High Availability Network for Critical Communications on Smart Grids

Milton Ruiz
GIREI-UPS
mruizm@ups.edu.ec

Paul Masache
GIREI-UPS
pmasache@ups.edu.ec

Juan Dominguez
GIETEC-UPS
jdominguez@ups.edu.ec

***Abstract*—This paper presents the configuration and the infrastructure for the development of a high availability network with critical communications used in Smart Grids (SM). The local area network (LAN) has been designed by 3 layer switches with Virtual Switching Systems (VSS) and Gateway Load Balancing Protocol (GLBP) configuration, the border routers are configured with Hot Standby Router Protocol (HSRP). The Wide Area Network (WAN) has been designed over a Multiprotocol Label Switching (MPLS) network and Dynamic Multipoint Virtual Private Network (DMVPN) has been configured with encrypted communications.**

***Index Terms*—DMVPN, OSPF, EIGRP, GLBP, HSRP, VSS, Smart Grid.**

I. Introducción

Los sistemas eléctricos presentan las redes de mayor despliegue a nivel mundial, la conciencia ecológica ha permitido evolucionar a las redes eléctricas inteligentes agrupando a numerosos sistemas y subsistemas interconectados con la finalidad de brindar seguridad, confiabilidad, vida útil, interoperabilidad, rentabilidad, consumo mínimo de energía, bajos costos de instalación y mantenimiento para suministrar energía eléctrica respondiendo al crecimiento de la demanda. La integración de energías renovables a gran escala plantean nuevos requerimientos de comunicaciones de alta disponibilidad permitiendo que la información sea procesada por los sistemas de cómputo, monitoreo y centros de control dando respuesta al problema de la generación de energía en tiempo real, para lo cual es indispensable comunicaciones bidireccionales entre los abonados del sector eléctrico y las centrales de generación a cientos he incluso miles de kilómetros.
La operación y confiabilidad de las redes eléctricas inteligentes involucran comunicaciones por medios alámbricos como la fibra óptica y por medios inalámbricos utilizando enlaces de radio o comunicaciones satelitales para los equipos críticos de protecciones desplegados en las redes[1].

Wide Area Network (WAN), está comprendida por la red de backbone, Metropolitan Area Network (MAN) y la red de backhaul. La red de backbone proporciona altas velocidades de comunicación y baja latencia comunicando a las subestaciones generalmente utilizando fibra óptica. La red MAN conecta las redes de backhaul en grandes ciudades o regiones metropolitanas. La red de backhaul es el enlace entre WAN y Neighborhood Area Network (NAN), proporciona conectividad de banda ancha a la red NAN. El principal servicio que presta la red WAN es el transporte de datos fiables, manteniendo la privacidad y seguridad de la información por toda la red eléctrica inteligente permitiendo la operación de todos los sistemas. La privacidad, fiabilidad y seguridad de la información son los principales aspectos que se evalúan en la red WAN.

El artículo está organizado de la siguiente manera. En la sección II, se describen los parámetros de diseño. En la sección III, se diseña la red. En la sección IV, se presentan los resultados de la simulación. Finalmente en la sección V se presentan las conclusiones.

II. Parámetros de Diseño

Para trabajar con conexiones entre las diferentes Local Area Network (LAN) que componga la infraestructura tecnológica de una organización o de una red de condiciones y características globales es necesario el uso de tecnologías de comunicaciones de área extendida WAN brindando respuesta a los requerimientos de comunicación sin afectar el rendimiento, seguridad o confiabilidad. Las alternativas de comunicación WAN se pueden clasificar en privadas (uso de recursos mediante un proveedor de servicios, ejemplo enlaces de datos arrendados dedicados) y públicas (uso de Internet a través de recursos de banda ancha, ejemplo Virtual Private Networks (VPN)).
En el protocolo OSPF cuando la cantidad de equipos enrutadores aumenta en la red de datos, las buenas prácticas de diseño recomienda la reducción del número de enrutadores por área para reducir el intercambio de los mensajes Link State Advertisement (LSA). Para reducir el intercambio de LSA en la red, se implementa OSPF en su modalidad de múltiple área que reduce el consumo de recursos de infraestructura tecnológica y de ancho de banda.

