

High Performance Application Delivery in Tactical Networks

Flexible Converged Services System – Type 1 Encryption (FCSS-T1E)
Converges Legacy and IP Services with Type 1 Encryption

A White Paper by



Ultra Electronics
DNE Technologies

and



Joint Tactical Solutions

Ultra Electronics-DNE Technologies
50 Barnes Park North
Wallingford, CT USA 06492
(203) 265-7151
sales@ultra-dne.com
www.ultra-dne.com

J2TS
Joint Tactical Solutions
53 Gladiola Drive
Howell, NJ USA 07731
(732) 982-4221
sales@j2ts.net
www.j2ts.net

This document, and the technical data within, is controlled for export by the United States Department of State. It, or any part thereof, may not be exported or transferred to any foreign person either in the United States or abroad, or disclosed to a national of another country without the prior written approval of the United States Department of State.

© 2007 Ultra Electronics-DNE Technologies. No reproduction or distribution can be made, whole or in part, without prior written consent of Ultra Electronics-DNE Technologies.

Revision 1 March, 2007

Table of Contents

Introduction	4
Benefits to the Warfighter	4
Flexible Converged Services System Network Diagram	4
Configuration 1: Multi-Service Convergence, with TRANSEC Encryption, over Point to Point Wireless (WiMax) Networks	5
Point to Point WiMax Diagram	5
Results and Observations	5
Configuration 2: Multi-Service Convergence, with TRANSEC Encryption, over Point to Multipoint Wireless (WiMax) Networks	8
Point to Multipoint WiMax Diagram	8
Results and Observations	8
Configuration 3: Multi-Service Convergence, with TRANSEC Encryption, over Point to Point IP Satellite Networks	11
Multi-Service Convergence with TRANSEC over Point to Point IP Satellite Network Diagram	11
Results and Observations	11
Configuration 4: Multi-Service Convergence, with TRANSEC Encryption and Secure Compressed Voice, over Point to Point IP Satellite Networks	13
Multi-Service Convergence with TRANSEC and Secure Compressed Voice over Point to Point IP Satellite Network Diagram	13
Results and Observations	13
Summary	15

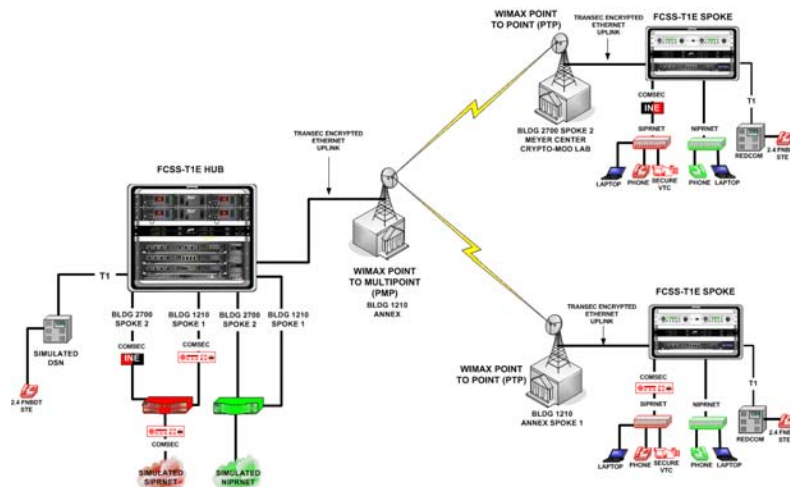
White Paper: High Performance Application Delivery in Tactical Networks *FCSS-T1E Converges Legacy and IP Services with Type 1 Encryption*

The Flexible Converged Services System – Type 1 Encryption (FCSS-T1E) is a tactical access communications platform, designed and implemented by J2TS. It securely converges legacy and IP services from a single hub location to remote units over multiple IP-based transmission facilities. Extensive Quality of Service (QoS) functionality allows network operators to ensure reliable delivery of high priority applications, while ensuring that remaining bandwidth is available to lower priority traffic. The FCSS-T1E also provides an innovative method for warfighters to use their existing Type 1 TRANSEC encryptors to secure IP-based transmission systems.

