Select bridge ports (AL1-AL4,unit:port...,?): 1:6-1:25
Enter tag type (untagged,tagged): untagged

Select menu option (bridge/vlan/modify):
Select menu option (bridge/vlan/modify): quit

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 create              - Create a VLAN
 delete              - Delete a VLAN
 detail              - Display detailed information
 modify              - Modify a VLAN
 summary             - Display summary information

Type "quit" to return to the previous menu or  ? for help
---------------------------------------- (1)----------------------------
Select menu option (bridge/vlan): detail
Select VLAN ID (1-2)[1]: 150

VLAN ID: 150    Name: aula

Unit              Untagged Member Ports      Tagged Member Ports
----------------- -------------------------------------------------------
1                 6-25                       none
Aggregated Links  none                       none

Select menu option (bridge/vlan): logout
```

```
Select menu option (bridge/vlan): create
Select VLAN ID (1-4094)[2]: 150
Enter VLAN Name [VLAN 2]: SMVIP

Select menu option (bridge/vlan): modify

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 addPort             - Add a port to a VLAN
 name                - Name a VLAN
 removePort          - Remove a port from a VLAN

Type "quit" to return to the previous menu or  ? for help
------------------------------------------ (1)----------------------------
Select menu option (bridge/vlan/modify): addport
Select VLAN ID (1-2)[1]: 150
Select bridge ports (AL1-AL4,unit:port...,?): 1:6-1:25
Enter tag type (untagged,tagged): untagged

Select menu option (bridge/vlan/modify):
 Select menu option (bridge): vlan

 Menu options: --------------3Com SuperStack 3 Switch 4200---------------
  create              - Create a VLAN
  delete              - Delete a VLAN
  detail              - Display detailed information
  modify              - Modify a VLAN
  summary             - Display summary information

 Type "quit" to return to the previous menu or  ? for help
 ------------------------------------------ (1)----------------------------
 Select menu option (bridge/vlan):
------------------------------------------ (1)----------------------------
Select menu option: bridge

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 addressDatabase    - Administer bridge addresses
 broadcastStormCont - Enable/disable broadcast storm control
 linkAggregation    - Administer aggregated links
 multicastFilter    - Administer multicast filtering
 port               - Administer bridge ports
 spanningTree       - Administer spanning tree
 summary            - Display summary information
 vlan               - Administer VLANs

Type "quit" to return to the previous menu or  ? for help
```

```
Connected to xxx.xxx.xxx.xxx.
Escape character is '^]'.

Login: admin
Password:

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 bridge              - Administer bridge-wide parameters
 gettingStarted      - Basic device configuration
 logout              - Logout of the Command Line Interface
 physicalInterface   - Administer physical interfaces
 protocol            - Administer protocols
 security            - Administer security
 system              - Administer system-level functions
 trafficManagement   - Administer traffic management

Type  ? for help
------------------------------------- (1)---------------------------
Select menu option: bridge

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 addressDatabase     - Administer bridge addresses
 broadcastStormCont  - Enable/disable broadcast storm control
 linkAggregation     - Administer aggregated links
 multicastFilter     - Administer multicast filtering
 port                - Administer bridge ports
 spanningTree        - Administer spanning tree
 summary             - Display summary information
 vlan                - Administer VLANs

Type "quit" to return to the previous menu or  ? for help
------------------------------------- (1)---------------------------
Select menu option (bridge):
Select menu option (bridge): vlan

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 create              - Create a VLAN
 delete              - Delete a VLAN
 detail              - Display detailed information
 modify              - Modify a VLAN
 summary             - Display summary information

