Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per D-Link DGS-1100 DGS-1100-26MPV2 o cerca il tuo prodotto tra le migliori offerte di Switch

D-Link
Building Networks for People

DGS-1100-16V2/24V2/24PV2/10MPV2/10MPPV2/26MPV2/26MPPV2/18PV2

Web UI Reference Guide

Ver. 2.10

Information in this document is subject to change without notice.
© 2020 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

Federal Communication Commission Interference Statement

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 this user's guide, 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.

Innovation, Science and Economic Development Canada (ISED) Statement

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

VCCI-A Warning

この装置は、クラス A 情報技術装置です。 この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。 この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Japan Voluntary Control Council for Interference Statement
This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

警告使用者:

此為甲類的資訊技術設備，在居住環境中使用時，可能會造成射頻擾動，在這種情況下，使用者會被要求採取某些適當的對策。

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.

CE Mark Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

SAFETY INSTRUCTIONS

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

• Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
• Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.
• Do not spill food or liquid on your product and never push any objects into the openings of your product.
• Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.
• Keep the product away from radiators and other heat sources.
• Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

SICHERHEITSVORSCHRIFTEN

Die folgenden allgemeinen Sicherheitsvorschriften dienen als Hilfe zur Gewährleistung Ihrer eigenen Sicherheit und zum Schutz Ihres Produkts. Weitere Details finden Sie in den Benutzeranleitungen zum Produkt.

• Statische Elektrizität kann elektronischen Komponenten schaden. Um Schäden durch statische Aufladung zu vermeiden, leiten Sie elektrostatische Ladungen von Ihrem Körper ab,
(z. B. durch Berühren eines geerdeten blanken Metallteils), bevor Sie das Produkt berühren.
• Unterlassen Sie jeden Versuch, das Produkt zu warten, und versuchen Sie nicht, es in seine Bestandteile zu zerlegen. Für einige Produkte mit austauschbaren Akkus lesen Sie bitte das Benutzerhandbuch und befolgen Sie die dort beschriebenen Anleitungen.
• Vermeiden Sie, dass Speisen oder Flüssigkeiten auf Ihr Produkt gelangen, und stecken Sie keine Gegenstände in die Gehäuseschlitze oder -öffnungen Ihres Produkts.
• Verwenden Sie dieses Produkt nicht in unmittelbarer Nähe von Wasser und nicht in Bereichen mit hoher Luftfeuchtigkeit oder Kondensation, es sei denn, es ist speziell zur Nutzung in
Außenbereichen vorgesehen und eingestuft.
• Halten Sie das Produkt von Heizkörpern und anderen Quellen fern, die Wärme erzeugen.
• Trennen Sie das Produkt immer von der Stromzufuhr, bevor Sie es reinigen und verwenden Sie dazu ausschließlich ein trockenes fusselfreies Tuch.

CONSIGNES DE SÉCURITÉ

Les consignes générales de sécurité ci-après sont fournies afin d'assurer votre sécurité personnelle et de protéger le produit d'éventuels dommages. Veuillez consulter les consignes d'utilisation du produit pour plus de détails.

• L'électricité statique peut endommager les composants électroniques. Déchargez l'électricité statique de votre corps (en touchant un objet en métal relié à la terre par exemple) avant de toucher le produit.
• N'essayez pas d'intervenir sur le produit et ne le démontez jamais. Pour certains produits contenant une batterie remplaçable par l'utilisateur, veuillez lire et suivre les consignes
contenues dans le manuel d'utilisation.
• Ne renversez pas d'aliments ou de liquide sur le produit et n'insérez jamais d'objets dans les orifices.

• N'utilisez pas ce produit à proximité d'un point d'eau, de zones très humides ou de condensation sauf si le produit a été spécifiquement conçu pour une application extérieure.
• Éloignez le produit des radiateurs et autres sources de chaleur.
• Débranchez toujours le produit de l'alimentation avant de le nettoyer et utilisez uniquement un chiffon sec non pelucheux.

INSTRUCCIONES DE SEGURIDAD

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.
• La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
• No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
• No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
• No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
• Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
• Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa

ISTRUZIONI PER LA SICUREZZA

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.
• La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
• No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
• No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
• No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
• Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
• Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa

VEILIGHEIDSINFORMATIE

De volgende algemene veiligheidsinformatie werd verstrekt om uw eigen persoonlijke veiligheid te waarborgen en uw product te beschermen tegen mogelijke schade. Denk eraan om de gebruikersinstructies van het product te raadplegen voor meer informatie.
• Statische elektriciteit kan schadelijk zijn voor elektronische componenten. Ontlaad de statische elektriciteit van uw lichaam (d.w.z. het aanraken van geaard bloot metaal) voordat u
het product aanraakt.
• U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
• Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
• Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
• Houd het product uit de buurt van radiators en andere warmtebronnen.
• U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek

Disposing and recycling your product

ENGLISH

EN

This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in the household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit www.dlinkgreen.com

DEUTSCH

DE

Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.

Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter www.dlinkgreen.com.

FRANÇAIS

FR

Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.

D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le www.dlinkgreen.com

ESPAÑOL

ES

Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio www.dlinkgreen.com

ITALIANO

IT

La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.

D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.

Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo www.dlinkgreen.com

NEDERLANDS

NL

Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen.
Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO2-emissies.

Breng een bezoek aan www.dlinkgreen.com voor meer informatie over onze milieuverantwoorde producten en verpakkingen

POLSKI

PL

Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze. Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

D-Link i środowisko

W D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO2.

Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną internetową www.dlinkgreen.com.

ČESKY

CZ

Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

D-Link a životní prostředí

Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály.

Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO2.

Více informací o našich ekologických výrobcích a obalech najdete na adrese www.dlinkgreen.com.

MAGYAR

HU

Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a www.dlinkgreen.com weboldalon tudhat meg.

NORSK

NO

Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til www.dlinkgreen.com

DANSK

DK

Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på www.dlinkgreen.com

SUOMI

FI

Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta www.dlinkgreen.com

SVENSKA

SE

Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar www.dlinkgreen.com

PORTUGUÊS

PT

Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO_2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite www.dlinkgreen.com

April, 2020

Table of Contents

Table of Contents x

1. Introduction 1

Audience 1
Other Documentation 1
Conventions 1
Notes, Notices, and Cautions 2

2. Product Introduction 3

DGS-1100-16V2 3
Front Panel 3
Rear Panel 4
DGS-1100-24V2 5
Front Panel 5
Rear Panel 5
DGS-1100-24PV2 6
Front Panel 6
Rear Panel 7
DGS-1100-10MPV2 7
Front Panel 7
Rear Panel 8
DGS-1100-10MPPV2 8
Front Panel 8
Rear Panel 9
DGS-1100-26MPV2 9
Front Panel 10
Rear Panel 10
DGS-1100-26MPPV2 11
Front Panel 11
Rear Panel 12
DGS-1100-18PV2 12
Front Panel 12
Rear Panel 13

3. Hardware Installation 14

Step1: Unpacking 14
Packing contents of DGS-1100-16V2 /24V2 /24PV2/10MPV2/10MPPV2/26MPV2/26MPPV2/18PV2 14
Step2: Switch Installation 14
Desktop or Shelf Installation 14
Rack Installation 15
Step 3 – Plugging in the AC Power Cord 16
Power Failure 16
Grounding the Switch 16

4. Web-based Switch Configuration 18

Management Options 18
Connecting using the Web User Interface 18
Logging onto the Web Manager 19

Smart Wizard....20
Web User Interface (Web UI)....23
Areas of the User Interface....23
5. System....24
Device Information....24
System Information Settings....25
System Information....25
IPv4 Interface....25
IPv6 Interface....26
Port Configuration....26
Port Settings(DGS-1100-16V2/24V2/24PV2/10MPV2/10MPPV2 Only)....26
Port Settings(DGS-1100-26MPV2/26MPPV2/18PV2 Only)....28
Port Status(DGS-1100-16V2/24V2/24PV2/10MPV2/10MPPV2 Only)....29
Port Status(DGS-1100-26MPV2/26MPPV2/18PV2 Only)....29
Jumbo Frame....30
PoE (PoE Model Only)....31
PoE System....31
PoE Status....32
PoE Configuration(DGS-1100-24PV2/10MPV2/26MPV2/18PV2 Only)....33
PoE Configuration(DGS-1100-10MPPV2/26MPPV2 Only)....34
PD Alive....36
System Log....37
System Log Settings....37
System Log Server Settings....37
System Log....38
Time....39
Clock Settings....39
Time Zone Settings....39
SNTP Settings....40
Time Range....41
6. Management....42
User Account Settings....42
SNMP....43
SNMP Global Settings....44
SNMP Community Table Settings....44
SNMP Host Table Settings....45
HTTP/HTTPS....46
D-Link Discovery Protocol....46
7. L2 Features....48
FDB....48
Static FDB....48
MAC Address Table Settings....49
MAC Address Table....50
VLAN....51
VLAN Configuration Wizard....51
802.1Q VLAN....51
Management VLAN....52

Asymmetric VLAN....52
VLAN Interface....53
Auto Surveillance VLAN....56
Voice VLAN....58
Spanning Tree....61
STP Global Settings....62
STP Port Settings....62
Loopback Detection....63
Link Aggregation....65
L2 Multicast Control....67
IGMP Snooping....67
Multicast Filtering....70
LLDP....71
LLDP Global Settings....71
LLDP Neighbor Port Information....71
8. Quality of Service (QoS)....72
802.1p Priority....72
Port Rate Limiting....73
9. Security....74
Safeguard Engine Settings....74
Traffic Segmentation....74
Storm Control....75
DoS Attack Prevention Settings....76
Zone Defense Settings....77
SSL....77
SSL Global Settings....77
10. OAM....79
Cable Diagnostics....79
11. Monitoring....81
Statistics....81
Port Counters....81
Mirror Settings....82
12. Green....83
Power Saving....83
EEE....85
13. Save and Tools....86
Save Configuration....86
Firmware Information....86
Firmware Upgrade & Backup....86
Firmware Upgrade from TFTP....87
Firmware Upgrade from HTTP....87
Firmware Backup to HTTP....87
Firmware Backup to TFTP....88
Configuration Restore & Backup....89
Configuration Restore from HTTP....89
Configuration Restore from TFTP....89

Configuration Backup to HTTP....90
Configuration Backup to TFTP....90
Log Backup....90
Log Backup to HTTP....90
Log Backup to TFTP....91
Ping....92
Reset....92
Reboot System....93
14. Appendix A - Ethernet Technology....94
Gigabit Ethernet Technology....94
Fast Ethernet Technology....94
Switching Technology....95
15. Appendix B - Technical Specifications....96
Hardware Specifications....96
Key Components / Performance....96
Port Functions....96
Physical & Environment....96
Emission (EMI) Certifications....96
Safety Certifications....96
Features....96
L2 Features....96
L2 Multicasting....97
VLAN....97
QoS (Quality of Service)....97
Security....97
Management....97
Power Saving....97
16. Appendix C –Rack mount Instructions....98
17. Appendix D–Trap Messages....99
18. Appendix E–Syslog Messages....101

1. Introduction

This manual's command descriptions are based on the software release 1.00. The commands listed here are the subset of commands that are supported by the DGS-1100 Series switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-1100 Series switch, which will be generally be referred to simply as "the Switch" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the switch. All the documents are available either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- *Getting started Guide*
- *D-Link Network Assistant (DNA) User Guide*

Conventions

Convention	Description
Boldface Font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. Bold font is also used to represent filenames, program names and commands. For example: use the **copy** command.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	Indicates the menu structure. **Device > Port > Port Properties** means the **Port Properties** menu option under the **Port** menu option that is located under the **Device** menu.
`Blue Courier Font`	This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

NOTE: A note indicates important information that helps you make better use of your device.

NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A caution indicates a potential for property damage, personal injury, or death.

2. Product Introduction

Thank you and congratulations on your purchase of D-Link DGS-1100 Series Switch Products.

D-Link's next generation DGS-1100 Series switches blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs.

The brand-new DGS-1100 series are born to be green by design of IEEE 802.3az Energy Efficient Ethernet compliant (abbreviated as EEE) and D-Link Green Technologies. It allows significant power saving during periods of low data activity. In most of use cases and environments, switches are idle in 90% or more of time. While no traffic in a short period of time, ports on DGS-1100 switch get into power saving mode automatically. Once if a packet is received, the switch wakes and works immediately. Connecting to EEE compliant devices, such as PCs and servers, the network can save energy without compromising any performance. While connecting to legacy devices which do not support IEEE 802.3az, D-Link Green Technologies can reduce power consumption by changing the power state of the link.

DGS-1100-16V2

16-Port 10/100/1000Mpbs Switch

Front Panel

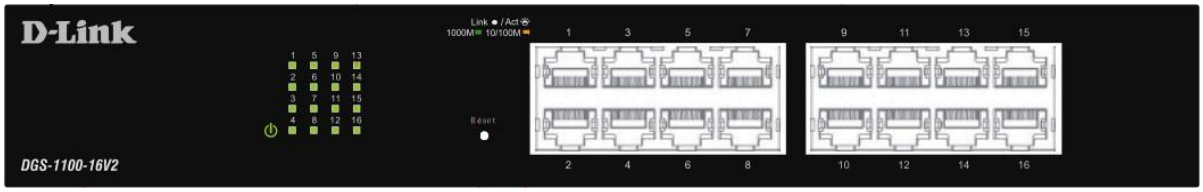


Figure 2-1- DGS-1100-16V2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Link/Act/Speed LED (Ports 1-16):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel

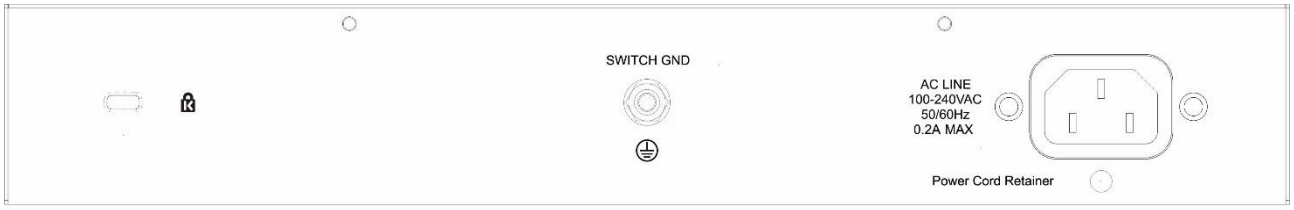


Figure 2-2 – DGS-1100-16V2 Rear Panel

Power: The power port is where to connect the AC power cord.

DGS-1100-24V2

24-Port 10/100/1000Mpbs Switch

Front Panel

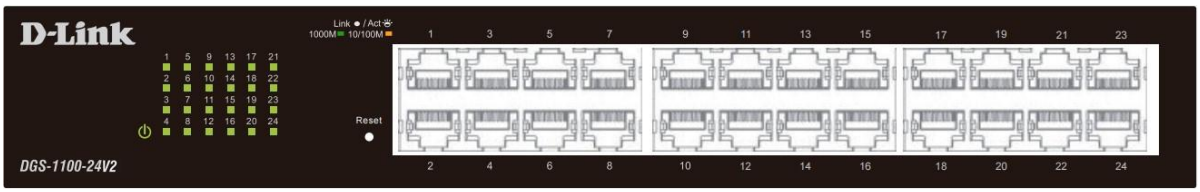


Figure 2-3 – DGS-1100-24V2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Link/Act/Speed LED (Ports 1-24):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel

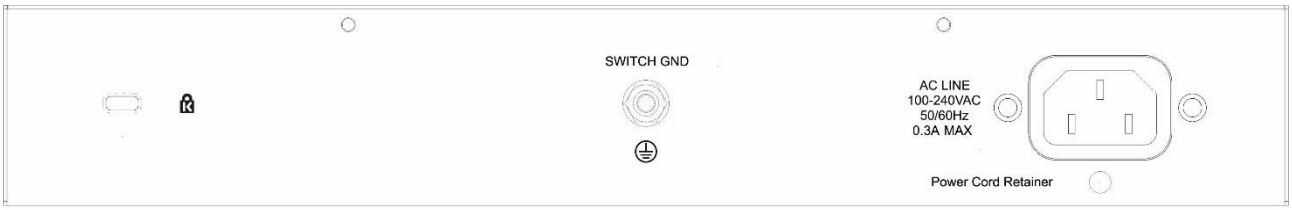


Figure 2-4– DGS-1100-24V2 Rear Panel

Power: Connect the supplied AC power cable to this port.

DGS-1100-24PV2

24-Port 10/100/1000Mpbs PoE Switch

Front Panel

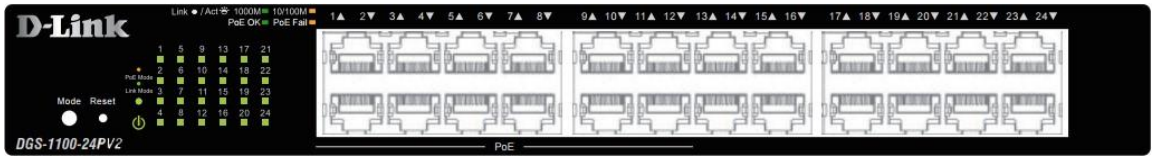


Figure 2-5 – DGS-1100-24PV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode
- PoE Mode

Link/Act/Speed LED (Ports 1-24):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-12):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-12 will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 12 PoE power budget is 30 watts/port. Total PoE Power budget is 100 watts.

Rear Panel

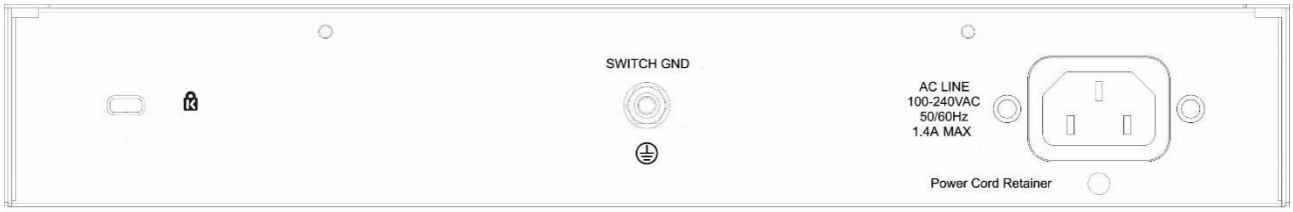


Figure 2-6– DGS-1100-24PV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

DGS-1100-10MPV2

8 x 10/100/1000 Mbps PoE + 2 x 100/1000 Mbps SFP Switch

Front Panel

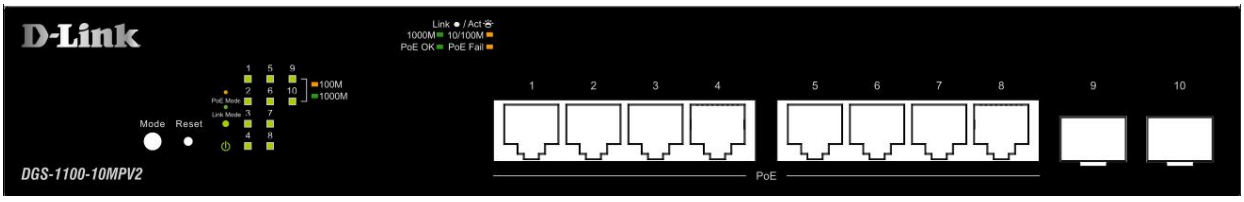


Figure 2-7 – DGS-1100-10MPV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode

- PoE Mode

Link/Act/Speed LED (Ports 1-10):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-8):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-8 will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 8 PoE power budget is 30 watts/port. Total PoE Power budget is 130 watts.

Rear Panel

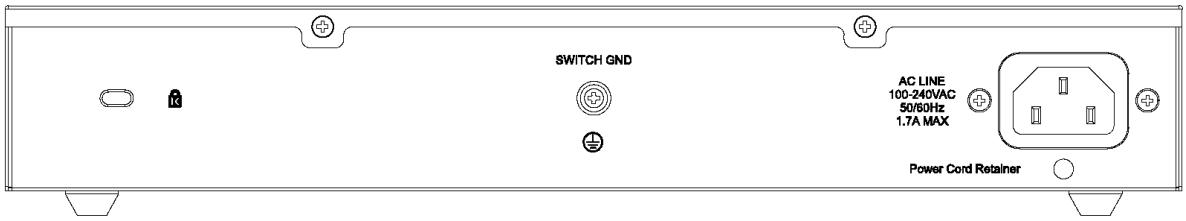


Figure 2-8– DGS-1100-10MPV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

DGS-1100-10MPPV2

8 x 10/100/1000 Mbps PoE + 2 x 100/1000 Mbps SFP Switch

Front Panel

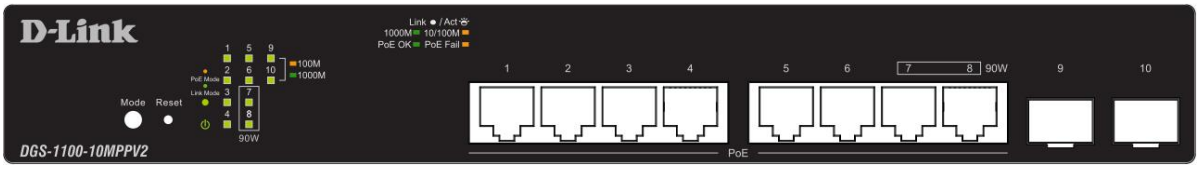


Figure 2-9 – DGS-1100-10MPPV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode
- PoE Mode

Link/Act/Speed LED (Ports 1-10):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-8):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-8 will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 6 PoE power budget is 30 watts/port. Port 7 ~ Port 8 PoE power budget is 90 watts/port. Total PoE Power budget is 242 watts.

Rear Panel

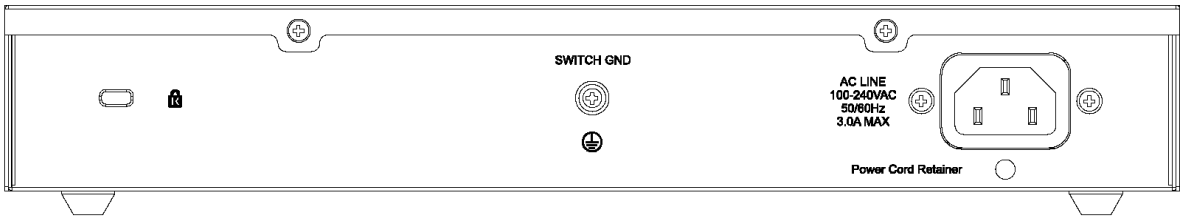


Figure 2-10– DGS-1100-10MPPV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

DGS-1100-26MPV2

24 x 10/100/1000 Mbps PoE + 2 x 100/1000 BASE-T/SFP Combo Switch

Front Panel

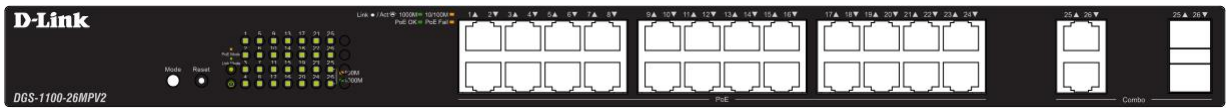


Figure 2-11 – DGS-1100-26MPV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode

- PoE Mode

Link/Act/Speed LED (Ports 1-26):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-24):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-24will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 24 PoE power budget is 30 watts/port. Total PoE Power budget is 370 watts.

Rear Panel

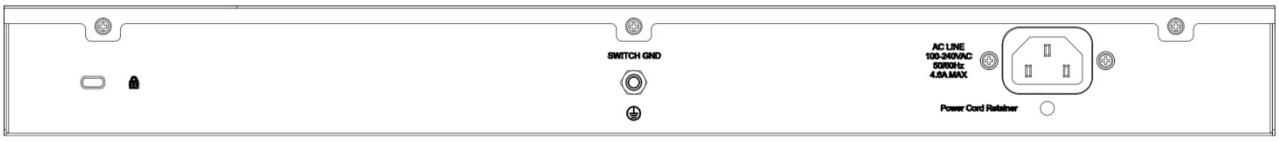


Figure 2-12– DGS-1100-26MPV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

DGS-1100-26MPPV2

24 x 10/100/1000 Mbps PoE + 2 x 100/1000 BASE-T/SFP Combo Switch

Front Panel

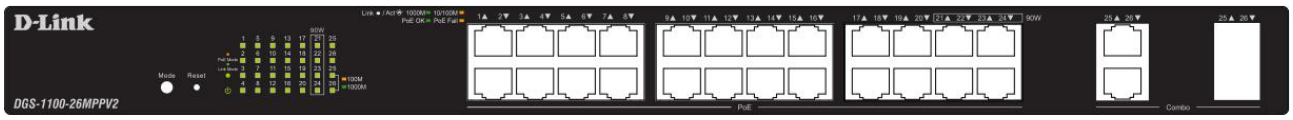


Figure 2-13 – DGS-1100-26MPPV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode

- PoE Mode

Link/Act/Speed LED (Ports 1-26):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-24):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-24will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 20 PoE power budget is 30 watts/port. Port 21 ~ Port 24 PoE power budget is 90 watts/port. Total PoE Power budget is 525 watts.

