Status of P1451.5 802.11 Sub-Specification

June 7, 2004

Ryon Coleman
Senior Systems Engineer

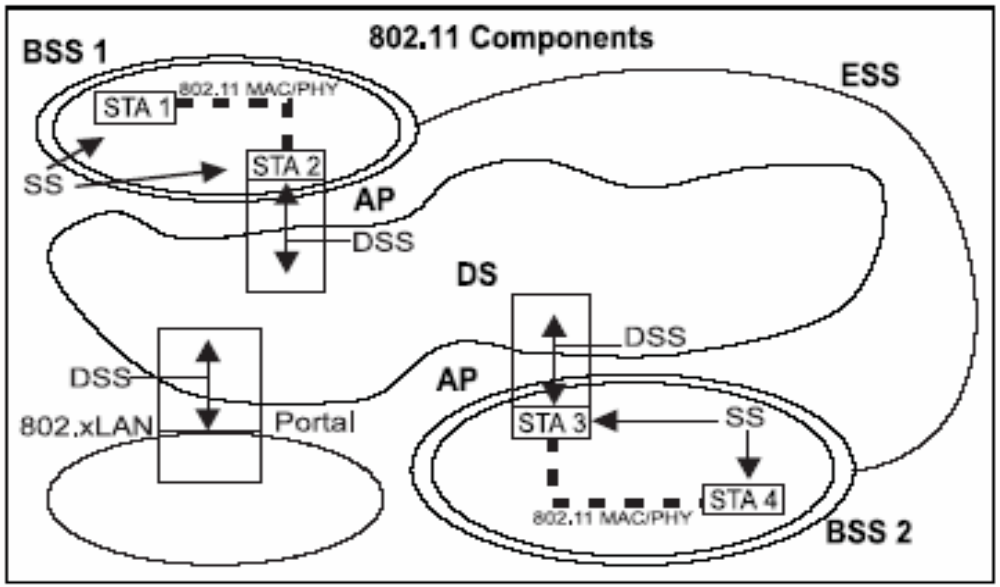
802.11 Subgroup

rcoleman@3eti.com

Agenda

1. IEEE 802.11 Architecture
2. Scope within the 1451 Reference Model
3. Layered Framework in NCAP & WTIM
4. 802.11 Specifications Supported
5. 802.11 MAC & PHY Specification
6. 802.11 Fragmentation
7. 802.11 Addressing
8. 802.11 PHYs Supported
9. IPv4 at Network Layer
10. IPv6 at Network Layer
11. UDP at Transport Layer
12. TCP at Transport Layer
13. Layer 5 (1451.0) Interface to TCP
14. Envisioned API with 1451.0
15. Next Steps

Complete IEEE 802.11 Architecture



Complete IEEE 802.11 Architecture
[ISO/IEC 8802-11: 1999(E) Figure 7]

BSS: Basic Service Set. This is the basic building block of an IEEE 802.11 LAN. Coverage area in which member stations of the BSS may remain in communication.

STA: Station. Envisioned as a 1451.5 WTIM.

AP: Access Point. Envisioned as a 1451.5 NCAP.

DS: Distribution System. Instead of existing independently, a BSS may also form a component of an extended form of network that is built with multiple BSSs. The DS is the architectural component used to interconnect the BSSs.

ESS: Extended Service Set. The DS and BSSs allow IEEE 802.11 to create a wireless network of arbitrary size and complexity, known as an extended service set network.