Type "quit" to return to the previous menu or  ? for help
------------------------------------- (1)---------------------------
Select menu option (bridge/vlan):
```



VioStor NVR
Grabadora de Vídeo en Red
Manual del usuario (Versión: 3.2.0)

PRÓLOGO

¡Gracias por haber elegido productos QNAP! Este manual de usuario proporciona instrucciones detalladas sobre el uso del producto. Por favor, léalo detenidamente y ¡comience a disfrutar las funciones poderosas del producto!

NOTA

 Todas las funciones, funcionalidades y otras especificaciones de producto son sujetas a cambios sin previo aviso u obligación.
 Todos los nombres y las marcas de productos mencionados son marcas registradas de sus correspondientes propietarios.

GARANTÍA LIMITADA

En ningún caso la responsabilidad de QNAP Systems, Inc. excederá el precio pagado
por el producto debido a daños directos, indirectos, especiales, fortuitos o derivados del software o su documentación. QNAP no ofrece reembolsos por sus productos. QNAP no ofrece ninguna garantía ni representación, ya sea expresa, implícita o estatutaria de sus productos, a los contenidos o al uso de esta documentación y todo el software que lo acompaña, y no se hace responsable específicamente de su calidad, rendimiento, comerciabilidad, o aptitud para un fin específico. QNAP se reserva el derecho a revisar o actualizar sus productos, software o documentación sin la obligación de notificarlo a ningún individuo o entidad.

Precaución

1. Recuerde siempre hacer una copia de seguridad de su sistema para evitar cualquier pérdida potencial de datos. QNAP no se hace responsable de cualquier tipo de pérdida de datos o de su recuperación.
2. Si devuelve cualquier componente del embalaje del producto para un reembolso o mantenimiento, asegúrese de que esté cuidadosamente embalado para envío. No se compensará ningún tipo de daño debido a un embalaje inadecuado.

Aviso Importante

 Leer las instrucciones

Por favor, lea las advertencias de seguridad y el manual del usuario detenidamente antes de usar este producto.

 Fuente de alimentación

Este producto sólo puede usarse con la fuente de alimentación proporcionado por el fabricante.

 Servicio

Por favor, contacte con técnicos cualificados para cualquier consulta técnica. No intente reparar este producto Ud. mismo para evitar cualquier peligro relacionado con tensiones u otros riesgos causados por la apertura de la tapa de este producto.

 Advertencia

Para evitar fuego o choque eléctrico, no use este producto bajo la lluvia o en ambientes húmedos. No coloque ningún objeto sobre este producto.

Contenido

Advertencia de Seguridad

1. Este producto puede funcionar con normalidad con temperaturas entre 0ºC y 40ºC y con una humedad relativa de entre 0% y 90%. Por favor, asegúrese de que el entorno esté bien ventilado.
2. El cable de alimentación y los dispositivos conectados a este producto deben proporcionar un voltaje de suministro correcto.
3. No coloque este producto bajo luz solar directa o cerca de productos químicos. Asegúrese de que la temperatura y la humedad ambientales estén en un nivel óptimo.
4. Desenchufe el cable de alimentación y todos los cables conectados antes de limpiarlo. Pase un paño húmedo por el producto. No use productos químicos ni aerosoles para limpiar este producto.
5. No coloque ningún objeto sobre este producto para garantizar el funcionamiento normal del servidor y para evitar un sobrecalentamiento.
6. Use los tornillos de cabeza plana incluidos en el embalaje del producto para asegurar los discos duros del producto durante su instalación para que funcione adecuadamente.
7. No coloque este producto cerca de ningún líquido.
8. No coloque este producto sobre una superficie desigual para evitar que se caiga y sufra daños.
9. Asegúrese de que el voltaje de su área sea correcto al usar este producto. Si tiene dudas sobre el voltaje, por favor, póngase en contacto con el distribuidor o con su compañía de suministro eléctrico local.
10. No coloque ningún objeto sobre el cable de alimentación.
11. No intente reparar este producto en ningún caso. Un desensamblaje incorrecto del producto puede exponerle a una descarga eléctrica o a otros riesgos. Para cualquier pregunta, por favor, póngase en contacto con el distribuidor.

Capítulo 1. Introducción al Viostor

1.1 Vista Preliminar del Producto

QNAP VioStor (de aquí en adelante se llamará NVR o VioStor) es la solución de supervisión de redes de alto desempeño para controlar con base en la red, las cámaras IP, grabación de vídeo, reproducción y acceso a los datos remotos. Se pueden controlar simultáneamente hasta 120 canales para múltiples servidores QNAP NVR. El NVR soporta cámaras basadas en IP desde AXIS, ACTi, A-MTK, Arecont Vision, AVTECH, Canon, CNB, DIGITUS, D-Link, EDIMAX, ELMO, EtroVision, GANZ, Hikvision, iPUX, IQeye, LevelOne, Messoa, MOBOTIX, Nakayo, Panasonic BB/ BL/ i-Pro, SANYO, SONY, TOSHIBA, TRENDnet, VIVOTEK, VIOSECURE y Y-CAM. Los usuarios pueden grabar vídeo usando formatos de compresión H.264, MxPEG, MPEG-4 o MJPEG. El NVR ofrece diversos modos de visualización y funciones de grabación, por Ej., grabación programada, grabación de alarma y horario de grabación de alarmas. El NVR soporta búsqueda de información guardada por fecha y hora, horarios, eventos, análisis inteligente de vídeos, incluyendo detección de movimientos, objetos perdidos, objetos extraños, desenfoques, oclusiones de la cámara, etc. Todas las funciones se pueden configurar para el navegador IE.
* La compresión de video MxPEG no la soportan el VS-201, VS-101, NVR-104.

1.2 Ilustración del Hardware

1.2.1 VS-8040U-RP/ 8032U-RP/ 8024U-RP

1. Indicadores LED: Estado, LAN, USB, HDD1–8

2. Botón de encendido
3. Botón de selección
4. Botón intro
5. Conector de alimentación
6. Botón para restablecer las configuraciones de Contraseña y red
7. RS-232
8. VGA (Reservado)
9. USB 2.0 x 4
10. Giga LAN x 2
10

1.2.2 VS-8040/ 8032/ 8024

1. Botón de Copia de Seguridad (Acceso directo de copia de seguridad de vídeo automática)
2. USB 2.0
3. Indicadores LED: Estado, LAN, USB, HDD1–8
4. Botón de encendido
5. Botón de selección
6. Botón intro
7. Conector de alimentación
8. Giga LAN x 2
9. USB 2.0 x 4
10. RS-232
11. VGA (Reservado)
12. Botón para restablecer las configuraciones de Contraseña y red
13. Ranura para el sistema de seguridad kensington
11

1.2.3 VS-5020/ VS-5012

1. Botón de Copia de acceso directo
2. USB 2.0
3. Indicadores LED: USB, Estado, HDD1–HDD5, LAN
4. Botón de encendido
5. Botón de selección
6. Botón intro
7. Conector de alimentación
8. Giga LAN x 2
9. USB 2.0 x 4
10. Conector eSATA
11. (Reservado)
12. Puerto RS-232
13. Botón para restablecer las configuraciones de Contraseña y red
14. Ranura para el sistema de seguridad kensington
12

1.2.4 VS-4016U-RP

1. Botón de copia de seguridad
2. USB 2.0
3. Indicadores LED: USB, Estado, HDD1–HDD4, LAN
4. Botón de encendido
5. Conector de alimentación
6. Giga LAN x 2
7. USB 2.0 x 2
8. Botón para restablecer las configuraciones de Contraseña y red
9. VGA (Reservado)
13

1.2.5 VS-2012/ VS-2008

1. Botón de Copia de Seguridad (Acceso directo de copia de seguridad de vídeo

automática)
2. USB 2.0
3. Indicadores LED: HDD1, HDD2, LAN, y eSATA
4. Botón de Encendido
5. Conector de Alimentación
6. Giga LAN x 2
7. USB 2.0 x 2
8. Interruptor de Reinicio de Configuraciones (Reinicio de Contraseña y configuraciones de red)
9. Ranura de Seguridad para un dispositivo de Bloqueo Kensington
10. eSATA x 2 (Reservado)
11. Adaptado (Reservado)
14

1.2.6 VS-201P/ V

1. Botón de Copia de Seguridad (Acceso directo de copia de seguridad de vídeo automática)
2. USB 2.0
3. Indicadores LED: USB, Estado, HDD1, HDD2, LAN, y Alimentación
4. Botón de Encendido
5. Conector de Alimentación
6. Giga LAN
7. USB 2.0 x 2
8. Interruptor de Reinicio de Configuraciones (Reinicio de Contraseña y configuraciones de red)
9. Ranura de Seguridad para un dispositivo de Bloqueo Kensington
15

1.2.7 NVR-104P/ V

1. Botón de Copia de Seguridad
2. USB 2.0
3. Indicadores LED
4. Botón de Encendido
5. USB 2.0 x 2
6. Puerto eSATA
7. Giga LAN
8. Interruptor de Reinicio de Configuraciones
9. Conector de Alimentación
10. Ranura de Seguridad K-lock
16

1.2.8 VS-101P/ V

1. Botón de Copia de Seguridad
2. USB 2.0
3. Indicadores LED
4. Botón de Encendido
5. Conector de Alimentación
6. Giga LAN
7. USB 2.0 x 2
8. Interruptor de Reinicio de Configuraciones
9. Ranura de Seguridad K-lock
10. Puerto eSATA
17

Capítulo 2. Instalar VioStor

Para obtener información sobre la instalación del hardware, por favor consulte "Guía
de Instalación Rápida" del paquete del producto.

2.1 Requisitos de Ordenador Personal

Para un mejor rendimiento del sistema, su ordenador debería cumplir al menos con los siguientes requisitos:

No. de Canales	Formato	CPU	Otros
4	M-JPEG	Procesador Intel® Pentium 4, 2.0 GHz o superior	
	MPEG-4/ MxPEG/ H.264	CPU de núcleo cuádruple, 2,0 GHz o superior	
8	M-JPEG	Procesador Intel® Pentium 4, 2,2 GHz o superior	
	MPEG-4/ MxPEG/ H.264	CPU de núcleo doble, 2,2 GHz o superior	
12	M-JPEG	Procesador Intel® Pentium 4, 2,4 GHz o superior	
	MPEG-4/ MxPEG/ H.264	CPU de núcleo doble, 2,4 GHz o superior	
16	M-JPEG	Procesador Intel® Pentium 4, 2,6 GHz o superior	
	MPEG-4/ MxPEG/ H.264	CPU de núcleo doble, 2,6 GHz o superior	
20	M-JPEG	Procesador Intel® Pentium 4, 2,8 GHz o superior	

- Sistema Operativo: Microsoft® Windows® XP/ Vista (64-bits)
- Memoria: 1 GB o superior
- Puertos de red: Puerto Ethernet de 100Mbps o superior
- Navegador Web:

Microsoft®
Internet Explorer
6.0 o superior
 Unidad de
DVD-ROM.
 Resolución
recomendada:
1024 x 768 pixeles
o superior
18
20 MPEG-4/ MxPEG/
H.264
CPU de núcleo doble, 2,8
GHz o superior
M-JPEG CPU de núcleo doble, 2,4
GHz o superior
40
MPEG-4/ MxPEG/
H.264
CPU Quad core, 2,4 GHz o
superior
19
Configuración de Seguridad del Explorador Web
Por favor, asegúrese de que el nivel de seguridad del Explorador IE esté
configurado
como "Media" o inferior en las "Opciones de Internet".
20

2.2 Lista de Recomendaciones para el Disco Duro

Este producto funciona con unidades de disco duro SATA de 2,5"/ 3,5" de las principales marcas de discos duros. Si desea consultar la lista de unidades HDD compatibles, visite la dirección http://www.qnapsecurity.com/pro_compatibility.asp. QNAP no se responsabiliza en ningún momento ni por ninguna razón por daño/avería del producto o por la pérdida/recuperación de datos debidos al mal uso o instalación inadecuada de los discos duros.

2.3 Lista de Cámaras de Red Compatibles

Para más información sobre los modelos de cámaras compatibles, por favor, visite el
sitio web de QNAP Security en
http://www.qnapsecurity.com/pro_compatibility_camera.asp.
21

2.4 Comprobar el Estado del Sistema

Indicadores LED y descripción general del estado del sistema
Indicador
LED
Color
Estado del
indicador LED
Descripción
Parpadea en azul
cada 0,5 segundos
1) Se ha detectado un dispositivo
USB
2) Se está desconectando del
NVR un dispositivo USB
3) Se está accediendo al

dispositivo USB conectado al puerto USB frontal del NVR
4) Se están copiando datos del NVR en el dispositivo USB externo
Azul
El dispositivo USB conectado al puerto USB frontal del NVR está listo
USB **Azul**
Desactivado
El NVR ha terminado de copiar los datos al dispositivo USB conectado al puerto USB frontal*
eSATA† **Naranja** Parpadeando
Se está accediendo al dispositivo eSATA
Estado del sistema
Rojo /
Verde
Parpadea alternativamente en verde y rojo cada 0,5 segundos
1) Se está formateando el disco duro del NVR
2) Se está inicializando el NVR
3) Se está actualizando el firmware del sistema
4) Se está llevando a cabo una reconstrucción RAID
5) Se está llevando a cabo una expansión de la capacidad RAID en línea
6) Se está llevando a cabo una migración de nivel RAID en línea
22
Rojo
1) El disco duro no es válido
2) El volumen de disco ha alcanzado su máxima capacidad
3) El volumen de disco está próximo a encontrarse lleno
4) El ventilador del sistema no funciona*
5) Se ha producido un error al acceder a los datos del disco (lectura / escritura)
6) Se ha detectado un sector defectuoso en el disco duro
7) El NVR está funcionando en

modo de sólo lectura
degradado (fallo de 2 unidades en una configuración RAID 5 o RAID 6, aún es posible leer los datos del disco)#
8) (Error en la prueba automática de hardware)
Parpadea en rojo cada 0,5 segundos
El NVR está funcionando en modo degradado (fallo de una unidad en una configuración RAID 1, RAID 5 o RAID 6)*
Parpadea en verde cada 0,5 segundos
1) El NVR se está iniciando
2) El NVR no está configurado
3) El disco duro no está formateado
Verde El NVR está listo
Desactivado
Todos los discos duros del NVR se encuentran en suspensión
Parpadea en rojo
Se está accediendo a los datos de la unidad de disco duro y se ha producido un error de lectura / escritura durante el proceso
Rojo
Se ha producido un error de lectura / escritura en la unidad de disco duro
Parpadea en verde
Se está accediendo a los datos del disco duro
HDD
Rojo /
Verde
Verde Es posible acceder al disco duro
Naranja El NVR está conectado a la red
LAN **Naranja** Parpadea en naranja
Se está accediendo al NVR desde la red
* No aplicable a los modelos de 1 bahía
† El puerto eSATA está disponible solamente en algunos modelos. Por favor consulte
las especificaciones del producto para obtener más información.
Solamente Modelos de 4 bahías o más

Zumbador de alarma (El zumbador de alarma se puede deshabilitar a través de “Herramientas de Sistema” > “Configuraciones de Hardware”)
Sonido N.º de veces Descripción
Sonido corto (0,5 segundos)

1 1) El NVR se está iniciando
2) El NVR se está apagando (apagado software)
3) El usuario ha pulsado el botón de restablecimiento para restablecer el NVR
4) Se ha actualizado el firmware del sistema
Sonido corto (0,5 segundos)
3 El usuario ha intentado copiar datos del NVR en un dispositivo de almacenamiento externo a través del puerto USB frontal, pero los datos no se pueden copiar.
Sonido corto (0,5 segundos), sonido largo (1,5 segundos)
3, cada 5 minutos
El ventilador del sistema no funciona*
2 1) El volumen de disco está próximo a encontrarse lleno
2) El volumen de disco ha alcanzado su máxima capacidad
3) Los discos duros del NVR se encuentran en modo degradado
4) El usuario ha iniciado el proceso de reconstrucción de HDD
Sonido largo (1,5 segundos)
1 1) Se ha forzado el apagado del NVR (apagado hardware)
2) El NVR se ha encendido con éxito y está listo
* No aplicable a los modelos de 1 bahía
24

2.5 Configuración del Sistema

Instalar el Buscador (Finder)

1. Ejecute el CD del producto. Aparecerá el siguiente menú. Seleccione "Instalar el Buscador".
25
2. Siga las instrucciones en pantalla para instalar el Buscador. El Buscador se ejecutará automáticamente. Si está usando Windows XP SP2, aparecerá la siguiente pantalla. Por favor, seleccione "Desbloquear".
3. El Buscador detectará VioStor en la red y le preguntará si quiere llevar a cabo una configuración rápida. Haga clic en "Aceptar" para continuar.
Nota: Si no se encuentra VioStor, haga clic en "Actualizar" para volver a intentarlo.
26
4. Debe introducir el nombre y la contraseña del administrador para realizar la configuración rápida.
El nombre y la contraseña del administrador por defecto son los siguientes:
Nombre del Usuario: **admin***
Contraseña: **admin**

* Si usa VS-201/ VS-101/ NVR-104, el nombre de usuario es 'administrator' y la contraseña es 'admin'.
Nota: Por favor, verifique que todas las cámaras de red estén configuradas y conectadas a la red.
5. Se mostrará la página de configuración rápida. Haga clic en "Continuar" y siga las instrucciones para finalizar la configuración. Para una configuración detallada, por favor, consulte el Capítulo 5.1.
27
6. Tras completar las configuraciones, haga clic en "Iniciar Instalación" para aplicar los cambios e inicializar el sistema.
7. La configuración rápida se ha completado y ya puede empezar a usar VioStor. Haga clic en "Iniciar Monitorización" para ver vídeo en directo desde las cámaras o haga clic en "Cerrar" para volver a la página de inicio de la administración del sistema.
28
8. Por favor, instale ActiveX la primera vez que se conecte al servidor. Siga las instrucciones para instalar ActiveX.
Cuando se muestre vídeo en directo y aparezca el indicador de grabación, habrá instalado VioStor con éxito.
29

Capítulo 3. Empezar a Usar VioStor

Cuando haya instalado VioStor y el resto del hardware y lo haya conectado a la red, podrá usar el explorador de su PC para conectarse a VioStor. Se recomienda usar Microsoft Internet Explorar para explorar.
Aviso Importante:
Antes de empezar a usar VioStor, debe instalar uno o dos discos duros en VioStor, finalizar la configuración del volumen de disco y formatear el/los Disco(s) duro(s). Si no lo hace, puede que el sistema no funcione correctamente.

3.1 Conectar a VioStor

Siga los siguientes pasos para conectarse a la página de monitorización de VioStor:
1. Abra un explorador IE e introduzca la dirección IP de VioStor. O ejecute el acceso directo al Finder ("Buscador") del Escritorio. Cuando se muestra la siguiente pantalla, haga doble clic en el nombre de VioStor.
Haga doble clic en el nombre de VioStor para iniciar sesión en el servidor
30
2. Introduzca el nombre de usuario y la contraseña para iniciar sesión en VioStor.
Nombre del Usuario por Defecto: **admin***
Contraseña por Defecto: **admin**
* Si usa VS-201/ VS-101/ NVR-104, el nombre de usuario es 'administrator' y la contraseña es 'admin'.
3. Para ver un vídeo de VioStor en directo, debe instalar primero el control ActiveX de VioStor. Siga las instrucciones del explorador para instalarlo.
31

3.2 Página de Monitorización

Cuando haya iniciado sesión con éxito en VioStor, se mostrará la página de monitorización. Seleccione el idioma de la pantalla. Puede ver el vídeo en directo desde las cámaras, ver el mapa electrónico y el estado de almacenamiento, ajustar el modo de visualización, habilitar la grabación manual, tomar una instantánea, etc.
Icono Descripción
Modo de visualización múltiple
Soporta modo de visualización múltiple. (Esta función

solamente se puede usar cuando el ordenador o el host está conectado a múltiples monitores.)

Monitorización multi-servidor:

Pueden agregarse hasta 120 canales de distintos servidores NVR para su monitorización.

Seleccionar idioma:

Seleccione el idioma de la pantalla.

Mapa Electrónico:

Muestra la ubicación de la cámara. El mapa electrónico

Ver el canal y los detalles de monitorización

Panel de control PTZ

Firmware del Sistema

Ajustar el modo de visualización

Nombre del servidor

puede cambiarse en la página de configuración del sistema.

Entrar en la página de configuración del sistema:

Iniciar sesión en la página de configuración del sistema, al cuál sólo puede acceder el administrador.

Configuraciones de monitor:

Esta página le permite ajustar las configuraciones avanzadas de las funciones de la página de monitorización, por ejemplo, la fuente de vídeo y audio, alertas por evento, y la ruta de almacenamiento de las tomas instantáneas.

Reproducción:

Entrar en la página de reproducción de la grabación. El administrador puede asignar el derecho del usuario para acceder a esta página.

Ayuda:

Ver la ayuda en línea para usar VioStor.

Terminar sesión:

Terminar sesión en la página de monitorización.

Instantánea:

Tomar una instantánea con la cámara seleccionada. Cuando se muestre la imagen, haga clic con el botón derecho en la imagen para guardarla en el ordenador.

Grabación manual:

Habilitar o deshabilitar la grabación manual en la cámara seleccionada. El administrador puede habilitar o deshabilitar esta opción en la página de configuración del sistema.

(Opción) Audio:

Habilitar/deshabilitar el soporte de audio para la página de monitorización.

Iniciar sesión en la página de inicio de la cámara de red:

Seleccione una cámara y haga clic en este botón para ir

a la página de inicio de la cámara seleccionada.

Notificación de Evento:

Cuando la grabación de la alarma esté habilitada y se detecte un evento, se mostrará este icono

automáticamente, Haga clic en este icono para ver los detalles de la alerta.

Zoom digital:

Seleccione una cámara y haga clic en este botón para habilitar la función de zoom automático de la cámara. (También puede hacer clic con el botón derecho en el canal de monitorización para habilitar esta función.) Mantenga pulsado el botón izquierdo del ratón para acercar el zoom o mantenga pulsado el botón derecho del ratón para alejar el zoom. Puede pulsar el botón izquierdo del ratón para arrastrar el ángulo de visión de la cámara.

También puede usar la rueda del ratón o el panel de control PTZ para usar la función de zoom digital.

Control de Enfoque:

Control de enfoque de la cámara PTZ.

Seleccionar las posiciones preestablecidas para la cámara PTZ:

Puede visualizar distintas posiciones preestablecidas de la cámara, haciendo clic en los botones numéricos. Para configurar las posiciones preestablecidas de la cámara, por favor, consulte el manual del usuario de la cámara.

Estado de almacenamiento de la grabación:

Muestra el porcentaje de almacenamiento y el espacio libre.

Nota:

1. Iniciar o parar la grabación manual no influirá en una grabación programada o de alarma. Son procesos independientes.
2. La ruta por defecto para guardar las instantáneas es la carpeta "Snapshot" situada en Mis Documentos en su ordenador.
3. Si la hora de la instantánea no es consistente con la hora real a la que se tomó la instantánea, esto es debido al ambiente de red, no a un error de sistema.
4. Haga clic en el icono de notificación de evento para ver los detalles del evento, habilitar o deshabilitar el sonido de alerta o para eliminar los registros de evento.

5. Cuando esté habilitada la función de zoom digital en múltiples cámaras, la función de zoom resultará afectada si el rendimiento de su ordenador no es lo bastante alto.
6. Haga clic con el botón secundario en el canal de monitorización en la página de vista en directo. Las siguientes funciones están disponibles en función del modelo de cámara.

a. Conectar a la página de inicio de la cámara.
b. Configuraciones de la Cámara: Acceder a la página de configuración de la cámara.
c. PTZ: Control de giro / inclinación / zoom de la cámara.
d. Preconfiguración: Seleccionar las posiciones preestablecidas para la cámara PTZ.
e. Habilitar el seguimiento en directo: Disponible en cámaras Panasonic NS202(A).

f. Deshabilitar el seguimiento en directo: Disponible en cámaras Panasonic NS202(A).
g. La función de auto navegación de VioStor NVR se usa para configurar las cámaras PTZ y poder navegar de acuerdo a las posiciones predefinidas y el tiempo establecido de permanencia establecido para cada posición.
h. Zoom digital: Habilitar / deshabilitar zoom digital.
i. Mantener la relación de aspecto.
35

3.2.1 Ventana de Vídeo en Directo

Si la cámara está configurada adecuadamente, podrá ver el vídeo actual desde la cámara de red remota dentro de la ventana de vídeo en directo.
Si su cámara es compatible con las funciones de giro e inclinación, puede hacer clic directamente en la ventana de vídeo para ajustar el ángulo de visión. Si la cámara es compatible con la función zoom, puede usar la rueda del ratón para ajustar la distancia del zoom moviendo la rueda. Estas operaciones dependen del modelo de la
cámara. Por favor, confirme el manual del usuario de su cámara para más información.
Cuando habilita el zoom digital, puede hacer clic con el botón derecho en la cámara y controlar la función PTZ. Puede mantener pulsado el botón izquierdo del ratón para acercar el zoom o mantener pulsado el botón derecho del ratón para alejar el zoom, o pulsar el botón izquierdo para arrastrar el ángulo de visión de la cámara.
36

Estado de Cámara

El estado de cámara se indica mediante los iconos mostrados a continuación:

Icono Estado de Cámara

Grabación programada o continua en progreso
Esta cámara soporta la función de audio
Esta cámara es compatible con la función PT (giro e inclinación)
La grabación manual está habilitada
La grabación activada por la administración avanzada de eventos ("Configuración de Camera" > "Configuración de Alarma" > "Modo Avanzado") está en proceso
La entrada de alarma 1 de la cámara ha sido activada y está en proceso de grabación
La entrada de alarma 2 de la cámara ha sido activada y está en proceso de grabación
La entrada de alarma 3 de la cámara ha sido activada y está en proceso de grabación
Está en proceso de grabación debido a una detección de movimiento
El zoom digital está habilitado

Mensaje de Conexión

Si VioStor no puede mostrar una cámara, aparecerá un mensaje en la ventana de vídeo en directo. Puede que aparezcan los siguientes mensajes:

 Conectando

Si la cámara de red está instalada en una red remota o en Internet, puede que lleve algún tiempo establecer conexión con la cámara.

 Desconectado

No se puede conectar con la cámara de red. Por favor, compruebe la conexión de red de su ordenador y la disponibilidad de la cámara de red. Si la cámara está instalada en Internet, el puerto para la cámara debe estar abierto en su enrutador o puerta de enlace.

 Sin Permiso

Este mensaje aparece cuando un usuario sin privilegios de acceso intenta ver esta cámara. Por favor, salga del sistema e inicie sesión como un usuario con

privilegios de acceso para ver esta cámara.
 Error del Servidor
Por favor, compruebe las configuraciones de la cámara o intente actualizar con una nueva versión el firmware de la cámara. Póngase en contacto con el soporte técnico si el problema no se resuelve tras la comprobación.
37

3.2.2 Modo de Visualización

Cambiando el modo de visualización, podrá ajustar fácilmente los efectos visuales al
ver un vídeo de una o varias cámaras.

3.2.3 Panel de Control de Cámara PTZ

PTZ significa control de cámara Pan/ Tilt/ Zoom ("Giro/ Inclinación/ Zoom"). Puede ejercer control PTZ en la cámara seleccionada. Estas funciones están disponibles dependiendo del modelo de la cámara; por favor, consulte el manual del usuario de la cámara. La función de zoom digital no se puede utilizar simultáneamente con la función PTZ.

Canal único

Modo 4 canales

Modo 8 canales

Modo 10 canales

Pantalla completa

Combinación de otro canal

Modo 9 canales

Modo 6 canales

Modo Imagen-en-Imagen

Modo secuencial

Ajustar tamaño de la
ventana

Ajustar el ángulo
PT (giro e
inclinación) de la
cámara.

Seleccione las
posiciones
preestablecidas de la
cámara PTZ

Alejar el zoom

Control de enfoque
de la cámara PTZ

Acercar el zoom

Inicio

Zoom digital

38

3.2.4 Monitorización multiservidor

1. Haga clic en "Lista de servidores" en la página de vista en directo.
a. Haga clic en "Detectar automáticamente" para buscar el NVR QNAP en la red LAN y agregar el servidor a la lista de servidores.

b. Haga clic en “Agregar” para agregar el NVR QNAP a la lista de servidores.
2. pueden agregarse hasta 120 canales de distintos servidores NVR para su monitorización.
39

3.2.5 Auto navegación

La función de auto navegación de VioStor NVR se usa para configurar las cámaras PTZ y poder navegar de acuerdo a las posiciones predefinidas y el tiempo establecido de permanencia establecido para cada posición.
Para usar la función de auto-navegación, siga estos pasos.
1. En la página de monitorización del VioStor NVR, haga clic en para ir a la página de configuración de la cámara PTZ.
2. Defina las posiciones predefinidas de la cámara PTZ.
3. Regrese a la página de monitorización del VioStor NVR. Haga clic derecho en la pantalla de la cámara PTZ. Seleccione “Auto navegación”.
40
4. Haga clic en los botones numéricos para ver las posiciones predefinidas de la cámara PTZ. Cuando hace clic en el botón, el nombre de la posición definida correspondiente se muestra en el menú desplegable “Predefinir nombre”.
41
5. Agregar: Para agregar especificaciones para auto navegación, seleccione “Predefinir Nombre” desde el menú desplegable y entre el tiempo de permanencia (intervalo, en segundos). Haga clic en “Agregar”
6. Actualizar: Para cambiar las especificaciones de la lista, resalte el elemento. Permite seleccionar otra posición predefinida desde el menú desplegable y/o cambiar el tiempo de permanencia (intervalo). Haga clic en “Actualizar”.
7. Eliminar: Para eliminar una especificación, resalte el elemento de la lista y clic en “Eliminar”. Para eliminar más de una especificación, presione y sostenga la tecla Ctrl y haga clic en las especificaciones. Luego haga clic en “Eliminar”.
42
8. Después de la configuración de auto navegación, escoja la casilla de verificación “Activar auto navegación” y haga clic en “OK”. El sistema empezará la auto navegación, de acuerdo con las especificaciones.

Nota:

1) El tiempo de permanencia por defecto (intervalo) de la posición predefinida es de 5 segundos. Puede entrar 5-999 segundos para esta especificación.
2) El sistema soporta hasta 10 posiciones predefinidas (las primeras 10) configuradas en las cámaras PTZ. Puede configurar hasta 20 especificaciones para auto navegación en el NVR. EN otras palabras, el NVR soporta 10 selecciones como máximo en el menú desplegable y 20 en la lista de auto navegación.
43

Capítulo 4. Reproducir Archivos de Vídeo

VioStor proporciona una interfaz web intuitiva para buscar y reproducir archivos grabados. No es necesaria la instalación de software adicional. Además, puede usar los servicios de archivo de red para acceder directamente a los archivos de vídeo grabados.

4.1 Usar la Interfaz de Reproducción Web (VioStor Player)

1. Haga clic en el botón de reproducción en la página de monitorización.
2. El reproductor VioStor se mostrará. Puede usar este programa para buscar y reproducir los ficheros guardados en los servidores de NVR. Para volver a la página de monitorización, haga clic en . Para entrar en la página de administración del sistema, haga clic en .
44

Nota: Si no tiene permiso de acceso a las cámaras, no podrá acceder a la lista de

archivos de grabación ni reproducir las grabaciones de vídeo de las cámaras. Por favor, consulte el Capítulo 5.5 para la configuración de privilegios de acceso.

4.1.1 Conectar al servidor para la reproducción

1. Haga clic en "Reproducir por hora" .

45

2. Se mostrará el siguiente cuadro de diálogo.

46

3. Configurar servidores:

a. Añadir: Añadir un servidor.

b. Modificar: Modificar un servidor.

c. Eliminar: Eliminar un servidor.

d. Automático: Búsqueda automática de servidores.

e. Configuraciones por defecto: Introduce el nombre de usuario y la contraseña por defecto para todos los servidores recién añadidos.

47

4. Seleccione el modo de búsqueda de datos

 Búsqueda de fecha y hora (Entrada de texto)

i. Seleccione los servidores NVR y la(s) cámara(s) IP*.

ii. Clic en la pestaña "Entrada de texto".

iii. Seleccione el tipo de grabación, el tiempo inicio y finalización cuando el video se graba.

iv. Haga clic en "Preview" (Vista previa) para la visualización previa del video buscado.

v. Clic en "Aceptar".

*** Puede seleccionar las 4 cámaras IP como máximo.**

48

 Búsqueda de cronograma

i. Seleccione el o los servidores y la(s) cámara(s) IP.

*** Puede seleccionar las 4 cámaras IP como máximo.**

ii. Clic en la pestaña "Entrada gráfica".

49

iii. Seleccione el tipo de grabación.

iv. Especifique el rango de tiempo cuando se guardarán los ficheros. Las especificaciones se aplicarán a todas las cámaras seleccionadas.

v. Haga clic en "Vista previa" para la visualización previa del video buscado.

vi. Haga clic en "OK".

50

 Entrada de evento

i. Seleccione el o los servidores y la(s) cámara(s) IP.

*** Puede seleccionar las 4 cámaras IP como máximo.**

ii. Clic en la pestaña "Entrada de evento".

51

iii. Seleccione el tipo de grabación.

iv. Especifique el rango de tiempo cuando se guardarán los ficheros.

v. Especifique el número de minutos para reproducir el video grabado antes y después del evento.

52

vi. Búsqueda de eventos. Esta función se usa para buscar todos los eventos ocurridos en las cámaras IP. Usted puede referirse a los detalles de eventos para buscar los datos de grabación.

 Buscar todos: Buscar los eventos especificados ocurridos en todas las cámaras IP de un NVR dentro del rango de tiempo especificado.

 Buscar: Buscar los eventos especificados ocurridos en una cámara de IP dentro del rango de tiempo especificado.

vii. Los eventos se mostrarán. Clic en "Aceptar".
53
5. Cuando los ficheros se muestran, puede reproducir el video.
Pista: Los datos de grabación normales se muestran en blanco. Las grabaciones de alarma están resaltados en rojo en la lista de reproducción.
54
4.1.2 Reproduzca los ficheros de video desde su ordenador
1. Haga clic en "Añadir a la lista de reproducción" .
55
2. Busque y seleccione los archivos a reproducir.
3. Aparecerá la lista de reproducción. Haga clic en "Reproducir" para comenzar la reproducción.
56
4.1.3 Reproducción en cuatro vistas (Quad-view Playback)
La reproducción en cuatro vistas le permite buscar los videos grabados por los servidores NVR rápidamente. Usted puede ver el video de cuatro cámaras IP simultáneamente o seleccionar para dividir el video de una cámara IP en cuatro períodos de tiempo y reproducirlos en una ventana de cuatro vistas.
Divide el tiempo seleccionado igualmente en cuatro ventanas de reproducción
Seleccione solamente una cámara. Haga clic en "Entrada de texto" o "Entrada gráfica". Entre el criterio de búsqueda y escoja la opción "Dividir el período de tiempo seleccionado igualmente en todas las ventanas de reproducción para reproducir". Clic en "Aceptar".
57
Reproducir el video de cuatro cámaras IP
Seleccione cuatro cámaras IP para la búsqueda de video. Entre el criterio de búsqueda en "Entrada de texto" o "Entrada gráfica". Cuando los resultados de búsquedas se muestran, usted puede reproducir los ficheros de videos de las cuatro cámaras de IP simultáneamente.
58
4.1.4 Análisis inteligente de vídeos (IVA)
QNAP NVR soporta Análisis inteligente de vídeo para permitir a los usuarios buscar los ficheros de vídeo eficientemente. El tiempo y esfuerzos para búsquedas de vídeo se reducen significativamente.
El análisis de vídeo soporta las siguientes funciones:
 Detección de movimiento: Detecta movimiento de objetos en el vídeo.
 Objetos extraños: Detecta nuevos objetos en el vídeo.
 Objetos perdidos: Detecta objetos perdidos en el vídeo.
 Desenfoque: Detecta desenfoques de la cámara en el vídeo.
 Oclusión de la cámara: Detecta si la cámara IP está obstruida.
Para usar esta función, por favor siga estos pasos:
1. Vaya a la página de Reproducción del NVR. Agregue los ficheros a la lista de reproducción.
Nota: El análisis de vídeo inteligente soporta búsquedas de vídeo en un canal solamente.
59
2. Haga clic en la ventana de reproducción .
60
Nota:
 Cuando escoja la opción "Pausar al encontrar", la búsqueda de datos se detiene cuando se encuentra un fichero de vídeo que cumple con los criterios de búsqueda.
 Cuando activa "Resaltar la zona de detección", los objetos en movimiento se resaltarán en paréntesis rojos; los objetos extraños o perdidos se

resaltarán en amarillo; la oclusión y desenfoque de la cámara se resaltará en rojo transparente.
3. Seleccione el modo de detección: Detección de movimiento, objetos extraños, objetos perdidos, desenfoque u oclusión de cámara. Puede seleccionar múltiples opciones.
4. Ajuste la sensibilidad para detección de objetos.
5. Ajuste el intervalo de tiempo para objetos extraños y perdidos. Si un objeto extraño aparece o un objeto perdido desaparece durante un período de tiempo mayor al del intervalo, el sistema grabará un evento.
Nota: La barra de deslizamiento de intervalos aparece solamente cuando se selecciona "objetos extraños" u "objetos perdidos".
61
6. Definir zona de detección. Ponga el puntero del ratón sobre el borde de la zona roja y use el ratón para definir la zona de detección. Haga clic en "Seleccionar todo" y resalte toda el área para la detección.
62
7. Defina el tamaño del objeto para la detección. Puede usar el ratón para arrastrar la zona amarilla y resaltar el tamaño mínimo del objeto para la detección.
Nota: Después de activar esta opción, todos los objetos más pequeños que la zona amarilla se ignorarán para la detección.
63
8. Haga clic en "Buscar" para empezar la búsqueda del vídeo por medio de IVA. Los resultados se mostrarán.
64
Nota:
 Puede hacer doble clic en una entrada del cuadro de diálogo de resultados de búsqueda para reproducir el vídeo. El vídeo se reproducirá a partir de los 15 segundos antes del evento, hasta 15 segundos después del evento.
 También puede hacer clic derecho en una entrada del cuadro de diálogo de resultados de búsqueda para exportar el vídeo y guardarlo en su PC. El vídeo exportado se reproducirá a partir de los 15 segundos antes del evento, hasta 15 segundos después del evento.
65

4.2 Watermark digital

El VioStor NVR soporta la watermark digital para proteger los videos y fotos instantáneas y evitar la modificación no autorizada. Puede seleccionar agregar watermark digital en el video y foto instantánea exportados del reproductor VioStor.
Se agregará una señal digital permanente a los ficheros exportados los cuales se seleccionan para aplicarles marcas de agua digitales. La watermark no se puede eliminar y solamente se puede ver a través de un software especial.

4.2.1 Exportar ficheros con Watermark Digital

Para que el reproductor VioStor pueda usar la watermark digital, siga estos pasos:
1. Haga clic en "Reproducir" para activar el reproductor VioStor.
2. Clic en "Especificaciones" .
66
3. Seleccione agregar watermark digital al video o foto instantánea exportados.
4. Seleccione los ficheros de grabación (Consulte Capítulo 4).
5. Haga clic en para convertir los ficheros de video en el formato AVI y entre el nombre del fichero.
67
6. Haga clic en para empezar a reproducir y exportar los ficheros.
Nota: Cuando haga clic en nuevamente, el NVR dejará de exportar los ficheros y reanudará en el modo de reproducción.

68

4.2.2 Prueba Watermark

Para usar la prueba de Watermark, siga estos pasos:
Después de instalar el reproductor VioStor, se instalará la prueba de Watermark. Desde el menú inicio de Windows, seleccione "Todos los Programas" > "QNAP" > "Reproductor" para localizar "Watermark Proof" (Prueba Watermark).
Ejecute Prueba Watermark. Aparecerá el siguiente cuadro de diálogo.
69
Clic en para buscar los ficheros. Puede seleccionar más de un fichero a la vez. Haga clic en para empezar a revisar los ficheros. El programa de prueba de Watermark empezará a buscar los ficheros y mostrar el resultado de la prueba. Si usted revisa escoge la opción "Detener cuando se encuentre un error en la Watermark", el procedimiento de revisión se detendrá cuando un fichero falle. De lo contrario el programa revisará todos los ficheros que usted ha seleccionado. Si se modifica un fichero, el resultado de la prueba se mostrará como "Fallido".
70

4.3 Acceder a las Grabaciones a través del Servicio de Archivos de Red

VioStor proporciona los tres servicios de archivos de red siguientes para que los usuarios accedan a los archivos de vídeo grabados en VioStor.
 Entorno de Red de Windows (SMB/CIFS)
 Administrador de Archivos de Red (HTTP)
 Servidor FTP (FTP)

Nota:

1. Para acceder directamente a los archivos de vídeo usando estos protocolos, se le pedirá que introduzca un nombre y una clave de usuario con privilegios de administrador.
2. Para poder usar estos servicios, habilite los servicios de archivos en "Configuraciones de Red" > "Servicios de Archivos", en la página de administración del sistema.

71

4.3.1 Entorno de Red de Windows (SMB/CIFS)

Puede acceder a los archivos grabados a través del protocolo SMB/CIFS, que es lo que se usa habitualmente en el sistema Windows. Puede conectarse a la carpeta de grabación de dos formas:
 Haga clic en el botón "SMB" en la Interfaz de Reproducción de Red.
 En Windows XP, ejecute "\\VioStorIP\" desde el menú de Inicio. Por ejemplo, desde el botón Inicio y haciendo clic en Ejecutar. Luego introduzca y ejecute "\\192.168.1.201\" si la dirección IP de su VioStor es 192.168.1.201.

4.3.2 Administrador de Archivos de Web (HTTP)

Puede acceder a los archivos grabados desde el explorador web de la siguiente forma:
 Haga clic en el botón "Web" en la Interfaz de Reproducción de Red.

72

4.3.3 Servidor FTP (FTP)

Puede acceder a los archivos grabados mediante el protocolo FTP de dos formas:
 Haga clic en el botón "FTP" en la Interfaz de Reproducción de Red.
 En Internet Explorer de Windows, introduzca la siguiente dirección ftp://username:password@VioStorIP/ para conectarse. Por ejemplo, introduzca "ftp://admin:admin@172.17.26.154/" si la dirección IP de su VioStor es 172.17.26.154.

73

Capítulo 5. Administración del Sistema

Para Iniciar sesión en la página de configuración del sistema VioStor, por favor, inicie
sesión en la página de monitorización como administrador y haga clic en .
La página de Administración del Sistema se abrirá como se indica a continuación:
74
Si el sistema todavía no está configurado, la página de Configuración Rápida primero le abrirá una página para guiarle a través de los pasos a seguir en la configuración.
Si tiene dudas, haga clic en el botón de ayuda de la esquina superior derecha. Las funciones de los botones se describen a continuación:
Volver a la página de monitorización
Reproducir vídeo grabado
Ver la ayuda En Línea
Terminar Sesión
75

5.1 Configuración rápida

Por favor, siga las instrucciones de la página web para configurar Viostor.
Nota: Cualquier cambio en las configuraciones se hará efectivo sólo cuando se haya aplicado el último paso.
Paso 1. Introduzca nombre del servidor.
Paso 2. Introduzca una nueva contraseña o seleccione usar la contraseña original.
76
Paso 3. Introducir la fecha, hora y la zona horaria para este servidor.
Paso 4. Introducir la dirección IP, la máscara de sub-red y la puerta de enlace por defecto para este servidor.
77
Paso 5. Seleccione la configuración del disco para inicializar el volumen de disco para la primera configuración. Se borrarán todos los datos en la(s) unidad(es) de disco.
78
Paso 6. Inicializar las configuraciones de la cámara IP
Puede incluir hasta 8 cámaras en las configuraciones de cámara. Seleccione el modelo de la cámara, introduzca el nombre y la dirección IP de la cámara, así como el nombre y contraseña de usuario para acceder a ella. También puede habilitar o deshabilitar la grabación en cada cámara, probar la conexión a las cámaras y luego hacer clic en "Guardar" para aplicar los cambios.
Haga clic en "Buscar" para buscar las cámaras IP en la red local. Seleccione un canal para la cámara y haga clic en "Añadir" para añadir la cámara. Al usar la función de búsqueda, los campos del modelo de la cámara y la dirección IP se completan automáticamente. Haga clic en "Cerrar" para cerrar los resultados de la búsqueda.
79
Tras completar las configuraciones, haga clic en "Iniciar Instalación" para aplicar los cambios e inicializar el sistema.
¡Felicidades! La configuración rápida se ha completado y ya puede empezar a usar VioStor. Haga clic en "Iniciar Monitorización" para ver vídeo en directo desde las cámaras o haga clic en "Cerrar" para volver a la página de inicio de la administración
del sistema.
80

5.2 Configuración del sistema

Puede ajustar las configuraciones básicas del sistema, incluyendo el nombre del servidor, la fecha y hora, y ver las configuraciones del sistema.

5.2.1 Nombre de servidor

El nombre del servidor puede incluir hasta 14 caracteres, que pueden ser una

combinación de letras (A-Z o a-z), números (0-9) y guiones (-). El servidor no acepta nombres con espacios, puntos (.), ni compuestos sólo de números.
. ; : " < > * + = \ | ? , [ ] /
81

5.2.2 Fecha y hora

Configure la fecha, la hora y la zona horaria con arreglo a su ubicación actual. Si introduce estos valores incorrectamente, pueden surgir los siguientes problemas:
 Al reproducir archivos de vídeo grabados, la hora en pantalla será incorrecta.
 La hora que aparece en el registro de eventos del sistema puede ser incorrecta comparada con la hora real a la que se produjeron las acciones.

Sincronizar automáticamente con un Servidor de Tiempo de Internet

Puede habilitar o usar el servidor NTP (Network Time Protocol) especificado para actualizar automáticamente la fecha y la hora del sistema. Luego, introduzca el intervalo de tiempo para ajustar la hora.
Las cámaras de la red u otros servidores pueden usar este sistema como un servidor
NTP por defecto. Para asegurar que la fecha y hora de las cámaras de la red estén sincronizadas con este servidor, por favor, configure todas las cámaras de la red introduciendo la dirección IP de este servidor como su servidor NTP.
Nota: La primera vez que habilite el servidor NTP, la sincronización de tiempo puede tardar varios minutos antes de que la hora sea aju stada correctamente.
82

5.2.3 Ver configuración del sistema

En esta página puede ver toda la configuración actual del sistema, por ejemplo, el nombre del servidor y el grupo de trabajo.
83

5.3 Configuración de red

Puede ajustar las configuraciones de la WAN y la LAN, el servicio DDNS, el servicio de archivos, el control de acceso del anfitrión, la administración de protocolo y ver las configuraciones de red en esta sección.

5.3.1 Configuración TCP/IP

Puede seleccionar uno de los dos métodos siguientes para configurar TCP/IP del NVR.
 Obtener la dirección IP automáticamente a través del DHCP
Si su red soporta DHCP, el NVR usará el protocolo DHCP para recuperar automáticamente la dirección IP y la información relacionada.
 Use la dirección IP estática
Para usar la dirección IP fija para conexión de la red, entre la dirección IP fija, la máscara subnet y el gateway por defecto.
Servidor DNS Primario: Entre la dirección IP del servidor DNS primario que suministra el servicio DNS para el NVR de la red externa.
Servidor DNS Secundario: Entre la dirección IP del servidor DNS secundario que suministra el servicio DNS para el NVR de la red externa.
Nota: La especificación Jumbo Frame solamente es válida en entornos de redes de 1 Gigabit. Además, todos los equipos conectados a la red deben activar Jumbo Frame y usar el mismo valor MTU.
84
Si su sistema soporta2 puertos de LAN, puede seleccionar para reconexión de emergencia, equilibrio de carga o configuración autosostenible. Para usar estas funciones, verifique que los dos puertos de la LAN estén conectados a la red.
85

Interfaces para la Configuración de la Red

 Redundancia (Especificaciones por defecto para los modelos NVR de LAN dual)
Redundancia es la capacidad de conmutar el puerto de transferencia de la red a otro puerto redundante de forma automática cuando falle el principal debido

a un error de hardware o conexión para evitar la desconexión de la red. Cuando el puerto principal vuelve a funcionar, la transferencia de red retorna automáticamente a ese puerto.
86
 Balance de carga
El balance de carga permite dispersar los recursos de la red entre dos o más interfaces de red para optimizar la transferencia de la red y mejorar el rendimiento del sistema. La función de balance de carga controla sólo la dirección IP de la fuente y la dirección IP de los paquetes de la red. Sólo funciona con protocolos de capa 3 (IP, NCP IPX). Los protocolos de multidifusión / emisión y otros protocolos no encaminables, como NetBEUI, sólo se pueden transferir por medio del puerto de red principal.
87
 Autónomo
La opción autónoma le permite asignar diferentes configuraciones IP a cada puerto de red. Diferentes grupos de trabajo pueden acceder al VioStor en dos subredes diferentes. Sin embargo, cuando esta función esté habilitada, la opción En caso de fallo no funciona. Sólo puede habilitar el servidor DHCP para el puerto de red primario (LAN 1).
 Velocidad de Transferencia de la Red
Puede seleccionar negociación automática (por defecto), 1000 Mbps, ó 100 Mbps. Se recomienda usar la configuración por defecto, en la que el servidor determinará automáticamente la velocidad de la red.
 Obtener configuración de dirección IP automáticamente a través de DHCP
Si su red es compatible con DHCP (Protocolo de configuración dinámica de host), VioStor utilizará automáticamente el protocolo DHCP para obtener la dirección IP (Protocolo de Internet) e información relacionada.
 Usar dirección IP estática
Se utilizará la configuración de dirección IP definida por el usuario.
88
 Servidor DNS Primario
Introduzca la dirección IP del servidor DNS primario que proporciona servicio DNS al VioStor en la red externa.
 Servidor DNS Secundario
Introduzca la dirección IP del servidor DNS secundario que proporciona servicio DNS al VioStor en la red externa.
Habilitar el Servidor DHCP
Si ningún DHCP está disponible en la LAN donde el VioStor está ubicado, puede activar esta función para habilitar el VioStor como un servidor DHCP y asignar la dirección IP dinámica a los clientes DHCP en la LAN.
Puede configurar el rango de direcciones IP asignados por el servidor DHCP, además
del tiempo de concesión. El tiempo de concesión se refiere al tiempo que una dirección IP está concedido a los clientes por un servidor DHCP. Cuando el tiempo finalice, el cliente debe conseguir de nuevo una dirección IP.
Nota: Si hay un servidor DHCP existente en su LAN, no habilite esta función. Si lo hace, habrá una asignación de dirección IP y errores de acceso a la red.
89
5.3.2 Servicio DDNS (Dynamic Domain Name)
El servicio DDNs les permite a los usuarios conectarse a VioStor directamente a través del nombre de dominio. No es necesario saber la dirección IP real del servidor.
Para habilitar el servicio del DDNS, tiene que registrar una cuenta de DDNS con un proveedor de DDNS. Por favor, consulte Apéndice A.

VioStor actualmente es compatible con los servicios DDNS proporcionados por:
1. DynDNS (http://www.dyndns.org/)
2. update.ods.org
3. members.dhs.org
4. www.dyns.cx
5. www.3322.org
6. www.no-ip.com
7. ipcam.jp

90

5.3.3 Servicios de Archivos

Puede habilitar los servicios de archivo SMB/ CIFS, el Administrador de Archivos Web y el servicio FTP para acceder a los archivos de vídeo grabados. Estas configuraciones están habilitadas por defecto.

Si su VioStor está instalado detrás del router, podría permitir del puerto ftp en mapeado, de modo que los usuarios de la red externa puedan tener acceso a VioStor vía FTP (refiera por favor a Apéndice B).

Rango de puertos FTP pasivo

Puede utilizar el rango de puertos predeterminado (55536-56559) o definir un rango de puertos superior a 1023. Si utiliza esta función, asegúrese de haber abierto el rango de puertos configurado en su router o firewall.

Responda con la dirección IP externa a una petición de conexión FTP pasiva

Puede habilitar esta función cuando se esté usando una conexión FTP pasiva y el VioStor esté configurado bajo un enrutador, si el ordenador remoto no puede conectarse al VioStor a través de la WAN. Habilitando esta función, el servicio FTP contesta a la IP especificada manualmente o detecta automáticamente la dirección IP externa de forma que el ordenador remoto pueda conectarse con éxito al VioStor.

91

5.3.4 Control de Acceso al Anfitrión

Especifica las conexiones permitidas y denegadas de acceso al servidor. Elija una de las siguientes opciones para restringir el acceso al servidor desde una red o una dirección IP (anfitrión):

1. Permitir todas las conexiones (Configuración por defecto)

Permite conexiones desde todos los anfitriones al servidor.

2. Sólo permitir conexiones de la lista

Permite solamente conexiones de los anfitriones especificados en la lista.

Nota: Cuando esta función está habilitada, sólo puede usar para conectar o buscar el servidor el PC cuya dirección IP está incluida en la lista de conexiones. Una dirección IP no incluida en la lista no será capaz de detectar el VioStor no incluido en la lista de conexiones permitidas.

3. Denegar conexiones de la lista

Deniega conexiones de los anfitriones especificados en la lista.

Nota: Asegúrese de que su PC esté incluido en la lista de anfitriones permitidos para poder conectar al servidor. Si no es así, el servidor se desconectará de su PC cuando se apliquen las nuevas configuraciones.

92

5.3.5 Administración de puerto

Para asignar un puerto específico de acceso VioStor a través del navegador web, active la opción "Especifique el número de puerto HTTP" e introduzca el número de puerto. La configuración predeterminada es 80.

RTP (Protocolo de transferencia en tiempo real) es un formato de paquetes estándar
para la entrega de datos de sonido y vídeo en tiempo real de cámaras de red a través de Internet. La transferencia de datos en tiempo real se supervisa y controla

a través de RTP (también RTCP). La configuración predeterminada es 6100-6299. Si
sus cámaras de red utilizan puertos RTP diferentes, active la opción "Especifique el rango del puerto RTP" e introduzca los números de los puertos.
Nota: asegúrese de haber abierto los puertos configurados en su router o firewall para garantizar la supervisión y grabación normal.
93

5.3.6 Ver configuración de red

En esta página puede ver toda la configuración de red actual, la configuración de servicios y la configuración de servicios VioStor.
94

5.4 Configuración del dispositivo

Puede configurar el disco SATA, herramienta de administración RAID, el disco USB y
las configuraciones SAI en esta sección.

5.4.1 Disco SATA

Esta página muestra el modelo, tamaño y estado actual del disco SATA en el VioStor.
Puede formatear y comprobar el disco, y buscar bloques defectuosos en el disco. Al formatear el disco SATA, el VioStor creará las siguientes carpetas de recursos compartidos por defecto.
 record_nvr: Es la carpeta para la grabación los archivos de grabación normales
 record_nvr_alarm: Es la carpeta para la grabación de alarmas

Configuración de Disco	Aplica a Modelos de NVR
Volumen de disco único	Todos los modelos
RAID 1, JBOD *(*just a bunch of disks - sólo un grupo de discos)	Modelos de 2 bahías o más
RAID 5, RAID 6, RAID 5+reposición en caliente	Modelos de 4 bahías o más
RAID 6+reposición en caliente	Modelos de 5 bahías o más

Puede crear los siguientes volúmenes de disco según sus necesidades.
95

Volumen de disco único

Cada disco duro se usa como un disco autónomo. Si un disco se daña, todos los datos se perderán.

JBOD (Solo un conjunto de discos)

JBOD es una colección de discos duros que no ofrece ninguna protección RAID. Los datos se graban en los discos físicos en forma secuencial. La capacidad total de almacenamiento es igual a la suma de la capacidad de cada disco miembro.

División de volumen de discos RAID 0

RAID 0 (división de discos) combina 2 o más discos duros en un volumen mayor. Los datos se graban en los discos duros sin ninguna información de paridad y sin redundancia. La capacidad del disco es igual al número de discos duros en el arreglo multiplicado por el tamaño del disco más pequeño.

Volumen de discos espejos RAID 1
RAID 1 duplica los datos entre dos discos duros para suministrar copia espejo del disco. Para crear un arreglo RAID 1, se necesitan como mínimo 2 discos duros.
96
Volumen de disco RAID 5
Los datos se dividen entre todos los discos de un arreglo RAID 5. La información de paridad se distribuye y almacena en cada disco. Si un disco falla, el arreglo entra en el modo degradado. Después de instalar un nuevo disco para reemplazar al dañado, los datos se pueden recuperar desde cualquiera de los discos miembros los cuales contienen la información de paridad.
Para crear un volumen de disco RAID 5, se necesitan como mínimo 3 discos duros.
La capacidad de almacenamiento de un arreglo RAID 5 es igual a (N-1). N es el total de discos miembros del arreglo.
Volumen de disco RAID 6
Los datos se dividen entre todos los discos de un arreglo RAID 6. RAID 6 difiere de RAID 5 en que un segundo grupo de información de paridad se almacena en los discos miembros del arreglo. Acepta fallas en dos discos miembros.
Para crear un volumen de disco RAID 6, se necesitan como mínimo 4 discos duros. La capacidad de almacenamiento de un arreglo RAID 6 es igual a (N-2). N es el total de discos miembros del arreglo.
97
5.4.2 Herramienta de administración RAID
* Esta función solamente aplica a VS-101, VS-201, NVR-104.
Esta función permite la expansión de capacidad, la migración de configuración RAID o la configuración de unidad de repuesto preservando los datos originales.
 Expandir capacidad
Esta función permite expandir la capacidad de la unidad reemplazando las unidades de la configuración una por una. Esta opción es compatible con las siguientes configuraciones de unidades:
- Expansión de RAID 1
- Expansión de RAID 5
- Expansión de RAID 6
 Añadir disco duro
Esta función permite añadir nuevos miembros de unidad a una configuración de unidades. Esta opción es compatible con las siguientes configuraciones de unidades:

- Expansión de RAID 5

 Migrar

Esta función permite migrar una configuración de disco duro a una configuración RAID diferente. Esta opción es compatible con las siguientes configuraciones de unidades:

- Migrar una unidad a RAID 1, 5, o 6
- Migrar de RAID 1 a RAID 5 o 6
- Migrar de RAID 5 a RAID 6

98

 Configurar disco de repuesto

Esta función permite añadir o eliminar unidades de repuesto RAID 5. Las opciones disponibles son:

- Añadir unidad de repuesto en RAID 5
- Extraer unidad de repuesto en RAID 5

Para conocer los detalles de funcionamiento, haga clic en el botón "Comentario" situado en la interfaz de administración para ver las instrucciones de uso detalladas.

99

5.4.3 Disco USB

El VioStor es compatible con el uso de discos USB para el almacenamiento de copias
de seguridad. Conecte el dispositivo USB al puerto USB del servidor. Cuando se detecta el dispositivo con éxito, los detalles aparecerán en esta página.

* VS-101, VS-201, NVR-104 no es compatible con FAT32 y NTFS.

100

5.4.4 UPS (SAI)

Si tiene instalado un SAI, puede habilitar el soporte SAI. Si la corriente CA no irregular, el sistema se apagará de acuerdo con las configuraciones. Si no ha finalizado el límite de tiempo y la alimentación del SAI no es suficiente, el sistema se
apagará inmediatamente para proteger al servidor.

*Se recomienda conectar el SAI a uno de los puertos USB de la parte posterior del servidor.

 Habilitar Soporte UPS

Marque esta opción para habilitar el soporte SAI. Puede configurar el tiempo tras el cual el sistema se apagará si el estado de la alimentación CA es irregular. En general, el SAI puede suministrar energía durante 5-10 minutos cuando haya un corte en el suministro CA, dependiendo de la carga máxima y del número de dispositivos conectados al SAI.

 Modelo UPS

Seleccione el modelo SAI en la lista. Si su SAI no aparece en la lista, por favor, póngase en contacto con el distribuidor o con el soporte técnico de QNAP.

 Dirección IP del UPS

Si selecciona "APC UPS with SNMP Management" (SAI APC con Administración a través de SNMP), por favor, introduzca la dirección IP del SAI.

Nota: Se recomienda usar la Tarjeta de Administración de Red APC Smart-SAI 700+APC.

101

5.5 Administración de usuarios

El NVR es compatible con administración de derechos de acceso seguro de usuarios. Un usuario se puede definir como administrador, gestor del sistema o como usuario normal y pueden tener diferentes derechos como monitorización, reproducción y administración del sistema.

Nota: El servidor admite hasta 32 usuarios (incluyendo el usuario por defecto del sistema).

El NVR permite 3 tipos de usuarios:
1. administrator (Administrador)
Las cuentas del administrador por defecto del sistema son "admin" y "supervisor" (contraseña por defecto: **admin**). Las dos tienen derechos de administración del sistema, monitorización y reproducción. Los administradores no se pueden eliminar. Ellos tienen los derechos para crear y eliminar nuevos administradores, gestores del sistema y usuarios normales así como también cambiar sus contraseñas. Los otros "administradores" recientemente creados, tiene los derechos de administración del sistema, monitorización y reproducción, sin embargo, algunos derechos son diferentes a los de "admin" y "supervisor". Por favor consulte el capítulo 5.5.4 para obtener más detalles.
2. system manager (Gestor del Sistema)
La cuenta por defecto del gestor del sistema es "sysmgr" (contraseña por defecto: **admin**). Esta cuenta tiene el derecho de administración del sistema y no se puede eliminar. "sysmgr" puede crear y eliminar otras cuentas de gestores del sistema y usuarios normales, así como también asignar a ellos derechos de monitorización, reproducción y administración. Los gestores del sistema recientemente creados también tendrán derechos de administración, sin embargo estos derechos son diferentes de los de "sysmgr". Por favor consulte el capítulo 5.5.4 para obtener más detalles.

3. user (Usuario normal)
Los usuarios normales solamente tienen los derechos de monitorización y reproducción de vídeo. Ellos no tienen derechos de administración. Por favor consulte el capítulo 5.5.4 para obtener más detalles.

5.5.1 Crear un Usuario

 Nombre de usuario
El nombre de usuario no puede tener más de 32 caracteres de longitud. No distingue entre mayúsculas y minúsculas y puede contener caracteres de doble byte (como los de los idiomas chino, japonés y coreano), pero no puede contener ninguno de los siguientes caracteres:
" / \ [ ] : ; | = , + * ? < > ` '
 Contraseña
La contraseña no puede tener más de 16 caracteres de longitud. Por cuestiones de seguridad, la contraseña debe tener al menos 6 caracteres. Intente evitar usar códigos que sean fácilmente descifrables.
 Seleccionar tipo de usuario
Permite definir al usuario como administrador, gestor del sistema o usuario normal.
 Control de acceso a las cámaras
Permite asignar al usuario, derechos de monitorización (vídeo/ audio), reproducción y control PTZ.
Nota: Por favor consulte el capítulo 5.5.4 para obtener más información sobre los derechos de acceso de los usuarios.

5.5.2 Editar un Usuario

Seleccione un usuario de la lista y haga clic en "Editar". Puede cambiar la contraseña,
asignar la administración del sistema y el control de acceso a las cámaras. Sin embargo, no se puede cambiar el nombre del usuario.

5.5.3 Eliminar un Usuario

Para eliminar un usuario, seleccione un usuario de la lista y haga clic en "Eliminar". Haga clic en "Aceptar" para confirmar.

Nota: Observe que el administrador (admin, supervisor, sysmgr) del sistema no puede eliminarse.

5.5.4 Comparación de los derechos de acceso de los usuarios

El VioStor NVR permite tres tipos de usuarios, los cuales son: administrador del sistema, gestor del sistema y usuario normal. Los administradores del sistema por defecto son "admin" y "supervisor", quienes no pueden cambiarse entre sí la contraseña, el tipo de usuario y derechos de acceso de control a las cámaras IP.

Nota 1: El usuario puede eliminar su cuenta

Nota 2: El usuario puede cambiar su contraseña

Derechos	**Administrador admin**	**Gestor del Sistema supervisor**	**Otros administradores sysmgr**	**Otros gestores del sistema**	**Usuario**
1. Crear nueva cuenta "admin"	Por defecto	Por defecto	No	No	No
2. Crear nueva cuenta "supervisor"	Por defecto	Por defecto	No	No	No
3. Crear nuevas cuentas de administrador	Sí	Sí	Sí	No	No
4. Eliminar otras cuentas de administradores	Sí	Sí	No (Nota 1)	No	No
5. Cambiar la contraseña de "admin"	Sí	No	No	No	No
6. Cambiar la contraseña de "supervisor"	No	Sí	No	No	No
7. Cambiar la contraseña de otros administradores	Sí	Sí	No (Nota 2)	No	No
8. Cambiar el tipo de usuario de admin	Por defecto	No	No	No	No
9. Cambiar el tipo de usuario de supervisor	No	Por defecto	No	No	No

10. Cambiar el tipo de usuario de otros administradores	Sí	Sí	Por defecto	No	No
11. Cambiar el control de acceso a las cámaras de admin	Sí	No	No	No	No
12. Cambiar el control de acceso a las cámaras					

de supervisor
No Sí No No No No
13. Cambiar el control de
acceso a las cámaras
de otros
administradores
No No Sí No No No
14. Crear sysmgr No No No Por defecto No No
15. Crear otras cuentas
de gestores del
sistema
Sí Sí Sí Sí Sí No
16. Eliminar sysmgr No No No No No No
17. Eliminar otras
cuentas de gestores
del sistema
Sí Sí Sí Sí No (Nota 1) No
18. Cambiar la
contraseña de sysmgr
Sí Sí Sí No (Nota 2) No No
19. Cambiar la
contraseña de otros
gestores del sistema
Sí Sí Sí Sí No (Note 2) No
20. Cambiar el tipo de
usuario de sysmgr
No No No Por defecto No No
21. Cambiar el tipo de
usuario de otros
gestores del sistema
Sí Sí Sí Sí No No
22. Cambiar el control de
acceso a las cámaras
de sysmgr
No No No No No No
23. Cambiar el control de
acceso a las cámaras
de otros gestores del
No No No No No No

sistema
24. Crear nuevos
usuarios
Sí Sí Sí Sí Sí No
25. Eliminar usuarios Sí Sí Sí Sí Sí No
26. Cambiar la
contraseña del
usuario
Sí Sí Sí Sí No No
27. Cambiar el tipo de
usuario de los
usuarios normales
Sí Sí Sí Sí No No
28. Cambiar el control de
acceso a las cámaras
de los usuarios
normales
Sí Sí Sí Sí Sí No
29. Administración del
Sistema
Sí Sí Sí Sí Sí No
30.
Monitorización Sí Sí Sí No No
Por
defecto
31.
Reproducción Sí Sí Sí No No
Por

defecto
32. Abrir la contraseña de
cifrado de datos
Sí Sí No No No No
108

5.6 Configuraciones de la Cámara

Puede configurar las configuraciones, la grabación, la programación, la alarma y las configuraciones avanzadas de la cámara.

5.6.1 Configuración de Cámara

Por favor, siga los pasos a continuación para configurar las cámaras de la red.
1. Seleccione un número de cámara.
2. Seleccione la marca de la cámara.
3. Seleccione un modelo de cámara.
4. Introduzca el nombre de la cámara.
5. Introduzca la dirección IP o el nombre de dominio de la cámara.
6. Introduzca el nombre y la contraseña del usuario para iniciar la sesión de la cámara.
7. Habilitar la grabación en esta cámara.
8. Haga clic en "Aplicar" para guardar las configuraciones.
109

Nota:

1. No todas las configuraciones tendrán efecto hasta que haga clic en el botón "Aplicar". Al aplicar los cambios, la grabación parará durante un rato (máximo 1 minuto) y luego se reiniciará.
2. Haga clic en "Buscar" para buscar las cámaras IP en la red local. Seleccione un canal para la cámara y haga clic en "Añadir" para añadir la cámara. Al usar la función de búsqueda, los campos del modelo de la cámara y la dirección IP se completan automáticamente. Haga clic en "Cerrar" para cerrar los resultados de la búsqueda.
110

Agregue soporte de cámaras genéricas IP por medio del comando CGI

QNAP NVR suministra una interfase para que los usuarios puedan entrar comandos JPEG CGI de las cámaras IP, con el fin de recibir la información de flujo de audio y vídeos desde las cámaras IP y así monitorizar, grabar y reproducir videos de las cámaras IP del NVR. Esta función mejora significativamente la compatibilidad y expansibilidad del NVR.

Por favor siga estos pasos para configurar su cámara IP.
1. Seleccione el número de la cámara IP.
2. Seleccione "Modelo Genérico" para la marca de la cámara.
3. Seleccione "JPEG Genérica" para el modelo de la cámara.
4. Entre la ruta del CGI de la cámara IP en el campo "HTTP URL".
5. Entre el nombre o dirección IP de la cámara.
6. Entre el nombre del usuario y la contraseña de la cámara IP.
7. Seleccione activar grabación o no.
8. Haga clic en "Aplicar" para guardar las especificaciones.
111

Nota: QNAP NVR solamente soporta la interfase de comandos JPEG CGI, pero esto no garantiza la compatibilidad con todas las marcas de cámaras IP.
112

5.6.2 Configuraciones de Grabación

Seleccione una cámara en la lista y configure la resolución de la grabación, la velocidad de imagen y la calidad. También puede habilitar la grabación manual. Haga clic en "Aplicar" para guardar las configuraciones.
1. **Compresión de Vídeo:** Escoja el formato de compresión de vídeo para grabación.
2. **Resolución:** Selecciona la resolución de la grabación.

3. **Frecuencia de Imagen:** Ajusta la velocidad de imagen de la grabación. Observe que la velocidad de imagen de la cámara puede resultar afectada por el tráfico de la red.
4. **Calidad:** Selecciona la calidad de imagen de la grabación. Una calidad mayor consumirá más espacio de disco.
5. **(Opción) Grabación de audio:** Para habilitar la grabación de audio, haga clic en Habilitar la grabación de audio en esta cámara.
6. **Espacio de almacenamiento estimado para grabaciones:** La cantidad de espacio de almacenamiento estimado para grabaciones es sólo una referencia. El espacio consumido real depende del entorno de red y del rendimiento de la

cámara.
7. **Habilitar grabación manual:** Para permitir la activación y desactivación de la función de grabación manual en la página de monitorización, habilite esta opción.

Nota:

 Iniciar o parar la grabación manual no influirá en una grabación programada o de alarma. Son procesos independientes.

 No todas las configuraciones tendrán efecto hasta que haga clic en el botón "Aplicar". Al aplicar los cambios, la grabación parará durante un rato (máximo 1 minuto) y luego se reiniciará.

5.6.3 Configuraciones de Programación

Puede seleccionar grabación continua o grabación programada. La grabación continua está configurada por defecto. Para configurar una programación de grabación, por favor, seleccione el número de cámara de la lista. Luego seleccione la
fecha y hora y haga clic en "Añadir". Haga clic en "Aplicar" para añadir las configuraciones de la cámara o en "Aplicar a todas las cámaras" para configurar todas las cámaras. Para eliminar una programación, haga clic en "Eliminar" en la lista de programación.

Nota:

1. Puede incluir hasta 15 programaciones.
2. No todas las configuraciones tendrán efecto hasta que haga clic en el botón "Aplicar". Al aplicar los cambios, la grabación parará durante un rato (máximo 1 minuto) y luego se reiniciará.

5.6.4 Configuraciones de Alarma

El NVR suministra el "Modo tradicional" y el "Modo avanzado" para la configuración de la alarma. Seleccione "Modo tradicional" para usar las especificaciones estándares de la alarma como respuesta a eventos de alarma. Para usar la administración avanzada de eventos, seleccione "Modo avanzado".

Nota: VS-201/ VS-101/ NVR-104 no permite el modo avanzado en "Configuración de Alarma".

Modo tradicional

Seleccione un canal (Cámara IP / servidor de vídeo) de la lista y configure la alarma.
La grabación del vídeo se activará cuando la entrada de alarma del canal seleccionado se active o se detecte un objeto en movimiento.
Cuando active la opción "Activar la grabación de alarma solamente en el programa seleccionado", la grabación de alarma se activará únicamente cuando la entrada de alarma se active o se detecte un objeto en movimiento dentro del programa.
Puede probar las especificaciones haciendo clic en "Probar". Haga clic en "Aplicar" para aplicar las especificaciones al canal seleccionado. Para aplicar las mismas especificaciones a todos los canales de la lista, haga clic en "Aplicar a todas las

cámaras”.
116
Nota:
• Todas las especificaciones tendrán efecto después de hacer clic en “Aplicar”. Cuando los cambios se están aplicando, el proceso de grabación actual se detendrá un momento (máximo 1 minuto) y luego reiniciará.
• Para evitar que el firewall haga bloqueos, las cámaras IP o los servidores de vídeo configurados para la grabación de alarmas, deben estar ubicados en la misma subnet del NVR.
• Para cambiar desde el modo tradicional o el modo avanzado, seleccione “Modo avanzado” y luego haga clic en “Ir a la página de especificaciones”.
117
Modo avanzado:
El modo avanzado consta de las secciones de eventos y acciones. Puede definir la acción para cada evento activado en las cámaras IP o los servidores de vídeo conectados al NVR.
Para configurar la administración avanzada de eventos por el “Modo avanzado”, seleccione un tipo de evento de la lista de canales izquierda y configure las acciones a realizar desde la parte derecha.
Nota:
• Haga clic en "Aplicar" para que las especificaciones tengan efecto o "Salir" para salir de la página de especificaciones. Si el "Modo Avanzado" aún está seleccionado en la página de "Especificaciones de Alarma", las especificaciones avanzadas se aplicarán después de reiniciar el NVR, incluso si ha seleccionado salir de la página de especificaciones. Las especificaciones se cancelarán si selecciona usar el “Modo tradicional” después de salir del “Modo avanzado”.
• Para evitar que el firewall haga bloqueos, las cámaras IP o los servidores de vídeo configurados para la grabación de alarmas, deben estar ubicados en la misma subnet del NVR.
• Para cambiar del modo avanzado al modo tradicional, seleccione “Modo tradicional” y luego haga clic en “Aplicar”.
118
 Eventos:
Los eventos que el NVR permite, están clasificados como eventos de cámaras (detección de movimiento, entrada de alarma, desconexión de cámara), eventos del NVR (error en la grabación) eventos externos (eventos definidos por el usuario).
Nota: Los eventos de cámaras disponibles varían de acuerdo a las funciones compatibles con las cámaras IP y los servidores de vídeo.
Botones de la lista de eventos
Agrega un evento externo. Este botón no se aplica a los eventos de cámaras ni a los eventos del NVR.
Edita un evento. Este botón no se puede usar para editar la desconexión de cámaras.
Elimina un evento externo. Este botón no se aplica a los eventos de cámaras ni a los eventos del NVR.
119
El NVR es compatible con los siguientes tipos de eventos. Antes de definir las especificaciones de acciones, seleccione los eventos a manejar y establezca las especificaciones.
(1) Entrada de Alarma
Esta opción le permite al NVR activar una acción, cuando se activa la entrada de alarma de una cámara IP o de un servidor de vídeo. Seleccione “Evento de cámara” de la “Lista de eventos”. Busque el canal compatible con la entrada de alarma y haga clic en “Entrada de alarma”. Luego, haga clic en el botón

editar ( ), active esta opción, configure las especificaciones y haga clic en "Aplicar". También puede establecer el programa para definir el período activo de las especificaciones de alarma. Después de eso, defina las especificaciones de acción en la parte derecha (discutido en secciones posteriores).
120
(2) Detección de movimiento
Esta opción le permite al NVR activar una acción, cuando la cámara IP o el servidor de vídeo detectan un objeto en movimiento. Seleccione "Evento de cámara" desde la "Lista de eventos". Busque el canal y haga clic en "Detección de movimiento". Luego, haga clic en el botón editar ( ), active esta opción, configure las especificaciones y haga clic en "Aplicar". También puede establecer el programa para definir el período activo de las especificaciones de alarma. Después de eso, defina las especificaciones de acción en la parte derecha (discutido en secciones posteriores).
(3) Evento de Alarma
Las especificaciones de entrada de alarma y detección de movimiento de algunas cámaras IP o servidores de vídeo se pueden combinar y se conocen como "Evento de Alarma" de la lista de eventos. Puede editar las especificaciones del evento y definir las especificaciones de acción en la parte derecha (discutido en secciones posteriores).
121
(4) Error en la conexión
Esta opción le permite al NVR activar una acción cuando la cámara IP o el servidor de vídeo se desconecta. Seleccione "Evento de cámara" de la "Lista de eventos". Busque el canal y haga clic en "Error en la conexión". Después de eso, defina las especificaciones de acción en la parte derecha (discutido en secciones posteriores).
