



Worldcast Research

M-PRESS

Describing need and method for enhanced security in point-to-multipoint IP communications using
SMART(p) technology

By Ian A. Stewart

Table of Contents

Contents

- Forward..... 1
 - Worldcast proposes research into M-PRESS..... 1
 - M-PRESS is impervious to an attack created with stolen (leaked) command and control software components 1
 - A national utility command and control system 1
- Why Worldcast? 1
 - Worldcast proposes the M-PRESS project to test multipoint connectivity 2
 - M-PRESS project proposes to test the use of existing infrastructure..... 2
- The Problem..... 2
 - Infrastructure’s vulnerability to worms and bots..... 2
- The Solution 3
 - The SMART enhanced security point-to-multipoint system..... 3
- Areas of infrastructure that is highly vulnerable:..... 5
 - Electronic monitoring systems (SCADA’s)..... 5
- Multipoint-infrastructure vulnerable to attack..... 6
 - The grid 6
 - Centralized control system..... 7
 - The role of enhanced security in point-to-multipoint communications in power generation 7
 - Concentration of power grid command centers 7

- How enhanced security point-to-multipoint technology can increase power survivability and reliability 8
- Enhanced security multipoint communications for emergency broadcast 9
 - The broadcast stations..... 9
- The SMART distribution system for command and control data or television..... 10
- Why enhanced security point-to-multipoint can support mass scale - 10
- The need: 10
- The solution:..... 11

List of Figures

- Figure 1 - Cyber attack of command and control systems 3
- Figure 2 - SMART data translation adds security to command and control network 4
- Figure 3 - Example of SCADA device..... 5
- Figure 4 - Example of a SCADA computer based command center 5
- Figure 5 - Even after the massive blackouts of 2003, 1977 and 1965, the national power grid remains in fragile, vulnerable condition. Energy spokespeople state investments of \$56 to \$450 billion is needed to fix this antiquated system..... 6
- Figure 6 - Enhanced security multipoint command and control System on US power grid 8
- Figure 7 - Enhanced security multipoint television or emergency broadcast 9
- Figure 8 - SMART technology as is relates to television 10
- Figure 9 - SMART allows for large audiences..... **Error! Bookmark not defined.**

Forward

Worldcast M-PRESS

M-PRESS stands for **Multipoint Repeating for Enhanced Security System**. An “M-PRESS” system is a multipoint network that hides the multipoint infrastructure addresses making it impervious to attack from stolen command and control software components. M-PRESS security is added to *base level point-to-multipoint* communications infrastructure with Worldcast’s **SMART REPEATING** technology. Worldcast’s technology layers security, reliability and provides for multipoint feedback from mass audience communication links (point-to-multipoint).

M-PRESS is impervious to an attack created with stolen (leaked) command and control software components

Because SMART technology uses a hardened REPEATING technology for communications over fiber or copper backbones, it could be used for enhancing security and to provide *point-to-multipoint* communications that would be impervious to attack from copied command and control software which had been stolen by Internet remote control worms. A REPEATING system is required to add security to the *base* (unsecure) *point-to-multipoint* Internet connections. Also, to be efficient, a mechanism is required to analyze the *base* multipoint rule-sets available and use the most secure multipoint link. Worldcast has also developed this system, and it’s called it SIMPLE - Self Implementing Multipoint Protocol Level Escalation.

A national utility command and control system

A multipoint backbone has been proposed to connect key infrastructure such as the monitoring and control of remote devices (also called SCADA). This proposal caused a security review which found that much of the US infrastructure had been compromised by internet worms which are under the control of individuals from Russia and China. The exact intention of the worms is not clear, but it was reported in the Wall Street Journal that the presence has cast a shadow over the plan to centralize infrastructure for command and control. For example; US power stations in might use remote SCADA technology for monitoring and remote switching.

Why Worldcast?

Worldcast is a provider of technology that enables point-to-multipoint IP communications with enhanced security, reliability and a bi-directional reporting mechanism designed for ultra secure multipoint applications.

The M-PRESS project creates multipoint connectivity

We propose the use of SMART technology to ameliorate distributed multipoint command and control's vulnerability to attack by Internet worms and bots. This document provides a look at the related infrastructures and their vulnerability, and shows how SMART technology overcomes those vulnerabilities in the most efficient way possible.