Rear Panel

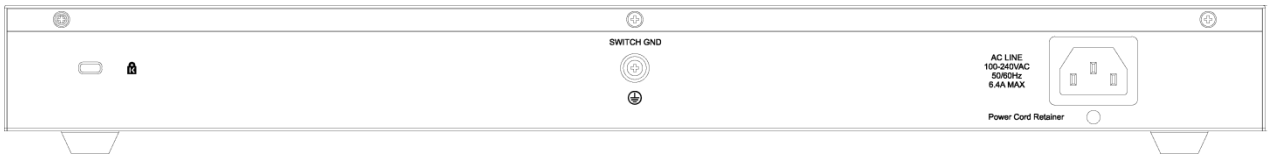


Figure 2-14– DGS-1100-26MPPV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

DGS-1100-18PV2

16*10/100/1000M PoE + 2 x 100/1000 BASE-T/SFP Combo Switch

Front Panel

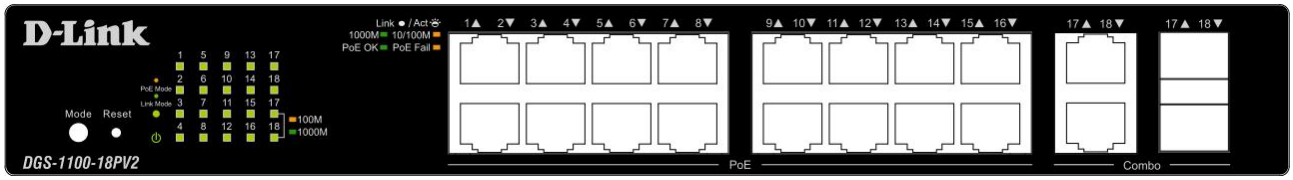


Figure 2-15 – DGS-1100-18PV2 Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Port LED Indicator(For PoE Model):

A LED select button to switch two modes in turn for all 10/100/1000Mbps ports:

- Link/Act/Speed Mode

- PoE Mode

Link/Act/Speed LED (Ports 1-18):

Solid Green: When there is a secure 1000Mbps connection at the port.

Blinking Green or Amber: When there is reception or transmission occurring at the port.

Solid Amber: When there is a secure 10/100Mbps connection at the port.

Light off: No link.

PoE Mode (Ports 1-16):

Green: PD device insert and power feeding.

Amber: PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.)

Light off: No PD device insert.

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE mode.

Reset: By pressing the Reset button until the all port LED turns amber, the Switch will change back to the default configuration and all changes will be lost.

Note: The LED behavior for ports 1-16will switch between Link mode and PoE mode when the PoE mode is active. Port 1 ~ Port 16 PoE power budget is 30 watts/port. Total PoE Power budget is 130 watts.

Rear Panel

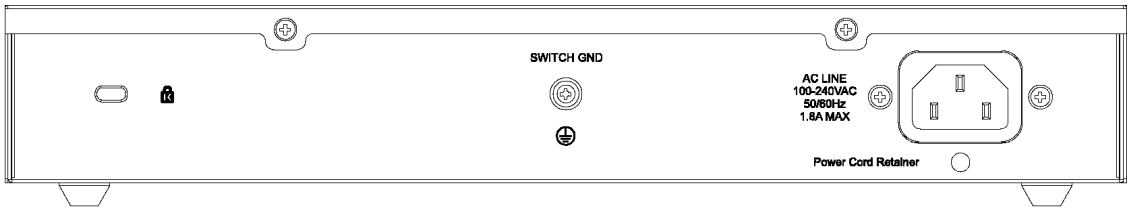


Figure 2-16– DGS-1100-18PV2 Rear Panel

Power: Connect the supplied AC power cable to this port.

CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

3. Hardware Installation

This chapter provides unpacking and installation information for the D-Link Switch.

Step1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for replacement.

Packing contents of DGS-1100-16V2 /24V2 /24PV2/10MPV2/10MPPV2/26MPV2/26MPPV2/18PV2

- One D-Link DGS-1100 Series Switch
- AC power cord
- Four rubber feet
- Screws and two mounting brackets
- One accessory kit for a ground screw
- One Getting Started Guide

If any item is found missing or damaged, please contact the local reseller for replacement.

Step2: Switch Installation

For safe switch installation and operation, it is recommended that you:

- Visually inspect the power cord to see that it is secured fully to the AC power connector.
- Make sure that there is proper heat dissipation and adequate ventilation around the switch.
- Do not place heavy objects on the switch.

Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

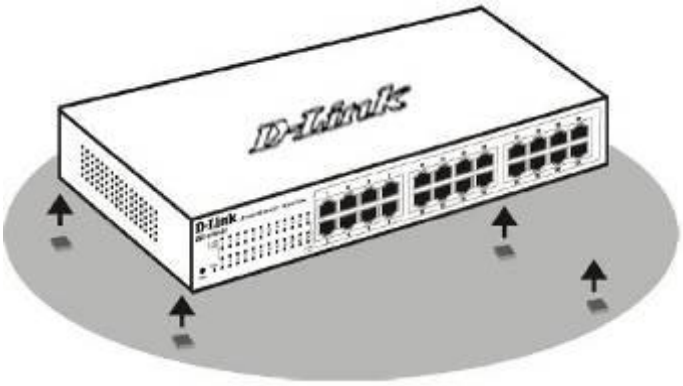


Figure 3-1 – Attach the adhesive rubber pads to the bottom

Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches).

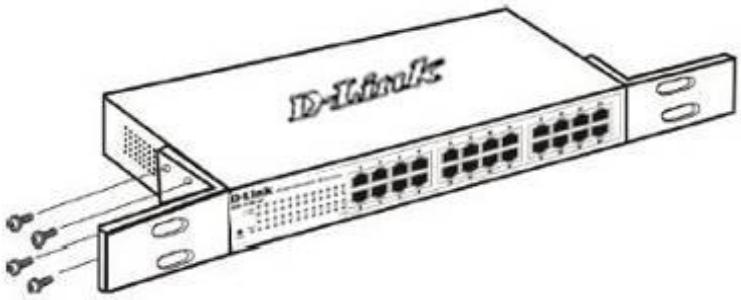


Figure 3-2 – Attach the mounting brackets to the Switch

Then, use the screws provided with the equipment rack to mount the switch in the rack.

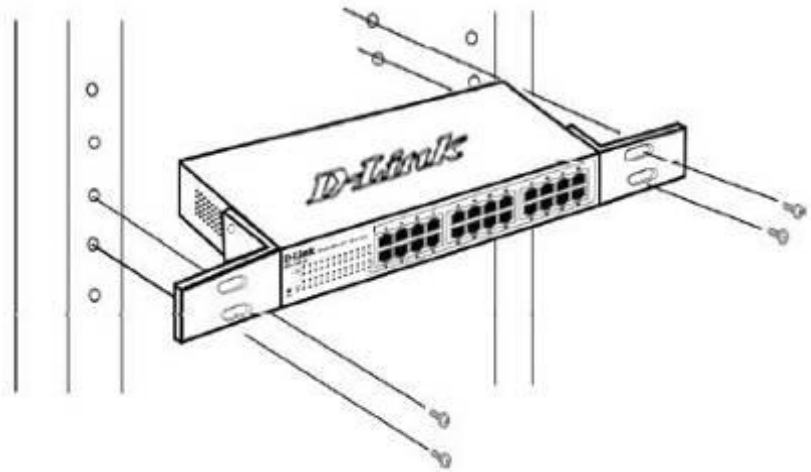


Figure 3-3– Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Step 3 – Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

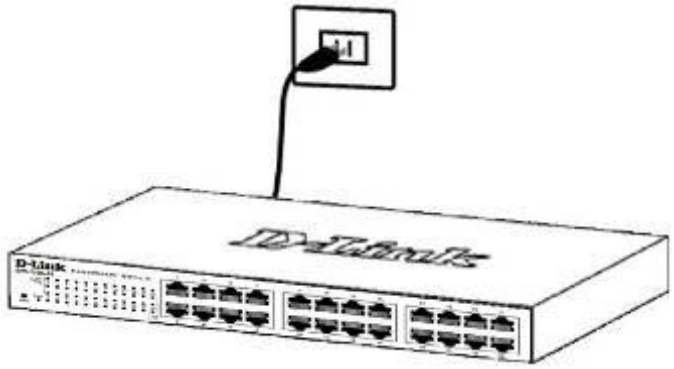


Figure 3-4 – Plugging the switch into an outlet

Power Failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

Grounding the Switch

This section describes how to connect the DGS-1100 Series Switch to ground. You must complete this procedure before powering your switch.

Required Tools and Equipment

- Ground screws (included in the accessory kit): One M4 x 6 mm (metric) pan-head screw
- Ground cable (not included in the accessory kit): The grounding cable should be sized according to local and national installation requirements. Depending on the power supply and system, a 12 to 6 AWG copper conductor is required for U.S installation. Commercially available 6 AWG wire is recommended. The length of the cable depends on the proximity of the switch to proper grounding facilities.
- A screwdriver (not included in the accessory kit)

The following steps let you connect the switch to a protective ground:

Step 1: Verify if the system power is off.

Step 2: Use the ground cable to place the #8 terminal lug ring on top of the ground-screw opening, as seen in the figure below.

Step 3: Insert the ground screw into the ground-screw opening.

Step 4: Using a screwdriver, tighten the ground screw to secure the ground cable to the switch.

Step 5: Attach the terminal lug ring at the other end of the grounding cable to an appropriate grounding stud or bolt on rack where the switch is installed.

Step 6: Verify if the connections at the ground connector on the switch and the rack are securely attached.

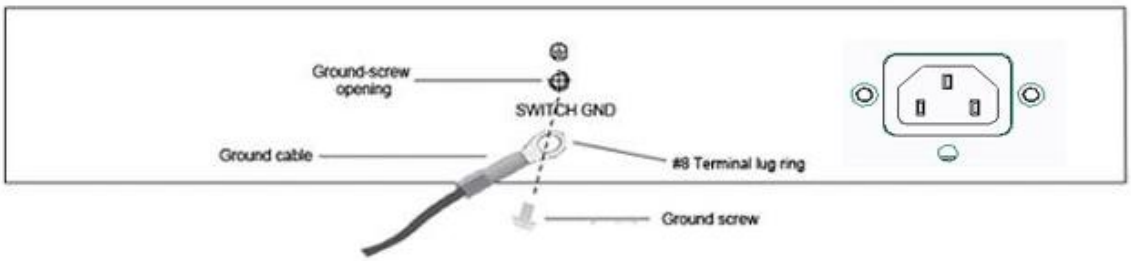


Figure 3-5 – Ground cable, screw and #8 terminal lug rings

4. Web-based Switch Configuration

Management Options
Connecting using the Web User Interface
Logging onto the Web Manager
Smart Wizard
Web User Interface (Web UI)

Management Options

The Switch provides multiple access platforms that can be used to configure, manage and monitor networking features available on the Switch. Currently there are three management platforms available and they are described below.

Web-based Management Interface

After successfully installing the Switch, the user can configure the Switch, and display statistics graphically using a Web browser, such as Microsoft® Internet Explorer, Opera Firefox, Safari, or Google Chrome.

SNMP-based Management

The Switch can be managed with an SNMP-compatible console program. The Switch supports SNMP version 1.0, and version 2c. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

D-Link Network Assistant

DNA (D-Link Network Assistant) is a program for discovering DGS-1100 Series Switches with the same L2 network segment connected to your PC.

Connecting using the Web User Interface

Most software functions of the DGS-1100 Series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard web browser. The web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP or HTTPS protocol.

You need the following equipment to begin the web configuration of your device:

- A PC with a RJ-45 Ethernet connection
- A standard Ethernet cable

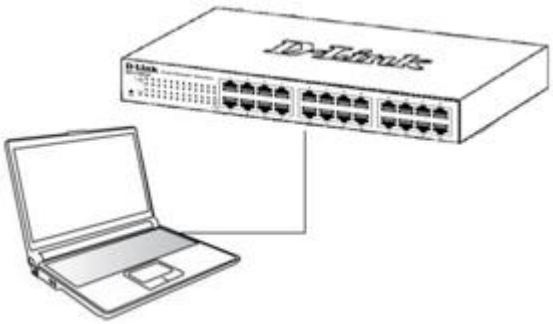


Figure 4-1 Connecting to a DGS-1100 Series Switch

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

Logging onto the Web Manager

To access the Web User Interface, simply open a standard web browser on the management PC and enter the Switch's default IP address into the address bar of the browser and press the **Enter** key.

NOTE: The default IP address of this switch is **10.90.90.90**, with a subnet mask of **255.255.255.0**.

Figure 4-2 Display entering the IP address in Internet Explorer

This will open the user authentication window, as seen below.

Figure 4-3 User Authentication window

By default, the username is "**admin"** and the password is also "**admin**". Click the **Login** button.

Smart Wizard

After a successfully connecting to the Web User Interface for the first time, the Smart Wizard embedded Web utility will be launched. This wizard will guide the user through basic configuration steps that is essential for first time connection to the Switch.

Step 1 – System IP Information

In this window, the user can configure the IP address assignment method, the static IP address, Netmask and Gateway address.

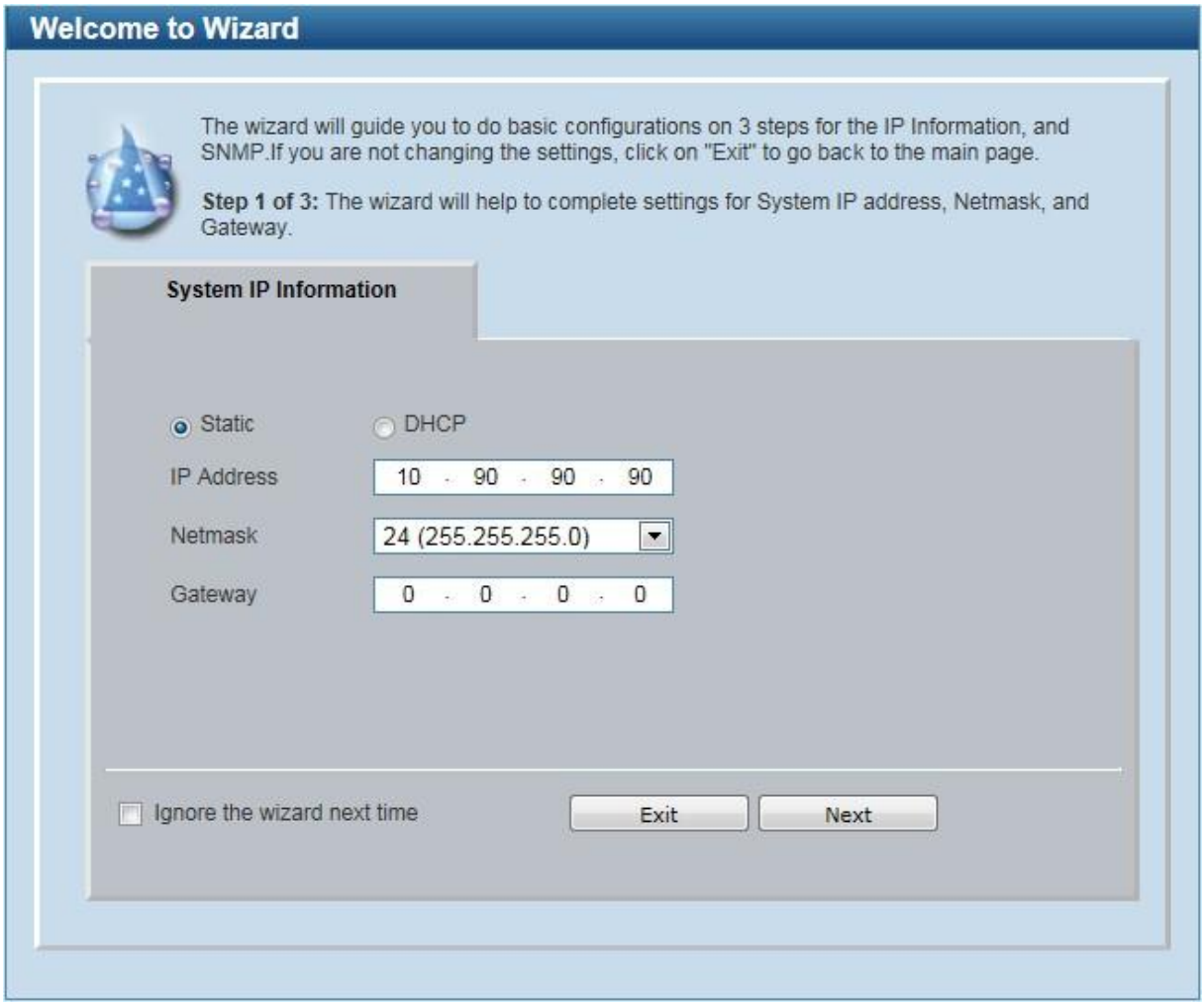


Figure 4-4 System IP Information window

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually configure and use IP address settings on this switch.
DHCP	Select this option to obtain IP address settings from a DHCP server.
IP Address	Enter the IP address of the Switch here.
Netmask	Select the Netmask option here.
Gateway	Enter the default gateway IP address here.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 2 – Admin Password

In this window, the user can set the password used with the admin account.

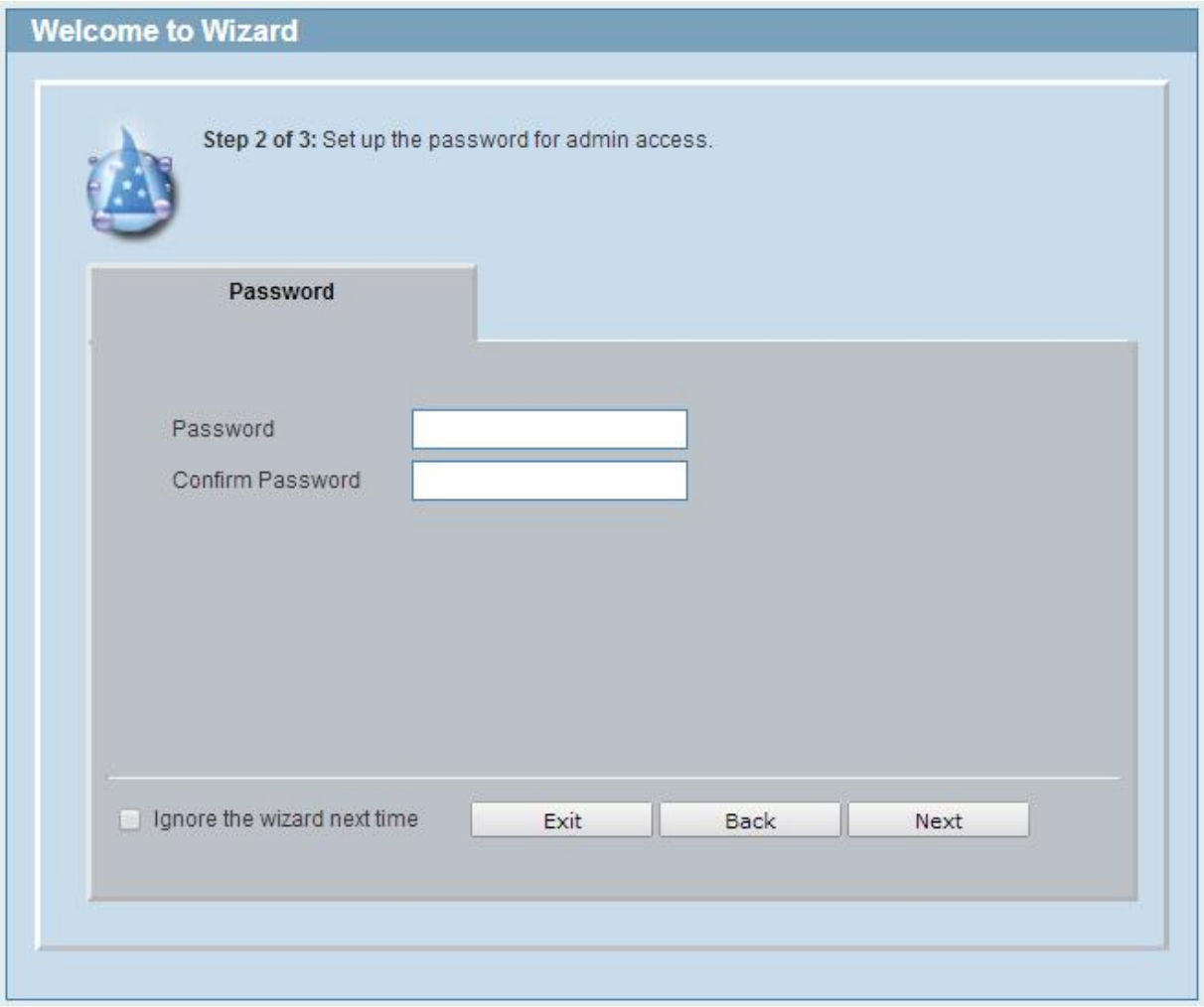


Figure 4-5 Admin Password

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 3 – SNMP Settings

In this window, the user can enable or disable the SNMP function.

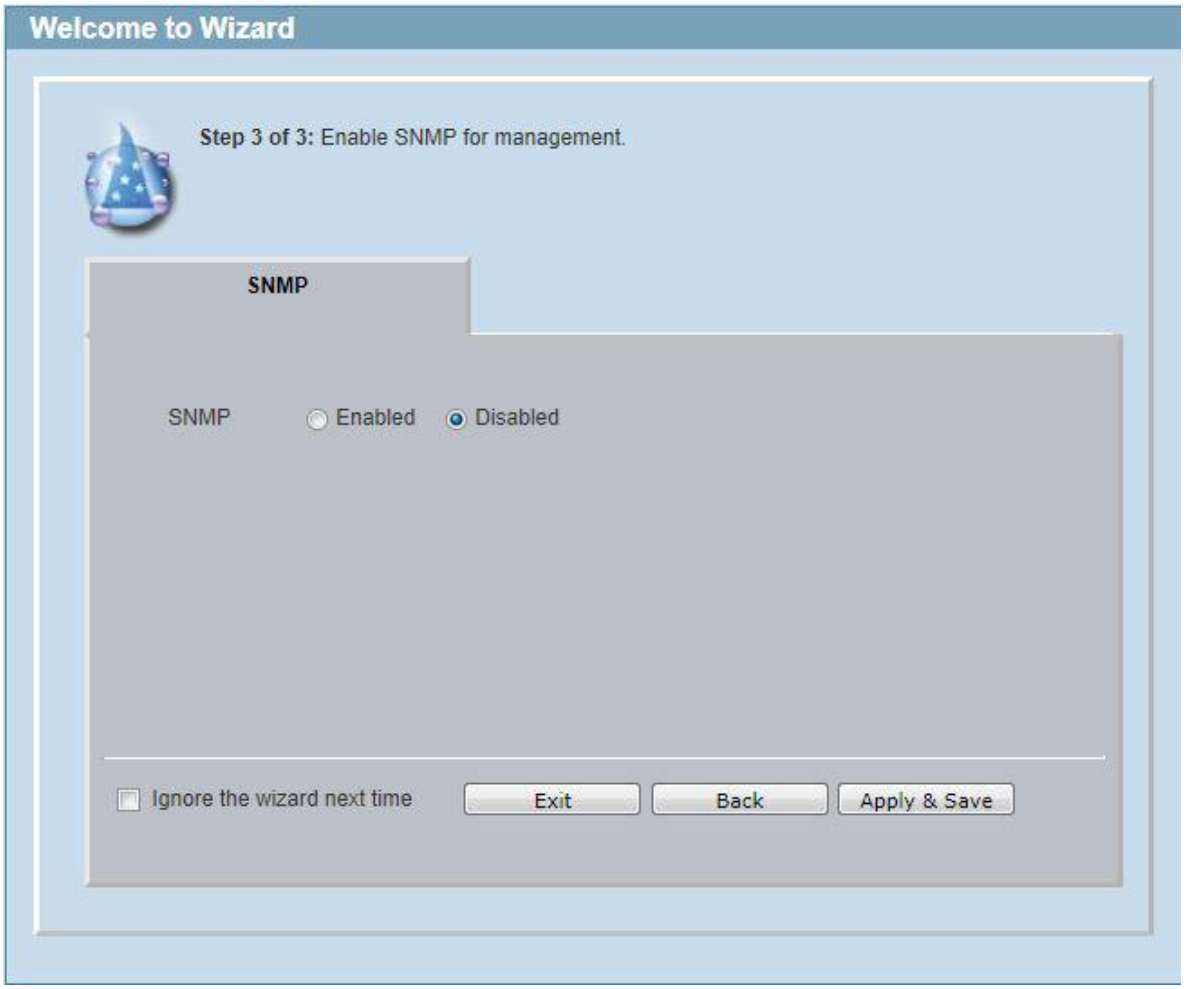


Figure 4-6 SNMP window

The fields that can be configured are described below:

Parameter	Description
SNMP	Select the **Enabled** option to enable the SNMP function. Select the **Disabled** option to disable the SNMP function.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Apply & Save** button to accept the changes made, and then continue to the Web UI.