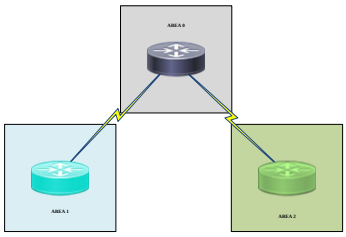

Fig. 1. OSPF Multiárea

In: Proceedings of the IV School of Systems and Networks (SSN 2018), Valdivia, Chile, October 29-31, 2018. Published at http://ceur-ws.org

La implementación de OSPF múltiple área o multiárea se puede resumir en cuatro procesos:
Recopilación de requisitos de red: Esta fase depende del resultado del establecimiento de la línea base de la red que permite conocer los requisitos y tamaño de la infraestructura.
Definición de parámetros de OSPF: Del resultado obtenido en el primer proceso se decide si la implementación de OSPF será la convencional de o la de multiárea (direccionamiento IP, número de áreas, topología, etc.).
Configuración de OSPF: Configuración de OSPF multiárea según parámetros y las necesidades de la red.
Verificación de la configuración de OSFP: Validación de la configuración según las necesidades y parámetros de la red.
La operación de OSPF multiárea hace que la operación de OSPF se segmente dentro de cada área que se ha creado y si existe la necesidad de enviar tráfico entre las áreas esta pasa en condiciones resumidas con procesos de sumarización para ahorrar el consumo de ancho de banda al transitar por el área de backbone que es el área 0. Cada equipo cumple un rol en cada área y tienen una propia nomenclatura.
El diferenciador para la elección de implementación de los protocolos EIGRP y OSPF es básicamente la marca de los equipos enrutadores que compondrán la red en la implementación de los diseños. Las mejores prácticas proponen diseños de inclusión de múltiples fabricantes y la ejecución de estándares que sean soportados por todos los dispositivos.
La tecnología DMVPN es una solución de Cisco para la creación dinámica de VPN. DMVPN utiliza una arquitectura centralizada para simplificar la gestión y reducir significativamente la complejidad para su implementación permitiendo que las sucursales se comuniquen directamente entre sí a través de la WAN privada o pública mejorando el rendimiento de la red al reducir la latencia, optimizando el uso del ancho de banda.

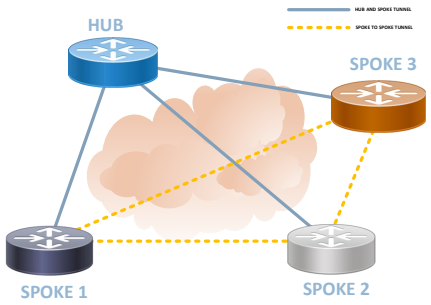

Fig. 2. Esquema de implementación de DMVPN

Los componentes básicos de DMVPN son:
Multipoint Generic Routing Encapsulation (mGRE) Tunnels: Es la configuración que permite a una interfaz túnel GRE admita múltiples túneles ayudando a reducir la complejidad y la cantidad de configuraciones en la implementación.
Next Hop Resolution Protocol (NHRP): Es un protocolo de capa de enlace de datos utilizado para mapear dinámicamente una dirección IP a la interfaz de los otros sistemas que forman parte de la red, permitiendo que estos sistemas se comuniquen directamente.
Enrutamiento dinámico: Los protocolos de enrutamiento dinámico soportados por DMVPN son Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP).
IPSec: Es el protocolo que asegura la comunicación, la implementación no es obligatorio y es compatible con el túnel IPsec IKE.
Cisco Express Forwarding (CEF): Con soporte de enrutamiento virtual y Virtual Routing and Forwarding (VRF) en los concentradores para segregar el tráfico de clientes.
La figura 3 muestra el esquema de red WAN utilizando DMVPN.