Worldcast is building enhanced security point-to-multipoint Internet infrastructure to create large scale transmissions of control data, media and distributed data. This infrastructure could provide scalable infrastructure that is resilient, security enhanced and redundant. This project M-PRESS is builds on base point-to-multipoint (Multicast) infrastructures creating the architecture for scalable applications to communicate with multipoint, enhanced security, and bi-directional (feedback) capabilities.

M-PRESS uses existing infrastructure

Elements that can benefit by use of SMART include routers network, switching for broadcast of multipoint data, command and control information, and emergency switch over systems.

The Problem

Infrastructure's vulnerability to worms and bots

The infrastructure in the United States of America is highly vulnerable to Internet worms and bots ("bots" are remote control programs that are copied to unsuspecting users computers with virus laden emails). Recently CBS Lesley Stahl reports that "bot" and "worms" have tripled activity and advisory of US-CERT technical Cyber Security has been issued for the "Conficker" types worm (<http://www.us-cert.gov/cas/techalerts/TA09-088A.html>) which is particularly devious because it deletes system restore points and block the ability to go to web sites that might remove it. If such a work were to propagate into for example, a nuclear power plant command and control the attacker could gain (copy) software that send the command and control messages. A rouge nation may consider this a cost effective weapon to cripple the United States of America. This type of attack requires little funding. From a position at any work station capable of tapping into backbone data, this weapon could confuse command and control (or SCADA devices) that were connected. Such an attack by remote or pre-programmed control, could wipe out many different infrastructure elements including Military command and control.

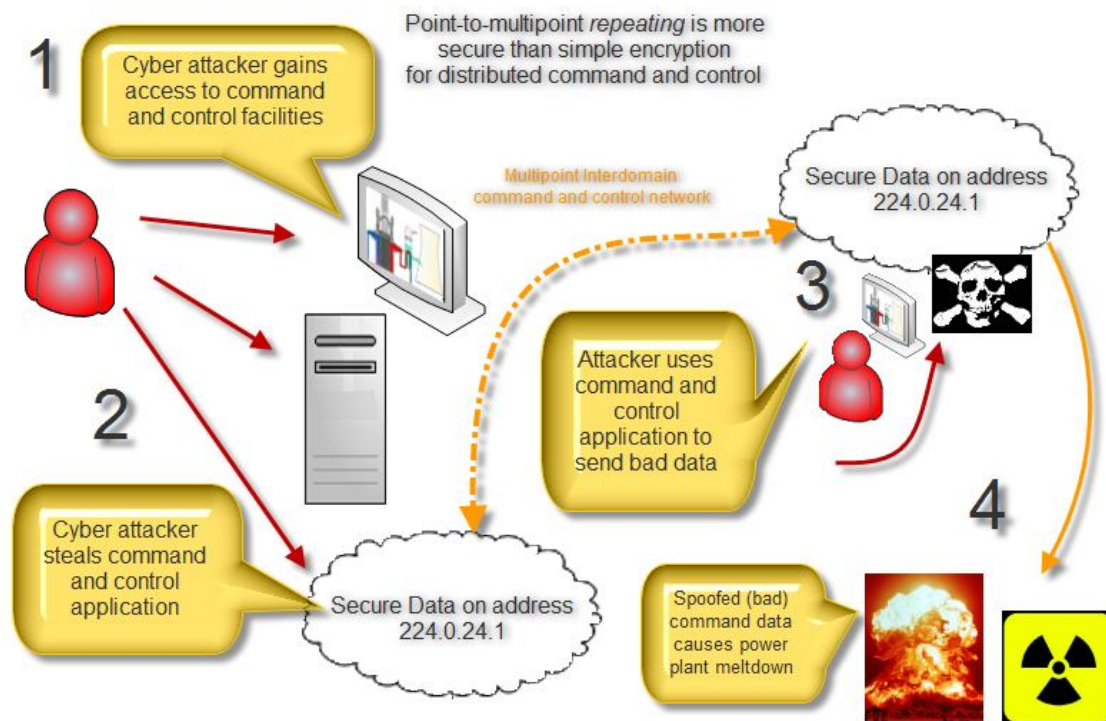


Figure 1 - Cyber attack of command and control systems

The Solution

The SMART enhanced security point-to-multipoint system

The SMART enhanced security multipoint system comprises a method for sending enhanced security multipoint transmissions. The sender side system includes a computer system coupled to a public network and configured to generate a multipoint broadcasts, and encrypt and repeat the generated multipoint broadcast on translated address. The system runs on routers coupled to the Public or private networking infrastructures. The system encrypts the data and translates the address from a well known list of addresses.