(5) Error en la grabación (Evento NVR)
Esta opción le permite al NVR activar una acción, cuando la grabación de vídeo de la cámara IP o el servidor de vídeo falla, debido a la presencia de sectores defectuosos en el disco duro, falla en el sistema de archivos u otras razones. Seleccione "Evento de NVR" de la "Lista de eventos". Haga clic en "Error en la grabación". Después de eso, defina las especificaciones de la acción en la parte derecha (discutido en secciones posteriores).
122
(6) Eventos externos (eventos definidos por el usuario)
Para crear un evento definido por el usuario en el NVR, seleccione "Evento definido por el usuario" en "Eventos externos" de la "Lista de eventos". Luego haga clic en el botón +. Escriba el nombre del evento, por ejemplo, "puerta". Después de crear el evento, haga clic en el nombre del evento y defina las especificaciones de acciones de la parte derecha (discutido en secciones posteriores). Después de configuración las especificaciones de acciones, puede usar el comando CGI (incluyendo el nombre del evento auto-definido) en el navegador Web (Explorador de Internet) para activar la acción en cualquier momento. El formato del comando CGI es: http://*NVRIP*/logical_input.cgi?name=*nombre-de-evento*. Por ejemplo, http://10.8.12.12:80/logical_input.cgi?name=puerta
123
Especificaciones del programa de eventos:
Cuando esté editando un evento (no se incluye la desconexión de cámaras, los eventos de NVR ni los eventos externos), puede hacer clic en "Definir programa" para definir el momento en el cual se activarán las especificaciones de alarma. Para crear un nuevo programa, seleccione "Nuevo" y escriba el nombre del programa. El nombre del programa acepta 25 caracteres como máximo (se

permiten caracteres de doble byte, espacios y símbolos). Seleccione el día y la hora en los cuales se activarán las especificaciones de alarma. Haga clic en + para agregar un programa o en – para eliminar un programa. Se pueden definir hasta 6 especificaciones para cada programa.
Las especificaciones se mostrarán en una tabla gráfica. Haga clic en "Aplicar" para guardar las especificaciones. Para usar el mismo programa para todos los eventos, haga clic en "Aplicar a todos los eventos". También puede seleccionar el programa por defecto o uno creado anteriormente desde la lista. Las especificaciones de alarma por defecto están activas durante todo el día, todos los días.
124
 Acciones:
El NVR permite diferentes acciones las cuales se pueden activar cuando los eventos seleccionados se activan en las cámaras IP o en los servidores de vídeo. Las acciones incluyen grabación de vídeo, alertas de correo-e, alertas SMS, timbre, control de cámaras PTZ, salida de alarma y salida lógica.
Botones de la lista de acciones
Agregar una acción:
Después de configurar un evento en la izquierda, haga clic en "Agregar" para crear una acción como respuesta al evento.
Haga clic en "Aplicar" para guardar las especificaciones.
Editar una acción:
Seleccione un evento de la parte izquierda. Se mostrarán todas las acciones definidas para este evento. Seleccione la casilla de verificación al frente del nombre que desea editar. Luego haga clic en este botón sobre la columna "Acción" para editar las especificaciones de la acción.
Eliminación de una acción:
Seleccione un evento de la parte izquierda. Se mostrarán todas las acciones definidas para este evento. Seleccione la casilla de verificación al frente del nombre que desea eliminar y haga clic en "Eliminar". Puede seleccionar eliminar varias acciones.
125
Nota: Verifique que haya activado la acción en las especificaciones de evento, de lo contrario no se ejecutará. Por ejemplo:
126
(1) Grabación:
Seleccione los canales (Cámaras IP o servidores de vídeo) los cuales iniciarán la grabación cuando se presente un evento. También puede seleccionar las siguientes opciones:
(i) Entre el tiempo (en segundos) en que la grabación se ejecutará después de activar el evento.
(ii) Inicia la grabación cuando el evento empieza y detiene la grabación cuando el evento termina.
La opción (ii) solo se aplica a la duración de los eventos. Un evento de duración es aquel que tiene tiempo de inicio y terminación y su duración es durante un período de tiempo. No incluye los eventos relacionados con el cambio de estado, tales como la desconexión de cámaras o error en la grabación del NVR.
Si el evento de duración activa la acción y las dos especificaciones (i, ii) están activas, el NVR solo ejecutará la segunda especificación (ii).
Haga clic en "seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
127
(2) Control de cámaras
Esta opción le permite configurar la cámara PTZ para ajustarla a la posición

predefinida para monitorización o para que actúe de acuerdo con la URL HTTP escrita cuando se activa un evento. Puede seleccionar una posición predefinida desde el menú desplegable o escribir la URL HTTP.
Haga clic en "Seleccionar de la lista" para seleccionar la especificación de acción que se haya configurado anteriormente.
Nota: Los nombres predefinidos aparecerán solamente después de que usted haya configurado las especificaciones de posición de las cámaras PTZ.
128
(3) Salida de alarma
Seleccione para activar el dispositivo de alarma conectado a la cámara IP cuando se activa un evento. También puede seleccionar las siguientes opciones:
(i) Escriba el total de segundos en el cual el dispositivo de alarma estará activo cuando se active un evento.
(ii) Activa el dispositivo de alarma cuando el evento inicia y detiene el dispositivo de alarma cuando el evento termina.
La opción (ii) solo se aplica a la duración de los eventos. Un evento de duración es aquel que tiene tiempo de inicio y terminación y su duración es durante un período de tiempo. No incluye los eventos relacionados con el cambio de estado, tales como la desconexión de cámaras o error en la grabación del NVR.
Haga clic en "seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
129
(4) Correo-e
Para que el administrador del sistema pueda recibir alertas instantáneas por correo-e, cuando se active un evento, escriba las especificaciones SMTP. Se pueden escribir varias direcciones de correo-e para el destinatario. también puede adjuntar fotos instantáneas para varios canales (cámaras IP / servidores de vídeo) disponibles en el NVR.
Haga clic en "Seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
130
(5) SMS
Para que el administrador del sistema pueda recibir alertas instantáneas SMS, cuando se active un evento, escriba el servidor SMS. El proveedor de servicios SMS por defecto es Clickatell. Para agregar otros proveedores de servicio SMS, haga clic en "Agregar" y escriba el nombre del proveedor y el texto de la plantilla URL.
Haga clic en "Seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
Nota: Si el texto de la plantilla URL ingresado no cumple con las normas del proveedor de servicios SMS, no podrá recibir SMS en forma apropiada.
131
(6) Timbre
Active el timbre cuando se activa un evento. También puede seleccionar las siguientes opciones:
(i) Entre el tiempo (en segundos) en que el timbre sonará cuando se activa el evento.
(ii) Ejecute el timbre cuando el evento inicie y detenga el timbre cuando el evento termina.
La opción (ii) solo se aplica a la duración de los eventos. Un evento de duración es aquel que tiene tiempo de inicio y terminación y su duración es durante un período de tiempo. No incluye los eventos relacionados con el cambio de estado, tales como la desconexión de cámaras o error en la

grabación del NVR.
Si el evento de duración activa la acción y las dos especificaciones (i, ii) están activas, el NVR solo ejecutará la segunda especificación (ii).
Haga clic en "seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
132

(7) Acción definida por el usuario

Puede ingresar una acción definida por el usuario cuando un evento se activa. Escriba el nombre de usuario y contraseña, dirección IP, puerto y la dirección URL HTTP de los otros dispositivos de supervisión. Usted puede manejar los dispositivos tales como dispositivos de protección contra incendios, controladores de energía y control de aire acondicionado.
Haga clic en "Seleccionar de la lista" para seleccionar una especificación de acción que se haya configurado anteriormente.
133

5.6.5 Configuraciones Avanzadas

Puede ajustar las configuraciones de grabación avanzadas en esta sección.
 Longitud máxima de cada archivo de grabación: Configura la longitud máxima de cada archivo de grabación (máximo 15 minutos).
 Cuando el almacenamiento disponible sea menor de … GB: Seleccione la acción a tomar cuando el almacenamiento disponible sea menor que al nivel preestablecido. Puede seleccionar sobrescribir las grabaciones más antiguas o parar las nuevas grabaciones.
 Guardar las grabaciones de alarma durante al menos … día(s): Especifica el número de días que se guardarán las grabaciones de alarma. Esto evitará que se sobrescriban archivos de grabación cuando el espacio de almacenamiento libre sea insuficiente.
 Eliminar las grabaciones tras … día(s): Introduzca el número de días naturales que desee que VioStor guarde los archivos de grabación.
Por favor, asegúrese de que su capacidad de almacenamiento sea suficiente para guardar los datos de los días naturales que haya configurado. Cuando los datos de grabación alcancen la fecha de expiración, los archivos de vídeo expirados serán eliminados. Por ejemplo, si ha configurado que los datos de grabación sean eliminados tras 7 días naturales, el 8º día serán eliminados los archivos guardados el primer día, de forma que VioStor pueda comenzar a guardar los datos del 8º día.
134

Grabaciones Pre/Post Alarma

 Comenzar la grabación de vídeo … segundo(s) antes de que ocurra el evento: Introduzca el número de segundos en el que comenzar la grabación antes de que ocurra el evento.
 Parar la grabación de vídeo … segundo(s) después de finalizar el evento: Introduzca el número de segundos en el que parar la grabación después de que finalice el evento.
El número máximo de segundos para las configuraciones anteriores de de 300, es decir, 5 minutos.
Nota: No todas las configuraciones tendrán efecto hasta que haga clic en el botón "Aplicar". Al aplicar los cambios, la grabación parará durante un rato (máximo 1 minuto) y luego se reiniciará.
135

5.7 Herramientas del sistema

Las Herramientas del Sistema le permiten optimizar el mantenimiento y administración del sistema. Puede configurar la notificación de alertas, reiniciar o apagar el servidor, configurar las configuraciones del hardware, hacer una copia de seguridad/restaurar/reajustar las configuraciones, configurar el mapa electrónico y

realizar una prueba de ping.

5.7.1 Notificación de alertas

Introduzca la dirección de correo electrónico del administrador y la dirección IP del servidor SMTP. En caso de aviso o avería, por ejemplo una interrupción del suministro eléctrico o una unidad desenchufada, se enviará automáticamente un correo electrónico al administrador. Puede ir al Registro de Eventos para comprobar los detalles de todos los errores y avisos.

Nota: Se recomienda enviar un correo electrónico de prueba para asegurarse de que puede recibir los correos de aviso.

136

5.7.2 Configuraciones SMSC

Puede configurar el SMSC (Centro de Servicio de Mensajes Cortos) para enviar mensajes de texto SMS a números móviles particulares cuando se presenta un evento en el NVR. El proveedor de servicio SMS por defecto es Clickatell. También puede añadir su propio proveedor de servicio SMS seleccionando "Añadir Proveedor SMS" en el menú desplegable.

Cuando seleccione "Añadir proveedor de servicio SMS", necesitará introducir el nombre del proveedor SMS y el texto de la plantilla URL.

Nota:

• No podrá recibir adecuadamente SMS si el texto de la plantilla URL introducido no sigue el protocolo de su proveedor de servicio SMS.

• Por favor envié un SMS de prueba para verificar que las especificaciones sean correctas.

• Cuando el "Modo avanzado" esté en uso en "Especificaciones de alarma", esta página se inactivará. Usted puede ir a "Especificaciones de cámara" > "Especificaciones de alarma" > "Modo avanzado" para editar las especificaciones de SMS o seleccionar el uso del "Modo tradicional" y configurar las especificaciones SMS en esta página.

137

138

5.7.3 Reiniciar / Apagar

Por favor, siga estos pasos para apagar o reiniciar el VioStor:

1. Pida a todos los usuarios que estén conectados en ese momento que guarden los archivos con los que estén trabajando y dejen de usar el VioStor.
2. Abra la página web de administración y vaya a Herramientas del sistema "Reiniciar /Apagar". Siga las instrucciones que se indican para reiniciar o apagar el sistema.

139

5.7.4 Configuración del hardware

Puede habilitar o inhabilitar las siguientes funciones de hardware del VioStor:

 Habilitar botón de restablecimiento de la configuración

Habilitando esta opción, puede pulsar el botón de restablecimiento durante 5 segundos para restablecer la contraseña y las configuraciones de red del administrador a sus valores por defecto.

Nota: El interruptor para restablecer la configuración está habilitado por defecto. Cuando esta opción sea deshabilitada, por favor, asegúrese de haber guardado su contraseña con seguridad. Si no es así, el servidor no podrá ser restablecido nunca más en caso de haber perdido la contraseña.

 Encendido automático al volver la energía tras una pérdida de corriente

Cuando se habilita esta opción, el servidor se encenderá automáticamente cuando se restablece la corriente tras un corte de suministro eléctrico.

140

 Habilitar el botón de copia de seguridad de la parte frontal del vídeo

El NVR permite copiar directamente los datos grabados en el servidor, al

dispositivo USB conectado a través del puerto USB. Puede definir el número de días que el video se graba para copiarlo al dispositivo. Para usar esta función, por favor siga estos pasos:
1. Defina el total de días en que deben hacer copias de seguridad de las grabaciones más recientes. Si se ingresa 3 días, se hará copia de seguridad de las grabaciones de hoy, ayer y anteayer. Active esta función.
2. Conecte el dispositivo de almacenamiento USB, por Ej., el disco USB en el puerto USB frontal del NVR.
3. Presione y sostenga durante 3 segundos*, el botón de copia de seguridad automática de videos de un sólo toque. Los datos de la grabación en el NVR empezarán a copiarse al dispositivo USB instantáneamente. Si se reconoce el dispositivo USB, el LED USB se enciende en azul. El LED USB destella en azul mientras se copian los datos. Al igual que cuando la copia de los datos termina. Ahora puede desconectar el dispositivo en forma segura.
Nota: La función de copia de seguridad de videos, solamente soporta dispositivos USB de al menos 10 GB de capacidad de almacenamiento. Esta función solamente aplica a VS-8040U-RP, VS-8032U-RP, VS-8024U-RP.
* Si está usando VS-101/ VS-201/ NVR-104, por favor presione y mantenga presionado el botón durante medio segundo para copiar los datos.

 Habilitar luz de señal de alerta cuando el espacio libre del disco SATA sea menor que este valor

El indicador LED de Estado parpadeará en rojo y verde cuando esta función esté habilitado y el espacio libre del disco SATA sea menor que el valor. El rango de valores es 1-51200 MB.

 Activar el zumbador de alarma

Active esta opción para que el sistema emita un sonido si se detecta un error.

 Habilitar el modo de fuente de alimentación redundante

Cuando el modo de fuente de alimentación redundante esté habilitado, el
141
servidor emitirá un pitido si cualquiera de las unidades de fuente de alimentación no funciona adecuadamente.
142

 Configuración de Ventilador Inteligente

Tras habilitar el Ventilador Inteligente, la velocidad de rotación del ventilador se ajustará automáticamente de acuerdo con la temperatura del servidor. Se recomienda habilitar esta opción. Al configurar manualmente la velocidad de rotación del ventilador, el ventilador rotará permanentemente a la velocidad definida.
* Esta función solamente aplica a VS-101, VS-201, NVR-104.
143

5.7.5 Actualización del sistema

Antes de actualizar el firmware del sistema, por favor, asegúrese de que el modelo del producto y la versión de firmware son correctos. Siga los siguientes pasos para actualizar el firmware:
1. Descargue las notas de distribución de la misma versión que el firmware en el sitio Web de QNAP en http://www.qnapsecurity.com/ Lea las notas de distribución con detenimiento para estar seguro de que necesita actualizar el firmware.
2. Antes de actualizar el firmware del sistema, haga una copia de seguridad de todos los datos de los discos del servidor para evitar una potencial pérdida de datos durante la actualización del sistema.

3. Haga clic en el botón [Examinar...] para seleccionar la imagen de firmware correcta para la actualización del sistema. Haga clic en el botón "Actualizar Sistema" para actualizar el firmware.
La actualización del sistema puede tardar entre varios segundos a varios minutos en
completarse, dependiendo del estado de la conexión de la red. Por favor, espere pacientemente. El sistema le informará cuando la actualización del sistema haya finalizado.
Cuando se lleve a cabo la actualización del sistema, por favor, asegúrese de que el suministro de corriente sea estable. Si no lo hace, puede que el sistema sea incapaz de iniciarse.
Nota: Si el sistema se está ejecutando correctamente no necesitará actualizar el firmware. QNAP no se hace responsable de ningún tipo de pérdida de datos causados por una actualización inadecuada o ilegal del sistema.
144

5.7.6 Seguridad / Restaurar / Reconfiguración

 Para restaurar un archivo de configuraciones de la copia de seguridad, haga clic en "Examinar..." para seleccionar el archivo y luego haga clic en "Restaurar".
 Para crear una copia de seguridad de las configuraciones, haga clic en "Copia de Seguridad".
 Para restaurar las configuraciones a los valores por defecto establecidos en fábrica, haga clic en "Restablecer".
Precaución: si pulsa el botón Reset en esta página, los datos de unidad, cuentas de usuario, carpetas de red y opciones de sistema se borrarán y restaurarán a sus valores predeterminados. Por favor, asegúrese de haber hecho una copia de seguridad de todos sus datos importantes y opciones de sistema antes de reiniciar el NVR.
145

5.7.7 Replicación Remota

Puede usar la función de replicación remota para copiar los datos de grabación del VioStor local a un almacenamiento conectado a una red QNAP remota (NAS, TS-509). El QNAP NAS remoto se denominará en lo sucesivo "dispositivo de almacenamiento remoto".
Nota: Antes de usar esta función, asegúrese de que esté habilitado el servicio de red Microsoft del dispositivo de almacenamiento remoto, y que la ruta de acceso y el derecho de acceso correspondientes hayan sido configurados correctamente.
1. Inicie sesión en VioStor y entre en la página "Herramientas de Sistema/ Replicación Remota".
146
2. Habilitar la replicación remota (soporta múltiples opciones)
En el ejemplo anterior, el sistema sólo copia los datos de grabación de alarma de los
últimos 3 días en el dispositivo de almacenamiento remoto.
 Marque el cuadro "Habilitar replicación remota" para activar esta función. El sistema ejecuta una copia de seguridad automática de los datos de grabación en el dispositivo de almacenamiento remoto, de acuerdo con las configuraciones.
 Cuando seleccione "Realizar copia de seguridad solamente de grabaciones de alarma (en lugar de todas las grabaciones)", el sistema sólo copiará los datos de las grabaciones de alarmas en el dispositivo de almacenamiento remoto. Si esta opción no está marcada, el sistema hará una copia de seguridad de todos los datos de grabación en el dispositivo de almacenamiento remoto.
 Cuando seleccione "Realizar copia de seguridad de las grabaciones de el/los último(s) … día(s) solamente" e introduce el número de días, el sistema realizará una copia de seguridad de los últimos datos de grabación en el

dispositivo de almacenamiento remoto de acuerdo con sus configuraciones. Si esta opción no está marcada, el sistema copiará todos los datos de grabación en el dispositivo de almacenamiento remoto.
3. Configurar su servidor de almacenamiento remoto
Nota: Se recomienda ejecutar la función "Comprobación de anfitrión remoto" para verificar que la conexión al dispositivo de almacenamiento remoto ha tenido éxito.
147
4. Configurar la programación de replicación remota
Por ejemplo, para habilitar el sistema para copiar datos de grabación automáticamente en un dispositivo de almacenamiento remoto a las 01:15 cada lunes, por favor, haga lo siguiente:
Marque el cuadro "Programación de Replicación", seleccione "Semanalmente", introduzca 01 Horas: 15 minutos, y seleccione "Lunes".
5. Opciones de Copia de Seguridad
 Seleccione "Replicación Ahora", el sistema realiza inmediatamente una copia de seguridad de los datos de grabación en un dispositivo de almacenamiento remoto.
 Seleccione "Sobrescribir las grabaciones más antiguas cuando el almacenamiento disponible del anfitrión remoto sea inferior a 4GB", el sistema sobrescribirá los datos de grabación más antiguos cuando el espacio libre del servidor sea inferior a 4GB.
 Seleccione "Realizar replicación en espejo, eliminando archivos extra en la replicación remota", el sistema sincronizará los datos de grabación entre VioStor y el dispositivo de almacenamiento remoto y eliminará cualquier archivo extra del destino remoto.
 Cuando estén marcadas todas las opciones mencionadas más arriba, el sistema ejecutará la replicación remota inmediatamente. Primero juzgará si hay archivos sobrantes en la localización remota que sean diferentes de los de la fuente local. Si es así, los archivos sobrantes serán eliminados. Después, el sistema ejecutará la copia de seguridad de los datos de grabación y verificará
148
si el espacio libre del disco duro interno es inferior a 4GB. Si la capacidad de almacenamiento es superior a 4GB, la replicación remota será ejecutada inmediatamente. Si el espacio de almacenamiento es inferior a 4GB, el sistema eliminará los datos de grabación del día con más antigüedad y ejecutará la replicación remota.
 El sistema mostrará los registros de las últimas 10 replicaciones remotas para que pueda analizar el estado y la resolución de problemas.
En el ejemplo anterior:
1. Si el estado aparece como "Error (Error de acceso remoto)": Podrá comprobar si el dispositivo de almacenamiento remoto está funcionando o si las configuraciones de la red son correctas.
2. Cuando el estado aparece como "Fallo (Ha ocurrido un error interno)": Podrá comprobar el estado del disco duro de VioStor o marcar los Registros de Eventos.
Nota: El tiempo necesario para que VioStor replique los datos en un dispositivo de almacenamiento remoto varía según el entorno de red. Si el tiempo de la replicación
remota es demasiado largo, algunos archivos de grabación pueden ser sobrescritos por el sistema. Para evitar esto, se recomienda consultar los mensajes de estado para analizar el tiempo que se necesita.
149

5.7.8 Disco duro SMART

* Esta función solamente aplica a VS-101, VS-201, NVR-104.
Esta página permite a los usuarios monitorizar el estado del disco duro, su

temperatura y estado de uso por medio del mecanismo S.M.A.R.T.
Seleccione el disco duro para ver la siguiente información haciendo clic en los botones correspondientes.

Campo Descripción

Resumen Muestra el resumen de información de disco duro y el último resultado de la prueba.

Información de disco duro Muestra los detalles del disco duro, p. ej. el modelo, número de serie, capacidad del disco, etc.

Información SMART Muestra la información SMART del disco duro. Cualquier elemento cuyo valor sea inferior al umbral se considerará anormal.

Prueba Para realizar una prueba SMART de disco duro rápida o completa y mostrar los resultados.

Configuración Para configurar la alarma de temperatura. Si la temperatura del disco duro excede los valores predefinidos, el sistema registrará un error.
También puede configurar el programa de pruebas rápidas y completas. El último resultado de prueba se mostrará en la página de Resumen.

150

151

5.7.9 Mapa Electrónico

Puede cargar un Mapa electrónico en VioStor para ilustrar la localización de las cámaras.

1. Para cargar un Mapa electrónico, haga clic en "Examinar..." y seleccione el archivo del mapa electrónico. Luego, haga clic en "Cargar".
2. Puede cambiar la leyenda del mapa electrónico y hacer clic en "Aplicar".
3. Tras cargar el mapa electrónico, haga clic en "Prueba" para ver el mapa.

5.7.10 Prueba de Ping

Para probar la conexión a una dirección IP específica, introduzca la dirección IP y haga clic en "Prueba".

152

5.7.11 Especificaciones avanzadas del sistema

Puede definir el período de tiempo límite, desde la página de configuración, para desconectar a los usuarios cuando se alcance el tiempo de inactividad.

Nota: El tiempo de espera no aplica a la monitorización, reproducción, modo avanzado, configuración de dispositivos, actualización del sistema, replicación remota, configuración de dispositivos, páginas de registros & estadísticas.

153

5.8 Registros y Estadísticas

5.8.1 Registros de eventos de sistema

El VioStor puede almacenar 10.000 registros de eventos recientes, incluyendo advertencias, errores y mensajes de información. En caso de una avería del sistema,
puede obtener los registros de eventos para que le ayuden a diagnosticar el problema que afecta al sistema.
Haga clic en "Guardar" para guardar los registros en formato csv. Haga clic en "Eliminar" para eliminar todos los registros.

5.8.2 Registros de vigilancia

Esta página muestra los registros de eventos de vigilancia, como conexiones de cámara, detecciones de movimiento y errores de autenticación de cámara.

154

5.8.3 Usuarios en línea

Esta página muestra la información de los usuarios activos actualmente, como el

nombre de usuario, la dirección IP, la hora de inicio de sesión y los servicios a los que
están accediendo.

5.8.4 Lista de Usuarios Históricos

Esta página muestra la información de los usuarios que han iniciado sesión en el sistema, incluyendo el nombre de usuario, la dirección IP, la hora de inicio de sesión
y los servicios a los que han accedido, etc.

5.8.5 Registros de conexión de sistema

Los registros de conexión al servidor por medio de samba, FTP, AFP, HTTP, HTTPS, Telnet y SSH se graban en esta página.
Puede seleccionar si desea iniciar o detener el registro. La transferencia de archivos podría verse ligeramente afectada por el registro de eventos.

5.8.6 Información del Sistema

Esta página muestra la información del sistema, como el uso de la CPU, la memoria y la temperatura del sistema.

Capítulo 6. Mantenimiento del Sistema

Esta sección proporciona una vista general del mantenimiento del sistema.

6.1 Reestablecer la Contraseña del Administrador y las Configuraciones de Red

Para reestablecer la contraseña del administrador y las configuraciones de red, pulse el botón Restablecer del servidor durante cinco segundos. Se escuchará un pitido.
Tras restablecer el sistema, podrá iniciar sesión en el servidor con el nombre de usuario y la contraseña establecidos por defecto.
Nombre del Usuario por Defecto: **admin***
Contraseña: **admin**
* Si usa VS-201/ VS-101/ NVR-104, el nombre de usuario es 'administrator' y la contraseña es 'admin'.
Nota: Para restablecer el sistema con el botón Restablecer, deberá activarse la opción "Habilitar botón de restablecimiento de la configuración" en las Configuraciones del Hardware.

6.2 Interrupción de Suministro o Apagado Anormal

En caso de interrupción de suministro o apagado anormal del servidor, el servidor volverá a su estado anterior al apagado. Si su servidor no funciona correctamente tras el reinicio, por favor, haga lo siguiente:
1. Si se ha perdido la configuración del sistema, configure de nuevo el sistema.
2. En el caso de funcionamiento anormal del servidor, póngase en contacto con el servicio al cliente para que le proporcionen servicio técnico.
Para evitar las anteriores situaciones, por favor, haga una copia de seguridad de sus
datos periódicamente y asegúrese de haber realizado lo siguiente:
 Seguir las instrucciones descritas en el Capítulo 5.7.2 para reiniciar o apagar el servidor.
 Si se prevé que puede ocurrir una interrupción en el suministro de energía, haga una copia de seguridad de los todos los datos importantes y apague el servidor correctamente hasta que se restablezca el suministro de energía.

6.3 Intercambio en Caliente del Disco (Configuración RAID)

* Esta función no la soportan los modelos NVR de una bahía.
El VioStor es compatible con el intercambio en caliente. Cuando falle un disco duro del volumen de disco en espejo RAID-1, el disco que haya fallado se podrá

remplazar con uno nuevo inmediatamente sin necesidad de apagar el sistema, y así se podrán conservar los datos grabados. Sin embargo, si el disco duro está funcionando correctamente y se está llevando a cabo una grabación, no realice un intercambio en caliente para evitar daños en los archivos grabados.
158

Capítulo 7. Usar el Panel LCD

* Solamente aplica para los modelos con panel LCD.
El NVR dispone de un cómodo panel LCD para permitirle realizar la configuración de discos y visualizar la información del sistema.
Al iniciarse el NVR, podrá ver el nombre del servidor y la dirección IP:

Durante la primera instalación, el panel LCD muestra el número de discos duros detectados y la dirección IP. Puede seleccionar configurar los discos duros.

Número de discos duros detectados	**Configuración por defecto del disco**	**Opciones disponibles de configuración del disco**
1	Único	Único
2	RAID 1	Único -> JBOD ->RAID 0 -> RAID 1
3	RAID 5	Único -> JBOD ->RAID 0 -> RAID 5
4 o superior	RAID 5	Único ->JBOD -> RAID 0 -> RAID 5 -> RAID 6

* Pulse el botón "Seleccionar" (Select) para elegir la opción. Pulse el botón “Intro” (Enter) para confirmar.
159
Por ejemplo, cuando encienda el NVR con 5 discos duros instalados, el panel LCD muestra:

Puede pulsar el botón “Seleccionar” (Select) para mostrar más opciones, como RAID 6.
Pulse el botón "Intro" (Enter) y aparecerá el siguiente mensaje. Pulse el botón “Seleccionar" (Select) para seleccionar “Sí" (Yes). Pulse de nuevo el botón "Intro” (Enter) para confirmar.

Cuando la configuración haya finalizado aparecerán el nombre del servidor y la dirección IP. Si el NVR no puede crear el volumen de disco aparecerá el siguiente mensaje.

160

Ver la información del sistema usando el panel LCD

Cuando el panel LCD muestre el nombre del servidor y la dirección IP, puede pulsar el botón “Intro” (Enter) para entrar en el Main Menu. El Main Menu se compone de

los siguientes elementos:
1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

1. TCP/ IP

En TCP/ IP podrá ver las siguientes opciones:
1.1 LAN IP Address
1.2 LAN Subnet Mask
1.3 LAN Gateway
1.4 LAN PRI. DNS
1.5 LAN SEC. DNS
1.6 Enter Network Settings
1.6.1 Network Settings – DHCP
1.6.2 Network Settings – Static IP*
1.6.3 Network Settings – BACK
1.7 Back to Main Menu
* En Network Settings – Static IP, puede configurar la dirección IP, la mascara de subred, el puerto de enlace y la DNS de LAN 1 y LAN 2.
161

2. Physical disk

En Physical disk podrá ver las siguientes opciones:
2.1 Disk Info
2.2 Back to Main Menu
La información del disco muestra la temperatura y la capacidad del disco duro.

3. Volume

Esta sección muestra la configuración de disco del NVR. La primera línea muestra la configuración RAID y la capacidad de almacenamiento, la segunda línea muestra el número de la unidad miembro de la configuración.

Si hay más de un volumen, pulse el botón "Seleccionar" (Select) para ver la información. En la siguiente tabla se indica la descripción de los mensajes LCD para la configuración RAID1.

Pantalla LCD Configuración de la Unidad

RAID5+S RAID5+reserva
RAID5 (D) RAID 5 modo degradado
RAID 5 (B) RAID 5 reconstrucción
RAID 5 (S) RAID 5 resincronización
RAID 5 (U) RAID está desmontado
RAID 5 (X) RAID 5 no activo
162

4. System

Esta selección muestra la temperatura del sistema y la velocidad de rotación del ventilador del sistema.

5. Shut down
Use esta opción para apagar el NVR. Pulse el botón "Seleccionar" (Select) para seleccionar "Sí" (Yes). Luego pulse el botón "Intro" (Enter) para confirmar.
6. Reboot
Use esta opción para reiniciar el NVR. Pulse el botón "Seleccionar" (Select) para seleccionar "Sí" (Yes). Luego pulse el botón "Intro" (Enter) para confirmar.
7. Password
La contraseña por defecto del panel LCD está en blanco. Entre en esta opción para cambiar la contraseña. Seleccione "Sí" (Yes) para continuar.

Puede introducir una contraseña con un máximo de 8 caracteres numéricos (0-9). Cuando el cursor se desplaza a "Aceptar" (OK), pulse el botón "Intro" (Enter). Verifique la contraseña para confirmar los cambios.

8. Back
Seleccione esta opción para volver al menú principal.

Mensajes del Sistema
Cuando el NVR encuentra un error del sistema, aparecerá un mensaje de error en el
panel LCD. Pulse el botón "Intro" (Enter) para ver el mensaje. Pulse el botón "Intro" (Enter) para ver el siguiente mensaje.

Mensaje del Sistema	Descripción
Sys. Fan Failed	Error en el ventilador del sistema
Sys. Overheat	El sistema se sobrecalienta
HDD Overheat	El Disco Duro se sobrecalienta
CPU Overheat	La CPU se sobrecalienta
Network Lost	Tanto el LAN 1 como el LAN 2 están desconectados en modo Error o Equilibrio de Carga
LAN1 Lost	LAN 1 está desconectado
LAN2 Lost	LAN 2 está desconectado
HDD Failure	Error en el Disco Duro
Vol1 Full	El volumen está lleno
HDD Ejected	El disco duro ha sido extraído
Vol1 Degraded	El volumen está en modo degradado
Vol1 Unmounted	El volumen está desmontado
Vol1 Nonactivate	El volumen no está activado

Capítulo 8. Resolución de Problemas
1. No aparece la pantalla de monitorización.
Por favor, compruebe lo siguiente:
A. Compruebe si ha instalado correctamente ActiveX al iniciar sesión en la página de monitorización. Configure el nivel de seguridad en "Medio" o inferior en las Opciones de Internet del explorador de IE.
B. Asegúrese de que VioStor esté apagado y de que la red esté conectada

correctamente.
C. Que la dirección IP de VioStor no entre en conflicto con otros dispositivos de la misma subred.
D. Compruebe las configuraciones de la dirección IP de VioStor y de su ordenador. Asegúrese de que estén en la misma subred.

2. No se puede ver el vídeo en directo de una de las cámaras en la página de monitorización.

Por favor, compruebe lo siguiente:
A. Que la dirección IP, el nombre y la contraseña introducidas en la página de configuración de la cámara sean las correctas. Puede usar la función "Prueba" para verificar la conexión.
B. Cuando el PC y la cámara de red estén en la misma subred, mientras que VioStor esté en otra, no podrá ver la pantalla de monitorización desde el PC. Puede resolver los problemas usando los siguientes métodos:
Método 1: Introduzca la dirección IP de la cámara de red como la IP WAN en VioStor.
Método 2: Configure el enrutador para permitir acceso interno a la dirección IP pública y a los puertos asignados de las cámaras de red.

3. La grabación no funciona correctamente.

A. Asegúrese de que la bandeja del disco duro esté correctamente bloqueada en VioStor.
B. Cuando sólo haya instalado un disco duro, asegúrese de que el disco esté instalado en la bandeja del disco duro 1. El disco duro 1 debería instalarse sobre el disco duro 2.
C. Compruebe si está habilitada la función de grabación en la página de Configuración de la Cámara (la función está habilitada por defecto).

Asegúrese de que la dirección IP, el nombre y la contraseña sean correctos.
D. Si se verifica que los elementos anteriores funcionan correctamente mientras el LED de estado parpadea en verde, el/los disco(s) duro(s) pueden estar dañados o no ser detectados. Por favor, apague el servidor e instale un nuevo disco duro.
Nota: Si ha actualizado las configuraciones de VioStor, la grabación se detendrá temporalmente y se reiniciará tras un corto período de tiempo.

4. No puedo iniciar sesión en la página de administración.

Por favor, compruebe si tiene autoridad de administrador. Sólo se permite a los administradores iniciar sesión en VioStor.

5. El vídeo en directo a veces no es nítido o no tiene una imagen clara.

A. La calidad de la imagen puede ser restringida o tener interferencias debido al tráfico actual de la red.
B. Cuando existe múltiples accesos a la cámara o al servidor VioStor, la calidad de la imagen puede verse reducida. También es recomendable tener, como máximo, tres conexiones simultáneas a la página de monitorización. Para un mejor rendimiento de grabación, por favor no abra demasiados exploradores IE para ver el vídeo en directo.
C. La misma cámara puede ser compartida por múltiples VioStors para una grabación simultánea. Por favor, use las cámaras dedicadas.

6. La grabación de alarma no funciona.

A. Por favor, inicie sesión en la página de administración y vaya a las Configuraciones de Cámara-Configuraciones de Alarma. Asegúrese de que la grabación de alarma esté habilitada para la cámara.
B. Al usar cámaras Panasonic BB-HCM311, el firmware de la cámara debe estar actualizada con la versión 1.3 para que la grabación de alarma funcione correctamente.

C. Si VioStor esté instalado tras un enrutador mientras que la cámara no lo está, la grabación de alarma no funcionará.
D. Si la grabación de alarma está habilitada, asegúrese de haber configurado el número de días durante los cuales las grabaciones de alarma serán guardadas en las Configuraciones de Cámara-Configuraciones Avanzadas. Si no es así, las grabaciones podrían ser sobrescritas.
166

7. El espacio de almacenamiento estimado para la grabación que se muestra en la página de Configuraciones de Grabación es diferente del valor real.

Este valor estimado sirve sólo como referencia. El espacio de disco real puede variar dependiendo de los contenidos de las imágenes, el entorno de red y el rendimiento de las cámaras.

8. La pantalla tiene una apariencia anormal, con extrañas líneas horizontales, si la resolución de la cámara Panasonic BB-HCM381 está configurada como 640x480.

Esto es debido al diseño de escaneado entrelazado de la cámara. Por favor, inicie sesión en la página de configuración de la cámara y vaya a Setup (Configuración)->Camera (Cámara)->Vertical Resolution (Resolución de Vertical). Luego, ajuste la configuración en 240.

9. El mapa electrónico no puede mostrarse correctamente.

Por favor, compruebe el formato del archivo. VioStor sólo es compatible con mapas electrónicos en formato JPEG.

10. No puedo localizar mi VioStor en el Buscador (Finder).

A. Compruebe si su VioStor está encendido.
B. Compruebe la conexión de red entre el ordenador y VioStor.
C. Refresque el Buscador y compruebe la dirección IP de VioStor. Asegúrese de haber apagado todos los cortafuegos de su ordenador.

11. Los cambios en las configuraciones del sistema no tienen efecto.

Tras cambiar las configuraciones en la página de administración, haga clic en el botón Aplicar para aplicar los cambios.

12. No se puede mostrar completamente la página de monitorización en el Internet Explorer.

Si está usando la función de zoom en el Internet Explorer 7, puede que la página no se muestre correctamente. Por favor, haga clic en F5 para refrescar la página.
167

13. No puedo usar las funciones de SMB, FTP y Web File Manager (Administrador de Archivos Web) de VioStor.

A. Por favor, vaya a la página de Configuraciones de Red-Servicios de Archivo y compruebe si están habilitadas estas tres funciones.
B. Si VioStor está instalado tras un enrutador y el acceso a VioStor esté fuera del enrutador, no podrá usar los servicios SMB ni FTP. Para usar los servicios SMB y FTP, puede abrir los puertos del enrutador. Por favor, consulte el Apéndice B para más detalles.

14. Al servidor le lleva demasiado tiempo reiniciar.

Si el servidor ha estado reiniciando durante más de 5 minutos, por favor, apáguelo y vuelva a encenderlo de nuevo. Si el problema persiste, por favor, póngase en contacto con el soporte técnico.
168

Apéndice A Registro de un Nombre de Dominio Dinámico

VioStor es compatible con los servicios DDNS proporcionados por DynDNS. Puede ir al sitio web de DynDNS http://www.dyndns.org/ para registrar un nombre de dominio dinámico.

Configure y active el servicio DDNS para habilitar los usuarios de Internet para que puedan acceder a su VioStor a través de este nombre de dominio dinámico. Cuando el IPS asigna una nueva dirección IP WAN, VioStor actualizará la nueva dirección al servidor DynDNS automáticamente.
169
Procedimiento de Registración
Por favor, siga los siguientes pasos para registrar un nombre de dominio dinámico. Esta guía sólo sirve sólo como referencia. Si hay cambios, por favor, consulte las instrucciones o documentos del sitio web.
1. Abra el explorador y conecte a (http://www.dyndns.com/) Haga clic en "Create Account" (Crear Cuenta) para comenzar la registración.
2. Introduzca el nombre de usuario, la dirección de correo electrónico y la contraseña para servicio DDNS. Por favor, verifique su dirección de correo electrónico para recibir el mensaje de confirmación del servidor.
170
3. Seleccione la opción para aceptar los términos del acuerdo.
4. Configure las listas de envío si es necesario. Luego, haga clic en "Create Account" (Crear Cuenta).
5. Cuando su cuenta haya sido creada con éxito, un mensaje de confirmación será enviado a su dirección de correo electrónico. Por favor, siga las instrucciones en el correo electrónico para activar su cuenta dentro de 48 horas. Cuando haya finalizado el proceso de confirmación, puede solicitar su propio nombre de dominio dinámico. Por favor, consulte el sitio web del proveedor de DDNS para más información.
171

Apéndice B Ejemplos de Configuración

Entorno 1: VioStor, la Cámara IP y el PC de monitorización están todos en la misma red.
Instalación de Vigilancia de Red para SOHO y SMB
Dirección IP
VioStor *192.168.1.1*
PC *192.168.1.100*
Cámara 1 *192.168.1.101*
Cámara 2 *192.168.1.102*
Cámara 3 *192.168.1.103*
En el ejemplo, simplemente agregue la cámara a VioStor, introduciendo la dirección IP de la cámara.
172
Entorno 2: VioStor y la cámara IP están instalados detrás el enrutador, y el PC de monitorización está tiene una ubicación remota.
Dirección IP Puerto Asignado del enrutador
VioStor *192.168.1.1 8000*
Cámara 1 *192.168.1.101 8001*
Cámara 2 *192.168.1.102 8002*
Cámara 3 *192.168.1.103 8003*
IP público del enrutador *219.87.144.205*
PC *10.8.10.100*
173
En este ejemplo, para permitir un PC remoto conectar a VioStor y a las cámaras, necesita:
Paso 1. Configurar la asignación de puertos (servidor virtual) en el enrutador.
De A
219.87.144.205:8000 192.168.1.1:80
219.87.144.205:8001 192.168.1.101:80
219.87.144.205:8002 192.168.1.102:80

219.87.144.205:8003 192.168.1.103:80
Paso 2. Añada la cámara a VioStor, introduciendo la dirección IP de la cámara en las
configuraciones "Dirección IP", y la dirección IP pública del enrutador y los puertos asignados de la cámara a las configuraciones de "Dirección IP WAN".
Nota: Al configurar la cámara de red, deben introducirse la IP WAN y la IP LAN.
Para abrir el FTP (puerto 21) y el SMB (puerto 445) de VioStor en la WAN, necesita configurar las siguientes asignaciones de puerto:
De A
219.87.144.205:21 192.168.1.1:21
219.87.144.205:139 192.168.1.1:139
219.87.144.205:445 192.168.1.1:445
Tras finalizar los dos pasos anteriores, puede acceder a VioStor a través de WAN, introduciendo la dirección IP http://219.87.144.205:8000 en el explorador IE. Luego, inicie sesión en VioStor usando el nombre de usuario y la contraseña correctos.
Si el puerto especificado para VioStor es 80, puede introducir http://219.87.144.205 para acceder a VioStor, ya que el puerto por defecto de HTTP
es 80.
Nota: Si el enrutador no usa una IP fija, necesitará configurar el DDNS en el enrutador. Las otras configuraciones son las mismas que las anteriores.

Entorno 3: VioStor y la Cámara IP son remotos
Dirección IP
VioStor *219.87.144.205*
Cámara 1 *61.62.100.101*
Cámara 2 *61.62.100.102*
Cámara 3 *61.62.100.103*
En este ejemplo, simplemente agregue la cámara a VioStor, introduciendo su dirección IP en las configuraciones de "Dirección IP".
Nota: Si hay un puerto especialmente designado para conectar la cámara, por favor, especifique el puerto en las configuraciones de VioStor.

Entorno 4: El VioStor y la cámara IP están instalados detrás del enrutador
Dirección IP
VioStor 1 192.168.1.101
VioStor 2 192.168.1.102
VioStor 3 192.168.1.103
Enrutador público IP 219.87.145.205
En el ejemplo, para permitir a un PC que sea remoto acceder a cada VioStor a través
de FTP, necesitará:
Paso 1. Configurar la asignación de puertos (el servidor virtual) en el enrutador
Desde A
VioStor 1 219.87.145.205:2001
VioStor 2 219.87.145.205:2002
VioStor 3 219.87.145.205:2003
Podría conectar directamente VioStor 1 a través de FTP usando ftp://219.87.145.205:2001
Podría conectar directamente VioStor 2 a través de FTP usando ftp://219.87.145.205:2002
Podría conectar directamente VioStor 3 a través de FTP usando ftp://219.87.145.205:2003
Paso 2. Habilitar la Asignación de Puertos FTP en el VioStor

Si desea conectar cada VioStor a través de FTP haciendo clic en el botón “FTP” de la página de reproducción de cada VioStor, necesita habilitar la asignación de puertos FTP en las “Configuraciones de Red” > “Servicios de Archivos” > “Servicio FTP” en la
página de administración de sistema y configurar el número del puerto asignado.
Puerto Asignado
VioStor 1 2001
VioStor 2 2002
VioStor 3 2003
Tras finalizar los dos pasos anteriores, podrá acceder a VioStor a través de FTP introduciendo la dirección IP en el explorador IE o haciendo clic en el botón “FTP” de
la página de reproducción. Luego, inicie sesión en el VioStor usando el nombre y la contraseña de usuario correctos.

Soporte Técnico

Para cualquier pregunta técnica, por favor, consulte el manual de usuario. QNAP también proporciona Soporte En-línea dedicado y servicio al cliente a través del Instant Messenger.
Soporte en línea: http://www.qnapsecurity.com/
MSN: q.support@hotmail.com
Skype: qnapskype

Soporte Técnico en EE.UU y Canadá:

Correo-e: q_supportus@qnap.com
TEL: 909-595-2819 ext. 185
Dirección: 168 University Parkway Pomona, CA 91768-4300
Horario de atención: 08:00–17:00 (GMT- 08:00 hora del pacífico, de lunes a viernes)

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble
The GNU General Public License is a free, copyleft license for software and other kinds of works.
The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to
your programs, too.
When we speak of free software, we are referring to freedom, not price. Our General
Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.
To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect

the freedom of others.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.
178
Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission
to copy, distribute and/or modify it.
For the developers' and authors' protection, the GPL clearly explains that there is no
warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.
Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.
Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.
The precise terms and conditions for copying, distribution and modification follow.
TERMS AND CONDITIONS
0. Definitions.
“This License” refers to version 3 of the GNU General Public License.
“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.
“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.
179
To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on”
the earlier work.
A “covered work” means either the unmodified Program or a work based on the Program.
To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the
public, and in some countries other activities as well.
To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey
the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.
1. Source Code.
The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.
A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular
programming language, one that is widely used among developers working in that language.
The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component,
but which is not part of that Major Component, and (b) serves only to enable use of 180
the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable
work runs, or a compiler used to produce the work, or an object code interpreter used to run it.
The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does
not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.
The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.
The Corresponding Source for a work in source code form is that same work.
2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights
of fair use or other equivalent, as provided by copyright law.
You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which

you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on
181
terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.
Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.
3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.
When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.
4. Conveying Verbatim Copies.
You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License
and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.
You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.
5. Conveying Modified Source Versions.
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided
that you also meet all of these conditions:
a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this
182
License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the
work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.
A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined
with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users

beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.
6. Conveying Non-Source Forms.
You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:
a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and

noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way
through the same place at no further charge. You need not require recipients to copy
the Corresponding Source along with the object code. If the place to copy the object
code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.
A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.
A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.
"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified

versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.
184
If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).
The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.
Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.
7. Additional Terms.
“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.
When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions
may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered
work, for which you have or can give appropriate copyright permission.
Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material)
185
supplement the terms of this License with terms:
a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it;
or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.
All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it,
contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.
If you add terms to a covered work in accord with this section, you must place, in the
relevant source files, a statement of the additional terms that apply to those files, or
a notice indicating where to find the applicable terms.
Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.
8. Termination.
You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent
186
licenses granted under the third paragraph of section 11).
However, if you cease all violation of this License, then your license from a particular
copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days
after the cessation.
Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.
Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.
9. Acceptance Not Required for Having Copies.
You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you
indicate your acceptance of this License to do so.
10. Automatic Licensing of Downstream Recipients.
Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this

License.
An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives
187
whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.
You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty,
or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing
the Program or any portion of it.
11. Patents.
A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.
A contributor's “essential patent claims” are all patent claims owned or controlled by
the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its
contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.
Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.
In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.
If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge
188
and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use
of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey,
or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and
works based on it.
A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered
work, unless you entered into that arrangement, or that patent license was granted,
prior to 28 March 2007.
Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.
12. No Surrender of Others' Freedom.
If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy
189
simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you
agree to terms that obligate you to collect a royalty for further conveying from those
to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.
13. Use with the GNU Affero General Public License.
Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the combination as such.
14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that

numbered version or of any later version published by the Free Software Foundation.
If the Program does not specify a version number of the GNU General Public License,
you may choose any version ever published by the Free Software Foundation.
If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.
Later license versions may give you additional or different permissions. However, no
additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.
15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE
190
COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
17. Interpretation of Sections 15 and 16.
If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.
END OF TERMS AND CONDITIONS

Table of Contents

Overview

VIVOTEK IP7330 is a cost-effective, bullet-style network camera designed for our customers'
needs in outdoor applications. With its weather-proof IP66-rated housing, the camera is shielded
from harsh conditions such as rain and dust and provides an all-in-one solution without the need
for additional accessories.
By integrating components for day/night functionality such as dual-band lens and built-in IR
illuminators with an effective range of up to 10 meters, the camera is able to achieve
superior performance in a compact design. The IP7330 also supports tamper detection, which
can detect events such as blockage, redirection, and spray-painting, making it an intelligent

solution to possible camera obstruction.
Incorporating a number of VIVOTEK's advanced features, including simultaneous dual streams,
dual-codec, 802.3af compliant PoE, and our free standard 16-channel recording software, the
IP7330 is the ideal solution for your outdoor surveillance needs.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera
is not only a high-performance web-ready camera but also can be part of a flexible surveillance
system. It is the user's responsibility to ensure that the operation of such devices is legal before
installing this unit for its intended use.
It is important to first verify that all contents received are complete according to the Package
contents listed below. Take notice of the warnings in Quick Installation Guide before the Network
Camera is installed; then carefully read and follow the instructions in the Installation chapter to
avoid damages due to faulty assembly and installation. This also ensures the product is used
properly as intended.
The Network Camera is a network device and its use should be straightforward for those who
have basic network knowledge. It is designed for various applications including video sharing,
general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the
Network Camera and ensure proper operations. For the creative and professional developers,

the URL Commands of the Network Camera section serves to be a helpful reference to
customize existing homepages or integrating with the current web server.

Package Contents

- IP7330
- Liquid Tight Connectors (3 holes, for backup use)
- Silica Gel
- Camera Stand
- Power Adapter
- RJ45 Female/Female Coupler
- Quick Installation Guide
- Warranty Card
- Software CD

Physical Description

Front Panel
Back Panel
Connectors

Lens IR LED
Light Sensor
Reset Button
Status LED
Ethernet 10/100 RJ45 Plug
Power Cord Socket (black)
General I/O Terminal Block

General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external
input / output devices. The pin definitions are described below.

Hardware Reset

The reset button is used to reset the system or restore the factory default settings. Sometimes
resetting the system can return the camera to normal operation. If the system problems remain

after reset, restore the factory settings and install again.

Reset: Press and release the reset button with a paper clip or thin object. Wait for the Network

Camera to reboot.

Restore: Press on the reset button continuously for over 5 seconds. Note that all settings will be

restored to factory default.

AV24V
AC24V
DI
GND

Pin Name

AV24V 24V+

AC24V 24VDI

Digital Iutput

GND Ground

Reset Button

Installation

Hardware Installation

1. Loose the liquid tight connectors, and then remove the rubber.
2. Loose the back cover.
3. Tear down the aluminum foil vacuum bag and take out the silica gel. Attach the supplied silica

gel to the inner side of the Network Camera. (Please replace the silica gel with a new one if

you open the back cover after installation.)

4. Make sure all cable lines are securely connected.
5. Tighten the back cover, rubber and liquid tight connectors.
6. Secure the Network Camera to the wall/ceiling by the supplied camera stand.

Note

If you want to use your own cable lines, please loose two supplied screws and take out the

power board. Then be careful to make connections as the illustration below.

Silica gel

Ceiling mount

Wall mount

Upper Side

Bottom Side

Power Cord

Terminal Block (from left to right)

1: AV24V (red)

2: AC24V (red)

3: DI (white)

4: GND (black)

Ethernet Cable

Screws

Network Deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera to Internet connection.

1. If you have external devices such as sensors and alarms, make the connection from the general I/O terminal block.

2. Use the supplied RJ45 female/female coupler to connect the Network Camera to a switch.

Use Category 5 Cross Cable when Network Camera is directly connected to PC.

3. Connect the power cable from the Network Camera to a power outlet.

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow

the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below.

Regarding how to obtain your IP address, please refer to Software installation on page 10 for

details.

AV24V: 24V+

AC24V: 24VDI

: Digital Input

GND: Ground

AV24V
AC24V
DI
GND

IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
LAN (Local Area Network)
192.168.0.1
Cable or DSL Modem
Router IP address :
WAN (Wide Area Network)
Router IP address : from ISP

2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is

192.168.0.3, please forward the following ports for the Network Camera on the router.

- HTTP port
- RTSP port
- RTP port for audio
- RTCP port for audio
- RTP port for video
- RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly

on your router. For information on how to forward ports on the router, please refer to your
router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider).

Use the public IP and the secondary HTTP port to access the Network Camera from the
Internet. Please refer to Network Type on page 30 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera.

Please refer to LAN on page 30 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to
PPPoE on page 31 for details.

Set up the Network Camera through Power over Ethernet (PoE)

When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet
cable. If your switch/router supports PoE, refer to the following illustration to connect the
Network Camera to a PoE-enabled switch/router.

power + data transmission

PoE Switch

When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect the
Network Camera and a non-PoE switch/router.

Non-PoE Switch

PoE Power Injector
(optional)

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up
your Network Camera on the LAN.

1. Install IW2 from the Software Utility directory on the software CD.
Double click the IW2 shortcut on your desktop to launch the program.
2. The program will conduct an analysis of your network environment.
After your network environment is analyzed, please click **Next** to continue the program.
3. The program will search for all VIVOTEK network devices on the same LAN.
4. After searching, the main installer window will pop up. Click on the MAC and model name
which matches the product label on your device to connect to the Network Camera via
Internet Explorer.

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players,
3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the Network Cameras installed on the LAN.

If your network environment is not a LAN, follow these steps to access the Network Camera:

1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).

2. Enter the IP address of the Network Camera in the address field. Press **Enter**.

3. The live video will be displayed in your web browser.

4. If this is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.

NOTE

► For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you donn't have Quick Time on your computer, please install it first, then launch the web browser.

► By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 24.

► If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.

1. Choose Tools > Internet Options > Security > Custom Level.
2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.
3. Refresh your web browser, then install the Active X® control. Follow the instructions to complete installation.

Using RTSP Players

To view the MPEG-4 streaming media using RTSP players, you can use one of the following
applications that support RTSP streaming.
Quick Time Player
Real Player
VLC media player
mpegable Player
pvPlayer
As most ISPs and players only allow RTSP streaming through port number 554, please set the
RTSP port to 554. For more information, please refer to RTSP Streaming on page 36.
For example:
4. The live video will be displayed in your player.
For more information on how to configure the RTSP access name, please refer to RTSP
Streaming on page 36 for details.
rtsp://192.168.5.151:554/live.sdp

1. Launch a RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or
stream2>

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network
Camera can be accessed over the Internet. For more information on how to set up the Network
Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 7.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make
sure the authentication mode of RTSP streaming is set to disable.
For more information, please refer to RTSP Streaming on page 36.

2. As the the bandwidth on 3G networks is limited, larger video sizes are not available. Please
set the video and audio streaming parameters as listed below.
For more information, please refer to Video on page 43.

Video Mode MPEG-4
Frame size 176 x 144
Maximum frame rate 5 fps
Intra frame period 1S
Video quality (Constant bit rate) 40kbps
Audio type (GSM-AMR) 12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set
the RTSP port to 554. For more information, please refer to RTSP Streaming on page 36.

4. Launch the player on the 3GPP-compatible mobile device (ex. Real Player).

5. Type the following URL command into the player.
The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming
access name for stream1 or stream2>.
For example:
rtsp://192.168.5.151:554/live.sdp

Using VIVOTEK Recording Software

The product software CD also contains VIVOTEK's recording software, allowing simultaneous
monitoring and video recording for multiple Network Cameras. Please install the recording

software, then launch the program to add the Network Camera to the Channel list. For detailed
information about how to use the recording software, please refer to the user's manual of the
software or download the manual from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections:
VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live
Video Window.

VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page
22.

Camera Control Area

Video Stream: This Network Cmera supports MJPEG or MPEG-4 dual streams simultaneously. You can
select either one for live viewing.
IR Illuminators: Click to turn on the IR LEDs for 20 seconds.

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to
Client Settings on page 19.
Configuration: Click this button to access the configuration page of the Network Camera. It is suggested
that a password be applied to the Network Camera so that only the administrator can configure the
Network Camera. For more information, please refer to Configuration on page 21.
Language: Click this button to choose a language for the user interface. Language options are available

in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Logo of VIVOTEK INC.

Live View Window

Camera Control Area

Configuration Area

Host Name

Live Video Window

■ The following window is displayed when the video mode is set to MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video settings on page 43.

MPEG-4 Protocol and Media Options: The transmission protocol and media options for MPEG-4 video
streaming. For further configuration, please refer to Client Settings on page 19.

Time: Display the current time. For further configuration, please refer to Video settings on page 43.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration,
please refer to Video settings on page 43.

Video Control Buttons: Depending on the Network Camera model and Network Camera configuration,
some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in
a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP
(*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation
screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To
move to a different area you want to magnify, drag the navigation screen image.

Pause: Pause the transmission of the streaming media. The button becomes the Resume button
after clicking the Pause button.

Stop: Stop the transmission of streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format. Press the

Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops

accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on

page 20 for details.

Video Control Buttons

MPEG-4 Protocol and Media Options

Video Title Time

Title and Time

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal

mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Video Settings on

page 43.

Time: Display the current time. For more information, please refer to Video Settings on page 43.

Title and Time: The video title and time can be stamped on the streaming video. For more information,

please refer to Video Settings on page 43.

Video Control Buttons: Depending on the Network Camera model and Network Camera configuration,

some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed

in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP

(*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation
screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To
move to a different area you want to magnify, drag the navigation screen image.
Start MP4 Recording: Click this button to record video clips in MP4 file format. Press the
Stop MP4 recording button to end recording. When you exit the web browser, video recording stops
accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on
page 20 for details.
Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal
mode.

Video Title Time

Title and Time

Video Control Buttons

Client Settings

This chapter explains how to select the stream transmission mode and saving options on the
local computer. When finished with the settings on this page, click **Save** on the bottom of the
page to enable the settings.

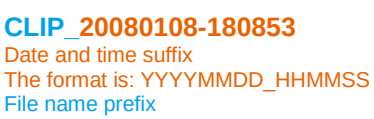
MPEG-4 Protocol Options

Depending on your network environment, there are four transmission modes for MPEG-4 streaming:
UDP unicast: This protocol allows for better real-time audio and video streams. However, network
packets may be lost due to network burst traffic and images may be broken. Activate the UDP connection
when occasions require time-sensitive responses and the video quality is less important. Note that each

unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up
to ten simultaneous accesses.
UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients
requesting streaming media. This helps to reduce the network transmission load of the Network Camera
while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must
be configured to enable multicast streaming at the same time. For more information, please refer to
RTSP Streaming on page 36.
TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video
quality. However, the real-time effect is not as good as that of the UDP protocol.
HTTP: This protocol allows for the same transmission quality as the TCP protocol without needing to
open specific ports for streaming under some network environments. Users inside a firewall can utilize
this protocol to allow streaming data through.

MP4 Saving Options

Users can record live video as they are watching by clicking Start MP4 Recording on the main page.
Here, you can specify the storage destination and file name.
Folder: Specify the storage destination for the recorded video files.
File name prefix: Enter the text that will be appended to the front of the video file name.
Add date and time suffix to the file name: Select this option to append the date and time to the end of the
file name.



Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only
Administrators can access the configuration page.
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with
minimal effort. To simplify the setting procedure, two types of user interfaces are available:
Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced
functions (HTTPS/ Access list/ Homepage layout/ Application/ Recording/ System log/ View
parameters) are not displayed in Basic Mode.
If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the
configuration list to quickly switch to Advanced Mode.
In order to simplify the user interface, the detailed information will be hidden unless you click on
the function item. When you click on the first sub-item, the detailed information for the first subitem
will be displayed; when you click on the second sub-item, the detailed information for the
second sub-item will be displayed and that of the first sub-item will be hidden.
The following is the interface of the Basic Mode and the Advanced Mode:

Basic Mode

Click to switch to Advanced mode
Firmware Version
Configuration list

Advanced Mode

Each function on the configuration list will be explained in the following sections. Those functions that are
displayed only in Advanced Mode are marked with Advanced Mode . If you want to set up the advanced

functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch over.

System

This section explains how to configure the basic settings for the Network Camera, including
host name and system time. It is composed of the following three columns: System, System
Time and DI. When completed with the settings on this page, click **Save** at the bottom of the
page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the
main page.

Click to switch to Basic mode
Firmware Version
Configuration list

System Time

Keep current date and time: Select this option to preserve the current date and time of the Network
Camera. The Network Camera's internal real-time clock maintains the date and time even when the
system power is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with
the local computer. The read-only date and time of the PC is displayed when updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format is
[yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically
querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank

connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly
basis.

Time zone Advanced Mode : Select the appropriate time zone from the list. If you want to upload
Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving
Time Configuration File on page 75 for details.

DI

Digital input: Select **High** or **Low** to define the normal status for the digital input. The Network Camera
will report the current status.

Security

This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add
more accounts in the Manage User column, please set a password for the “root” account first.

1. Type the password in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their
respective fields to access the Network Camera.

Manage Privilege Advanced mode

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a
User ID and Password.

Manage User

Administrators can add up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators
can access the Configuration page. Operators cannot access the Configuration page but can use the
URL Commands to get and set the value of parameters. For more information, please refer to URL
Commands of the Network Camera on page 78. Viewers access only the main page for live viewing.
Here you also can change a user's access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL
(Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher
security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS"
or "HTTPS only". Note that you have to create and install a certificate first in the second column before
clicking the **Save** button.

Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first.
There are three ways to create and install a certificate:

Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: "HTTP
& HTTPS" or "HTTPS only".
3. Click **Save** to generate a certificate.

4. The Certificate Information will automatically de displayed in the third column as shown below. You can
click **Property** to view detailed information about the certificate.