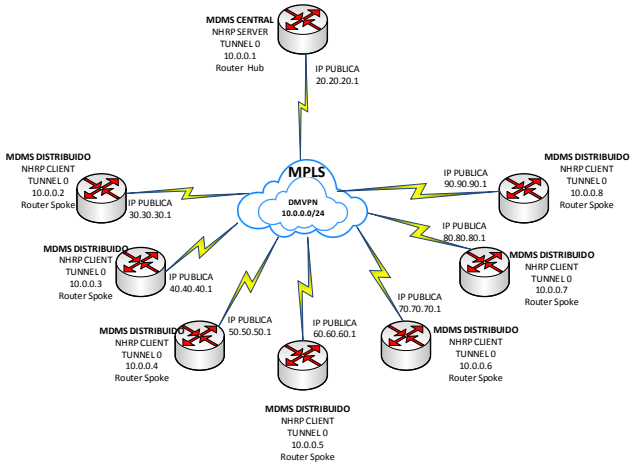

Fig. 3. Red WAN con DMVPN

La arquitectura DMVPN se basa en la implementación de Hub y Spoke. El Hub representa el nodo central de la red y spoke es una ubicación remota. La principal ventaja de la solución DMVPN consiste en la creación de enlaces privados entre spokes bajo demanda sin enrutar todo el tráfico a través del Hub. DMVPN representa una tecnología de túneles dinámicos y escalables punto multipunto permitiendo la comunicación directa entre sucursales sin requerir una conexión VPN permanente[2], [3] DMVPN se puede implementar en la red del Internet service provider (ISP) o en redes WAN privadas. Con DMVPN, el usuario final puede tener túneles de sitio a sitio en sus dispositivos y no necesita tener acceso a internet del mismo proveedor en las diferentes áreas regionales, solo se requiere un acceso a Internet estándar. Las características principales del protocolo DMVPN son creación de rutas dinámicas sobre VPN, sobrecarga de configuración reducida, Network Address Translation (NAT) Traversal, soporte para tráfico IP de multidifusión, soporte avanzado de QoS (Quality of Service), escalabilidad, alta disponibilidad y soporte sobre Multiprotocol Label Switching (MPLS)[4], [5], [6]. La red de frontera está constituida por dos routers firewall comunicados mediante GLBP permitiendo balancear las cargas y en caso de falla de uno de los equipos el router activo posee la capacidad para enrutar todo el tráfico generado.

III. Diseño de Red

Con la finalidad de garantizar alta disponibilidad, confiabilidad y seguridad de las comunicaciones entre las empresas eléctricas y el centro de control de energía. La red de comunicaciones WAN ha sido diseñada bajo una arquitectura centralizada fácil de implementar y gestionar conocida como DMVPN, esta solución crea redes privadas virtuales seguras y escalables.

Es necesario diseñar la arquitectura de comunicaciones de forma distribuida y escalable, permitiendo que la infraestructura de medición avanzada se integre a las redes eléctricas inteligentes mediante el uso de redes celulares como tecnología de comunicación entre los medidores y las empresas eléctricas. Fibra óptica como medio de comunicación entre las empresas eléctricas y el centro de control de energía[7].

La figura 4 muestra el modelo del Meter Data Management System (MDMS) totalmente distribuido que representa una red de comunicaciones a nivel nacional. Cada provincia o estado cuenta con un sistema MDMS distribuido que reciben los datos de sus abonados y son enviados a un MDMS central.

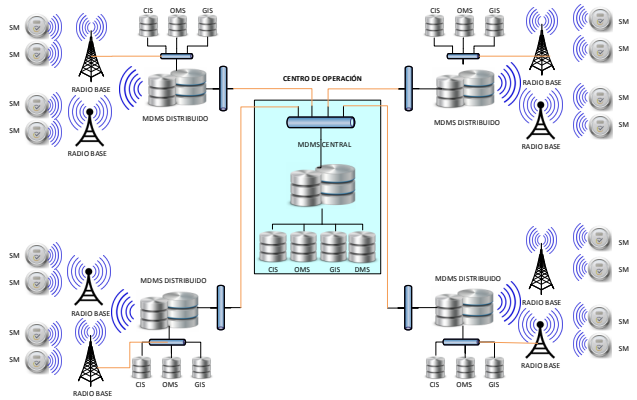

Fig. 4. Arquitectura de comunicación en redes inteligentes

En la arquitectura de comunicación totalmente distribuida en redes inteligentes, existen múltiples MDMS desplegados a nivel nacional, cada MDMS se encarga del procesamiento y almacenamiento de información proporcionada por los medidores inteligentes de cada región. Al implementar arquitecturas distribuidas se optimiza el ancho de banda en las comunicaciones ya que se reduce la cantidad de datos a transmitir a una arquitectura centralizada. La información efectiva por cada provincia son los datos depurados que han sido procesados por cada uno de los MDMS, ya que sólo una pequeña parte de los datos es necesaria para los servicios de operación y gestión.

