Wireless Fundamentals: Part II and Part III

InFocus Research and Development

Joseph Castaldi and Rob Hoeye

Note:

Part II of Wireless Fundamentals is intended to provide a more in depth discussion about the Networking topics in general and specifically about version 1.2 of the LiteShow Product. To that end we cover some topics that are more technical in nature. We anticipate that this document can be shared by InFocus Sales and Marketing to provide to our customers valuable background information.

Part III, Wireless LAN Security, is combined into this document, and describes several current topics in the field of cryptosystems.

Part II: 802.11 Network Architecture

Network Configurations

Part I of our white paper, *Wireless Fundamentals*, documented two typical network topologies in wide use today, ad-hoc or peer-to-peer networks, and the more common infrastructure topology. Both can be built using 802.11b hardware and software.

Ad-hoc Mode

Ad-hoc is a simplified peer-to-peer configuration that allows two or more mobile stations to establish a local network group known as an IBSS (Independent Basic Service Set). The minimal configuration includes a common SSID spelling and a common IP address scheme, (in LiteShow this Network Name or WLAN is spelled '*LiteShow*'). Ad-hoc mode is especially useful in the case where shared network resources are not required (e.g. network printers) or where a small community of users needs only temporary network connections. This is the wireless networking mode that is supported in the initial versions of LiteShow v1.0 and v1.1.

Infrastructure Mode

Infrastructure mode is a network configuration that includes: the presence of one or more Access Points (AP); a common IP address scheme and optionally; a common security plan. See the section on Wireless LAN Security for more details on security considerations. Infrastructure mode is the typical network topology used in businesses and increasingly, in the home. Typically this configuration also includes the use of a DHCP server for IP Address management, routers and switches for sub-network management, and network servers for providing centralized network-based resources. This more advanced mode of operation is supported in the newest version of InFocus LiteShow version 1.2.

Infrastructure mode is becoming more common in the home with the advent of consumer quality access points, hubs, and routers. Infrastructure mode is preferred in the case where the user wishes to have intranet and/or internet connectivity while simultaneously using the LiteShow screen scrape function to wirelessly display the computer screen data onto the LiteShow-enabled projector.

One crucial difference between ad-hoc network groups and infrastructure groups involves the need for constant discovery of peer radios. See the section below on 802.11b beacons. In the Infrastructure configuration, the Access Point takes this periodic beacon responsibility, thereby freeing the mobile stations from constantly 'announcing' their presence. In the ad-hoc configuration, the mobile stations (laptops) must take this role of frequent beacon transmission, possibly leading to decreased laptop battery life.

Wireless Performance

In the LiteShow System, end-to-end performance considerations may play into the choice between using ad-hoc network connection or infrastructure connections between the client (LiteShow Manager) and the server (LiteShow adapter).

Since the point-to-point ad-hoc connection requires that the scrape data is transferred only once, theoretically, the end to end system performance should be optimal in this mode. If the use model presumes that high resolution, high dynamic data is required, then the best choice is to use a simple ad-hoc network configuration.

Since an infrastructure connection involves an intervening Access Point, the scrape data is transferred at least twice; i.e. once from the client to the AP, and then once more from the AP to the server. This two-hop transfer can nonetheless be very fast and the casual user may not notice the difference, especially with non-dynamic source screen changes.

Access to shared network resources is supported as well as the possibility of performing multi-projector management; remote conferencing using infrastructure mode.

802.11 Beacons

The IEEE definition for 802.11b wireless communication includes a method for individual mobile stations to cooperatively participate in a distributed wireless network. Periodic 802.11b beacons are transmitted by the Access Point (or stations in Ad-hoc mode) and received by all stations for several purposes. Each radio must have a shared concept for time synchronization, power management and supported data rates. These behaviors are accomplished via the beacons.

Authentication and Association

In an infrastructure network, mobile stations must authenticate with an Access Point to obtain network connectivity. The minimal method required is for the mobile station to be configured with the same spelling for the WLAN NetworkName. (In LiteShow we have used ‘LiteShow’ as that case-sensitive spelling.) This mode corresponds to *Open Authentication*.