The receive side systems are configured to request (join) multipoint groups or broadcasts, where the user system is associated with the router performing the reverse translation and thereby requesting to join the translated multipoint group. The SMART system is configured to retrieve the encrypted

multicast broadcast from the computer system over the public network, decrypt the sent multipoint broadcast, and send the decrypted multipoint broadcast to the user system requesting to join.

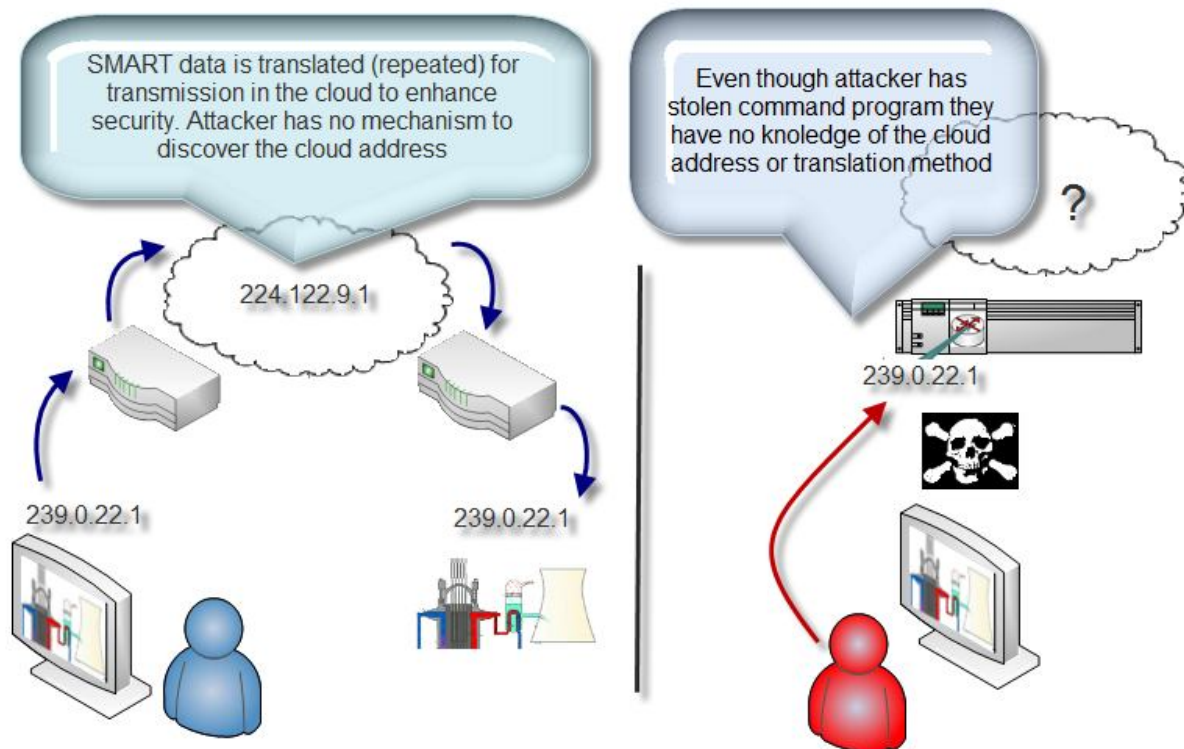


Figure 2 - SMART data translation adds security to command and control network

Areas of infrastructure that is highly vulnerable:

Electronic monitoring systems (SCADA's).



Figure 3 - Example of SCADA device

- SCADA systems are heavily used in critical infrastructure components like, the US power grid, drinking water management, and oil and gas pipeline distribution. In November of 1999, ships radar was able to block the electronic control of the San Diego aqueduct system. A crew was dispatched to manually control the flood gates averting a **“catastrophic failure” of the aqueduct**. Most importantly, monitoring of the status of these devices is not distributed. Even if some command centers survived the attack, the statuses of those

centers are unknown to other command centers.