5. Click **Home** to return to the main page. Change the address from “http://” to “https://“ in the address
bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to
enable HTTPS.
https://192.168.5.151/index.html
https://

Create self-signed certificate manually
1. Select this option.
2. Click **Create** to open a Create Certificate page, then click **Save** to generate the certificate.
3. The Certificate Information will automatically be displayed in the third column as shown below. You
can click **Property** to see detailed information about the certificate.
Create certificate and install : Select this option if you want to create an official certificate issued by
a CA (Certificate Authority).
1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

3. If you see the following Information bar, click **OK** and click on the Information bar on the top of the
page to allow pop-ups.
4. The pop-up window shows an example of a certificate request.

5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait
for the certificate authority to issue a SSL certificate; click Browse... to search for the issued certificate,

then click **Upload** in the second column.

NOTE

► How do I cancel the HTTPS settings?

1. Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.
2. Click **OK** to disable HTTPS.
3. The webpage will redirect to a non-HTTPS page automatically.

► If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, uncheck **Enable HTTPS secure connection** in the first column and click **Save**.

Then click **Remove** to erase the certificate.

Network

This section explains how to configure a wired network connection for the Network Camera.

Network Type

LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.

1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software installation on page 10 for details.
2. Enter the static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera
so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras
will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently,
UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the
UPnP™ component is installed on your computer.

Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to
allow the Network Camera to open ports on the router automatically so that video streams can be sent
out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as
there is an Internet connection. Note that to utilize this feature, it requires an account provided by your
ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page
62) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 65). Select
System log so that you will receive the system log in TXT file format which contains the Network
Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password

provided by your ISP. Click **Save** to enable the setting.

5. The Network Camera will reboot.

6. Disconnect the power to the Network Camera; remove it from the LAN environment.

NOTE

► If the default ports are already used by other devices connected to the same router, the Network

Camera will select other ports for the Network Camera.

► If UPnP™ is not supported by your router, you will see the following message:

Error: Router does not support UPnP port forwarding.

Network Camera (192.168.5.151)

► Steps to enable UPnP™ user interface on your computer:

Note that you must log on to the computer as a system administrator to install the UPnP™

components.

1. Go to Start, click **Control Panel**, and then click **Add or Remove Programs**.

2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.

3. In the Windows Components Wizard dialog box, select **Networking Services** and then click **Details**.

4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.

5. Click **Next** in the following window.

6. Click **Finish**. UPnP™ is enabled.

► How does UPnP™ work?

UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices

added to a network. Services and capabilities offered by networked devices, such as printing and file

sharing, are available among each other without the need for cumbersome network configuration. In

the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

► Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the
router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network
Camera's public address in order to access the Network Camera from the Internet. For example,
when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for
the Network Camera's IP address.

From the Internet In LAN

http://203.67.124.123:8080 http://192.168.4.160 or
http://192.168.4.160:8080

► If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the
Network Camera to factory default; please refer to Restore on page 74 for details. After the Network
Camera is reset to factory default, it will be accessible on the LAN.

HTTP Advanced Mode

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first;
please refer to Security on page 26 for details.

Authentication: Depending on your network security requirements, the Network Camera provides two
types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential
risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5
algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is
set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are

incorrectly assigned, the following warning messages will be displayed:

To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

In LAN

http://192.168.4.160 or

http://192.168.4.160:8080

URL command -- http://<ip address>:<http port>/<access name for stream1 or stream2>

For example, when the Access name for stream 2 is set to video2.mjpg:

1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

NOTE

► Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.

HTTPS

By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

FTP

The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK Installation Wizard
2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to
another port number between 1025 and 65535.
http://192.168.5.151/video2.mjpg

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network
Camera first; please refer to Security on page 24 for details.
Authentication: Depending on your network security requirements, the Network Camera provides three
types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential
risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using
MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed in the following table:
Access name for stream 1 / Access name for stream 2: This Network camera supports dual streams
simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to
MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the URL command in the text box. For example:
4. The live video will be displayed in your player as shown
below.
rtsp://192.168.5.151:554/live.sdp

Quick Time player Real Player
Disable O O
Basic O O
Digest O X

RTSP port /RTP port for video, audio/ RTCP port for video, audio

■ RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always odd. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:

Multicast settings for stream 1 / Multicast settings for stream 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or stream 2.

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even
number and the multicast RTCP port number is the multicast RTP port number plus one, and is thus
always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.
If the multicast RTP video ports are incorrectly assigned, the following warning message will be
displayed:
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a
packet can be forwarded.

DDNS

This section explains how to configure the dynamic domain name service for the Network
Camera. DDNS is a service that allows your Network Camera, especially when assigned with a
dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is
recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet.
Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.
com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the
terms of the Service Agreement.

2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, then
click **Register**. After a host name has been successfully created, a success message will be displayed
in the DDNS Registration Result column.
3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields
in the DDNS column at the top of the page as seen in the picture.

[Register] Successfully Your account information has
been mailed to registered e-mail address

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system
integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system
integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a
host name has been successfully created, you will see a success message in the DDNS Registration
Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the
DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your
account information will be sent to your email address.

Refer to the following links to apply a dynamic domain account when selecting other DDNS
providers:

■ Dyndns.org (Dynamic) / Dyndns.org (Custom): visit http://www.dyndns.com/

■ TZO.com: visit http://www.tzo.com/

■ DHS.org: visit http://www.dhs.org/

■ dyn-interfree.it: visit http://dyn-interfree.it/

[Register] Successfully Your account information has
been mailed to registered e-mail address

Access List Advanced Mode

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10
clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**,
all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick
Time Player).

View Information: Click this button to display the connection status window showing a list of the current
connections. For example:

■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name
and password to access the live video. The user name will be displayed in the User ID column. If the
administrator allows clients to link to the webpage without a user name and password, the User ID
column will be empty.

There are some situations which allow clients access to the live video without a user name and
password:

1. The administrator does not set up a root password. For more information about how to set up a root
password and manage user accounts, please refer to Security on page 24.

2. The administrator has set up a root password, but set **RTSP Authentication** to “disable“. For more
information about **RTSP Authentication**, please refer to RTSP Streaming on page 36.
3. The administrator has set up a root password, but allows anonymous viewing. For more information
about **Allow Anonymous Viewing**, please refer to Security on page 24.

■ Refresh: Click this button to refresh all current connections.
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List
to deny access. Please note that those checked connections will only be disconnected temporarily
and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the
denied list, please check **Enable access list filtering** and click **Save** in the first column.
■ Disconnect: If you want to break off the current connections, please select them and click this
button. Please note that those checked connections will only be disconnected temporarily and will
automatically try to re-link again (IE Explore or Quick Time Player).
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering
function.

Filter

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP

addresses are on the Allowed list and not on the Denied list can access the Network Camera.

■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules for user to set up:

Single: This rule allows the user to add an IP address to the Allowed/Denied list.

For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the

Allow/Deny List.

For example:

IP address 192.168.2.x will be bolcked.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is

only applied to IPv4.

For example:

■ Delete Allowed/Denied list:

In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.

NOTE

► For example, when the range of IP addresses in the allowed list is set from 1.1.1.0 to 192.255.255.255

and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IP located between

171.0.0.0 and 192.255.255.255 can access the Network Camera.

Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's

IP address in this field to make sure the Administrator can always connect to the device.

Allowed List
Denied List

Video

This section explains how to cofigure the audio and video settings of the Network Camera.

Video Settings

Video title: Enter a name that will be displayed on the title bar of the live video.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image
flickering associated with fluorescent lights. Note that after the power line frequency is changed, you
must disconnect and reconnect the power cord of the Network Camera in order for the new setting to
take effect.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display
of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling)
to correct the image orientation.

Maximum exposure time: Select a proper maximum exposure time according to the light source of the
surroundings. The exposure times are selectable for the following durations: 1/30 second, 1/15 second,
and 1/5 second. Shorter exposure times result in less light.

Video title

Overlay title and time stamp on video: Select this option to place the video title and time on the video
streams.

Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be
stamped on the video streams.

Indoor Mode: To prevent color rolling effect under fluorescent light, please check this item to adjust the
parameter.

Image Settings Advanced Mode

Click **Image Settings** to open the Image Settings page. On this page, you can tune White balance,
Brightness, Saturation, Contrast, and Sharpness for the video.
White balance: Adjust the value for best color temperature.
■ Auto
The Network Camera automatically adjusts the color temperature of light in response to different light
sources. The white balance setting defaults to Auto and works well in most situations.

■ Keep current value
Follow the steps below to manually set the white balance to compensate for the ambient lighting
conditions.
1. Set the White balance to Auto and click **Save**.
2. Place a sheet of white paper in front of the lens; then allow the Network Camera to adjust the color
temperature automatically.
3. Select Keep current value to confirm the setting while the white balance is being measured.
4. Click **Save** to take effect.
Image Adjustment
■ Brightness: Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.
■ Saturation: Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.
■ Contrast: Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.
■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to 0.
You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without
incorporating the changes. When completed with the settings on this page, click **Save** to enable the
setting and click **Close** to exit the page.

Privacy Mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to
address privacy concerns.

■ To set the privacy mask windows, follow the steps below:

1. Click New to add a new window.
2. Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size
of the object (height and width) you want to cover.
3. Enter a Window Name and click Save to enable the setting.
4. Select Enable privacy mask to enable this function.

NOTE

► Up to 5 privacy mask windows can be set up on the same screen.

► If you want to delete the privacy mask window, please click the 'x' on the upper right-hand corner of
the window.

Video quality settings for stream 1 / stream 2 Advanced Mode

The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4
and MJPEG.

Click the items to display the detailed configuration settings. You can set up two seperate streams for the
Network Camera for different viewing devices. For example, set a smaller frame size and lower bit rate
for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web
browsers.

If **MPEG-4** mode is selected, it is streamed in RTSP protocol. There are four parameters provided in
MPEG-4 mode which allow you to adjust the video performance:

■ Frame size

Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are
selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video
quality.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps,
8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are
selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select
Customize and manually enter a value.

■ Intra frame period

Determine how often to plant an I frame. The shorter the duration, the more likely you will get better
video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period
from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed
for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at
a selected level, resulting in mutable video quality performance. The bit rates are selectable at the
following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps,
1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality;
bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following

settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and
manually enter a value.
If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing
a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same
image quality, which in turn comes at the expense of variable bandwidth usage. Because the media
contents are a combination of JPEG images, no audio data is transmitted to the client. There are three
parameters provided in MJPEG mode to control the video performance:

■ Frame size

Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are
selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate

This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video
quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps,
2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the
frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps
and 30fps. You can also select **Customize**, and manually enter a value.

■ Video quality

The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and
Excellent. You can also select **Customize**, and manually enter a value.

NOTE

► The value of video quality and fixed quality refers to the **compression rate**, so the lower value will
produce the higher quality.

Day/Night Settings

Switch to B/W in night mode

Select this to enable the Network Camera to automatically switch to B/W during night mode.

IR LED

With built-in IR illuminators, up to 15m, this Network Camera can make use of IR light during low light
conditions.

The IR LED supports five modes, Auto, Day, Night, Schedule and Disabled.

■ Auto mode

The Network Camera automatically control the IR LED by judging the level of ambient light.

■ Day mode

Select “Day mode” to turn on the IR LED.

■ Night mode

Select “Night mode” to turn off the IR LED.

■ Schedule mode

Select “Schedule mode” to control the IR LED by schedule. Enter the start and end time for day mode.

Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and
end time of day mode are set to 07:00 and 18:00.

Light sensor sensitivity

Select Low, Normal, or High for the light sensor sensibility.

Disable IR LED

If you do not want to use the IR illuminators, you can select this option to turn it always off.

Motion Detection

This section explains how to configure the Network Camera to enable motion detection. A total
of three motion detection windows can be configured.

Follow the steps below to enable motion detection:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
■ To move and resize the window, drag and drop your mouse on the window.
■ To delete window, click X on the top right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the
Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:

The Percentage Indicator will rise or fall depending on the variation between sequential images. When
motions are detected by the Network Camera and are judged to exceed the defined threshold, the
red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be
captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a
trigger source. For more information on how to set an event, please refer to Application on page 56.

Motion Detection Setting 2:
for special situation
Motion Detection Setting 1:
for normal situation

A green bar indicates that even though motions have been detected, the event has not been triggered
because the image variations still fall under the defined threshold.
If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile**
to open the Motion Detection Profile Settings page as shown below. A total of three motion detection
windows can be configured on this page as well.

Please follow the steps beolw to set up a profile:

1. Create a new motion detection window.
2. Check Enable this profile.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
4. Click Save to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 58 for detailed information.

Percentage = 30%

NOTE

► How does motion detection work?

There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as “alerted pixels” (frame D).

Percentage is a value that expresses the proportion of “alerted pixels” to all pixels in the motion detection window. In this case, 50% of pixels are identified as “alerted pixels”. When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will

be outlined in red.

For applications that require a high level of security management, it is suggested to use higher

sensitivity settings and smaller percentage values.

Camera Tampering Detection

This section explains how to set up camera temper detection. With tamper detection, the

camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even

spray paint.

Please follow the steps below to set up the camera tamper detection function:

1. Check Enable camera tampering detection.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the

tampering factor (the difference between current frame and pre-saved background) exceeds the trigger

threshold.

3. Set up the event source as Camera Tampering Detection on Application page > Event Settings /

Server Settings (how to send alarm message) / Media Settings (send what type of alarm message).

Please refer to page 65 for detailed information.

Homepage Layout Advanced Mode

This section explains how to set up your own customized homepage layout.

Preview

This column shows the settings of your homepage layout. You can manually select the background and

font colors in Theme Options, the third column on this page. The settings will automatically show up in

this Preview field. The following shows the homepage using the default settings:

Logo

Here you can change the logo at the top of your homepage.

Follow the steps below to upload a new logo:

1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you

to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the

settings.

Font Color

Background Color of the

Control Area

Font Color of the Configuration Area

Background Color of the

Configuration Area

Font Color of the Video

Title

Background Color of the

Video Area

Frame Color

Preset Patterns

■ Follow the steps below to set up the customed homepage:

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.
3. The palette window will pop up as shown below.
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will show up in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

1

2

3

4

Color Selector

Custom

Pattern

Application Advanced Mode

This section explains how to configure the Network Camera to react in response to particular
situations (event). A typical application is that when a motion is detected, the Network Camera
sends buffered images to a FTP server or e-mail address as notifications.

Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on
configuring the settings. Please note that there is a limited number of customized scripts you can upload;
if the current amount of customized scripts has reached the limit, an alert message will pop up. If you
need more information, please ask for VIVOTEK's technical support.

Click to upload
a file.

Click to modify the
script online

In the illustration on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.

Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. On this page, you can

arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be
configured.
Event name: Enter a name for the event setting.
Enable this event: Select this option to enable the event setting.
Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority
setting will be executed first.
Detect next event after seconds: Enter the duration in seconds to pause motion detection after a
motion is detected.

An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the
following three elements: Trigger, Event Schedule, and Action.

Trigger

This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can
be configured to use the Network Camera's built-in motion detection mechanism or external digital input
devices.
There are several choices of trigger sources as shown below. Select the items to display the detailed
configuration options.

■ Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this
function, you need to configure a Motion Detection Window first. For more information, please refer to
Motion detection on page 49 for details.

■ Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999
minutes are allowed.

■ Digital input

This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound and light, etc.

■ System boot

This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data. If you want receive **Recording notify message**, please refer to page 67 for detailed information.

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 52 for detailed information.

Event Schedule

Specify the period for the event.

■ Select the days of the week.

■ Select the recording schedule in 24-hr time format.

Action

Define the actions to be performed by the Network Camera when a trigger is activated.

■ Turn on IR Illuminators for seconds

Select this to turn on IR Illuminators when a trigger is activated every time or only in low light conditions. Specify the length of trigger interval in the text box.

To set an event with recorded video or snapshots, it is necessary to configure the server and
media settings so that the Network Camera will know what action to take (such as which server
to send the media files to) when a trigger is activated.

■ Add Server / Add Media

Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings
on page 62.

Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on
page 65.

Here is an example of Event Settings page:

When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new
event settings / server settings / media settings will appear in the event drop-down list on the Application
page.

Here is an example of Application page with an event setting:

When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will
automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove
the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**.

Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**.

Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify
where the notification messages are sent when a trigger is activated. A total of 5 server settings can be
configured.

Server name: Enter a name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item
to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.

- Sender email address: Enter the email address of the sender.
- Recipient email address: Enter the email address of the recipient.
- Server address: Enter the domain name or IP address of the email server.
- User name: Enter the user name of the email account if necessary.
- Password: Enter the password of the email account if necessary.
- Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure
connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up
window. If successful, you will also receive an email indicating the result.

Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.

- Server address: Enter the domain name or IP address of the FTP server.
- Server port

By default, the FTP server port is set to 21. It can also be assigned to another port number between
1025 and 65535.

■ User name: Enter the login name of the FTP account.
■ Password: Enter the password of the FTP account.
■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network
Camera will create one on the FTP server.
■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server
supports passive mode, select this option to enable passive mode FTP and allow data transmission to
pass through the firewall.
To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up
window as shown below. If successful, you will also receive a test.txt file on the FTP server.
Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.
■ URL: Enter the URL of the HTTP server.
■ User name: Enter the user name if necessary.
■ Password: Enter the password if necessary.
To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up
window as below. If successful, you will receive a test.txt file on the HTTP server.
Click **Save** to enable the settings, then click **Close** to exit the page.
Network storage: Select to send the media files to a network storage location when a trigger is activated.
Please refer to **Network Storage Setting** on page 69 for details.
Click **Save** to enable the settings, then click **Close** to exit the page.
When completed, the new server settings will automatically be displayed on the Event Settings page.
For example:

Media Settings

Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can
specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be
configured.

Media name: Enter a name for the media setting.

Media Type

There are three choices of media types available: Snapshot, Video clip, and System log. Select the item
to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

- Source: Select to take snapshots from stream 1 or stream 2.
- Send pre-event images

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number
to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

- Send post-event images

Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can
be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15
images are generated after a trigger is activated.

- File name prefix

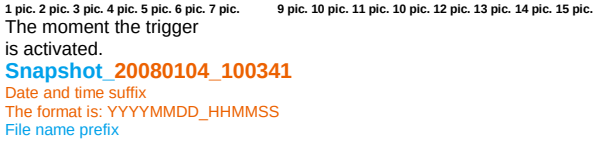
Enter the text that will be appended to the front of the file name.

- Add date and time suffix to the file name

Select this option to add a date/time suffix to the file name.

For example:

Click **Save** to enable the settings, then click **Close** to exit the page.



Video clip: Select to send video clips when a trigger is activated.

■ Source: Select to record video clips from stream 1 or stream 2.

■ Pre-event recording

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number
to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration

Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten
seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.

■ Maximum file size

Specify the maximum file size allowed.

■ File name prefix

Enter the text that will appended to the front of the file name.
For example:

Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.

Click **Save** to enable the settings, then click **Close** to exit the page.

Video_20080104_100341
Date and time suffix
The format is: YYYYMMDD_HHMMSS
File name prefix
1 sec. 2 sec. 3 sec. 4 sec. 5 sec. **7 sec. 8 sec. 9 sec. 10 sec.**
Trigger Activation

Recording notify message: Select to send a recording notify message when a trigger is activated.

Following is an example of recording notify message (.txt file), which shows a list of deleted recorded
data due to cycle recording.

When completed, click **Save** to take effect and then click **Close** to quit this page. The new media settings
will show up on the Event Settings page.

Then you can continue to select a server and media type for the event.

■ Create folders by date, time, and hour automatically: If you check this item, the system will generate
folders automatically by date.

■ View: Click this button to open a file list window. This function is only for Network Storage.

The following is an example of a file destination with video clips:

20081120
20081121
20081122

Click to delete selected items Click to delete all recorded data

The format is: YYYYMMDD

Click to open the directory

Click **20081120** to open the directory:

The format is: HH (24r)

Click to open the file list of that hour

The format is: File name prefix + Minute (mm)

You can set up the File name prefix on Media Settings page.

Please refer to page 65 for detailed information.

Click to delete
selected items

Click to delete all
recorded data

Click to go back to the previous
level of the directory

Recording Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

NOTE

► Before setting up this page, please set up the Network Storage on the Server Settings page first.

Network Storage Setting

Click Server to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.

For example:

2. Click **Test** to check the setting. The result will be shown in the pop-up window.

1

2

3

4

the path of the network storage
(\\server name or IP address\folder name)
the user name and password of
your server

If successful, you will receive a test.txt file on the network storage server.

3. Enter a server name.

4. Click **Save** to complete the settings and click **Close** to exit the page.

Recording Settings

Click **Add** to open the recording setting page. On this page, you can define the recording source,
recording schedule and recording capacity. A total of 2 recording settings can be configured.

Recording name: Enter a name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of the recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 or stream 2).

Recording Schedule: Specify the recording duration.

■ Select the days of the week.

■ Select the recording start and end times in 24-hr time format.

Destination: You can select the network storage to store the recorded video files.

Capacity: You can choose either the “entire free space available” or “limit the recording size”. The
recording size limit must be larger than the reserved amount for cyclic recording.

File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file
will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent

malfunction. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger >**

Recording notify on page 58 for detailed information.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit

this page. When the system begins recording, it will send the recorded files to the Network Storage.

The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click

Delete.

■ Click **Video (Name)**: Opens the Recording Settings page to modify.

■ Click **ON (Status)**: The Status will become **OFF** and stop recording.

■ Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about

folder naming rule, please refer to page 67 for details.

20081120
20081121
20081122

System Log Advanced Mode

This section explains how to configure the Network Camera to send the system log to the

remote server as backup.

Remote Log

You can configure the Network Camera to send the system log file to a remote server as a log backup.

Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log

messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.

com/kiwi-syslog-daemon-overview/.

Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.

2. In the port text box, enter the port number of the remote server.

3. When completed, select **Enable remote log** and click **Save** to enable the setting.

Current Log

This column displays the system log in chronological order. The system log is stored in the Network
Camera's buffer area and will be overwritten when reaching a maximum limit.

View Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in alphabetical order. If you
need technical assistance, please provide the information listed on this page.

Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware
version, etc.

Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When
completed, the live video page will be displayed in your browser. The following message will be displayed
during the rebooting process.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the
address field to resume the connection.

Restore

This feature allows you to restore the Network Camera to factory default settings.

Network Type: Select this option to retain the Network Type settings. (Please refer to Network Type on
page 30.)

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings. (Please refer to
System on page 22.)

Custom Language: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.

Export / Upload Files Advanced Mode

This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting
backup files.

Export daylight saving time configuration file: Click to set the start and end time of DST. Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the
Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to
store the file for editing.
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST.
When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at
2:00 a.m. on the first Sunday in November.

Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload.
If the incorrect date and time are assigned, you will see the following warning message when uploading
the file to the Network Camera.

The following message is displayed when attempting to upload an incorrect file format.

Export language file: Click to export language strings. VIVOTEK provides nine languages: English,
Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters for the device and user-defined scripts.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model
and firmware version of the device should be the same as the setting backup file. If you have set up a
fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade Firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to
complete the process.

Note: Do do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:

1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade
completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, reaccess
the Network Camera.

The following message is displayed when the upgrade has succeeded.

The following message is displayed when you have selected an incorrect firmware file.

Reboot system now!!
This connection will close.
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

Appendix

URL Commands for the Network Camera

Overview

For some customers who already have their own web site or web control application, the Network

Camera/Video Server can be easily integrated through URL syntax. This section specifies the external
HTTP-based application programming interface. The HTTP-based camera interface provides the
functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set
internal parameter values. The image and CGI-requests are handled by the built-in Web server.

Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that
is to be replaced with either a value or a string. When replacing the text string, the angle brackets
should also be replaced. An example of this is the description of the name for the server, denoted with
<servername> in the URL syntax description below, that is replaced with the string myserver in the URL
syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced
syntax as shown below. For example, name of the server is written as <servername> and is intended to
be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.
adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

http://<servername>/cgi-bin/viewer/video.jpg

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data
returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line
Feed (CRLF) printed as \r\n.

Return:

HTTP/1.0 <HTTP code> <HTTP text>\r\n

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box

with the example.

Example: request a single snapshot image

http://mywebserver/cgi-bin/viewer/video.jpg

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators.
When the CGI request includes internal camera parameters, the internal parameters must be written exactly
as they are named in the camera or video server. The CGIs are organized in function related directories
under the cgi-bin directory. The file extension of the CGI is required.
Syntax:
http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]
Example: Setting digital output #1 to active
http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

Security level

SECURITY
LEVEL
SUB-DIRECTORY DESCRIPTION
0 anonymous Unprotected.
1 [view] anonymous, viewer 1. Can view, listen, talk to camera
2. Can control dido, ptz of camera
4 [operator] anonymous, viewer,
operator
Operator's access right can modify most of camera's
parameters except some privilege and network options
6 [admin] anonymous, viewer,
operator, admin
Administrator's access right can fully control the camera's
operation.
7 N/A Internal parameters. Unable to be changed by any external
interface.

Get server parameter values

Note: The access right depends on the URL directory.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]
http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]
http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]
where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>] If you do not specify the
any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the
parameters of related group will be returned.
When query parameter values, the current parameter value are returned.
Successful control request returns paramter pairs as follows.
Return:
HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
<length> is the actual length of content.
Example: request IP address and it's response
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Set server parameter values

Note: The access right depends on the URL directory.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]
http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
PARAMETER VALUE DESCRIPTION
<group>_<name> value to assigned Assign <*value*> to the parameter <*group*>_<*name*>
update <boolean> set to 1 to actually update all fields (no need to use update parameter in each group)
return <*return page*> Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.
(note: The return page can be a general HTML file(.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
Only the parameters that you set and readable will be returned.
Example: Set the IP address of server to 192.168.0.123
Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n

Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Available parameters on the server

Valid values:
VALID VALUES DESCRIPTION
string[<n>] Text string shorter than 'n' characters. The characters ",', <,>,& are invalid.
password[<n>] The same as string but display '*' instead
integer Any number between (-2^{31} – 1) and (2^{31} – 1)
positive integer Any number between 0 and (2^{32} – 1)
<m> ~ <n> Any number between 'm' and 'n'
domain name[<n>] A string limited to contain a domain name shorter than 'n' characters (eg.
www.ibm.com)
email address [<n>] A string limited to contain a email address shorter than 'n' characters (eg.
joe@www.ibm.com)
ip address A string limited to contain an ip address (eg. 192.168.1.1)
mac address A string limited to contain mac address without hyphen or colon connected
boolean A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>,
<value2>,
<value3>,
…
Enumeration. Only given values are valid.
blank A blank string
everything inside <> As description
NOTE: The camera should prevent to restart when parameter changed.

Group: **system**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
hostname string[40] 1/6 host name of server
(Network Camera,
Wireless Network Camera,
Video Server,
Wireless Video Server)
lowlight <boolean> 6/6 (0) Turn on white light LED in all condition
(1) Only turn on white light LED in low light
condition
(product dependent)
date <yyyy/mm/dd>,
keep,
auto
6/6 Current date of system. Set to 'keep'
keeping date unchanged. Set to 'auto' to
use NTP to synchronize date.
time <hh:mm:ss>,
keep,
auto
6/6 Current time of system. Set to 'keep'
keeping time unchanged. Set to 'auto' to
use NTP to synchronize time.
datetime <MMDDhhmmYYYY.ss> 6/6 Another current time format of system.
ntp <domain name>,
<ip address>,
<blank>
6/6 NTP server

*do not use “skip to invoke default server”
for default
timezoneindex -489 ~ 529 6/6 Indicate timezone and area
-480: GMT-12:00 Eniwetok, Kwajalein
-440: GMT-11:00 Midway Island, Samoa
-400: GMT-10:00 Hawaii
-360: GMT-09:00 Alaska
-320: GMT-08:00 Las Vegas,
San_Francisco, Vancouver
-280: GMT-07:00 Mountain Time, Denver
-281: GMT-07:00 Arizona
-240: GMT-06:00 Central America, Central
Time, Mexico City, Saskatchewan
-200: GMT-05:00 Eastern Time, New York,
Toronto
-201: GMT-05:00 Bogota, Lima, Quito,
Indiana
-180: GMT-04:30 Caracas

-160: GMT-04:00 Atlantic Time, Canada, La
Paz, Santiago
-140: GMT-03:30 Newfoundland
-120: GMT-03:00 Brasilia, Buenos Aires,
Georgetown, Greenland
-80: GMT-02:00 Mid-Atlantic
-40: GMT-01:00 Azores, Cape_Verde_IS.
0: GMT Casablanca, Greenwich Mean Time:
Dublin, Edinburgh, Lisbon, London
40: GMT 01:00 Amsterdam, Berlin, Rome,
Stockholm, Vienna, Madrid, Paris
41: GMT 01:00 Warsaw, Budapest, Bern
80: GMT 02:00 Athens, Helsinki, Istanbul,
Riga
81: GMT 02:00 Cairo
82: GMT 02:00 Lebanon, Minsk
83: GMT 02:00 Israel
120: GMT 03:00 Baghdad, Kuwait, Riyadh,
Moscow, St. Petersburg, Nairobi
121: GMT 03:00 Iraq
140: GMT 03:30 Tehran
160: GMT 04:00 Abu Dhabi, Muscat, Baku,
Tbilisi, Yerevan
180: GMT 04:30 Kabul
200: GMT 05:00 Ekaterinburg, Islamabad,
Karachi, Tashkent
220: GMT 05:30 Calcutta, Chennai,
Mumbai, New Delhi
230: GMT 05:45 Kathmandu
240: GMT 06:00 Almaty, Novosibirsk,
Astana, Dhaka, Sri Jayawardenepura
260: GMT 06:30 Rangoon
280: GMT 07:00 Bangkok, Hanoi, Jakarta,
Krasnoyarsk
320: GMT 08:00 Beijing, Chongging, Hong
Kong, Kuala Lumpur, Singapore, Taipei
360: GMT 09:00 Osaka, Sapporo, Tokyo,
Seoul, Yakutsk

380: GMT 09:30 Adelaide, Darwin

400: GMT 10:00 Brisbane, Canberra,
Melbourne, Sydney, Guam, Vladivostok
440: GMT 11:00 Magadan, Solomon Is.,
New Caledonia
480: GMT 12:00 Aucklan, Wellington, Fiji,
Kamchatka, Marshall Is.
520: GMT 13:00 Nuku'Alofa
daylight_enable <boolean> 6/6 enable automatic daylight saving to time
zone
daylight_dstactual
mode
<boolean> 6/7 check if current time is under daylight
saving time.
daylight_auto_begi
ntime
string[19] 6/7 display the current daylight saving begin
time.
(product dependent)
daylight_auto_endt
ime
string[19] 6/7 display the current daylight saving end
time.
(product dependent)
updateinterval 0,
3600,
86400,
604800,
2592000
6/6 0 to Disable automatic time adjustment,
otherwise, it means the seconds between
NTP automatic update interval.
restore 0,
<positive integer>
7/6 Restore the system parameters to default
value after <value> seconds.
reset 0,
<positive integer>
7/6 Restart the server after <value> seconds if
<value> is non-negative.
restoreexceptnet <Any value> 7/6 Restore the system parameters to default
value except (ipaddress, subnet, router,
dns1, dns2, pppoe).
This command can cooperate with other
"restoreexceptXYZ" commands. When
cooperating with others, the system
parameters will be restored to default value
except a union of combined results.
restoreexceptdst <Any value> 7/6 Restore the system parameters to default
value except all daylight saving time
settings.

This command can cooperate with other
"restoreexceptXYZ" commands. When
cooperating with others, the system
parameters will be restored to default value
except a union of combined results.
restoreexceptlang <Any Value> 7/6 Restore the system parameters to default
value except custom language file user
uploaded.
This command can cooperate with other

“restoreexceptXYZ” commands. When
cooperating with others, the system
parameters will be restored to default value
except a union of combined results.
SubGroup of **system**: **info** (The fields in this group are unchangeable.)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
modelname string[40] 0/7 Internal model name of server (eg. IP7139)
serialnumber <mac
address>
0/7 12 characters mac address without hyphen
connected
firmwareversion string[40] 0/7 The version of firmware, including model,
company, and version number in the format
<MODEL-BRAND-VERSION>
language_count <integer> 0/7 number of webpage language available on the
server
language_i<0~(count-1)> string[16] 0/7 Available language lists
customlanguage_maxcoun
t
<integer> 0/7 Maximum number of custom language supported
on the server
customlanguage_count <integer> 0/7 Number of custom language which has been
uploaded to the server
customlanguage_i<0~(ma
xcount-1)>
string 0/7 Custom language name
Group: **status**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
di_i<0~(ndi-1)> <boolean> 1/7 0 => Inactive, normal
1 => Active, triggered
do_i<0~ndi-1)> <boolean> 1/7 0 => Inactive, normal

1 => Active, triggered
daynight day,
night
7/7 The day/night status judge by light sensor
onlinenum_rtsp integer 6/7 current RTSP connection numbers
onlinenum_httppush integer 6/7 current HTTP push server connection numbers
Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
normalstate high,
low
1/1 indicate whether open circuit or closed circuit
represents inactive status
Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
normalstate open,
grounded
1/1 indicate whether open circuit or closed circuit
represents inactive status
Group: **security**
NAME VALUE SECURITY

(get/set)
DESCRIPTION
user_i0_name string[64] 6/7 User's name of root
user_i<1~20>_name string[64] 6/7 User's name
user_i0_pass password[64] 6/6 root's password
user_i<1~20>_pass password[64] 7/6 User's password
user_i0_privilege viewer,
operator,
admin
6/7 root's privilege
user_i<1~20>_
privilege
viewer,
operator,
admin
6/6 User's privilege.
Group: **network**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
type lan,
pppoe
6/6 Network connection type
resetip <boolean> 6/6 1 => get ipaddress, subnet, router, dns1, dns2 from

DHCP server at next reboot
0 => use preset ipaddress, subnet, rounter, dns1, and
dns2
ipaddress <ip address> 6/6 IP address of server
subnet <ip address> 6/6 subnet mask
router <ip address> 6/6 default gateway
dns1 <ip address> 6/6 primary DNS server
dns2 <ip address> 6/6 secondary DNS server
wins1 <ip address> 6/6 primary WINS server
wins2 <ip address> 6/6 secondary WINS server
Subgroup of **network**: **ftp**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 21, 1025~65535 6/6 local ftp server port
Subgroup of **network**: **http**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 80, 1025 ~
65535
6/6 HTTP port
alternateport 1025~65535 6/6 Alternative HTTP port
authmode basic,
digest
1/6 HTTP authentication mode
s0_accessname string[32] 1/6 Http server push access name for stream 1
(capability.protocol.spush_mjpeg =1 and
video.stream.count>0)
s1_accessname string[32] 1/6 Http server push access name for stream 2
(capability.protocol.spush_mjpeg =1 and
video.stream.count>1)
anonymousviewing <boolean> 1/6 Enable anoymous streaming viewing.
Subgroup of **network**: **https**
NAME VALUE SECURITY

(get/set)
DESCRIPTION
port 443, 1025 ~ 65535 6/6 HTTPS port
Subgroup of **network**: **rtsp**

NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 554, 1025 ~ 65535 1/6 RTSP port
(capability.protocol.rtsp=1)
anonymousviewing <boolean> 1/6 Enable anoymous streaming viewing.
authmode disable,
basic,
digest
1/6 RTSP authentication mode
(capability.protocol.rtsp=1)
s0_accessname string[3b;42] 1/6 RTSP access name for stream1
(capability.protocol.rtsp=1 and
video.stream.count>0)
s1_accessname string[32] 1/6 RTSP access name for stream2
(capability.protocol.rtsp=1 and
video.stream.count>1)
Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast=1)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
alwaysmulticast <boolean> 4/4 Enable always multicast
ipaddress <ip address> 4/4 Multicast IP address
videoport 1025 ~ 65535 4/4 Multicast video port
ttl 1 ~ 255 4/4 Mutlicast time to live value
Subgroup of **network**: **rtp**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
videoport 1025 ~ 65535 6/6 video channel port for RTP
(capability.protocol.rtp_unicast=1)
Subgroup of **network**: **pppoe**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
user string[128] 6/6 PPPoE account user name

pass password[64] 6/6 PPPoE account password
Group: **ipfilter**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable ipfilter settings
admin_enable <boolean> 6/6 Enable or disable the function always allow the
admin IP address to access this device
admin_ip 1.0.0.0 ~
255.255.255.255
6/6 Always allow this IP connect to camera when
admin_enable=1
maxconnection 0~10 6/6 Maximum number of concurrent streaming
connection(s) limit
allow_i<0~9>_start 1.0.0.0 ~
255.255.255.255
6/6 Allowed starting IP address for RTSP connection

allow_i<0~9>_end 1.0.0.0 ~
255.255.255.255
6/6 Allowed ending IP address for RTSP connection
deny_i<0~9>_start 1.0.0.0 ~
255.255.255.255
6/6 Denied starting IP address for RTSP connection
deny_i<0~9>_end 1.0.0.0 ~
255.255.255.255
6/6 Denied ending IP address for RTSP connection
Group: **videoin**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
cmosfreq 50, 60 4/4 CMOS frequency
(videoin.type=2)
(product dependent)
whitebalance auto, manual 4/4 auto, auto white balance
manual
indoor, 3200K
fluorescent, 5500K
outdoor, > 5500K
atwbvalue 0 ~ 65535 4/4 The auto white balance value.
Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number
NAME VALUE SECURITY
(get/set)
DESCRIPTION
color 0, 1 4/4 0 =>monochrome

1 => color
flip <boolean> 4/4 flip the image
mirror <boolean> 4/4 mirror the image
text string[16] 1/4 enclosed caption
imprinttimestamp <boolean> 4/4 Overlay time stamp on video
maxexposure 1~30 4/4 Maximum exposure time
scenemode 0, 1 4/4 0 => outdoor mode
1 => indoor mode
s<0~(m-1)>_codectype mpeg4, mjpeg 4/4 video codec type
s<0~(m-1)>_resolution VGA CMOS =>
176x144,
320x240,
640x480
4/4 Video resolution in pixel
s<0~(m-1)>_mpeg4_intrap
eriod
250, 500, 1000,
2000, 3000,
4000
4/4 The period of intra frame in
milliseconds
s<0~(m-1)>_mpeg4_rateco
ntrolmode
cbr, vbr 4/4 cbr, constant bitrate
vbr, fix quality
s<0~(m-1)>_mpeg4_quant 0, 1~5 4/4 quality of video when choosing vbr in
"ratecontrolmode".
0 is customized manual input setting.
1 is worst quality and 5 is the best
quality.
s<0~(m-1)>_mpeg4_qvalue 1~31 7/4 The specific quality parameter of
mpeg4 encoder.

1 is best quality and 31 is the worst
quality.
s<0~(m-1)>_mpeg4_bitrate 1000~4000000 4/4 Set bit rate in bps when choose cbr in
"ratecontrolmode"
s<0~(m-1)>_mpeg4_maxfr
ame
1~25,
26~30 (only for
NTSC or 60Hz
CMOS)
4/4 set maximum frame rate in fps (for
MPEG-4)
s<0~(m-1)>_mjpeg_quant 0 ~ 5 4/4 quality of jpeg video.
0 is customized manual input setting.
1 is worst quality and 5 is the best
quality.
s<0~(m-1)>_mjpeg_qvalue 10~200 7/4 The specific quality parameter of jpeg

encoder.
10 is best quality and 200 is the worst
quality.
s<0~(m-1)>_mjpeg_maxfra
me
1~25,
26~30 (only for
60Hz CMOS)
4/4 set maximum frame rate in fps (for
JPEG)
s<0~(m-1)>_forcei 1 7/6 Force I frame
Group: **image_c<0~(n-1)>** for n channel products
NAME VALUE SECURITY
(get/set)
DESCRIPTION
brightness -5 ~ 5 4/4 Adjust brightness of image according to mode settings.
saturation -5 ~ 5 4/4 Adjust saturation of image according to mode settings.
contrast -5 ~ 5 4/4 Adjust contrast of image according to mode settings.
sharpness -3 ~ 3 4/4 Adjust sharpness of image according to mode settings.
Group: **imagepreview_c<0~(n-1)>** for n channel products
NAME VALUE SECURITY
(get/set)
DESCRIPTION
brightness -5 ~ 5 4/4 Preview of adjusting brightness of image according to
mode settings.
Saturation -5 ~ 5 4/4 Preview of adjusting saturation of image according to
mode settings.
Contrast -5 ~ 5 4/4 Preview of adjusting contrast of image according to mode
settings.
Sharpness -3 ~ 3 4/4 Preview of adjusting sharpness of image according to
mode settings.
videoin_whitebalance auto,
manual
4/4 Preview of adjusting white balance of image according to
mode settings
videoin_restoreatwb 0, 1~ 4/4 Restore of adjusting white balance of image according to
mode settings
Group: **motion_c<0~(n-1)>** for n channel product
NAME VALUE SECURITY
(get/set)
DESCRIPTION
Enable <boolean> 4/4 enable motion detection

win_i<0~2>_enable <boolean> 4/4 enable motion window 1~3
win_i <0~2>_name string[14] 4/4 name of motion window 1~3
win_i <0~2>_left 0 ~ 320 4/4 Left coordinate of window position.

win_i <0~2>_top 0 ~ 240 4/4 Top coordinate of window position.
win_i <0~2>_width 0 ~ 320 4/4 Width of motion detection window.
win_i<0~2>_height 0 ~ 240 4/4 Height of motion detection window.
win_i<0~2>_objsize 0 ~ 100 4/4 Percent of motion detection window.
win_i<0~2>_sensitivity 0 ~ 100 4/4 Sensitivity of motion detection window.
Group: **motion_ c<0~(n-1)>_profile_i<0~(m-1)>** for n channel, m motion profile product (capability_nmotionprofile > 0)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
Enable <boolean> 4/4 enable motion detection
Policy day,
night,
schedule
4/4 When the condition match the policy, use this profile
Begintime hh:mm 4/4 If choose "schedule" mode as profile policy, the begin time of this profile when enabled
Endtime hh:mm 4/4 If choose "schedule" mode as profile policy, the end time of this profile when enabled
win_i<0~2>_enable <boolean> 4/4 enable motion window 1~3
win_i <0~2>_name string[14] 4/4 name of motion window 1~3
win_i <0~2>_left 0 ~ 320 4/4 Left coordinate of window position.
win_i <0~2>_top 0 ~ 240 4/4 Top coordinate of window position.
win_i <0~2>_width 0 ~ 320 4/4 Width of motion detection window.
win_i<0~2>_height 0 ~ 240 4/4 Height of motion detection window.
win_i<0~2>_objsize 0 ~ 100 4/4 Percent of motion detection window.
win_i<0~2>_sensitivity 0 ~ 100 4/4 Sensitivity of motion detection window.
Group: **tampering_c<0~(n-1)>** for n channel,
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 4/4 Enable or disable camera tampering detection
threshold 0 ~ 255 4/4 The sensitivity to judge if camera has been tampered
0: lowest sensitivity
255: highest sensitivity
duration 10 ~ 600 4/4 Judge camera has been tampered if exceeding this duration

Group: **ddns**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the dynamic dns.
provider Safe100,
DyndnsDynamic,
DyndnsCustom,
TZO,
DHS,
DynInterfree,
CustomSafe100
6/6 Safe100 => safe100.net
DyndnsDynamic => dyndns.org (dynamic)
DyndnsCustom => dyndns.org (custom)
TZO => tzo.com
DHS => dhs.org

DynInterfree =>dyn-interfree.it
CustomSafe100 =>
Custom server using safe100 method
<provider>_hostn
ame
string[128] 6/6 Your dynamic hostname.
<provider>_usern
ameemail
string[64] 6/6 Your user or email to login ddns service provider
<provider>_passw
ordkey
string[64] 6/6 Your password or key to login ddns service
provider
<provider>_server
name
string[128] 6/6 The server name for safe100.
(This field only exists for provider is
customsafe100)
Group: **upnppresentation**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the UPNP presentation service.
Group: **upnpportforwarding**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the UPNP port forwarding service.
upnpnatstatus 0~3 6/7 The status of UpnP port forwarding, used internally.
0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do
port forwarding
Group: **syslog**
NAME VALUE SECURITY DESCRIPTION

(get/set)
enableremotelog <boolean> 6/6 enable remote log
serverip <IP address> 6/6 Log server IP address
serverport 514, 1025~65535 6/6 Server port used for log
level 0~7 6/6 The levels to distinguish the importance of
information.
0: LOG_EMERG
1: LOG_ALERT
2: LOG_CRIT
3: LOG_ERR
4: LOG_WARNING
5: LOG_NOTICE
6: LOG_INFO
7: LOG_DEBUG
Group: **layout** (product dependent)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
Logo_default <boolean> 1/6 0 => Custom logo
1 => Default logo
logo_link string[64] 1/6 Hyperlink of the logo
theme_option 1~4 1/6 1~3: One of the default themes
4: Custom definition
theme_color_font string[7] 1/6 Font color
theme_color_configfont string[7] 1/6 Font color of configuration area
theme_color_titlefont string[7] 1/6 Font color of video title

theme_color_controlbackgroun
d
string[7] 1/6 Background color of control area
theme_color_configbackground string[7] 1/6 Background color of configuration area
theme_color_videobackground string[7] 1/6 Background color of video area
theme_color_case string[7] 1/6 Frame color
Group: **privacymask_c<0~(n-1)>** for n channel product
NAME VALUE SECURITY
(get/set)
DESCRIPTION

enable <boolean> 4/4 Enable the privacy mask
win_i<0~4>_enable <boolean> 4/4 Enable the privacy mask window
win_i<0~4>_name string[14] 4/4 The name of privacy mask window
win_i<0~4>_left 0 ~ 320/352 4/4 Left coordinate of window position.
win_i<0~4>_top 0 ~ 240/288 4/4 Top coordinate of window position.
win_i<0~4>_width 0 ~ 320/352 4/4 Width of privacy mask window
win_i<0~4>_height 0 ~ 240/288 4/4 Height of privacy mask window
win_i<0~4>_color 0 ~ 13 4/4 Color of privacy mask window
Group: **capability**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
api_httpversion 0200a 0/7 The HTTP API version.
bootuptime <positive integer> 0/7 The server bootup time
nir 0,
<positive integer>
0/7 number of IR interface
npir 0,
<positive integer>
0/7 number of PIR
ndi 0,
<positive integer>
0/7 number of digital input
ndo 0,
<positive integer>
0/7 number of digital output
naudioin 0,
<positive integer>
0/7 number of audio input
naudioout 0,
<positive integer>
0/7 number of audio output
nvideoin <positive integer> 0/7 number of video input
nmediastream <positive integer> 0/7 number of media stream per channel
nvideosetting <positive integer> 0/7 number of video settings per channel
naudiosetting <positive integer> 0/7 number of audio settings per channel
nuart 0,
<positive integer>
0/7 number of UART interface
nmotionprofile 0, 0/7 number of motion profiles

<positive integer>
ptzenabled < positive integer > 0/7 An 32-bits integer, each bit can be set
separately as follows:
Bit 0 => Support camera control function
0(not support), 1(support)
Bit 1 => Build-in or external camera.
0(external), 1(build-in)

Bit 2 => Support pan operation. 0(not
support), 1(support)
Bit 3 => Support tilt operation. 0(not
support), 1(support)
Bit 4 => Support zoom operation.
0(not support), 1(support)
Bit 5 => Support focus operation.
0(not support), 1(support)
Bit 6 => Support iris operation.
0(not support), 1(support)
Bit 7 => External or build-in PT. 0(build-in),
1(external)
Bit 8 => Invalidate bit 1 ~ 7.
0(bit 1 ~ 7 are valid),
1(bit 1 ~ 7 are invalid)
Bit 9 => Reserved bit; Invalidate lens_pan,
Lens_tilt, lens_zoon, lens_focus, len_iris.
0(fields are valid),
1(fields are invalid)
protocol_https < boolean > 0/7 indicate whether to support http over SSL
protocol_rtsp < boolean > 0/7 indicate whether to support rtsp
protocol_sip <boolean> 0/7 indicate whether to support sip
protocol_maxconnect
ion
<positive integer> 0/7 The maximum allowed simultaneous
connections
protocol_maxgencon
nection
<positive integer> 0/7 The maximum allowed general
simultaneous connections
protocol_maxmegaco
nnection
<positive integer> 0/7 The maximum allowed megapixel
simultaneous connections
protocol_maxrtspcon
nection
<positive integer> 0/7 The maximum allowed rtsp simultaneous
connections

protocol_rtp_multica
st_scalable
<boolean> 0/7 indicate whether to support scalable
multicast
protocol_rtp_multica
st_backchannel
<boolean> 0/7 indicate whether to support backchannel
multicast
protocol_rtp_tcp <boolean> 0/7 indicate whether to support rtp over tcp
protocol_rtp_http <boolean> 0/7 indicate whether to support rtp over http
protocol_spush_mjpe
g
<boolean> 0/7 indicate whether to support server push
motion jpeg
protocol_snmp <boolean> 0/7 indicate whether to support snmp
videoin_type 0, 1, 2 0/7 0 => Interlaced CCD
1 => Progressive CCD
2 => CMOS
videoin_resolution <a list of the
available resolution
separates by comma)

0/7 available resolutions list
videoin_maxframerat
e
<a list of the
available max frame
rate separates by
comma>
0/7 available framerate at the
videoin_resolution list index
videoin_codec <a list of the
available codec types
separates by comma)
0/7 available codec list
videoout_codec <a list of the
available codec types
separates by comma)
0/7 available codec list
transmission_mode Tx,
Rx,
Both
0/7 Indicate what kind of transmission mode
the machine used. TX: server, Rx: receiver
box, Both: DVR?.
network_wire <boolean> 0/7 Indicate whether to support the Ethernet
network_wireless <boolean> 0/7 Indicate whether to support the wireless
derivative_brand <boolean> 0/7 Indicate whether to support upgrade
function for the derivative brand. For
example, if the value is true, the VVTK
product can be upgraded to VVXX.
(TCVV<->TCXX is excepted)
evctrlchannel <boolean> 0/7 Indicate whether to support the http tunnel

for event/control transfer
joystick <boolean> 0/7 Indicate whether to support the joystick
control
Group: **event_i<0~2>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
enable 0, 1 6/6 To enable or disable this event.
priority 0, 1, 2 6/6 Indicate the priority of this event.
"0" indicates low priority.
"1" indicates normal priority.
"2" indicates high priority.
delay 1~999 6/6 Delay seconds before detect next event.
trigger boot,
di,
motion,
seq,
recnotify,
tampering
6/6 Indicate the trigger condition.
"boot" indicates system boot.
"di" indicates digital input.
"motion" indicates video motion detection.
"seq" indicates periodic condition.
"visignal" indicates video input signal loss
"recnotify" indicates space for recording media is full
"tampering" indicates camera tampering detected

di <integer> 6/6 Indicate which di detected.
This field is required when trigger condition is “di”.
One bit represents one digital input. The LSB indicates
DI 0.
mdwin <integer> 6/6 Indicate which motion detection windows detected.
This field is required when trigger condition is “md”.
One bit represents one window.
The LSB indicates the 1st window.
For example, to detect the 1st and 3rd windows, set
mdwin as 5.

mdwin0 <integer> 6/6 Indicate which motion detection windows of motion
profile 0 detected.
This field is required when trigger condition is “md”.
One bit represents one window.
The LSB indicates the 1st window.
For example, to detect the 1st and 3rd windows, set
mdwin as 5.
inter 1~999 6/6 Interval of period snapshot in minute.
This field is used when trigger condition is “seq”.
weekday <interger> 6/6 Indicate which weekday is scheduled.
One bit represents one weekday.
The bit0 (LSB) indicates Saturday.
The bit1 indicates Friday.
The bit2 indicates Thursday.
The bit3 indicates Wednesday.
The bit4 indicates Tuesday.
The bit5 indicates Monday.
The bit6 indicates Sunday.
For example, to detect events on Friday and Sunday,
set weekday as 66.
begintime hh:mm 6/6 Begin time of weekly schedule.
endtime hh:mm 6/6 End time of weekly schedule.
(00:00 ~ 24:00 means always.)
lowlightcondition 0, 1 6/6 Turn on IR led in some condition:
0: all conditions
1: low light condition
action_do_i<0~(ndo-1
)>_enable
0, 1 6/6 To enable or disable trigger digital output.
action_do_i<0~(ndo-1
)>_duration
1~999 6/6 The duration of digital output is triggered in seconds.
action_server_i<0~4>
_enable
0, 1 6/6 To enable or disable this server action.
The default value is 0.
action_server_i<0~4>
_media
NULL, 0~4 6/6 The index of attached media.
action_server_i<0~4>
__datefolder
<boolean> 6/6 Enable or disable create folders by date time and hour
automatically
Group: **server_i<0~4>**

PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION

name string[40] 6/6 The identification of this entry
type email,
ftp,
http,
ns
6/6 Indicate the server type.
"email" is email server.
"ftp" is ftp server.
"http" is http server.
"ns" is network storage.
http_url string[128] 6/6 The url of http server to upload.
http_username string[64] 6/6 The username to login in the server.
http_passwd string[64] 6/6 The password of the user.
ftp_address string[128] 6/6 The ftp server address
ftp_username string[64] 6/6 The username to login in the server.
ftp_passwd string[64] 6/6 The password of the user.
ftp_port 0~65535 6/6 The port to connect the server.
ftp_location string[128] 6/6 The location to upload or store the media.
ftp_passive 0, 1 6/6 To enable or disable the passive mode.
0 is to disable the passive mode.
1 is to enable the passive mode.
email_address string[128] 6/6 The email server address
email_sslmode <boolean> 6/6 To enable or disable the SSL mode
0 is to disable the SSL mode
1 is to enable the SSL mode
email_username string[64] 6/6 The username to login in the server.
email_httpsmode 0, 1 6/6 Enable support SSL
email_port 0~65535 6/6 The port to connect the server.
email_passwd string[64] 6/6 The password of the user.
email_senderemail string[128] 6/6 The email address of sender.
email_recipientemail string[128] 6/6 The email address of recipient.
ns_location string[128] 6/6 The location to upload or store the media.
ns_username string[64] 6/6 The username to login in the server.
ns_passwd string[64] 6/6 The password of the user.
ns_workgroup string[64] 6/6 The workgroup for network storage.

Group: **media_i<0~4>**(media_freespace is used internally.)
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
type snapshot,
systemlog
videoclip
6/6 The media type to send to the server or store by the server.
snapshot_source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
snapshot_prefix string[16] 6/6 Indicate the prefix of the filename.
snapshot_datesuffix 0, 1 6/6 To add date and time suffix to filename or not.
1 means to add date and time suffix.
0 means not to add it.
snapshot_preevent 0 ~ 7 6/6 It indicates the number of pre-event images.
snapshot_postevent 0 ~ 7 6/6 The number of post-event images.
videoclip_source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
videoclip_prefix string[16] 6/6 Indicate the prefix of the filename.
videoclip_preevent 0 ~ 9 6/6 It indicates the time of pre-event recording in seconds.

videoclip_maxduration 1 ~ 10 6/6 The time of maximum duration of one video clip in seconds.
videoclip_maxsize 50 ~ 600 6/6 The maximum size of one video clip file in Kbytes.
Group: **recording_i**<0~1>
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
enable 0, 1 6/6 To enable or disable this recoding.
priority 0, 1, 2 6/6 Indicate the priority of this recoding.
"0" indicates low priority.
"1" indicates normal priority.
"2" indicates high priority.

source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
weekday <interger> 6/6 Indicate which weekday is scheduled.
One bit represents one weekday.
The bit0 (LSB) indicates Saturday.
The bit1 indicates Friday.
The bit2 indicates Thursday.
The bit3 indicates Wednesday.
The bit4 indicates Tuesday.
The bit5 indicates Monday.
The bit6 indicates Sunday.
For example, to detect events on Friday and Sunday, set
weekday as 66.
begintime hh:mm 6/6 Begin time of weekly schedule.
endtime hh:mm 6/6 End time of weekly schedule.
(00:00~24:00 means always.)
prefix string[16] 6/6 Indicate the prefix of the filename.
limitsize 0,1 6/6 0: Entire free space mechanism
1: Limit recording size mechanism
cyclesize 16~ 6/6 The maximum size for cycle recording in Kbytes when choose limit recording size.
cyclic 0,1 6/6 0: Disable cyclic recording
1: Enable cyclic recording
notify 0,1 6/6 0: Disable recording notification
1: Enable recording notification
notifyserver 0~31 6/6 Indicate which notification server is scheduled.
One bit represents one application server (server_i0~i4).
The bit0 (LSB) indicates server_i0.
The bit1 indicates server_i1.
The bit2 indicates server_i2.
The bit3 indicates server_i3.
The bit4 indicates server_i4.
For example, enable server_i0, server_i2 and server_i4 to be
notification server. The notifyserver value is 21.
clearamount 10~ 6/6 The clear amount in Mbytes when choose cyclic recording mechanism.

reserveamount 15~ 6/6 The reserve amount in Mbytes when choose cyclic recording mechanism.
dest cf,
0~4
6/6 The destination to store the recording data.
"cf" means CF card.
"0~4" means the index of network storage.

cffolder string[128] 6/6 folder name.
Group: **custom_i<0~2>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of customize event script file.
Group: **path**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
encoder1_start <boolean> 7/7 Specify the http push server is active for stream 1
encoder2_start <boolean> 7/7 Specify the http push server is active for stream 2
Group: **https** (product dependent)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
connect 1025 ~ 65535 7/7 Specify the stunnel connect port
enable <boolean> 6/6 To enable or disable this secure http
policy <Boolean> 6/6 If the value is 1, it will force http connection redirect to https connection
method auto,
manual,
install
6/6 auto => Create self-signed certificate automatically
manual => Create self-signed certificate manually
install => Create certificate request and install
status -2 ~ 1 6/6 Specify the https status.
-2=>invalid public key
-1=>waiting for certificated
0=>not installed
1=>active
countryname string[2] 6/6 country name in certificate information
stateorprovince
name
string[128] 6/6 state or province name in in certificate information

localityname string[128] 6/6 the locality name in certificate information
organizationna
me
string[64] 6/6 organization naem in certificate information
unit string[32] 6/6 organizational unit name in certificate information
commonname string[64] 6/6 common name in certificate information
validdays 0 ~ 9999 6/6 certificatation valid period

Query status of the digital input

Note: This request requires the privilege of viewer.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0]
If no parameter is specified, all the status of digital input will be returned.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <*length*>\r\n
\r\n
[di0=<*state*>]\r\n
where <*state*> can be 0 or 1.
Example: Query the status of digital input 1
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di0

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di0=1\r\n

Capture single snapshot

Note: This request require normal user privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
If the user requests the size larger than all stream setting on the server, this request will failed!
PARAMETER VALUE DEFAULT DESCRIPTION
channel 0~(n-1) 0 the channel number of video source
resolution <available
resolution>
0 The resolution of image
quality 1~5 3 The quality of image
Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and
quality of image will be set according to the video settings on the server.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]
<binary JPEG image data>

Account management

Note: This request requires administrator privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][...][&return=<*return page*>]

PARAMETER VALUE DESCRIPTION
Add Add an account to server. When using this method, "username"