Web User Interface (Web UI)

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas that divide the user interface, as described in the table.

Figure 4-7 Main Web UI window

Area Number	Description
AREA 1	In this area, a folder tree layout is displayed of functions that can be configured using the Web UI. Open folders and click the hyperlinked menu buttons to access each individual page for configuration. The **DGS-1100-24V2** link is the default page that will display basic monitoring settings for this switch.
AREA 2	In this area, the Switch's configuration page can be found, based on the selection made in **Area** 1.

5. System

Device Information
System Information Settings
Port Configuration
PoE (PoE Model Only)
System Log
Time
Time Range

Device Information

In this window, the Device Information is displayed. It appears automatically when you log in the Switch. To return to the Device Information window after viewing other windows, click the **DGS-1100-24V2** link.

Figure 5-1 Device Information window

System Information Settings

System Information

The user can enter a System Name, System Location, and System Contact to aid in defining the Switch.

To view the following window, click **System > System Information Settings>System Information**, as shown below:

Figure 5-2 System Information Settings window

The fields that can be configured are described below:

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

Click the **Apply** button to accept the changes made.

IPv4 Interface

This window is used to configure the IPv4 settings of the switch.

To view the following window, click **System > System Information Settings > IPv4 Interface**, as shown below:

Figure 5-3 Peripheral Settings window

The fields that can be configured are described below:

Parameter	Description
Get IP From	Select DHCP to automatically obtain an IP address. Select Static to manually configure the IP address settings.
IP Address	If Static is selected, enter the IP address of the switch. If DHCP is selected, the automatically obtained IP address will be displayed.
Mask	If Static is selected, enter the IP address of the switch. If DHCP is selected, the automatically obtained network mask will be displayed.
Gateway	If Static is selected, enter the IP address of the switch. If DHCP is

	selected, the automatically obtained gateway will be displayed.
DHCP retry Time	If DHCP is selected, enter the number of times to retry obtaining an IP address.

Click the **Apply** button to accept the changes made.

IPv6 Interface

This window is used to configure the IPv6 settings of the switch.

To view the following window, click **System > System Information Settings > IPv6 Interface**, as shown below:

Figure 5-4 Peripheral Settings window

The fields that can be configured are described below:

Parameter	Description
IPv6 State	Select whether to **Enable** or **Disable** IPv6 functionality.
Static IPv6 Address	If enabled, enter the static IPv6 address of the switch.

Click the **Apply** button to accept the changes made.

Port Configuration

Port Settings(DGS-1100-16V2/24V2/24PV2/10MPV2/10MPPV2 Only)

This window is used to view and configure the Switch's port settings.

To view the following window, click **System > Port Configuration > Port Settings**, as shown below:

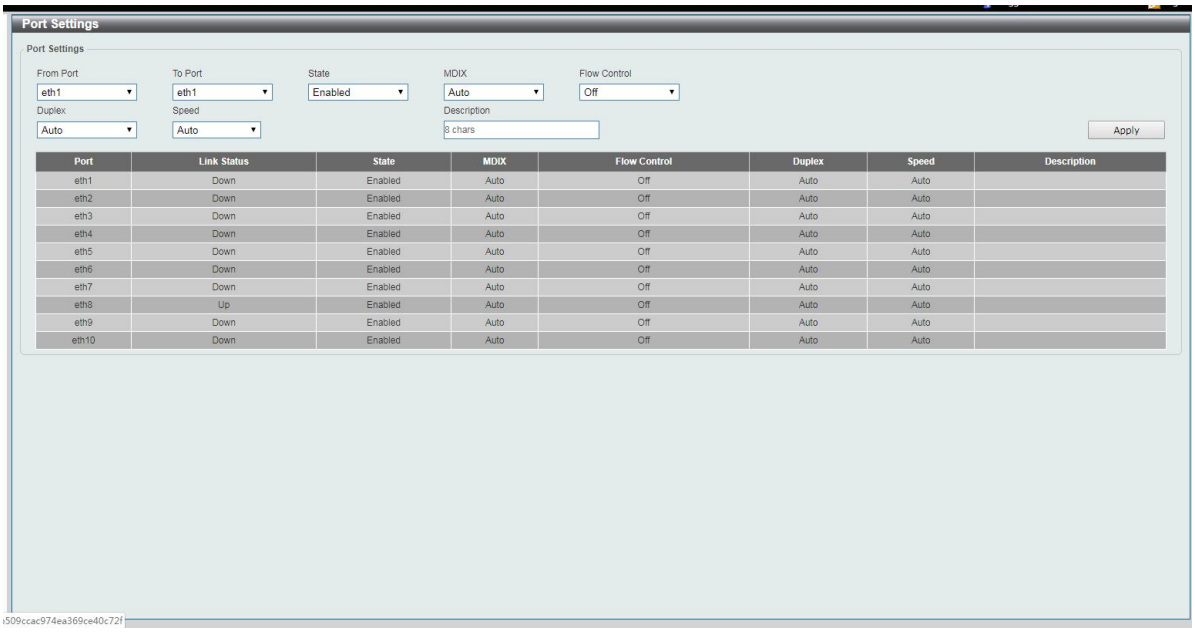


Figure 5- 5 Port Settings window

The fields that can be configured are described below:

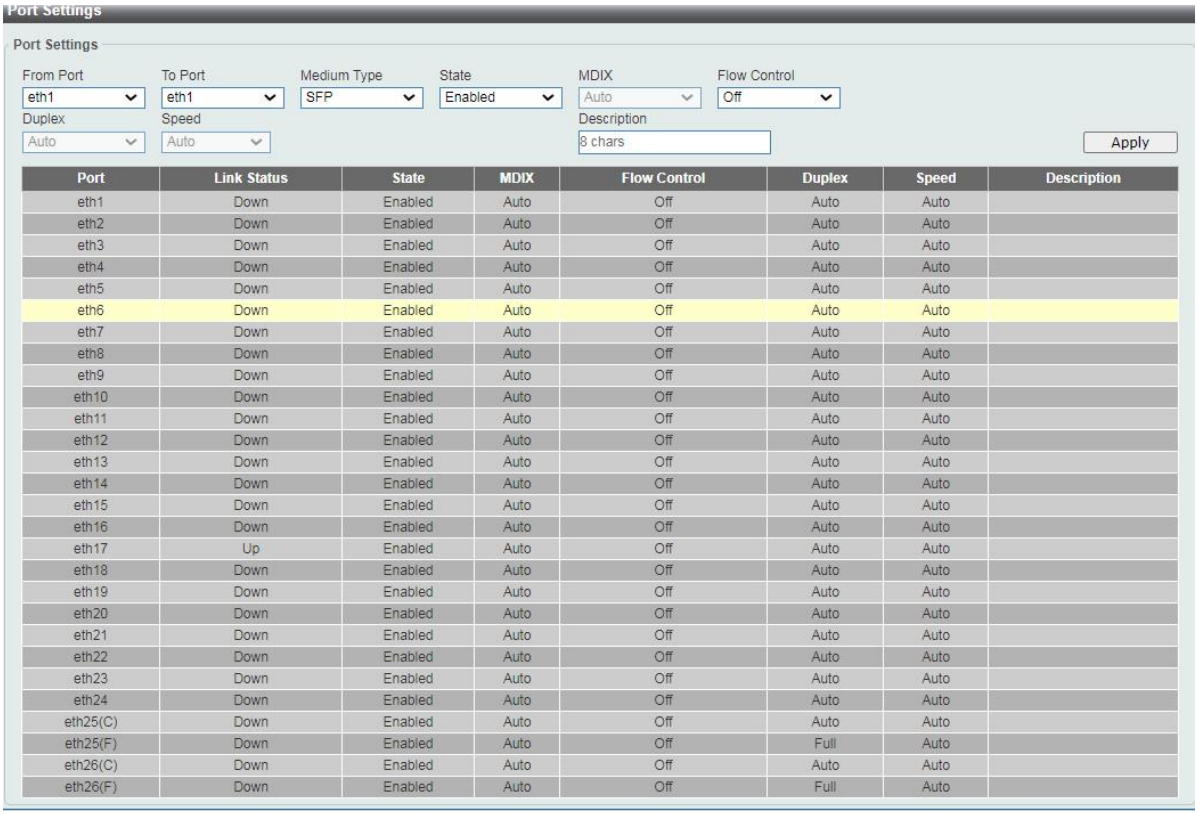
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to **enable** or **disable** the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are **Auto**, **Normal**, and **Cross**. **Auto** - Select this option for auto-sensing of the optimal type of cabling. **Normal** - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable. **Cross** - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a straight cable.
Flow Control	Select to either turn flow control **On** or **Off** here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are **Auto**, **Half**, and **Full**.
Speed	Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are **Auto**, **10M**, **100M**. 1000M speed is only available when **Auto** is selected.
Description	Enter an 8 characters description for the corresponding port here.

Click the **Apply** button to accept the changes made.

Port Settings(DGS-1100-26MPV2/26MPPV2/18PV2 Only)

This window is used to view and configure the Switch's port settings.

To view the following window, click **System > Port Configuration > Port Settings**, as shown below:



Port	Link Status	State	MDIX	Flow Control	Duplex	Speed	Description
eth1	Down	Enabled	Auto	Off	Auto	Auto	
eth2	Down	Enabled	Auto	Off	Auto	Auto	
eth3	Down	Enabled	Auto	Off	Auto	Auto	
eth4	Down	Enabled	Auto	Off	Auto	Auto	
eth5	Down	Enabled	Auto	Off	Auto	Auto	
eth6	Down	Enabled	Auto	Off	Auto	Auto	
eth7	Down	Enabled	Auto	Off	Auto	Auto	
eth8	Down	Enabled	Auto	Off	Auto	Auto	
eth9	Down	Enabled	Auto	Off	Auto	Auto	
eth10	Down	Enabled	Auto	Off	Auto	Auto	
eth11	Down	Enabled	Auto	Off	Auto	Auto	
eth12	Down	Enabled	Auto	Off	Auto	Auto	
eth13	Down	Enabled	Auto	Off	Auto	Auto	
eth14	Down	Enabled	Auto	Off	Auto	Auto	
eth15	Down	Enabled	Auto	Off	Auto	Auto	
eth16	Down	Enabled	Auto	Off	Auto	Auto	
eth17	Up	Enabled	Auto	Off	Auto	Auto	
eth18	Down	Enabled	Auto	Off	Auto	Auto	
eth19	Down	Enabled	Auto	Off	Auto	Auto	
eth20	Down	Enabled	Auto	Off	Auto	Auto	
eth21	Down	Enabled	Auto	Off	Auto	Auto	
eth22	Down	Enabled	Auto	Off	Auto	Auto	
eth23	Down	Enabled	Auto	Off	Auto	Auto	
eth24	Down	Enabled	Auto	Off	Auto	Auto	
eth25(C)	Down	Enabled	Auto	Off	Auto	Auto	
eth25(F)	Down	Enabled	Auto	Off	Full	Auto	
eth26(C)	Down	Enabled	Auto	Off	Auto	Auto	
eth26(F)	Down	Enabled	Auto	Off	Full	Auto	

Figure 5- 6 Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Media Type	Select the port media type here. Options to choose from are **Auto**, **RJ45**, and **SFP**. Selecting the **SFP** option includes the use of SFP+ transceivers for 10G connectivity.
State	Select this option to **enable** or **disable** the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are **Auto**, **Normal**, and **Cross**. **Auto** - Select this option for auto-sensing of the optimal type of cabling. **Normal** - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable. **Cross** - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to

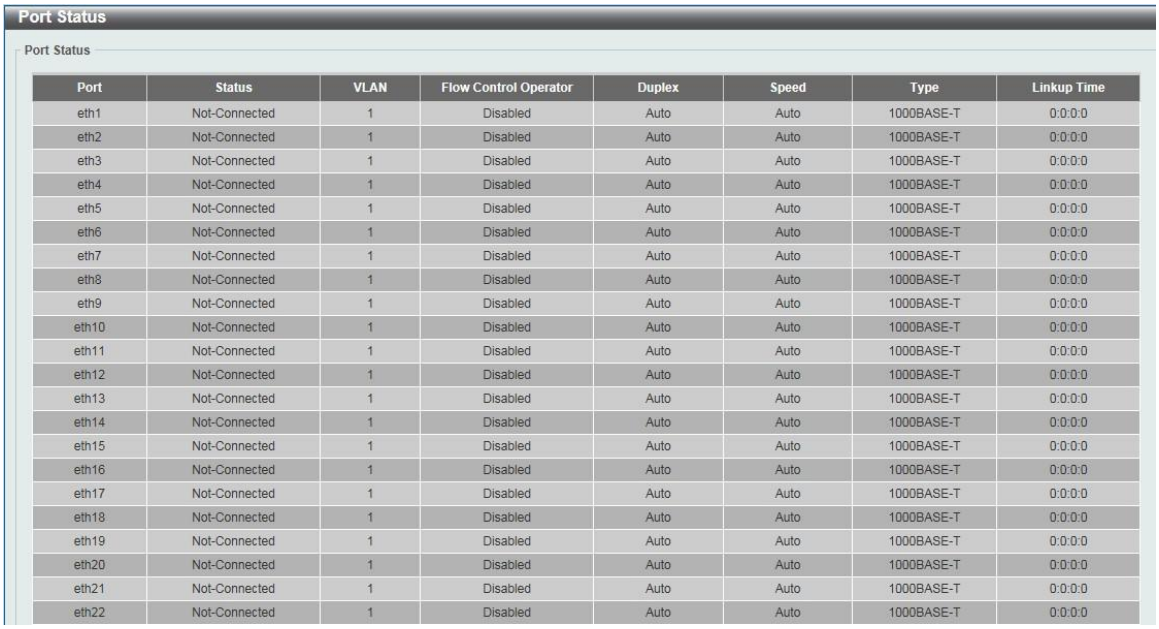
	a port (in the MDIX mode) on another switch through a straight cable.
Flow Control	Select to either turn flow control **On** or **Off** here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are **Auto**, **Half**, and **Full**.
Speed	Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are **Auto**, **10M**, **100M**. 1000M speed is only available when **Auto** is selected.
Description	Enter an 8 characters description for the corresponding port here.

Click the **Apply** button to accept the changes made.

Port Status(DGS-1100-16V2/24V2/24PV2/10MPV2/10MPPV2 Only)

This window is used to view the Switch's port status.

To view the following window, click **System > Port Configuration > Port Status**, as shown below:



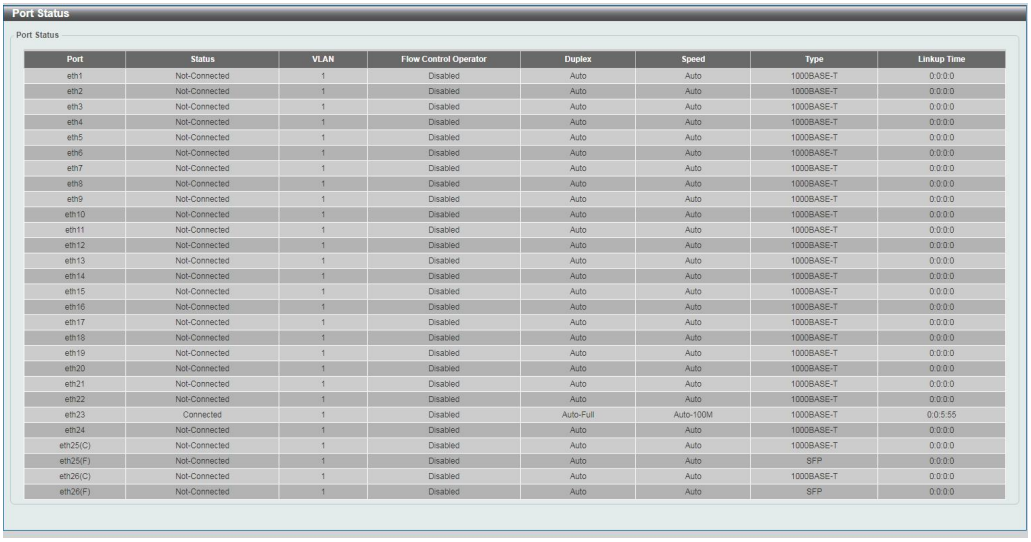
Port	Status	VLAN	Flow Control Operator	Duplex	Speed	Type	Linkup Time
eth1	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth2	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth3	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth4	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth5	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth6	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth7	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth8	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth9	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth10	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth11	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth12	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth13	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth14	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth15	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth16	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth17	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth18	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth19	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth20	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth21	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth22	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0

Figure 5-7 Port Status window

Port Status(DGS-1100-26MPV2/26MPPV2/18PV2 Only)

This window is used to view the Switch's port status.

To view the following window, click **System > Port Configuration > Port Status**, as shown below:



Port	Status	VLAN	Flow Control Operator	Duplex	Speed	Type	Linkup Time
eth1	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth2	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth3	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth4	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth5	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth6	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth7	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth8	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth9	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth10	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth11	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth12	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth13	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth14	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth15	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth16	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth17	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth18	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth19	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth20	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth21	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth22	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth23	Connected	1	Disabled	Auto-Full	Auto-100M	1000BASE-T	0:0:5:55
eth24	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth25(C)	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth25(F)	Not-Connected	1	Disabled	Auto	Auto	SFP	0:0:0:0
eth26(C)	Not-Connected	1	Disabled	Auto	Auto	1000BASE-T	0:0:0:0
eth26(F)	Not-Connected	1	Disabled	Auto	Auto	SFP	0:0:0:0

Figure 5-8 Port Status window

Jumbo Frame

This window is used to view and configure the Jumbo Frame settings. The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 10240 bytes.

To view the following window, click **System > Port Configuration > Jumbo Frame**, as shown below:

Figure 5-9 Jumbo Frame window

The fields that can be configured are described below:

Parameter	Description
Frame State	Select whether to **Enable** or **Disable** support for Jumbo Frames on the switch.

Click the **Apply** button to accept the changes made.

PoE (PoE Model Only)

The DGS-1100 PoE Model switch supports Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at.DGS-1100 MPP series also support the IEEE 802.3bt standard.

The ports and power ratings per switch are as follows:

Switch Model	Port Numbers	Power Rating
DGS-1100-10MPV2	1-8	30W
DGS-1100-10MPPV2	1-8 7-8	30W 90W
DGS-1100-26MPV2	1-24	30W
DGS-1100-26MPPV2	1-24 21-24	30W 90W
DGS-1100-24PV2	1-12	30W
DGS-1100-18PV2	1-16	30W

Ports can be supplied at 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The Switches work with all D-Link 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD (Powered Device) and automatically sends power to it.
- The Auto-disable feature occurs under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Based on 802.3af/at PDs receive power according to the following classification:

Class	Maximum power used by PD
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	25.5W

PSE provides power according to the following classification:

Class	Max power supplied by PSE
0	16.2W
1	4.2W
2	7.4W
3	16.2W
4	31.6W

PoE System

This window is used to configure the PoE system and display the detailed power information and PoE Trap parameters for PoE modules.

To view the following window, click **System > PoE > PoE System**, as shown below:

Figure 5-10 PoE System window

The fields that can be configured are described below:

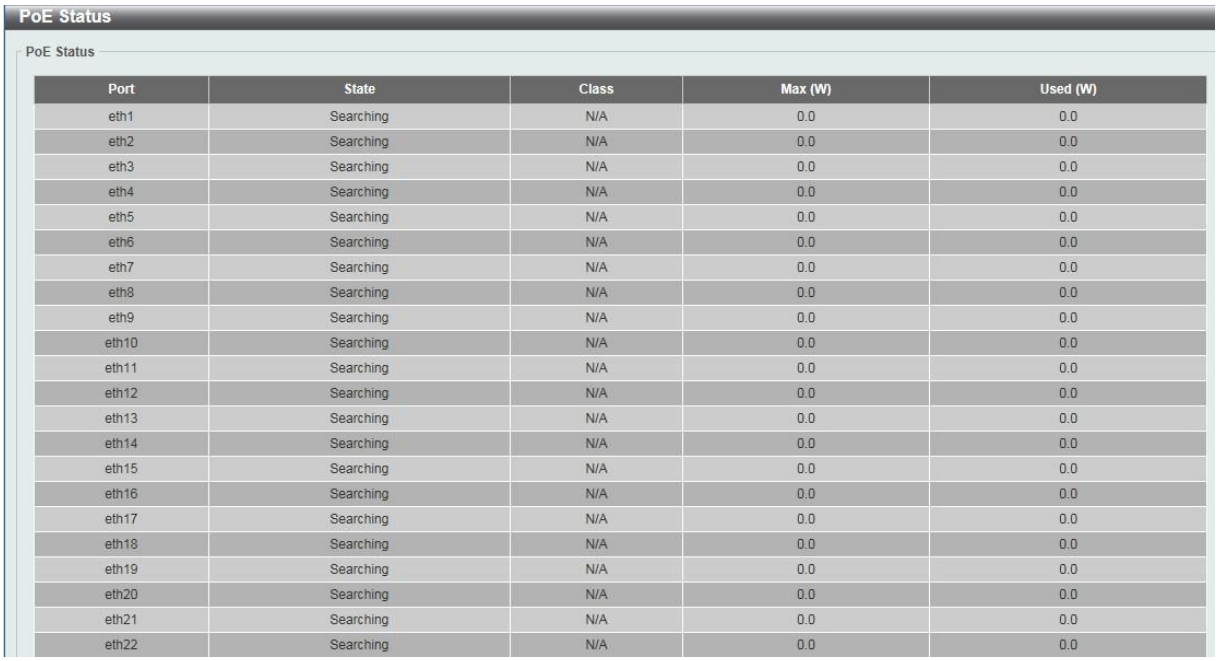
Parameter	Description
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification.
Trap State	Select this option to enable or disable the sending of PoE notifications.

Click the **Apply** button to accept the changes made.

PoE Status

This window displays the PoE status of each port.

To view the following window, click **System > PoE > PoE Status**, as shown below:



PoE Status

Port	State	Class	Max (W)	Used (W)
eth1	Searching	N/A	0.0	0.0
eth2	Searching	N/A	0.0	0.0
eth3	Searching	N/A	0.0	0.0
eth4	Searching	N/A	0.0	0.0
eth5	Searching	N/A	0.0	0.0
eth6	Searching	N/A	0.0	0.0
eth7	Searching	N/A	0.0	0.0
eth8	Searching	N/A	0.0	0.0
eth9	Searching	N/A	0.0	0.0
eth10	Searching	N/A	0.0	0.0
eth11	Searching	N/A	0.0	0.0
eth12	Searching	N/A	0.0	0.0
eth13	Searching	N/A	0.0	0.0
eth14	Searching	N/A	0.0	0.0
eth15	Searching	N/A	0.0	0.0
eth16	Searching	N/A	0.0	0.0
eth17	Searching	N/A	0.0	0.0
eth18	Searching	N/A	0.0	0.0
eth19	Searching	N/A	0.0	0.0
eth20	Searching	N/A	0.0	0.0
eth21	Searching	N/A	0.0	0.0
eth22	Searching	N/A	0.0	0.0

Figure 5-11 PoE Status window

Note: For the PoE Status table, if the classification was shown as “Legacy PD”, it will be classified to non-AF PD or Legacy PD.