Another mode, called *Shared Key Authentication* involves the use of a *WEP key* that is exchanged between the mobile station and the Access Point to determine if the parties share that key. If the WEP key that is exchanged does match, then the mobile station is authenticated and then granted the ability to associate. Plainly described, you authenticate with the network and you associate with an access point.

An example will illustrate: the user with a wireless laptop has been configured to use the NetworkName that is in use for her company and the access points have been configured to use a common network name, thus forming an Extended Service Set (ESS). When the laptop is turned on it goes through the

authentication step and is granted the ability to associate with an Access Point that is located near her desk. Later, our user takes her laptop to a conference room in another location in the building that is out of range of the original Access Point. At that point the wireless radio in the laptop has 'roamed' to a new Access Point. The *authentication* remains intact across the ESS, and as the mobile station moves throughout the facility, it may need to re-*associate* with another AP.

IP Address Schemes

In an infrastructure network, all network devices must be granted an IP address using a consistent address scheme. Two of the most common schemes in use are static IP addresses and dynamic IP addresses. A network administrator typically makes this decision, and is very involved in managing static IP address schemes. A more typical scheme involves the use of a DHCP server to automatically assign the IP addresses whenever a computer is connected to the network. Most users are at least somewhat familiar with 'Obtain an IP Address automatically'.

In the LiteShow product, we presume that DHCP is in use in the infrastructure network, or that static IP addresses are used in the ad-hoc network. To be technically correct, in the ad-hoc mode the LiteShow product uses a special form of static IP address that is an IANA range address of the form: 169.239.xxx.yyy

DHCP Assumptions

The LiteShow product does make a few presumptions about the address schemes.

We expect that DHCP is the IP Address scheme in an infrastructure network and therefore expect that a DHCP server is present to supply an address. We also expect that in an ad-hoc network that DHCP is not used, and therefore a DHCP server is not present.

See the note above about IANA range addresses.

IP Address and RADIUS Servers

When an infrastructure network administrator implements IP address management, through the use of a RADIUS server, all network devices must go through a more complex sequence of authentication, association and finally IP address allocation. This scheme can also include the use of WEP keys and MAC address filtering. The LiteShow product version 1.2 supports the use of this more elaborate scheme including the use of WEP.

Technical Topics

LiteShow Discovery via Periodic Multicast UDP

LiteShow creates a dynamic discovery mechanism via periodic application-level UDP 'beacons'. These messages are addressed as administrative-scoped multicasts using the multicast group 239.210.99.83 which is described in RFC 2365 *Administratively-scoped IP Multicast*.

BSSID Mobility

When a mobile station (laptop or LiteShow adapter) associates with an Access Point it adopts an Ethernet address known as a Basic Service Set Identifier (BSSID).

All 802.11b mobile stations have the characteristic whereby the BSSID can change according to the association with an Infrastructure AP. We refer to this characteristic as BSSID Mobility. In an Infrastructure configuration, this is generally not an issue, because typically all Access Points have been given the same NetworkName, (ESS) which corresponds to a single IP segment. i.e 192.168/16

Multiple Subnet Considerations

In an infrastructure configuration that segments a single ESS into several sub-networks, (i.e 192.168.1/8 and 192.168.2/8, … etc.) and access to one AP is lost for some reason, the mobile station will re-associate with another BSSID (IP segment). This is specifically a consideration when the IP segments are defined by overlapping Rf coverage zones. In the use case where the LiteShow adapter is on one subnet and the laptop on another subnet, the Multicast UDP LiteShow 'beacons' must be allowed to be routed from one subnet to another to support the LiteShow discovery feature.

TTL – Time To Live

In a network configuration with routers that provide routeability between sub-nets, the number of times that a given packet can be moved across a router is important. To control the undesirable behavior of packets being endlessly routed, the internet community uses Time To Live (TTL) to manage this behavior. We have implemented a TTL value of 15 on the LiteShow adapter which serves to limit the number of hops to within the local domain. The dynamic discovery of LiteShow enabled projectors is facilitated in this type of configuration by allowing the multicast LiteShow beacons to be routed to the next sub-network.