field is necessary. It will use default value of other fields if not
specified.
Delete Remove an account from server. When using this method,
"username" field is necessary, and others are ignored.
method
edit Modify the account password and privilege. When using this
method, "username" field is necessary, and other fields are
optional. If not specified, it will keep original settings.
username <name> The name of user to add, delete or edit
userpass <value> The password of new user to add or that of old user to modify.
The default value is an empty string.
<value> The privilege of user to add or to modify.
viewer viewer's privilege
operator operator's privilege
privilege
admin administrator's privilege
return <return page> Redirect to the page <*return page*> after the parameter is
assigned. The <*return page*> can be a full URL path or relative
path according the the current path. If you omit this parameter,

it will redirect to an empty page.

System logs

Note: This request require administrator privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/syslog.cgi
Server will return the up-to-date system log.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n

\r\n
<system log information>\r\n

Upgrade firmware

Note: This request requires administrator privilege
Method: POST
Syntax:
http://<*servername*>/cgi-bin/admin/upgrade.cgi
Post data:
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
Server will accept the upload file named <file name> to be upgraded the firmware and return with <return
page> if indicated.

System Information

Note: This request requires normal user privilege (obsolete)
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/sysinfo.cgi
Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All the fields
in the previous version (0100) is obsolete. Please use "getparam.cgi?capability" instead.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n

CapVersion=0200\r\n
PARAMETER(supported
capability version)
VALUE DESCRIPTION
Model system.firmwareversion Model name of server.
Ex:IP3133-VVTK-0100a
CapVersion MMmm, MM is major version from 00 ~ 99
mm is minor version from 00 ~ 99
ex: 0100
The capability field version

IP filtering

Note: This request requires administrator access privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>]

[&return=<return page>]
PARAMETER VALUE DESCRIPTION
addallow Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
adddeny Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
Method
deleteallow Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.

deletedeny Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start <ip address> The start IP address to add or to delete.
end <ip address> The end IP address to add or to delete.
index <value> The start position to add or to delete.
return <return page> Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Event/Control HTTP tunnel channel

Note: This request requires admin privilege
Method: GET and POST
Syntax:
http://<*servername*>/cgi-bin/admin/ctrlevent.cgi

GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie
in the GET and POST should be the same to be recognized as a pair for one session. The contents of

upstream should be base64 encoded to be able to pass through some proxy server.
This channel will help to do real-time event notification and control. The event and control format are
described in another document.

Get SDP of Streamings

Note: This request requires viewer access privilege
Method: GET/POST

Syntax:
http://<*servername*>/<network_rtsp_s<0~m-1>_accessname>
"m" is the stream number.
"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the
"subgroup of network: rtsp" for setting the accessname of SDP.
You can get the SDP by HTTP GET method.

Open the network streamings

Note: This request requires viewer access privilege
Syntax:
For http push server (mjpeg):
http://<*servername*>/<network_http_s<0~m-1>_accessname>
For rtsp (mp4), user needs to input the url below for a rtsp compatible player.
rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>
"m" is the stream number.
For detailed streaming protocol, please refer to "control signaling" and "data format" documents.

Technical Specifications

Ver. 0.2
Distributed by:
6F, NO.192, Lien-cheng Rd.,Chung-Ho, Taipei County, Taiwan
T: +886 2 82455282 F: +886 2 82455532 E: Sales@vivotek.com

. CPU: VVTK-1000 SoC
. Flash: 8 MB
. RAM: 32 MB
. Embedded OS: Linux 2.4
. Board lens, dual-band, f= 4.0 mm, F1.8, Fixed
. IR corrected
. 56° (horizontal)
. 42° (vertical)
. 71° (diagonal)
. 1/5 sec. to 1/15000 sec.
. 1/4" CMOS sensor in VGA resolution
. 0 Lux / F1.8 (IR LED on)
. IR LED x 12 (850 nm)
. Effective up to 10 meters
Networking
Alarm and
Event Management
Security
Users
Dimension
Weight
LED Indicator
Power
System
Lens
Angle of View
Shutter Time
Image Sensor
Minimum Illumination
IR Illuminators
Video
Image Settings
. 10/100 Mbps Ethernet, RJ-45
. Protocols: IPv4, TCP/IP, HTTP, HTTPS, UPnP,
RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP,
NTP, DNS, DDNS, and PPPoE
. Triple-window video motion detection
. Tamper detection
. One D/I for external sensor

. Event notification using HTTP, SMTP, or FTP
. Local recording of MP4 file
. Multi-level user access with password protection
. IP address filtering
. HTTPS encrypted data transmission
. Camera live viewing for up to 5 clients
. Ø59.4 mm x 150 mm
. Net: 630 g
. System restore status indicator

Operating Environments

. Temperature: -20 ~ 50 °C (-4 ~ 122 °F)
. Humidity: 90% RH
. 12V DC
. 24V AC
. Power consumption: Max. 4 W with IR LED on
. 802.3af compliant Power-over-Ethernet

Housing . Weather-proof IP66-rated housing

Approvals . CE, LVD, FCC, VCCI, C-Tick
. Compression: MJPEG & MPEG-4
. Streaming:
Simultaneous dual-stream
MPEG-4 streaming over UDP, TCP, HTTP, or HTTPS
MPEG-4 multicast streaming
MJPEG streaming over HTTP or HTTPS
. Supports 3GPP mobile surveillance
. Frame rates:
MPEG-4: 640x480 up to 30/25fps
MJPEG: 640x480 up to 30/25fps
. Adjustable image size, quality, and bit rate
. Time stamp and text caption overlay
. Flip & mirror
. Configurable brightness, saturation contrast, sharpness and white balance
. AGC, AES
. Automatic, manual or scheduled day/night mode
. Supports privacy masks

Viewing System Requirements

Installation, Management, and Maintenance Applications

. OS: Microsoft Windows 2000/XP/Vista
. Browser: Internet Explorer 6.x or above
. Cell phone: 3GPP player
. Real Player 10.5 or above
. Quick Time 6.5 or above
. SDK available for application development and system integration
. Installation Wizard 2
. 16-CH recording software
. Supports firmware upgrade

Warranty . 12 months

PC with Recording Software
Router
Notebook with Web Browser
3G Cell Phone

IP7330

Ethernet 10/100

RJ45 Plug

Power Cord

Socket (Black)

General I/O

Terminal Block

IR LED Lens

Light Sensor

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY
NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU
MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO
HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE
PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE
WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT
WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/
OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO.
NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION
INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY
BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH
RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA
CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621;
CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621;
GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621;

SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT.
9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK
PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP.
8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO
TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT
HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired
operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant
to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against
harmful interference when the equipment is operated in a commercial environment. This equipment
generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance
with the installation manual, may cause harmful interference to radio communications. Operation of this
equipment in a residential area is likely to cause harmful interference, in which case the user will be
required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which

case the user may be required to take adequate measures.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right
to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty
of any kind with regard to the material contained within this document, including, but not limited to, the
implied warranties of merchantability and fitness for any particular purpose.

Table of Contents

Overview

VIVOTEK FD7131 is a full-featured 3-axis dome network camera designed for indoor
surveillance. It comes with a wide-angle, vari-focal lens, allowing you to have a wide open
view for maximum coverage. With the sophisticated 3-axis mechanical and industrial design,
it offers a very flexible, easy hardware installation for either ceiling or wall mount. To prevent
false alarms, it is also equipped with a PIR (Passive Infrared) sensor, which can detect motion
causing temperature changes in the infrared range emitted by surrounding objects. When the
environment is short of sufficient light source, the built-in white-light illuminators will be activated
automatically or manually so as to supplement the low light situation without additional equipment.
Embedded with VIVOTEK VVTK-1000 SoC, it simultaneously delivers dual streams with

different resolutions up to 30fps in VGA resolution and video qualities upon different multimedia
devices for real-time viewing. Additionally, by offering more advanced features such as 3GPP
mobile surveillance, built-in 802.3af compliant PoE, two-way audio, and so on, FD7131 allows
users to build up a powerful, cost-effective IP surveillance system for various indoor applications
with ease.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera
is not only a high-performance web-ready camera but can also be part of a flexible surveillance
system. It is the user's responsibility to ensure that the operation of such devices is legal before
installing this unit for its intended use.
It is important to first verify that all contents received are complete according to the Package
Contents listed below. Take note of the warnings in the Quick Installation Guide before the
Network Camera is installed; then carefully read and follow the instructions in the Installation
chapter to avoid damage due to faulty assembly and installation. This also ensures the product
is used properly as intended.
The Network Camera is a network device and its use should be straightforward for those who
have basic networking knowledge. It is designed for various applications including video sharing,
general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the

Network Camera and ensure proper operations. For creative and professional developers, the
URL Commands of the Network Camera section serves as a helpful reference to customizing
existing homepages or integrating with the current web server.

Package Contents

- FD7131
- Power Adapter
- Software CD
- Alignment Sticker
- Warranty Card
- Quick Installation Guide
- Screwdriver
- Screws and I/O Connector

Physical Description

General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external
input / output devices. The pin definitions are described below.

1 2 3 4

1: Power
2: Digital output
3: Digital input
4: Ground

Lens
Tilt Screw
Built-in MIC
PIR Sensor
White-light LEDs
Power Cord Socket
Indented Reset Button Ethernet 10/100 RJ45 Socket

1 2 3 4 Audio Out Mic. In Ext. Int.

Focus Controller
Zoom Controller

General I/O Terminal Block

Audio Out

MIC in

External/Internal MIC Switch

Keep a note of the MAC address

before installing the camera.

Drill Holes

Pan Screw

Dome Cover

Image Adjustment Screw

Status LED

DI/DO Diagram

Refer to the following illustration for the connection method.

12V

+12V

Digital output

PIN 1

Power+12V

PIN 2

Digital input

PIN 3

Ground

PIN 4

Status LED

The LED indicates the status of the Network Camera.

Description Status LED

Blinking green and orange (twice) Power on or reset

Non light During booting procedure

Steady orange till IP address is confirmed Detecting and setting network

Blinking orange and red continuously After network is setup (system up)

Rapidly blink orange till firmware is upgraded During the upgrade firmware process

Hardware Reset

The reset button is used to reset the system or restore the factory default settings. Sometimes

resetting the system can return the camera to normal operation. If the system problems remain
after reset, restore the factory settings and install again.
Reset: Press and release the indented reset button with a paper clip or thin object. Wait for the
Network Camera to reboot.
Restore: Press and hold the reset button until the status LED rapidly blinks. It takes about 30
seconds. Note that all settings will be restored to factory default. Upon successful restore, the
status LED will blink green and red during normal operation.

Installation

Hardware Installation

1. Use the supplied screwdriver to detach the dome cover from the camera base. Then, follow
the steps below to install the camera; either to a ceiling or to a wall.

Installation Tips

Before installing the camera, look for a spot that best suits your needs. The built-in PIR sensor
is designed to be triggered when a person enters its detection range. Therefore, it is crucial to
install the camera at a place with the PIR sensor facing the desired direction. (The sensitivity
of PIR sensor depends on object size and temperature differences between the object and the
background environment.)

I/O

Audio 1 2 3 4 Out Mic. In Ext. Int.

Indented Reset Button

Status LED

3. Feed power to the Network Camera and connect it to the Internet. For more information,

please refer to Network deployment on page 9 for details.

4. Install the “Installation Wizard 2“ to assign IP address to the Network Camera. For more

information, please refer to Software installation on page 12 for details.

5. Access to the Network Camera from the Internet. For more information, please refer to

Accessing the Network Camera on page 13 for details.

6. Based on the live image retrieved from the camera, adjust the camera lens as following steps.

To adjust the viewing angle

■ Loosen the pan screw, then turn the lens module left and right. Upon completion,

tighten the pan screw.

■ Loosen the tilt screws on both side of the camera, then turn the lens module up and

down. Upon completion, tighten the tilt screws.

■ Loosen the image adjustment screw, then turn the lens to adjust the image orientation.

Upon completion, tighten the image adjustment screw.

When mounting to a ceiling

Through the two holes on each side of the camera base,

insert the supplied two screws to corresponding holes and

secure them with a screwdriver.

When mounting to a wall

■ Attach the alignment sticker to the wall.

■ Through the two circles on the sticker, drill two pilot holes into the wall.

■ Hammer the supplied plastic anchors into the holes.

■ Align the two holes on each side of the camera base with the two plastic anchors on the wall, insert the supplied screws to corresponding holes and secure them with a screwdriver.

Rotate the screw

Turn the lens

To adjust the zoom factor and focus range

■ Loosen the zoom controller, then adjust zoom factor by moving the controller left and

right. Upon completion, tighten the zoom controller.

■ Loosen the focus controller, then adjust focus range by moving the controller left and

right. Upon completion, tighten the focus controller.

7. Attach the dome cover to camera. Secure the two dome screws with a screwdriver.

Finally, make sure all parts of the camera are securely installed.

DO NOT over tighten the controllers.
Doing so can damage the structure
of camera lens.
The supplied screwdriver is exclusively
designed to match the dome screws. In
case you will need to adjust the lens at a
later time, do not discard the screwdriver.

Network Deployment

Setting up the Network Camera over the Internet

This section explains how to configure the Network Camera to an Internet connection.

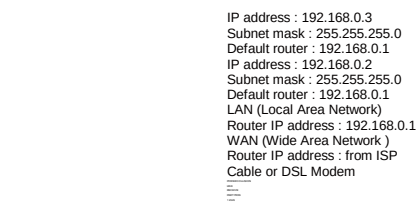
1. If you have external devices such as sensors and alarms, make the connection from the
general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the supplied power cable from the Network Camera to a power outlet.
There are several ways to set up the Network Camera over the Internet. The first way is to set
up the Network Camera behind a router. The second way is to utilize a static IP. The third way is
to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow
the steps below.
1. Connect your Network Camera behind a router, the Internet environment is illustrated below.
Regarding how to obtain your IP address, please refer to Software installation on page 12 for
details.

Ethernet Switch

1: Power
2: Digital output
3: Digital input
4: Ground



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is
192.168.0.3, please forward the following ports for the Network Camera on the router.

- HTTP port
- RTSP port
- RTP port for audio
- RTCP port for audio
- RTP port for video
- RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly
on your router. For information on how to forward ports on the router, please refer to your
router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider).
Use the public IP and the secondary HTTP port to access the Network Camera from the
Internet. Please refer to Network Type on page 33 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera.
Please refer to LAN on page 33 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to
PPPoE on page 34 for details.

Set up the Network Camera through Power over Ethernet (PoE)

When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet

cable. If your switch/router supports PoE, refer to the following illustration to connect the

Network Camera to a PoE-enabled switch/router.

When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect

between the Network Camera and a non-PoE switch/router.

PoE Switch

non-PoE Switch

PoE Power Injector

(optional)

power + data transmission

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up

your Network Camera on the LAN.

1. Install the IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.
2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.
3. The program will search all VIVOTEK devices on the same LAN.
4. After searching, the main installer window will pop up. Click on the MAC and model name

which matches the product label on your device to connect to the Network Camera via

Internet Explorer.

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players,
3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:

1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as
shown below. Follow the instructions to install the required plug-in on your computer.

NOTE

► For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live
video. If you donn't have Quick Time on your computer, please download it first, then launch
the web browser.

► By default, the Network Camera is not password-protected. To prevent unauthorized access,
it is highly recommended to set a password for the Network Camera. For more information
about how to enable password protection, please refer to Security on page 27.

► If you see a dialog box indicating that your security settings prohibit running ActiveX®
Controls, please enable your ActiveX® Controls for your browser.

1. Choose Tools > Internet Options > Security > Custom Level.
2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.
3. Refresh your web browser, then install the Active X® control. Follow the instructions to
complete installation.

Using RTSP Players

To view the MPEG-4 streaming media using RTSP players, you can use one of the following
players that support RTSP streaming.

Quick Time Player
Real Player
VLC media player
mpegable Player
pvPlayer

As most ISPs and players only allow RTSP streaming through port number 554, please set the
RTSP port to 554. For more information, please refer to RTSP Streaming on page 42.

For example:

4. The live video will be displayed in your player.

For more information on how to configure RTSP access name, please refer to RTSP
Streaming on page 42 for details.

rtsp://192.168.5.151:554/live.sdp

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.

3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for
stream1 or stream2>

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network
Camera can be accessed over the Internet. For more information on how to set up the Network
Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 9.
To utilize this feature, please check the following settings on your Network Camera:
1. Because most players on 3GPP mobile phones do not support RTSP authentication, make
sure the authentication mode of RTSP streaming is set to disable.
For more information, please refer to RTSP Streaming on page 42.
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size.
Please set the video and audio streaming parameters as listed below.
For more information, please refer to Audio and Video on page 49.
Video Mode MPEG-4
Frame size 176 x 144
Maximum frame rate 5 fps
Intra frame period 1S
Video quality (Constant bit rate) 40kbps
Audio type (GSM-AMR) 12.2kbps
3. As most ISPs and players only allow RTSP streaming through port number 554, please set
the RTSP port to 554. For more information, please refer to RTSP Streaming on page 42.
4. Launch the players on 3GPP-compatible mobile devices (ex. Real Player).
5. Type the following URL commands in the player.

The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming
access name for stream1 or stream2>.
For example:
rtsp://192.168.5.151:554/live.sdp

Using VIVOTEK Recording Software

The product software CD also contains recording software, allowing simultaneous monitoring
and video recording for multiple Network Cameras. Please install the recording software; then
launch the program to add the Network Camera to the Channel list. For detailed information
about how to use the recording software, please refer to the user's manual of the software or
download it from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections:
VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live
Video Window.

VIVOTEK INC. Logo

Click this logo to visit VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page
25.

Camera Control Area

Video Stream: This Network Cmera supports MJPEG or MPEG-4 dual streams simultaneously. You can
select either one for live viewing.
Digital Output: Click to turn the digital output device on or off.

White-light illuminators: Click to turn on the White-light LEDs for 20 seconds.

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to
Client Settings on page 22.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested
that a password be applied to the Network Camera so that only the administrator can configure the
Network Camera. For more information, please refer to Configuration on page 24.

Language: Click this button to choose a language for the user interface. Language options are available
in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

VIVOTEK INC. Logo
Live View Window
Camera Control Area
Configuration Area
Host Name

Live Video Window

■ The following window is displayed when the video mode is set to MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video Settings on
page 49.

MPEG-4 Protocol and Media Options: The transmission protocol and media options for MPEG-4 video
streaming. For further configuration, please refer to Client Settings on page 22.

Time: Display the current time. For further configuration, please refer to Video settings on page 49.

Title and Time: Video title and time can be stamped on the streaming video. For further configuration,
please refer to Video settings on page 49.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera
configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed
in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP
(*.bmp) format.
Digital zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation
screen indicates which part of the image being magnified. To control the zoom level, drag the slider bar.
To move to a different area you want to magnify, drag the navigation screen.
Pause: Pause the transmission of the streaming media. The button becomes the Resume button
after clicking the Pause button.
Stop: Stop the transmission of streaming media. Click the Resume button to continue transmission.
Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press
the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops
accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on
page 23 for details.
Video and Audio Control Buttons
MPEG-4 Protocol and Media Options
Video Title Time
Title and Time

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the
local computer.
Mute: Turn off the volume at local computer. The button becomes the Audio On button after
clicking the Mute button.
Talk: Click this button to talk to people around the Network Camera. Audio will project from

the external speaker connected to the Network Camera. Click this button again to end talking
transmission.
Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume at local computer.
Mute: Turn off the Mic volume at local computer. The button becomes the Mic On button
after clicking the Mute button.
Full Screen: Click this button to switch to full screen mode. Press “Esc” key to switch back to normal
mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Video Settings on
page 49.
Time: Display the current time. For more information, please refer to Video Settings on page 49.
Title and Time: Video title and time can be stamped on the streaming video. For more information, please
refer to Video Settings on page 49.
Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera
configuration, some buttons may not be available.
Snapshot: Click this button to capture and save still images. The captured images will be displayed
in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP
(*.bmp) format.

Video Title Time
Title and Time
Video Control Buttons

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation

screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To
move to a different area you want to magnify, drag the navigation screen.
Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer.
Press the Stop MP4 recording button to end recording. When you exit the web browser, video
recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving
Options on page 23 for details.
Full Screen: Click this button to switch to full screen mode. Press “Esc” key to switch back to normal
mode.

Client Settings

This chapter explains how to select the stream transmission mode and saving options on the
local computer. When completed with the settings on this page, click **Save** on the page bottom
to enable the settings.

MPEG-4 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options

Depending on your network environment, there are four transmission modes of MPEG-4 streaming:
UDP unicast: This protocol allows for more real-time audio and video streams. However, network
packets may be lost due to network burst traffic and images may be broken. Activate UDP connection
when occasions require time-sensitive responses and the video quality is less important. Note that each
unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up

to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients
requesting streaming media. This helps to reduce the network transmission load of the Network Camera
while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera
must be configured to enable multicast streaming at the same time. For more information, see RTSP
Streaming on page 34.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video
quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for
streaming under some network environments. Users inside a firewall can utilize this protocol to allow
streaming data through.

MP4 Saving Options

Users can record the live video as they are watching it by clicking Start MP4 Recording on the main
page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

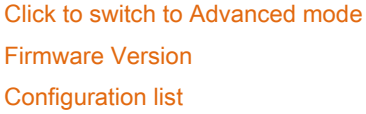
Add date and time suffix to the file name: Select this option to append the date and time to the end of the
file name.

CLIP_20080108-180853
Date and time suffix
The format is: YYYYMMDD_HHMMSS
File name prefix

Configuration

Click **Configuration** on the main page will enter the camera setting pages. Note that only
Administrators can access the configuration page.
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with
minimal effort. To simplify the setting procedure, two types of user interfaces are available:
Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced
functions (ex. HTTPS/ Access list/ Homepage layout/ Application/ Recording/ System log/ View
parameters...) are not displayed in Basic Mode.
If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the
configuration list to quickly switch to Advanced Mode.
In order to simplify the user interface, the detailed information will be hidden unless you click
on the function item. When you click on the first sub-item, the detailed information for the first
subitem will be displayed; when you click on the second sub-item, the detailed information for
the second sub-item will be displayed and that of the first sub-item will be hidden.
The following is the interface of the Basic Mode and the Advanced Mode:

Basic mode



Advanced Mode

Each function on the configuration list will be explained in the following sections. Those functions

that are displayed only in Advanced Mode are marked with Advanced Mode . If you want to set
up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to
quickly switch over.

System

This section explains how to configure the basic settings for the Network Camera, such as the
host name and system time. It is composed of the following three columns: System, System
Time and DI and DO. When completed with the settings on this page, click **Save** at the bottom
of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the
main page.
Turn off the LED indicators: If you don't want to let others know that the network camera is working, you
can select this option to turn off the LED indicators.

Click to switch to Basic mode
Firmware Version
Configuration list

System Time

Keep current date and time: Select this option to preserve the current date and time of the Network
Camera. The Network Camera's internal real-time clock maintains the date and time even when the
power of the system is turned off.
Sync with computer time: Select this option to synchronize the date and time of the Network Camera with
the local computer. The read-only date and time of the PC is displayed as updated.
Manual: The administrator can enter the date and time manually. Note that the date and time format are

[yyyy/mm/dd] and [hh:mm:ss].
Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically
querying an NTP Server.
NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank
connects the Network Camera to the default time servers.
Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly
basis.
Time zone Advanced Mode : Select the appropriate time zone from the list. If you want to upload
Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving
Time Configuration File on page 80 for details.

DI and DO

Digital input: Select High or Low to define normal status of the digital input. The Network Camera will
report the current status.
Digital output: Select Grounded or Open to define normal status of the digital output. The Network
Camera will show whether the trigger is activated or not.

Security

This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add
more accounts in Manage User column, please apply a password for the “root” account first.
1. Type the password identically in both text boxes, and click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their

respective fields to access the Network Camera.

Manage Privilege Advanced Mode

Digital Output & IR illuminators: You can modify the manage privilege of operators or viewers. Check or
uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will
also have the ability to control the Network Camera through the main page. (Please refer to Main Page
on page 18.)

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a
User ID and Password.

Manage User

Administrators can add up to 20 user accounts.

1. Input the new user's name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the settings.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can
access the Configuration page. Though operators cannot access the Configurationpage, they can use
the URL Commands to get and set the value of parameters. For more information, please refer to URL
Commands of the Network Camera on page 83. Viewers access only the main page for live viewing.

Here you also can change a user's access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes, then click **Update** or **Delete** to enable the settings.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL
(Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher

security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS"
or "HTTPS only". Note that you have to create and install certificate first in the second column before
clicking the **Save** button.

Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first.

There are three ways to create and install a certificate:

Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: “HTTP
& HTTPS” or “HTTPS only”.
3. Click **Save** to generate a certificate.

4. The Certificate Information will automatically de displayed in the third column as shown below. You can
click **Property** to view detailed information about the certificate.
5. Click **Home** to return to the main page. Change the address from “http://” to “https://“ in the address
bar and press Enter on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable
HTTPS.

https://192.168.5.151/index.html

https://

Create self-signed certificate manually

1. Select this option.
2. Click **Create** to open a Create Certificate page, then click **Save** to generate the certificate.
3. The Certificate Information will automatically be displayed in the third column as shown below. You
can click **Property** to see detailed information about the certificate.

Create certificate and install : Select this option if you want to create a certificate from a certificate
authority.
1. Select this option.
2. Click **Create** to open a Create Certificate page, then click **Save** to generate the certificate.

3. If you see the following Information Bar, click **OK** and click on the Information bar on the top of the
page to allow pop-ups.
4. The Pop-up window shows an example of a certificate request.

5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera.
Wait for the certificate authority to issue a SSL certificate; click **Browse...** to search for the issued
certificate, then click **Upload** in the second column.

NOTE

► How to cancel HTTPS settings?

1. Uncheck **Enable HTTPS secure connection** in the first column, then click **Save**, then a warning
dialog will pop up.
2. Click **OK** to disable HTTPS.
3. The webpage will redirect to a non-HTTPS page automatically.

► If you want to create and install other certificates, please remove the existing one. To remove the
signed certificate, uncheck **Enable HTTPS secure connection** in the first column and click **Save**.
Then click **Remove** to erase the certificate.

Network

This section explains how to configure wired network connection for the Network Camera.

Network Type

LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended
to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click
Save when you complete the Network Settings.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by
the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.

1. You can make use of VIVOTEK installation wizard 2 on the software CD to easily set up the Network
Camera on LAN. Please refer to Software installation on page 12 for details.
2. Enter the static IP, Subnet mask, Default router, Primary DNS provided by your ISP.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera
so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras
will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently,
UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the
UPnP™ component is installed on your computer.

Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to
allow the Network Camera to open ports on the router automatically so that video streams can be sent
out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as

there is an Internet connection. Note that to utilize this feature, it requires an account provided by your
ISP.
Follow the steps below to acquire your Network Camera's public IP address.
1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page
67) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 70). Select
System log so that you will receive the system log in TXT file format which contains the Network
Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password
provided by your ISP. Click **Save** to enable the settings.
5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

NOTE

► If the default ports are already used by other devices connected to the same router, the Network
Camera will select other ports for the Network Camera.

► If UPnPTM is not supported by your router, you will see the following message:

Error: Router does not support UPnP port forwarding.

Network Camera (192.168.5.151)

► Steps to enable UPnP™ user interface on your computer:

Note that you must log on to the computer as a system administrator to install the UPnP™ components.

1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.

4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.

5. Click **Next** in the following window.

6. Click **Finish**. UPnP™ is enabled.

► How does UPnP™ work?

UPnPTM networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

► Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 79 for details. After the Network Camera is reset to factory default, it is accessible on the LAN.

Enable IPv6

Select this option and click **Save** to enable IPv6 settings.

Please note that this only works if your network environment and hardware equipment support IPv6. The

browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

When IPv6 is enabled, by default, the network camera will listen to router advertisements and be

assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

If your IPv6 settings are successful, the IPv6 address list will listed in the pop-up window. The IPv6

address will be displayed as follows:

Link-global IPv6 address/network mask

Link-local IPv6 address/network mask

Refers to Ethernet

Please follow the steps below to link to IPv6 address:

1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.

For example:

NOTE

► If you have the Secondary HTTP port (the default value is 8080), you can also link to the webpage in

the following address format: (Please refer to **HTTP** on page 39 for detailed information.)

► If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6

information column as shown below.

Manually setup the IP address: Select this option to manually set up IPv6 settings if your network

environment does not have DHCPv6 server and router advertisements-enabled routers.

If you check this item, the following blanks will be displayed for you to enter the corresponding
information:

http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/
IPv6 address
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080
IPv6 address Secondary HTTP port

HTTP Advanced Mode

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first;
please refer to Security on page 27 for details.

Authentication: Depending on your network security requirements, the Network Camera provides two
types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential
risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5
algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is
set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are
incorrectly assigned, the following warning messages will be displayed:

To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used
to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP
port is set to 8080, refer to the list below for the Network Camera's IP address.

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the
streaming source.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to

JPEG, users will receive video comprised of continuous JPEG images. This technology, known as “server
push”, allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

In LAN

http://192.168.4.160 or

http://192.168.4.160:8080

URL command -- http://<ip address>:<http port>/<access name for stream1 or stream2>

For example, when the Access name for stream 2 is set to video2.mjpg:

1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

NOTE

► Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.

HTTPS

By default, the HTTPS port is set to 443. It also can be assigned with another port number between 1025
and 65535.

Two Way Audio

By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number
between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive
audio simultaneously. By using the Network Camera’s built-in or external microphone and an external
speaker, you can communicate with people around the Network Camera.

http://192.168.5.151/video2.mjpg

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio

function, make sure the video mode is set to “MPEG-4” on the Audio and Video Settings page and the
media option is set to “Video and Audio” on the Client Settings page. Please refer to Client Settings on
page 22 and Audio and Video Settings on page 49.
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP

The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK Installation Wizard
2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to
another port number between 1025 and 65535.

Audio send from operators
Audio send to operators
America Taiwan

Mute

Audio is being transmitted to the Network Camera

Talk Button Mic Volume

RTSP Streaming

To utilize the RTSP streaming authentication, make sure that your have set a password for the Network
Camera first; please refer to Security on page 27 for details.
Authentication:Depending on your network security requirements, the Network Camera provides three
types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If basic authentication is selected, the password is sent in plain text format, but there can be potential
risks of it being intercepted. If digest authentication is selected, user credentials are encrypted using
MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed in the following table:
Access name for stream 1 / Access name for stream 2: This Network camera supports dual streams
simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the Network Camera, you have to set the video mode to
MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the URL command in the text box. For example:
4. The live video will be displayed in your player as shown
below.
rtsp://192.168.5.151:554/live.sdp
Quick Time player Real Player
Disable O O
Basic O O
Digest O X

RTSP port /RTP port for video, audio/ RTCP port for video, audio
The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port
number is set to 554.
■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By
default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by
monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port
for audio is set to 5559.
The five ports can be changed to values between 1025 and 65535. The RTP port must be an even
number and the RTCP port is the RTP port number plus one, and thus is always odd. When the RTP port
changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:

Multicast settings for stream 1 / Multicast settings for stream 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or stream 2.

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The five ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and is thus always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:

Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic Domain Name Service

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the Provider drop-down list.

VIVOTEK offers **Safe100.net**, a free dynamic domain name service to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's network camera from the Internet.

Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.

Note that before utilizing this function, please apply a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click Register. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.
3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.

[Register] Successfully Your account information has been mailed to registered e-mail address

4. Select Enable DDNS, then click **Save** to enable the settings.

■ CustomSafe100

VIVOTEK offers documents to establish CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click Register. After a

host name has been successfully created, you will see a success message in the DDNS Registration
Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the
DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.
Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your
account information will be sent to your email address.
Refer to the following links to apply a dynamic domain account when selecting other DDNS
providers:

- Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
- TZO.com: visit http://www.tzo.com/
- DHS.org: visit http://www.dhs.org/
- dyn-interfree.it: visit http://dyn-interfree.it/

[Register] Successfully Your account information has
been mailed to registered e-mail address

Access List Advanced Mode

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10
clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**,
all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick
Time Player).
View Information: Click this button to display the connection status window showing a list of the current
connections. For example:

- IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 27.
2. The administrator has set up a root password, but set RTSP Authentication to “disable“. For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 42.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to Security on page 27.

■ Refresh: Click this button to refresh all current connections.

■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the

denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this
button. Please note that those checked connections will only be disconnected temporarily and will
automatically try to re-link again (IE Explore or Quick Time Player).

Enable access list filtering: Check this item and click Save if you want to enable the access list filtering
function.

Filter

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP
addresses are on the Allowed list and not on the Denied list can access the Network Camera. Please
note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page.

For more information about **IPv6 settings**, please refer to page 37 for detailed information.

■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list. There are three types of rules:

Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the
Allow/Deny List.
For example:

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is
only applied to IPv4.
For example:

■ Delete Allowed/Denied list:

In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.

NOTE

► For example, when the range of IP addresses in the allowed list is set from 1.1.1.0 to 192.255.255.255

and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IP located between

171.0.0.0 and 192.255.255.255 can access the Network Camera.

Administrator IP Address

Always allow the IP address to access this device: You can check this item and add the Administrator's

IP address in this field to make sure the Administrator can always connect to the device.

Allowed List
Denied List

IP address 192.168.2.x will be blocked.

Audio and Video

This section explains how to cofigure the audio and video settings of the Network Camera. It is

composed of the following two columns: Video Settings and Audio Settings.

Video Settings

Video title: Enter a name that will be displayed on the title bar of the live video.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image

flickering associated with fluorescent lights. Note that after the power line frequency is changed, you

must disconnect and reconnect the power cord of the Network Camera in order for the new setting to

take effect.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display

of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling)

to correct the image orientation.

Maximum exposure time: 1/30 S, 1/15 S, and 1/5 S.

Overlay title and time stamp on video: Select this option to place the video title and time on video
streams.
Video title
Title and time

Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be
stamped on the video streams.
Image Settings Advanced Mode
Click **Image settings** to open the Image Settings page. On this page, you can tune the White balance,
Brightness, Saturation, Contrast, and Sharpness settings for the video.
White balance: Adjust the value for best color temperature.
■ Auto
The Network Camera automatically adjusts the color temperature of light in response to different light
sources. The white balance setting defaults to **Auto** and works well in most situations.

■ Keep current value
Follow the steps below to manually set the white balance to compensate for the ambient lighting
conditions.
1. Set the White balance to **Auto** and click **Save**.
2. Place a sheet of white paper in front of the lens, then allow the Network Camera to adjust the color
temperature automatically.
3. Select Keep Current Value to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the settings.
Image Adjustment
■ Brightness: Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.

■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to +3.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without
incorporating the changes. When completed with the settings on this page, click **Save** to enable the
settings and click **Close** to exit the page.

Privacy Mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to
address privacy concerns.

■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window.
2. Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size
of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Select **Enable privacy mask** to enable this function.

NOTE

► Up to 5 privacy mask windows can be set up on the same screen.

► If you want to delete the privacy mask window, please click the ‘x’ on the upper right-hand corner of
the window.

Video quality settings for stream 1 / stream 2 Advanced Mode

The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4
and MJPEG.

Click the items to display the detailed configuration settings. You can set up two seperate streams for the

Network Camera for different viewing devices. For example, set a smaller frame size and lower bit rate
for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web
browsers.
If MPEG-4 mode is selected, the video is streamed via RTSP protocol. There are four parameters
provided in MPEG-4 mode which allow you to adjust the video performance:
■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are
selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.
■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video
quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps,
8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are
selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select
Customize and manually enter a value.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get a better
video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period
from the following durations: 1 second, 2 seconds, 3 seconds, and 4 seconds.
■ Video quality
A complex scene generally produces larger file size, meaning that higher bandwidth will be needed

for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at
a selected level, resulting in mutable video quality performances. The bit rates are selectable at the
following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps,
1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.
On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality;
bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following
settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and
manually enter a value.
If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing
a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image
quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents
are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters
provided in MJPEG mode to control the video performance:

■ Frame size

Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are
selectable in the following resolutions: 176 x 144, 320 x 240, and 640 x 480.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video
quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps,

8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are
selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps.

■ Video quality

The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and
Excellent. You can also select **Customize** and manually enter a value.

NOTE

► Video quality and fixed quality refers to the compression rate, so a lower will produce higher quality.

Audio Settings

Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that
if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the
Client Settings page. In that case, the following message is displayed:

Internal microphone input gain: Select the gain of the internal audio input according to ambient
conditions. Adjust the gain from +12 db (most sensitive) ~ -34.5 db (least sensitive).

External microphone input: Select the gain of the external audio input according to ambient conditions.
Adjust the gain from +20 db (most sensitive) or 0 db (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate Advanced Mode .

■ AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are
selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.

■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are
selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps,10.2Kbps, and
12.2Kbps.

When completed with the settings on this page, click **Save** to enable the settings.

NOTE

► The Network Camera offers two inputs to capture audio - internal microphone or external microphone.

The internal/external microphone switch is located on the side of the Network Camera.

Motion Detection

This section explains how to configure the Network Camera to enable motion detection. A total

of three motion detection windows can be configured.

Follow the steps below to enable motion detection:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.

■ To move and resize the window, drag and drop your mouse on the window.

■ To delete window, click X on the top right corner of the window.

3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the

Sensitivity and Percentage slider bar.

4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:

The Percentage Indicator will rise or fall depending on the variation between sequential images. When

motions are detected by the Network Camera and are judged to exceed the defined threshold, the

red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be

captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a

trigger source. For more information on how to set an event, please refer to Application on page 61.

A green bar indicates that even though motions have been detected, the event has not been triggered

because the image variations still fall under the defined threshold.

NOTE

► How does motion detection work?

There are two motion detection parameters: Sensitivity and Percentage. In the illustration above,
frame A and frame B are two sequential images. Pixel differences between the two frames are
detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity
is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to
detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set
to 70%, the Network Camera defines the pixels in the purple areas as “alerted pixels” (frame D).
Percentage is a value that expresses the proportion of “alerted pixels” to all pixels in the motion
detection window. In this case, 50% of pixels are identified as “alerted pixels”. When the percentage is
set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will
be outlined in red.
For applications that require a high level of security management, it is suggested to use higher
sensitivity settings and smaller percentage values.

Percentage = 30%

Camera Tampering Detection

This section explains how to set up camera temper detection. With tamper detection, the
camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even

spray paint.

Please follow the steps below to set up the camera tamper detection function:

1. Check **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Application page > Event Settings / Server Settings (how to send alarm message) / Media Settings (send what type of alarm message)**. Please refer to page 65 for detailed information.

Homepage Layout Advanced Mode

This section explains how to set up your own customized homepage layout.

Preview

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the third column on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

Logo

Here you can change the logo at the top of your homepage.

Follow the steps below to upload a new logo:

1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the

settings.

Font Color of the Video Title

Font Color

Background Color of the Control Area

Font Color of the Configuration Area

Background Color of the Configuration Area

Background Color of the Video Area

Frame Color

Preset Patterns

■ Follow the steps below to set up the customed homepage:

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.
3. The palette window will pop up as shown below.
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

1

2

3

4

Color Picker

Customed Pattern

Application Advanced Mode

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications.

Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on

configuring the settings. Please note that there is a limited number of customized scripts you can upload;
if the current amount of customized scripts has reached the limit, an alert message will pop up. If you
need more information, please ask for VIVOTEK technical support.

In the illustration on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.

Click to upload a file.

Click to modify the script online

Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. On this page, you can
arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be
configured.

Event name: Enter a name for the event setting.

Enable this event: Select this option to enable this event setting.

Priority: Select the relative importance of this event (High, Normal, or Low). Events with higher priority
setting will be executed first.

Detect next event after seconds: Enter the duration in seconds to pause motion detection after a
motion is detected.

An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the
following three elements: Trigger, Event Schedule, and Action.

Trigger

This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can
be configured to use the Network Camera's built-in motion detection mechanism or external digital input
devices.

There are several choices of trigger sources as shown below. Select the item to display the detailed
configuration options.

■ Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this
function, you need to configure a Motion Detection Window first. For more information, please refer to
Motion detection on page 55 for details.

■ Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999
minutes are allowed.

■ Digital input

This option allows the Network Camera to use an external digital input device or sensor as a trigger
source. Depending on your application, there are many choices of digital input devices on the market
which helps to detect changes in temperature, vibration, sound, and light, etc.

■ PIR

This option allows the Network Camera to trigger when the built-in PIR (Passive Infrared) sensor
detects any motion objects by their thermal to prevent occurrences of false alarms.

■ System boot

This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording
starts to rewrite older data. If you want receive **Recording notify message**, please refer to page 72
for detailed information.

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered
with. To enable this function, you need to configure the Tampering Detection option first. Please refer
to page 57 for detailed information.

Event Schedule

Specify the period for the event.

■ Select the days of the week.

■ Select the recording schedule in 24-hr time format.

Action

Define the actions to be performed by the Network Camera when a trigger is activated.

■ Trigger digital output for seconds

Select this option to turn on the external digital output device when a trigger is activated. Specify the
length of the trigger interval in the text box.

■ Turn on IR Illuminators for seconds

Select this to turn on IR Illuminators when a trigger is activated every time or only in low light
conditions. Specify the length of trigger interval in the text box.

To set an event with recorded video or snapshots, it is necessary to configure the server and
media settings so that the Network Camera will know what action to take (such as which server
to send the media files to) when a trigger is activated.

■ Add Server / Add Media

Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings
on page 67.
Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on
page 70.
Here is an example of Event Settings page:

When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new
event settings / server settings / media settings will appear in the event drop-down list on the Application
page.
Here is an example of the Application page with an event setting:
When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will
automatically send snapshots via e-mail.
If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove
the event setting.
To remove a server setting from the list, select a server name from the drop-down list and click **Delete**.
Note that only when the server setting is not being applied to an event setting can it be deleted.
To remove a media setting from the list, select a media name from the drop-down list and click **Delete**.
Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify
where the notification messages are sent when a trigger is activated. A total of 5 server settings can be
configured.

Server name: Enter a name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item
to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.

- Sender email address: Enter the email address of the sender.
- Recipient email address: Enter the email address of the recipient.
- Server address: Enter the domain name or IP address of the email server.
- User name: Enter the user name of the email account if necessary.
- Password: Enter the password of the email account if necessary.
- Server port: The defualt mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure
connection (SSL).**

To verify if the email settings are correctly configured, click Test. The result will be shown in a pop-up
window. If successful, you will also receive an email indicating the result.

Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.

- Server address: Enter the domain name or IP address of the FTP server.
- Server port

By default, the FTP server port is set to 21. It can also be assigned to another port number between
1025 and 65535.

- User name: Enter the login name of the FTP account.
- Password: Enter the password of the FTP account.
- Remote folder name

Enter the folder where the media file will be placed. If the folder name does not exist, the Network
Camera will create one on the FTP server.

- Passive mode

Most firewalls do not accept new connections initiated from external requests. If the FTP server
supports passive mode, select this option to enable passive mode FTP and allow data transmission to
pass through the firewall.
To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up
window as shown below. If successful, you will also receive a test.txt file on the FTP server.
Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.
- URL: Enter the URL of the HTTP server.
- User name: Enter the user name if necessary.
- Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up
window as below. If successful, you will receive a test.txt file on the HTTP server.
Click **Save** to enable the settings, then click **Close** to exit the page.
Network storage: Select to send the media files to a network storage location when a trigger is activated.
Please refer to **Network Storage Setting** on page 74 for details.
Click **Save** to enable the settings, then click **Close** to exit the page.
When completed, the new server settings will automatically be displayed on the Event Settings page.
For example:

Media Settings

Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can
specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be
configured.
Media name: Enter a name for the media setting.

Media Type

There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item
to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

■ Source: Select to take snapshots from stream 1 or stream 2.

■ Send pre-event images

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number
to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

■ Send post-event images

Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can
be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15
images are generated after a trigger is activated.

■ File name prefix

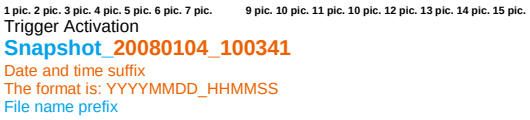
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name

Select this option to add a date/time suffix to the file name.

For example:

Click **Save** to enable the settings, then click **Close** to exit the page.



Video clip: Select to send video clips when a trigger is activated.

■ Source: Select to record video clips from stream 1 or stream 2.

■ Pre-event recording

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number
to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration

Specify the maximum recording duration in seconds. Up to 10 seconds can be set.

For example, if pre-event recording is set to five seconds and the maximum duration is set to ten

seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.

■ Maximum file size

Specify the maximum file size allowed.

■ File name prefix

Enter the text that will be appended to the front of the file name.

For example:

Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.

Click **Save** to enable the settings, then click **Close** to exit the page.

Video_20080104_100341
Date and time suffix
The format is: YYYYMMDD_HHMMSS
File name prefix
1 sec. 2 sec. 3 sec. 4 sec. 5 sec. **7 sec. 8 sec. 9 sec. 10 sec.**
Trigger Activation

Recording notify message: Select to send a recording notification message when a trigger is activated.

The following is an example of a recording notification message (.txt file), which shows a list of deleted

previously-recorded data due to cycle recording.

When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media

settings will appear on the Event Settings page.

You can continue to select a server and media type for the event. Please go back to page 66 for detailed

information.

■ Create folders by date, time, and hour automatically: If you check this item, the system will generate

folders automatically by date.

■ View: Click this button to open a file list window. This function is only for Network Storage.

The following is an example of a file destination with video clips:

20081120
20081121
20081122

Click to delete selected items Click to delete all recorded data

The format is: YYYYMMDD

Click to open the directory

Click **20081120** to open the directory:

Click to delete

selected items

Click to delete all

recorded data

Click to go back to the previous

level of the directory

The format is: HH (24r)

Click to open the file list for that hour

The format is: File name prefix + Minute (mm)

You can set up the file name prefix on Media Settings page.

Please refer to page 70 for detailed information.

Recording Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

NOTE

► Before setting up this page, please set up the Network Storage on the Server Settings page first.

Network Storage Setting

Click Server to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.

For example:

2. Click **Test** to check the setting. The result will be shown in the pop-up window.

1

2

3

4

Network storage path

(\\server name or IP address\folder name)
User name and password for your server

If successful, you will receive a test.txt file on the network storage server.

3. Enter a server name.

4. Click **Save** to complete the settings and click **Close** to exit the page.

Recording Settings

Click **Add** to open the recording setting page. In this page, you can define the recording source,
recording schedule and recording capacity. A total of 2 recording settings can be configured.

Recording name: Enter a name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of this recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 or stream 2).

Recording Schedule: Specify the recording duration.

■ Select the days of the week.

■ Select the recording start and end times in 24-hr time format.

Destination: You can select the SD card or network storage that was set up for the recorded video files.

Capacity: You can choose either the entire free space available or limit the recording size. The recording
size limit must be larger than the reserved amount for cyclic recording.

File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file
will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent
malfunction. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger >**
Recording notify on page 64 for detailed information.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit
this page. When the system begins recording, it will send the recorded files to the Network Storage.
The new recording name will appear in the drop-down list on the recording page as shown below.
To remove a recording setting from the list, select a recording name from the drop-down list and click
Delete.

- Click **Video (Name)**: Opens the Recording Settings page to modify.
- Click **ON (Status)**: The Status will become **OFF** and stop recording.
- Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about
folder naming rules, please refer to page 72 for details.

20081120
20081121
20081122

System Log Advanced Mode

This section explains how to configure the Network Camera to send the system log to the
remote server as backup.

Remote Log

You can configure the Network Camera to send the system log file to a remote server as a log backup.
Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log
messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit
http://www.kiwisyslog.
com/kiwi-syslog-daemon-overview/.
Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to enable the setting.

Current Log

This column displays the system log in chronological order. The system log is stored in the Network
Camera's buffer area and will be overwritten when reaching a certain limit.

View Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in alphabetical order. If you
need technical assistance, please provide the information listed on this page.

Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware
version, etc.

Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When
completed, the live video page will be displayed in your browser. The following message will be displayed
during the reboot process.
If the connection fails after rebooting, manually enter the IP address of the Network Camera in the
address field to resume the connection.

Restore

This feature allows you to restore the Network Camera to factory default settings.
Network Type: Select this option to retain the Network Type settings (please refer to Network Type on
page 33).
Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to
System on page 25).
Custom Language: Select this option to retain the Custom Language settings.
If none of the options is selected, all settings will be restored to factory default.
The following message is displayed during the restoring process.

Export / Upload Files Advanced Mode

This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting
backup files.

Export daylight saving time configuration file: Click to set the start and end time of DST. Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the
Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to
store the file for editing.
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST.
When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at
2:00 a.m. on the first Sunday in November.

Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload. If the incorrect date and time are assigned, you will see the following warning message when uploading
the file to the Network Camera.

The following message is displayed when attempting to upload an incorrect file format.

Export language file: Click to export language strings. VIVOTEK provides nine languages: English,
Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters for the device and user-defined scripts.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model

and firmware version of the device should be the same as the setting backup file. If you have set up a
fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade Firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to
complete the process.

Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:

1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade
completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, reaccess
the Network Camera.

The following message is displayed when the upgrade has succeeded.

The following message is displayed when you have selected an incorrect firmware file.