PoE Configuration(DGS-1100-24PV2/10MPV2/26MPV2/18PV2 Only)

This window is used to configure the PoE port.

To view the following window, click **System > PoE > PoE Configuration**, as shown below:

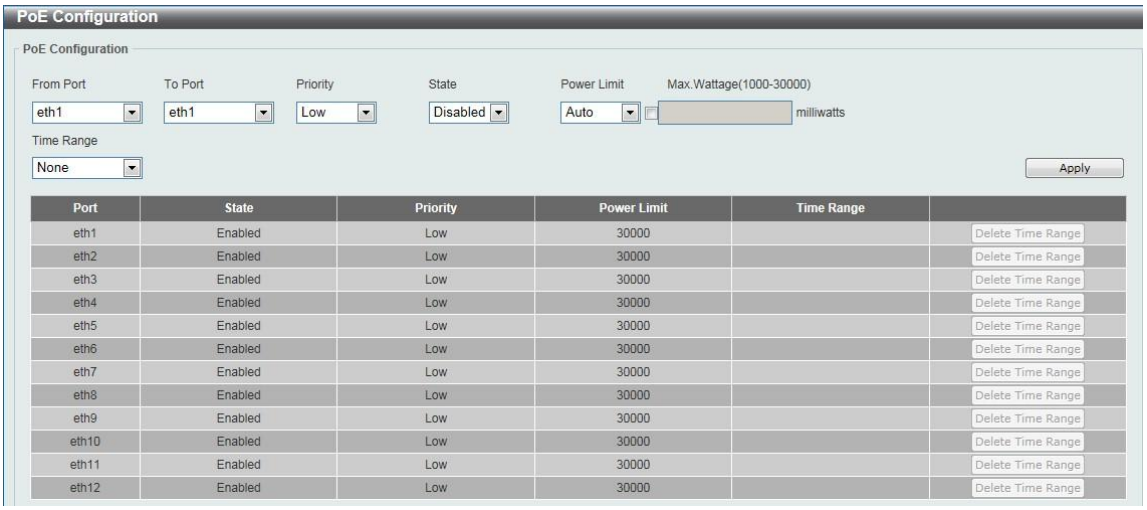


Figure 5-12 PoE Configuration window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are **Critical**, **High** and **Low**.
State	Select this option to enable or disable the PoE functionality.
Power Limit	Select the power management mode for the PoE ports. Options to choose from are **Auto, Class 1, Class 2, Class 3, and Class 4**.
Max Wattage	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	Select the **Time Range** from the drop-down list. **Note**: The **Time Range** drop down menu will only have available options if a time profile has been created.

Click the **Delete Time Range** button to clear the setting in the corresponding Time Range field.

Click the **Apply** button to accept the changes made.

Note: The **Max Wattage** option will only be available if the check box next to the input field is enabled. When enabled, the Power Limit drop down menu will not be available.

Note: If the switch failed to supply power to the IEEE 802.3at PD (Powered Device),

1.Check if the PD connected to the port supports the IEEE 802.3at standard.

2.Manually configure the corresponding port's power limit value to 30 Watts.

PoE Configuration(DGS-1100-10MPPV2/26MPPV2 Only)

This window is used to configure the PoE port.

To view the following window, click **System > PoE > PoE Configuration**, as shown below:

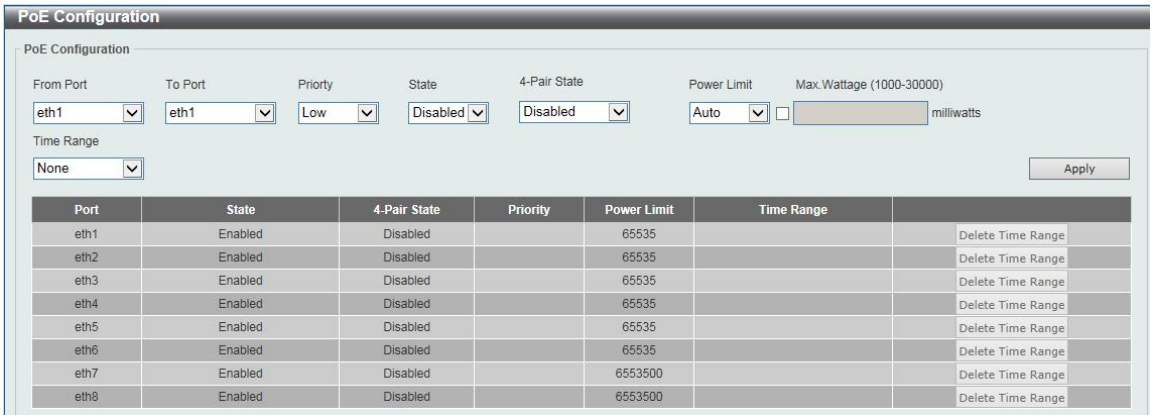


Figure 5-13 PoE Configuration window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are **Critical**, **High** and **Low**.
State	Select this option to enable or disable the PoE functionality.
4-Pair State	Select the power management mode for the PoE ports. Options to choose from are **Disable, 60W Enabled, 90W Enabled**.
Power Limit	Select the power management mode for the PoE ports. Options to choose from are **Auto, Class 1, Class 2, Class 3, and Class 4**. (When 4-Pair State is enabled, Power Limit is Auto always.)
Max Wattage	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	Select the **Time Range** from the drop-down list. **Note**: The **Time Range** drop down menu will only have available options if a time profile has been created.

Click the **Delete Time Range** button to clear the setting in the corresponding Time Range field.

Click the **Apply** button to accept the changes made.

Note: The **Max Wattage** option will only be available if the check box next to the input field is enabled. When enabled, the Power Limit drop down menu will not be available.

Note: If the switch failed to supply power to the IEEE 802.3at PD (Powered Device),

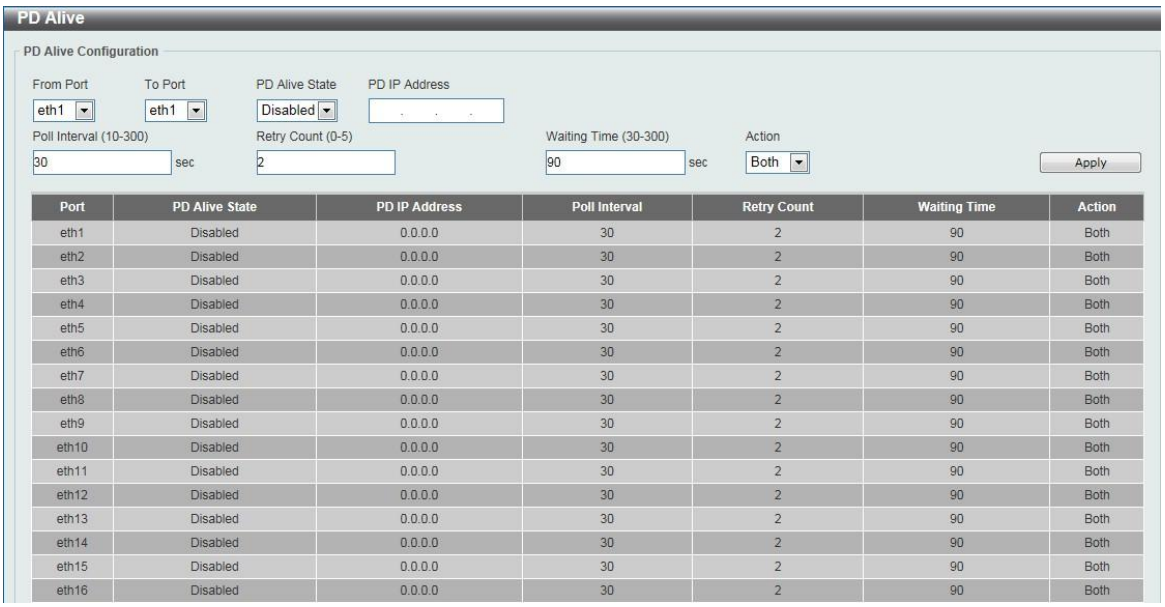
1.Check if the PD connected to the port supports the IEEE 802.3at standard.

2.Manually configure the corresponding port's power limit value to 30 Watts.

PD Alive

This window is used to configure the PoE port.

To view the following window, click **System > PoE > PD Alive**, as shown below:



Port	PD Alive State	PD IP Address	Poll Interval	Retry Count	Waiting Time	Action
eth1	Disabled	0.0.0.0	30	2	90	Both
eth2	Disabled	0.0.0.0	30	2	90	Both
eth3	Disabled	0.0.0.0	30	2	90	Both
eth4	Disabled	0.0.0.0	30	2	90	Both
eth5	Disabled	0.0.0.0	30	2	90	Both
eth6	Disabled	0.0.0.0	30	2	90	Both
eth7	Disabled	0.0.0.0	30	2	90	Both
eth8	Disabled	0.0.0.0	30	2	90	Both
eth9	Disabled	0.0.0.0	30	2	90	Both
eth10	Disabled	0.0.0.0	30	2	90	Both
eth11	Disabled	0.0.0.0	30	2	90	Both
eth12	Disabled	0.0.0.0	30	2	90	Both
eth13	Disabled	0.0.0.0	30	2	90	Both
eth14	Disabled	0.0.0.0	30	2	90	Both
eth15	Disabled	0.0.0.0	30	2	90	Both
eth16	Disabled	0.0.0.0	30	2	90	Both

Figure 5-14 PD Alive window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the state of the PoE alive function on the specified port(s) here.
PD IP Address	Enter the IPv4 address of the target PD here.
Poll Interval (10-300)	Enter the poll interval value here. The range is from 10 to 300 seconds. This is the interval at which ping requests will be sent to the target PD to check the status.
Retry Count (0-5)	Enter the retry count value here. The range is from 0 to 5. This is the amount of times that the ping request will be resend if the target PD does not respond.
Waiting Time (30-300)	Enter the waiting time value here. The range is from 30 to 300 seconds. This is the time the Switch will wait for the PD to recover from rebooting.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state. • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps and then to reset the PoE port state.

Click the **Apply** button to accept the changes made.

System Log

System Log Settings

This window is used to view and configure the system's log settings.

To view the following window, click **System > System Log > System Log Settings**, as shown below:

Figure 5-15 System Log Settings window

The fields that can be configured for **Global State** are described below:

Parameter	Description
System Log	Select this option to enable or disable the System Log functionality.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Buffer Log Settings** are described below:

Parameter	Description
Buffer Log State	Select whether the enable or disable the buffer log's global state here. Options to choose from are **Enable**, **Disabled**.

Click the **Apply** button to accept the changes made.

System Log Server Settings

This window is used to view and configure system log's server settings.

To view the following window, click **System > System Log > System Log Server Settings**, as shown below:

Figure 5-16 System Log Server Settings window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the system log server's IPv4 address here.
UDP Port	Enter the system log server's UDP port number here. This value must be between 1024 and 65535. By default, this value is 514.
Facility	Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 to Local 7).
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **Warning, informational,** and **All** The possible levels are: **Warning** - The lowest level of a device warning. The device is functioning, but an operational problem has occurred. **Informational** - Provides device information. **All** - Displays all levels of system logs.

Click the **Apply** button to accept the changes made.

System Log

This window is used to view and clear the system log.

To view the following window, click **System > System Log > System Log**, as shown below:

Figure 5- 17 System Log window

Click the **Clear Log** button to clear the system log entries displayed in the table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Time

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the SNTP subnet of servers and clients, and adjust the system clock in each participant.

Clock Settings

This window is used to configure the time settings for the Switch.

To view the following window, click **System > Time > Clock Settings**, as shown below:

Figure 5-18 Clock Settings window

The fields that can be configured are described below:

Parameter	Description
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.
Date (DD / MM / YYYY)	Enter the current day, month, and year to update the system clock.

Click the **Apply** button to accept the changes made.

Time Zone Settings

This window is used to configure time zones and Daylight Savings Time settings for SNTP.

To view the following window, click **System > Time > Time Zone Settings**, as shown below:

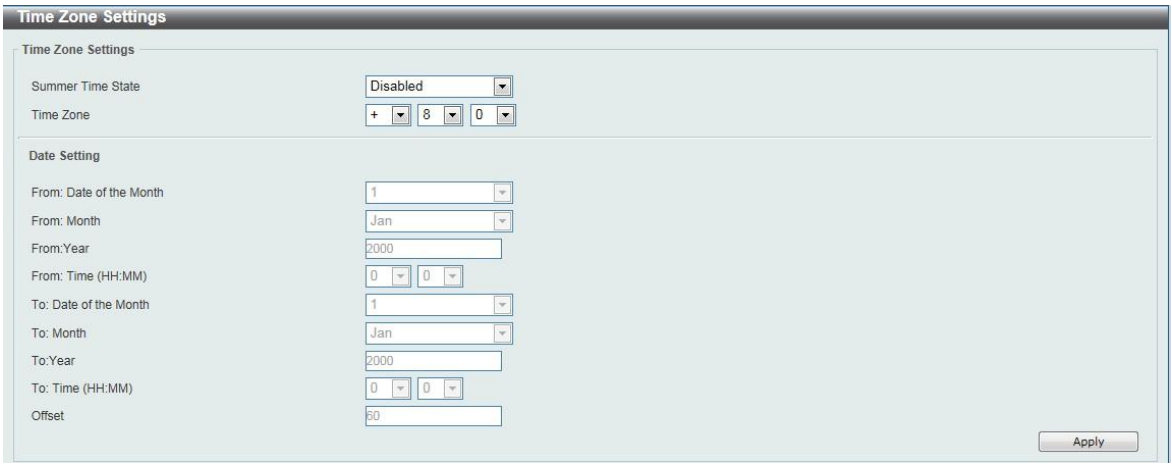


Figure 5-19 Time Zone Settings window

The fields that can be configured are described below:

Parameter	Description
Summer Time State	Select the summer time setting. Options to choose from are **Disabled**, and **Date Setting**. **Disabled** - Select to disable the summer time setting. **Date Setting** - Select to configure the summer time that should start and end on the specified date.
Time Zone	Select to specify your local time zone's offset from Coordinated Universal Time (UTC).

The fields that can be configured for **Date Setting** are described below:

Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time (HH:MM)	Select the time of the day that summer time will start.
To: Date of the Month	Select date of the month that summer time will end.
To: Month	Select the month that summer time will end.
To: Year	Enter the year that the summer time will end.
To: Time (HH:MM)	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

Click the **Apply** button to accept the changes made.

SNTP Settings

This window is used to configure the time settings for the Switch.

To view the following window, click **System > Time > SNTP Settings**, as shown below:

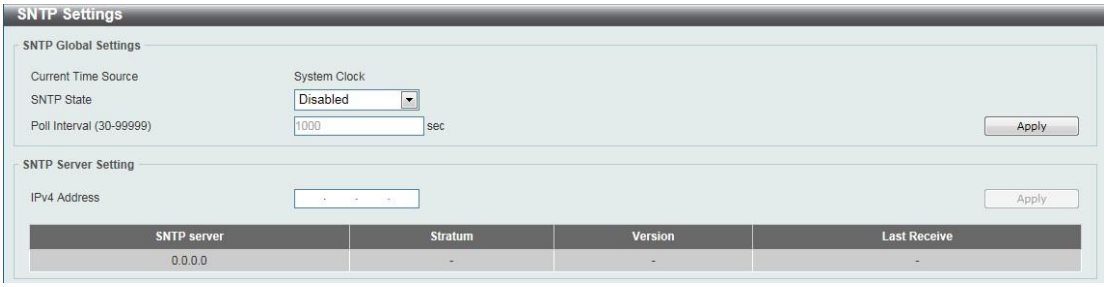


Figure 5-20 SNTP Settings window

The fields that can be configured for **SNTP Global Settings** are described below:

Parameter	Description
SNTP State	Select this option to enable or disable SNTP.
Pool Interval	Enter the synchronizing interval in seconds. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **SNTP Server Setting** are described below:

Parameter	Description
IPv4 Address	Enter the IP address of the SNTP server which provides the clock synchronization.

Click the **Apply** button to add the SNTP server.

Click the **Delete** button to remove the specified entry.

Time Range

This window is used to view and configure the time range settings. The maximum number of time profiles supported by the switch is 4.

To view the following window, click **System > Time Range**, as shown below:

Figure 5-21 Time Range window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the name of the time range. This name can be up to 8 characters long.
From Week / To Week	Select the starting and ending days of the week that will be used for this time range. Tick the **Daily** option to use this time range for every day of the week. Tick the **End Week Day** option to use this time range from the starting day of the week until the end of the week, which is Sunday.
From Time / To Time	Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

6. Management

User Account Settings
SNMP
HTTP/HTTPS
D-Link Discovery Protocol

User Account Settings

This window is used to configure the user accounts. The active user account sessions can be viewed.

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**.

NOTE: By default, the admin account is created on the Switch.

To view the following window, click **Management > User Account Settings**, as shown below:

Figure 6-1 User Management Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user account name here.
Password	Enter the password for the account here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified user account entry.

Note: Only one user can be logged into the switch at any time.

SNMP

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, and 2c. The two versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v2c, user authentication is accomplished using ‘community string’, which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, and Topology Change.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, and 2c. The administrator can specify the SNMP version used to monitor and control the Switch.

SNMP settings are configured using the menus located on the SNMP folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

This window is used to configure the SNMP global settings and trap settings.

To view the following window, click **Management > SNMP > SNMP Global Settings**, as shown below:

Figure 6-2 SNMP Global Settings window

The fields that can be configured for **SNMP Global Settings** are described below:

Parameter	Description
SNMP Global State	Select this option to enable or disable the SNMP feature.

The fields that can be configured for **Trap Settings** are described below:

Parameter	Description
Trap Global State	Select this option to enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Tick this option to control the sending of SNMP authentication failure notifications.
Port Link Up	Tick this option to control the sending of port link up notifications.
Port Link Down	Tick this option to control the sending of port link down notifications.
Coldstart	Tick this option to control the sending of SNMP Coldstart notifications.
Warmstart	Tick this option to control the sending of SNMP Warmstart notifications.

Click the **Apply** button to accept the changes made.

SNMP Community Table Settings

This window is used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To view the following window, click **Management > SNMP > SNMP Community Table Settings**, as shown below:

Figure 6-3 SNMP Community Table Settings window

The fields that can be configured are described below:

Parameter	Description
Access Right	Select the access right here. Options to choose from are **Read Only** and **Read Write**. **Read Only** - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. **Read Write** - SNMP community members using the community string created can read from and write to the contents of the MIBs on the Switch.
Community Name	Enter an alphanumeric string of up to 16 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.

Click the **Apply** button to accept the changes made.

SNMP Host Table Settings

This window is used to configure and display the recipient of the SNMP notification.

To view the following window, click **Management > SNMP > SNMP Host Table Settings**, as shown below:

Figure 6-4 SNMP Host Table Settings

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options to choose from are **SNMPv1**, and **SNMPv2c**. **SNMPv1** - Select to allow the group user to use the SNMPv1 security model. **SNMPv2c** - Select to allow the group user to use the SNMPv2c security model.
Community String	Enter the community string to be sent with the notification packet.

Click the **Apply** button to accept the changes made.

HTTP/HTTPS

This window is used to configure Web settings on the Switch.

To view the following window, click **Management > HTTP/HTTPS**, as shown below:

Figure 6-5 HTTP/HTTPS window

The fields that can be configured for **HTTP/HTTPS Settings** are described below:

Parameter	Description
Web Session	Select this option to enable the configuration through HTTP or HTTPS. **Note:** When switching from HTTP to HTTPS mode, the switch will take about 30 seconds to initialize the secured HTTP environment.
Web Session Timeout	Enter a value for the amount of time in seconds before the web session expires.

Click the **Apply** button to accept the changes made.

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

D-Link Discovery Protocol

This window is used to configure and display D-Link Discovery Protocol (DDP).

To view the following window, click **Management > D-Link Discovery Protocol**, as shown below:

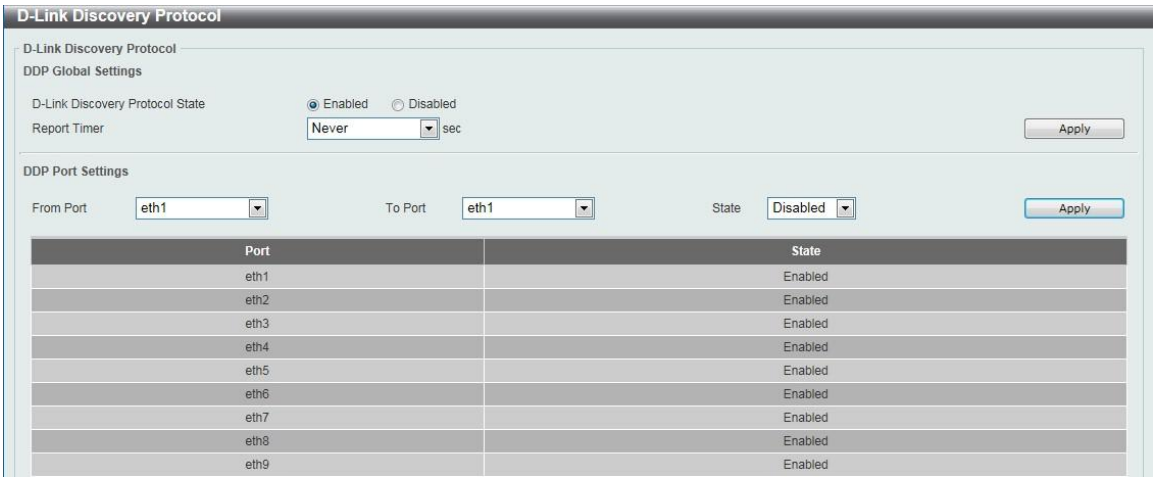


Figure 6-6 D-Link Discovery Protocol window

The fields that can be configured for **D-Link Discovery Protocol** are described below:

Parameter	Description
D-Link Discovery Protocol State	Select this option to enable or disable DDP global state.
Report Timer	Select the interval in seconds between two consecutive DDP report messages. Options to choose from are **30**, **60**, **90**,**120**, and **Never**.

Click the **Apply** button to accept the changes made.

7. L2 Features

FDB

VLAN

Spanning Tree

Loopback Detection

Link Aggregation

L2 Multicast Control

LLDP

FDB

Static FDB

Unicast Static FDB

This window is used to view and configure the static unicast forwarding settings on the Switch.

To view the following window, click **L2 Features> FDB > Static FDB > Unicast Static FDB**, as shown below:

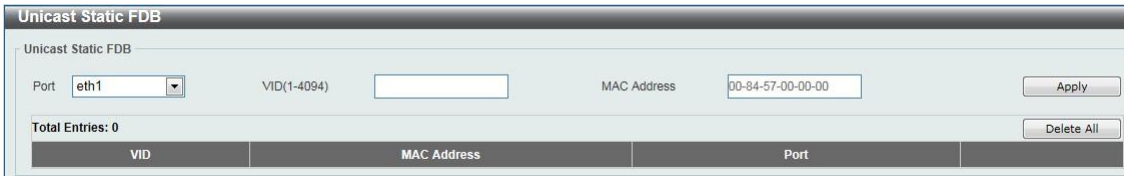


Figure 7-1 Unicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
Port	Allows the selection of the port number on which the MAC address entered resides.
VID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to delete all the entries found in the display table.

Click the **Delete** button to remove the specified entry.

Multicast Static FDB

This window is used to view and configure the multicast static FDB settings. To view the following window, click **L2 Features > FDB > Static FDB > Multicast Static FDB**, as shown below:

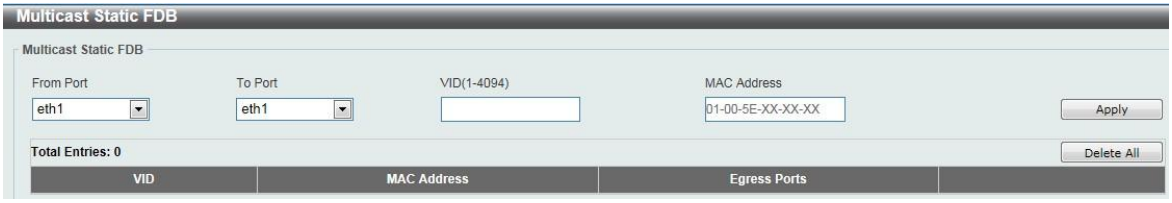


Figure 7-2 Multicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specific entry.

MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

To view the following window, click **L2 Features > FDB > MAC Address Table Settings**, as shown below:

Figure 7-3 MAC Address Table Settings (Global Settings) window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

Click the **Apply** button to accept the changes made.

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.

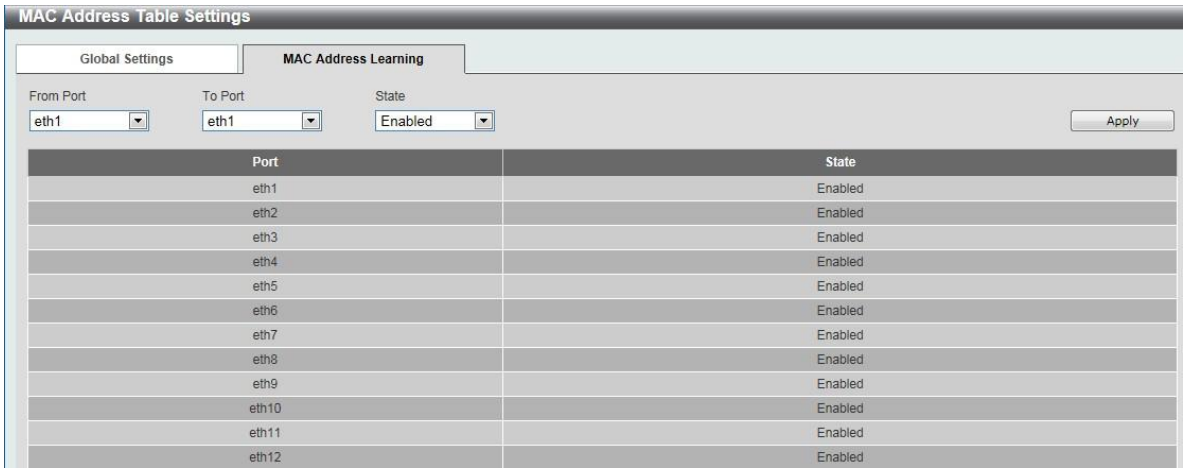


Figure 7-4 MAC Address Table Settings (MAC Address Learning) window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the MAC address learning function on the ports specified here.

Click the **Apply** button to accept the changes made.

MAC Address Table

This window is used to view the entries listed in the MAC address table.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as shown below:

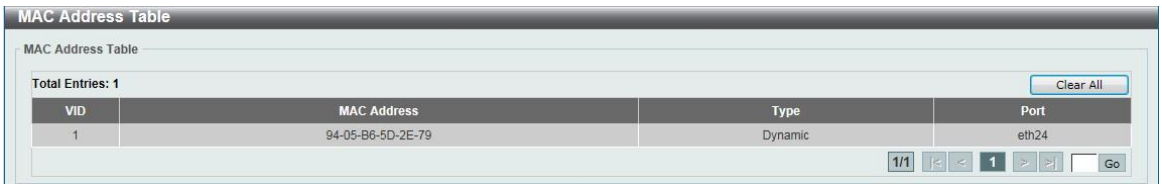


Figure 7-5 MAC Address Table window

Click the **Clear All** button to clear all dynamic MAC addresses.

VLAN

VLAN Configuration Wizard

This window is used to view and configure the VLAN settings on this switch.

To view the following window, click **L2 Features > VLAN > VLAN Configuration Wizard**, as shown below:

Figure 7-6 VLAN Configuration Wizard window

The fields that can be configured for **VLAN Configuration Wizard** are described below:

Parameter	Description
Create VLAN VID	Create VLAN ID
Configure VLAN VID	Configure VLAN ID

Click the **Next** button to accept the changes made.

This window is used to create the VLAN on this switch.

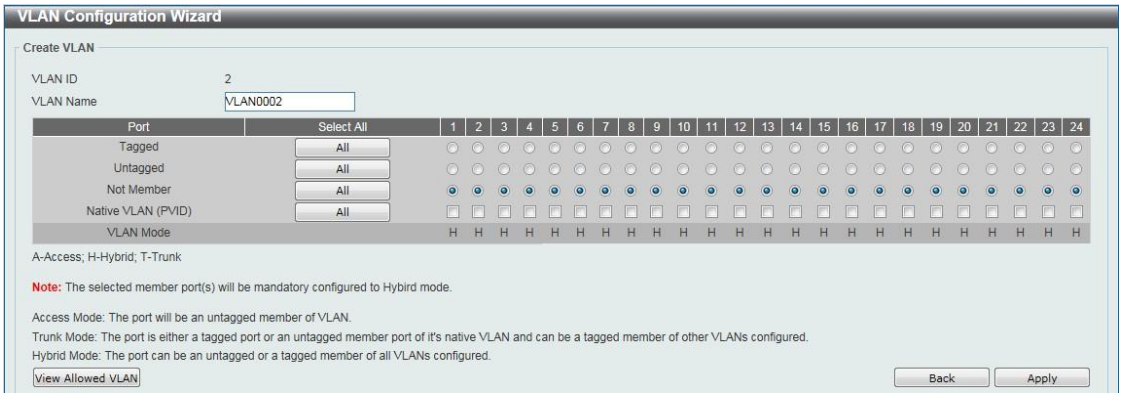


Figure 7-7 VLAN Configuration Wizard window

The fields that can be configured for **VLAN Configuration Wizard** are described below:

Parameter	Description
VLAN ID	Create VLAN VID
VLAN Name	VLAN Group name

Click the **Apply** button to accept the changes made.

802.1Q VLAN

This window is used to view and configure the VLAN settings on this switch.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN**, as shown below:

Figure 7-8 802.1Q VLAN window

The fields that can be configured for **802.1Q VLAN** are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be created here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Management VLAN

This window is used to configure the Management VLAN function.

To view the following window, click **L2 Features > VLAN > Management VLAN**, as shown below:

Figure 7-9 Management VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
Management VLAN State	Select this option to enable or disable the Management VLAN function.
VID	VLAN VID is a unique number (between 1 and 4094) that identifies a particular VLAN.

Click the **Apply** button to accept the changes made.

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click **L2 Features > VLAN > Asymmetric VLAN**, as shown below:

Figure 7-10 Asymmetric VLAN window

The fields that can be configured are described below:

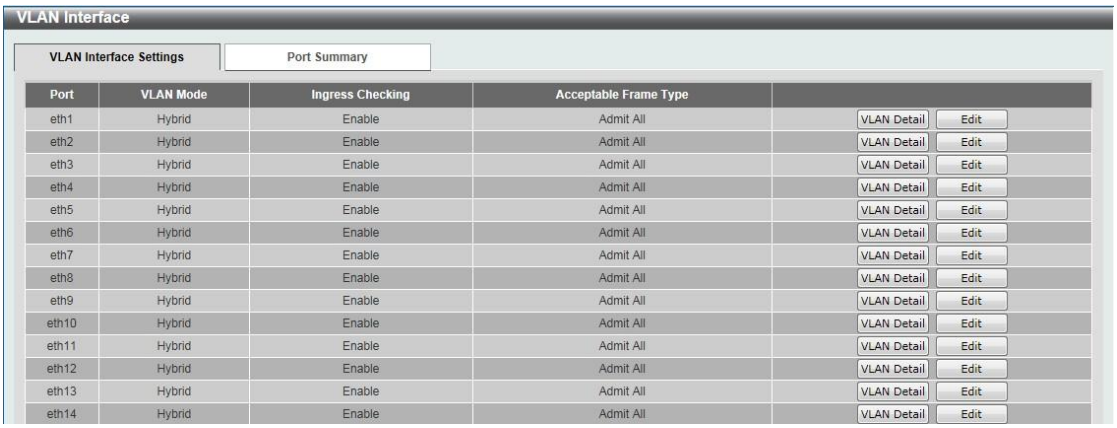
Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the asymmetric VLAN function

Click the **Apply** button to accept the changes made.

VLAN Interface

This window is used to view and configure VLAN interface settings.

To view the following window, click **L2 Features > VLAN > VLAN Interface**, as shown below:



Port	VLAN Mode	Ingress Checking	Acceptable Frame Type		
eth1	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth2	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth3	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth4	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth5	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth6	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth7	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth8	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth9	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth10	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth11	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth12	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth13	Hybrid	Enable	Admit All	VLAN Detail	Edit
eth14	Hybrid	Enable	Admit All	VLAN Detail	Edit

Figure 7-11 VLAN Interface window

Click the **View Detail** button to view more detailed information about the VLAN on the specific interface.

Click the **Edit** button to re-configure the specific entry.

After clicking the **VLAN Detail** button, the following page will appear.

Port	eth1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1,
Hybrid Tagged VLAN	-
Ingress Checking	Enabled
Acceptable Frame Type	Admit All

Figure 7-12 VLAN Interface Information window

More detailed information about the VLAN of the specific interface is displayed.

Click the **Back** button to return to the previous window.

After the **Edit** button is clicked, the following window will appear. This is a dynamic window that will change when a different **VLAN Mode** was selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

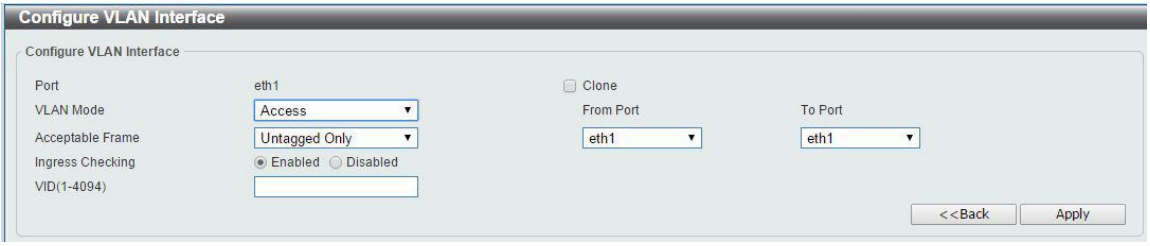


Figure 7-13 Configure VLAN Interface - Access window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select this option to enable or disable the ingress checking function. When ingress checking is enabled, the packet will be dropped if the received port is not member port of the VLAN classified for the received packet.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

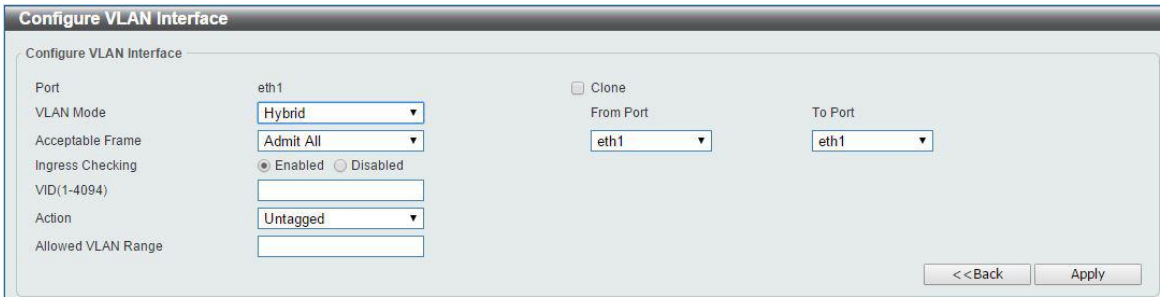


Figure 7-14 Configure VLAN Interface - Hybrid window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to

	choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select this option to enable or disable the ingress checking function. When ingress checking is enabled, the packet will be dropped if the received port is not member port of the VLAN classified for the received packet.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are **Remove**, **Tagged**, and **Untagged**.
Allowed VLAN Range	Enter the allowed VLAN range information here.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Trunk** is selected as the **VLAN Mode**, the following page will appear.

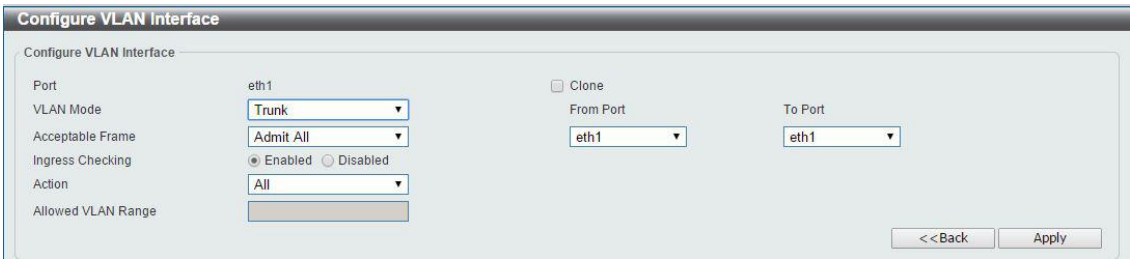


Figure 7-15 Configure VLAN Interface - Trunk window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select this option to enable or disable the ingress checking function. When ingress checking is enabled, the packet will be dropped if the received port is not member port of the VLAN classified for the received packet.
Action	Select the action that will be taken here. Options to choose from are **Remove**, **Tagged**, and **Untagged**.
Allowed VLAN Range	Enter the allowed VLAN range information here.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Note: In VLAN Mode, when a port is set to access mode, this port will be untagged member of the access VLAN configured for the port.

When a port is set to hybrid mode, the port can be untagged or tagged member of all VLANs configured by the user.

When a port is set to trunk mode, this port is either tagged or untagged member port of its native VLAN and can be tagged member of other VLANs configured by the user. The purpose of a trunk port is to support the switch-to-switch connection.

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:

Figure 7-16 Auto Surveillance Properties window

The fields that can be configured for **Global Settings** are described below:

Parameter	Description
Surveillance VLAN	Select this option to enable or disable the surveillance VLAN state
Surveillance VLAN ID	Enter the surveillance VLAN ID. The range is from 2 to 4094.
Surveillance VLAN CoS	Select the priority of the surveillance VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop.

Click the **Apply** button to accept the changes made.

MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device**, as shown below:

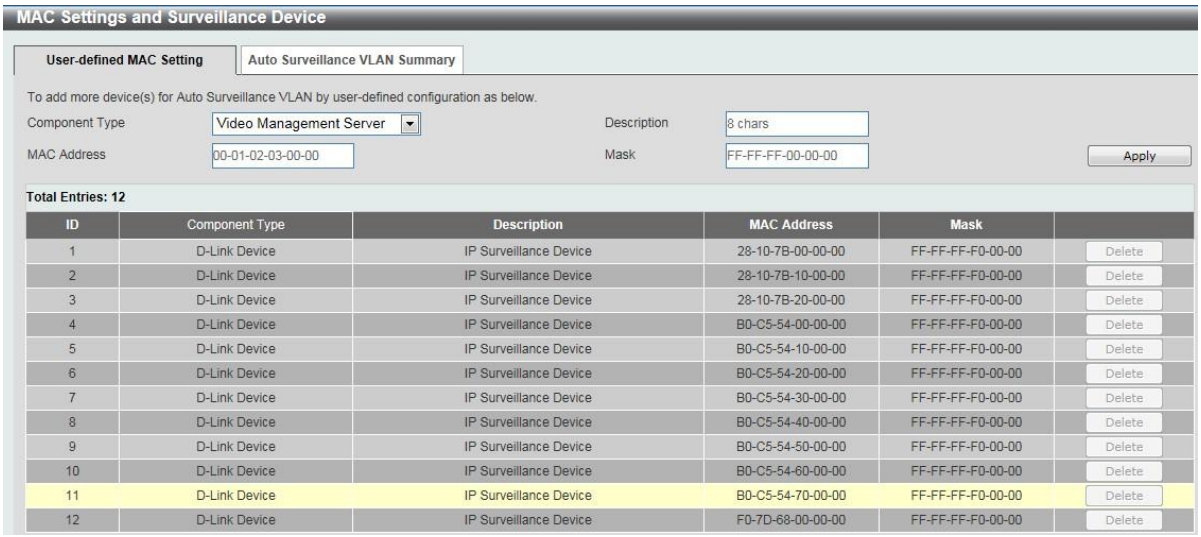


Figure 7-17 User -defined MAC Settings window

The fields that can be configured are described below:

Parameter	Description
Component Type	Select the surveillance component type. Options to choose from are **Video Management Server**, **VMS Client/Remote Viewer**, **Video Encoder**, **Network Storage**, and **Other IP Surveillance Device**.
Description	Enter the description for the user-defined OUI with a maximum of 8 characters.
MAC Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **Auto Surveillance VLAN Summary** tab, the following page will appear.

Figure 7-18 Auto Surveillance VLAN Summary window

Voice VLAN

Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global**, as show below:

Figure 7-19 Voice VLAN Global window

The fields that can be configured are described below:

Parameter	Description
Voice VLAN State	Select this option to enable or disable the voice VLAN.
Voice VLAN ID	Enter the voice VLAN ID. The value is range from 2 to 4094.
Voice VLAN CoS	Select the priority of the voice VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

Click the **Apply** button to accept the changes made for each individual section.

Voice VLAN Port

This window is used to configure the user-defined voice traffic's port.

To view the following window, click **L2 Features > VLAN >Voice VLAN > Voice VLAN OUI**, as show below:

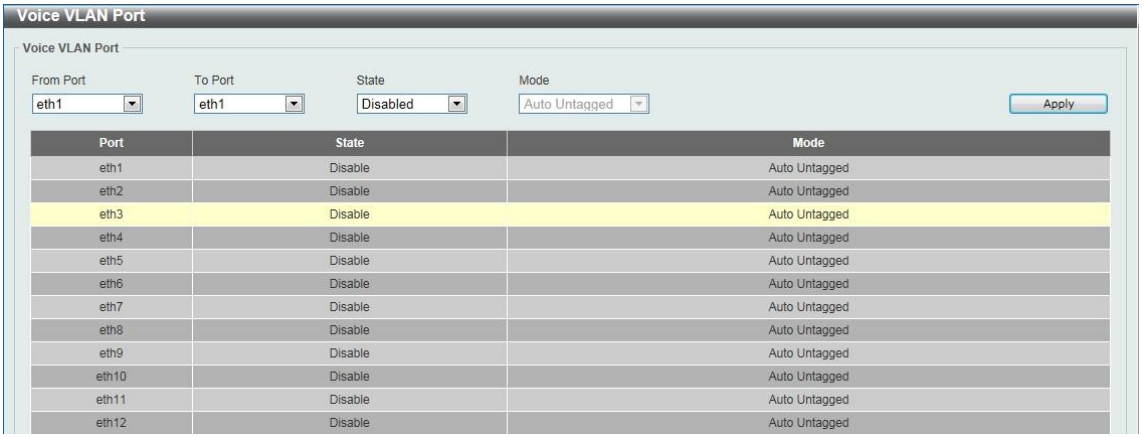


Figure 7-20 Voice VLAN Port window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the range of ports that will be used for this configuration here.
State	Select this option to enable or disable the Voice VLAN state of the port.
Mode	Choose the Voice VLAN mode for the port. This can be **Auto untagged**, **Auto Tagged**, or **Manually** configured.

Click the **Apply** button to accept the changes made.

Voice VLAN OUI

This window is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click **L2 Features > VLAN >Voice VLAN > Voice VLAN OUI**, as show below:

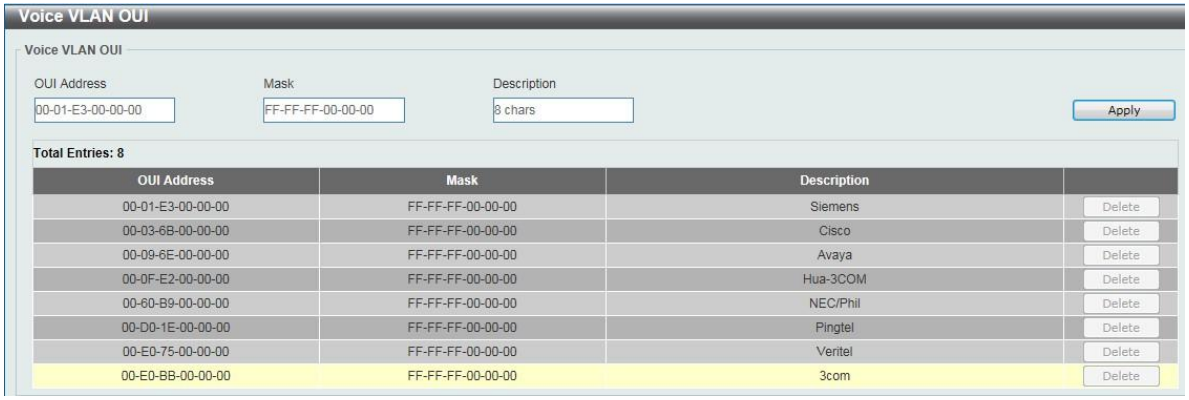


Figure 7-21 Voice VLAN OUI window

The fields that can be configured are described below:

Parameter	Description
OUI Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.
Description	Enter the description for the user-defined OUI with a maximum of 8 characters.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click **L2 Features > VLAN >Voice VLAN > Voice VLAN Device**, as show below:

Figure 7-22 Voice VLAN Device window

Spanning Tree

This Switch supports two versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP has been recently introduced to DGS-1100 switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP.

802.1D-2004 Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however, the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available.

STP Global Settings

This window is used to view and configure the STP global settings.

To view the following window, click **L2 Features > Spanning Tree > STP Global Settings**, as shown below:

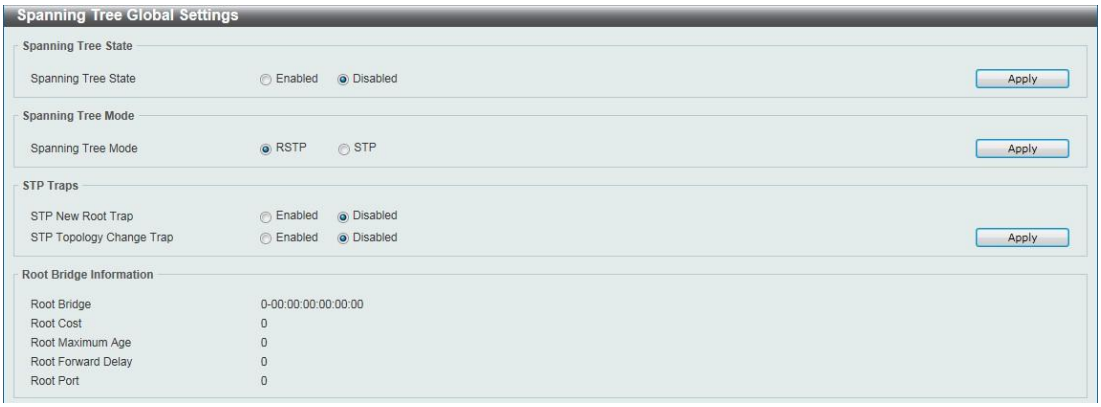


Figure 7-23 STP Global Settings window

The field that can be configured for **Spanning Tree State** is described below:

Parameter	Description
Spanning Tree State	Select this option to enable or disable the STP global state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Mode** are described below:

Parameter	Description
Spanning Tree Mode	Select the STP mode used here. Options to choose from are **RSTP**, and **STP**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select this option to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select this option to enable or disable the STP topology change trap option here.

Click the **Apply** button to accept the changes made.