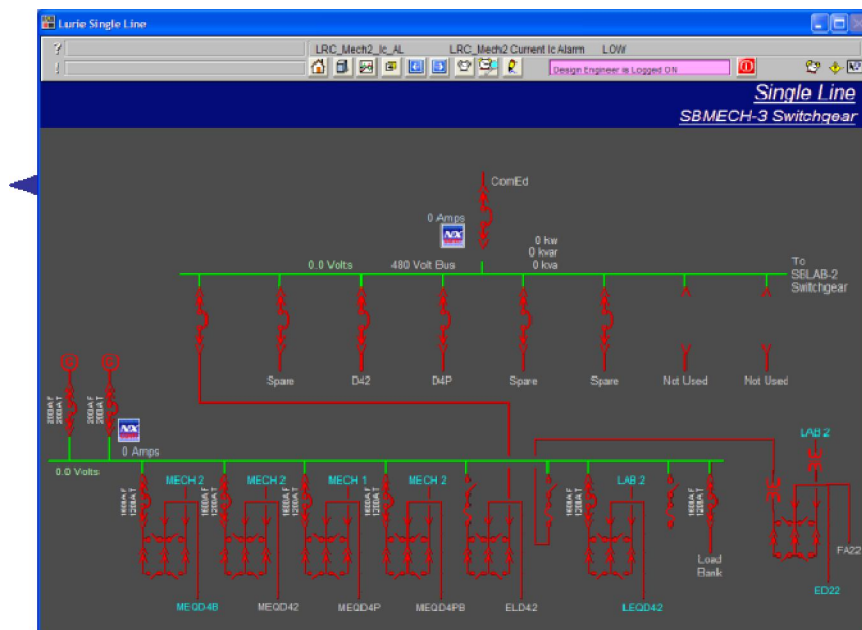


Figure 4 - Example of a SCADA computer based command center

Multipoint-infrastructure vulnerable to attack

The grid

- The electrical system in the USA requires management of a power grid that currently is run at peak times close to the point of failure. The national power grid is operated by a maze of contributors where a problem of a small contributor can mushroom into a catastrophic failure. Upsetting this grid by EMP/S would cause widespread failure of the system. As we have seen in the massive and deadly power failures of 2003, 1977 and 1965, the balance of the grid requires the control and energy output reporting of every grid participant, in order to enable the system operator to maintain the delicate balance between energy consumption and energy use.

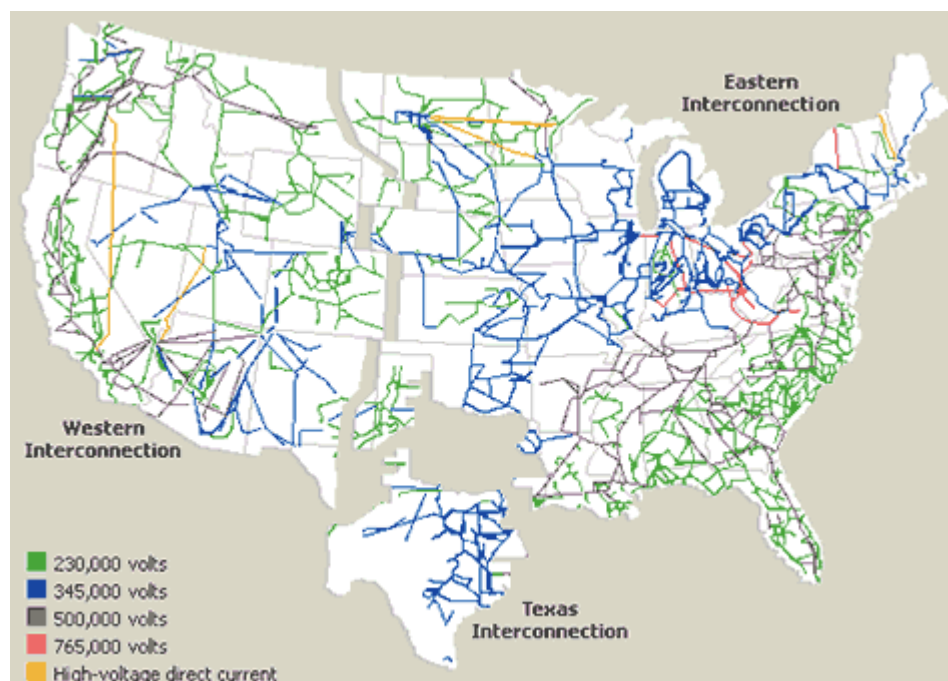


Figure 5 - Even after the massive blackouts of 2003, 1977 and 1965, the national power grid remains in fragile, vulnerable condition. Energy spokespeople state investments of \$56 to \$450 billion is needed to fix this antiquated system

Centralized control system

- Currently power grid control systems are centralized at a small number of command stations. The use of enhanced security point-to-multipoint communications could allow a decentralized command structure, thus increasing survivability.