Benefits to the tactical Warfighter include:

- Utilization of existing TRANSEC assets
- Reduced equipment footprint by converging disparate legacy and IP-based services onto a single common platform
- A substantial improvement in bandwidth utilization at a lower cost, compared to competitors' solutions.

Extensively tested in a variety of configuration scenarios, the FCSS-T1E has demonstrated its ability to provide significant gains in application delivery performance, information assurance and bandwidth utilization over congestion-prone IP transmission facilities. ***The objective of this paper is to describe and quantify four of the many configuration scenarios in which the FCSS-T1E solution has been tested and demonstrated to provide definitive benefits to the tactical communications environment.***

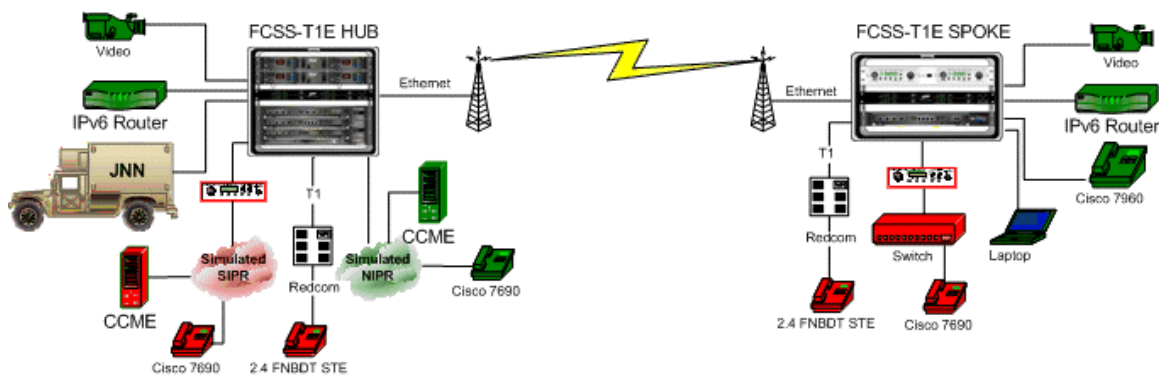


Basic FCSS-T1E Network Diagram

Configuration 1: Multi-Service Convergence, with TRANSEC Encryption, over Point to Point Wireless (WiMAX) Networks

Description

In this configuration, an array of simulated services is transmitted across a point to point wireless network utilizing WiMAX radio systems. The FCSS-T1E applies QoS to each service, converges them into a single IP stream and applies TRANSEC before being transmitted “over-the-air” in Layer 2 packets. The simulated services include SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data. The TRANSEC encryption devices used are the KIV-19A and KIV-7M. WiMAX radio systems used include models from Redline, Orthogon and Nortel.



Configuration #1
Point-to-Point WiMAX

Results and Observations

All SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data services were successfully connected in this configuration at speeds of 1024K, 2048K, 4096K, 8192K and 16MB using the Redline WiMAX system.

All services were sent over the Redline point to point system simultaneously through the TRANSEC. The TRANSEC was forced to resync, proving that it was indeed connected and able to successfully resync in this configuration. (Note that NSA does not recommend the 16MB rate, as the KIV-19A and the KIV-7M are only supposed to operate at speeds up to 13MB.)

Due to limited equipment availability, this configuration was successfully tested only at 2.048MB using the Orthogon and Nortel systems.

For each of the applications tested, Quality of Service was defined as Committed Bit Rate (CBR) or Uncommitted Bit Rate (UBR). CBR was doubled for each increase in speed, while UBR was set at the defined aggregate speed. For example:

At 1024K:

- VoIP was assigned a CBR of 256K
- Video was assigned a CBR of 256K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 1024K

While at 2048K:

- VoIP was assigned a CBR of 512K
- Video was assigned a CBR of 512K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 2048K

At 4096K:

- VoIP was assigned a CBR of 1024K
- Video was assigned a CBR of 1024K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 4096K

At 8192K:

- VoIP was assigned a CBR of 2048K
- Video was assigned a CBR of 2048K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 8192K

Finally, at 16MB:

- VoIP was assigned a CBR of 4096K
- Video was assigned a CBR of 4096K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 16MB

The SIPRNET input to the FCSS was Ethernet, converted to serial data by the FCSS so a KIV-7HSB device could encrypt it, then converted back to Ethernet. It was able to maintain sync with the distant end and resync when necessary.