STP Port Settings

This window is used to view and configure the STP port settings.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as shown below:

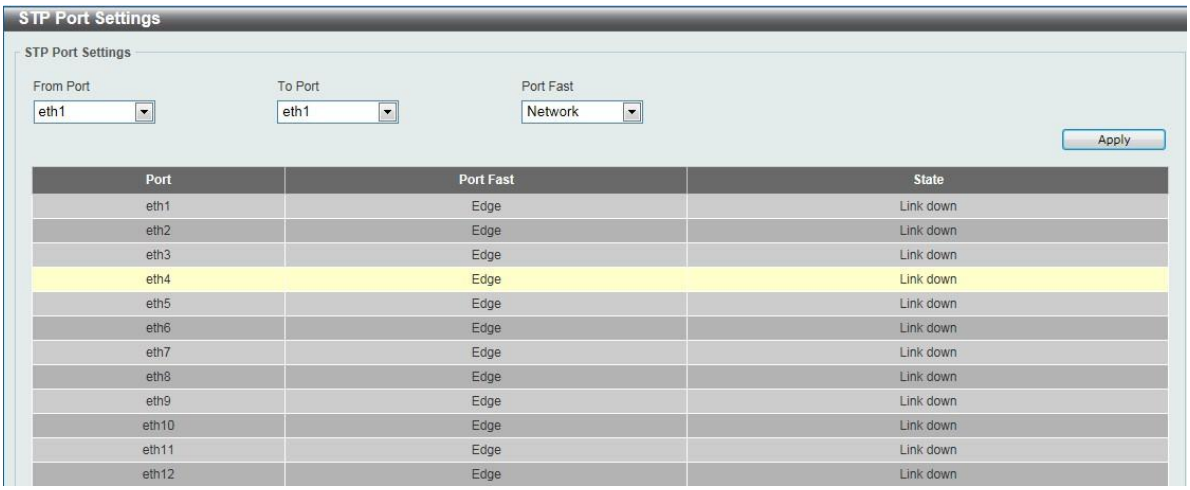


Figure 7-24 STP Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Port Fast	Select the port fast option here. Options to choose from are **Network**, **Disabled**, and **Edge**. In the **Network** mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the **Disable** mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the **Edge** mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is **Edge**.

Click the **Apply** button to accept the changes made.

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, this signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

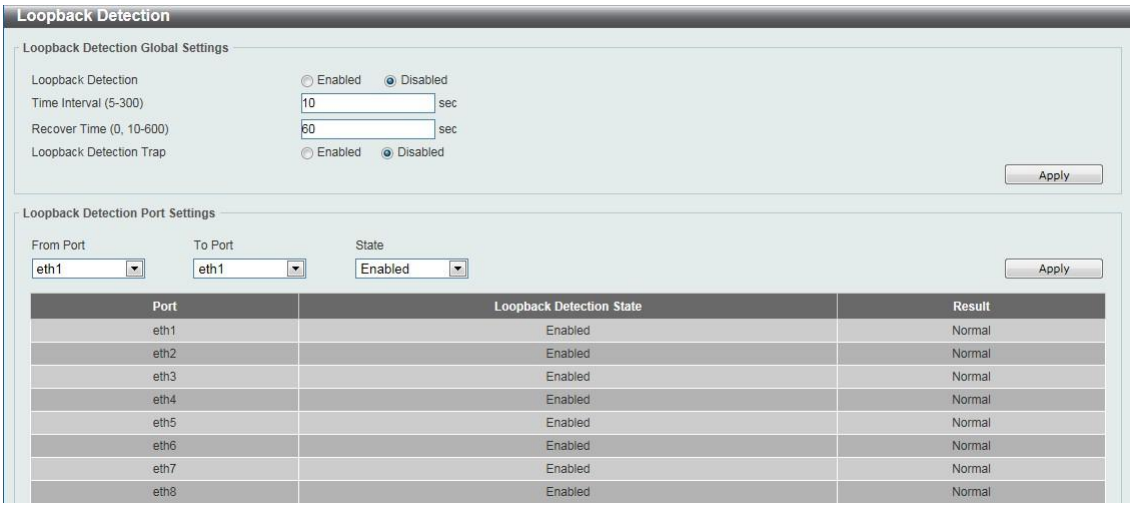


Figure 7-25 Loopback Detection window

The fields that can be configured for **Loopback Detection Global Settings** are described below:

Parameter	Description
Loopback Detection	Select to enable or disable loopback detection. The default is **Disabled**.
Time Interval	Set a Loop detection Interval between *1* and *32767* seconds. The default is *10* seconds.
Recover Time	Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop Detection Recover Time. The default is *60* seconds.
Loopback Detection Trap	Select to enable or disable the loopback detection trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Loopback Detection Port Settings** are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

Click the **Apply** button to accept the changes made.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

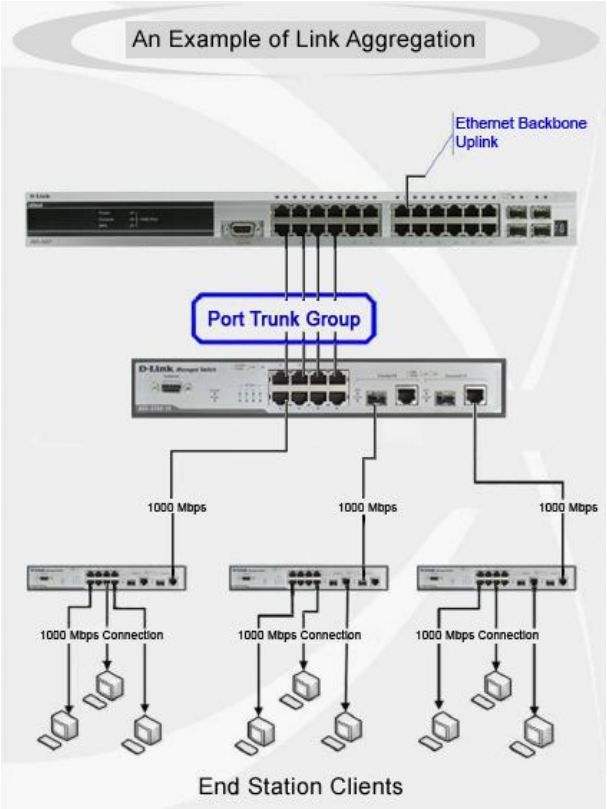


Figure 7-26 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

This window is used to view and configure the link aggregation settings.

NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

the following window, click **L2 Features > Link Aggregation**, as shown below:

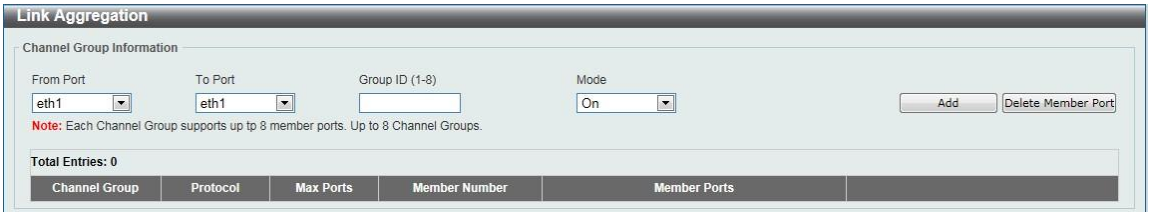


Figure 7-27 Link Aggregation window

The fields that can be configured for **Channel Group Information** are described below:

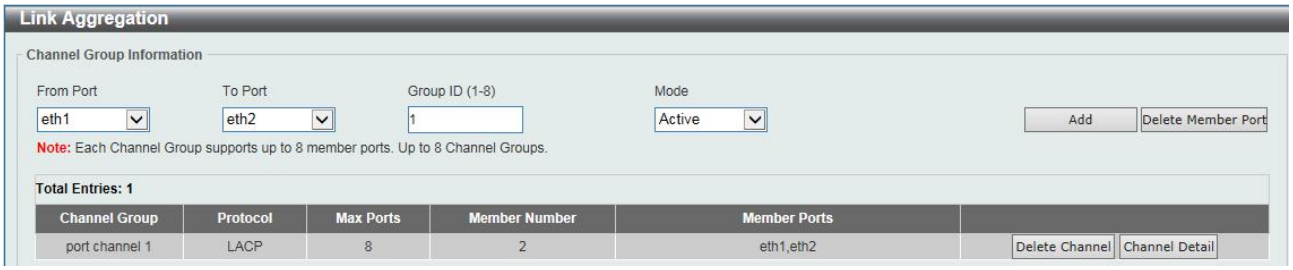
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Group ID	Enter the channel group number here. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group. **Active** - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. **Passive** - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports

Click the **Add** button to add a new entry based on the information entered.

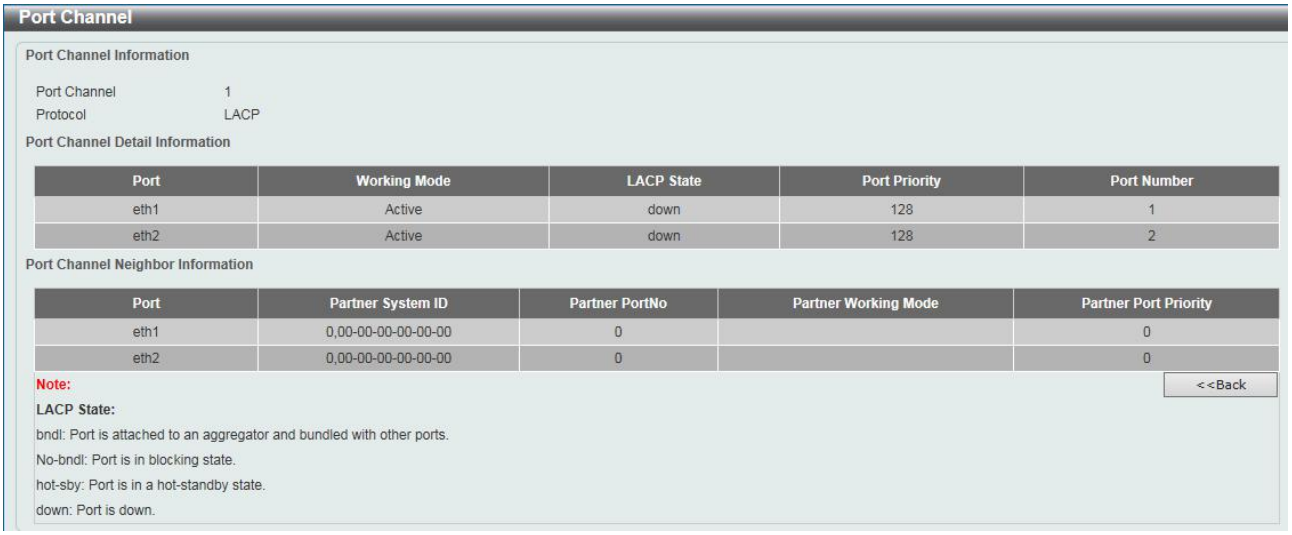
Click the **Delete Member Port** button to remove the specific member port.

NOTE: Modules that support LACP:Port Settings, D-Link Discovery Protocol, FDB, VLAN Configuration Wizard, 8021Q VLAN, Port-based VLAN, VLAN Interface, MAC Settings and Surveillance Device, Voice VLAN Port, Voice VLAN Device, Spanning Tree, Loopback Detection, Link Aggregation, IGMP Snooping Groups Settings, LLDP Neighbor Port Information, Traffic Segmentation and Mirror Settings.

View the following window, click **L2 Features > Link Aggregation>Add**, as shown below:



View the following window, click **L2 Features > Link Aggregation>Add>Channel Detail**, as shown below:



L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

To view the following window, click **L2 Features > L2 Multicast Control >IGMP Snooping > IGMP Snooping Settings**, as shown below:

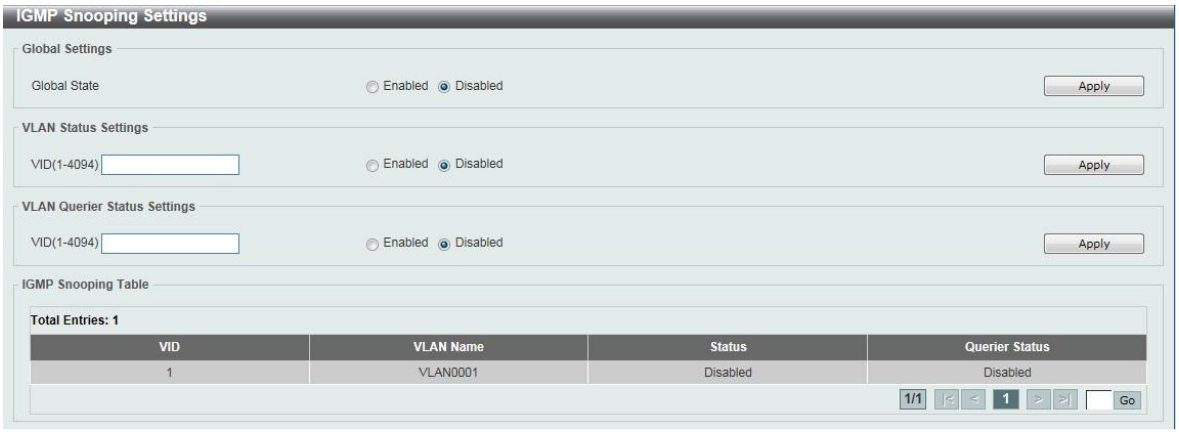


Figure 7-28 IGMP Snooping Settings window

The field that can be configured for **Global Settings** is described below:

Parameter	Description
Global State	Select this option to enable or disable IGMP snooping global state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094 and select to enable or disable IGMP snooping on the VLAN.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **VLAN Querier Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094 and select to enable or disable IGMP snooping on the VLAN.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Snooping Groups Settings

This window is used to configure and view the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control >IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

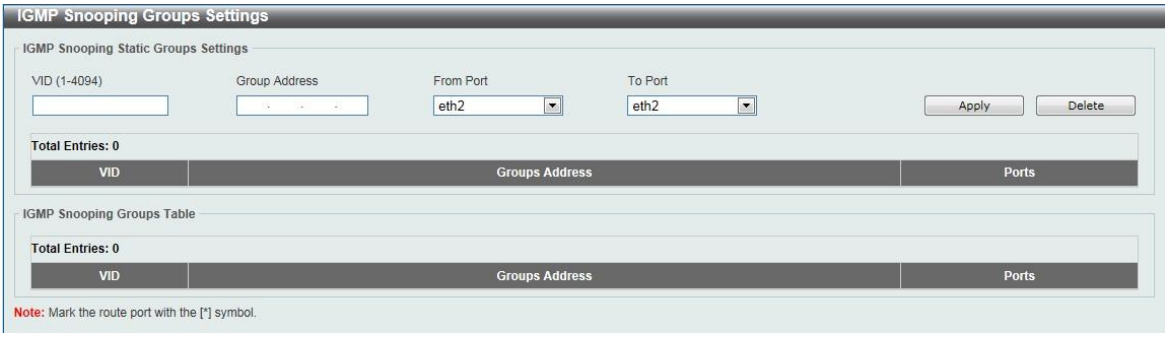


Figure 7-29 IGMP Snooping Groups Settings

The fields that can be configured for **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IP multicast group address.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Multicast Filtering

This window is used to view and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:

Figure 7-30 Multicast Filtering window

The fields that can be configured are described below:

Parameter	Description
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are **Forward Unregistered**, and **Filter Unregistered**. When selecting the **Forward Unregistered** option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the **Filter Unregistered** option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to accept the changes made.

LLDP

LLDP Global Settings

LLDP (Link Layer Discovery Protocol) provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices.

This window is used to configure the LLDP global settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

Figure 7-31 LLDP Global Settings window

The fields that can be configured for **LLDP Global Settings** are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Trap State	Select this option to enable or disable the LLDP trap state.

Click the **Apply** button to accept the changes made.

LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click **L2 Features > LLDP >LLDP Neighbor Port Information**, as show below:

Figure 7-32 LLDP Neighbor Port Information window

8. Quality of Service (QoS)

802.1p Priority
Port Rate Limiting

802.1p Priority

This window is used to view and configure the port's default CoS settings.

To view the following window, click **QoS > 802.1p Priority**, as shown below:

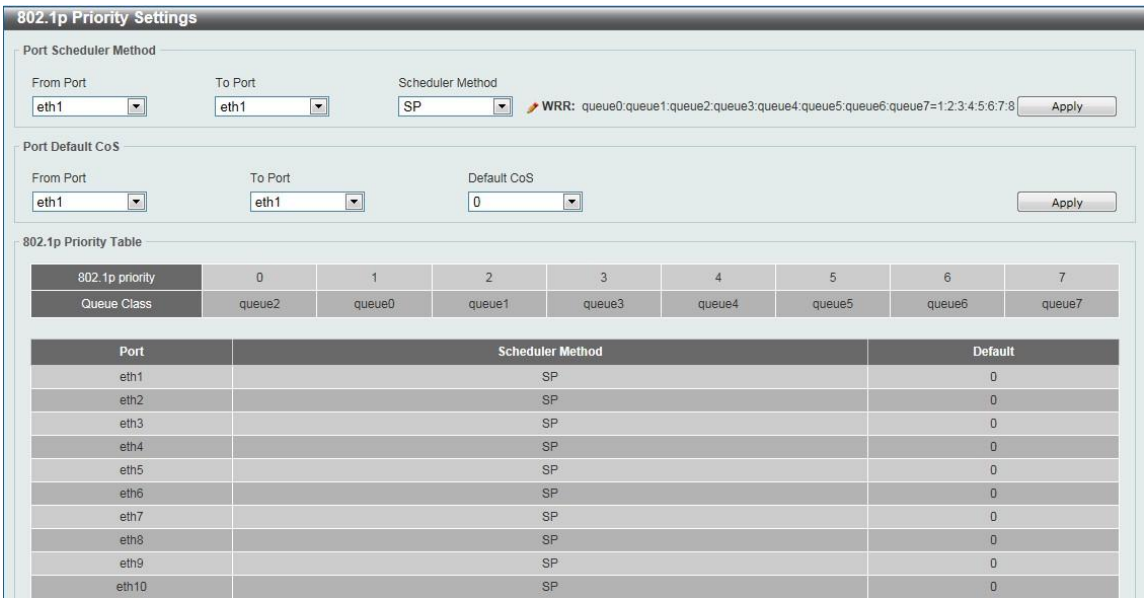


Figure 8-1 Port Default CoS window

The fields that can be configured for Port Scheduler Method are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Scheduler Method	**SP** - Denoting a Strict Priority scheduling will set the highest queue to be emptied first while the other queues will follow the weighted round-robin scheduling scheme **WRR** - Use the weighted round-robin (WRR) algorithm to handle packets in an even distribution in priority classes of service.

Click the **Apply** button to accept the changes made.

The fields that can be configured Port Default CoS are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. The priorities are **Highest**, **High**, **Medium** and **Low**.

Click the **Apply** button to accept the changes made.

Port Rate Limiting

This window is used to view and configure the port rate limiting settings.

To view the following window, click **QoS > Port Rate Limiting**, as shown below:

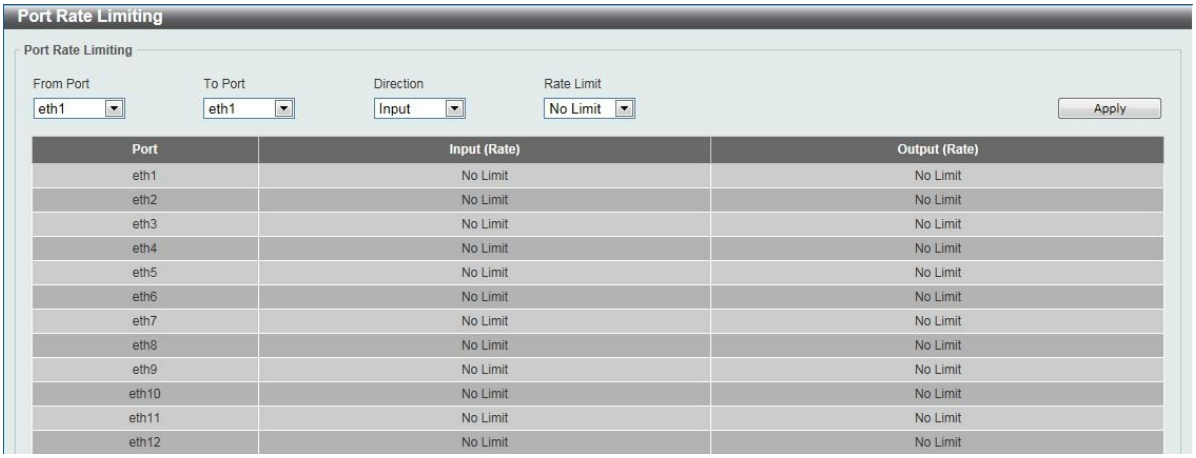


Figure 8-2 Port Rate Limiting window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Options to choose from are **Input** and **Output**. When **Input** is selected, the rate limit for ingress packets is configured. When **Output** is selected, the rate limit for egress packets is configured.
Rate Limit	Select the rate limit value here. When **Direction** is **Input**, this drop-down menu allows you to select data rate from 16Kbps to 512Mbps. When **Direction** is **Output**, this drop-down menu allows you to select data rate from 16Kbps to 512Mbps.

Click the **Apply** button to accept the changes made.

9. Security

Safeguard Engine Settings
Traffic Segmentation
Storm Control
DoS Attack Prevention Settings
Zone Defense Settings
SSL

Safeguard Engine Settings

D-Link's Safeguard Engine is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Smart Switch from being interrupted by malicious viruses or worm attacks.

This window is used to view and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine Settings**, as shown below:

Figure 9-1 Safeguard Engine Settings window

The fields that can be configured for **Safeguard Engine Settings** are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.

Traffic Segmentation

This window is used to view and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

To view the following window, click **Security > Traffic Segmentation**, as shown below:

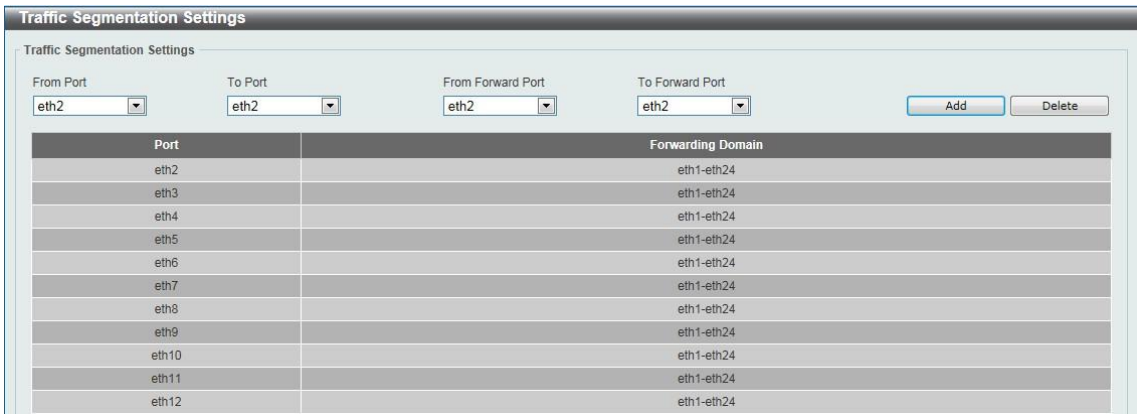


Figure 9-2 Traffic Segmentation Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the receiving port range used for the configuration here.
From Forward Port / To Forward Port	Select the forward port range used for the configuration here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control

This window is used to view and configure the storm control settings. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

To view the following window, click **Security > Storm Control**, as shown below:

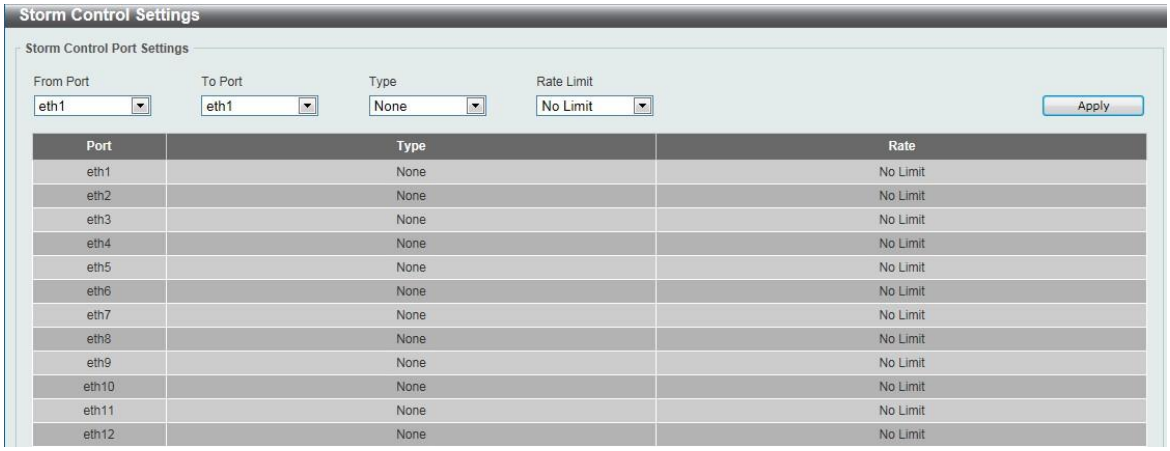


Figure 9-3 Storm Control window

The fields that can be configured for **Storm Control Port Settings** are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**.
Rate Limit	Select a data rate from 16Kbps to 512Mbps.

Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to view and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack**: This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

Figure 9-4 DoS Attack Prevention Settings window

The fields that can be configured for **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the DoS attack prevention feature's global state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

Click the **Apply** button to accept the changes made.

Zone Defense Settings

This window is used to view and configure the Zone Defense setting.

To view the following window, click **Security > Zone Defense Settings**, as shown below:

Figure 9-5 Zone Defense Settings window

The fields that can be configured for **Zone Defense Settings** are described below:

Parameter	Description
State	Select to enable or disable the Zone Defense feature's global state here.

Click the **Apply** button to accept the changes made.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption.

SSL Global Settings

This window is used to view and configure the SSL feature's global settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

Figure 9-6 SSL Global Settings window

The fields that can be configured for **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the SSL feature's global status here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Upgrade Certificate and key** are described below:

Parameter	Description

Key	Upgrade the key
Certificate	Upgrade the Certificate

Click the **Apply** button to accept the changes made.

10. OAM

Cable Diagnostics

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

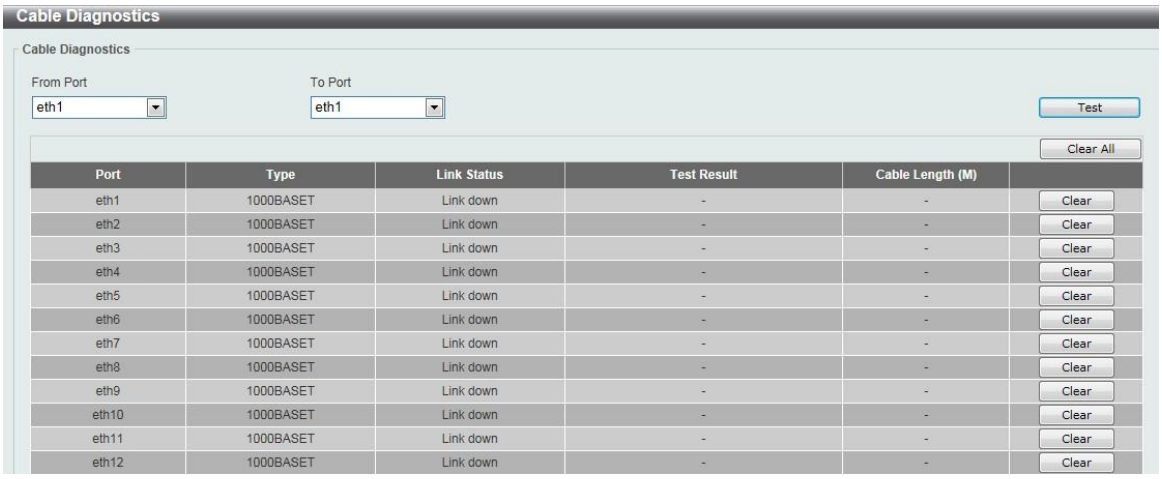


Figure 10-1 Cable Diagnostics window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

Note: The Cable Diagnostics feature is only supported on the copper ports on all DGS-1100 Series switches. Please be sure that Power Saving feature is disabled before enabling Cable Diagnostics function.

Test Result: The description of the cable diagnostic results.

• OK means the cable is good for the connection. Short in Cable means the wires of the RJ45 cable may be in contact somewhere.

• Open in Cable means the wires of RJ45 cable may be broken, or the other end of the cable is simply disconnected.

• Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 1 meters, it will show “0”.

• Cable Length (meter): If the test result is OK and the cable length is less than 15M, then "<15M" will be displayed. If the test result is OK and the cable length is more than 15M and less than 200m, then the cable length will be represented by the total cable length.

11. Monitoring

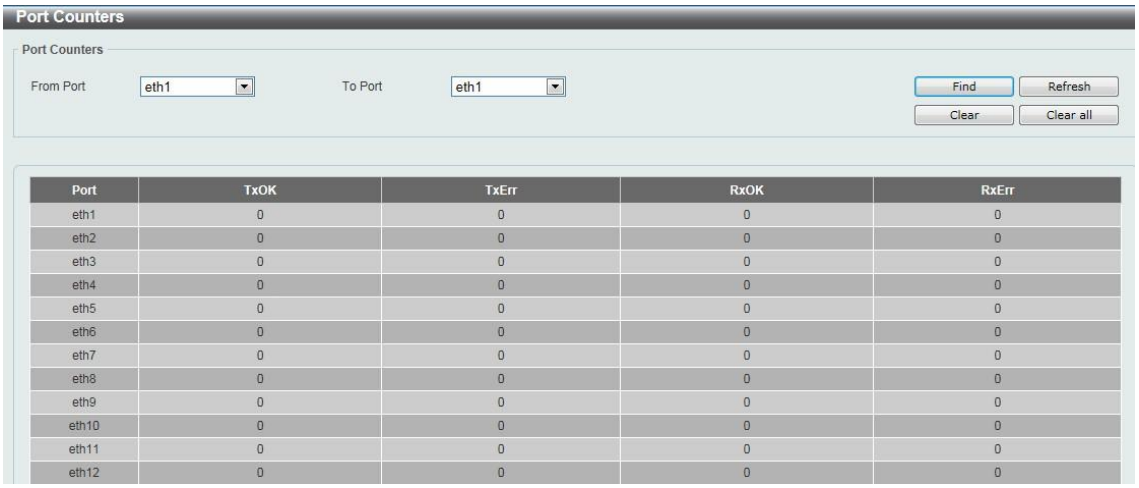
Statistics
Mirror Settings

Statistics

Port Counters

This window is used to display port counter statistics.

To view the following window, click **Monitoring > Statistics > Port Counters**, as show below:



Port	TxOK	TxErr	RxOK	RxErr
eth1	0	0	0	0
eth2	0	0	0	0
eth3	0	0	0	0
eth4	0	0	0	0
eth5	0	0	0	0
eth6	0	0	0	0
eth7	0	0	0	0
eth8	0	0	0	0
eth9	0	0	0	0
eth10	0	0	0	0
eth11	0	0	0	0
eth12	0	0	0	0

Figure 11-1 Port Counters window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.

TxOK: Number of packets transmitted successfully.

RxOK: Number of packets received successfully.

TxError: Number of transmitted packets resulting in error.

RxError: Number of received packets resulting in error

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

Mirror Settings

This window is used to view and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

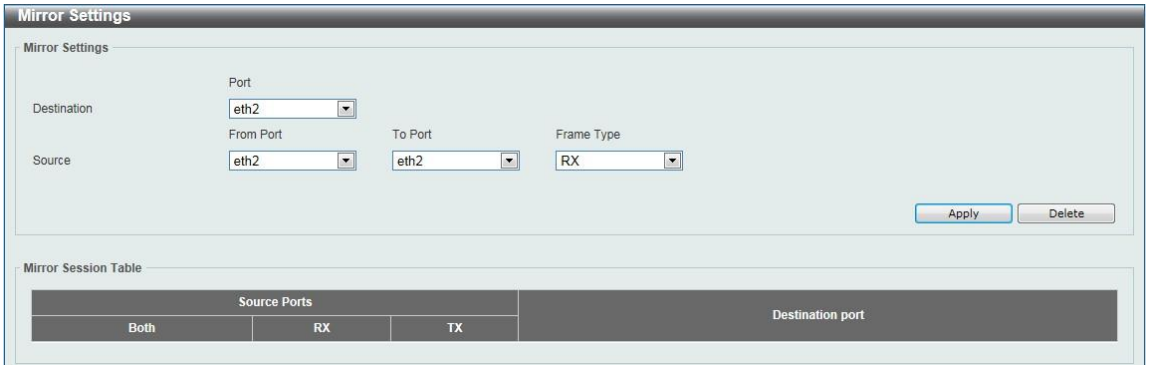


Figure 11-2 Mirror Settings window

The fields that can be configured for **Mirror Settings** are described below:

Parameter	Description
Destination	Select one destination port from drop-down menu.
Source	Select **From Port** number and the **To Port** number as source port from drop-down menu. Lastly select the **Frame Type** option. Options to choose from as the **Frame Type** are **Both**, **RX**, and **TX**. When selecting Both, traffic in both the incoming and outgoing directions will be mirrored. When selecting **RX**, traffic in only the incoming direction will be mirrored. When selecting **TX**, traffic in only the outgoing direction will be mirrored.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

12. Green

Power Saving
EEE

Power Saving

This window is used to configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

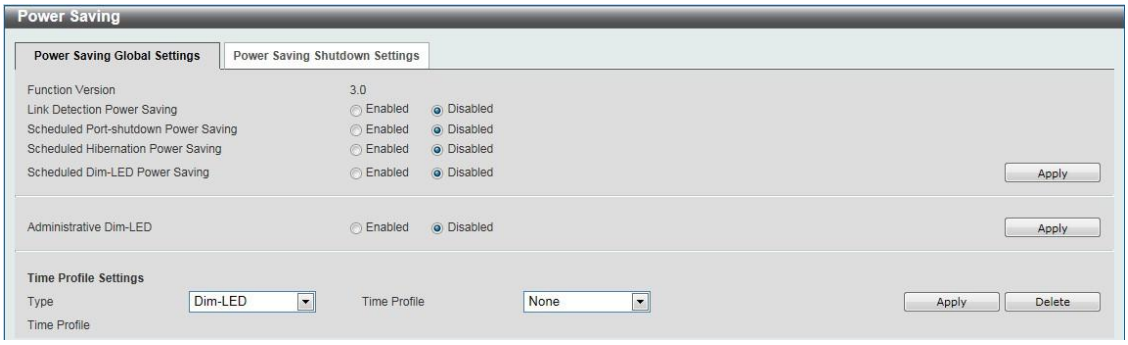


Figure 12-1 Power Saving window

The fields that can be configured are described below:

Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select this option to enable or disable applying the power saving by scheduled hibernation power.
Scheduled Dim-LED Power Saving	Select this option to enable or disable applying the power saving by scheduled dimming LED's.
Administrative Dim-LED	Select this option to enable or disable the port LED function.
Type	Select the type of power saving. Option to choose from is **Dim-LED** or **Hibernation**.
Time Profile	If a Time Profile was previously created, select the desired profile from the drop-down list.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

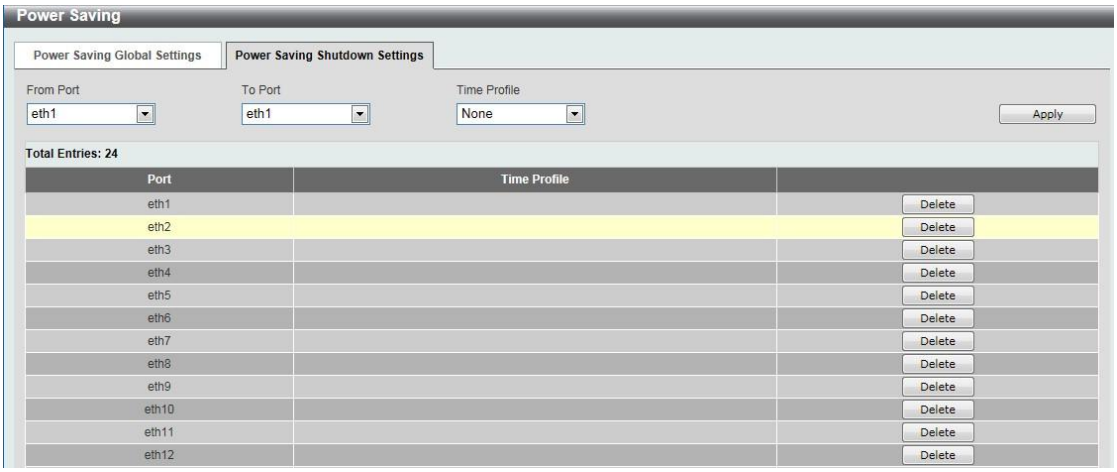


Figure 12-2 Power Saving Shutdown Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Time Range	If a Time Profile was previously created, select the desired profile from the drop-down list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

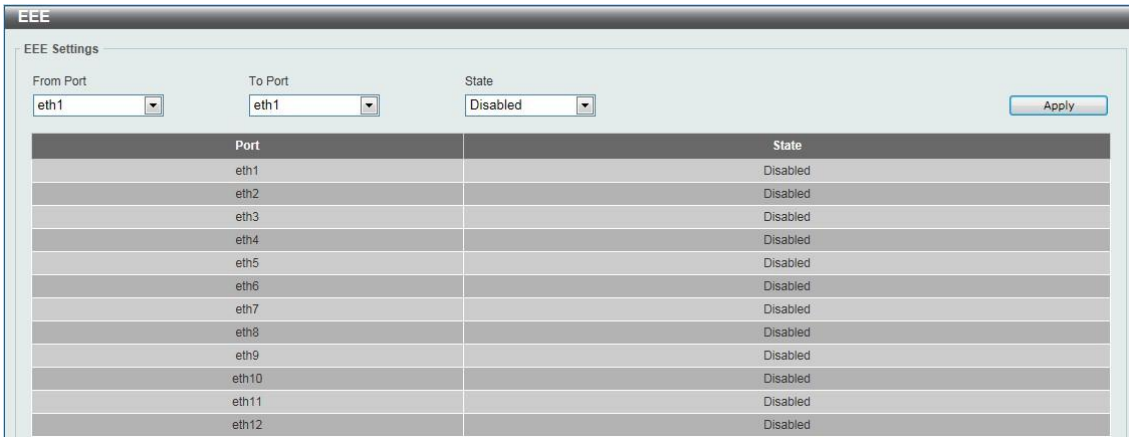


Figure 12-3 EEE window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of this feature here.

Click the **Apply** button to accept the changes made.

Note: The EEE feature is only supported on the copper ports on all DGS-1100 Series switches.

13. Save and Tools

Save Configuration
Firmware Information
Firmware Upgrade & Backup
Configuration Restore & Backup
Log Backup
Ping
Reset
Reboot System

Save Configuration

This window is used to save the running configuration to the start-up configuration of the Switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

Figure 13-1 Save Configuration window

Click the **Apply** button to save the configuration to the switch's flash memory.

Firmware Information

This window is used to show firmware information.

To view the following window, click **Tools > Firmware Information**, as shown below:

Figure 13-2 Firmware Information window

Boot Up: Clicking the **Boot Up** button will set that firmware image as the active image to use upon the next system start up.

Note: Changing the firmware only happens after the switch has been manually rebooted. In order to boot with the newly selected firmware, make sure that the switch is rebooted.

Firmware Upgrade & Backup

Note: When upgrading the firmware on the DGS-1100 Series switch, only the image not currently active can be upgraded. All DGS-1100 Series switches come with two images, however only one can be active at any time. (e.g. If image 1 is currently in use, only image 2 can be upgraded, and vice versa.)

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP**, as shown below:

Figure 13-3 Firmware Upgrade from TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

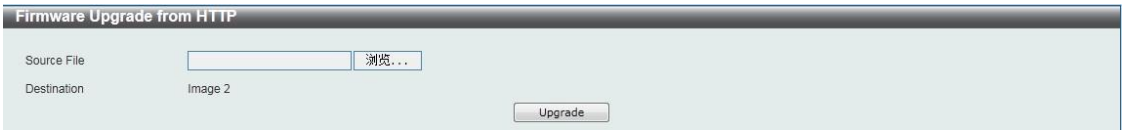


Figure 13-4 Firmware Upgrade from HTTP window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the source filename and path of the firmware file located on the local PC. Alternatively click the **Browse** button to navigate to the location of the firmware file located on the local PC.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 13-5 Firmware Backup to HTTP window

The fields that can be configured are described below:

Parameter	Description
Source	Select the source image to use for the firmware backup.

Click the **Backup** button to initiate the firmware backup.

Note: Firmware backup need to wait around 40 ~ 50 seconds when pushing Backup button due to encrypt firmware. It will take more time when accessing switch via HTTPS

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

Figure 13-6 Firmware Backup to TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Source	Select the source image to use for the firmware backup.
Destination File	Enter the destination path and location where the firmware file should be stored on the TFTP server.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

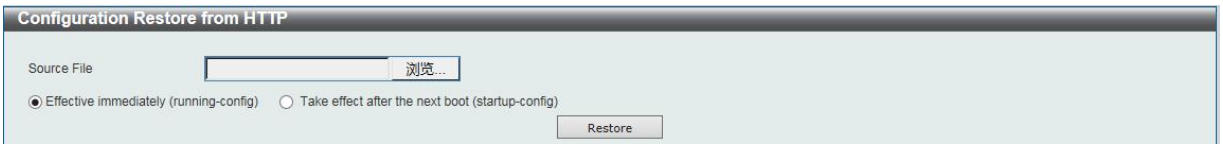


Figure 13-7 Configuration Restore from HTTP window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the source filename and path of the configuration file located on the local PC. Alternatively click the **Browse** button to navigate to the location of the configuration file located on the local PC.

Click the **Restore** button to initiate the configuration restore.

Click **Effective immediately (running-config)** to have the uploaded configuration loaded immediately.

Click **Take effect after the next boot (startup-config)** to load the configuration after the switch has been rebooted.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

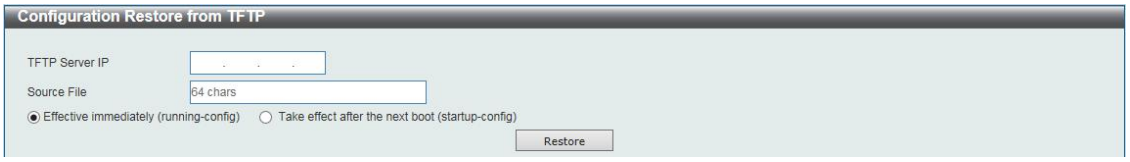


Figure 13-8 Configuration Restore from TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here.

Click the **Restore** button to initiate the configuration restore.

Click **Effective immediately (running-config)** to have the uploaded configuration loaded immediately.

Click **Take effect after the next boot (startup-config)** to load the configuration after the switch has been rebooted.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

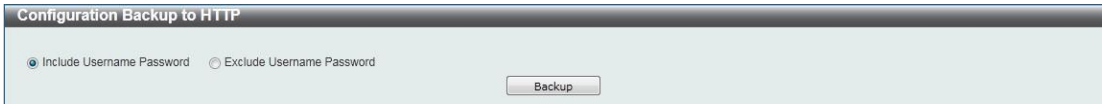


Figure 13-9 Configuration Backup to HTTP window

Select **Include Username Password** to save the switch user accounts and passwords to the backup file.

Select **Exclude username password** to save the switch user accounts and passwords to the backup file.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

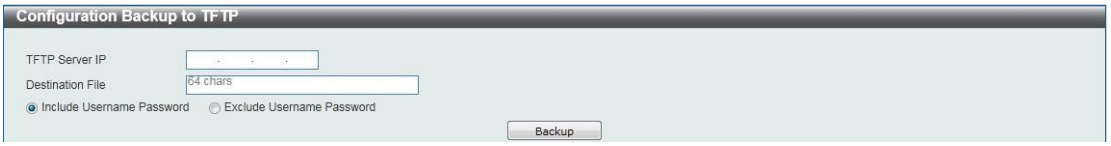


Figure 13-10 Configuration Backup to TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server.

Select **Include Username Password** to save the switch user accounts and passwords to the backup file.

Select **Exclude Username Password** to save the switch user accounts and passwords to the backup file.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

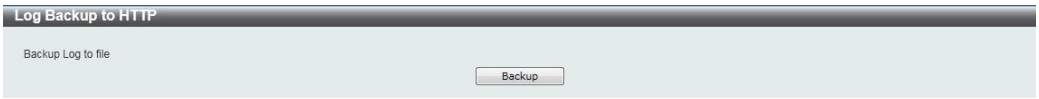


Figure 13-11 Log Backup to HTTP window

Click the **Backup** button to initiate the system log backup.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

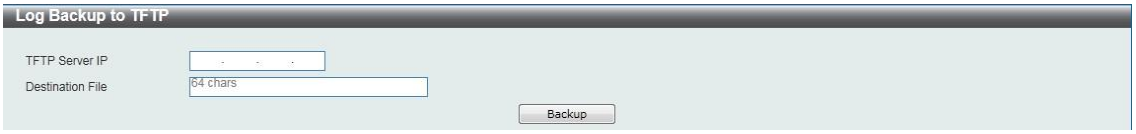


Figure 13-12 Log Backup to TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view the following window, click **Tools > Ping**, as shown below:

Figure 13-13 Ping window

The fields that can be configured for **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

Figure 13-14 Ping - IPv4 Ping Result window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Reset

This window is used to reset the Switch’s configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

Figure 13-15 Reset window

Select **The Switch will be reset to its factory defaults including IP address, and the will save, reboot** option to reset the Switch's configuration to its factory default settings.

Select **The Switch will be reset to its factory default except IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select **The Switch will be reset to its factory defaults including IP address** option to reset the Switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so. To view the following window, click **Tools > Reboot System**, as shown below:

Figure 13-16 Reboot System window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

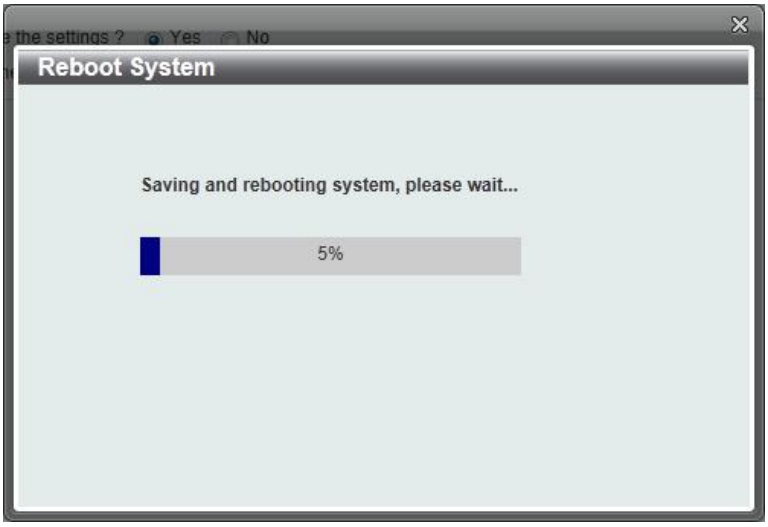


Figure 13-17 Reboot System - Rebooting window

14. Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link DGS-1100 Series Switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential to help solving network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection which will create a flexible foundation for the next generation of network technology products.

Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high-performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

15. Appendix B - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity:
  - DGS-1100-16V2 : 32Gbps
  - DGS-1100-24V2 : 48Gbps
  - DGS-1100-24PV2 : 48Gbps
  - DGS-1100-10MPV2 : 20Gbps
  - DGS-1100-10MPPV2 : 20Gbps
  - DGS-1100-26MPV2 : 52Gbps
  - DGS-1100-26MPPV2 : 52Gbps
  - DGS-1100-18PV2 : 36Gbps

- Max. Forwarding Rate:
  - DGS-1100-16V2 : 23.81Mpps
  - DGS-1100-24V2 : 35.71Mpps
  - DGS-1100-24PV2 : 35.71Mpps
  - DGS-1100-10MPV2 : 14.88Mpps
  - DGS-1100-10MPPV2 : 14.88Mpps
  - DGS-1100-26MPV2 : 38.69Mpps
  - DGS-1100-26MPPV2 : 38.69Mpps
  - DGS-1100-18PV2 : 26.784Mpps

- Forwarding Mode: Store and Forward
- Packet Buffer memory:
  - DGS-1100-16V2 : 4.1M bit
  - DGS-1100-24V2 : 4.1M bit
  - DGS-1100-24PV2 : 4.1M bit
  - DGS-1100-10MPV2 : 4.1M bit
  - DGS-1100-10MPPV2 : 4.1M bit
  - DGS-1100-26MPV2 : 4.1M bit
  - DGS-1100-26MPPV2 : 4.1M bit
  - DGS-1100-18PV2 : 4.1M bit

- Flash Memory: 16M Byte

Port Functions

- 10/100/1000BaseTX ports compliant with the following standards:
  - IEEE 802.3compliance
  - IEEE 802.3ucompliance
  - IEEE 802.3ab compliance
  - IEEE802.3at (Only DGS-1100-24PV2 、DGS-1100-10MPV2/ 10MPPV2/26MPV2/26MPPV2/18PV2)
  - IEEE802.3bt(OnlyDGS-1100-10MPPV2 /26MPPV2)
  - Supports Full/half-Duplex operations at 10/100Mbps
  - Supports Full-Duplex operation at 1000Mbps
  - Supports IEEE 802.3x Flow Control
  - Support Auto-Negotiation
  - Compliant to IEEE 802.3az Energy Efficiency Ethernet.