Con la finalidad de brindar confiabilidad en la red interna es necesario dos equipos de core conectados mediante VSS gestionando la conmutación de paquetes entre los equipos permitiendo alta disponibilidad y fiabilidad de las comunicaciones entre los servidores internos.

Los dispositivos de acceso deben permitir la creación de redes lógicas o VLANs con la finalidad de seccionar los dominios de difusión y garantizar permisos de acceso a servidores en la red interna dependiendo de permisos con la creación de ACLs.

La figura 5 muestra el diseño de la red de comunicaciones para aplicaciones críticas.

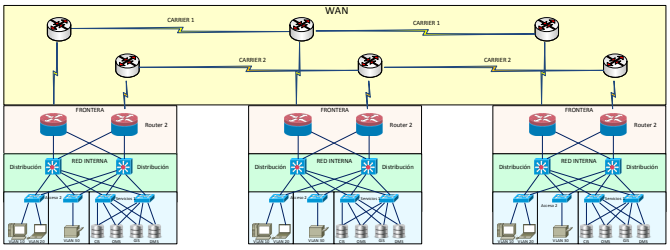

Fig. 5. Diseño de red de alta disponibilidad

Se evidencia las características propuestas de escalabilidad de la red y las condiciones que la hace tolerante a fallos a través de la disminución de los puntos de falla simple y la inclusión de la tecnología para la creación de VPN dinámicas DMVPN.

IV. Simulación

A continuación se presenta los resultados del diseño de red de frontera y de la red local de las empresas eléctricas. Por la criticidad de los datos se ha diseñado una arquitectura de red de alta disponibilidad, para lo cual es necesario de dos proveedores de servicios de telecomunicaciones, dos routers de frontera configurados con HSRP y dos dispositivos de core configurados con VSS y GLBP con la finalidad de balacear el tráfico.

La figura 6 muestra la topología física de la red al igual que la distribución del direccionamiento ip.

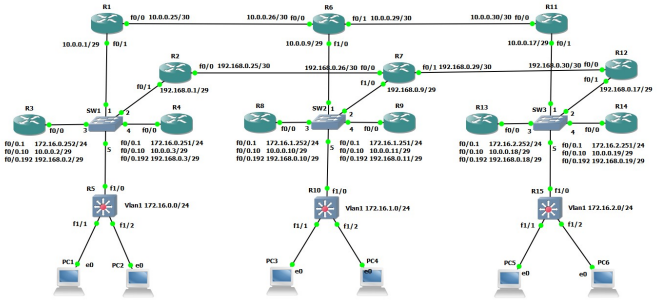

Fig. 6. Red WAN con DMVPN

DMVPN proporciona una malla completa entre todos los nodos actores de la red permitiendo reconfiguraciones de las rutas dinámicamente en caso de que una ruta no se encuentre activa. DMVPN reemplaza las rutas estáticas por el protocolo de enrutamiento dinámico EIGRP. DMVPN consta de un equipo central denominado HUB que se encarga de levantar VPNs de forma dinámica y posee la información de enrutamiento de los demás equipos de la red denominados SPOKES.

Si el equipo central conocido como HUB pierde comunicación con sus SPOKES las redes privadas virtuales dejan de

comunicarse. Para preservar las comunicaciones activas es necesario un segundo proveedor de servicios, el mismo que brindará redundancia en una segunda infraestructura de comunicaciones basada en DMVPN.

OSPF es el protocolo de enrutamiento configurado entre los proveedores de servicios y como red de acceso se ha configurado MPLS simulando una red real que es utilizada en la actualidad por los ISPs.

EIGRP es el protocolo de enrutamiento utilizado entre los routers de frontera de cada empresa.