VoIP testing was done with a Cisco Call Manager Express (CCME) at one end of the circuit and a VoIP phone plugged directly into the FCSS at the other end. 100% call completion rates were attained in this configuration. Calls that were in progress during a forced resync at the TRANSEC were automatically reconnected without requiring a redial.

Another VoIP test was conducted using the simulated SIPRNET, with the KIV-7HSB used for COMSEC at both ends. At one end of the circuit, the SIPRNET router ran the CCME through a KIV-7HSB; at the other end a VoIP phone was connected to a switch that, in turn, was COMSEC-encrypted by another KIV-7HSB. Again, 100% call completion rates were attained in this configuration, along with high Mean Opinion Scores (MOS). During the calls, the COMSEC was forced to resync, and the calls were able to stay connected even after the COMSEC was out for five minutes. (Note that during the outage no conversation is possible, but each end remains connected to its circuit until COMSEC sync is reestablished.)

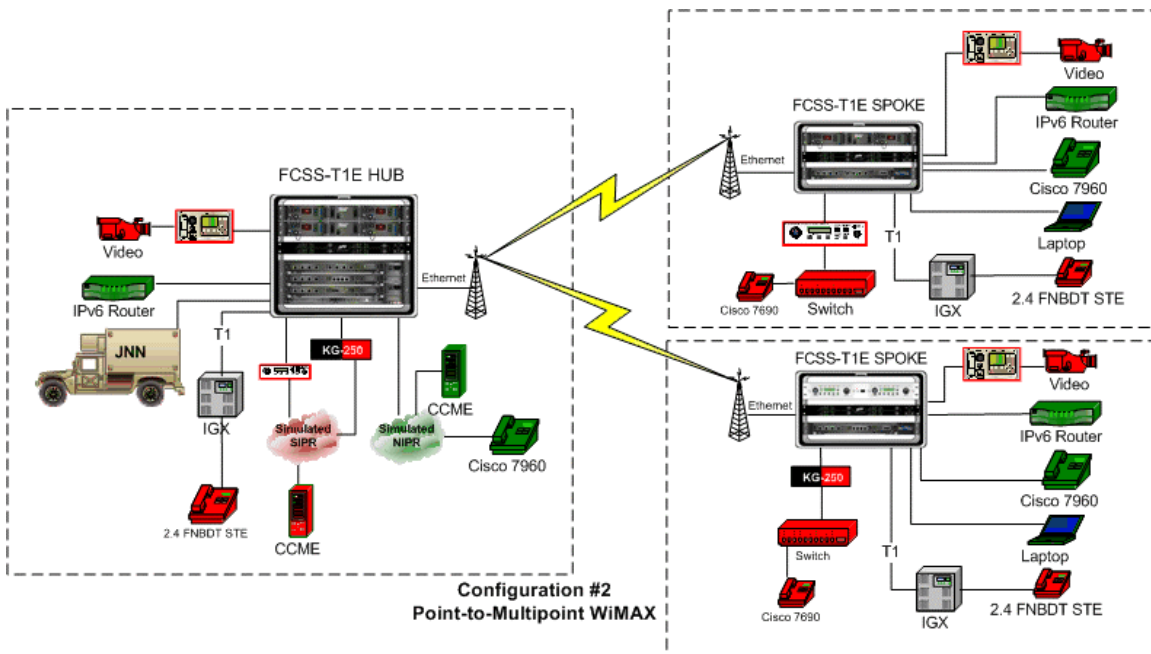
Concurrent with these tests, a 256K video teleconference, NIPRNET and IPv6 traffic were also active. The IPv6 service was successfully encrypted and sent through this configuration with no dual stacking required. The IPv6 testing was done using two routers, each with IPv6 ports defined, and continuously pinging each other.

Throughout this testing scenario, the total aggregate bandwidth loss of the FCSS, the TRANSEC and the wireless system (in combination) was measured at 12 – 13.7%.