```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail
```

Appendix

URL Commands for the Network Camera

Overview

For some customers who already have their own web site or web control application, the Network
Camera/Video Server can be easily integrated through URL syntax. This section specifies the external

HTTP-based application programming interface. The HTTP-based camera interface provides the
functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set
internal parameter values. The image and CGI-requests are handled by the built-in Web server.

Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that
is to be replaced with either a value or a string. When replacing the text string, the angle brackets
should also be replaced. An example of this is the description of the name for the server, denoted with
<servername> in the URL syntax description below, that is replaced with the string myserver in the URL
syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced
syntax as shown below. For example, name of the server is written as <servername> and is intended to
be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.
adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

http://<servername>/cgi-bin/viewer/video.jpg

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is
returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

HTTP/1.0 <HTTP code> <HTTP text>\r\n

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box
with the example.

Example: request a single snapshot image

http://mywebserver/cgi-bin/viewer/video.jpg

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or
other separators. When the CGI request includes internal camera parameters, the
internal parameters must be written exactly as they are named in the camera or video
server. The CGIs are organized in function related directories under the cgi-bin
directory. The file extension of the CGI is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Setting digital output #1 to active

Security level

SECURITY
LEVEL
SUB-DIRECTORY DESCRIPTION
0 anonymous Unprotected.
1 [view] anonymous, viewer,
dido, camctrl
1. Can view, listen, talk to camera
2. Can control dido, ptz of camera
4 [operator] anonymous, viewer,
dido, camctrl,
operator
Operator's access right can modify most of
camera's parameters except some privilege and
network options
6 [admin] anonymous, viewer,
dido, camctrl,
operator, admin
Administrator's access right can fully control the
camera's operation.
7 N/A Internal parameters. Unable to be changed by
any external interface.

Get server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]
http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]
http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]

[&<parameter>…]
http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]
where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>] If you
do not specify the any parameters, all the parameters on the server will be returned. If
you specify only <*group*>, the parameters of related group will be returned.
When query parameter values, the current parameter value are returned.
Successful control request returns paramter pairs as follows.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>
where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
<length> is the actual length of content.
Example: request IP address and it's response
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Set server parameter values

Note: The access right depends on the URL directory.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]
http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
PARAMETER VALUE DESCRIPTION
<group>_<name> value to assigned Assign <*value*> to the parameter <*group*>_<*name*>
update <boolean> set to 1 to actually update all fields (no need to use update parameter in each group)
return <*return page*> Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a

full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.
(note: The return page can be a general HTML file (.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n

\r\n
<parameter pair>
where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]
Only the parameters that you set and readable will be returned.
Example: Set the IP address of server to 192.168.0.123
Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

Available parameters on the server

Valid values:
VALID VALUES DESCRIPTION
string[<n>] Text string shorter than 'n' characters. The characters ",', <,>,&
are invalid.
password[<n>] The same as string but display '*' instead
integer Any number between ($-2^{31} - 1$) and ($2^{31} - 1$)
positive integer Any number between 0 and ($2^{32} - 1$)
<m> ~ <n> Any number between 'm' and 'n'
domain name[<n>] A string limited to contain a domain name shorter than 'n'
characters (eg. www.ibm.com)
email address [<n>] A string limited to contain a email address shorter than 'n'
characters (eg. joe@www.ibm.com)
ip address A string limited to contain an ip address (eg. 192.168.1.1)
mac address A string limited to contain mac address without hyphen or colon
connected

boolean A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].

<value1>,
<value2>,
<value3>,
…
Enumeration. Only given values are valid.
blank A blank string
everything inside <> As description
NOTE: The camera should prevent to restart when parameter changed.
Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	host name of server
ledoff	<boolean>	6/6	turn on(0) or turn off(1) all led indicators
lowlight	<boolean>	6/6	(0) Turn on white light LED in all condition (1) Only turn on white light LED in low light condition
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to 'keep' keeping date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of system. Set to 'keep' keeping time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYY.ss>	6/6	Another current time format of system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server *do not use "skip to invoke default server" for default
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa

-400: GMT-10:00 Hawaii
-360: GMT-09:00 Alaska
-320: GMT-08:00 Las Vegas, San_Francisco, Vancouver

-280: GMT-07:00 Mountain Time, Denver
-281: GMT-07:00 Arizona
-240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan
-200: GMT-05:00 Eastern Time, New York, Toronto
-201: GMT-05:00 Bogota, Lima, Quito, Indiana
-160: GMT-04:00 Atlantic Time, Canada, Caracas, La Paz, Santiago
-140: GMT-03:30 Newfoundland
-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland
-80: GMT-02:00 Mid-Atlantic
-40: GMT-01:00 Azores, Cape_Verde_IS.
0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris
41: GMT 01:00 Warsaw, Budapest, Bern
80: GMT 02:00 Athens, Helsinki, Istanbul, Riga
81: GMT 02:00 Cairo
82: GMT 02:00 Lebanon, Minsk
83: GMT 02:00 Israel
120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi
121: GMT 03:00 Iraq
140: GMT 03:30 Tehran
160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan
180: GMT 04:30 Kabul
200: GMT 05:00 Ekaterinburg,

Islamabad, Karachi, Tashkent
220: GMT 05:30 Calcutta, Chennai,

Mumbai, New Delhi
230: GMT 05:45 Kathmandu
240: GMT 06:00 Almaty, Novosibirsk,
Astana, Dhaka, Sri Jayawardenepura
260: GMT 06:30 Rangoon
280: GMT 07:00 Bangkok, Hanoi,
Jakarta, Krasnoyarsk
320: GMT 08:00 Beijing, Chongqing,
Hong Kong, Kuala Lumpur, Singapore,
Taipei
360: GMT 09:00 Osaka, Sapporo,
Tokyo, Seoul, Yakutsk
380: GMT 09:30 Adelaide, Darwin
400: GMT 10:00 Brisbane, Canberra,
Melbourne, Sydney, Guam, Vladivostok
440: GMT 11:00 Magadan, Solomon
Is., New Caledonia
480: GMT 12:00 Aucklan, Wellington,
Fiji, Kamchatka, Marshall Is.
520: GMT 13:00 Nuku'Alofa
daylight_enabl
e
<boolean> 6/6 enable automatic daylight saving to
time zone
daylight_dstac
tualmode
<boolean> 6/7 check if current time is under daylight
saving time.
daylight_auto_
begintime
string[19] 6/7 display the current daylight saving
begin time.
daylight_auto_
endtime
string[19] 6/7 display the current daylight saving end
time.
daylight_timez
ones
strings 6/7 list of time zone which has daylight
saving time
updateinterval 0,
3600,
86400,
604800,
2592000
6/6 0 to disable automatic time
adjustment, otherwise, it means the
seconds between NTP automatic
update interval.
restore 0,

<positive
integer>
7/6 Restore the system parameters to
default value after <value> seconds.

reset 0,
<positive
integer>
7/6 Restart the server after <value>
seconds if <value> is non-negative.
restoreexceptn
et
<Any value> 7/6 Restore the system parameters to
default value except (ipaddress,
subnet, router, dns1, dns2, pppoe).
This command can cooperate with
other "restoreexceptXYZ" commands.
When cooperating with others, the
system parameters will be restored to
default value except a union of
combined results.
restoreexceptd
st
<Any value> 7/6 Restore the system parameters to
default value except all daylight saving
time settings.
This command can cooperate with
other "restoreexceptXYZ" commands.
When cooperating with others, the
system parameters will be restored to
default value except a union of
combined results.
restoreexceptl
ang
<Any Value> 7/6 Restore the system parameters to
default value except custom language
file user uploaded.
This command can cooperate with
other "restoreexceptXYZ" commands.
When cooperating with others, the
system parameters will be restored to
default value except a union of
combined results.
SubGroup of **system**: **info**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
modelname string[40] 0/7 model name of server
extendedmodelname string[40] 0/7 equal to "modelname"

serialnumber <mac
address>
0/7 12 characters mac address without
hyphen connected
firmwareversion string[40] 0/7 The version of firmware, including
model, company, and version number

in the format
<MODEL-BRAND-VERSION>
language_count <integer> 0/7 Default number of webpage language
available on the server
language_i<0~(coun
t-1)>
string[16] 0/7 Available default language lists
customlanguage_ma
xcount
<integer> 0/7 Maximum number of custom
language supported on the server
customlanguage_cou
nt
<integer> 0/7 Number of custom language which
has been uploaded to the server
customlanguage_i<0
~(maxcount-1)>
string 0/7 Custom language name
Group: **status**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
di_i<0~(ndi-1)> <boolean> 1/7 0 => Inactive, normal
1 => Active, triggered
do_i<0~ndi-1)> <boolean> 1/7 0 => Inactive, normal
1 => Active, triggered
onlinenum_rtsp integer 6/7 current RTSP connection numbers
onlinenum_httppush integer 6/7 current HTTP push server
connection numbers
eth_i0 <string> 1/99 Get network information from
mii-tool
Group: **di_i<0~(ndi-1)>**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
normalstate high,
low
1/1 indicate whether open circuit or
closed circuit represents inactive
status
Group: **do_i<0~(ndo-1)>**
NAME VALUE SECURITY

(get/set)
DESCRIPTION
normalstate open,
grounded
1/1 indicate whether open circuit or closed
circuit represents inactive status

Group: **security**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
privilege_do view, operator,
admin
6/6 Indicate which privilege and above
can control digital output
user_i0_name string[64] 6/7 User's name of root
user_i<1~20>_name string[64] 6/7 User's name
user_i0_pass password[64] 6/6 root's password
user_i<1~20>_pass password[64] 7/6 User's password
user_i0_privilege viewer,
operator,
admin
6/7 root's privilege
user_i<1~20>_
privilege
viewer,
operator,
admin
6/6 User's privilege.
Group: **network**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
type lan,
pppoe
6/6 Network connection type
preprocess 0~15 6/6 Stop related process before set port value
resetip <boolean> 6/6 1 => get ipaddress, subnet, router, dns1,
dns2 from DHCP server at next reboot
0 => use preset ipaddress, subnet,
rounter, dns1, and dns2
ipaddress <ip address> 6/6 IP address of server
subnet <ip address> 6/6 subnet mask
router <ip address> 6/6 default gateway
dns1 <ip address> 6/6 primary DNS server
dns2 <ip address> 6/6 secondary DNS server
wins1 <ip address> 6/6 primary WINS server
wins2 <ip address> 6/6 secondary WINS server
Subgroup of **network**: **ipv6**

NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable IPv6
addonipaddress <ip address> 6/6 IPv6 IP address

addonprefixlen 0~128 6/6 IPv6 prefix length
addonrouter <ip address> 6/6 IPv6 router address
addondns <ip address> 6/6 IPv6 DNS address
allowoptional <boolean> 6/6 Allow Manually setup the IP address
setting
Subgroup of **network**: **sip**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 554, 1025~ 65535 6/6 SIP port
Subgroup of **network**: **ftp**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 21, 1025~65535 6/6 local ftp server port
Subgroup of **network**: **http**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 80, 1025~ 65535 6/6 HTTP port
alternateport 1025~65535 6/6 Alternative HTTP port
authmode basic,
digest
1/6 HTTP authentication mode
s0_accessname string[32] 1/6 Http server push access name
for stream 1
s1_accessname string[32] 1/6 Http server push access name
for stream 2
Subgroup of **network**: **https**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 443, 1025~ 65535 6/6 HTTPS port
Subgroup of **network**: **rtsp**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
port 554, 1025 ~ 65535 1/6 RTSP port
authmode disable,
basic,
1/6 RTSP authentication mode

digest
s0_accessname string[32] 1/6 RTSP access name for stream1
s1_accessname string[32] 1/6 RTSP access name for stream2
s0_audiotrack <integer> 6/6 The current audio track for stream1.
-1 => audio mute
s1_audiotrack <integer> 6/6 The current audio track for stream2.
-1 => audio mute
Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count
NAME VALUE SECURITY (get/set)
DESCRIPTION
alwaysmulticast <boolean> 4/4 Enable always multicast
ipaddress <ip address> 4/4 Multicast IP address
videoport 1025 ~ 65535 4/4 Multicast video port
audioport 1025 ~ 65535 4/4 Multicast audio port
ttl 1 ~ 255 4/4 Multicast time to live value
Subgroup of **network**: **rtp**
NAME VALUE SECURITY (get/set)
DESCRIPTION
videoport 1025~ 65535 6/6 video channel port for RTP
audioport 1025~ 65535 6/6 audio channel port for RTP
Subgroup of **network**: **pppoe**
NAME VALUE SECURITY (get/set)
DESCRIPTION
user string[128] 6/6 PPPoE account user name
pass password[64] 6/6 PPPoE account password
Group: **ipfilter**
NAME VALUE SECURITY (get/set)
DESCRIPTION
enable <boolean> 6/6 Enable access list filtering
admin_enable <boolean> 6/6 Enable administrator IP address
admin_ip String[44] 6/6 Administrator IP address
maxconnection 1~10 6/6 Maximum number of concurrent streaming connection(s)
allow_i<0~9>_start 1.0.0.0 ~ 255.255.255.255 6/6 Allowed starting IPv4 address for connection
allow_i<0~9>_end 1.0.0.0 ~

255.255.255.255
6/6 Allowed ending IPv4 address for
connection
deny_i<0~9>_s
tart
1.0.0.0 ~
255.255.255.255
6/6 Denied starting IPv4 address for
connection
deny_i<0~9>_e
nd
1.0.0.0 ~
255.255.255.255
6/6 Denied ending IPv4 address for
connection
ipv6_allow_i<0~
9>
String[44] 6/6 Allowed IPv6 address for
connection
ipv6_deny_i<0~
9>
String[44] 6/6 Denied IPv6 address for connection
Group: **videoin**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
cmosfreq 50, 60 4/4 CMOS frequency
whitebalance auto,
manual
4/4 auto, auto white balance
manual
atwbvalue 0 ~ 65535 4/4 The auto white balance value.
Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number
NAME VALUE SECURITY
(get/set)
DESCRIPTION
color 0, 1 4/4 0 =>monochrome
1 =>color
flip <boolean> 4/4 flip the image
mirror <boolean> 4/4 mirror the image
ptzstatus <integer> 1/7 An 32-bits integer, each bit can be set
separately as follows:
Bit 0 => Support camera control
function 0(not support), 1(support)
Bit 1 => **Build-in** or **external**
camera. 0(external), 1(build-in)
Bit 2 => Support **pan** operation.
0(not support), 1(support)
Bit 3 => Support **tilt** operation.
0(not support), 1(support)

Bit 4 => Support **zoom**
operation. 0(not support), 1(support)
Bit 5 => Support **focus**
operation. 0(not support), 1(support)
text string[16] 1/4 enclosed caption
imprinttimestamp <boolean> 4/4 Overlay time stamp on video
maxexposure 1~120 4/4 Maximum exposure time
s<0~(m-1)>_codec
type
mpeg4,
mjpeg
4/4 video codec type
s<0~(m-1)>_resol
ution
176x144,
320x240,
640x480
4/4 Video resolution in pixel
s<0~(m-1)>_mpeg
4_intraperiod
250, 500,
1000, 2000,
3000, 4000
4/4 The period of intra frame in
milliseconds
s<0~(m-1)>_mpeg
4_ratecontrolmode
cbr, vbr 4/4 cbr, constant bitrate
vbr, fix quality
s<0~(m-1)>_mpeg
4_quant
1~5 4/4 quality of video when choosing vbr in
"ratecontrolmode".
1 is worst quality and 5 is the best
quality.
s<0~(m-1)>_mpeg
4_qvalue
1~31 7/4 Quality parameter of mpeg4 encoder.
1 is best quality and 31 is the worst
quality.
s<0~(m-1)>_mpeg
4_bitrate
1000~4000
000
4/4 Set bit rate in bps when choose cbr in
"ratecontrolmode"
s<0~(m-1)>_mpeg
4_maxframe

1, 2, 3, 5,
10, 15, 20,
25, 30 (only
for NTSC or
60Hz CMOS)
4/4 set maximum frame rate in fps (for
MPEG-4)
s<0~(m-1)>_mjpe
g_quant
1 ~ 5 4/4 quality of jpeg video.
1 is worst quality and 5 is the best
quality.
s<0~(m-1)>_mjpe
g_qvalue
10~200 7/4 The specific quality parameter of jpeg
encoder.
10 is best quality and 200 is the worst
quality.
s<0~(m-1)>_mjpe 1~25, 4/4 set maximum frame rate in fps (for

g_maxframe 26~30 (only
for NTSC or
60Hz CMOS)
JPEG)
s<0~(m-1)>_forcei 1 7/6 Force I frame
Group: **audioin_c<0~(n-1)>** for n channel products
NAME VALUE SECURITY
(get/set)
DESCRIPTION
source micin,
linein
4/4 micin => use external microphone
input
linein => use line input
mute 0, 1 1/4 Enable audio mute
gain 0~31 4/4 Gain of input
boostmic 0, 1 4/4 Enable microphone boost
s<0~(m-1)>_codectype aac4, gamr 4/4 set audio codec type for input
s<0~(m-1)>_aac4_bitra
te
16000,
32000,
48000,
64000,
96000,
128000
4/4 set AAC4 bitrate in bps
s<0~(m-1)>_gamr_bitr
ate

4750,
5150,
5900,
6700,
7400,
7950,
10200,
12200
4/4 set AMR bitrate in bps
Group: **image_c<0~(n-1)>** for n channel products
NAME VALUE SECURITY
(get/set)
DESCRIPTION
brightness -5 ~ 5 4/4 Adjust brightness of image according to
mode settings.
saturation -5 ~ 5 4/4 Adjust saturation of image according to
mode settings.
contrast -5 ~ 5 4/4 Adjust contrast of image according to
mode settings.

sharpness -3 ~ 3 4/4 Adjust sharpness of image according to
mode settings.
Group: **imagepreview_c<0~(n-1)>** for n channel products
NAME VALUE SECURITY
(get/set)
DESCRIPTION
brightness -5 ~ 5 4/4 Preview of adjusting brightness of
image according to mode settings.
saturation -5 ~ 5 4/4 Preview of adjusting saturation of
image according to mode settings.
contrast -5 ~ 5 4/4 Preview of adjusting contrast of
image according to mode settings.
sharpness -3 ~ 3 4/4 Preview of adjusting sharpness of
image according to mode settings.
videoin_whitebalance auto,
manual
4/4 Preview of adjusting white balance
of image according to mode settings
videoin_restoreatwb 0, 1~ 4/4 Restore of adjusting white balance of
image according to mode settings
Group: **motion_c<0~(n-1)>** for n channel product
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 4/4 enable motion detection
win_i<0~2>_enable <boolean> 4/4 enable motion window 1~3
win_i<0~2>_name string[14] 4/4 name of motion window 1~3
win_i<0~2>_left 0 ~ 320 4/4 Left coordinate of window position.
win_i<0~2>_top 0 ~ 240 4/4 Top coordinate of window position.

win_i<0~2>_width 0 ~ 320 4/4 Width of motion detection window.
win_i<0~2>_height 0 ~ 240 4/4 Height of motion detection window.
win_i<0~2>_objsize 0 ~ 100 4/4 Percent of motion detection
window.
win_i<0~2>_sensitiv
ity
0 ~ 100 4/4 Sensitivity of motion detection
window.
Group: **tampering_c<0~(n-1)>** for n channel product
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 4/4 Enable or disable tampering detection.
threshold 0 ~ 255 4/4 Threshold of tampering detection

duration 10 ~ 600 4/4 If tampering value exceeds the
'threshold' for more than 'duration'
then tampering detection is triggered.
Group: **privacymask_c<0~(n-1)>** for n channel product
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 4/4 Enable the privacy mask
win_i<0~4>_enable <boolean> 4/4 Enable the privacy mask window
win_i<0~4>_name string[14] 4/4 The name of privacy mask window
win_i<0~4>_left 0 ~ 320/352 4/4 Left coordinate of window position.
win_i<0~4>_top 0 ~ 240/288 4/4 Top coordinate of window position.
win_i<0~4>_width 0 ~ 320/352 4/4 Width of privacy mask window
win_i<0~4>_height 0 ~ 240/288 4/4 Height of privacy mask window
Group: **ddns**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the dynamic dns.
provider Safe100,
DyndnsDynamic,
DyndnsCustom,
TZO,
DHS,
DynInterfree,
CustomSafe100
6/6 Safe100 => safe100.net
DyndnsDynamic => dyndns.org
(dynamic)
DyndnsCustom => dyndns.org
(custom)
TZO => tzo.com
DHS => dhs.org
DynInterfree =>dyn-interfree.it

CustomSafe100 =>
Custom server using safe100 method
<provider>_
hostname
string[128] 6/6 Your dynamic hostname.
<provider>_
usernameem
ail
string[64] 6/6 Your user or email to login ddns service
provider
<provider>_
passwordkey
string[64] 6/6 Your password or key to login ddns
service provider
<provider>_ string[128] 6/6 The server name for safe100.

servername (This field only exists for provider is
customsafe100)
Group: **upnppresentation**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the UPNP
presentation service.
Group: **upnpportforwarding**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enable <boolean> 6/6 Enable or disable the UPNP port
forwarding service.
upnpnatstatus 0~3 6/7 The status of UpnP port forwarding, used
internally.
0 is OK, 1 is FAIL, 2 is no IGD router, 3 is
no need to do port forwarding
Group: **syslog**
NAME VALUE SECURITY
(get/set)
DESCRIPTION
enableremotelog <boolean> 6/6 enable remote log
serverip <IP address> 6/6 Log server IP address
serverport 514,
1025~65535
6/6 Server port used for log
level 0~7 6/6 The levels to distinguish the
importance of information.
0: LOG_EMERG
1: LOG_ALERT
2: LOG_CRIT
3: LOG_ERR

4: LOG_WARNING
5: LOG_NOTICE
6: LOG_INFO
7: LOG_DEBUG

Group: **capability**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	The server bootup time
nir	0, <positive integer>	0/7	number of IR interface
npir	0, <positive integer>	0/7	number of PIR
ndi	0, <positive integer>	0/7	number of digital input
ndo	0, <positive integer>	0/7	number of digital output
naudioin	0, <positive integer>	0/7	number of audio input
naudioout	0, <positive integer>	0/7	number of audio output
nvideoin	<positive integer>	0/7	number of video input
nmediastream	<positive integer>	0/7	number of media stream per channel
nvideosetting	<positive integer>	0/7	number of video settings per channel
naudiosetting	<positive integer>	0/7	number of audio settings per channel
nuart	0, <positive integer>	0/7	number of UART interface
ptzenabled	< positive integer >	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => Build-in or external camera. 0(external), 1(build-in) Bit 2 => Support pan

operation. 0(not support),
1(support)
Bit 3 => Support tilt

operation. 0(not support),
1(support)
Bit 4 => Support zoom
operation.
0(not support), 1(support)
Bit 5 => Support focus
operation.
0(not support), 1(support)
protocol_https < boolean > 0/7 indicate whether to support
http over SSL
protocol_rtsp < boolean > 0/7 indicate whether to support
rtsp
protocol_sip <boolean> 0/7 indicate whether to support
sip
protocol_maxconnect
ion
<positive integer> 0/7 The maximum allowed
simultaneous connections
protocol_maxgencon
nection
<positive integer> 0/7 The maximum general
streaming connections
protocol_maxmegaco
nnection
<positive integer> 0/7 The maximum mega-pixels
streaming connections
protocol_rtp_multica
st_scalable
<boolean> 0/7 indicate whether to support
scalable multicast
protocol_rtp_multica
st_backchannel
<boolean> 0/7 indicate whether to support
backchannel multicast
protocol_rtp_tcp <boolean> 0/7 indicate whether to support
rtp over tcp
protocol_rtp_http <boolean> 0/7 indicate whether to support
rtp over http
protocol_spush_mjpe
g
<boolean> 0/7 indicate whether to support
server push motion jpeg
protocol_snmp <boolean> 0/7 indicate whether to support
snmp
protocol_ipv6 <boolean> 0/7 indicate whether to support

IPv6
videoin_type 0, 1, 2 0/7 0 => Interlaced CCD
1 => Progressive CCD
2 => CMOS
videoin_resolution <a list of the
available resolution
separates by
0/7 available resolutions list

comma)
videoin_maxframerat
e
<a list of available
maximum frame rate
separates by
comma>
0/7 available maximum frame
list
videoin_codec <a list of the
available codec
types separaters by
comma)
0/7 available codec list
videoout_codec <a list of the
available codec
types separaters by
comma)
0/7 available codec list
audio_aec <boolean> 0/7 indicate whether to support
acoustic echo cancellation
audio_extmic <boolean> 0/7 indicate whether to support
external microphone input
audio_linein <boolean> 0/7 indicate whether to support
external line input
audio_lineout <boolean> 0/7 indicate whether to support
line output
audio_headphoneout <boolean> 0/7 indicate whether to support
headphone output
audioin_codec <a list of the
available codec
types separaters by
comma)
0/7 available codec list
audioout_codec <a list of the
available codec
types separaters by
comma)
0/7 available codec list
uart_httptunnel <boolean> 0/7 Indicate whether to support

the http tunnel for uart
transfer
transmission_mode Tx,
Rx,
Both
0/7 Indicate what kind of
transmission mode the
machine used. TX: server,
Rx: receiver box, Both:
DVR?.

network_wire <boolean> 0/7 Indicate whether to support
the Ethernet
network_wireless <boolean> 0/7 Indicate whether to support
the wireless
wireless_802dot11b <boolean> 0/7 Indicate whether to support
the wireless 802.11b+
wireless_802dot11g <boolean> 0/7 Indicate whether to support
the wireless 802.11g
wireless_encrypt_we
p
<boolean> 0/7 Indicate whether to support
the wireless WEP
wireless_encrypt_wp
a
<boolean> 0/7 Indicate whether to support
the wireless WPA
wireless_encrypt_wp
a2
<boolean> 0/7 Indicate whether to support
the wireless WPA2
Group: **event_customtaskfile_i<0~2>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[41] 6/6 The custom scripts identification of this entry
date string[17] 6/6 Date of custom scripts
Group: **event_i<0~2>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
enable 0, 1 6/6 To enable or disable this event.
priority 0, 1, 2 6/6 Indicate the priority of this event.
"0" indicates low priority.
"1" indicates normal priority.
"2" indicates high priority.
delay 1~999 6/6 Delay seconds before detect next event.

trigger boot,
di,
motion,
seq,
pir,
recnotify,
audioswitch,
tampering
6/6 Indicate the trigger condition.
“boot” indicates system boot.
“di” indicates digital input.
“motion” indicates video motion detection.
“seq” indicates periodic condition.
“pir” indicates PIR detection.
“recnotify” indicates recording notify.
“audioswitch” indicates audio switch.
“tampering” indicates tampering detection.
di <integer> 6/6 Indicate which di detected.
This field is required when trigger condition
is “di”.
One bit represents one digital input. The
LSB indicates DI 0.
mdwin <integer> 6/6 Indicate which motion detection windows
detected.
This field is required when trigger condition
is “motion”
One bit represents one window.
The LSB indicates the 1st window.
For example, to detect the 1st and 3rd
windows, set mdwin as 5.
inter 1~999 6/6 Interval of period snapshot in minute.
This field is used when trigger condition is
“seq”.
weekday <interger> 6/6 Indicate which weekday is scheduled.
One bit represents one weekday.
The bit0 (LSB) indicates Saturday.
The bit1 indicates Friday.
The bit2 indicates Thursday.
The bit3 indicates Wednesday.
The bit4 indicates Tuesday.
The bit5 indicates Monday.
The bit6 indicates Sunday.
For example, to detect events on Friday and
Sunday, set weekday as 66.
begintime hh:mm 6/6 Begin time of weekly schedule.
endtime hh:mm 6/6 End time of weekly schedule.
(00:00 ~ 24:00 means always.)

lowlightcondition 0, 1 6/6 0 => Do action at all times
1 => Do action in low-light conditions
action_do_i<0~(n
do-1)>_enable
0, 1 6/6 To enable or disable trigger digital output.
action_do_i<0~(n
do-1)>_duration
1~999 6/6 The duration of digital output is triggered in
seconds.
action_cf_enable 0. 1 6/6 To enable put media on CF.
action_cf_folder string[128] 6/6 The path to store media.
action_cf_media NULL, 0~4 6/6 The index of attached media.
action_cf_datefold
er
<boolean> 6/6 Enable this to create folders by date time
and hour automatically.
action_server_i<0
~4>_enable
0, 1 6/6 To enable or disable this server action.
The default value is 0.
action_server_i<0
~4>_media
NULL, 0~4 6/6 The index of attached media.
action_server_i<0
~4>_datefolder
<boolean> 6/s6 Enable this to create folders by date time
and hour automatically.
Group: **server_i<0~4>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
type email,
ftp,
http,
ns
6/6 Indicate the server type.
"email" is email server.
"ftp" is ftp server.
"http" is http server.
"ns" is network storage.
http_url string[128] 6/6 The url of http server to upload.
http_username string[64] 6/6 The username to login in the server.
http_passwd string[64] 6/6 The password of the user.
ftp_address string[128] 6/6 The ftp server address
ftp_username string[64] 6/6 The username to login in the server.
ftp_passwd string[64] 6/6 The password of the user.
ftp_port 0~65535 6/6 The port to connect the server.
ftp_location string[128] 6/6 The location to upload or store the media.

ftp_passive 0, 1 6/6 To enable or disable the passive mode.
0 is to disable the passive mode.
1 is to enable the passive mode.
email_address string[128] 6/6 The email server address
email_sslmode 0, 1 6/6 Enable support SSL
email_port 0~65535 6/6 The port to connect the server.
email_username string[64] 6/6 The username to login in the server.
email_passwd string[64] 6/6 The password of the user.
email_senderemail string[128] 6/6 The email address of sender.
email_recipientemail string[128] 6/6 The email address of recipient.
ns_location string[128] 6/6 The location to upload or store the media.
ns_username string[64] 6/6 The username to login in the server.
ns_passwd string[64] 6/6 The password of the user.
ns_workgroup string[64] 6/6 The workgroup for network storage.
Group: **media_i<0~4>**
PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
type snapshot,
systemlog,
videoclip,
recordmsg
6/6 The media type to send to the server or
store by the server.
snapshot_source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
snapshot_prefix string[16] 6/6 Indicate the prefix of the filename.
snapshot_datesuffix 0, 1 6/6 To add date and time suffix to filename
or not.
1 means to add date and time suffix.
0 means not to add it.
snapshot_preevent 0 ~ 7 6/6 It indicates the number of pre-event
images.
snapshot_postevent 0 ~ 7 6/6 The number of post-event images.

videoclip_source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
videoclip_prefix string[16] 6/6 Indicate the prefix of the filename.
videoclip_preevent 0 ~ 9 6/6 It indicates the time of pre-event
recording in seconds.
videoclip_maxduration 1 ~ 10 6/6 The time of maximum duration of one
video clip in seconds.
videoclip_maxsize 50 ~ 1500 6/6 The maximum size of one video clip file
in Kbytes.
Group: **recording_i**<0~1>

PARAMETER VALUE SECURITY
(get/set)
DESCRIPTION
name string[40] 6/6 The identification of this entry
enable 0, 1 6/6 To enable or disable this recoding.
priority 0, 1, 2 6/6 Indicate the priority of this recoding.
"0" indicates low priority.
"1" indicates normal priority.
"2" indicates high priority.
source <integer> 6/6 Indicate the source of media stream.
0 means the first stream.
1 means the second stream and etc.
limitsize 0,1 6/6 0: Entire free space mechanism
1: Limit recording size mechanism
cyclic 0,1 6/6 0: Disable cyclic recording
1: Enable cyclic recording
notify 0,1 6/6 0: Disable recording notification
1: Enable recording notification

notifyserver 0~31 6/6 Indicate which notification server is scheduled.
One bit represents one application server (server_i0~i4).
The bit0 (LSB) indicates server_i0.
The bit1 indicates server_i1.
The bit2 indicates server_i2.
The bit3 indicates server_i3.
The bit4 indicates server_i4.
For example, enable server_i0, server_i2 and server_i4 to be notification server.
The notifyserver value is 21.
weekday <interger> 6/6 Indicate which weekday is scheduled.
One bit represents one weekday.
The bit0 (LSB) indicates Saturday.
The bit1 indicates Friday.
The bit2 indicates Thursday.
The bit3 indicates Wednesday.
The bit4 indicates Tuesday.
The bit5 indicates Monday.
The bit6 indicates Sunday.
For example, to detect events on Friday and Sunday, set weekday as 66.
begintime hh:mm 6/6 Begin time of weekly schedule.
endtime hh:mm 6/6 End time of weekly schedule.
(00:00~24:00 means always.)
prefix string[16] 6/6 Indicate the prefix of the filename.
cyclesize 20~ 6/6 The maximum size for cycle recording in Kbytes when choose limit recording size.
reserveamount 15~ 6/6 The reserved amount in Mbytes when

choose cyclic recording mechanism.
dest cf,
0~4
6/6 The destination to store the recording
data.
"cf" means CF card.
"0~4" means the index of network
storage.
cffolder string[128] 6/6 folder name.

Group: **https** (product dependent)
NAME VALUE SECURITY
(get/set)
DESCRIPTION
connect 1025 ~ 65535 7/7 Specify the stunnel connect port
enable <boolean> 6/6 To enable or disable this secure http
policy <Boolean> 6/6 If the value is 1, it will force http
connection redirect to https
connection
method auto,
manual,
install
6/6 auto => Create self-signed certificate
automatically
manual => Create self-signed certificate
manually
install => Create certificate request and install
status -2 ~ 1 6/6 Specify the https status.
-2=>invalid public key
-1=>waiting for certificated
0=>not installed
1=>active
countryname string[2] 6/6 country name in certificate
information
stateorprovincena
me
string[128] 6/6 state or province name in in
certificate information
localityname string[128] 6/6 the locality name in certificate
information
organizationname string[64] 6/6 organization naem in certificate
information
unit string[32] 6/6 organizational unit name in
certificate information
commonname string[64] 6/6 common name in certificate
information
validdays 0 ~ 9999 6/6 certificatation valid period
Group: **layout**
NAME VALUE SECURITY

(get/set)
DESCRIPTION
logo_default <boolean> 1/6 0 => Custom logo
1 => Default logo
logo_link string[40] 1/6 Hyperlink of the logo

theme_option 1~4 1/6 1~3: One of the default themes
4: Custom definition
theme_color_font string[7] 1/6 Font color
theme_color_configfon
t
string[7] 1/6 Font color of configuration area
theme_color_titlefont string[7] 1/6 Font color of video title
theme_color_controlba
ckground
string[7] 1/6 Background color of control area
theme_color_configbac
kground
string[7] 1/6 Background color of configuration
area
theme_color_videobac
kground
string[7] 1/6 Background color of video area
theme_color_case string[7] 1/6 Frame color

Drive the digital output

Note: This request requires the privilege of viewer.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]
Where state is 0, 1. "0" means inactive or normal state while "1" means active or
triggered state.
PARAMETER VALUE DESCRIPTION
do<num> 0, 1 0 – inactive, normal state
1 – active, triggered state
return <*return page*> Redirect to the page <*return page*> after the
parameter is assigned. The <*return page*> can be a
full URL path or relative path according the the
current path. If you omit this parameter, it will
redirect to an empty page.
Example: Drive the digital output 1 to triggered state and redirect to an empty page
http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query status of the digital input

Note: This request requires the privilege of viewer.
Method: GET/POST

Syntax:
http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
If no parameter is specified, all the status of digital input will be returned.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <*length*>\r\n
\r\n
[di0=<*state*>]\r\n
[di1=<*state*>]\r\n
[di2=<*state*>]\r\n
[di3=<*state*>]\r\n
where <*state*> can be 0 or 1.
Example: Query the status of digital input 1
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n

Query status of the digital output

Note: This request requires the privilege of viewer.
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
If no parameter is specified, all the status of digital output will be returned.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <*length*>\r\n
\r\n
[do0=<*state*>]\r\n
[do1=<*state*>]\r\n
[do2=<*state*>]\r\n
[do3=<*state*>]\r\n
where <*state*> can be 0 or 1.
Example: Query the status of digital output 1
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n

Capture single snapshot

Note: This request require normal user privilege
Method: GET/POST

Syntax:
http://<*servername*>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
If the user requests the size larger than all stream setting on the server, this request will failed!

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	the channel number of video source
resolution	<available resolution>	0	The resolution of image
quality	1~5	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of image will be set according to the video settings on the server.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]
<binary JPEG image data>

Account management

Note: This request requires administrator privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/editaccount.cgi?method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	add	Add an account to server. When using this method, "username" field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit

userpass <value> The password of new user to add or that of old user to modify. The default value is an empty string.
<value> The privilege of user to add or to modify.
viewer viewer's privilege
operator operator's privilege
privilege
admin administrator's privilege
return <return page> Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or
relative path according to current path. If you omit this
parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/syslog.cgi
Server will return the up-to-date system log.
Return:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n

Upgrade firmware

Note: This request requires administrator privilege
Method: POST
Syntax:
http://<*servername*>/cgi-bin/admin/upgrade.cgi
Post data:
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
Server will accept the upload file named <file name> to be upgraded the firmware and
return with <return page> if indicated.

IP filtering

Note: This request requires administrator access privilege
Method: GET/POST
Syntax:
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>]
[&return=<return page>]
PARAMETER VALUE DESCRIPTION
addallow Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is
specified, it will try to add starting from index position.
adddeny Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is

specified, it will try to add starting from index position.
Method
deleteallow Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.

deletedeny Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start <ip address>
The start IP address to add or to delete.
end <ip address>
The end IP address to add or to delete.
index <value> The start position to add or to delete.
return <return page>
Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to current path. If you omit this parameter, it will redirect to an empty page.

Event/Control HTTP tunnel channel

Note: This request requires admin privilege
Method: GET and POST
Syntax:
http://<*servername*>/cgi-bin/admin/ctrlevent.cgi

GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT

User must use GET and POST to establish two channels for downstream and upstream.

The x-sessioncookie in the GET and POST should be the same to be recognized as a pair
for one session. The contents of upstream should be base64 encoded to be able to pass
through some proxy server.
This channel will help to do real-time event notification and control. The event and
control format are described in another document.

Get SDP of Streamings

Note: This request requires viewer access privilege
Method: GET/POST
Syntax:
http://<*servername*>/<network_rtsp_s<0~m-1>_accessname>
"m" is the stream number.
"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m".
Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.
You can get the SDP by HTTP GET method.

Open the network streamings

Note: This request requires viewer access privilege
Syntax:
For http push server (mjpeg):
http://<*servername*>/<network_http_s<0~m-1>_accessname>
For rtsp (mp4), user needs to input the url below for a rtsp compatible player.
rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>
"m" is the stream number.
For detailed streaming protocol, please refer to "control signaling" and "data format"
documents.

Technical Specifications

Distributed by:

. CE, LVD, FCC, VCCI, C-Tick
. CPU: VVTK-1000 SoC
. Flash: 8MB
. RAM: 64MB
. Embedded OS: Linux 2.4
. Board lens, vari-focal, f=2 ~ 4 mm, F1.4 (wide), F1.8 (tele), focus range: 50 cm to infinity
. 1/5, 1/15, 1/30 sec.
. 53.2° ~ 105.1° (horizontal)
. 39.8° ~ 77.4° (vertical)
. 1/4" CMOS sensor in VGA resolution
. 1.5 Lux / F1.4

Networking
Alarm and
Event Management
Security
Users

Dimension

Weight

LED Indicator

Power

Approvals

Operating

Environments

System

Lens

Shutter Time

Image sensor

Angle of View

Minimum

Illumination

Video

Image Settings

Audio

Viewing System

Requirements

Installation, Management,

and Maintenance

Applications

. 10/100 Mbps Ethernet, RJ-45
. Protocols: IPv4, TCP/IP, HTTP, HTTPS, UPnP, RTSP/
RTP/RTCP, IGMP,SMTP, FTP, DHCP, NTP, DNS,
DDNS, and PPPoE
. Triple-window video motion detection
. One D/I and one D/O for external sensor and alarm
. Passive infrared sensor (PIR) for human detection
. White-light illuminators for low light condition when
event triggered
. Event notification using HTTP, SMTP, or FTP
. Muilti-level user access with password protection
. IP address filtering
. HTTPS encrypted data transmission
. Camera live viewing for up to 10 clients
. Ø 143 mm x 106 mm
. Net: 575.5 g
. System power and status indicator
. System activity and network link indicator
. 12V DC
. Power consumption: Max. 3.6 W
. 802.3af compliant Power-over-Ethernet
. Temperature: 0 ~ 50 °C (32 ~ 122 °F)
. Humidity: 20% ~ 80% RH
. Compression:
GSM-AMR speech encoding, bit rate:
4.75 kbps to 12.2 kbps
MPEG-4 AAC audio encoding, bit rate:
16 kbps to 128 kbps
. Interface:
Built-in microphone
External microphone input
Audio output
External/Internal microphone switch
. Supports two-way audio via SIP protocol
. Supports audio mute
. Compression: MJPEG & MPEG-4
. Streaming:
Simultaneous dual-streaming
MPEG-4 streaming over UDP, TCP, HTTP or HTTPS
MPEG-4 multicast streaming
MJPEG streaming over HTTP or HTTPS
. Supports 3GPP mobile surveillance
. Frame rates:
MPEG-4: Up to 30/25 fps at 640x480
MJPEG: Up to 30/25 fps at 640x480
. Adjustable image size, quality, and bit rate
. Time stamp and text caption overlay

. Flip & mirror
. Configurable brightness, contrast, saturation, sharpness, and white balance
. AWB
. Supports privacy masks
. OS: Microsoft Windows 2000/XP/Vista
. Browser: Internet Explorer 6.x or above
. Cell phone: 3GPP player
. Real Player: 10.5 or above
. Quick Time: 6.5 or above
. SDK available for application development and system integration

Warranty . 24 months

. 3-axis mechanism for flexible ceiling and wall mount installation
. Installation Wizard 2
. 16-CH recording software
. Supports firmware upgrade

P/N: 011000302 Ver 1.0

White-light LEDs

Status LED

Power Cord Socket

Ethernet 10/100 RJ45 Socket

Lens

Tilt Srew

Built-in MIC

PIR Sensor

Indented Reset Button

Focus Controller

Zoom Controller

External/Internal MIC Switch

General I/O Terminal Block

Image Adjustment

MIC In

Pan Screw

Audio Out

Recessed Kit PoE Injector

PC with
Recording Software

Speaker
External
Microphone

Router

Notebook with
Web Browser

3G Cell Phone

FD7131

6F, No.192, Lien-Cheng Rd., Chung-Ho, Taipei County, Taiwan
Tel: +886 2 8245 5282|Fax: +886 2 8245 5532|E-mail: sales@vivotek.com
VIVOTEK USA, INC.
470 Lakeside Drive Suite C, Sunnyvale, CA 94085 USA
Tel: 408-773-8686 | Fax: 408-773-8298 | E-mail: salesusa@vivotek.com

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY

NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE,

OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION,

PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE
PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE
WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT
WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/
OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO.
NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION
INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY
BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH
RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA
CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621;
CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621;
GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621;
SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT.
9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK
PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP.
8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO
TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT

HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired

operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant

to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful

interference in a residential installation. This equipment generates, uses and can radiate radio frequency

energy and, if not installed and used in accordance with the instructions, may cause harmful interference

to radio communications. However, there is no guarantee that interference will not occur in a partial

installation. If this equipment does cause harmful interference to radio or television reception, which

can be determined by turning the equipment off and on, the user is encouraged to try to correct the

interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which

case the user may be required to take adequate measures.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right
to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty
of any kind with regard to the material contained within this document, including, but not limited to, the
implied warranties of merchantability and fitness for any particular purpose.

Power Over Ethernet (PoE)

Introducción

La alimentación local y autónoma de un dispositivo resulta a menudo problemática cuando dicho elemento se pretende instalar en lugares poco accesibles o desprovistos de alimentación eléctrica; tal es el caso de las cámaras de vigilancia IP. Instalar alimentación eléctrica cerca de estos elementos puede resultar a veces muy dificultoso y caro.

Esta problemática se resuelve gracias a la tecnología PoE, diseñada para entregar a los dispositivos de red la alimentación que necesitan a través del propio cable de red.