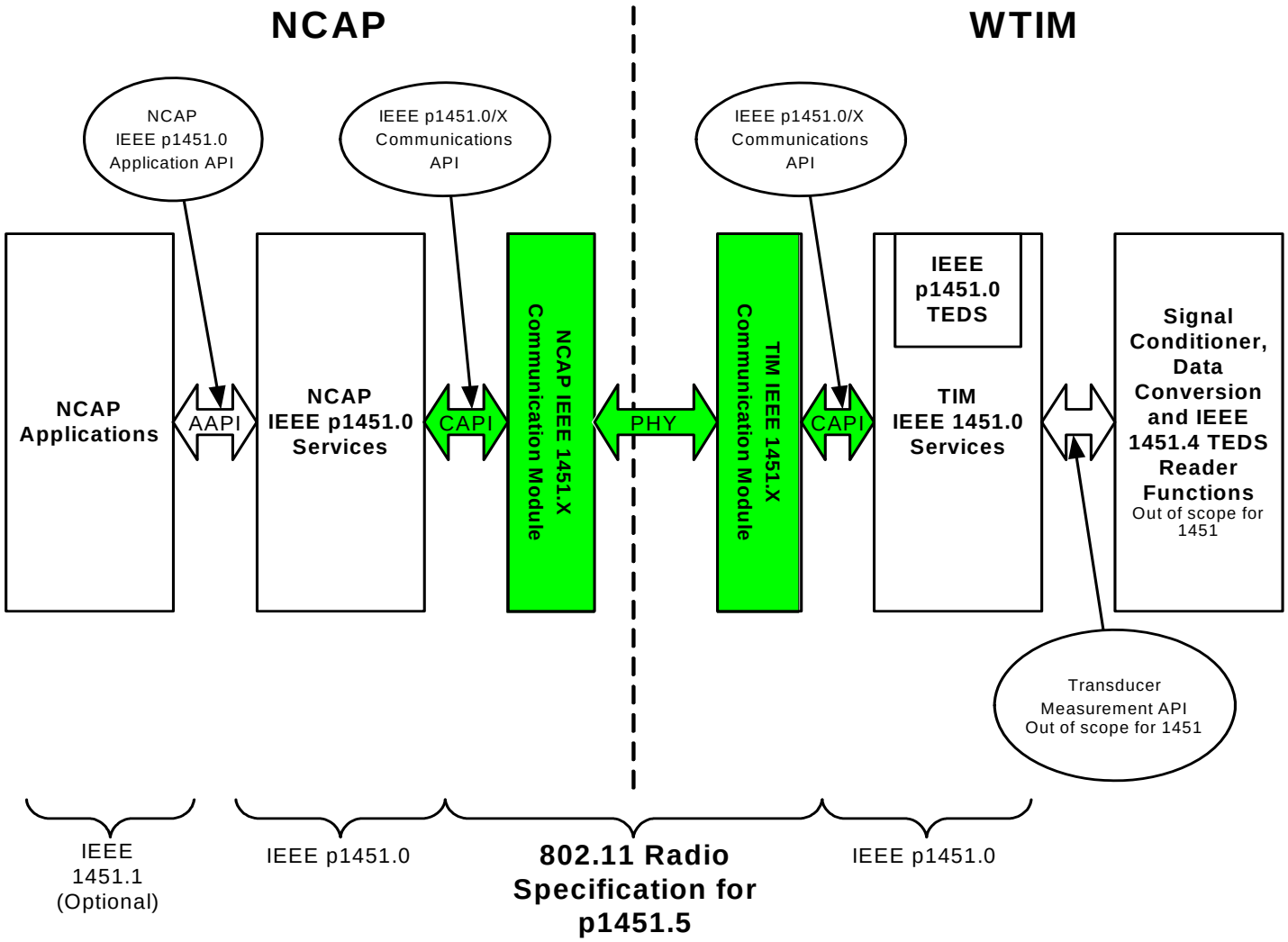
DSS: Distribution System Service. A STA that is providing access to DSS is an AP. **For 1451.5, the AP is envisioned as the NCAP.** The DSS includes:

a) Association
b) Disassociation
c) Distribution
d) Integration
e) Reassociation

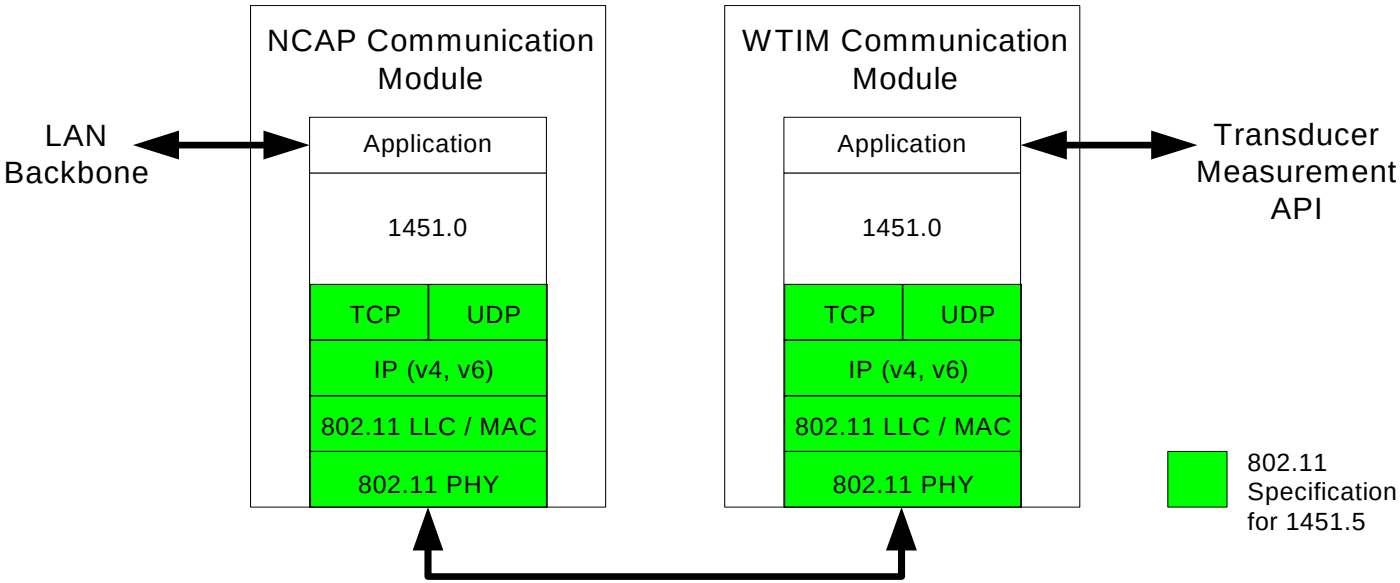
SS: Station Service. The SS is present in every IEEE 802.11 station and AP. The SS includes:

a) Authentication
b) Deauthentication
c) Privacy
d) MSDU (MAC Service Data Unit) delivery

Scope within 1451 Reference Model



Layered Framework in NCAP & WTIM



- **802.11,a/b/g at PHY (physical layer)**
- **802.11,i/e at MAC (datalink layer)**
- **IP version 4 or version 6 (network layer)**
- **TCP or UDP (transport layer)**
- **IEEE p1451.0/X Communications API (communication management)**
- **Application to LAN backbone (NCAP) or TMAPI (WTIM)**

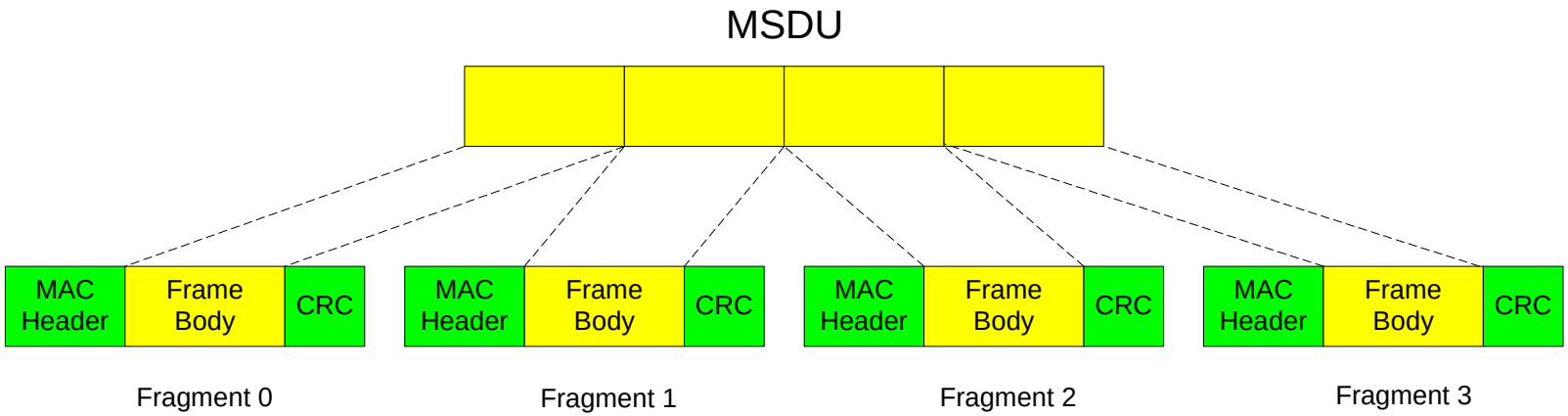
What 802.11 specifications are supported?

- **ANSI/IEEE Std 802.11, 1999 Edition**, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- **IEEE Std 802.11a, 1999**, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band
- **IEEE Std 802.11b, 1999**, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
- **IEEE Std 802.11g, 2003**, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band
- **IEEE Std 802.11i, 2004**, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment i: Medium Access Control (MAC) Security Enhancements
- **PLACEHOLDER: IEEE Std 802.11e, 200?**, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment e: Enhancement for QoS, dynamic frequency selection, power control

802.11 MAC & PHY Specification

- **Multiple logical address spaces within 802.11 MAC & PHY**
- **General Description of 802.11 Radio Specification**
  - 802.11i Security Enhancements General Description
- **MAC Service definition**
  - 802.11i Service definition
- **MAC Frame formats**
  - **802.11b** Beacon frame format, Probe Response frame format, Capability Information field, Status Code field, and Supported Rates element.
  - **802.11g** Format of individual frame types, Control frames, Management frames, Management frame body components, Fixed fields, and Information elements.
  - **802.11i** Protected frames, frame control field, format of individual frame types including data frames and management frames (with RSN Information Element), management frame body components with Capability Information fixed field, RSN Information Element, Cipher Suites, Authentication and Key Management Suites, RSN Capabilities, PMKID, and RSN IE Examples.