A continuación se presentan los datos de los comandos de verificación propios de DMVPN. La respuesta al comando *show ip nhrp*, muestra las entradas de caché de IP Next Hop Resolution Protocol. Se puede identificar las rutas establecidad, los tiempos de expiración de los tuneles y si los mismos son estáticos o dinámicos.

ROUTER # : *show ip nhrp*
10.1.1.2/32 via 10.1.1.2
. Tunne1100 created 2w6d, expire 01:43:45
. Type: dynamic, Flags: unique registered used nhop NBMA
. address: 10.0.0.46
10.1.1.3/32 via 10.1.1.3
. Tunne1100 created 2w6d, expire 01:33:02
. Type: dynamic, Flags: unique registered used nhop NBMA
. address: 10.0.0.2
10.1.1.4/32 via 10.1.1.4
. Tunne1100 created 2w6d, expire 01:41:05
. Type: dynamic, Flags: unique registered used nhop NBMA
. address: 192.168.29.254
10.1.1.5/32 via 10.1.1.5
. Tunne1100 created 2w6d, expire 01:49:56
. Type: dynamic, Flags: unique registered used nhop NBMA
. address: 172.16.1.5
10.1.1.6/32 via 10.1.1.6
. Tunne1100 created 2w6d, expire 00:09:01
. Type: dynamic, Flags: unique registered used nhop NBMA
. address: 172.18.95.5
10.2.2.1/32 via 10.2.2.1
. Tunnel200 created 2w6d, never expire
. Type: static, Flags: used NBMA address: 172.16.1.1

A continuación se presenta la respuesta al comando *show ip nhrp traffic*, se muestra la información estadística del tráfico de nhrp que cursan por las interfaces túneles creadas por DMVPN

ROUTER # : *show ip nhrp traffic*
Tunne1100: Max-send limit:100Pkts/10Sec, Usage:0%
. Sent: Total 12010
. 15 Resolution Request 0 Resolution Reply
. 0 Registration Request 11961 Registration Reply
. 14 Purge Request 14 Purge Reply 6 Error
. 0 Traffic Indication 0 Redirect Suppress
. Rcvd: Total 12010
. 21 Resolution Request 0 Resolution Reply
. 11961 Registration Request 0 Registration Reply
. 14 Purge Request 14 Purge Reply 0 Error
. 0 Traffic Indication 0 Redirect Suppress
Tunne1200: Max-send limit:100Pkts/10Sec, Usage:0%
. Sent: Total 5475
. 3667 Resolution Request 1052 Resolution Reply
. 756 Registration Request 0 Registration Reply
. 0 Purge Request 0 Purge Reply 0 Error
. 0 Traffic Indication 0 Redirect Suppress
. Rcvd: Total 5228
. 1052 Resolution Request 3428 Resolution Reply
. 0 Registration Request 748 Registration Reply
. 0 Purge Request 0 Purge Reply 0 Error
. 0 Traffic Indication 0 Redirect Suppress

A continuación se presenta la respuesta al comando *show ip nhrp nhs detail*, se muestra en detalle el tiempo de espera del protocolo NHRP de DMVPN.

ROUTER # : *show ip nhrp nhs detail*
Tunnel200:
. 10.2.2.1 RE priority = 0 cluster = 0 req-sent 756 req-failed
. 0 repl-recv 748 (00:38:31 ago)

Finalmente se muestra la salida de las interfaces creadas dinámicamente por el protocolo DMVPN a través de la ejecución del comando *show dmvpn detail*.

ROUTER # : *show dmvpn detail*
Interface Tunne1100 is up/up, Addr. is 10.1.1.1, VRF
. Tunnel Src./Dest. addr: 10.0.0.22/MGRE, Tunnel VRF
. Protocol/Transport: "multi-GRE/IP", Protect "PROFILE"
. Interface State Control: Disabled
. nhrp event-publisher : Disabled
. Type.Hub, Total NBMA Peers (v4/v6): 5

Peer NBMA	Peer Tunnel	State	UpDn	Target Network
. 10.0.0.46	10.1.1.2	UP	2w6d	10.1.1.2/32
. 10.0.0.2	10.1.1.3	UP	2w6d	10.1.1.3/32
. 172.16.1.5	10.1.1.5	UP	2w6d	10.1.1.5/32
. 172.18.95.5	10.1.1.6	UP	2w6d	10.1.1.6/32
.192.168.29.254	10.1.1.4	UP	2w6d	10.1.1.4/32

V. Conclusiones

El tráfico encriptado con IPSec puede ocacionar retardos en la red debido a que en primera instancia el Hub debe desencriptar la información, verificar el destino y crear el tunel DMVPN.