Physical & Environment

- DGS-1100-xxV2 : AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Operation Temperature: -5~50°C
- Storage Temperature: -40~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- BSMI

Safety Certifications

- UL, LVD, CB, BSMI
- CCC for DGS-1100-16V2/24V2/26PV2 only

Features

L2 Features

- DGS-1100-xxV2: 8K MAC address.
- Loopback Detection

- Port Mirroring
- Link Aggregation
- Cable Diagnostics
- Spanning Tree

L2 Multicasting

- IGMP Snooping

VLAN

- 802.1Q VLAN standard
- Port-Based VLAN
- Surveillance VLAN
- Voice VLAN:
- Asymmetric VLAN

QoS (Quality of Service)

- 802.1p priority,
- 8 queues
- Bandwidth Control

Security

- Storm Control
- DoS Attack Prevention
- SSL
- D-Link Safeguard

Management

- Web-based GUI or D-Link Network Assistant
- Configuration backup/restoration via Web-based management
- Firmware backup & upgrade via Web-based management
- Reset, Reboot system
- Factory reset by pressing reset button
- SNMP, LLDP, Dual Image, 2 level user account, SNTP

Power Saving

- IEEE 802.3az Compliant (Energy Efficient Ethernet)
- D-Link Green Technologies
  - Power saving by link status
  - Power Saving by LED Shut-Off:
  - Power Saving by Port Shut-Off
  - Power Saving by System Hibernation

16. Appendix C –Rack mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)

17. Appendix D–Trap Messages

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

Trap Name	OID	Description
newRoot	1.3.6.1.2.1.17.0.1	The trap is sent by a bridge soon after its election as the new root.
topologyChange	1.3.6.1.2.1.17.0.2	The trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.
coldStart	1.3.6.1.6.3.1.1.5.1	The trap is sent when the system coldStart.
warmStart	1.3.6.1.6.3.1.1.5.2	The trap is sent when the system warm start.
linkDown	1.3.6.1.6.3.1.1.5.3	The trap is sent by a bridge when an interface is link down. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus
linkUp	1.3.6.1.6.3.1.1.5.4	The trap is sent by a bridge when an interface is link up. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus
authenticationFailure	1.3.6.1.6.3.1.1.5.5	The trap is sent when the community isn't acceptable.
lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts
pethPsePortOnOffNotification	1.3.6.1.2.1.105.0.1	This Notification indicates if Pse Port is delivering ornot power to the PD. Binding objects: (1) pethPsePortDetectionStatus
pethMainPowerUs	1.3.6.1.2.1.105.0.2	This Notification indicate PSE Threshold

ageOnNotification		usageindication is on, the usage power is above thethreshold. Binding objects: (1) pethMainPseConsumptionPower
pethMainPowerUsageOffNotification	1.3.6.1.2.1.105.0.3	This Notification indicates PSE Threshold usage indicationoff, the usage power is below the threshold. Binding objects: (1) pethMainPseConsumptionPower
v1LbdLoopOccurred	1.3.6.1.4.1.171.11.170.1000.7.0.1	This trap is sent when an interface loop occurs. Binding objects: (1) v1LbdNotifyInfoIfIndex
v1LbdLoopRecovery	1.3.6.1.4.1.171.11.170.1000.7.0.2	This trap is sent when an interface loop recovery. Binding objects: (1) v1LbdNotifyInfoIfIndex
v1LldpExtDatabaseChanged	1.3.6.1.4.1.171.11.170.1000.8.0.1	This trap is sent when LLDP database changed.
v1PoeIfPdAliveFailOccurNotification	1.3.6.1.4.1.171.11.170.1000.11.0.1	This trap is sent when the PD device has the stop working or no response problem. Binding objects: (1) v1oeIfPdAliveCfgPdIpType (2) v1oeIfPdAliveCfgPdIpAddr

18. Appendix E–Syslog Messages

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

ZONEDEFENSE

Log Description	Severity
Event Description: Zone defense function has been enable/disable by SNMP. **Log Message**: ZONEDEFENSE: Zone defense function has been <status>by SNMP. **Parameters Description**: **Status**: enable or disable.	warning
Event Description: Zone defense function has been enable/disable by WEB **Log Message**: ZONEDEFENSE: Zone defense function has been <status>by WEB (Username:<Username>, IP:<IP>) **Parameters Description**: **Status** :enable or disable. **Username**: User Name **IP**:IP Address	warning

POE

Log Description	Severity
Event Description: port poe power switch to on/off. **Log Message:** **POE:** <port> poe power switch to <status>. **Parameters Description:** **Status:** on or off. **Port:**The port number.	INFO
Event Description:port poe power status change **Log Message:** **POE:** <port> poe power status change	INFO

Parameters Description: **Port:**The port number.	
Event Description: port detect pd-alive failed. **Log Message:** **POE:** <port>detect pd-alive failed. **Parameters Description:** **Port:**The port number.	INFO

STP

Log Description	Severity
Event Description: A port detect as half-duplex loop. **Log Message**: STP:<port>detect half-duplex loop, turn to Discarding. **Parameters Description**: **port**: The port number.	warning
Event Description: A port release half-duplex loop, initialize port state. **Log Message**: STP:<port> release half-duplex loop, initialize port state. **Parameters Description**: **port**: The port number.	warning
Event Description: STP queue is full, ignore timer tick message. **Log Message**: STP queue is full, ignore timer tick message. **Parameters Description**: None	warning
Event Description: Port becomes Backup port. **Log Message**: STP:STP detect loop,<port> becomes Backup port,turns to Discarding. **Parameters Description**: **port**: The port number.	warning

Event Description: Max-age timer expired. **Log Message**: STP: Max-age timer expired<port>, role <port role>Designated. **Parameters Description**: **port**: The port number. **port role: The** port role.	warning
Event Description: Set port State to hardware failed. **Log Message**: STP: Set <port><port state> to hardware failed. **Parameters Description**: **port**: The port number. **port state**: The STP Port State	warning
Event Description: At the time of STP detection, the port receives the RX BPDU, turn to Discarding. **Log Message**: STP:STP detect loop<port> Rx BPDU sent by itself, turn to Discarding. **Parameters Description**: **port**: The port number.	warning
Event Description: Not detected Collisions at port. **Log Message**: STP :Not detected Collisions at port <port>.Release the loop-back. **Parameters Description**: **port**: port number.	warning
Event Description: TC protection for this port is in effect. **Log Message**: STP:<port> TC Protection take into effect. **Parameters Description**: **port**: The port number.	INFO
Event Description: Discard the old root port. **Log Message**: STP: Old Root port <port> turn to Discarding.	INFO

Parameters Description: **port**: The port number.	
Event Description: Alternate port become Root port. **Log Message**: STP: Alternate port <port>become Root port, turn to Forwarding. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port TC Protection return to normal, flush ARL(Address Resolution Logic). **Log Message**: STP:<port> TC Protection return to normal, flush ARL(Address Resolution Logic). **Parameters Description**: **port**: The Port number.	INFO
Event Description: Selected the Root bridge. **Log Message**: STP:<priority><MAC> is selected as Root bridge. **Parameters Description**: **Priority**: Designate Root Priority. **MAC**: Designate Root MAC Address.	INFO
Event Description: Port Rx TC BPDU. **Log Message**: STP:<port> Rx TC BPDU. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port Rx TCN BPDU. **Log Message**: STP:<port> Rx TCN BPDU. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port Rx BPDU, change from Edge to Non-Edge. **Log Message**: STP:<port> Rx BPDU, change from Edge to Non-Edge.	INFO

Parameters Description: **port**: The port number.	

DEVICE

Log Description	Severity
Event Description: Port abnormal. **Log Message**: DEVICE: port <port> abnormal. **Parameters Description**: **port**: The port number.	INFO
Event Description: The port recover. **Log Message**: DEVICE: The port <port> recover. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port flow normal. **Log Message**: DEVICE: Port <port> flow normal. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port flow exceed. **Log Message**: DEVICE: Port <port> flow exceed. **Parameters Description**: **port**: The port number.	INFO
Event Description: Port LinkUp. **Log Message**: DEVICE:<port> LinkUp. **Parameters Description**: **port**: The port number.	warning
Event Description: Port Error-LinkDown.	warning

Log Message: DEVICE:<port> Error-LinkDown. **Parameters Description**: **port**: The port number.	
Event Description: Port LinkDown. **Log Message**: DEVICE:<port> LinkDown. **Parameters Description**: **port**: The port number.	warning
Event Description: Power-saving linkdetect(all ports) Log Message: DEVICE: power-saving linkdetect, status =<status>, ret = <result> **Parameters Description**: **status:** saving or no-saving. **result**：function return value.	INFO
Event Description: Power-saving linkdetect(only one port) Log Message: DEVICE: power-saving linkdetect from <port>, status =<status>, ret = <result> **Parameters Description**: **port**: The port number. **status:** saving or no-saving. **result**：function return value.	INFO
Event Description: Power-saving hibernation **Log Message:** DEVICE:power-saving hibernation status = <status>, ret = <result> **Parameters Description:** **status**: saving or no-saving **result:**function return value	INFO
Event Description: Power-saving dim led **Log Message:** DEVICE:power-saving dim led status = <status>, ret = <result> **Parameters Description:** **status**: saving or no-saving	INFO

result：function return value	
Event Description:power-saving port shutdown(only one port) **Log Message:** DEVICE:power-saving port-shutdown from <port> status = <status>, ret = <result> **Parameters Description:** **port**: The port number. **status**: saving or no-saving. **result**：function return value.	INFO
Event Description:power-saving port shutdown(all port) **Log Message:** DEVICE:power-saving port-shutdown status = <status>, ret = <result> **Parameters Description:** **status**: saving or no-saving. **result**：function return value .	INFO
Event Description:power-timeRange(only one port) **Log Message:** DEVICE:power-timeRange from <port> status = <status>, ret = <result> **Parameters Description:** **port**: The port number. **status**: power-on or power-off. **result**：function return value	INFO
Event Description:power-timeRange(all port) **Log Message:** DEVICE:power-timeRange status = <status>, ret = <result> **Parameters Description:** **status**: power-on or power-off. **result**：function return value .	INFO
Event Description:power-control(only one port) **Log Message:** DEVICE:power-control from <port>, status = <status>, ret = <result>	INFO

Parameters Description: **port**: The port number. **status**: power-on or power-off. **result**：function return value .	
Event Description:power-control(all port) **Log Message:** DEVICE:power-control status = <status>, ret = <result> **Parameters Description:** **status**: power-on or power-off. **result**：function return value .	INFO

LBD

Log Description	Severity
Event Description: LBD detect loop and discarding port. **Log Message**: LBD:LBD detect loop [Tx <port1>, Rx <port2>,vid <id>], Discarding <port3> **Parameters Description**: **port1**:TX port number. **port2**:RX port number. **port3**:Discarding port number. **id**: The vlan number of the port.	warning
Event Description: LBD detect loop and shutdown port. **Log Message**: LBD:LBD detect loop [Tx <port1>, Rx <port2>,vid <id>], Shutdown <port3>. **Parameters Description**: **port1**:TX port number. **port2**:RX port number. **port3**:Shutdown port number. **id**: The vlan number of the port.	warning
Event Description: LBD detect loop and just send log and trap. **Log Message**:	warning

LBD:LBD detect loop [Tx <port1>, Rx <port2>,vid <id>]. **Parameters Description**: **port1**:TX port number. **port2**:RX port number. **id**: The vlan number of the port.	
Event Description: LBD port auto recover **Log Message**: LBD:<port> vid <vid> AutoRecover timer expired, recover from LBD loop. **Parameters Description**: **port**: The port number. **id**: The vlan number of the port.	warning
Event Description: Send trap after LBD detect loop **Log Message**: LBD:come in send trap	warning

SYSLOG

Log Description	**Severity**
Event Description: Port reach learning limit. **Log Message**: SYSLOG:<port> reach learning limit. **Parameters Description**: **port**: The port number.	warning

LLDP

Log Description	Severity

Event Description: Delete information about neighbor devices. **Log Message**: LLDP: Delete neighbor entry<index> of port <port>. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: Update Neighbor Table Items. **Log Message**: LLDP: Update neighbor entry<index> of port <port>. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: Failed to delete neighbor table entries. **Log Message**: LLDP: Fail to delete neighbor entry <index> of port <port>. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: Successful deletion of neighbor entries. **Log Message**: LLDP: Delete neighbor entry <index> of port <port> successfully. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: Creating Port Neighbor Table Items. **Log Message**: LLDP: Create neighbor entry <index> of port <port>. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: Port application for idle neighbor entry failed. **Log Message**: LLDP_fail: Port <port> get free neighbor entry failed.	warning

Parameters Description: **port**: The port number.	
Event Description: Port Application Memory Failure. **Log Message**: LLDP: Memory application failed for <port>. **Parameters Description**: **port**: The port number.	warning
Event Description: LLDP task queue is full. **Log Message**: LLDP:LLDP task queue is full. **Parameters Description**: None	warning
Event Description: Aging of Neighbor Table Items. **Log Message**: LLDP: Neighbor entry<index> of port <port> has been time out. **Parameters Description**: **index**: Neighbor Table Item Index. **port**: The port number.	warning
Event Description: LLDP send disconnect frame **Log Message**: LLDP: Port <port> send a shutdown LLDP message. **Parameters Description**: **port**: The port number.	warning
Event Description: LLDP local system setting have changed **Log Message**: LLDP: Local Management Address has changed. **Parameters Description**:	warning
Event Description: LLDP local system setting have changed **Log Message**: LLDP: VLAN ID of Port <port> has changed **Parameters Description**:	warning

port: The port number.	
Event Description: LLDP local system setting have changed **Log Message**: LLDP: Link aggregation of Port <port> has changed **Parameters Description**: **port**: The port number.	warning
Event Description: LLDP local system setting have changed **Log Message**: LLDP: MAC PHY status of Port <port> has changed **Parameters Description**: **port**:The port number.	warning
Event Description: LLDP local system setting have changed **Log Message**: LLDP: Port <port> Description has changed **Parameters Description**: **port**: The port number.	warning
Event Description: LLDP local system setting have changed **Log Message**: LLDP: Local sysName has changed **Parameters Description**:	warning

LACP

Log Description	Severity
Event Description: Create eth-trunk message ,group id is invalid. **Log Message**: LACP: Create eth-trunk message ,Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Cancel eth-trunk message ,group Id is invalid. **Log Message**: LACP: Cancel eth-trunk message ,Id =<group id> is invalid.	warning

Parameters Description: **Group id**: The group id.	
Event Description: Cancel eth-trunk, group Id is not active. **Log Message**: LACP: Cancel eth-trunk, group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Add eth-trunk member ,group Id is invalid. **Log Message**: LACP: Add eth-trunk member ,group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Add eth-trunk member ,port Id is invalid. **Log Message**: LACP: Add eth-trunk member ,port Id =<port> is invalid. **Parameters Description**: **Port**: The port number.	warning
Event Description: Add eth-trunk member, port Id is already in LAG. **Log Message**: LACP: Add eth-trunk member, port Id =<port> is already in LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Add eth-trunk member, port Idis half duplex. **Log Message**: LACP: Add eth-trunk member, port Id =<port>is half duplex. **Parameters Description**: **Port**: The port number.	warning
Event Description: Add eth-trunk member, get port Id speed error. **Log Message**: LACP :Add eth-trunk member, get port Id =<port> speed error.	warning

Parameters Description: **Port**: The port number.	
Event Description: Add eth-trunk member, get port Id VLAN mode or pvid error. **Log Message**: LACP :Add eth-trunk member, get port Id =<port> VLAN mode or pvid error. **Parameters Description**: **Port**: The port number.	warning
Event Description: Add eth-trunk member, get port Id VLAN info error. **Log Message**: LACP: Add eth-trunk member, get port Id =<port> VLAN info error. **Parameters Description**: **Port**:The port number.	warning
Event Description: Add eth-trunk member ,the total ports of LAG is full now. **Log Message**: LACP: Add eth-trunk member ,the total ports of LAG<group id> is full now. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Add eth-trunk member ,speed of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,speed of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Spanning tree path cost judgment. **Log Message**: LACP :Add eth-trunk member ,stp path cost of port <port>(<cost>) does not correspond to LAG:<group id>(<cost>). **Parameters Description**:	warning

Port: The port number. **Cost**: The port path cost. **Group id**: The group id . **Cost**: The stp path cost.	
Event Description: Add eth-trunk member, stp protocol of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,stp protocol of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Add eth-trunk member ,stp priority of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,stp priority of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**:The port number. **Group id**: The group id.	warning
Event Description: Add eth-trunk member ,pvid of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,pvid of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: The Add eth-trunk member ,trunk/access of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,trunk/access of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Add eth-trunk member, VLAN-list of port does	warning

not correspond to LAG. **Log Message**: LACP: Add eth-trunk member , VLAN-list of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id** :group id.	
Event Description: Add eth-trunk member ,loopback-detection protocol of port does not correspond to LAG. **Log Message**: LACP: Add eth-trunk member ,loopback-detection protocol of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Add member ,input port has no same multicast as LAG. **Log Message**: LACP: Add member ,multicast entry of port <port> does not correspond to LAG<group id>. **Parameters Description**: **Port**: The port number. **Group id**: The group id.	warning
Event Description: Query eth-trunk member ,group Id is invalid. **Log Message**: LACP: Query eth-trunk member ,group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Delete eth-trunk member ,group Id is invalid. **Log Message**: LACP: Delete eth-trunk member ,group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Get port lacp mode, port Id is invalid. **Log Message**: LACP: Get port LACP mode, port Id =<port> is invalid.	warning

Parameters Description: **Port**: The port number.	
Event Description: Set port LACP mode, port Id is invalid. **Log Message**: LACP: Set port LACP mode, port Id =<port> is invalid. **Parameters Description**: **Port**: The port number.	warning
Event Description: Renew trunk hardware table failed. **Log Message**: LACP: Renew trunk hardware table failed. **Parameters Description**: None.	warning
Event Description: Getting port belong to which ag, port Id is invalid. **Log Message**: LACP: Get port belong to which ag, port Id =<port> is invalid. **Parameters Description**: **Port**: The port number.	warning
Event Description: Get the brother of a port ,port Id is invalid. **Log Message**: LACP: Get the brother of a port ,port Id =<port> is invalid. **Parameters Description**: **Port**:The port number.	warning
Event Description: Reconfiguring eth-trunk, group Id is invalid. **Log Message**: LACP: Reconfigure eth-trunk, group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: Reconfigure eth-trunk, group Id is not active. **Log Message**: LACP: Reconfigure eth-trunk, group Id =<group id> is not active.	warning

Parameters Description: **Group id**: The group id.	
Event Description: Reconfigure eth-trunk, get port Id speed error. **Log Message**: LACP: Reconfigure eth-trunk, get port Id =<port> speed error. **Parameters Description**: **Port**: The port number.	warning
Event Description: Reconfigure eth-trunk, get port Id VLAN mode or pvid error. **Log Message**: LACP: Reconfigure eth-trunk, get port Id =<port> VLAN mode or pvid error. **Parameters Description**: **Port**: The port number.	warning
Event Description: Reconfigure eth-trunk, get port Id vlan info error. **Log Message**: LACP: Reconfigure eth-trunk, get port Id =<port> VLAN info error. **Parameters Description**: **Port**: The port number.	warning
Event Description: Reconfigure eth-trunk, config code is invalid. **Log Message**: LACP: Reconfigure eth-trunk, config code =<code> is invalid. **Parameters Description**: **Code**: The code.	warning
Event Description: Lacp failed notify ,group Id is invalid. **Log Message**: LACP: Lacp failed notify ,group Id =<group id> is invalid. **Parameters Description**: **Group id**: The group id.	warning
Event Description: The group Id is not active. **Log Message**: LACP: Lacp failed notify ,group Id =<group id> is not active.	warning

Parameters Description: **Group id**: The group id.	
Event Description: LACP receive message to shutdown port, port Id is invalid. **Log Message**: LACP: LACP receive message to shutdown port, port Id =<port> is invalid. **Parameters Description**: **Port**: The port number.	warning
Event Description: The port Id is invalid. **Log Message**: LACP :LACP receive message to no shutdown port, port Id =<port> is invalid. **Parameters Description**: **Port**: The port number.	warning
Event Description: getting port ID error failed.. **Log Message**: LACP: eth-trunk port=<port> link up, and ID is not valid. **Parameters Description**: **Port**: The port id .	warning
Event Description:getting port speed failed.. **Log Message**: LACP: eth-trunk port=<port> link up, Error returning invalid data read. **Parameters Description**: **Port**: The port number.	warning
Event Description: Speed compatibility judgment. **Log Message**: LACP: eth-trunk port=<port> link up ,but speed does not correspond to LAG<channel index>. **Parameters Description**: **Port**: The port number. **Channel index**: The channel index.	warning
Event Description: Spanning tree paths cost compatibility determination.	warning

Log Message: LACP: Lac port=<port> link up ,but stp port path cost(<cost>) does not correspond to LAG<channel index>(<group id>). **Parameters Description**: **Port**: The port number. **Cost**: spanning tree path cost. **Channel index**: channel index. **Group id**: The group id.	
Event Description: Set LACP period Failed **Log Message**: LACP: Set LACP period Failed. **Parameters Description**: None.	warning
Event Description: The channel id is full. **Log Message**: LACP: The channel <channel index> is full in hardware now,can not add more port into it. **Parameters Description**: **Channel index**: channel Index.	warning

System

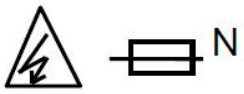
Log Description	Severity
Event Description: System Hot Start. **Log Message**: SYS: System WarmStart. **Parameters Description**: None.	warning
Event Description: System Cold Start. **Log Message**: SYS: System ColdStart. **Parameters Description**: None.	warning

Voice vlan

Log Description	Severity
Event Description: Add Voice Vlan Device **Log Message**: VOICEVLAN: Add device in <port> <(mac address)>. **Parameters Description**: **Port**: The port number. **MacAddr :** Device's source MAC Address	INFO
Event Description: Delete Voice Vlan Device **Log Message**: VOICEVLAN: Delete device in <port> <(mac address)>. **Parameters Description**: **Port**: The port number. **Mac address :** Device's source MAC Address	INFO
Event Description: Device MAC address will overwrite . **Log Message:** EVENT:Device [MACAddr] will over write (Port id:[PortNum],original vlan id:[VIDRang]) . **Parameters Description:** **PortNum:**Port number range . **VIDRang:**VLAN ID range.	INFO

Surveillance vlan

Log Description	Severity
Event Description: Surveillance vlan add device. **Log Message**: SURVEILLANCEVLAN:Add device in <port> (<MAC Address>). **Parameters Description**: **port**: port number **MAC Address**: mac address	INFO
Event Description: Surveillance vlan delete device. **Log Message**: SURVEILLANCEVLAN:Delete device in <port> (<MAC Address>). **Parameters Description**: **port**: port number **MAC Address**: mac address	INFO
Event Description: Device MAC address will overwrite . **Log Message**: SURVEILLANCEVLAN:Device <MACAddr> will overwrite [Port id: <port1>--><port2>, Original vlan id : <Vid1>--><Vid2>]. **Parameters Description:** **MACAddr:**Device's source MAC Address . **Port1**:the old port number. **Port2**:the new port number. **Vid1**:the old vlan id. **Vid2**:the new vlan id.	INFO



Fuse is in the neutral, and that the mains shall be disconnected to de-energize the phase conductors.

CAUTION

DOUBLE POLE/NEUTRAL FUSING

Attention
Fusion bipolaire / neutre