En Junio del 2003, se aprobó el estándar IEEE 802.3af por el que se establecen las características de los equipos y tecnología PoE, definiéndose la máxima potencia que puede ser entregada a los dispositivos utilizando formatos de transmisión 10BASE-T, 100BASE-T y 1000BASE-T.

Anteriormente a este estándar, compañías como Cisco desarrollaron soluciones propietarias para alimentar remotamente dispositivos Ethernet. La tecnología de Cisco la llamaron Cisco Inline Power (ILP), lanzada en Marzo del 2000. Desde entonces, Cisco ILP ha sido instalado en numerosas redes anteriores a la aparición del estándar IEEE. Esta situación ha hecho que Cisco desarrollase una nueva tecnología de PoE retrocompatible con las instalaciones ILP.

Las ventajas de PoE son:

· Alimentación y comunicaciones de datos sobre el mismo cable

· Mayor control sobre el dispositivo

· Favorece la movilidad de los equipos (cambios de ubicación no requieren instalación de cableado eléctrico).

· Gestión de alimentación y monitorización vía SNMP

· No es necesaria la actualización del cableado (Cat5 o superior)

IEEE 802.3af

El estándar IEEE802.3af es capaz de entregar una potencia máxima de **15,4 Watt**., por puerto Ethernet, usando una tensión típica de **48 volt**. Se especifica una corriente alrededor de **350 mA** por conexión, que sobre 48 volt representan una potencia de **16W** por dispositivo. Los dispositivos a alimentar pueden ser puntos de acceso inalámbricos, teléfonos IP, cámaras IP, lectores de tarjetas, impresoras, existiendo también la posibilidad de alimentar otros elementos no contemplados hasta ahora en el estándar como ordenadores portátiles y de sobremesa. Estos dispositivos, por el momento, no es posible alimentarlos vía PoE.

IEEE 802.3af define dos principales piezas de hardware, el Dispositivo Alimentado (Powered Device – PD) y el Equipo de Alimentación (Power Sourcing Equipment – PSE). Una cámara IP es un ejemplo de PD y un switch con PoE es un ejemplo de PSE. Este estándar también define el proceso de detección de PD´s y como la alimentación se mantiene o se corta según el dispositivo que se conecte al switch.

PSE- Power Sourcing Equipment

El PSE tiene tres funciones primordiales:

· Detectar un PD que acepte PoE

· Suministrar alimentación al PD

· Monitorizar y cortar la alimentación cuando sea necesario.

Dentro de la definición de PSE, existen dos tipos descritos: PSE Final y PSE Intermedio. Un **PSE Final** es un **switch PoE** sobre el cual se conecta directamente el

latiguillo de conexión del dispositivo PD. Un **PSE intermedio** es un **adaptador** que tiene dos entradas (la alimentación y el cable de datos) y una sola salida RJ45 (datos y alimentación por cable de red).
Ejemplo de configuración con **PSE Final** (Switch PoE):
La alimentación que entrega el PSE Final alcanza el PD usando los **pares de datos activos** (normalmente el naranja y el verde – pines 1,2 y 3,6) o **pares separados** (marrón y azul – pines 4,5 y 7,8). Estas dos opciones se denominan Alternativa A y B respectivamente. La alternativa A usa los pares activos; y la alternativa B usa pares separados.
ALTERNATIVA A: Pares activos ALTERNATIVA B: Pares separados
Con objetivo de cumplir con el estándar IEEE 802.3af, el **PSE debe cumplir con ambas alternativas.** Sin embargo, sólo una alternativa debe ser usada para alimentar el dispositivo. La **más usada** es la alternativa **A**.
De acuerdo con el estándar, los dispositivos **PSE Intermedios** sólo suministarán PoE de acuerdo con la alternativa B (**pares separados**), y por tanto **no** podrán suministrar PoE a través de **1000-BASE-T** (donde todos los pares se usan para transmitir datos).
PD- Powered Device
Un PD que cumpla con el estándar IEEE 802.3af es capaz de ser alimentado de acuerdo con **las dos alternativas**, A y B. Existen en el mercado PD´s que sólo funcionan con alguna de las dos alternativas y por tanto no cumplen con el estándar.
El estándar define la posibilidad de que el PD especifique al PSE la alimentación que requieren. Según estos requisitos, los PD se clasifican en distintas clases. Los PD´s se pueden clasificar en clases de acuerdo con la potenc ia requerida. Estas clasificaciones son las siguientes:
· Clase 0: Desde 0,44 a 12,95 Watt
· Clase 1: Desde 0,44 a 3,84 Watt
· Clase 2: Desde 3,84 a 6,49 Watt
· Clase 3: Desde 6,49 a 12,95 Watt
Nota: La potencia sobre el PD es menor que la potencia medid a sobre el PSE, debido a la caída de tensión del cable. Por ejemplo, sobre un PD clase 0, el PSE puede suministrar hasta
15,4 Watt.
Los PDs suelen ser de **clase 0**.
El PSE averigua la clase del PD conectado inyectando tensión sobre el par positivo de alimentación y midiendo la atenuación de esta tensión sobre el par negativo de alimentación.
Un PD de clase 3 o 4 tiene ciertas ventajas sobre un PD que opera sólo en modo 15,4 Watt. Por un lado, si el PD puede funcionar con una potencia inferior a la máxima, el PSE puede suministrar menos potencia sobre ese puerto ahorrando parte de ella y pudiendo suministrarla sobre otro puerto. Por ejemplo, si existen tres cámaras conectadas que sólo requieren 6,3 Watt, el PSE puede ahorrar 9,1 Watt por puerto, lo que representa un ahorro total de 27,3 Watt. Esto puede implicar igualmente una disminución de calentamiento del PSE, alargando su vida útil.
Cómo Descubrir un PD Conectado
Un requerimiento obvio del estándar IEE 802.3af es evitar dañar dispositivos Ethernet que no necesitan PoE. Un PSE no aplicará tensión sobre un puerto hasta que se verifique que el PD conectado necesita alimentación. Esto ocurre antes de que se active el enlace Ethernet, obviamente, ya que el PD no está aún alimentado.

El proceso de detección especificado en el estándar 802.3af arranca desde el PSE examinando la conexión, probando si el PD soporta PoE. Este proceso se lleva a cabo aplicando una pequeña tensión limitada en corriente al PD sobre los pares de transmisión y recepción, midiendo la carga aplicada al dispositivo. Los PD´s que aceptan PoE tendrán una impedancia de 25 KO entre los pares de transmisión y recepción. Los PD´s que no presenten esta impedancia entre pares no recibirán alimentación. Una vez que se ha detectado un PD válido, se empezará con el proceso de clasificación.
El PSE enviará señales de detección sobre los pares activos e inactivos del puerto Ethernet para detectar el PD conectado, con un tiempo de espera de al menos 2 segundos entre señales. Esas señales de detección continuarán hasta que se requiera alimentación del PD. Si el dispositivo conectado no acepta PoE, dichas señales continuarán para comprobar el tipo de dispositivo conectado. El proceso de detección se debe producir en menos de 500 ms.

Desconexión de Alimentación

Si un usuario intercambia un dispositivo que acepta PoE por otro que no lo acepta, la tensión de 48 volt. podría ocasionar daños sobre este segundo dispositivo. El estándar IEEE 802.3af establece la desconexión de potencia hacia un dispositivo cuando no se cumpla el proceso de detección anteriorment e explicado. Cuando se termine la conexión, la alimentación debe ser interrumpida en un tiempo máximo de 250 ms.

PoE Plus

En Noviembre de 2004, se formó un grupo de trabajo con el propósito de crear PoE Plus. Este grupo está desarrollando el futuro PoE, con el principal objetivo de alimentar dispositivos que necesiten más del doble de la potencia máxima que establece el actual IEEE 802.3af, tal como ordenadores de sobremesa o portátiles.
Las características de PoE Plus son:

· Un PSE PoE Plus será compatible con el actual IEEE 802.3af, siendo posible la alimentación de PD´s 802.3af y PoE Plus.
· PoE Plus debe suministrar al menos 30 Watt a cada PD.
· Desarrollo de PSE Intermedios para funcionar con 1000BASE-T.
· Desarrollo de PSE Finales e Intermedios para funcionar con 10GBASE-T.

Posibles problemas con PoE

PoE es una tecnología muy resistente. Si el PSE y el PD hablan el mismo idioma (802.3af o Cisco ILP), los problemas de alimentación de dispositivos serán escasos o inexistentes. La mayor consideración a tener en cuenta cuando se usa PoE es el cálculo de la potencia máxima a suministrar por el PSE.
A continuación presentamos un ejemplo práctico:
En una oficina existen 220 cámaras IP y 15 puntos de acceso, todos ellos necesitados de PoE. Sin tener en cuenta la gestión de alimentación comentada, cada dispositivo puede requerir hasta 15,4 Watt., resultando un total de 3619 Watt. Además el switch suele necesitar una alimentación de 1500 Watt, por lo que el resultado suma una potencia total de 4200 Watt por switch.
No se puede dar por sentado que la alimentación eléctrica del cuarto de telecomunicaciones podrá proporcionar dicha potencia. Los típicos circuitos de alimentación de 230Volt/16Amp podrán suministrar como mucho **3680 Watt**., por lo que será necesaria una instalación especial. Adicionalmente, el sistema de refrigeración tendrá que ser estudiado para evitar excesivos sobrecalentamientos.

Sumario

PoE es una tecnología que a día de hoy podemos encontrar en prácticamente cualquier sitio. Con la creciente demanda de las tecnologías Wireless y VoIP, PoE está creciendo aún más. Antes de alimentar el dispositivo, el PSE testea si dicho dispositivo soporta 802.3af. Después de dicha detección, se aplicará una tensión de 48 volt y 350 mA. Si el PSE el del tipo Final, se usarán los pares de datos (1,2 y 3,6), y si se usa un PSE Intermedio normalmente se usarán los pares no utilizados (4,5 y 7,8).
La norma IEEE 802.3af define funciones que permiten alimentar al PD con la potencia estrictamente necesaria, gracias a una clasificación de los PD, la cual es detectada por el PSE.
El cálculo de la potencia total consumida y el sistema de refrigeración son factores muy importantes. Los sistemas UPS de reserva deben ser considerados.

Productos PoE ImaginArt:

1) CÁMARAS MOBOTIX:

Todas las series de Mobotix tienen PoE incorporado; posibilidad de alimentarlas con el adaptador PoE suministrado por el fabricante alemán o a través de switches compatibles con el estándar 802.3af.

Adaptador PoE de Mobotix

Esquema de red con adaptador PoE de mobotix:

Esquema de red con switch PoE final:

2) CÁMARAS VIVOTEK:

PoE incorporado: Nueva serie de cámaras **IP7131** (calidad VGA) e IP **7138** (MegaPixel), **IZ7151, FD7131, IP7151**

Posibilidad de alimentar estas cámaras directamente desde un switch compatible PoE o a través de un splitter (o "separador"): dispositivo que tiene dos entradas (el cable de datos UTP y la alimentación) y una única salida (el cable UTP con alimentación y datos) que irá directamente conectado a la cámara).

Esquema de red con Switch compatible PoE

Para el **resto de series**: posibilidad de hacer la tranmisión de datos y alimentación a través de PoE gracias al "KIT PoE" de Vivotek , con un inyector en un extremo (junta señal de alimentación y datos en cable UTP) y un separador (Splitter) antes de llegar ala cámara (con una salida de alimentación y otra de datos UTP). *Kit PoE de Vivotek*

Inyector PoE de Vivotek

PoE (Power Over Ethernet) 802.3af

? Definición: Datos y alimentación por un solo cable de datos ethernet, CAT5, CAT6.

? Utilidad: Reducir el cableado en una instalación, reducir el coste y a veces la dificultad de tener una toma de corriente para cada equipo.

? Elementos:

- Switch PoE --> Equipo de red que distribuye el acceso a la red a los distintos equipos, directamente por un solo cable ethernet con los datos y la alimentación.
- Midspan PoE --> Si el switch que disponemos no cumple con PoE, existe este equipo, situado entre el switch normal y los equipos a los cuales hay que dotar de acceso a la red. De este equipo saldran todas las connexiones con un solo cable (con datos y alimentación) alos diferentes equipos.
- Splitter --> Elemento que separa la señal de datos de la alimentación para los equipos que no esten preparados para recibir las 2 señales en un solo cable ethernet.

? Distinción:

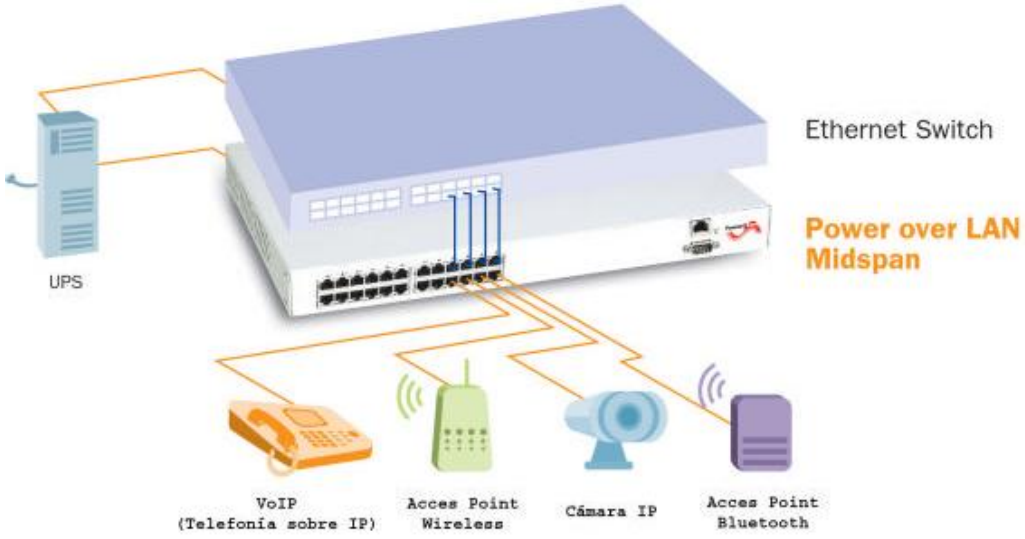
- Equipos que cumplen 802.3af --> Se les puede conectar directamente el cable ethernet que proviene del Switch PoE, o del Mid span PoE con los datos y la alimentación al puerto RJ45.
- Equipos que **NO** cumplen 802.3af--> Antes de conectarles lo que viene por el único cable ethernet, es necesario disponer del Splitter, para entregar por separado los datos por el puerto RJ45, y la alimentación por el connector de alimentación.

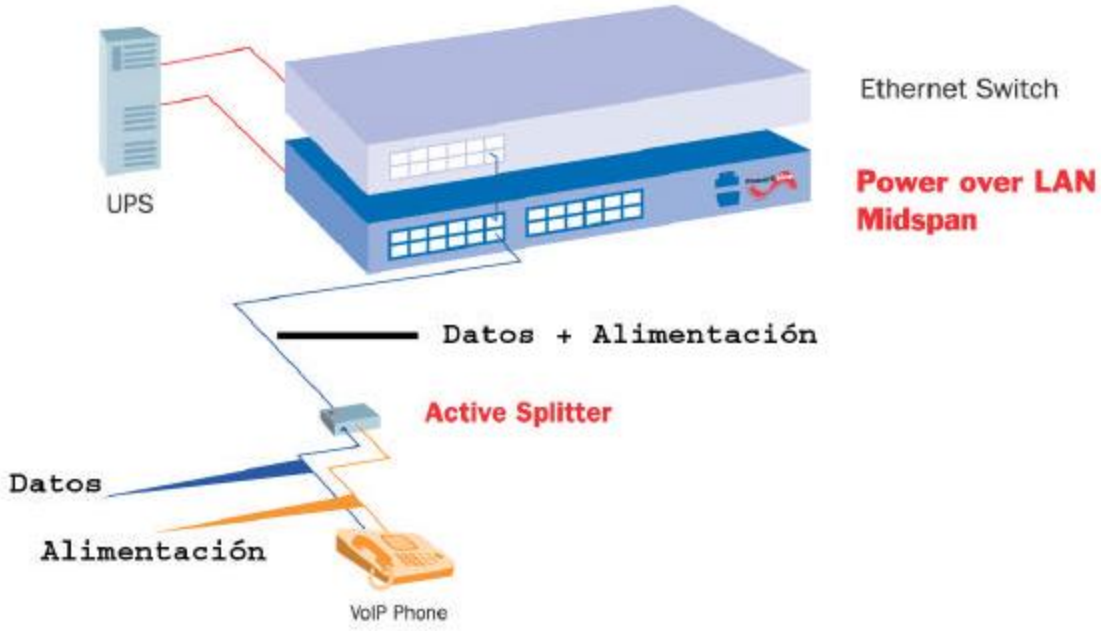
? Nuestros proveedores:

- Vivotek --> ningún modelo está preparado para PoE (802.3af). Vivotek lo soluciona con su propio Midspan (individual, uno por cámara) y su propio Splitter.
- Mobotix --> Su propia solución. Como accesorio tiene el midspan (alimentador PoE). No hace falta Splitter, la cámara soporta los datos y la alimentación que entren juntas por el puerto RJ45. Como accesorio tiene midspan para 4, 8 y para 20 cámaras.
- Sony--> Modelos preparados para 802.3af: Z20P, DF40P, DF70P
Los demás modelos, requieren de Splitter.
- Canon--> Su modelo requiere de Splitter

? Esquema con Switch estandard y Midspan PoE:

? Esquema con Splitter


Ethernet Switch
Power over LAN
Midspan
UPS
VoIP
(Telefonía sobre IP)
Acces Point
Wireless
Cámara IP
Acces Point
Bluetooth


Ethernet Switch
Power over LAN
Midspan
UPS
Datos + Alimentación
Active Splitter
Datos
Alimentación
VoIP Phone

FACULTAD DE INGENIERIAS Y CIENCIAS AGROPECUARIAS ESCUELAS DE TECNOLOGÍAS DE REDES Y TELECOMUNICACIONES

ESTUDIO E IMPLEMENTACION DE UN SISTEMA DE VIGILANCIA Y MONITOREO IP SOBRE UNA INTRANET

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de
Tecnólogo en Redes Y Telecomunicaciones

Profesor Guía

Ing. David González

Autor

Santiago García Jaramillo

Año

2011

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

…….

David González

Ingeniero

CI: 171598487-6

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

…….

Santiago García

171658923-7

RESUMEN

En el presente proyecto se explicará como implementar un Sistema de Vigilancia y Monitoreo basado en “IP” (Protocolo Internet), se expondrán los conceptos básicos de lo que son las redes de datos y el funcionamiento de estas, además se expondrá los protocolos utilizados para la captura y transmisión de streaming (flujo de datos multimedia), se expondrá los equipos a utilizar, estándares de funcionamiento y características de estos, además se expondrá paso a paso el cómo configurar todos los equipos del Sistema de Vigilancia y Monitoreo IP, además se explicara cómo funcionará el mismo.

ABSTRACT

In this project we will explain how to implement a surveillance and monitoring system based on "IP" (Internet Protocol), should be present the basics of what are the data network and the operation of these, plus should be exposed to protocols used capture and transmission of streaming (multimedia data stream), should be expose the equipment to use, standards of operation and characteristics of these also, should be explain step by step how to configure all devices in the Surveillance and IP Monitoring, besides will be explained how to operate it.

INDICE

Índice de Figuras

Índice de Tablas

Introducción

La implementación de un Sistema de Vigilancia y Monitoreo IP es conveniente debido a que en la actualidad contamos con cableados de redes de datos en las infraestructuras de nuestros lugares de trabajo e incluso en nuestros hogares. Conjuntamente contamos con la convergencia, que es la capacidad de las redes de datos de comunicar servicios multimedia como voz (VoIP: Voz sobre Protocolo Internet) y vídeo (IPTV: Vídeo sobre IP) principalmente. Por lo cual en la actualidad es factible y conveniente un "Sistema de Vigilancia y Monitoreo" usando tecnología IP, utilizando de mejor manera los beneficios que nos brindan las redes de datos.

Aprovechando la convergencia y a través del cableado de redes de datos, se implementará un sistema de vigilancia y monitoreo IP, el cual trabajara a través de dicho cableado, empleando estándares internacionales para su funcionamiento como el MPEG4 para el vídeo, AAC y GSM-AMR para el audio los cuales han sido optimizados para este tipo de aplicaciones. Ofreciendo como resultado gran calidad de imagen en las transmisiones de vídeo, con un pequeño consumo de AB en comparación a otros métodos; lo cual resulta de gran utilidad ya que a lo largo de la red en las diferentes dependencias contamos con distintos valores en el “ancho de banda” que usan cada una de estas dependencias.

Para la implementación del sistema se contara con cámaras IP y GVR (Grabador de Vídeo en Red), los cuales se integrarán a la red del cliente encargándose de transmitir los sucesos de las diferentes dependencias a la central de monitoreo y grabar los mismos en los GVR´s colocados en cada dependencia según se requiera.

La colocación de los equipos se la realizará en base a las necesidades de cada dependencia, la central de monitoreo será la que monitoreará constantemente y en a la que se almacenarán los sucesos previamente grabados en los GVR de cada dependencia, según el administrador del Sistema de Vigilancia y Monitoreo IP lo requiera.

Capítulo I

ESTUDIO E IMPLEMENTACION DE UN SISTEMA DE VIGILANCIA Y MONITOREO IP

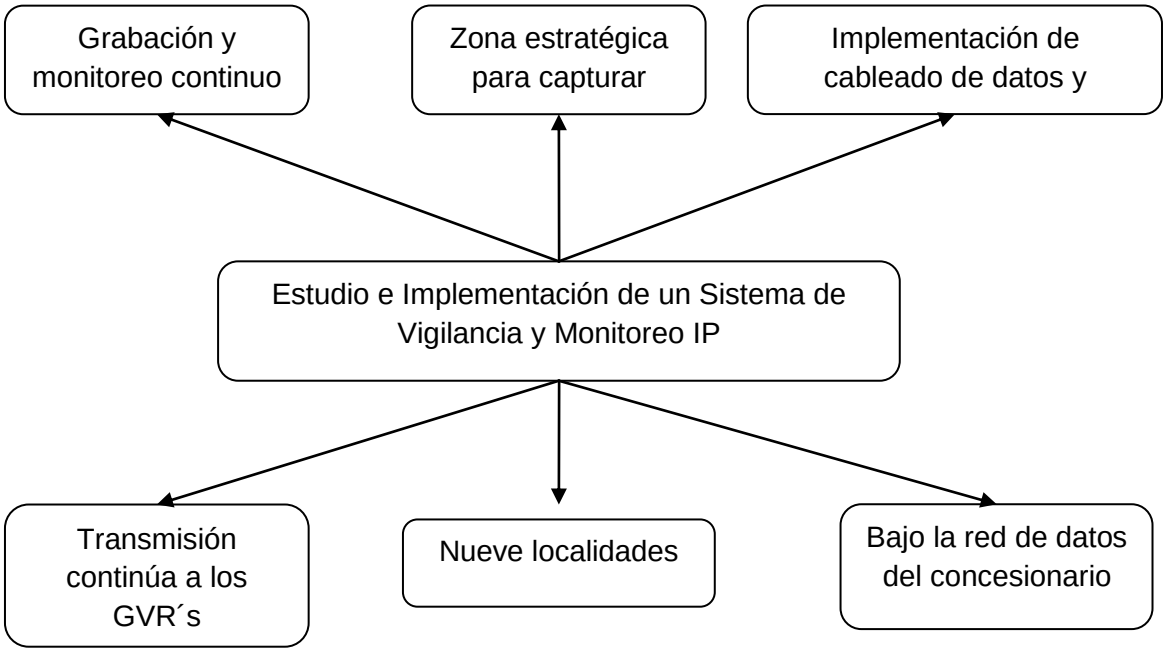
1.1 Contextualización

Actualmente los Sistemas de Vigilancia y Monitoreo IP son usados alrededor del mundo por empresas, instituciones e incluso en muchos hogares, siendo estos sistemas principalmente orientados a la seguridad, empleados de igual manera para monitoreo de ciudades, exploración de lugares donde no puede accesar una persona, en robots enviados incluso a otros planetas, entre otras. Los que son orientados a seguridad comparten por lo general los eventos con empresas privadas de seguridad ya que debido a la flexibilidad de este tipo de sistemas, a la facilidad que hay al contratar servicios de Banda Ancha es muy común que se esté migrando de los sistemas de vigilancia analógicos a este tipo de sistemas que se los denominaría como digitales.

En Ecuador a pesar de no ser muy común la utilización de sistemas de seguridad basados en IP, también se cuenta con este tipo de sistemas, como por ejemplo en los circuitos de vigilancia existentes en estaciones de transporte público como: (en Quito) El Trolebús, El Corredor Central Norte, La Ecovía, (en Guayaquil) La Metrovía; todos estos cuentan con una rede de datos a lo largo de todas sus estaciones o paradas, sobre la cual en su mayoría posee un sistema de vigilancia IP. Sin embargo uno de los más grandes y del cual se ha aprovechado mejor su aplicación es el sistema "Ojos de Águila", el cual trabaja a través de la red del Municipio de Quito, que ha revelado las locaciones de mayor peligro en sectores de la ciudad, además es usado para monitoreo del tráfico en la capital, aunque su cobertura es limitada ya que no cubre el distrito metropolitano en su totalidad (solo cubre alrededores de la trayectoria del Trolebús).

1.2 Análisis Crítico.

Figura 2. 1.1 Análisis Crítico



Fuente: Santiago García

1.3 Formulación del Problema.

Se implementará un Sistema de Vigilancia y Monitoreo IP, de manera que desde una central de monitoreo, se pueda gestionar y visualizar lo que sucede en las diferentes dependencias.

1.4 Delimitación del Proyecto.

El desarrollo del proyecto incluyendo el estudio e implementación del mismo, va hacer realizado por el Sr. Santiago García Jaramillo, estudiante de la Universidad de las Américas en la ciudad de Quito, desde el 15 de Abril hasta aproximadamente el 5 de Julio del 2010.

1.5 Interrogantes.

1.5.1 ¿Dónde se implementará?

El proyecto será implementado en la Intranet de un concesionario de autos, que se compone de cinco dependencias conectadas a una oficina matriz en Quito y otras dos sucursales conectadas a otra oficina matriz en Guayaquil, las oficinas matrices cuentan con un enlace de fibra óptica que las conecta entre sí a altas velocidades.

1.5.2 ¿Qué se necesita?

Anchos de banda en los se puedan transmitir audio y vídeo de las cámaras IP, cableado eléctrico para energizar las cámaras, cableado de red para conectar las cámaras a la red de datos, cámaras IP, GVR´s (Grabador de vídeo en red), un equipo (PC) para la central de monitoreo y elementos de la red IP en la que se trabaje como switches, routers entre otros.

1.5.3 ¿Cómo trabajará el sistema de vigilancia y monitoreo IP sobre la red?

El sistema de vigilancia y monitoreo IP trabajará con una o más cámaras, dependiendo de cada sucursal o matriz. Transmitirá vídeo en vivo desde las dependencias y matriz de Guayaquil a un centro de monitoreo en la matriz de Quito, contará con un GVR de pequeña capacidad de almacenaje que grabará los sucesos en cada dependencia y uno de gran capacidad en la central de monitoreo el cual gestionará los archivos deseados desde las dependencias según el administrador lo requiera.

1.6 Objetivos.

1.6.1 Objetivo general

"Implementar un Sistema de Vigilancia y Monitoreo IP sobre la Intranet de un Concesionario de Automóviles"

1.6.2 Objetivos específicos

a. *Analizar y especificar los protocolos a utilizarse para la transmisión de voz y vídeo sobre la red de datos.*

b. *Analizar las características de la Intranet del concesionario, paralelamente determinar los requerimientos para la transmisión y recepción de vídeo.*

c. *Diseñar un Sistema de Vigilancia y Monitoreo IP, y definir equipos a utilizarse.*

d. *Implementar y probar el Sistema de Vigilancia y Monitoreo IP.*

1.7 Justificación.

Actualmente y en especial en Ecuador se cuenta con sistemas de vigilancia y monitoreo, en su mayoría analógicos. Los cuales requieren de un cableado adicional, su calidad de imagen no es muy buena, no se puede transmitir el vídeo en vivo y para hacerlo se necesita de una gran inversión, entre otras limitaciones generadas por el tipo de tecnología.

Al implementar sistemas de vigilancia y monitoreo IP obtenemos: mayor calidad de imagen en la transmisión y recepción de vídeo, facilidad en el almacenamiento de voz y vídeo, además permite la transmisión del audio y vídeo en vivo desde varias localidades a través del Internet o de una Intranet (red privada que utiliza tecnología IP para compartir de forma segura cualquier información o programa).

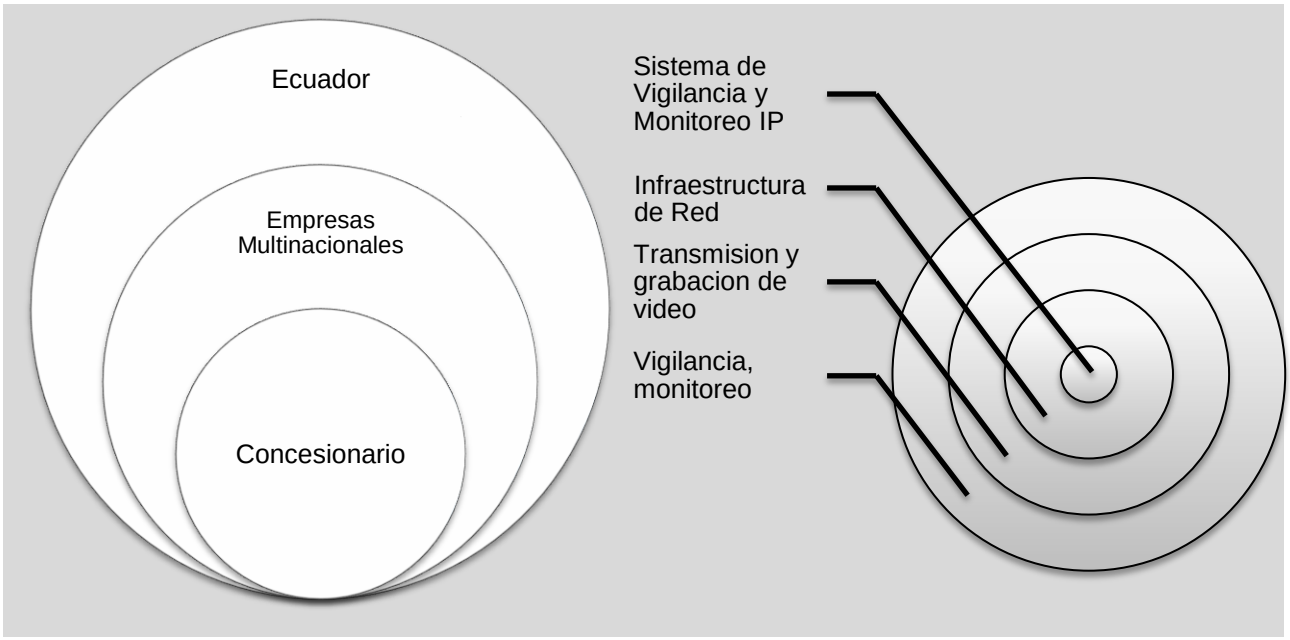
Logrando con esto ahorro de tiempo y de costos de infraestructura, ya que se utilizaría la red de datos previamente implementada, e incluso el estructurarla o ampliarla no es tan costoso como con sistemas analógicos, además nos brinda gestión, control y acceso remoto a la mayoría de elementos en la red IP, así como del sistema de vigilancia y monitoreo entre otros beneficios.

En base a estas consideraciones se implementará un Sistema de Vigilancia y Monitoreo IP, ofreciendo así una solución inteligente de tener bajo un mismo sistema de monitoreo todas las dependencias (seis en Pichincha y tres en Guayas) pertenecientes a un Concesionario de Automóviles.

Capítulo II

2.1 Mapa de Inclusión.

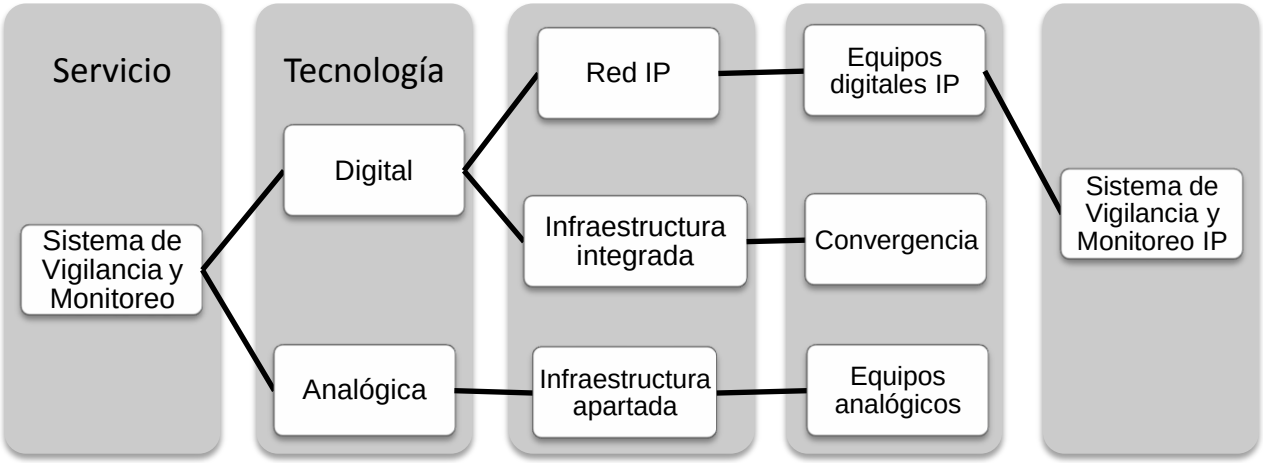
Figura 2.1. Mapa de Inclusión



Fuente: Santiago García

2.2 Constelación de Ideas.

Figura 2. 2. Constelación de Ideas



Fuente: Santiago García

2.3 Metodología del Proyecto.

2.3.1 Características Generales

El análisis e implementación del proyecto se llevará a cabo en un concesionario de automóviles, se contará con la colaboración del personal encargado del área técnica para la especificación, análisis y reconocimiento de la estructura de la Intranet.

2.3.2 Metodología a utilizar

En el desarrollo del proyecto se usará el método descriptivo mediante el cual se realizará un análisis detallado de cómo y que se necesita para la implementación de un Sistema de Vigilancia y Monitoreo IP; desde los análisis previos hasta las pruebas e instalación del mismo.

2.3.3 Métodos y técnicas a utilizar

a) La información se recopilará con ayuda de personal del área técnica del concesionario, la misma que se complementará con visitas, en las que se realizarán análisis y se ejecutarán reconocimientos de la Intranet

b) Se determinará los requerimientos de la Intranet, para la implementación de protocolos de transmisión, recepción de voz y vídeo IP, mediante la investigación de estándares internacionales para aplicaciones multimedia sobre IP, de igual forma en base a estándares de funcionamiento y características de los equipos a implementar.

c) Se detallará que elementos compondrán el SVMIP, además se diseñará la distribución de los mismos en base a la información recopilada de esquemas, estudios y de las visitas realizadas.

d) Será implementado, en base al diseño, realizando trabajos adicionales como: Cableado para energizar las cámaras IP, cableado de red para conectarlas a la Intranet y otros trabajos según se requieran al momento de la implementación.

2.3.4 Recursos del Proyecto

a) Recursos Humanos:

Nombres	**Personal**
David González	Coordinador del Proyecto
Patricio Jácome	Coordinador del Proyecto por parte del concesionario.
Santiago García	Técnico 1
Franklin Quiroz	Técnico 2
Nelson Tutillo	Técnico 3

b) Recursos Materiales:

Tipo de Material	**Modelo**	**Cantidad**
Cámara IP tipo domo a color	FD7131	17
Cámara IP tipo tubo exterior	IP7330	5
Disco Duro (HDD) SATA 1TB	WD10EACS	8
GVR 4 canales, 1 HDD	QN-GVR-104V	6
GVR 20 canales, 5 HDD	QN-VS-5020	1
Herramientas para Instalación	Varios	_

Tabla 1 - Recursos materiales

c) Recursos Financieros:

Concepto de gasto	**Presupuesto**
Transporte	80 USD
Viáticos	120 USD
Imprevistos	50 USD

Tabla 2 - Recursos financieros

2.3.5 Presupuesto del Proyecto.

Para la implementación del proyecto se requieren 12000 dólares los cuales se distribuyen de la siguiente manera:

Se destinarán 8000 dólares a la adquisición de los equipos tal como se detalla a continuación:

Equipo:	**Cantidad:**	**Costo:**
Cámaras IP domo	17	3400
Cámaras IP externas	5	1500
Discos Duros HDD	8	650
GVR´s de 20 canales	6	2400
GVR de 40 canales	1	500
Total		**8450**

Tabla 3 - Presupuesto de Equipos

Se destinarán 3550 al pago por mano de obra configuración e instalación del SVMIP.

Este valor incluye la compra de material adicional como: cableado canaletas decorativas, tubería entre otros.

2.3.6 Cronograma de actividades.

	Número de Semanas							
Actividades	1	2	3	4	5	6	7	8
Análisis de la red								
Análisis de protocolos y								

requerimientos								
Diseño del sistema								
Selección de equipos, análisis de costos								
Implementación del proyecto								
Pruebas y evaluación del proyecto								
Capítulo 1								
Capítulo 2								
Capítulo 3								
Capítulo 4								
Capítulo 5								
Entrega de Informe								

Tabla 4 - Cronograma de actividades

Capítulo III

3.1 Redes Convergentes

3.1.1 Las Redes de Datos

Son redes de computadores, las cuales son diseñadas para transmisión de información mediante intercambio de datos entre dispositivos, las mismas que están conformadas por los siguientes elementos:

Elemento:	Función:
Dispositivos	Elementos o equipos que conforman la red de datos o el segmento de la misma: PC´s, impresoras, teléfonos IP, etc.
Terminal	Medio por el cual ingresan los mensajes a transmitir, por ejemplo un teclado de PC, mouse, teléfono IP. Medio por el cual se muestran los mensajes recibidos, por ejemplo: Un monitor de PC, teléfonos IP, parlantes de PC.
Reglas	Estándares y protocolos los cuales definen como trabaja una red. "TCP/IP"(Protocolo de Control y Transmisión Protocolo Internet). TCP/IP.- Encargado de seleccionar el camino para el envió del mensaje, además mediante el cual se establece una "red de datos" y es el que define el segmento al que pertenecen los dispositivos.
Medio	Es el medio físico por el cual fluirá la información: El aire en redes inalámbricas, ya que utiliza ondas de radio. El plástico o vidrio en fibra óptica ya que utiliza luz. El cobre en cables de par trenzado, coaxiales, UTP (cuatro pares trenzados) ya que utiliza pulsos eléctricos.
Mensaje	Son los datos de texto o multimedia que se van a transformar en "bits" (señales digitales), para ser transmitidos por la red de datos.

Tabla 5 - Elementos de las redes de datos

- Ejemplo de una red de datos:

En la "Figura 1" se representa un chat local entre el "usuario A" mediante un terminal de entrada (el teclado) teclea y envía un saludo al "usuario W", este saludo se convierte en bits (dígitos binarios), sale del computador y por medio de un cable UTP se dirige a un dispositivo de distribución en la red (switch),en el cual se conectan un grupo de usuarios (usuarios B,C,…..Z) y mediante las reglas (TCP/IP) encuentra y entrega el saludo al "usuario W", mismo que visualiza el saludo por un terminal de salida (la pantalla).

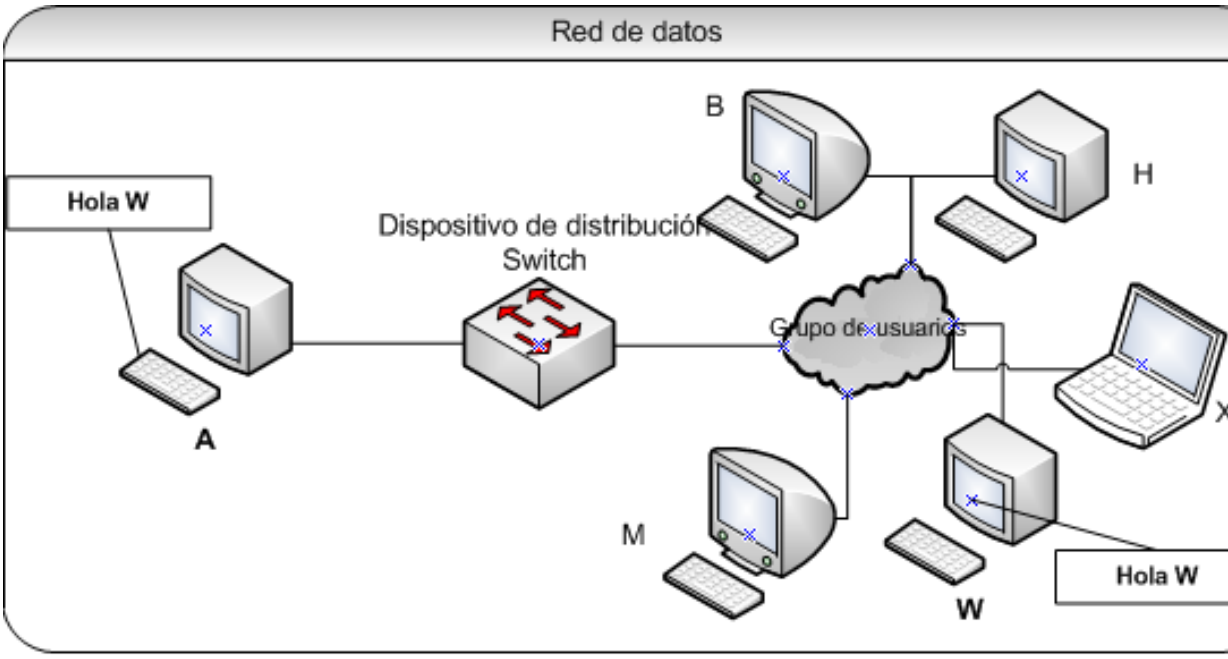


Figura 1 - Ejemplo de Red de Datos

Las redes de datos se diseñan según los objetivos de uso, funcionan mediante “conmutación de paquetes”, que es el intercambio de la información la cual es dividida en pequeños grupos de bits (paquetes) los cuales son enviados a través de una o más rutas a un mismo destino en el cual se re-ensamblan a su estado original para ser leída y mostrada a través de los terminales. En la “Figura - 2” se puede apreciar un ejemplo de conmutación de paquetes:

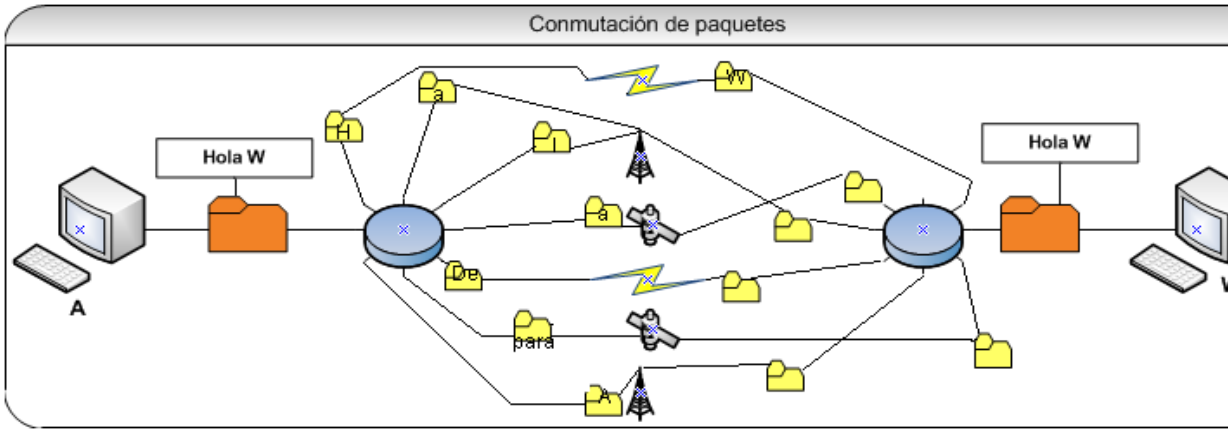


Figura 2 - Conmutación de Paquetes

3.1.2 Convergencia

Es la capacidad de las redes de datos de transportar servicios multimedia simplificando el uso de aplicaciones, dándole un uso más eficiente al ancho de banda. La convergencia se construye bajo una arquitectura de red multipropósito, funcionalmente distribuida y basada en IP.

En conclusión las redes convergentes son las redes en las que tenemos adicionalmente servicios multimedia, con dispositivos y terminales orientados a este tipo de servicios los cuales están integrados a nuestra red.

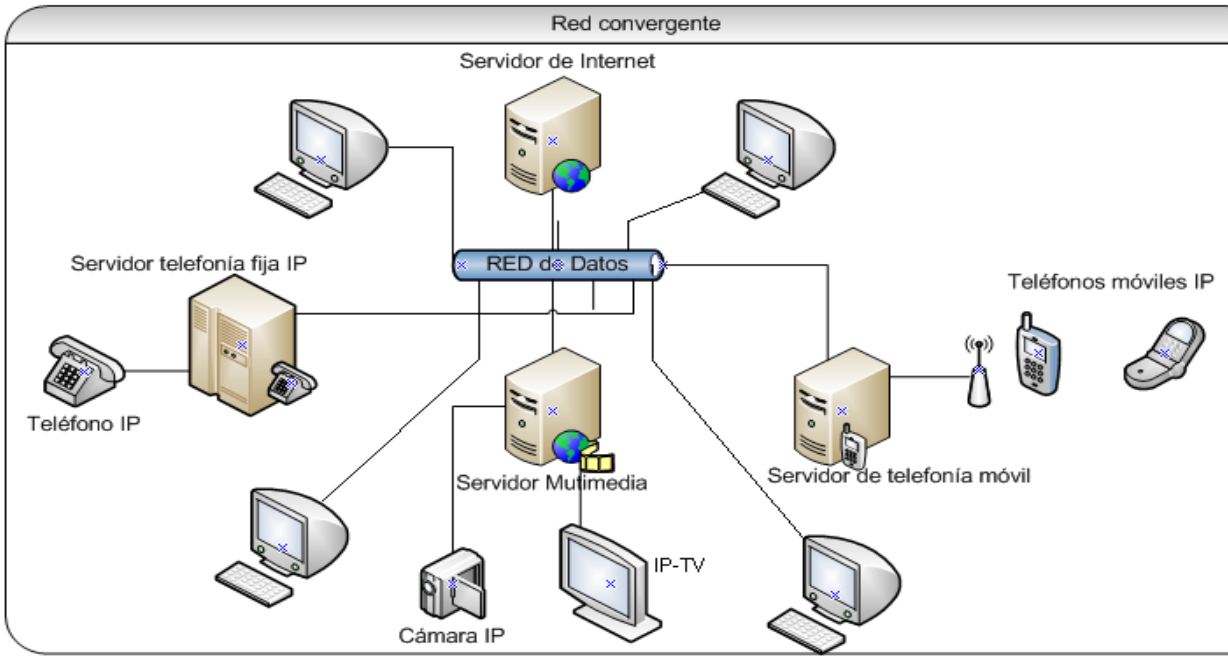


Figura 3 - Red Convergente

3.2 Análisis de la Intranet y Requerimientos del Concesionario

3.2.1 Estructura y Características de la Intranet del Concesionario

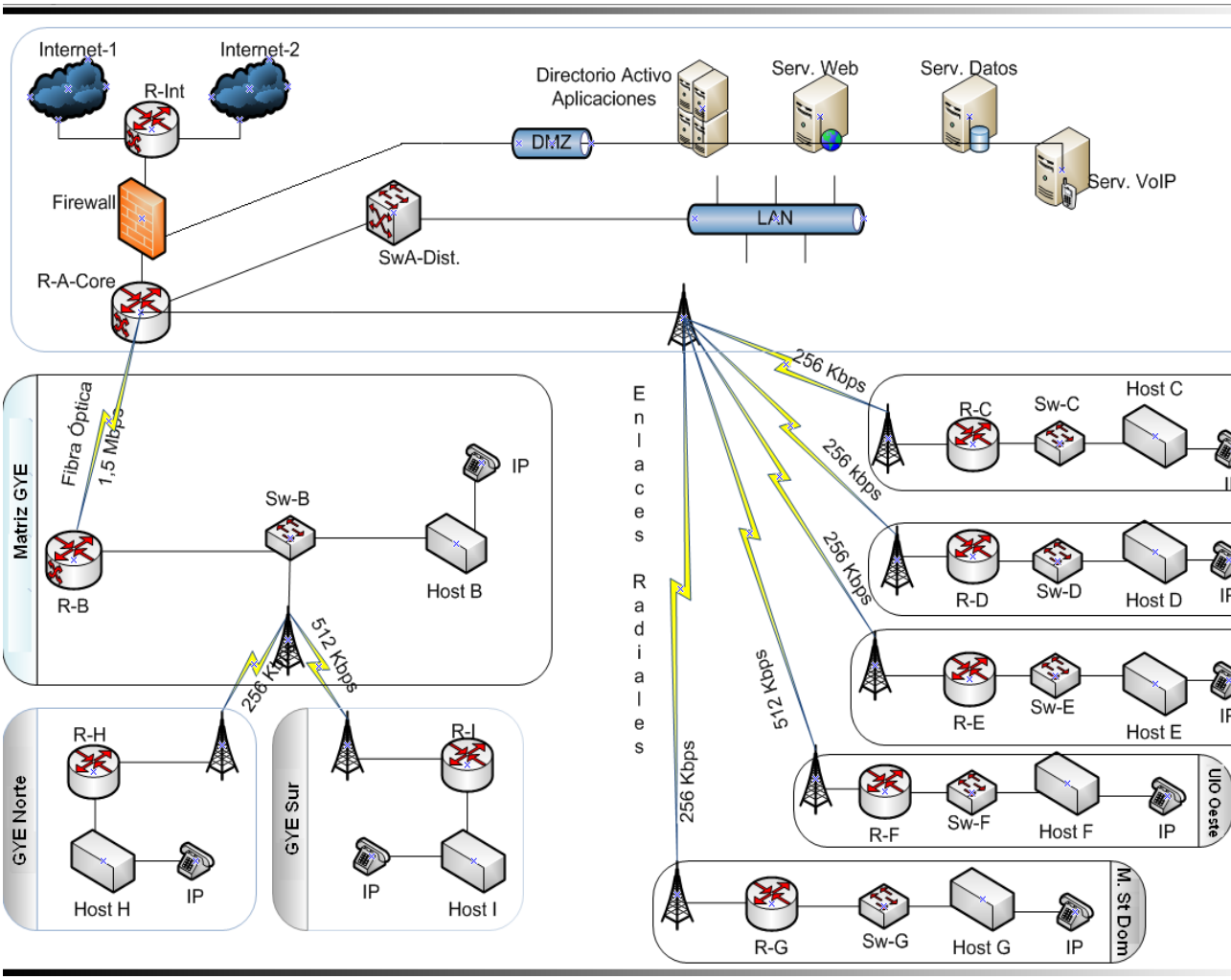


Figura 4 - Estructura de la Intranet del concesionario

- Matriz UIO (**A**)

  En esta se encuentra una central de datos la cual ofrece el servicio de Internet, datos, acceso a aplicaciones, base de datos de repuestos, directorios y también cuenta con un Firewall para seguridad de la DMZ.

  Esta agencia es a su vez la estación central a la cual mediante enlaces radiales se conectan las sucursales: C, D, E, F, en UIO.

Además conectándose mediante un enlace de F.O. (Fibra Óptica) a la "Agencia Matriz GYE" (B) que a su vez mediante enlaces radiales se conecta a las sucursales: H, I, en GYE.

- Matriz Santo Domingo (**C**)

  Se conecta mediante un enlace de 256 Kbps.

- Sucursal UIO - Oeste (**D**)

  Se conecta mediante un enlace de 256 Kbps.

- Sucursal UIO - Norte (**E**)

  Se conecta mediante un enlace de 256 Kbps.

- Sucursal UIO - Este (**F**)

  Se conecta mediante un enlace de 512 Kbps.

- Sucursal UIO - Sur (**G**)

  Se conecta mediante un enlace de 256 Kbps.

- Matriz GYE (**B**)

  Se conecta mediante un enlace de 1,5 Mbps

- Sucursal GYE - Norte(**H**)

  Se conecta mediante un enlace de 256 Kbps.

- Sucursal GYE - Sur (**I**)

  Se conecta mediante un enlace de 512 Kbps.

Para más detalles acerca de la intranet del concesionario ver: Anexo 1, Estructura detallada de la Red.

3.2.2 Requerimientos del Concesionario

En la siguiente “Tabla – 6” se enumerara las cámaras que requiere dependiendo la agencia y las áreas a las que estas serán orientadas.

Agencia	Cámaras	Tipos	Áreas
Matriz UIO	4 2	Internas Externas	Entradas internas – externas, ventas, show room, recepción, talleres.
Sto. Domingo	2	Internas	Entrada interna, ventas.
UIO Oeste	1	Externa	Entrada taller.
UIO Norte	3	Internas	Entrada interna, entrada trasera, caja, gerencia.
UIO Este	1 1	Interna Externa	Entrada externa, parqueadero, ventas.
UIO Sur	1	Externa	Entrada interna.
Matriz GYE	2	Interna Externa	Entrada externa, parqueadero, ventas, show room.
GYE Norte	2	Internas	Entrada interna, caja.
GYE Sur	2	Internas	Entrada interna, ventas.

Tabla 6 - Requerimientos del Concesionario

3.3 Análisis de Tráfico Generado por el Sistema

En base a estándares de calidad orientados a los Sistemas de Vídeo Vigilancia IP, se calculará un aproximado del tráfico que generará el SVMIP.

El consumo en disco será igual al "bitrate"(cantidad de dígitos binarios o bits) o tasa de bit, que genere cada cámara, el cual está definido por "bps" bits por segundo.

Las transmisiones de vídeo IP trabajan en función de:

3.3.1 Bitrate

Cantidad de dígitos binarios generados en determinada cantidad de tiempo:

a) CBR (constante bitrate).- Cuando el flujo de bits es constante en una cantidad de tiempo, sin que la tasa de bits dependa de lo que se esté capturando y transmitiendo.

b) VBR (variable bitrate).- Cuando el flujo de bits varia constantemente en una cantidad de tiempo, es decir que la tasa de bits varía según lo que se capture y transmita.

3.3.2 Resolución

Tamaño del vídeo, el cual se define en base a CIF (Formato Intermedio Común):

Resolución:	**Tamaño:**	**Observaciones:**
SQCIF	128x99	Fuera de estándares.
Sub-Cuarta CIF		Utilizado en aplicaciones móviles y de telefonía celular.
QCIF	176x145	Resolución mínima estándar.
Cuarta CIF		Utilizado en aplicaciones móviles y de telefonía celular
CIF	320x160	Resolución media estándar.
		Utilizado como resolución mínima estándar en aplicaciones multimedia de alta calidad.
2CIF	640x320	Resolución máxima dentro del estándar.
		Utilizado como resolución estándar en aplicaciones multimedia de alta calidad.
4CIF	1280x640	Resolución máxima con la que ciertas cámaras IP trabajan. Resolución alta en

aplicaciones multimedia.

Tabla 7 - Resoluciones de Imagen

3.3.3 Cuadros por segundo (FPS)

La cantidad de imágenes captadas en un segundo, define la secuencia del movimiento a más Fps. más fluido será el movimiento captado y a menos Fps. menos fluido será este, como se explicará en la siguiente tabla:

FPS:	**Secuencia:**	**Observaciones:**
1 a 10	Mínima	La fluidez del movimiento sería brusca no secuencial
10 – 20	Media (aceptable)	La fluidez del movimiento sería casi normal
20 – 30	Máxima (ideal)	La fluidez del movimiento sería normal

Tabla 8 - Cuadros por segundo

Los Fps. dependen del nivel de actividad en el área y lo que se requiera captar en la misma ya que si es un área de gran actividad deberían captarse la mayor cantidad de Fps. posibles, en cambio si es un área de muy poca actividad captar todos los Fps. sería innecesario ya que la mayoría de estos serían los mismos.

3.3.4 Tasa de bits en base a CIF y Fps.

La tabla a continuación “Tabla – 9” es solo para el formato MPEG-4 no se ha determinado para MJPEG ya que a pesar de ser usado con frecuencia en sistemas de vídeo vigilancia IP no es considerado en estándares de calidad para vídeo vigilancia ya

que con este formato se generan muchas perdidas en calidad y secuencia de la captura.

A continuación en base a los estándares mencionados y a valores manejados por proveedores de sistemas de vigilancia IP, expondremos una tabla con un bitrate aproximado que generaría cada cámara IP, en el sistema según los parámetros a emplearse:

Resolución	Calidad Equivalente	Fps.	Captura de Movimiento	Kbps (aprox)
CIF	Baja	3	Baja	160
CIF	Baja	7	Media	185
CIF	Baja	15	Media alta	200
CIF	Baja	30	Alta	500
2CIF	Media	3	Baja	320
2CIF	Media	7	Media	370
2CIF	Media	15	Media alta	400
2CIF	Media	30	Alta	1000
4CIF	Alta	3	Baja	640
4CIF	Alta	7	Media	740
4CIF	Alta	15	Media alta	800
4CIF	Alta	30	Alta	2000

Tabla 9 - Tasa de Bits en base Fps. y CIF.

3.4 Análisis de protocolos

Debido a que las cámaras IP trabajan en base a protocolos y estándares, se los describirá y explicará su funcionamiento.

Ciertas cámaras IP en su mayoría las usadas en aplicaciones en interiores cuentan con servicios para emisión y recepción de audio por lo cual se verá acerca de VoIP y protocolos de compresión de audio.

3.4.1 VoIP

Voz sobre el Protocolo Internet, es la tecnología que permite transmitir audio utilizando como medio a las redes IP. Trabaja mediante conmutación de paquetes por medio de códecs (codificadores-decodificadores) encargados de transformar la señal analógica de la voz en impulsos eléctricos (señal digital) y así transmitirla a través de la red; a diferencia de la telefonía analógica, la cual trabaja mediante conmutación de circuitos enlazando al emisor con su destinatario.

Funciona mediante protocolos entre los cuales el más importante es el "SIP" (Sesion Inition Protocol – Protocolo de Inicio de Sesión), en cargado de la transmisión de audio en tiempo real el cual es usado por aplicaciones como: NetMeeting y Skype, entre otros para la realización de llamadas IP. Es el encargado de establecer, modificar, finalizar transmisiones de audio y vídeo tipo conferencia, usado generalmente en telefonía IP y Vídeo conferencia, ya que registra y localiza a los participantes para una transmisión.

Está compuesto por:

Elemento	**Función**
Vía	La ruta de la transmisión (Tx).
From - Desde	Indica el origen de la Tx.
To - Para	Indica el destino de la Tx.
Call Id – Identificador de llamada	Contiene la dirección física (dirección Mac) del host, relaciona peticiones y respuestas.

Tabla 10 - Elementos de SIP

Puede ser utilizado en diferentes formatos de compresión en transmisiones IP compatibles con el estándar de SIP, entre los cuales a continuación se vera los más comunes en Sistemas de Vigilancia IP:

a. ACC

El AAC (Código Avanzado de Audio) es una extensión de los formatos MPEG especialmente del mpeg2. Su rendimiento excepcional en cuanto a compresión y calidad de audio ha hecho que este se encuentre dentro de los estándares MPEG-4, "3GPP y 3GPP2" (3ra generación de proyectos asociados), formatos de vídeo utilizados en aplicaciones de vídeo para equipos móviles como por ejemplo celulares, entre otros. Convirtiéndolo en la mejor opción en cuanto a aplicaciones para Internet, aplicaciones inalámbricas y de radio difusión digital, entre otras aplicaciones.

b. AMR

AMR (Compresión Adaptiva Multitasa) es un formato de compresión de audio optimizado para la codificación de audio utilizado en vídeos 3GPP. Aunque los niveles de calidad no son muy buenos ha sido orientado a aplicaciones móviles debido a su alto nivel de compresión y por lo tanto mínimo consumo de ancho de banda y de almacenamiento.

3.4.2 Vídeo IP

Funciona de una manera parecida a VoIP. Por medio de "códecs" (codificador-decodificador), transformando el streaming de vídeo analógico en digital y lo transmite por la red IP mediante broadcast, siendo una transmisión unidireccional de un archivo con streaming de vídeo. Además de la misma manera que VoIP trabaja por medio de SIP para la transmisión del vídeo.

Cabe mencionar que los terminales o equipos finales son solo visualizadores pasivos sin control sobre la sesión; además la transmisión desde el servidor hacia los equipos finales puede ser:

Tipos de Tx:	**Características:**
Unicast	Cuando el servidor hace un réplica de la transmisión para cada visualizador terminal.
Multicast	La misma señal es enviada sobre la red como una sola transmisión, pero hacia varios terminales o hacia un grupo de usuarios.

Tabla 11 - Tipos de Transmisión

El vídeo IP es utilizado en vídeo conferencias e incluso en aplicaciones de chat como por ejemplo el Messenger, entre otras.

Entre sus códecs y estándares vamos a destacarlos siguientes debido a que son los más usados en cámaras IP.

3.4.2.1 MJPEG - JPEG en Movimiento.

Protocolo que trata al vídeo como una secuencia de imágenes a las cuales les aplica JPEG (Joint Photographic Experts Group) el cual es un algoritmo de compresión con pérdida. Trabaja a cuatro modos de captura *progresiva* entrelazando ficheros, *secuencial* capturando secuencialmente, *sin pérdida* capturando con la menor perdida, *jerárquica* tal cual JPEG es decir con perdida.

Genera un CBR lo cual implica que sin movimiento en el área la calidad es aceptable con bajo consumo de AB, pero con movimiento la calidad en la imagen baja, sin embargo se mantiene el consumo de AB.

3.4.2.2 MPEG4.

MPEG (Grupo de Expertos en Imágenes en Movimiento) trabaja en base a una tasa de Kbps (Kilobits por segundo), FPS (cuadros por segundo) y tamaño de vídeo; trabaja mediante una compresión temporal y espacial mediante redundancia y muestreo, las muestras tomadas de imagen son divididas en pequeños fragmentos y solamente las diferencias comparadas con la imagen de muestreo son reconstruidas y algún extra necesario para llevar a cabo la predicción es almacenado utilizando códecs de compresión, generando de esta manera bajas pérdidas. La cuarta versión MPEG4 nos ofrece la mayor calidad posible en este tipo de aplicaciones, con la mitad de bits. Ofreciéndonos una gran compresión por lo que este formato es empleado, vídeo conferencias, para Internet y un sinnúmero de equipos móviles y reproductores de multimedia como Ipods, celulares, entre otros.

Genera un VBR lo cual implica que sin movimiento en el área la calidad es alta con bajo consumo de AB, ya que no envía FPS constantemente ya que la imagen no cambia; pero con movimiento sube el consumo de AB sin bajar la calidad en la imagen.

3.5 Características y Requerimientos del Concesionario

Se expondrán las características de las localidades y los requerimientos en base a:

Área de cobertura, resolución y secuencia. Para lo cual vamos a definir:

Área:	Cobertura:	Resolución:	Secuencia:
1	Extensa	Alta	Movimiento frecuente
2	Extensa	Alta	Movimiento moderado
3	Extensa a Pequeña	Alta	Poco movimiento
4	Pequeña	Media	Movimiento moderado

Tabla 12 - Tipos de Área

Para la siguiente tabla vamos a tomar en cuenta:

Tabla 6 - Requerimientos del Concesionario en la sección 3.3.2 en la página 21.

Tabla 7 - Resoluciones en la sección 3.3.2 en la página 22.

Tabla 9 - Tasa de Bits en base Fps. y CIF. En la sección 3.3.4 en la página 23.

- Para más detalle acerca de las áreas de cobertura, ver anexo 2.

Agencias: Cámaras: Área: Resol: Movimiento: Área Tipo:

	1 externa	Entrada	2-4 CIF	frecuente	1
	1 interna	Show room	2-4 CIF	moderado	2
	1 interna	Ventas	2-4 CIF	moderado	1
Matriz UIO	1 interna	Talleres	0-2 CIF	frecuente	1
	1 interna	Ventas	2-4 CIF	frecuente	3
	1 externa	Entrada	2-4 CIF	moderado	4
Sto.	1 interna	Entrada	2-4 CIF	moderado	3
Domingo	1 interna	Ventas	2-4 CIF	moderado	2
UIO Oeste	1 interna	Entrada	2-4 CIF	moderado	2
	1interna	Caja	0-2 CIF	moderado	2
UIO Norte	1 interna	Entrada	0-2 CIF	moderado	4
	1 interna	Ventas	0-2 CIF	moderado	2
UIO Este	1 interna	Ventas	2-4 CIF	moderado	2
	1 externa	Entrada	0-2 CIF	frecuente	1
UIO Sur	1 interna	Entrada	2-4 CIF	moderado	4
Matriz	1 interna	Ventas	2-4 CIF	moderado	2
GYE	1 externa	Entrada	2-4 CIF	moderado	4
GYE Norte	1 interna	Entrada	0-2 CIF	moderado	4
	1 interna	Caja	0-2 CIF	moderado	2
GYE Sur	1 interna	Entrada	0-2 CIF	moderado	4
	1 interna	Ventas	2-4 CIF	moderado	2

Tabla 13 - Resumen de Características y Requerimientos

3.6 Estudio de Factibilidad

Determinaremos la factibilidad para la implementación de las cámaras, en base a:

- Estructura y Características de la Intranet del Concesionario, en la página 19.
- Tasa de bits en base a CIF y Fps., en la página 23.
- Tabla - 13 Resumen de Características y Requerimientos.

Agencia:	Bps (aprox):	AB disp:	Conclusión:	Recomendación:
Matriz UIO	2,4 Mbps	100 Mbps	Si	Ninguna
Sto. Domingo	280 Kbps	256 Kbps	No	Ampliar el AB al doble. Utilizar configuración más baja.
UIO Oeste	140 Kbps	256 Kbps	Si	Ninguna
UIO Norte	240 Kbps	256 Kbps	No	Ampliar el AB al doble. Utilizar configuración más baja.
UIO Este	220 Kbps	512 Kbps	Si	Ninguna
UIO Sur	140 Kbps	256 Kbps	Si	
GYE Norte	240 Kbps	256 Kbps	No	Ampliar el AB al doble. Utilizar configuración más baja.
GYE Sur	260 Kbps	512 Kbps	Si	Ninguna
Matriz GYE	(280 Kbps)			
GYE: Matriz + Norte + Sur	780 Kbps	1,5 Mbps	Si	

Tabla 14 - Factibilidad para Implementación

- Más detalles ver Anexo 3

Capítulo IV

4.1 Diseño del Sistema de Vigilancia y Monitoreo IP

Tomando en cuenta las necesidades del concesionario expuestas en:

3.5. Características y requerimientos del Concesionario

Se representara gráficamente el Sistema de Vigilancia y Monitoreo IP.

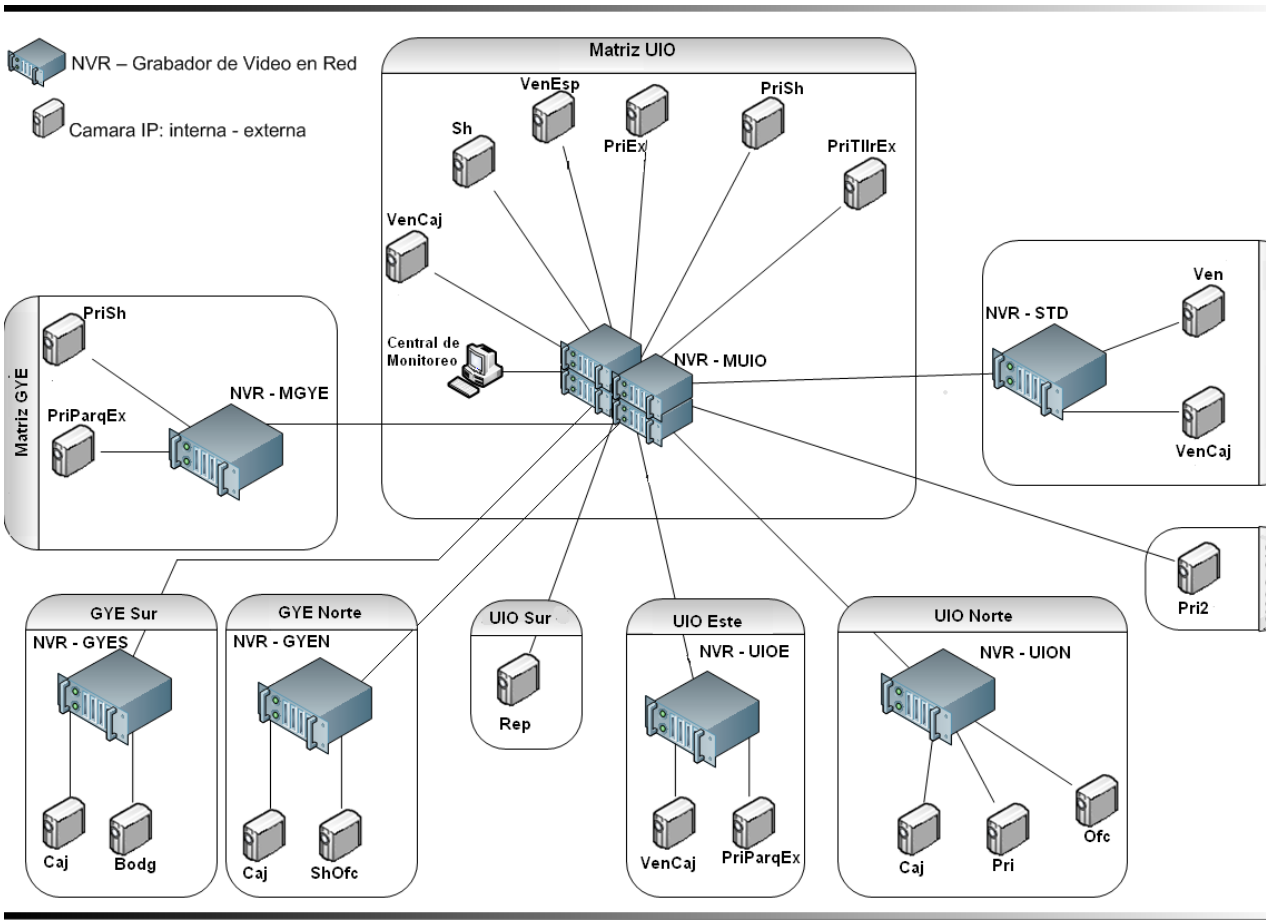


Figura 5 - Esquema del Sistema de Vigilancia y Monitoreo IP

A continuación se detallará el funcionamiento del Sistema de Vigilancia y Monitoreo IP:

Los GVR´s (NVR-Network video recorder) se colocarán de acuerdo al streaming generado por las cámaras IP en cada agencia, cabe especificar que no se enviará las grabaciones de las cámaras IP directamente a la central de monitoreo ya que agotaría

innecesariamente el espacio para almacenamiento de dicha central, la cual está orientada al respaldo de las grabaciones según los eventos o sucesos y al criterio del administrador.

4.2 Distribución y Funcionalidad del Sistema de Vigilancia y Monitoreo IP

4.2.1 Distribución

Matriz UIO.

En esta agencia se colocará un GVR de gran capacidad ya que en esta agencia se encuentra la central de monitoreo, la cual administrará todas las cámaras del sistema y se almacenarán los eventos de todas las sucursales según el criterio del administrador; cabe acotar que las cámaras de esta agencia generarán una gran cantidad de streaming de vídeo debido a la configuración de las mismas por lo cual es muy ventajoso que se encuentren en la misma agencia que la central de monitoreo.

El GVR-A se conectará a los GVR´s de las agencias restantes, para una fácil administración del sistema como de las grabaciones.

Matriz GYE, Sto. Domingo, UIO Norte, Este, GYE Norte, GYE Sur.

En estas agencias se colocarán GVR´s de pequeña capacidad en los cuales se grabarán los eventos ocurridos en la agencia, para luego ser gestionado por el administrador desde la central de monitoreo.

Agencias UIO Oeste y Sur.

En estas agencias debido a que solo poseen una cámara IP respectivamente y sus parámetros de configuración-consumo son bajos no se colocarán GVR´s y se enviará directamente el streaming

de vídeo para grabación directamente a el GVR-A en la central de monitoreo.

4.2.2 Función del Sistema de Vigilancia y Monitoreo IP

Debido a los requerimientos del concesionario y función de los equipos, se resumirá como trabajara el sistema en la siguiente tabla:

Elementos	**Función**
Central de Monitoreo	Monitoreará los sucesos en el transcurso de horarios laborables y administrara el vídeo almacenado en los GVR.
GVRs	Grabarán las 24 horas continuas.
Cámaras IP	Internas: Transmitirán continuamente en horarios laborables (8:00 -18:00) y fuera de estos solamente al detectar movimiento. Externas: Transmitirán continuamente las 24 horas.

Tabla 15 - Función del Sistema de Vigilancia y Monitoreo IP

4.3 Diagrama de Acoplamiento del SVMIP a la red del Concesionario.

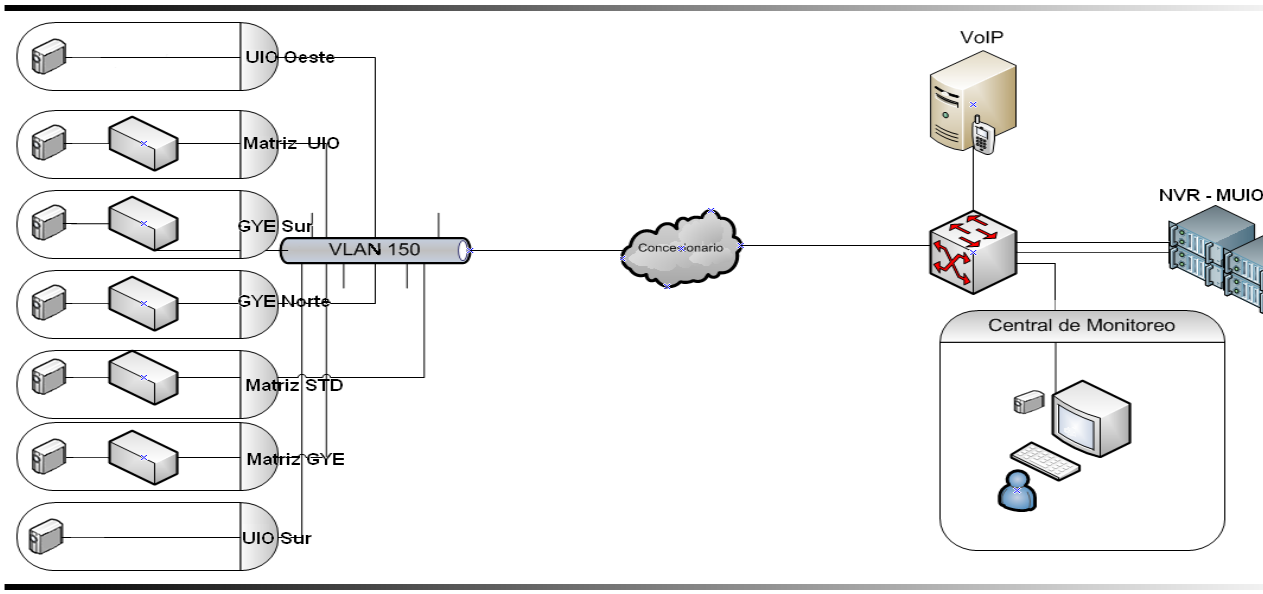


Figura 6 - Diagrama de acoplamiento del SVMIP al concesionario.

4.3.1 Descripción del Diagrama de Acoplamiento.