Configuration 2: Multi-Service Convergence, with TRANSEC Encryption, over Point to Multipoint Wireless (WiMAX) Networks

Description

In this configuration, an array of simulated services is transmitted across a point to multipoint wireless network (a hub and two spokes), utilizing a multipoint WiMAX radio system. At each spoke, the FCSS-T1E applies QoS to each service, converges them into a single IP stream and applies TRANSEC before being transmitted “over-the-air” in Layer 2 packets to the hub location, where the converged services are ultimately forwarded to their appropriate destinations via an additional FCSS-T1E. The simulated services include SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data. The TRANSEC encryption devices used are a mix of KIV-19A and KIV-7M. The WiMAX radio system used is a multipoint unit from Redline.



Results and Observations

All SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data services were successfully connected in this configuration at speeds up to 16 MB (per spoke) using the Redline WiMAX system. This is the maximum rate that can be supported by the Redline system in this configuration.

All services were sent over the Redline point to multipoint simultaneously through the TRANSEC to each spoke. The TRANSEC was forced to resync to show that it was indeed connected and able to resync in this configuration. (Note that NSA

does not recommend the 16MB rate, as the KIV-19A and the KIV-7M are only supposed to operate at speeds up to 13MB.)

Encryption was applied to the hub and spokes as follows:

- Hub: KIV-19A used for TRANSEC
- Spoke 1: KIV-19A used for TRANSEC, KIV-7HSB for SIPRNET input
- Spoke 2: KIV-7M used for TRANSEC, KG-250 for SIPRNET input, TACLANE HAIPE for video input

For each of the applications tested, Quality of Service was defined as Committed Bit Rate (CBR) or Uncommitted Bit Rate (UBR). CBR was doubled for each increase in speed, while UBR was set at the defined aggregate speed. For example:

At 1024K:

- VoIP was assigned a CBR of 256K
- Video was assigned a CBR of 256K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 1024K

While at 2048K:

- VoIP was assigned a CBR of 512K
- Video was assigned a CBR of 512K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 2048K

At 4096K:

- VoIP was assigned a CBR of 1024K
- Video was assigned a CBR of 1024K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 4096K

At 8192K:

- VoIP was assigned a CBR of 2048K
- Video was assigned a CBR of 2048K
- T1 Voice (automatically set to CBR) was fractionalized at 256K
- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 8192K

Finally, at 16MB:

- VoIP was assigned a CBR of 4096K
- Video was assigned a CBR of 4096K
- T1 Voice (automatically set to CBR) was fractionalized at 256K

- SIPR and NIPR data were assigned an UBR equal to the aggregate speed of 16MB

The SIPRNET input on Spoke 1 was Ethernet, converted to serial data by the FCSS so a KIV-7HSB device could encrypt it, and then converted back to Ethernet. It was able to maintain sync with the distant end and resync when necessary. Inline Network Encryptors (INEs) were used on Spoke 2.

VoIP testing was done with a Cisco CCME at one end of the circuit and the VoIP phones plugged directly into the FCSS spokes. 100% call completion rates were attained. Calls that were in progress during a resync at the TRANSEC were automatically reconnected without requiring a redial.

Another VoIP test was conducted using the simulated SIPRNET with the KIV-7HSB being used for COMSEC at both ends for Hub-to-Spoke 1 and HAIPE devices being used for Hub-to-Spoke 2. The SIPRNET router at the hub ran the CCME through the KIV-7HSB for Spoke 1 and a HAIPE device for Spoke 2. VoIP phones were connected to each spoke and the hub. All phones were able to call each other, including Spoke 1 to Spoke 2. Again, 100% call completion rates were attained in this configuration, with high MOS scores. During calls the COMSEC was forced to resync, and the calls were able to stay connected even after the COMSEC was out for 5 minutes. (Note that during the outage no conversation is possible but each end remains connected to their end till COMSEC sync is reestablished.)

Concurrent with these tests, a 256k video teleconference, NIPRNET, SIPRNET and IPv6 traffic were also active. The IPv6 service was also successfully encrypted and sent through this configuration with no dual stacking required. Testing was done using two routers with IPv6 ports defined, and continuously pinging each other.