Server MAC Address

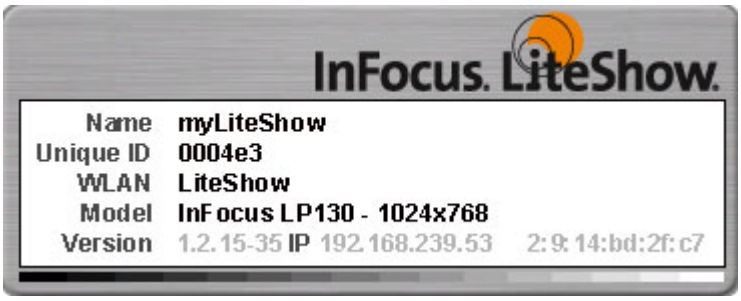
The entire server MAC address can be found on the back of the Netgear Wireless CF Card of the LiteShow adapter.

WLAN Character Set Restriction

The LiteShow system employs a WLAN character set that includes the range from 0x01 through 0x255. The LiteShow server utilizes a font set that is based on the Western Latin-1 font page. In addition, the LiteShow Manager applications utilize the native code page that is the default for that platform, either PC or MAC. This may result in high ascii foreign characters on the Mac or the PC to be displayed differently from the characters displayed on the splashette.

Trouble shooting Techniques

Decoding the LiteShow Splashette Information



LiteShow Name is:	‘myLiteShow’
Automatically generated unique identifier:	0004e3
Wireless LAN Name:	‘LiteShow’
Projector Model – preferred resolution:	InFocus LP130 – 1024x768
Firmware Version:	1.2.15
BootCode Version:	-35
IP Address:	192.168.239.53
BSSID:	02:09:14:bd:2f:c7

Factory Reset

There may exist conditions that require the LiteShow device must have the original factory settings restored. The method to perform this restoration is described in detail in the user manual. In short, disconnect the device, remove the radio, reconnect the device and wait for the countdown mechanism to expire, then replace the radio.

Ping

Confirmation of correct configurations can be preformed using a simple ping test from a wireless laptop to the LiteShow adapter.

IPConfig

On a client machine running the LiteShow Manager software, a convenient method to determine if the wireless configuration settings for the client are correct for the LiteShow adapter, run the command *ipconfig /all* at a command prompt. Significant to observe is the BSSID information for the wireless interface. The BSSID information on the LiteShow splashette should match the BSSID for the client wireless interface. See the section on *Decoding the LiteShow Splashette Information*. On Unix variants, like an Apple Macintosh, the command to use is *ifconfig /a*.

Unique LiteShow Names

We recommend that the default LiteShow name, 'myLiteShow' is changed by the owner of the device and that in an installation where several devices are co-located, each device be given a unique name. In addition, the owner may wish to apply the LiteShow settings password protection option on the device to prevent unwanted changes.

Unique LiteShow WLAN Names

We recommend that the default WLAN name, 'LiteShow' is changed by the owner of the device and the password protection option is enabled. In an infrastructure configuration with a common WLAN name, interoperability with the local shared network resources is provided.

Wireless Infrastructure Terminology

Most of the relevant terminology has been set down in Part I of this white paper.

ESS	***E**xtended **S**ervice **S**et* – a network of two or more Access Points that are configured to use the same NetworkName, thus forming the ESS.
EAP	***E**xtensible **A**uthentication **P**rotocol* - (see RFC draft-ietf-radius-eap-05.txt "Extensible Authentication Protocol Support in RADIUS"). LEAP is a Cisco-proprietary extension to EAP.
RADIUS	***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice* - an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.
TKIP	***T**emporal **K**ey **I**ntegrity **P**rotocol – see WPA*
VPN	***V**irtual **P**rivate **N**etwork* - a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data
WEP	***W**ired **E**quivalence **P**rivacy* – a data encryption technique designed to provide a certain level of data protection.
WPA	***W**i-Fi **P**rotected **A**ccess*, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that

have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP: Improved data encryption through the temporal key integrity protocol (TKIP); User authentication, which is generally missing in WEP, through the Extensible Authentication Protocol (EAP).