El análisis de rendimiento realizado, nos permite determinar cuál de los protocolos de enrutamiento utilizados para la conexión DMVPN asegura el menor valor de retardo. Se recomienda el uso de protocolos EIGRP. En este último caso, no hay límites en el número de tránsitos, como cuando se utiliza el protocolo RIP. La universalidad del protocolo EIGRP radica en su funcionalidad en las redes con otros protocolos de enrutamiento, ya que la información de todos los protocolos de enrutamiento se puede unir por medio de EIGRP. Sin embargo, al igual que con todas las redes EIGRP, el número de vecinos debe limitarse para garantizar que el enrutador

concentrador pueda restablecer las comunicaciones después de una interrupción importante.

DMVPN con el uso de los diferentes protocolos de IGP, y con las características propias de su tecnología hace posible el soporte de escalabilidad de la red a un escenario diverso de condiciones, variables de tamaños y topologías de implementación, debido a la gran simplificación de complejidad y de ahorro de configuraciones.

Los protocolos Interior Gateway Protocol (IGP) analizados en el documento EIGRP y OSPF brindan la posibilidad de ejecutar procesos de afinamiento que facilita el soporte de condiciones de escalamiento en redes de gran tamaño. Estos procesos van desde la posibilidad de modificación de los temporizadores que gestionan los tiempos en los que se intercambian información de estado y actividad, soporte de pilas de protocolo en la capa IP en versiones de IPv6 hasta modificaciones en su comportamiento para soporte de redes de una gran cantidad de enrutadores.

La red DMVPN permite optimizar el rendimiento y reducir la latencia de las comunicaciones entre sitios. DMVPN es una tecnología que integra diferentes conceptos como Generic Routing Encapsulation (GRE), encripción IPsec, Next-Hop Resolution Protocol (NHRP) y Routing para proporcionar una solución sofisticada que permite a los usuarios finales comunicarse de manera efectiva a través de placas estáticas y los túneles IPsec creados dinámicamente. Por lo tanto, la selección del mejor protocolo de enrutamiento al considerar diferentes criterios de selección se vuelve importante durante la fase de planificación de la red.

REFERENCES

[1] Y. Gobena, A. Durai, M. Birkner, Practical Architecture Considerations for Smart Grid WAN Network, 2011, pp. 0–5. doi:10.1109/PSCE.2011.5772481.

[2] R. Jankuniene, Route Creation Influence on DMVPN QoS, 2009, pp. 609–614. doi:10.1109/ITI.2009.5196156.

[3] I. Network, S. Agency, A. Ababa, K.-h. Kim, Dynamic Routing Influence on Secure Enterprise Network Based on DMVPN, 2017, pp. 756–759. doi:10.1109/ICUFN.2017.7993894.

[4] N. Angelescu, D. C. Puchianu, G. Predusca, L. D. Circiumarescu, G. Movila, DMVPN simulation in GNS3 network simulation software, 2017, pp. 1–4. doi:10.1109/ECAI.2017.8166444.

[5] H. Chen, Design and Implementation of Secure Enterprise Network Based on DMVPN. doi:10.1109/ICBMEI.2011.5916984.

[6] H. Li, P. W. C. Prasad, A. Alsadoon, L. Pham, A. Elchouemi, An improvement of Backbone Network security using DMVPN over an EZVPN structure, 2016, pp. 14–16. doi:10.1109/ICAEES.2016.7888039.

[7] S. Mohagheghi, J. Stoupis, Z. Wang, Z. Li, Integration into the Distribution Management System, 2010, pp. 501–506. doi:10.1109/SMARTGRID.2010.5622094.