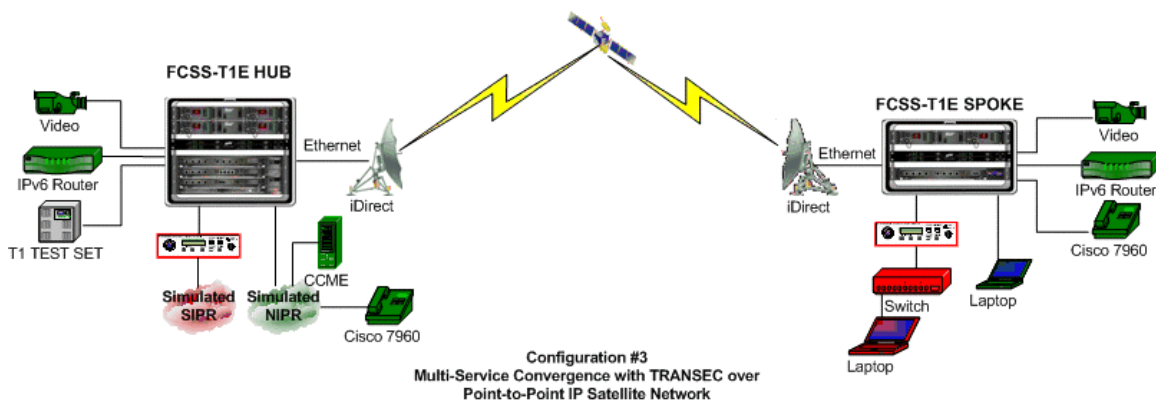
T1 testing in this scenario was done using two T1 BERT testers at the hub and T1 loopback plugs at the spokes.

Throughout this testing scenario, the total aggregate bandwidth loss of the FCSS, the TRANSEC and the wireless system (in combination) was measured at 12 – 13.7% on each spoke.

Configuration 3: Multi-Service Convergence, with TRANSEC Encryption, over Point to Point Satellite Networks

Description

In this configuration, an array of simulated services is transmitted across a point to point network utilizing an IP-based satellite transmission system. At each site, the FCSS-T1E applies QoS to each service, converges them into a single IP stream and applies TRANSEC before being transmitted “over-the-air” in Layer 3 packets. The simulated services include SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data. The TRANSEC encryption device used is the KIV-19A. The satellite transmission system used is an iDirect NetModem II IP modem.



Results and Observations

All SIPRNET, NIPRNET, T1 Voice, VoIP, Video and Data services were successfully connected in this configuration at speeds up to 1.024 MB using the iDirect system. For each of the applications tested, Quality of Service was defined as Committed Bit Rate (CBR) and Uncommitted Bit Rate (UBR).

At 512K:

- Video was assigned a CBR of 384K
- SIPR and NIPR were assigned an UBR equal to the aggregate speed of 512K

And at 1024K:

- VoIP was assigned a CBR of 256K
- Video was assigned a CBR of 256K
- SIPR and NIPR were assigned an UBR equal to the aggregate speed of 1024K

VoIP testing was done with a Cisco Call Manager Express (CCME) at one end of the circuit and a VoIP phone plugged directly into the FCSS at the other end. 100% call completion rates were attained in this configuration. Calls that were in progress during a forced resync at the TRANSEC were automatically reconnected without requiring a redial.