Part III: Wireless LAN Security

The following topics summarize the Security and Encryption techniques used in InFocus LiteShow products.

- 128-bit AES encryption – used for encryption of wireless data stream.
- Digitally signed Message Authentication Code (MAC) – used for confirming that software updates are authorized by InFocus.
- Diffie-Hellman key exchange – used to secure the AES key to ensure it is not disclosed at the session setup time.
- session authentication – used to authenticate the user at the beginning of each session.
- physical security of keys – offsite storage facility managed by third party.

Security

Adequate levels of secure wireless communication are achievable, but become increasingly costly for each increase in security. The wireless community has adopted several approaches to create a more secure communication medium. The WiFi Alliance initiatives such as Wired Equivalent Privacy have been useful but incomplete.

Wi-Fi

A widely used and adopted technique for creating a more secure link has involved the use of pre-assigned, static WEP keys. This technique unfortunately has many shortcomings and has in fact been 'cracked', or compromised, especially since the keys are rarely, periodically changed, if ever. Nonetheless, it serves as a minimum level of security that all wireless vendors support. We have included the support for 64-bit and 128-bit WEP keys in the LiteShow product. To support the correct configuration of the LiteShow adapter, the WEP keys are stored in the LiteShow, in a manner that makes them difficult to retrieve. They are sent to the device to the LiteShow manager in an encrypted data stream using 128-bit AES encryption.

Encryption

AES

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, conducted a competition to replace the aging Data Encryption Standard (DES). FIPS-197 describes AES, the Advanced Encryption Standard, as the successor to DES. AES is being incorporated into next generation software throughout the computing industry. InFocus was a leader in adopting AES encryption which is already used by the LiteShow product. InFocus has adopted an AES key length that has been calculated to provide a reasonable level of secure encryption of the wireless content. The encryption community uses a *Work Function* as a part of modeling attacks on a system which is expressed as a dollar amount and a length of time devoted to the attack. The work function that InFocus adopted in 2003 for the LiteShow 1.x product, requires an attacker to spend at least $10,000 on the decoding hardware/software and 10 years of compute time on *each recorded data stream*. Every new data stream requires this expenditure of time and materials. The data stream includes the entire session of information that is sent from the LiteShow Manager to the LiteShow device *when the encryption option is enabled.*

The LiteShow session key exchange at the beginning of a secure session and utilizes the Diffie-Hellman secret key exchange protocol.

LiteShow Secure Updates

The InFocus wireless software update feature provides the means to upgrade the LiteShow adapter firmware. The use of AES encryption during an upgrade ensures that unauthorized programs and content are not placed onto a device. Each update item is signed using an RSA key of length 1,536 bits. If an upgrade payload is tampered with in any manner, the LiteShow device rejects the upgrade. Firmware upgrades comply with the work function described above.

The physical Private key management is handled according to best practices in the industry.

Summary

Following on the background information that has been laid out in a separate document, *Wireless Fundamentals: Part I*, we have provided a more in-depth discussion, in particular concerning Network Architectures and Wireless LAN Security.

We have covered the topics that are important for wireless products to participate in an Infrastructure type network: we define the important hardware and software components that are involved; describe specific methods that are utilized by the InFocus LiteShow product to seamlessly interoperate within pre-existing wireless networks and we conclude with information to assist network administrators to integrate this product. To that extent this document goes beyond the typical white paper content by describing real world example conditions and configurations as they relate to the LiteShow product.

We continue in Part III with a discussion of Wireless LAN Security. We define many of the concepts in the wide field of cryptosystems and compare and contrast the relatively weak Wi-Fi techniques with those employed by LiteShow.