En la Figura - 6 se puede apreciar que las cámaras IP, GVR's de las agencias del concesionario trabajarán sobre la VLAN 150, creada para el SVMIP y mediante la cual se acoplará a la red de datos del concesionario hasta la central de monitoreo. Los streamings (flujo de voz o vídeo continuo) de las diferentes agencias convergirán en un switch capa 3, el cual trabaja solamente con VoIP y los streamings que generará el SVMIP, se conectará al GVR de gran capacidad que estará en la Matriz UIO, mediante dos enlaces Ethernet, ya que así permitirá realizar balanceo de carga ya que el GVR así lo permite, acoplándose de esta manera a la red del concesionario.

4.3.2 Tabla de Direccionamiento IP

Agencia	**Equipo**	**Modelo**	**IP**	**GW**
	Grabador de vídeo	QN-VS-5020	192.168.150.12	
	Cámara IP domo	FD7131	192.168.150.4	
	Cámara IP domo	FD7131	192.168.150.5	
Agencia A	Cámara IP domo	FD7131	192.168.150.6	192.168.150.1

	Cámara IP domo	FD7131	192.168.150.7	
	Cámara IP externa	IP7330	192.168.150.8	
	Cámara IP externa	IP7330	192.168.150.9	
Agencia B	Cámara IP domo	FD7131	192.168.3.197	192.168.3.60
	Cámara IP externa	IP7330	192.168.3.198	
	Grabador de vídeo	NVR-104V	192.168.3.199	
Agencia C	Cámara IP domo	FD7131	192.168.15.100	192.168.15.1
	Cámara IP domo	FD7131	192.168.15.101	
	Grabador de vídeo	NVR-104V	192.168.15.102	
Agencia D	Cámara IP externa	FD7131	192.168.10.100	192.168.10.254
Agencia E	Cámara IP domo	FD7131	192.168.8.101	192.168.8.254
	Cámara IP domo	FD7131	192.168.8.102	
	Cámara IP domo	FD7131	192.168.8.103	
	Grabador de vídeo	NVR-104V	192.168.8.100	
Agencia F	Cámara IP domo	FD7131	192.168.2.101	192.168.2.254
	Cámara IP externa	IP7330	192.168.2.102	
	Grabador de vídeo	NVR-104V	192.168.2.100	

Agencia G	Cámara IP domo	FD7131	192.168.7.100	192.168.7.254
Agencia H	Cámara IP domo	FD7131	192.168.6.100	192.168.6.254
	Cámara IP domo	FD7131	192.168.6.101	
	Grabador de vídeo	NVR-104V	192.168.6.102	
Agencia I	Cámara IP domo	FD7131	192.168.6.100	192.168.6.254
	Cámara IP domo	FD7131	192.168.6.101	
	Grabador de vídeo	NVR-104V	192.168.6.102	

Tabla 16 - Direccionamiento IP de los elementos del SVM IP.

4.4 Parámetros de Configuración

Para la configuración de los equipos es necesario conectarnos a los mismos, con un cable de red directo entre el computador y el equipo a configurar. Se puede utilizar un switch si se va a configurar más de un equipo o si se requiere configurar las cámaras IP con ayuda del GVR, ya que las detecta y muestra las direcciones IP de las mismas, permitiendo además accesar a ellas con una simple selección.

4.5.1 GVR

Para configurar este equipo se puede hacerlo con el CD de instalación, el cual viene con el mismo o manualmente ingresando la dirección IP del equipo.

Y empezamos a configurarlo:

4.5.1.1 Configuración Básica

1.- Al aparecer la configuración rápida del equipo, que será la que guiará para la configuración básica del mismo se selecciona continuar.

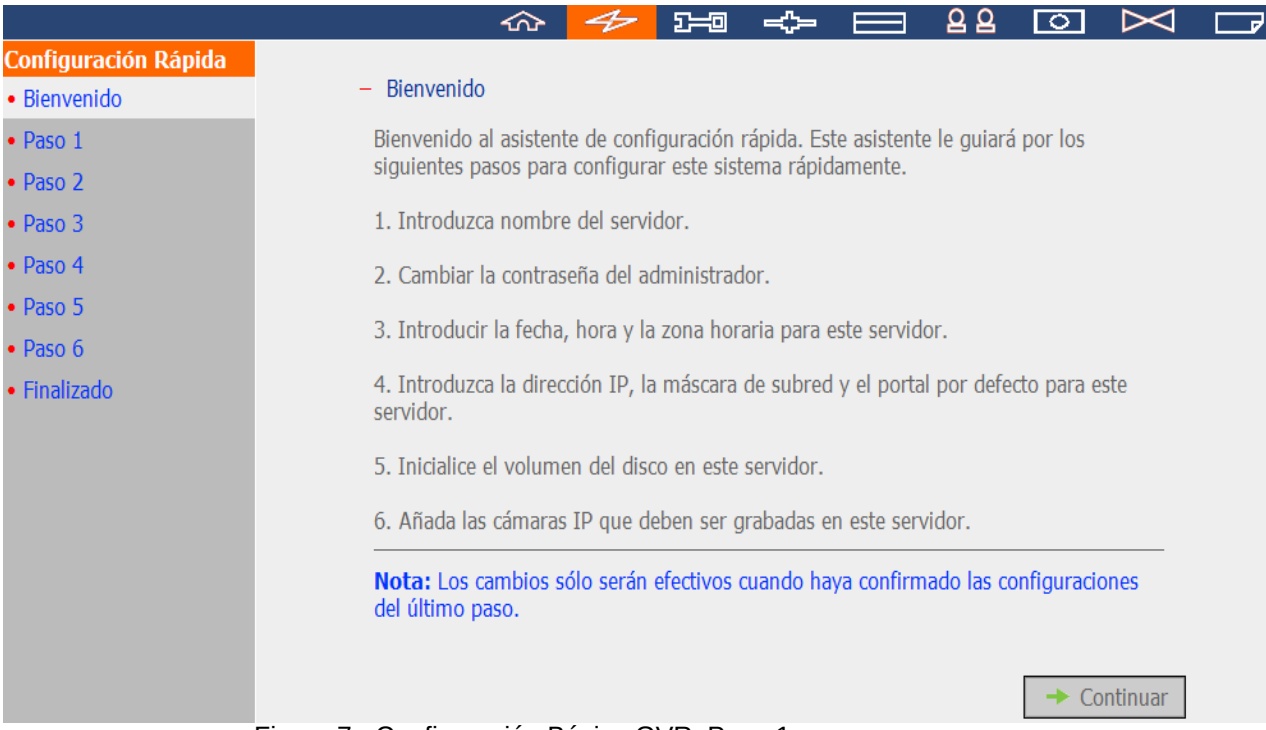


Figura 7 - Configuración Básica GVR. Paso 1

2.- En la siguiente pantalla se asigna un nombre al GVR.

Es recomendable asignar nombres únicos por cada GVR.

Y se selecciona siguiente.

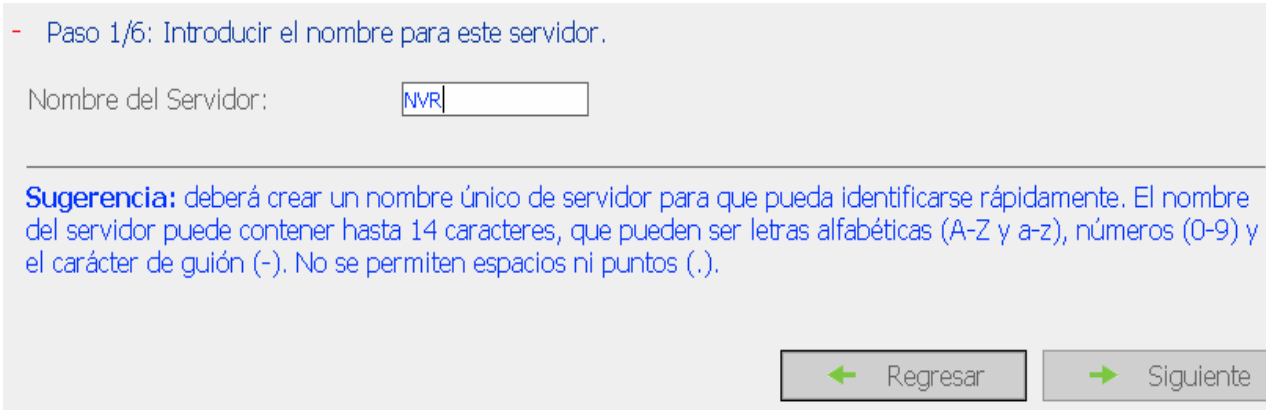


Figura 8 - CB.GVR. Paso 2

3.- En la siguiente pantalla se asigna una contraseña al GVR.

Y se selecciona siguiente.

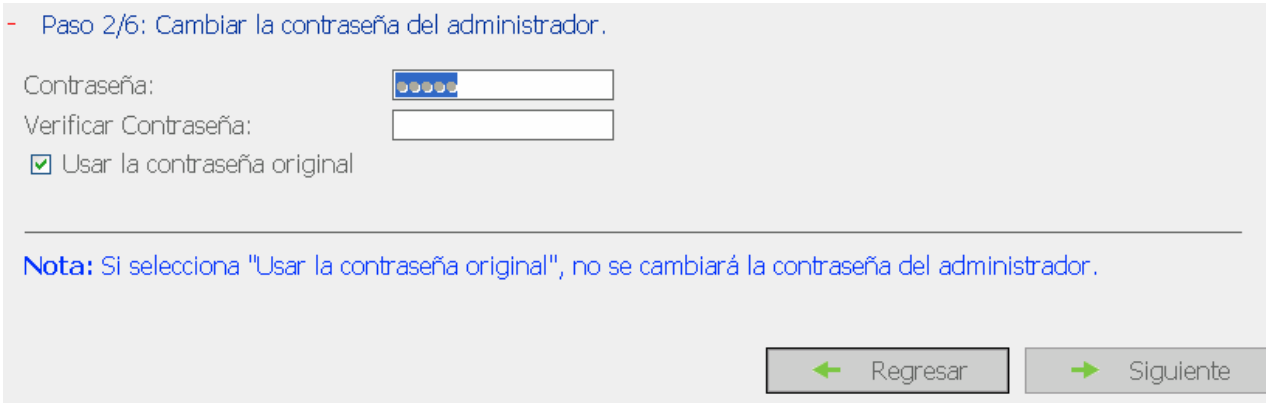


Figura 9 - CB.GVR. Paso 3

4.- Se configura fecha, hora y zona horaria.

Y se selecciona siguiente.

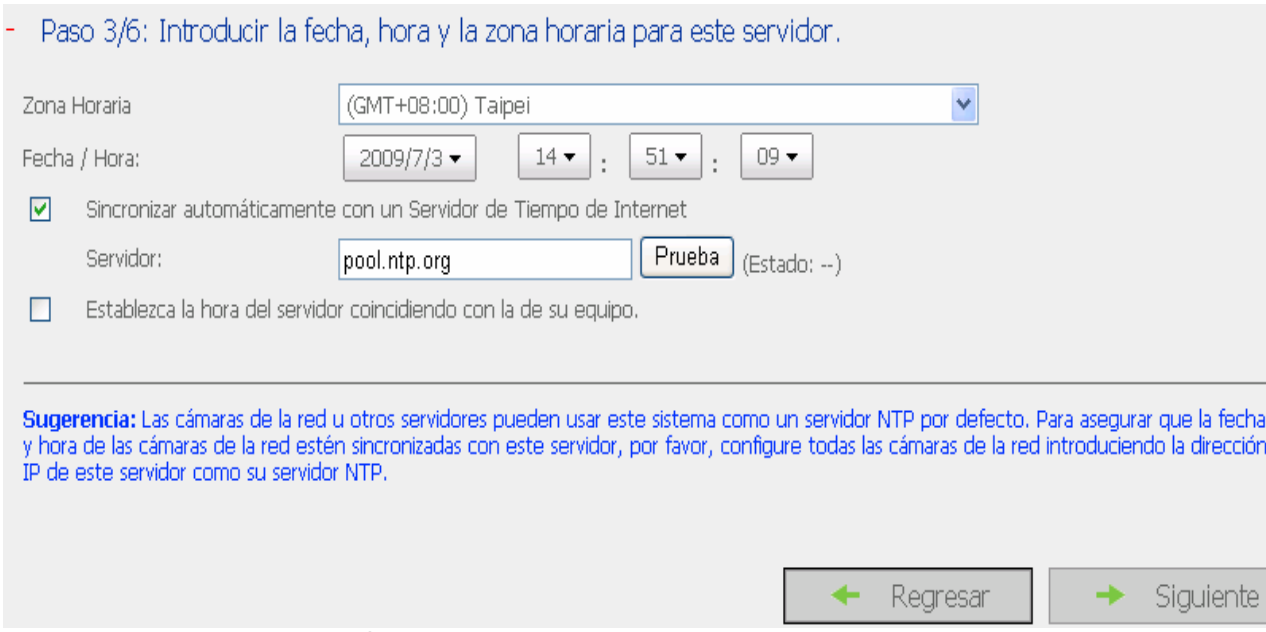


Figura 10 - CB.GVR. Paso 4

5.- 5.- Se asigna una dirección IP, de la red o sub red con la que se esté trabajando, se asigna de igual manera la puerta de enlace de la red y si así lo requerimos los DNSs.

Y se selecciona siguiente.

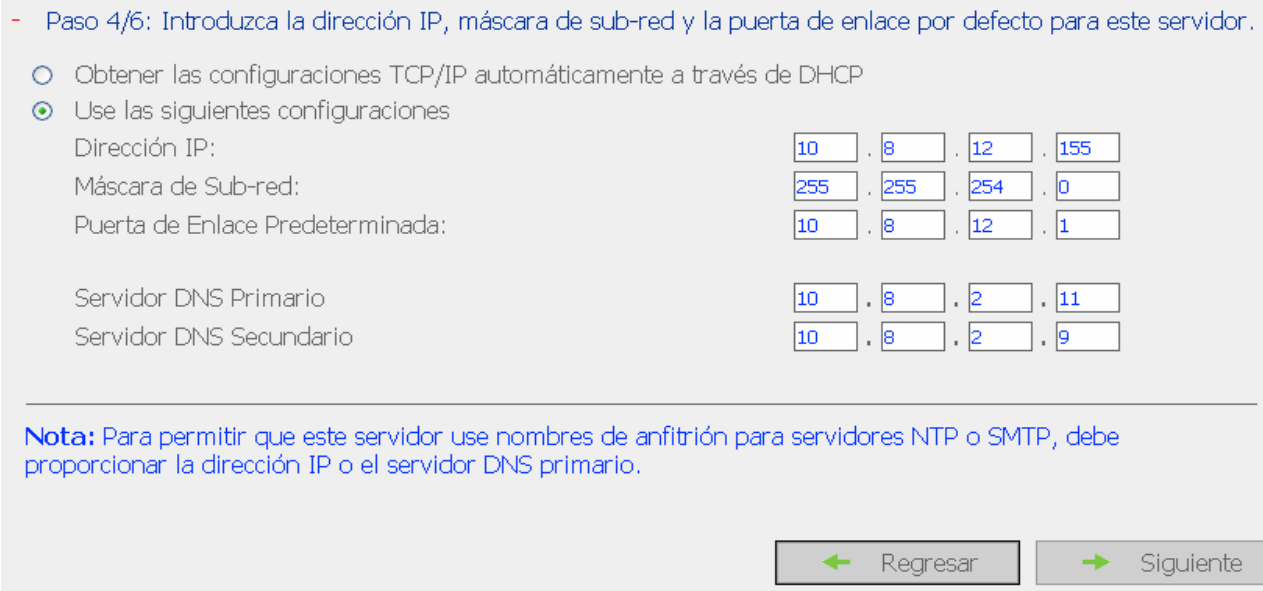


Figura 11 - CB.GVR. Paso 5

6.- En la siguiente pantalla el GVR detectará el HDD y mostrará dos opciones:

Definir configuración del disco. -Formateará el HDD al concluir la configuración.

No definir la configuración del disco. -No formateará el HDD.

Y se selecciona siguiente.

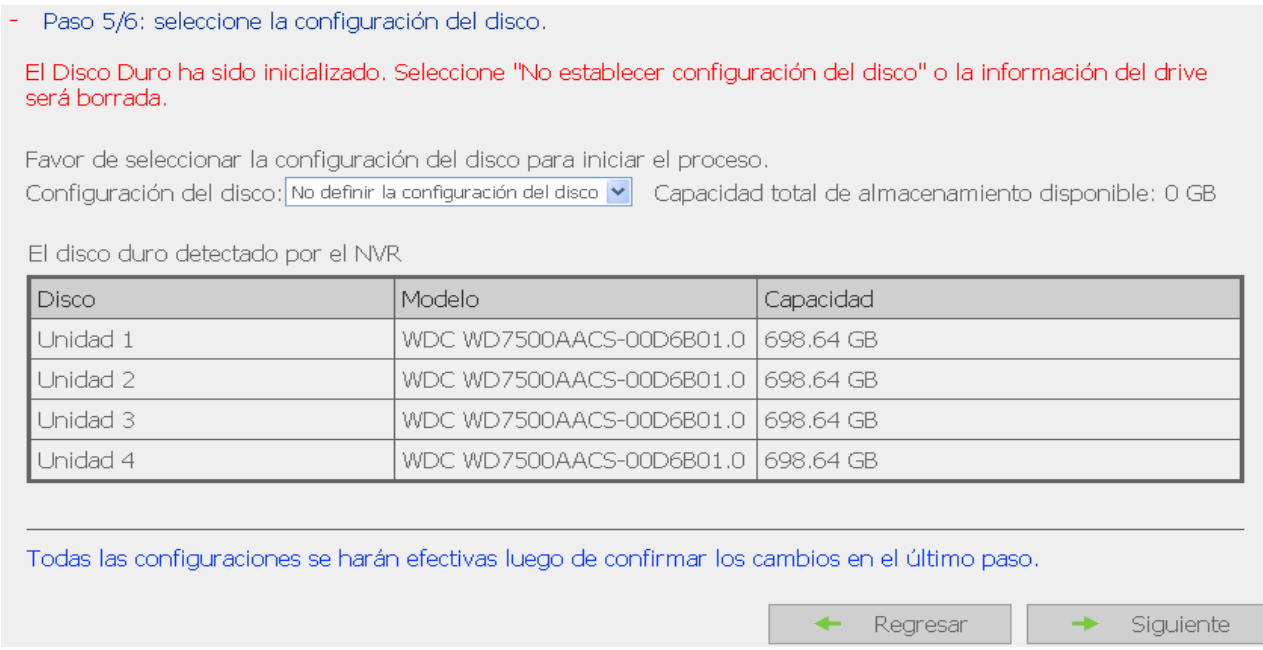


Figura 12 - CB.GVR. Paso 6

7.- En la pantalla siguiente se selecciona las cámaras IP en la red.

Con "Buscar" nos aparecen las cámaras que estén conectadas a la red de datos.

El GVR detectará las cámaras, pero es necesario colocar nombres de usuario y contraseñas para unificar la administración.

Se puede cambiar el direccionamiento IP y el puerto de acceso si así se lo requiere.

Se ingresa nombres de usuario y password, previamente configurados.

Con "Prueba" se verifica que los datos estén correctos y se tenga acceso a la cámara IP.

Con "Guardar" una vez verificado que los datos sean correctos los guardamos.

Se selecciona "Habilitar la grabación".

Y se selecciona siguiente.

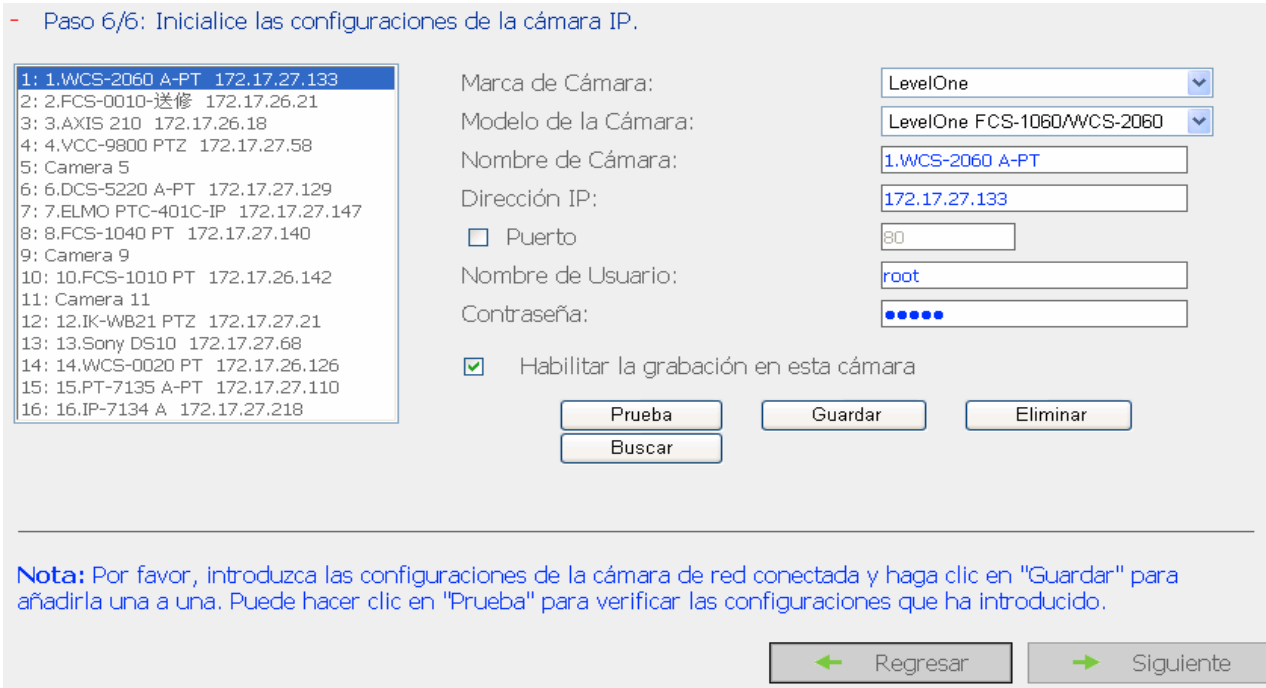


Figura 13 - CB.GVR. Paso 7

8.- En la siguiente pantalla se selecciona “Instalar”.

Con lo cual se aplicará la configuración, se formateará el HDD y se reiniciará el GVR.

Se selecciona Iniciar Instalación.

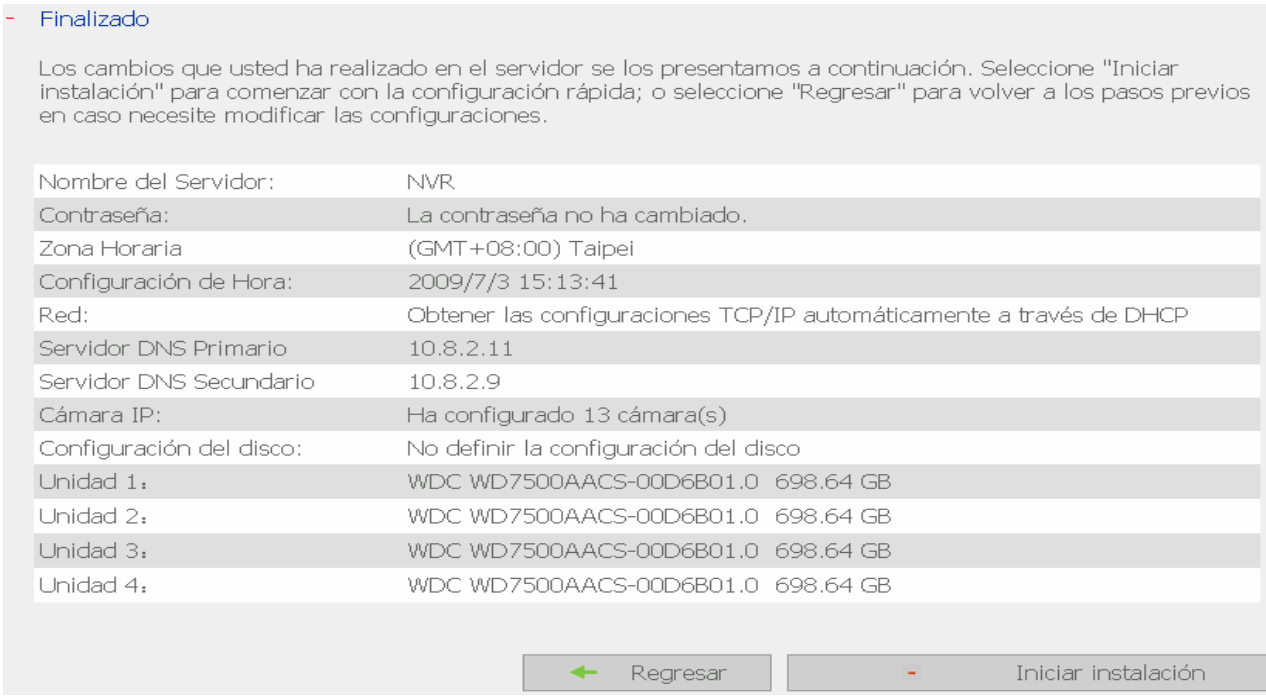


Figura 14 - CB.GVR. Paso 8

Este proceso durara de 10 a 30 min dependiendo el tamaño del HDD.

9.- La siguiente pantalla indica que ya finalizo los procesos el GVR y está listo para empezar la monitorización - grabación.

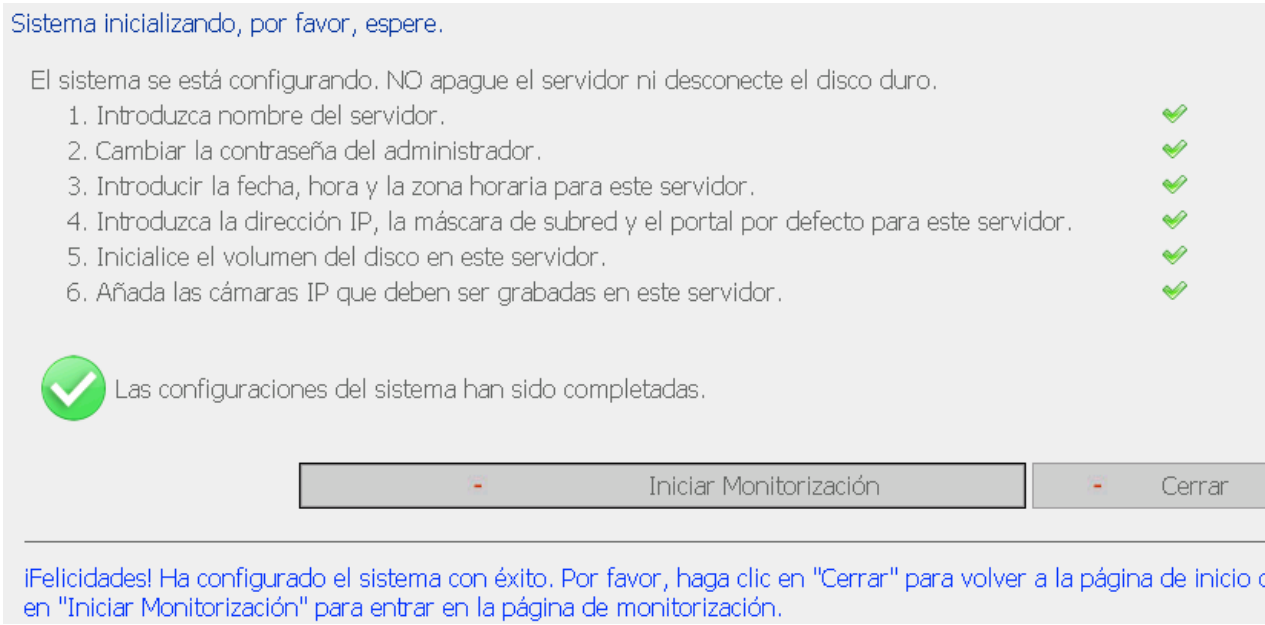


Figura 15 - CB.GVR. Paso 9

10.- Por último se selecciona "Iniciar Monitorización" y aparecerá la siguiente pantalla:

Figura 16 - Pantalla de Monitoreo del GVR

4.5.2 **Cámaras IP**

Para configurar este equipo podemos hacerlo con el CD el cual viene con el mismo o manualmente ingresando la dirección IP del equipo. Y empezamos a configurarlo:

4.5.2.1 Configuración Básica:

1.- Aparece la interfaz web de configuración y visualización del equipo, desde la cual se configurará al equipo.

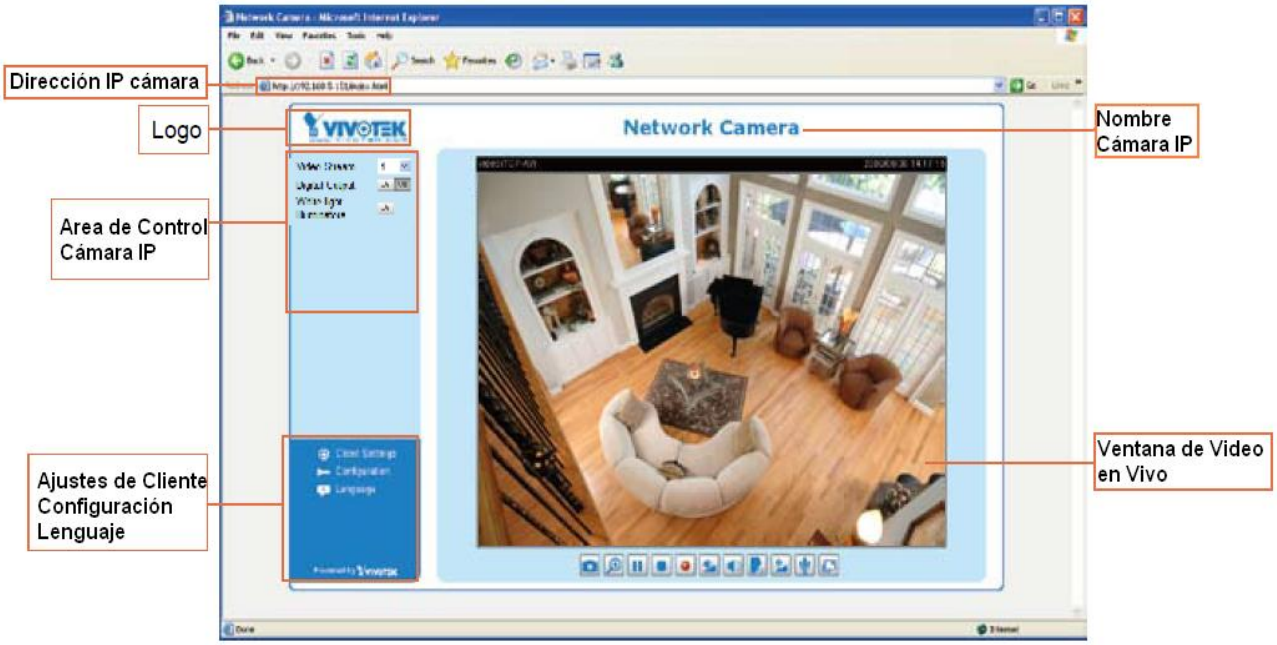


Figura 17 - Interfaz web de Configuración

En esta pantalla también se podrá:

Activar manualmente iluminación de luces blancas o de luces nocturnas.

Activar o desactivar la salida digital del equipo.

2.- Se ingresa a “Configuración” y aparecerá la siguiente pantalla:

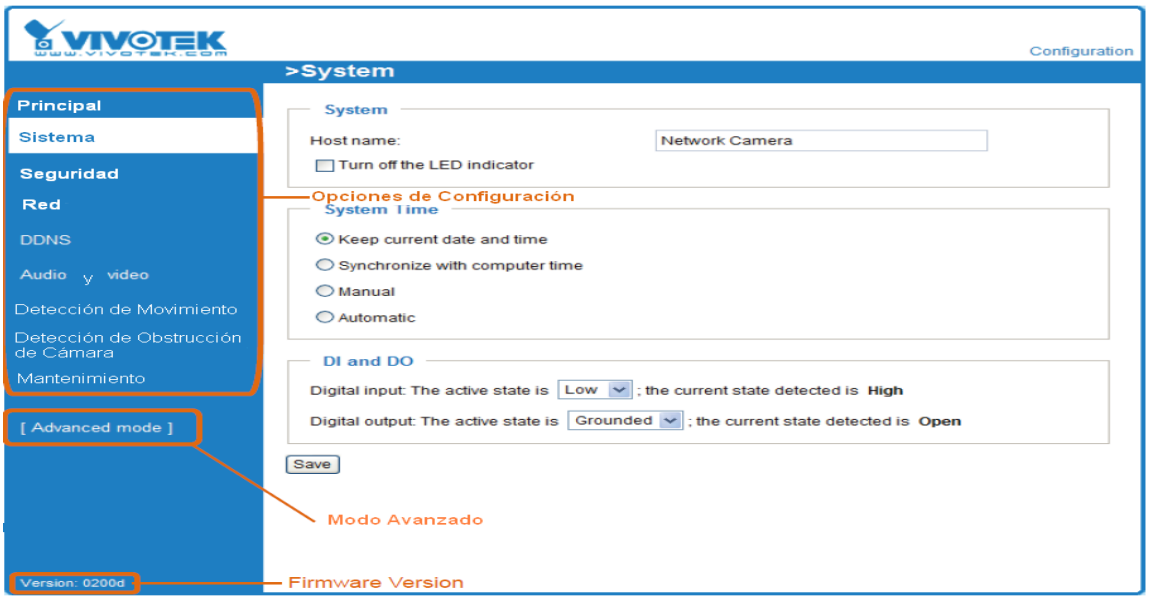


Figura 18 - Interfaz de Configuración

Desde esta pantalla se podrá accesar a configurar los parámetros de:

Sistema: para cambiar el nombre que aparecerá del equipo, sincronizar u optimizar parámetros de hora y fecha, también para modificar parámetros de entrada y salida digital e incluso apagar el indicador de encendido de la cámara IP.

3.- Ingresando a seguridad:

Para crear o modificar la clave de administración, entre otras como: crear usuarios, dar o quitar privilegios según el tipo de usuario, activar encriptación https.

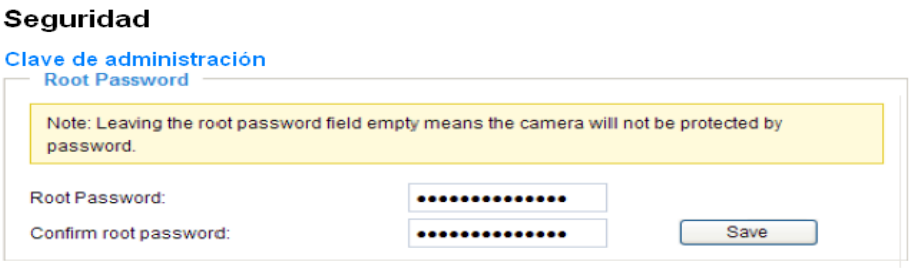


Figura 19 - Configuración de Clave de Administración

4.- Ingresando a Red:

Para configurar parámetros de red, según el tipo de conexión.

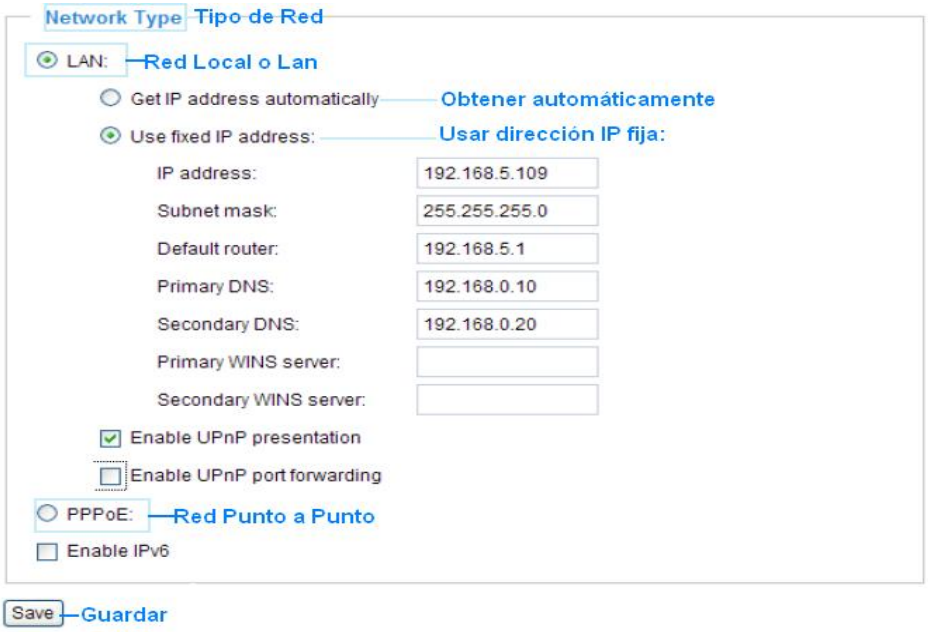


Figura 20 - Configuración de Red

5.- DDNS: para activar o desactivar y configurar parámetros de DNS. Se puede seleccionar dinámica o configurar manualmente los servidores.

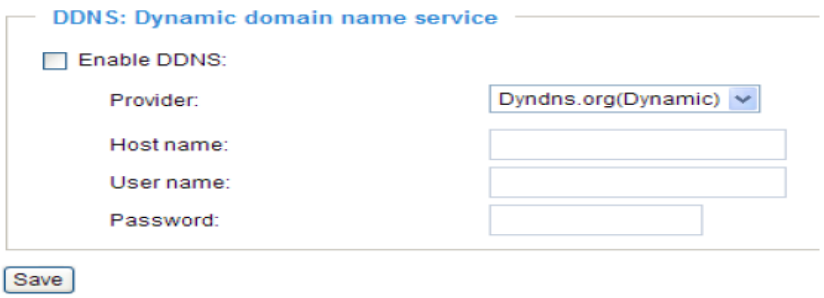


Figura 21 - Configuración DNS

6.- Ingresamos a Vídeo

Donde se configurara los parámetros de calidad y secuencia de captura.

(Muestra la opción de 2 streamings de vídeo aunque solo se usará uno de los 2).

Figura 22 - Configuraciones de Vídeo

7.- Detección de Movimiento

Para crear y configurar el o las áreas para detección de movimiento. Ubicamos el área de detección y colocamos el porcentaje de sensibilidad en esta.

Figura 23 - Configuración Detección de Movimiento

8.- Detección de Obstrucción:

Para configurar la sensibilidad de la detección.

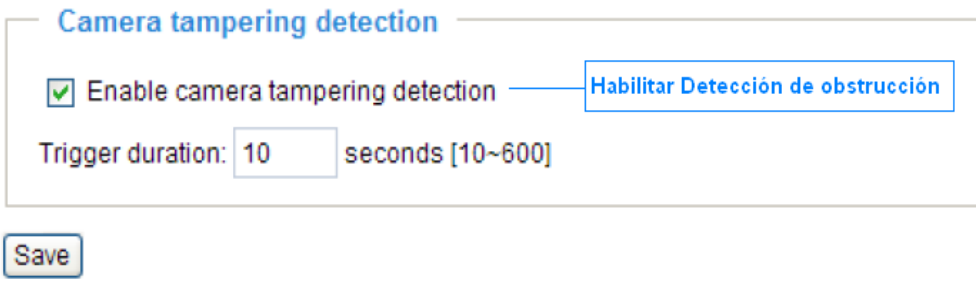


Figura 24 - Configuración Detección de Obstrucción

9.- Por último se verá una de las aplicaciones más importantes y la cual se va a utilizar.

Activación por evento.

(Permite a la cámara grabar fuera de horario programado, por detección de un evento en particular).

En esta pantalla se asignará un nombre de evento, se elige su prioridad, el tiempo que transcurrirá hasta el siguiente evento, la causa que lo activará, los horarios en los que se activará la detección de eventos y las acciones a tomar por el SVMIP.

Tal como podemos apreciar en la siguiente captura:

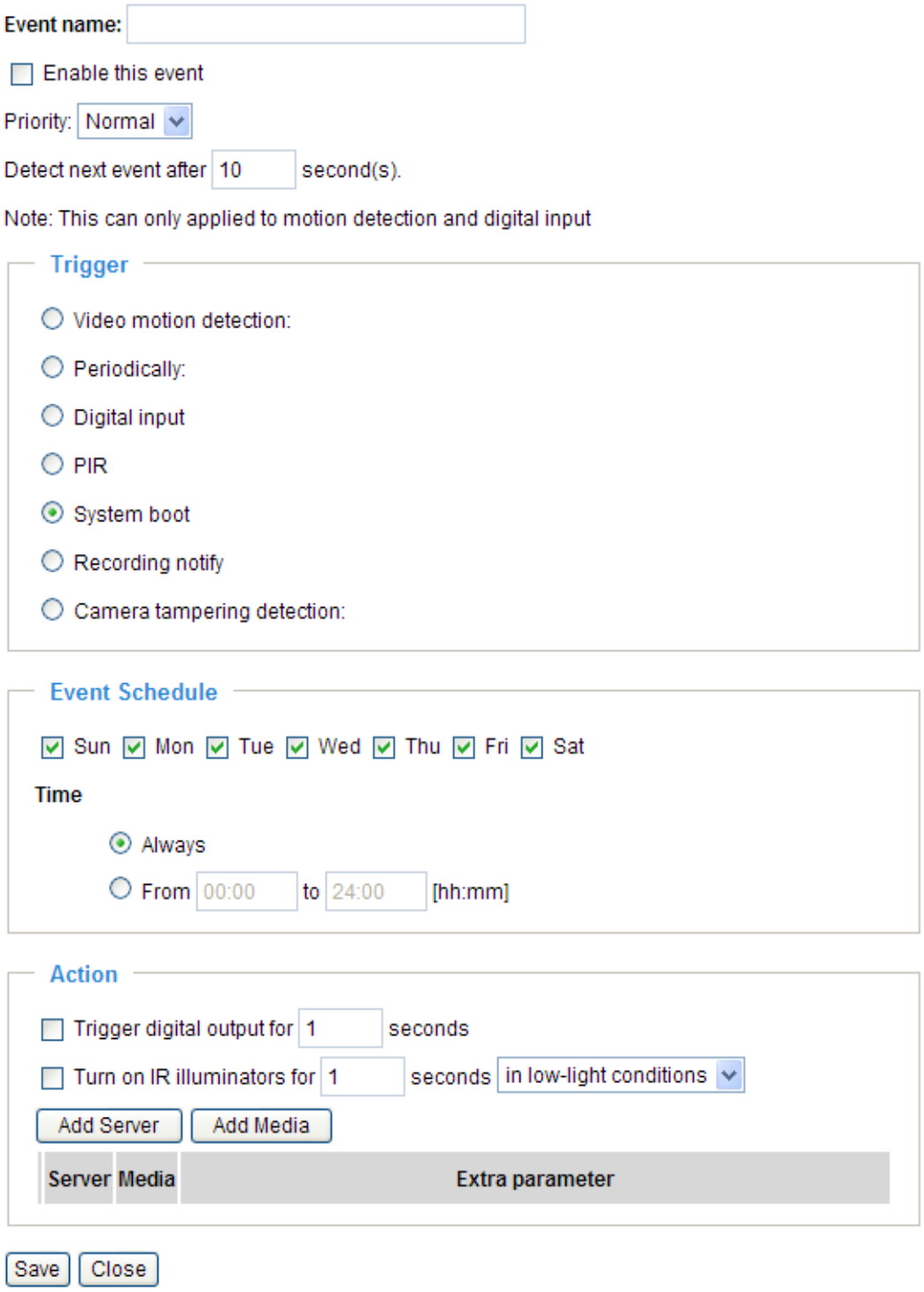


Figura 25 - Configuración de Eventos

Capítulo V

5.1 Cableado del SVMIP

Para la instalación del SVMIP y de acuerdo a lo expuesto en la sección “3.6. Estudio de Factibilidad” en la página 30, es necesaria la implementación de cableado de red y energía hasta el punto estratégico (PE) según la localidad y donde serán colocadas las cámaras IP.

En todos los casos y localidades que se requiera una gran extensión del cableado, se lo realizará siguiendo las normas de cableado estructurado más básicas:

a. Cableado de energía:

- Estará separado del cableado de red.
- El circuito eléctrico de las Cámaras IP separado del circuito eléctrico del lugar.
- Ira desde el panel de breakers o energía principal a uno o más tomacorrientes ubicados cerca a los “Puntos estratégicos” de las cámaras para energizar las mismas.
- Será realizado con tres hilos, cada uno correspondiente a la misma polaridad: Negro negativo, rojo positivo, verde tierra.

b. Cableado de red:

- Será no mayor a 90 metros del rack a la cámara IP.
- Ira desde el patch panel en un Rack o cuarto de equipos a cajetines rectangulares con conectores jacks cercanos a los “Pes”.
- Conectores rj45 y jacks se realizaran según la norma 568-B (Define la asignación de pares/pines en los cables de red de 8 hilos).

c. Materiales utilizados en exteriores e interiores:

- Para interiores se utilizará canaleta divida, según sea el caso.
- Para exteriores se utilizará tubería galvanizada o tubería anillada plástica o de cobre según sea el caso.

5.2 Configuración del SVMIP

5.2.1 Configuración del Switch

En este switch se creará la VLAN 150 por la cual trabajará el SVMIP.

Podemos configurarlo vía interfaz web y vía consola.

a. Configuración Web:

1. Se accesa al switch mediante la dirección IP pre-configurada.
2. Se digita el nombre de usuario y la contraseña asignada al mismo.
3. se seleccionará “Dispositivo” y la opción “VLAN”.
4. Se digita el ID de la VLAN a crear, la cual será 150.
5. Se selecciona “Crear”.
6. Por último asignaremos los puertos a dicha VLAN.
7. Y salimos de la Interfaz Web.

b. Configuración por consola.

Para esta es necesario utilizar un cable de consola, y utilizando el programa Hyper Terminal o ingresando al equipo mediante una conexión SSH (Secure SHell, - intérprete de órdenes segura).

1. Se digita el nombre de usuario y la contraseña asignada al mismo.
1. Se digita la opción ‘Bridge’ para administrar las opciones de ancho de “puente’’.

2. Se digita la opción ‘’VLAN’’ para administrar las opciones de VLAN.
3. Se digita la opción "Crear" para crear la VLAN deseada.
4. Se digita el ID de la VLAN y el nombre para la misma.
5. Se digita la opción ‘’Modificar’’.
6. Se digita la opción ‘’agregar puerto’’.
7. Se selecciona el ID de la VLAN a la cual deseamos agregar los puertos.
8. Se digita el Slot, seguido del puerto inicio, guion el slot y puerto final.
9. Se digita la opción untagged ya que no es VoIP.
10. Se digita ‘’quitar’’ para salir de la opción ‘’modificar’’,
11. Se digita la opción ‘’detallar’’ y seleccionamos la ‘’VLAN’’ deseada para verificar la misma.
12. Y por último, se da por terminada la sesión con el comando ‘’Logout’’.

5.2.2 Configuraciones Generales

Se detallará los parámetros de configuración de hora y de resolución de DNS.

a) Configuraciones de Hora:

Para la hora en todos los dispositivos del sistema se utilizará la característica de configuración de hora por “Protocolo de Tiempo para Redes - Network Time Protocol” con la dirección IP: 192.168.4.196, el cual es un equipo local con esta característica activa.

b) Configuraciones de Resolución DNS:

Para la resolución de DNS se utilizará los servidores del “ISP” (Proveedor de Servicio de Internet).

5.2.3 Configuración IP

a. Cámaras IP y GVR´s

- La configuración IP será según la Tabla 16 - Direccionamiento IP de los elementos del SVM IP., en la página 37, de la sección 4.3.2
- Se pre-configura las cámaras y GVRs según la Tabla 13 - Resumen de Características y Requerimientos en la página 30y se procede a probar el SVMIP de manera local. Sin presentarse ningún inconveniente.
- Se realizan pruebas de conexión y transmisión comprobando el correcto funcionamiento del SVMIP.

5.2.4 Configuración Resolución de Vídeo

EQUIPO	IMAGEN
Cámaras de vídeo IP: IP7330 FD7131	Compresión de vídeo: MPEG4 Calidad: 2CIF Resolución: 640 x 480 Imágenes por segundo: 5

Tabla 17 - Configuración de Resolución de Vídeo

5.2.5 Configuración de seguridades en equipos

EQUIPO	USUARIO	CONTRASEÑA
GVR-104 GVR-5020	Admin	GVR.BACK.210
	Control	co.VASA.210
Cámaras: IP7330	Admin	ip.BACK.210

FD7131		

Tabla 18 - Configuraciones Seguridades

5.2.6 Cámaras configuradas por GVR

			CAPACIDAD INSTALADA		
AGENCIA	**GVR**	**CAPACIDAD TOTAL**	**DOMO**	**EXTERNAS**	**TOTAL**
Matriz UIO	GVR-MUIO	20 Cámaras IP	4	2	11 CAMARAS
Sto. Domingo	GVR-STD	4 Cámaras IP	2		2 CAMARAS
UIO Norte	GVR-UION	4 Cámaras IP	3		3 CAMARAS
UIO Este	GVR-UIOE	4 Cámaras IP	1	1	2 CAMARAS
Matriz GYE	GVR-MGYE	4 Cámaras IP	1	1	3 CAMARAS
GYE Norte	GVR-GYEN	4 Cámaras IP	2		2 CAMARAS
GYE Sur	GVR-GYES	4 Cámaras IP	2		2 CAMARAS

Tabla 19 - Cámaras configuradas por GVR

5.2.7 Detalle de cámaras y canales por GVR instalado

GVR Agencia	**Nº Canal**	**Nombre Cámara IP**	**Ubicación**

GVR-MUIO	1	UIO-VenCaj	Área de ventas y caja.	
	2	UIO-Sh	Área lavadora de autos.	
	3	UIO-VenEsp	Área de ventas, caja, sala de espera.	
	4	UIO-PriEx	Área de la puerta principal de acceso, parqueaderos.	
	5	UIO-PriSh	Área de la entrada principal de acceso a showroom.	
	6	UIO-PriTllrEx	Área de entrada principal de talleres.	
	7	UIO-Oe-Pri2	Área de la entrada.	
	8	UIO-Su-Rep	Área de entrada principal de acceso.	
			GVR-MUOI Canal	**Ubicación**
GVR-STD	1	STD-Ven	9	Enfoca el sector de ventas y caja.
	2	STD-VenCaj	10	Enfoca el sector de ventas y caja.
GVR-UION	1	UIO-N-Caj	11	Enfoca sector de caja.
	2	UIO-N-Pri	12	Enfoca entrada principal.
	3	UIO-N-Ofc	13	Enfoca entrada de oficinas.
GVR-UIOE	1	UIO-E-VenCaj	14	Enfoca sector de ventas y caja.
	2	UIO-E-PriParqEx	15	Área de entrada principal y parqueaderos.
GVR-MGYE	1	GYE-PriSh	16	Enfoca entrada principal a showroom
	2	GYE-PriParqEx	17	Enfoca entrada principal de vehículos
GVR-GYEN	1	GYE-N-Caj	18	Enfoca sector de caja.
	2	GYE-N-ShOfc	19	Área showroom, oficinas y sala de espera.
GVR-GYES	1	GYE-S-Caj	20	Enfoca sector de caja.
	2	GYE-S-Bodg	21	Enfoca sector de bodeguero.

Tabla 20 - Cámaras y Canales por GVR instalado

5.2.8 Configuración horarios de Grabación

Agencia	Nombre Cámara IP	Grabación Continua	Grabación por Evento
Matriz UIO	UIO-VenCaj	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-Sh	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-VenEsp	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-Pri	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-PriSh	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-PriTllr	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-Oe-Pri2	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-Su-Rep	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
Sto. Domingo	STD-Ven	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	STD-VenCaj	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
UIO Norte	UIO-N-Caj	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-N-Pri	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-N-Ofc	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
UIO Este	UIO-E-VenCaj	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	UIO-E-PriParq	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
Matriz GYE	GYE-PriSh	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	GYE-PriParq	Lun - Dom de 07:00 a	Lun - Dom de 20:00 a 7:00

		20:00	
GYE Norte	GYE-N-Caj	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
	GYE-N-ShOfc	Lun - Dom de 07:00 a 20:00	Lun - Dom de 20:00 a 7:00
GYE Sur	GYE-S-Caj	Lun- Vier 7:00 a 19:00	Lun- Vier 19:00 a 7:00
	GYE-S-Bodg	Sábado de 08:00 a 13:00	Sábado de 13:00 a 00:00 Domingo las 24 horas

Tabla 21 - Configuración Horarios de Grabación

5.3 Procesos y Pruebas del Sistema.

La siguiente tabla se expresa las pruebas realizadas, para verificar la correcta implementación del Sistema de Vigilancia y Monitoreo IP.

	Agencias								
Pruebas	A	B	C	D	E	F	G	H	I
Conectividad GVR principal	X	X	X	X	X	X	X	X	X
Conectividad GVR agencia (local)		X	X		X	X		X	X
Pruebas Puntos eléctricos	X	X	X	X	X	X	X	X	X
Pruebas conectividad puntos de red	X	X	X	X	X	X	X	X	X
Visualización de cámara IP en Monitor	X	X	X	X	X	X	X	X	X
Enfoque y Zoom	X	X	X	X	X	X	X	X	X
Visualización en GVR Principal	X	X	X	X	X	X	X	X	X

Tabla 22 - Procesos y Pruebas del Sistema

5.4 Almacenamiento Instalado.

La siguiente tabla detalla la capacidad de almacenamiento instalada en cada GVR.

GVR/Agencia	Almacenamiento
GVR-MUIO	2 TB
GVR-STD	1 TB
GVR-UION	1 TB
GVR-UIOE	1 TB
GVR-MGYE	1 TB
GVR-GYEN	1 TB
GVR-GYES	1 TB

Tabla 23 - Almacenamiento Instalado

5.5 Capacidad de Almacenamiento GVR.

La siguiente tabla expresa y detalla un estimado del consumo en disco y capacidad de almacenamiento según cada sucursal. Cabe mencionar que el almacenamiento total en el NVR de gran capacidad será la suma de todos los GVR.

	Cámaras IP	Horario de Almacenaje	
GVR-A	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
A	VASAUIO P2-REPUESTOS	2,5 GB	500 MB
	VASAUIO-P1-PARQ-CLIE	2,5 GB	500 MB
	VASAUIO P1-SHOWROOM	3 GB	500 MB
	VASAUIO P1-PRT-SROOM	2,5 GB	500 MB
	VASAUIO-P1-IN-PRINCI	3,5 GB	3,5 GB

	VASAUIO-P2-IN-TALLER	3 GB	3 GB
D	SIVASAUIO-CHEDIAK-TA	5 GB	500 MB
G	DOBLEUIO-AMERICA-EXT	2,5 GB	500 MB

Consumo diario		24.5 GB	9.5 GB
TOTAL	34 GB		
DIAS DE ALMACENAMIENTO SOPORTADOS	59		

		Horario de Almacenaje	
GVR-F	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
F	FULLUIO-6DIC-MOSTRAD	2 GB	200 MB
	FULLUIO-6DIC-EXTERNA	3 GB	3 GB

Consumo diario		5 GB	3.2 GB
TOTAL	8.2 GB		
DIAS DE ALMACENAMIENTO SOPORTADOS	125		

		Horario de Almacenaje	
GVR-E	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
E	SIVASAUIO-CAJA	1,4 GB	200 MB
	SIVASAUIO-ENTRADA-	1,6 GB	200 MB

	PR		
	SIVASAUIO-ENTRADA-OF	1,8 GB	100 MB

Consumo diario		4.8 GB	0.5 GB
TOTAL	5.3 GB		
DIAS DE ALMACENAMIENTO SOPORTADOS	193		

		Horario de Almacenaje	
GVR-B	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
B	VASAGYE-SHOWROOM	3 GB	1.5 GB
	VASAGYE-ENTRADA PR	2.4 GB	200 MB
	ALBANGYE-SHOWROOM	2 GB	200 MB

Consumo diario		7,4 GB	1.9 GB
TOTAL	9.3 GB		
DIAS DE ALMACENAMIENTO SOPORTADOS	110		

		Horario de Almacenaje	
GVR-H	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
H	SIVASAGYE-CAJA	1.3 GB	200 MB
	SIVASAGYE-SHOWROOM	1.8 GB	200 MB

Consumo diario		3.1 GB	0.4 GB
TOTAL	3.5 GB		
DIAS DE ALMACENAMIENTO SOPORTADOS	290		

		Horario de Almacenaje				
GVR-I	Nombre configurado	Lunes a Viernes de 07:00 a 19:00	Sábado de 08:00 a 13:00	Lunes a Viernes de 19:00 a 07:00	Sábado de 13:00 a 00:00	Domingo las 24 horas
I	FULLGYE-CAJA	2.2 GB	1 GB	1 GB	1.2 GB	1.8 GB
	FULLGYE-MOSTRADOR	2.2 GB	1 GB	1 GB	1.2 GB	1.8 GB

Consumo diario		4.4 GB	2 GB	2 GB	2.4 GB	3.6 GB
TOTAL	6.4 GB					
DIAS DE ALMACENAMIENTO SOPORTADOS	160					

		Horario de Almacenaje	
GVR-C	Nombre configurado	Lunes a Domingo de 07:00 a 20:00	Lunes a Domingo de 20:00 a 07:00
C	SIVASASD-CAJA	1.3 GB	200 MB
	FULLSD-CAJA	1.8 GB	200 MB

Consumo diario		3.1 GB	0.4 GB
TOTAL	3.5 GB		

DIAS DE ALMACENAMIENTO SOPORTADOS	290

Tabla 24 - Almacenamiento por GVR

5.6 Resumen de días de almacenamiento GVR

La siguiente tabla detalla en resumen un estimado de los días de almacenamiento antes de la saturación del disco.

Agencia	Días de Almacenamiento Soportado
A	59
B	110
C	290
E	193
F	59
H	160
I	290

Tabla 25 - Resumen de Almacenamiento

5.7 Ventajas y Desventajas de la Solución

Ventajas

- Los usuarios autorizados pueden acceder al SVMIP simultáneamente para ver imágenes de calidad superior con diferentes resoluciones

desde cualquier lugar del mundo y en cualquier momento a través de Internet o las redes de celulares 3GPP.

- Permite zoom digital en vivo o en retransmisión.
- Permite realizar cambios en la configuración de manera sencilla desde cualquier punto de la red.
- Permite conexión de elementos como detectores de movimiento, magnéticos o de temperatura, para la entrada de alarma en las cámaras IP.
- Se puede expandir el número de cámaras IP fácilmente si es requerido.
- Permite transmitir y recibir audio.
- Se puede configurar cada cámara con parámetros diferentes según la calidad o le escena que se requiera capturar.
- La conexión inalámbrica (Wireless) y la tecnología PoE (Power Over Ethernet) brindan un ahorro de costos en vigilancia IP
- El cifrado a través de IPSec (seguridad IP) puede ser aplicado entre las terminales de vídeo para asegurar la privacidad de los datos
- VLAN, y otras técnicas de virtualización de red puede utilizarse para el segmento de terminales de vídeo y servidores.

Desventajas

- EL vídeo en MPEG-4 normalmente se transmite a través del protocolo de datagramas de usuario (UDP), el cual no garantiza la entrega y no ofrece facilidades para la retransmisión de paquetes perdidos.
- Al utilizar configuración o resolución alta genera retrasos y no puede ser en tiempo real por completo.
- Es necesario tener una distribución de la luz equilibrada dentro del área de vigilancia

- Reproducción de archivos podrían dejar de iniciar si el soporte de disco se llena.
- La calidad de la imagen se reducirá debido a fuertes contraluces o manchones blancos.
- Una infraestructura de red IP es necesaria
- Las estaciones PCs deben tener Internet Explorer (IE) con los controles Active-X.
- Ancho de banda WAN es la más costosa y los tipos de transporte disponibles dependen del proveedor que ofrece servicio en el área geográfica.
- Implementar una solución de vigilancia de vídeo a través de un entorno WAN presenta desafíos que no se suelen ver en una LAN.
- En algunos casos, puede haber un retraso hasta un minuto, desde el momento en que un operador selecciona una fuente de la cámara, hasta que la secuencia aparezca en pantalla.

Capítulo VI

De los resultados obtenidos en las pruebas se pueden extraer las conclusiones que se indican a continuación. Igualmente, después de realizado el trabajo, de la experiencia adquirida es posible emitir algunas recomendaciones.

6.1 Conclusiones

- Se debe tomar en cuenta la ruta del cableado según requerimientos del cliente.
- Un SVMIP es sencillo, fácil y rápido de implementar.
- Un SVMIP nos ofrece varias características o servicios adicionales bastante útiles que se pueden utilizar inmediata o posteriormente según los requerimientos o necesidades.
- Un SVMIP permite un monitoreo bastante flexible.
- Una expansión o modificación del SVMIP sería bastante sencilla y no interrumpiría la configuración o funcionamiento actual.
- Para aprovechar o utilizar la mayoría de características es necesaria una fuerte inversión en equipos como sensores de alarma, switchs POE que tienen un costo alto en el mercado.
- Las cámaras IP externas necesitan un mayor ancho de banda que las interiores ya que poseen una resolución más alta.
- El bitrate o consumo del sistema no es proporcional a la calidad y Kbps aproximado ya que depende de la cantidad de movimiento en el área de la cámara IP.
- La grabación y reproducción en vídeo representa una herramienta muy útil para los operadores del SVMIP, sea para registrar o revisar actitudes o escenas sospechosas para tomar medidas preventivas.
- Debido a la centralización del SVMIP el mismo puede ser administrado por una sola persona sea de forma presencial o remota según se requiera.

6.2 Recomendaciones

- Siempre que sea posible, utilizar la característica de PoE en el uso de cámaras IP ya que esto simplifica la instalación ya que solo se realiza un tipo de cableado.
- Es recomendable implementar QoS para el tráfico IP de vídeo vigilancia ya sea por prioridad de encolamiento IP o por ancho de banda.
- Protocolo de Tiempo para Redes o Network Time Protocol (NTP) debe estar configurado para un recurso de hora exacta y coherente para todos los dispositivos de vídeo vigilancia en la red.
- La mayoría de las implementaciones se requieren por lo menos 4 CIF de resolución de vídeo para una alta calidad de vídeo.
- Es recomendable configurar la detección de movimiento luego de agregar la cámara IP al GVR y activar la grabación de eventos en el mismo.
- Para mantener la calidad de la señal de video debe monitorear el ancho de banda de la conexión y establecer una codificación adecuada que se ajuste al ancho de banda disponible.
- Se debe asignar convenientemente las claves de acceso al SVMIP, para prevenir accesos no autorizados al mismo.
- Se recomienda realizar inspecciones periódicas en todas las conexiones tanto eléctricas, inalámbricas y mecánicas para mantener en buen funcionamiento todo el sistema.
- Se recomienda realizar un respaldo del video almacenado cada 20 días con el objetivo de no perder información cuando el grabador sobre escriba el video almacenado.
- Se recomienda instruir al personal que administrara el sistema para administración y configuración avanzada del SVMIP, logrando que este se familiarice con todas las características del SVMIP.

Bibliografía

- 3cx Voip (25 Febrero 2010)

  Disponible en: www.3cx.es.

- Aníbal R, Figueiras. Madrid 2002. Una Panorámica de las telecomunicaciones Convergencia IP pág. 93,94.

- Ateinco Redes Diseño de Red Convergencia de Redes IP (24 Febrero 2010).

  Disponible en: www.ateinco.com.

- GUSTAVO CABRERA - DIRECTOR ICONO Capital Consulting and Traiding Nuevos Sistemas de Vigilancia Cámaras IP (25 Febrero 2010).

  Disponible en: www.cap-consulting.com.

- IP.TV inicio Que es (26 Febrero 2010).

  Disponible en: www.ip.tv/iptv_site/esp/htm/plataforma.html.

- Iain E.G. Richardson Inglaterra 2003. H.264 and MPEG-4. pág. 5, 6,7.

- Mitecnologico Main Redes Convergentes (24 Febrero 2010).

  Disponible en: www.mitecnologico.com.

- Rob Koenen Overview of the MPEG-4 Standard March 2002.

  Disponible en: mpeg.chiariglione.org/standards/mpeg-4/mpeg-4.htm.

- Tecnología Media Solutions Vídeo Digital (25 Febrero 2010).

  Disponible en: media-solutions.buscamix.com.

- Voip-voice-over-ip VoIp Standards y Protocols (25 Febrero 2010).

  Disponible en: www.voip-voice-over-ip.com.

- Estimación de Ancho de Banda (2010).

  Disponible en: http://www.visionxip.com.

- Estimación de Ancho de Banda (Mayo 2006).

  Disponible en: http://www.boschsecurity.com

Anexos

Anexo 1 Estructura detallada de la Red

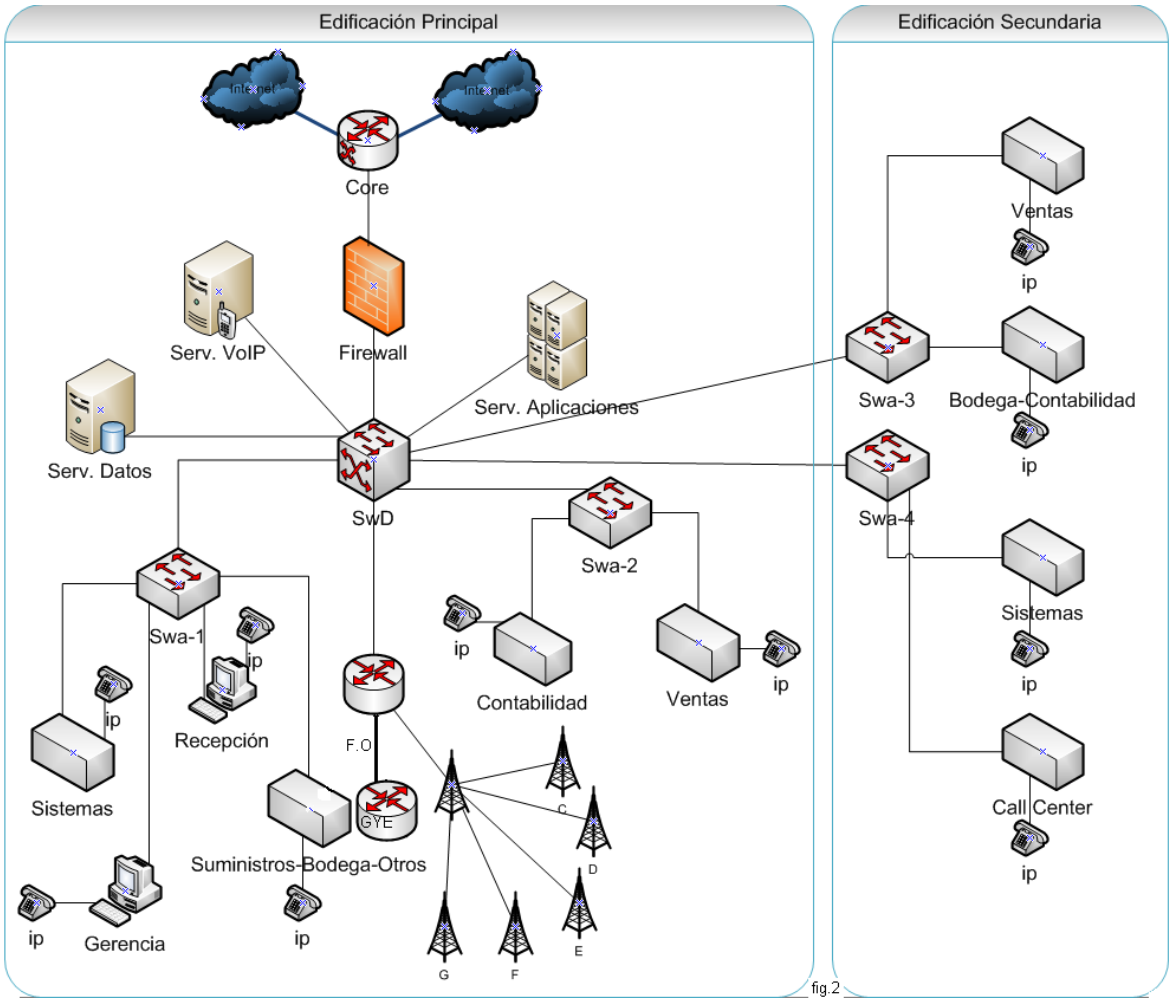


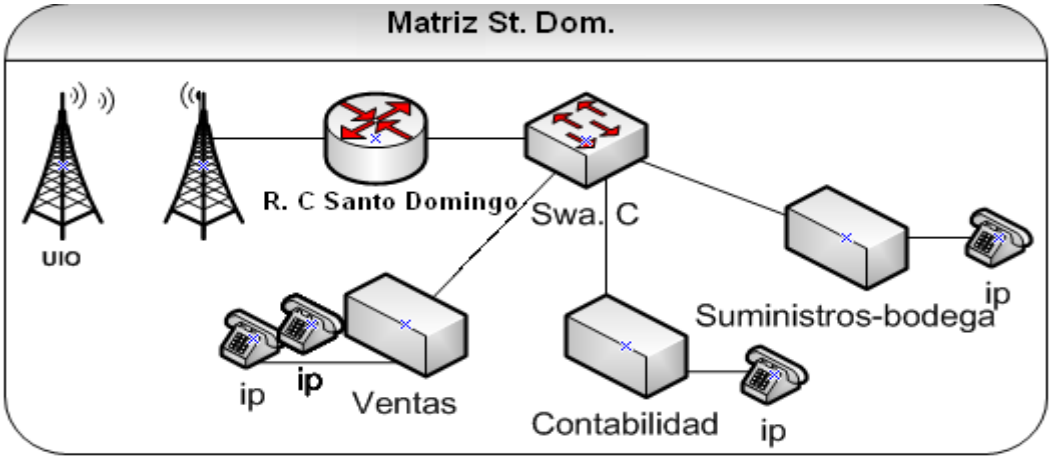
fig.2

- **Matriz - UIO**

  Su estructura se compone de dos edificaciones una principal y otra secundaria donde se expenden repuestos. La edificación principal la cual es muy amplia cuenta con una Central de Datos, donde se encuentra: Varios patch panels en un rack pequeño para datos y de reflejo para líneas telefónicas, un router de core el cual brinda la salida hacia internet (mediante una salida principal y una de backup), mismo que va conectado a un Firewall, después a un switch de distribución, al cual van conectados los servidores de Datos, de Aplicaciones y de VozIP, después a switches de acceso que van orientados a los usuarios de diferentes áreas como por ejemplo: contabilidad, sistemas, ventas, entre otras; un router el cual se

conecta mediante un enlace de fibra óptica a la sucursal principal en Guayaquil y mediante un enlace radial a las sucursales B,C, D,E,F. En esta localidad se colocarían cuatro cámaras IP una externa y tres internas, las cuales se integrarían de cableado estructurado, mismo al que se fusionará el cableado para las cámaras IP en un tramo ya que para otro habrá que realizarlo, hasta llegar a uno de los patch panel de datos que cuenta con puertos libres en el centro de datos, integrando así las cámaras IP a la red.

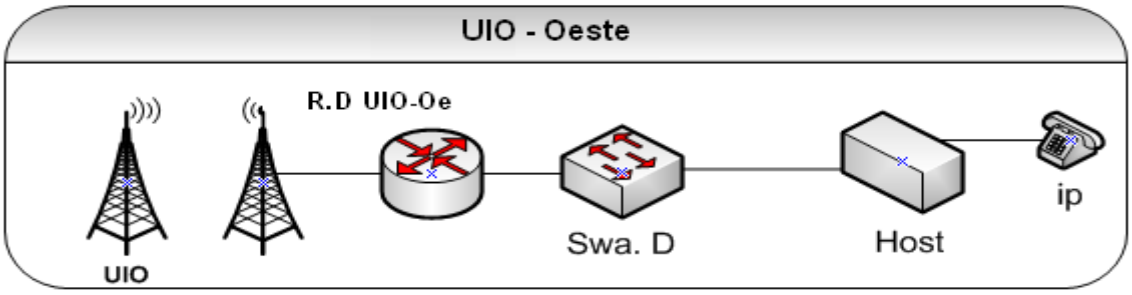
En la edificación secundaria se encuentra un rack de pared con switches de acceso de los cuales uno tiene una conexión a el switch de distribución en el centro de datos; y a los que se conectan los usuarios que se encuentran en las áreas de ventas, bodega, sistemas y call center de esta edificación, patch panel para datos y de reflejo para voz. En esta localidad se colocarían des cámaras IP una externa y una interna, las cuales se integrarán en la mayor parte al cableado estructurado de la localidad.



- **Matriz St. Dom.**

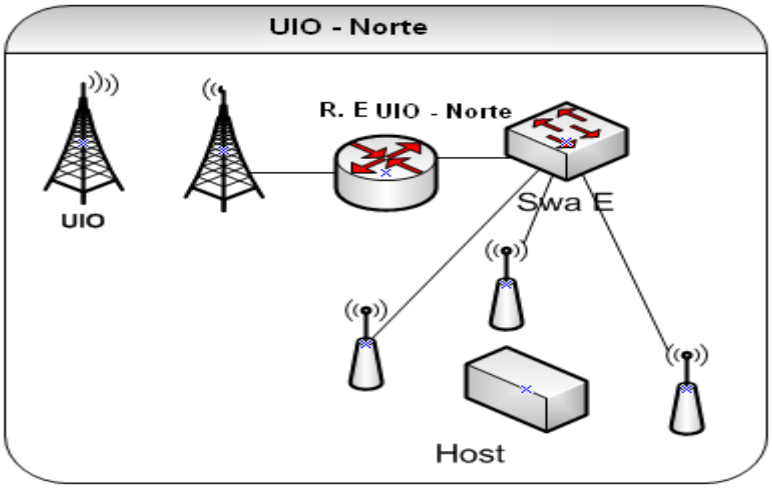
  Esta localidad cuenta con un pequeño rack de pared conformado por un router que mediante el enlace radial es el encargado de la conexión al centro de datos, un switch orientado al acceso del personal de ventas, de contabilidad y de suministros. En esta localidad se colocarían dos cámaras IP internas, las cuales se

integrarían en determinado tramo al cableado estructurado de la localidad.



- **UIO - Oeste**

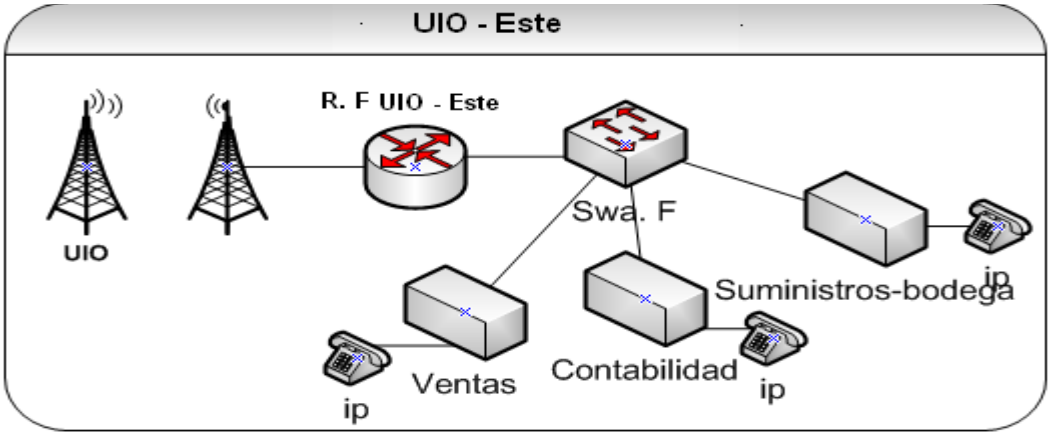
  Cuenta con un pequeño rack conformado por el router que se encarga de la conexión con el centro de datos, un switch de acceso al cual van conectados un solo grupo usuarios en esta sucursal.En esta localidad se colocaría una cámara IP externa, la cual no se integrara al cableado de esta localidad ya que su ruta será diferente y muy corta para llegar a uno de los puntos en el rack.



- **UIO - Norte**

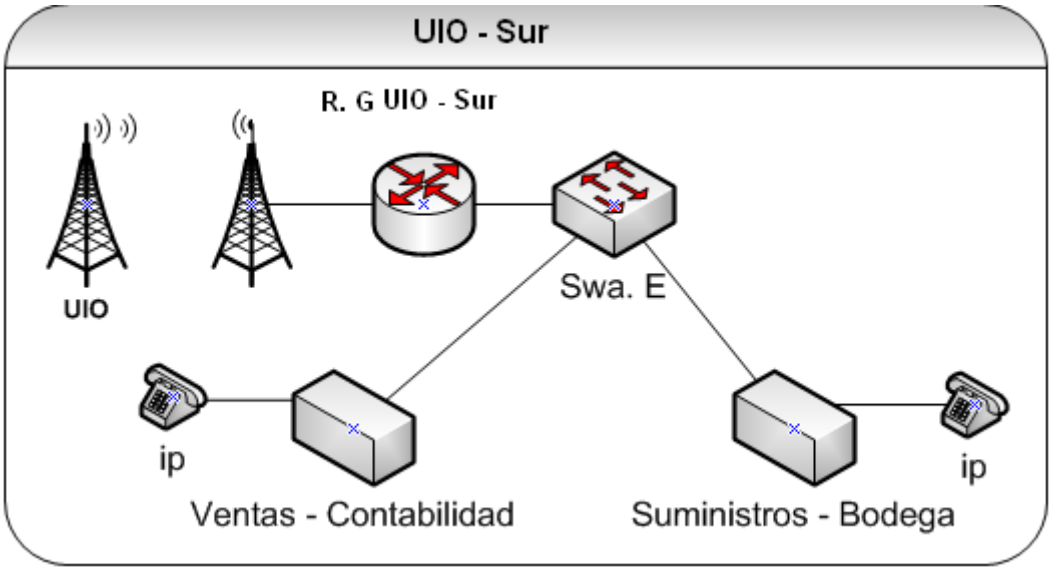
  Cuenta con un pequeño rack conformado por el router que se encarga de la conexión con el centro de datos, un switch de acceso al cual van conectados tres puntos de acceso inalámbrico mediante los cuales se conectan los usuarios a la red conformando así una

pequeña red inalámbrica. En esta localidad se colocarían dos cámaras IP internas, las cuales debido a que la red es inalámbrica; Por lo cual tomando en cuenta que el área de la localidad no es muy extensa se realizará el cableado de las cámaras en todo su trayecto hacia el rack.



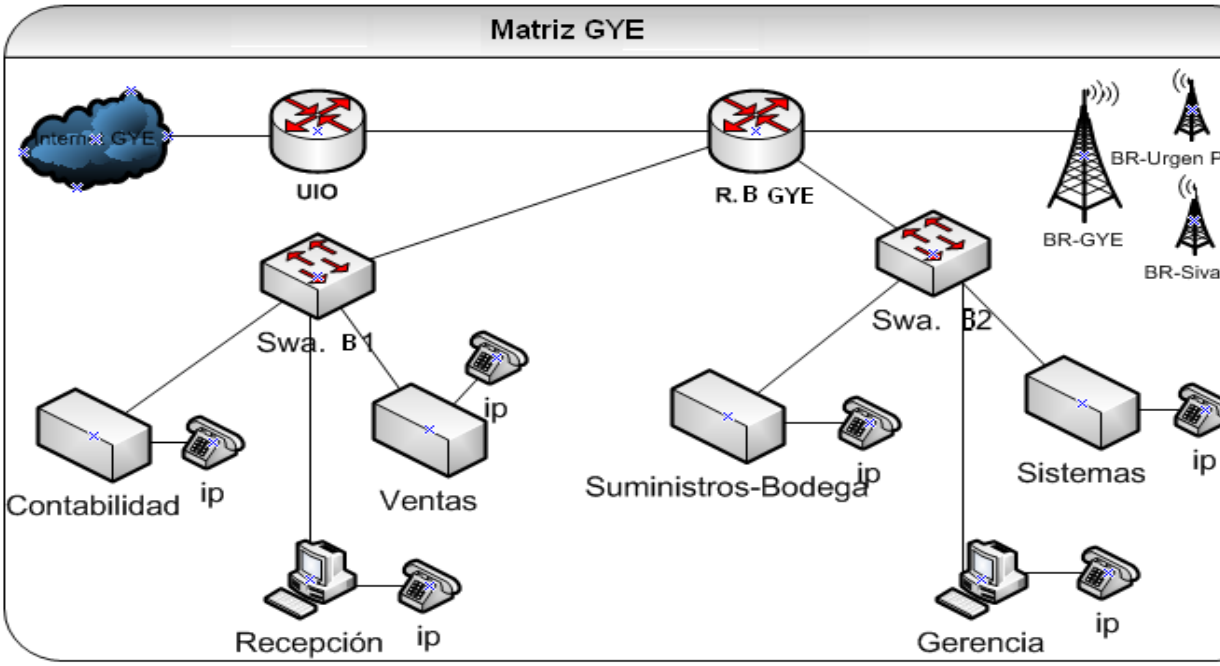
- **UIO - Este**

  Cuenta con un pequeño rack de pared conformado por un router que mediante el enlace radial es el encargado de la conexión al centro de datos, un switch orientado al acceso del personal de ventas, a un área de contabilidad y suministros. En esta localidad se colocarían dos cámaras IP una externa y una interna, cuyo cableado no se integrara al de la localidad, tomando una ruta diferente para llegar al rack.



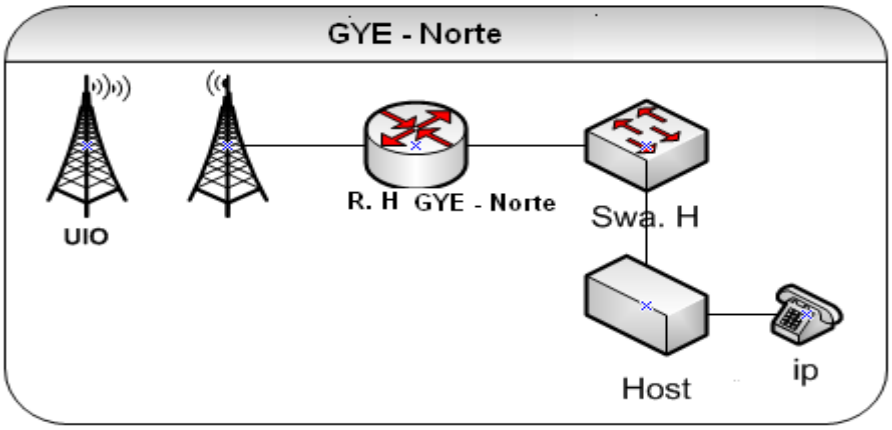
- **UIO - Sur**

  De forma parecida a la sucursal anterior cuenta con un pequeño rack conformado por el router que se encarga con la conexión con el centro de datos, un switch de acceso al cual van conectados los usuarios de ventas y suministros en esta sucursal. En esta localidad se colocaría una cámara IP externa con ruta diferente del cableado estructurado de la localidad para llegar hasta el rack.



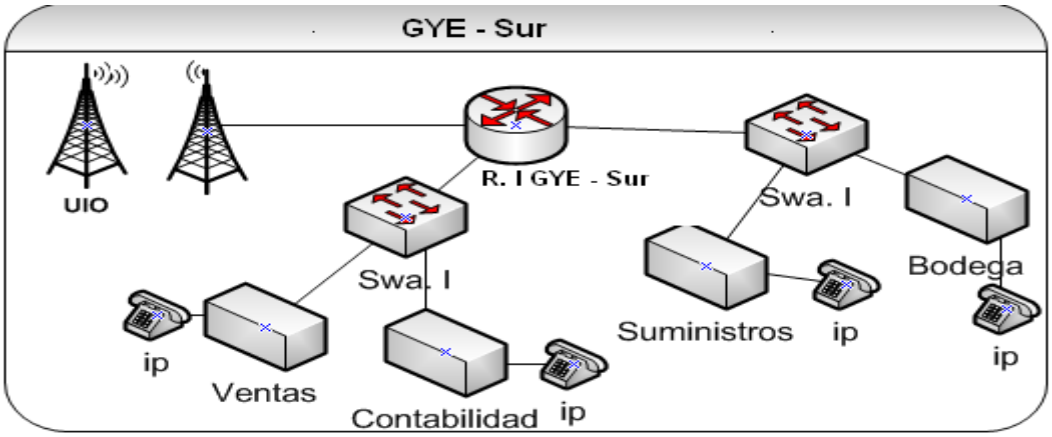
- **Matriz GYE**

Cuenta con un pequeño rack el cual está conformado por un router conectado por medio de un enlace de fibra óptica al centro de datos en Quito, mediante bases radiales a dos sucursales en Guayaquil y provee de un servicio de internet a las mismas ya que posee salida a este servicio por medio de un proveedor local, cuenta con 2 switches para el acceso de las áreas de ventas, contabilidad, sistemas, entre otras. En esta localidad se colocarían dos cámaras IP una externa y una interna, para las cuales habrá que cablear fuera del cableado estructurado de la localidad, hasta determinado tramo en el que se integrará al de la sucursal para llegar hasta el rack.



- **GYE - Norte**

  Cuenta con un rack conformado por un router el cual mediante una base radial se encarga con la conexión a la sucursal principal de Guayaquil, dos switches de acceso a los que se conectan los usuarios en la sucursal. En esta localidad se colocarían dos cámaras internas, las cuales debido a su ubicación habría que realizar un cableado separado al ya establecido para llegar más fácilmente hasta el rack.



- **GYE - Sur**

  De forma similar cuenta con un rack conformado por un router el cual mediante una base radial se encarga con la conexión a la sucursal principal de Guayaquil, dos switches de acceso a los que se conectan los usuarios en las áreas de ventas, contabilidad y suministros de la sucursal. En esta localidad se colocarían dos cámaras IP una externa y una interna, para las cuales habrá que cablear fuera de la ruta establecida hasta determinado tramo en el que se integrará al de la sucursal para llegar hasta el rack.

Anexo 2 Detallado Áreas de cobertura y Factibilidad

a. Detallado Áreas de cobertura

A continuación se detallará las características de las aéreas donde se colocara cada cámara IP.

- **Matriz - UIO**

En la edificación principal se colocarían seis cámaras IP cubriendo las áreas:

1. La entrada externa de la edificación como del ingreso de automóviles. Siendo necesaria una buena secuencia ya que es un área con movilidad y de gran rango por lo que la resolución deberá ser buena

2. El show-room cubriendo la entrada a la edificación y el área de exhibición de los automóviles más importantes. Siendo necesaria una alta resolución mas no secuencia.

3. El área de ventas, cubriendo un hall extenso. Siendo necesaria una buena resolución y la secuencia puede ser normal ya que si hay movimiento el mismo es moderado.

4. El área de talleres, cubriendo una superficie muy extensa y de constante movimiento. Siendo necesaria una buena secuencia y buena resolución.

En la edificación secundaria se colocarían dos cámaras IP cubriendo las áreas:

5. La entrada a los talleres y al área de venta de repuestos. Siendo necesaria una buena resolución y secuencia ya que es un área de movimiento frecuente.

6. El área de ventas, cubriendo la entrada principal y una secundaria. Siendo necesaria una buena resolución y secuencia moderada.

- **Matriz St. Dom.**

  En esta sucursal se colocaran dos cámaras IP en las aéreas:

  1. La entrada cubriendo recepción, un pequeño showroom junto. Siendo necesaria una buena resolución y la secuencia puede ser normal ya que el mismo es moderado.

  2. El área de Ventas cubriendo otra parte del showroom. Siendo necesaria una buena resolución y la secuencia puede ser normal ya que si hay movimiento el mismo es moderado.

- **UIO - Oeste**

  En esta sucursal se colocara una cámara IP cubriendo.

  1. La entrada al taller. Siendo necesaria una buena resolución y la secuencia puede ser normal ya que el movimiento moderado.

- **UIO - Norte**

  En esta sucursal se colocaran tres cámaras cubriendo las aéreas:

  1. La entrada principal y el área de caja. Siendo una localidad no muy extensa la resolución no necesita ser muy alta y la secuencia puede ser normal ya que el movimiento es moderado.

  2. La caja y una entrada trasera. Utilizando los mismos parámetros que la anterior.

  3. La entrada al área de gerencia y tres ventanales a un lado de la entrada. La superficie igualmente es pequeña, por lo que utilizaría una resolución y secuencia normal.

- **UIO - Este**

  En esta sucursal se colocara dos cámaras IP cubriendo.

  1. La entrada a la localidad y el parqueadero. Debido a que la cámara ira en exteriores es necesaria una buena resolución y la secuencia normal ya que el movimiento es moderado.

  2. El área de ventas. Siendo un área pequeña y cercana a la cámara IP, la resolución no necesita ser muy alta y la secuencia puede ser normal ya que el movimiento es moderado.

- **UIO - Sur**

  En esta sucursal se colocara una cámara IP cubriendo.

  1. La entrada a la localidad. Debido a que la cámara ira en exteriores es necesaria una buena resolución y la secuencia normal ya que el movimiento es moderado.

- **Matriz - GYE**

  En esta sucursal se colocaran dos cámaras IP cubriendo:

  1. La entrada a la localidad y el parqueadero. Debido a que la cámara ira en exteriores es necesaria una buena resolución y la secuencia normal ya que el movimiento es moderado.

  2. El área de Ventas y cubriendo un pequeño showroom. Siendo necesaria una buena resolución y la secuencia puede ser normal ya que si hay movimiento el mismo es moderado.

- **GYE - Norte**

  En esta sucursal se colocaran dos cámaras IP cubriendo:

  1. La entrada principal. Siendo una localidad no muy extensa la resolución no necesita ser muy alta y la secuencia puede ser normal ya que el movimiento es moderado.

2. El área de caja. Siendo un área no muy extensa, la resolución no necesita ser muy alta y la secuencia puede ser normal ya que el movimiento es moderado.

- **GYE - Sur**

  En esta sucursal se colocaran dos cámaras IP cubriendo:

  1. La entrada principal. Siendo una localidad no muy extensa la resolución no necesita ser muy alta y la secuencia puede ser normal ya que el movimiento es moderado.

  2. El área de ventas. Siendo un área extensa, la resolución necesita ser buena y la secuencia puede ser normal ya que el movimiento es moderado.

b. Detallado de Factibilidad

- **Matriz UIO**

  En esta localidad se dispone de un AB de una red LAN es decir 100 Mbps (que equivale a 100000000 Kbps) ya que el sistema de monitoreo ira en esta localidad, por lo cual se utilizaran parámetros altos de CIF y FPS, para las seis cámaras, las cuales generan un consumo aproximado de 14.4 Mbps.

  En conclusión si es factible ya que se dispone de 100 Mbps.

- **Matriz St. Dom.**

  En esta localidad se dispone de un AB de 256 Kbps y se colocarán dos cámaras IP con parámetros bajos a medios de CIF y FPS generando un consumo aproximado de 280 Kbps.

  En conclusión no es factible ya que el AB es insuficiente por lo cual:

  -Es necesario que se amplié el AB actual a mínimo el doble.

-Se configuraría las cámaras IP con parámetros bajos, lo cual no es recomendable, sin embargo sería una opción.

- **UIO - Oeste**

  En esta localidad disponemos de un AB de 256 Kbps y se colocaran una cámara IP con parámetros bajos a medios de CIF y FPS generando un consumo aproximado de 140 Kbps.

  En conclusión sería factible ya que el AB disponible es de casi el doble del que se necesitaría.

- **UIO - Norte**

  En esta localidad disponemos de un AB de 256 Kbps y se colocaran tres cámaras IP con parámetros bajos a medios generando un consumo aproximado de 240 Kbps.

  En conclusión no es factible ya que en vista que es un valor aproximado, podría saturar el AB por el cual fluye el tráfico de la localidad. Por lo cual:

  -Es necesario que se amplié el AB actual a mínimo el doble.

  -Se configuraría las cámaras IP con parámetros bajos.

- **UIO - Este**

  En esta localidad disponemos de un AB de 512 Kbps y se colocaran dos cámaras IP con parámetros bajos a medios generando un consumo aproximado de 220 Kbps.

  En conclusión sería factible ya que el AB disponible es de casi el doble del que se necesitaría.

- **UIO - Sur**

En esta localidad se dispone de un AB de 256 Kbps y se colocará una cámara IP con parámetros medios de CIF y FPS generando un consumo aproximado de 140 Kbps.

En conclusión sería factible ya que el AB disponible es de casi el doble del que se necesitaría.

- **GYE - Norte**

  En esta localidad se dispone de un AB de 256 Kbps y se colocaran dos cámaras IP con parámetros bajos a medios generando un consumo aproximado de 240 Kbps.

  En conclusión no es factible ya el consumo aproximado, podría saturar el AB de la localidad. Por lo cual:

  -Es necesario que se amplié el AB actual a mínimo el doble.

  -Se configuraría las cámaras IP con parámetros bajos.

- **GYE - Sur**

  En esta localidad se dispone de un AB de 512 Kbps y se colocaran dos cámaras IP con parámetros bajos a medios generando un consumo aproximado de 260 Kbps.

  En conclusión sería factible ya que el AB disponible es de casi el doble del que se necesitaría.

- **Matriz GYE**

  En esta localidad se dispone de un AB de 1.5 Mbps y se colocarán dos cámaras IP con parámetros bajos a medios generando un consumo aproximado de 280 Kbps, además el AB de esta localidad es por el cual se enviará las transmisiones de las dos sucursales de Guayaquil por lo que el consumo generado aproximado total sería de:

280 Kbps la localidad + 260 Kbps GYE-Norte + 240 Kbps GYE-Sur; dándonos un total de 780 Kbps.

En conclusión sería factible ya que el AB disponible es de casi el doble del que se necesitaría.

Anexo 3 Características y Equipos del Sistema de Vigilancia y Monitoreo IP

Central de Monitoreo

Para la central de monitoreo se utilizarán dos monitores de 17” a 19”, para visualizar todas las cámaras IP a la vez; conectaos a un computador con las siguientes características:

HARDWARE	SOFTWARE
Procesador Core 2 Duo 2,4 Ghz, o superior. Memoria de 2 GB o superior. Unidad de cd-rom. Tarjeta para manejo de al menos 2 monitores. Tarjeta de vídeo para manejar resoluciones de mínimo 1024 x 768. Tarjeta de red.	Windows XP Internet Explorer 6.0 o superior

Características del Computador de Monitoreo.

GVR (NVR)

Siendo uno de los elementos más importantes del sistema y para que sea un Sistema de Vigilancia y Monitoreo IP escalable se seleccionara un equipo de alta flexibilidad, compatibilidad y de interfaz agradable para el usuario. Por ello se trabajará con equipos QNAP, los mismos que son reconocidos y premiados internacionalmente.

Se utilizarán estos equipos porque tiene un alto nivel de compatibilidad con variedad de marcas en cámaras IP, como con Discos Duros (HDD. 1 por GVR y 5 en el de gran capacidad). Los equipos que se utilizarán son:

Equipo:	Localidad:
GVR – 104V	Para almacenamiento en las agencias y sucursales.
VS – 8040	Para almacenamiento en la Agencia Matriz
GVR de gran capacidad	(Central de Monitoreo).

GVR del Sistema de Vigilancia y Monitoreo.

Características GVR's

a) GVR – 104V

Las que más destacan son:

- Grabación ultra estable y fiable sin PC
- Grabaciones de alta calidad depende de la cámara
- Grabación programada, grabación de alarmas, programación de grabación de alarmas
- Monitorización desde múltiples servidores QNAP GVR a través de LAN o WAN.
- Acceso a datos mediante un explorador web, FTP, y el Entorno de Red.
- Búsqueda fácil de información por fecha & hora, horarios, análisis inteligente de eventos y de vídeos (IVA).
- Zoom digital para monitorización y reproducción.
- Notificación de alarmas durante la monitorización.
- Registros de eventos y sistema detallados.
- Programación de replicación o copias de seguridad de las grabaciones.
- Botón de copia de seguridad de un solo toque para una fácil copia de grabación.
- Grabación continua/ manual/ programada.
- Grabación de alarmas (mediante detección de movimiento o activada por sensor).
- E-mapa exclusive para permitirle subir imágenes de los sitios de monitorización.

- Soporta la grabación de audio para una vigilancia completa (depende de la cámara).
- Soporta 1 Disco Duro SATA de Alta Velocidad, Ampliable a 2TB mediante un Dispositivo SATA Externo.
- Alta Fiabilidad y Funciones Inteligentes.
- La fecha y hora de las cámaras de red puede sincronizarse con el GVR.

b) GVR – 8040

Posee características parecidas agregando:

- Incluye un Sistema exclusivo con Linux integrado, SO dual a prueba de fallos para una mayor fiabilidad, CPU Intel® Core™, con microprocesador 2 Duo de 2,8GHz y memoria DDRII de 2GB.
- Para grabaciones largas tiene una capacidad de almacenamiento de hasta 16TB.
- Diseño de cambio en caliente, entre otras ventajas.

Más información en: www.qnap.com

Cámaras IP

En estos equipos trabajaremos con la marca Vivotek, la cual está especializada en aplicaciones de vídeo vigilancia. Posee una gran variedad de cámaras IP de las cuales trabajaremos con:

Equipo:	Área:
FD7131	Interna
IP7330	Externa

Cámaras IP del Sistema de Vigilancia y monitoreo IP

Características Cámaras IP

a) FD7131

Las que más destacan son:

- Lente varifocal de ángulo extendido.
- Compresión en tiempo real MPEG-4 y MJPEG.
- Soporta streaming dual simultáneo.
- Sensor de movimiento incorporado para la detección de personas.
- Iluminadores de luz blanca incorporados
- Soporta vigilancia Móvil 3GPP
- Soporta audio bidireccional mediante protocolo SIP
- Entrada digital para sensor externo
- HTTPS

b) IP7330

Posee características parecidas agregando:

- Lente con filtro de banda dual para perfecto funcionamiento Día/Noche.
- Iluminador infra rojo integrado con alcance de hasta 10 m.
- Resistencia anti vandalismo y protección.
- Detecta intentos de alteración como bloqueo, re direccionamiento o pintura en espray, entre otras.

Más información en: www.vivotek.com

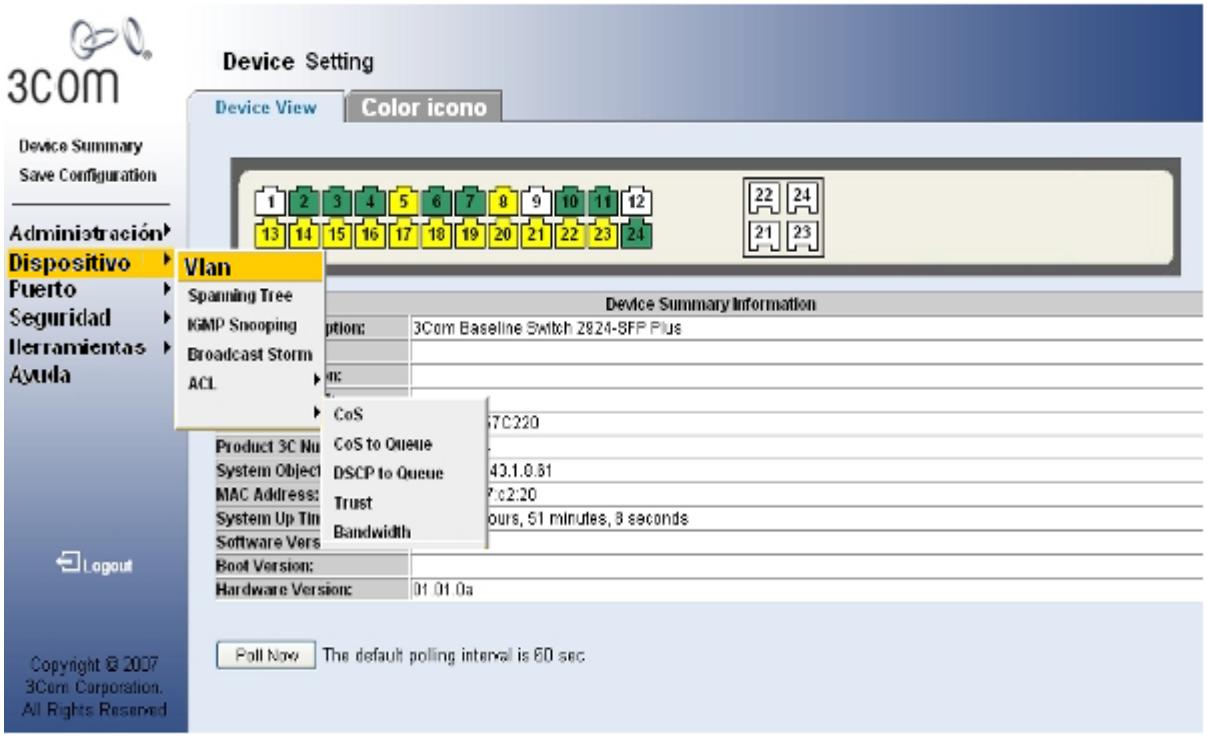
Anexo 4 Configuración Switch

a. Configuración web:

1) Se accesa al switch mediante la dirección IP pre-configurada.

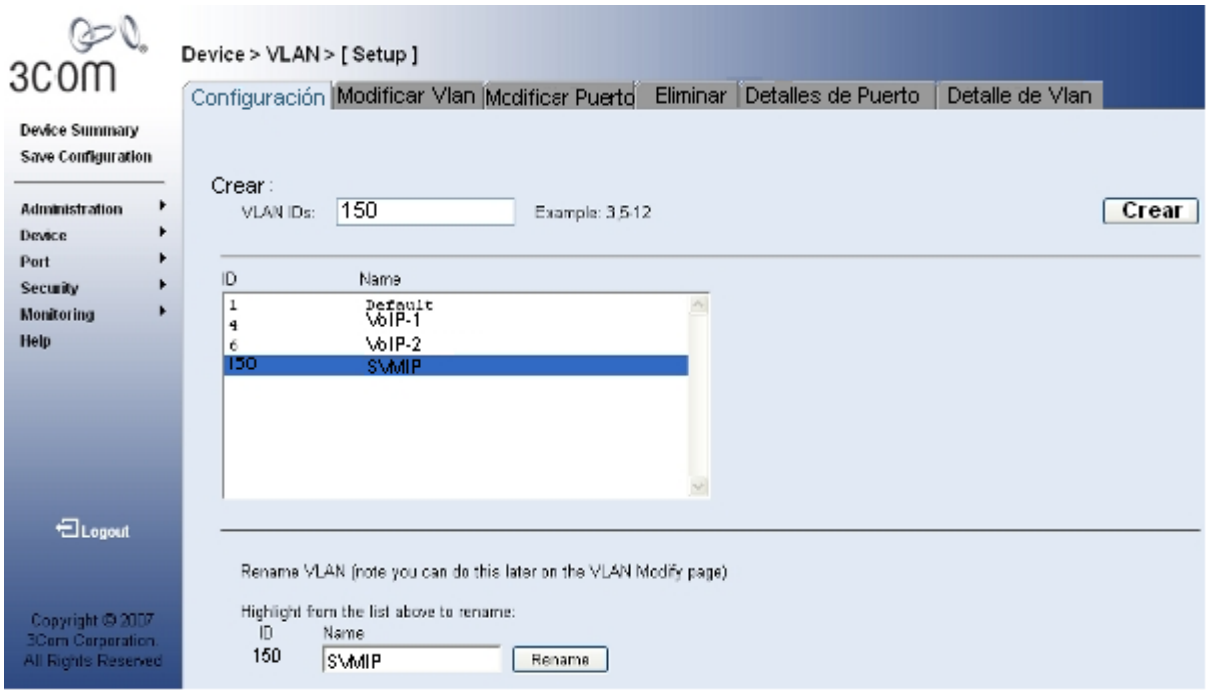
   Mediante el nombre de usuario y la clave asignada al mismo.

   Luego de lo cual nos aparecerá la siguiente pantalla, en la que se seleccionará “Dispositivo” y la opción “VLAN”:



Interface Web Del Switch

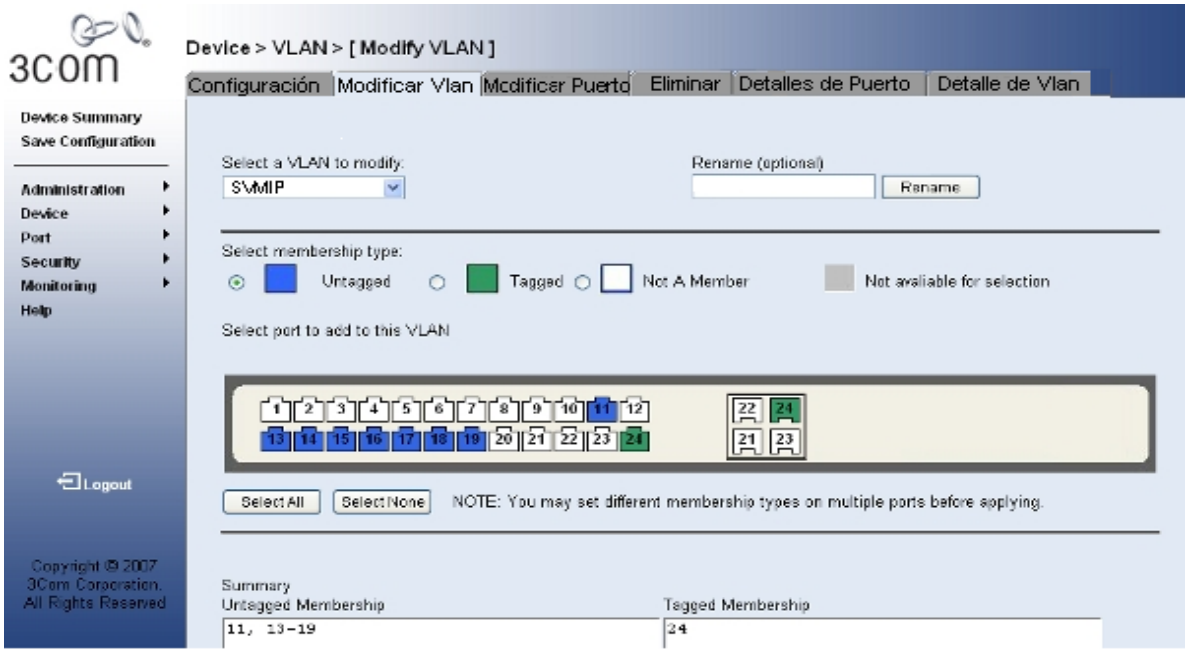
2) Se digita el ID de la VLAN a crear, la cual será 150 y seleccionamos "crear":



Configuración de VLAN

3) Se selecciona “Crear” y aparecerá la siguiente pantalla:

Por último asignaremos los puertos a dicha VLAN.

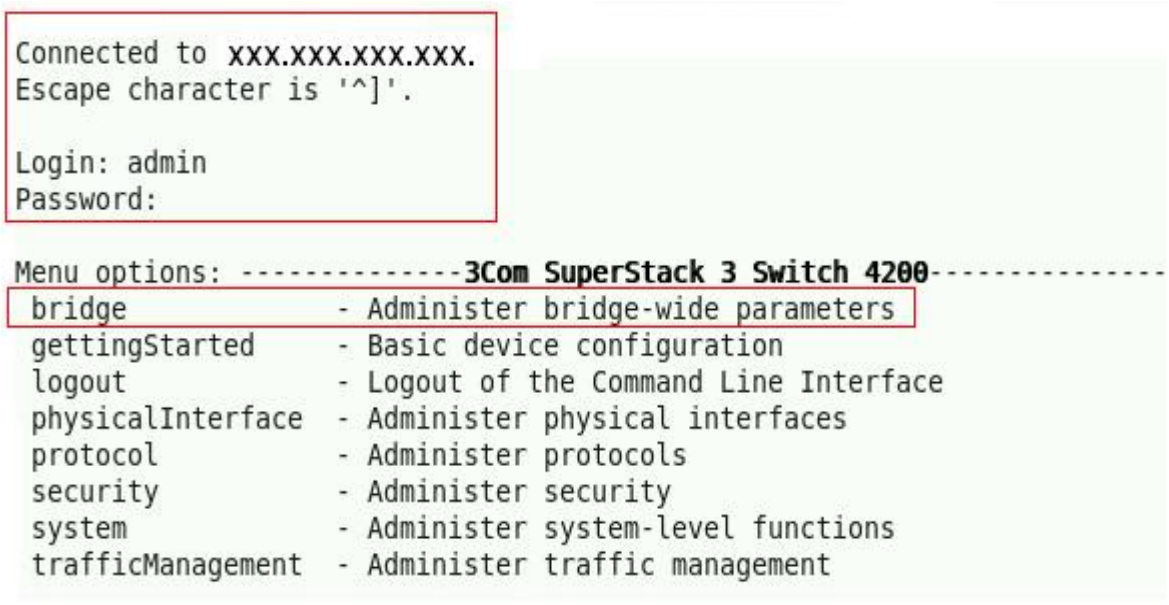


Interface para Gestión de VLANs

b. Configuración vía consola:

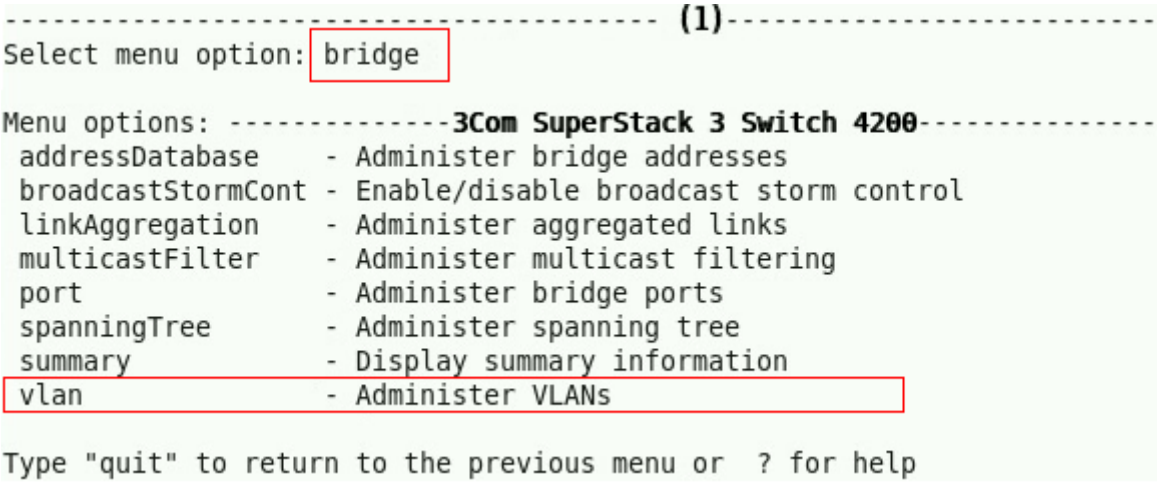
Para esta es necesario utilizar un cable de consola, y utilizando el programa Hyper Terminal o ingresando al equipo mediante SSH o Telnet.

1) Se establece la conexión con el “Switch”, es necesario autentificarse colocando el nombre de usuario y clave asignada.



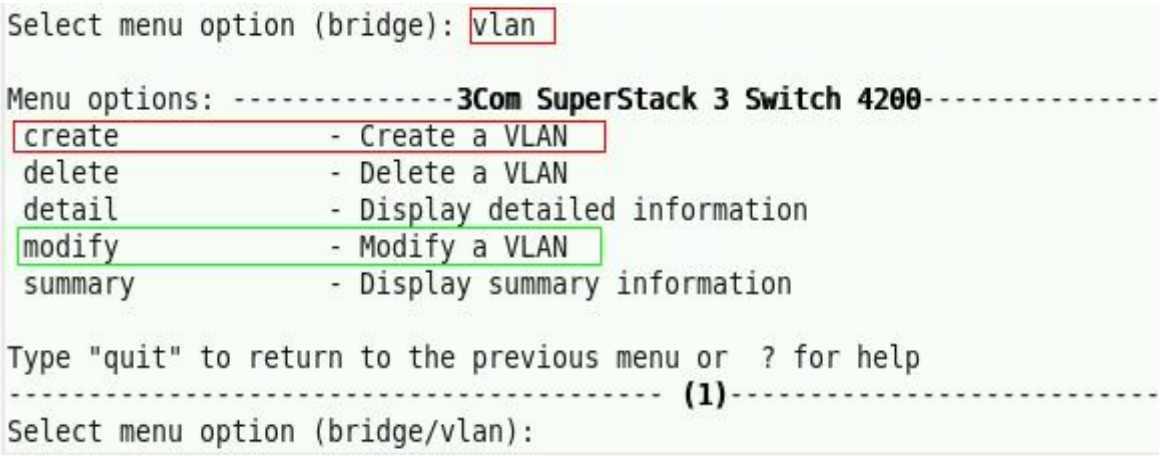
Interfaz de Consola

2) Se digita la opción ‘Bridge’ para administrar las opciones de ancho de “puente”.



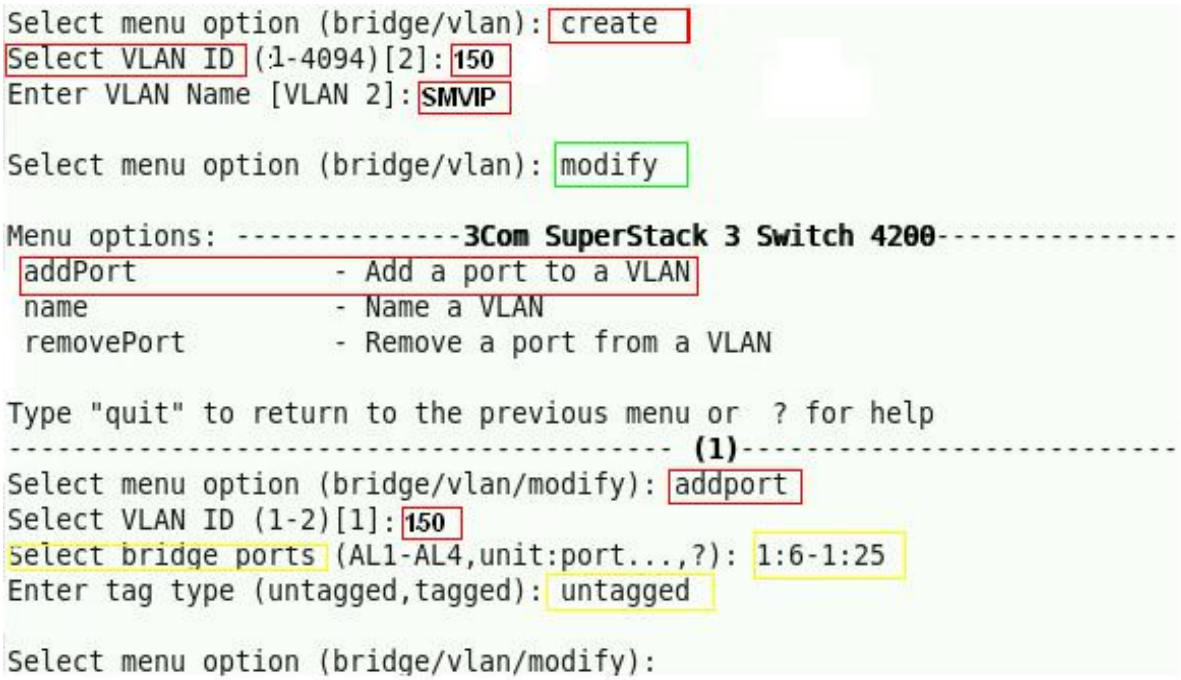
Opciones de Configuración

3) Se digita la opción ‘’VLAN’’ para administrar las opciones de VLAN.



Gestión de VLANs

4) Se digita la opción crear para crear la VLAN deseada, se digita el ID de la VLAN y el nombre para la misma, luego la opción ‘’modificar’’ para ingresar a dichas opciones se digita la opción ‘’agregar puerto’’, se selecciona el ID de la VLAN a la cual deseamos agregar los puertos, se digita el Slot, seguido del puerto inicio, guion el slot y puerto final, se digita la opción untagged ya que no es VoIP.



Asignación de Puertos

5) Se digita ‘’quitar’’ para salir de la opción ‘’modificar’’, se digita la opción ‘’detallar’’ y seleccionamos la ‘’VLAN’’ deseada para verificar

la misma. Y por último, se da por terminada la sesión con el comando ‘’Logout’’.

```
Select menu option (bridge/vlan/modify): quit

Menu options: --------------3Com SuperStack 3 Switch 4200---------------
 create             - Create a VLAN
 delete             - Delete a VLAN
 detail             - Display detailed information
 modify             - Modify a VLAN
 summary            - Display summary information

Type "quit" to return to the previous menu or  ? for help
---------------------------------------- (1)---------------------------
Select menu option (bridge/vlan): detail
Select VLAN ID (1-2)[1]: 150

VLAN ID: 150     Name: aula

Unit              Untagged Member Ports      Tagged Member Ports
----------------- -------------------------------------------------------
1                 6-25                       none
Aggregated Links  none                       none

Select menu option (bridge/vlan): logout
```

Verificación de la Configuración