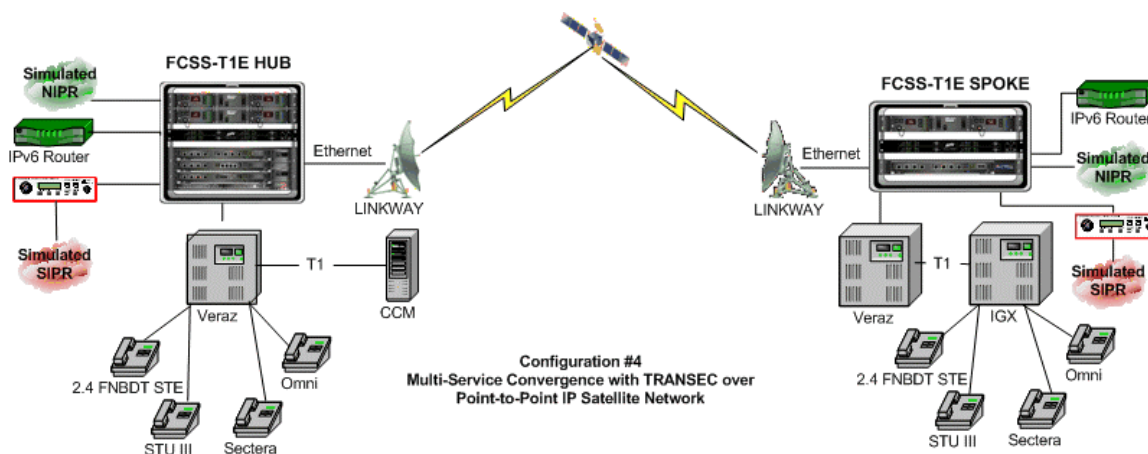
Concurrent with this test, a 256K video teleconference, NIPRNET, SIPRNET and IPv6 traffic were also active. The IPv6 service was successfully encrypted and sent through this configuration with no dual stacking required, even though the transmission path was an IPv4-based system.

T1 testing in this scenario was done using a T1 BERT tester at one spoke and a T1 loopback plug at the other spoke.

Configuration 4: Multi-Service Convergence, with TRANSEC Encryption, over Point to Point Satellite Networks

Description

In this configuration, an array of simulated services is transmitted across a point to point network utilizing an IP-based satellite transmission system. At each site, the FCSS-T1E applies QoS to each service, converges them into a single IP stream and applies TRANSEC before being transmitted “over-the-air” in Layer 3 packets. The simulated services include SIPRNET, NIPRNET and compressed T1 for secure and non-secure voice over Ethernet. The TRANSEC encryption device used is the KIV-19A. Satellite transmission is via LINKWAY IP modem. The compressed T1 over Ethernet was provided by a Veraz I-Gate 4000 EDGE media gateway.



Results and Observations

All SIPRNET and NIPRNET compressed T1 secure and non-secure voice over Ethernet and data services were successfully connected in this configuration at 1.488 MB using the LINKWAY system. For each of the applications tested, Quality of Service was defined as Committed Bit Rate (CBR) or Uncommitted Bit Rate (UBR).

At 1.488MB:

- Compressed T1 Secure and Non-secure voice over Ethernet was assigned a CBR of 795k
- SIPR and NIPR were assigned an UBR equal to the aggregate speed of 1.488MB

Various secure devices including the STU III Secure phones, 2.4 FNBDT Secure phones, OMNIs, and SECTERAs were tested using the Veraz compression box over the LINKWAY IP Modem satellite system. A REDCOM T1 was sent thru the VERAZ to a Cisco Call Manager (CCM) using T1 and FXS Cards. A call generator was used from the REDCOM to the CCM with up to 10 calls being up at any given time. Secure calls were then made at various phone rates. These circuits, plus simulated SIPRNET, NIPRNET, and an IPv6 circuit were all TRANSEC encrypted at the FCSS. The secure call completion rate was 100% in almost all scenarios. The compression rates used were based on the following table:

CODEC	# Active Calls	Bandwidth	Compression Ratio
G.711	3 to 10	397k to 447k	2:1
G.729	3 to 10	223k to 227k	12:1
AMR	3 to 10	256k to 273k	7:1

In this configuration the TRANSEC provided by the FCSS remained in sync for 2 days with no packet loss over the LINKWAY. The LINKWAY had 3MB of bandwidth overall; the FCSS held 2.976mb of the bandwidth with no packet loss.

Summary

In summary, the FCSS-T1E system successfully bridged legacy and IP protocols to traditional NSA-approved COMSEC/TRANSEC technology in each of the four configuration scenarios tested:

- Point to Point WiMAX Networks (via Redline, Orthogon, Nortel 802.16d systems)
- Point to Multipoint WiMAX Networks (via Redline 802.16d system)
- Point to Point Satellite Networks (via iDirect IP modem)
- Point to Point Satellite Networks (via Linkway IP modem)

The system also provided aggregated DoD services (voice/video/data) on a single multiplexed Ethernet stream conditioned for both IP and serial encryptors, with minimal aggregate bandwidth loss.