The role of enhanced security in point-to-multipoint communications in power generation

- Using enhanced security point-to-multipoint communications in power grid stations and sensing components will allow a nationwide awareness of power generation status and capability. This reduces the power grids vulnerability to attack. Using a secure reliable point-to-multipoint system with bi-directional feedback would allow a distributed command and control and provide the ability to create redundancy for power grid, command, and grid command and control stations.

Concentration of power grid command centers

- The concentration of grid command centers makes them an appealing target for persons who wish to see our infrastructure damaged. The consequences of nation wide power failure that would result from an attack of our control facilities would have had far greater effect for the average American than the 911 attack of the twin towers.

How enhanced security point-to-multipoint technology can increase power survivability and reliability

Distributed power grid command and control with added security is possible with enhanced security reliable point-to-multipoint technology. Essentially any point with access to a multipoint enabled connection could, providing the access level, authority and enhanced security multipoint network, function as command point. Using multipoint technology, command points could be mobile and standby computers (laptops or otherwise) could be stored for immediate interconnection in the event of attack. Grid related SCADA devices could be controlled using enhanced security point-to-multipoint systems.

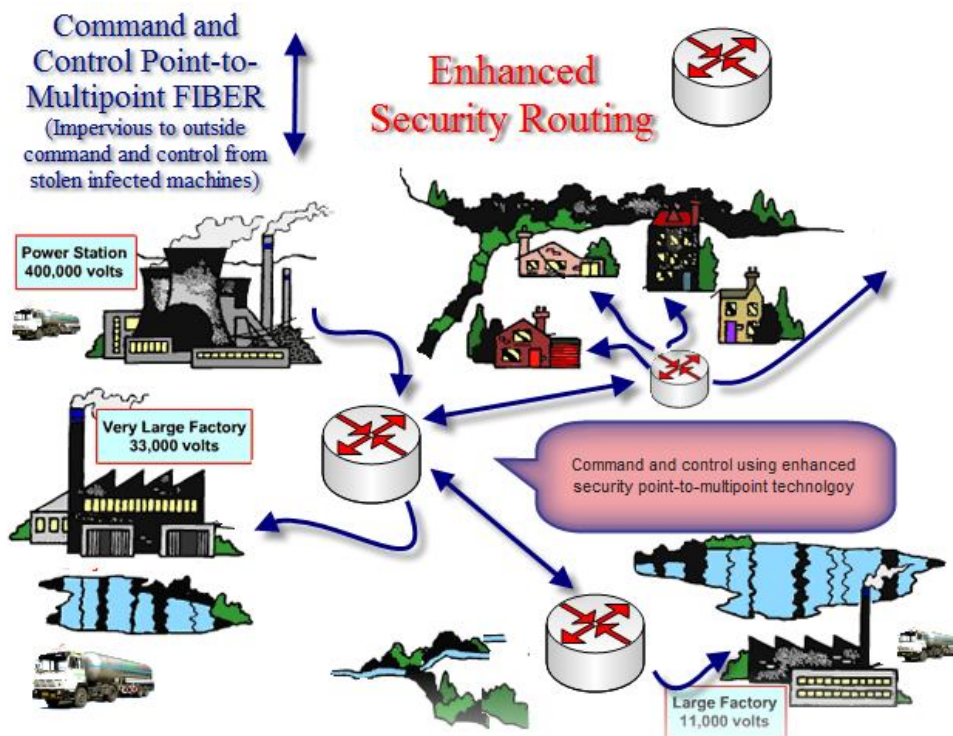


Figure 6 - Enhanced security multipoint command and control System on US power grid

Enhanced security multipoint communications for emergency broadcast

The broadcast stations

By using SMART point-to-multipoint fiber based technology, a system could be created that would be resistant to cyber attack.



Figure 7 - Enhanced security multipoint television or emergency broadcast

The point-to-multipoint base infrastructure that SMART enhanced security REPEATING technology is built upon provides the ability to have Secure Reliable point-to-multipoint communications that also contain a feedback mechanism. The feedback mechanism provides the operator a method to discover the end user quality of service. With this feature the total soles hearing the command and control or emergency transmission can be known. SMART security has a plug-in in module that is currently set to use Advanced Encryption Standard (AES). AES is currently the mechanism for "Top Secret" documents used by the US government; however a SMART system can easily accommodate any encryption types.

The SMART distribution system for command and control data or television

Why enhanced security point-to-multipoint can support mass scale -

Worldcast has developed an Internet software solution for worldwide communications of any type of data structure to mass audiences.

SMART sends one signal to millions simultaneously. It is exponentially cost and bandwidth efficient when compared to Unicast (TCP) transmission. Unicast bandwidth cost is per customer with no economy of scale (in fact, it doesn't scale). SMART's efficiency increases with each user added and the cost approaches zero-per-user in mass media application.

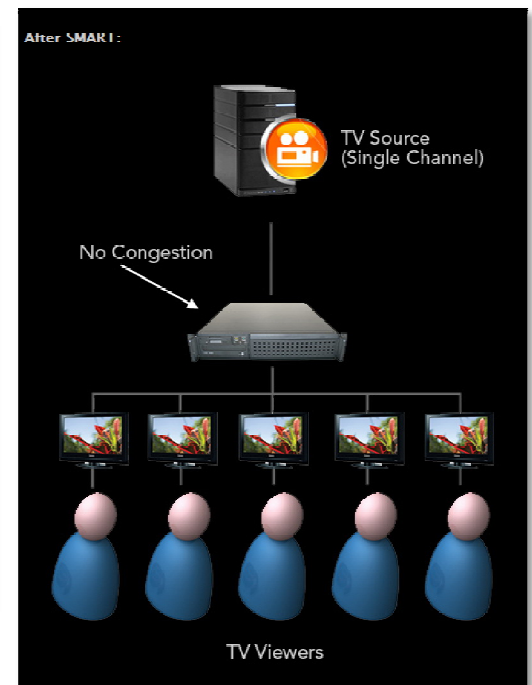
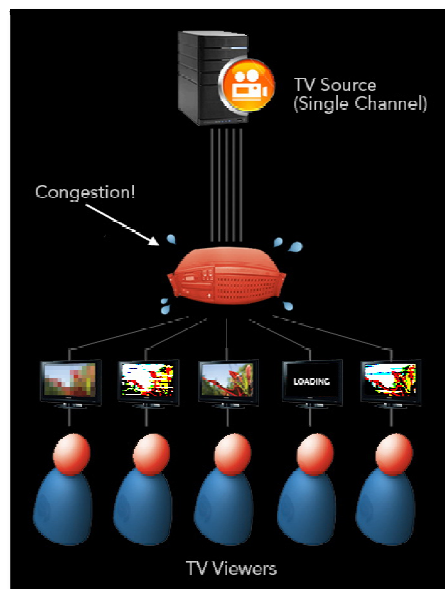
SMART is another step in the convergence of communication technology, bringing enhanced security point-to-multipoint communications. SMART is ubiquitous, able to transport all types of data across all systems (cable/copper, fiber and wireless) to all devices.

SMART has been lab tested and is in operation now.

Figure 8 - SMART technology as it relates to television – before SMART and after SMART

The need:

The quantity of data traveling across the Internet is growing at an almost exponential rate. For Internet service providers (ISPs), bandwidth, or the lack thereof, is becoming a critical issue. For example; for video data to be received with acceptable frame rate or clarity and speed, Internet congestion must be managed. Current technology – commonly called Unicast – requires sending a separate signal for each end-user; therefore, audiences larger than a few hundred



thousand are not possible without causing congestion and loss of quality. These systems can easily consume more bandwidth than is available. SMART has similar results when applied to any type of data needing to be distributed to massive audiences.

By comparison, the SMART software system that is far less expensive to operate and far easier to implement. With Worldcast' secure, reliable SMART technology, one signal can be sent to millions simultaneously, with a cable-like quality picture, making it possible to launch a television system over the Internet. SMART combines television with the power of the computer, making full interaction with the viewer possible, all at exponentially reduced costs. Applications extend far beyond just television and include; video movie rental, video conferencing, military applications, broadcast to portable/mobile devices and command and control.

The solution:

SMART makes use of existing Internet protocols, and then adds the point-to-multipoint functionality that hereto has been missing. A protocol is a set of rules used by all Internet communications. Protocols in use today are well established, e.g., Transmission Control/Internet Protocol or TCP/IP. SMART technology has been through rigorous testing in the University systems.

Worldcast holds the key to multipoint infrastructure network solutions, for which it holds five patents (three issued and two published/pending). Worldcast's technical staff has over eleven years experience in SMART research and development.