802.11 Fragmentation



- **Fragmentation** creates MPDUs (MAC Protocol Data Units) smaller than the original MSDU (MAC Service Data Unit).
  - Increases **reliability**, by increasing the probability of successful transmission of the MSDU in cases where channel characteristics limit reception reliability for longer frames.
- Fragmentation is accomplished at each immediate transmitter.
- Defragmentation recombines the MPDUs into the original MSDU and is accomplished at each immediate recipient.

802.11 MAC & PHY Specification (continued)

- **Security: 802.11i (optional)**
  - Includes framework, pre-RSNA security methods, RSNA data confidentiality protocols including TKIP and CCMP, RSNA security association management, keys and key distribution including key hierarchy, EAPOL-KEY frames, 4-way handshake, group key handshake, RSNA supplicant key management state machine, RSNA authenticator key management state machine, and nonce generation (informative), mapping EAPOL keys to IEEE 802.11 keys, and per-frame pseudocode including WEP frame pseudocode and RSNA frame pseudocode.
- **MAC Sublayer functional description**
  - Fragmentation and defragmentation, Multirate support, allowable frame exchange sequences, additional restrictions to limit the cases in which MSDUs are reordered or discarded.
- **Layer Management 802.11a/b/g/i**
  - Overview of management model, generic management primitives, MLME SAP (MAC sublayer management entity service access point) interface, and PLME SAP interface.
  - **802.11i** Scan, Associate, Reassociate, SetKeys, DeleteKeys, Michael MIC Failure Event, EAPOL (Michael MIC Failure Report).

802.11 Addressing

- **Individual Address**: 48-bit MAC address (IEEE Std. 802-1990) associated with a particular station (STA or AP).
- **Multicast Group Address**: An address associated with a higher-level convention with a group of logically related stations.
- **Broadcast Address**: All 1's in the Destination Address field are interpreted as the broadcast address. Set of all stations on a given LAN

802.11 supports Individual, Multicast & Broadcast Addressing

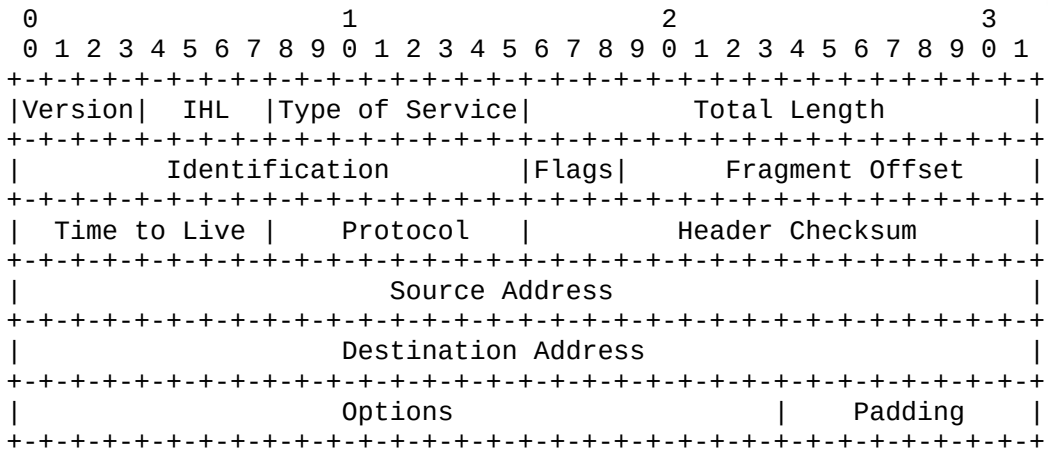
802.11 PHYs Supported

- **Frequency-Hopping spread spectrum** (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band (optional) **802.11-99**
- **Direct sequence spread spectrum** (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications (optional) **802.11-99**
- **Infrared** (IR) PHY specification (optional) **802.11-99**
- **OFDM PHY** specification for the 5 GHz band (optional) **802.11a**
- High Rate, direct sequence spread spectrum PHY specification (optional) **802.11b**
- High Rate, direct sequence spread spectrum PHY specification for **802.11g** (optional)
- **Extended Rate PHY specification for 802.11g** (optional)

IPv4 (optional) at Network Layer

- IETF **RFC 791**: Internet Protocol, DARPA Internet Program, Protocol Specification, September 1981
- IPv4 provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses.
- IPv4 provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.
- The purpose of IPv4 is to move datagrams through an interconnected set of networks. This is done by passing the datagrams from one NCAP communication module to WTIM communication module, or vice versa, until the destination is reached.
- Support for IPv4 is optional; however, either IPv4 or IPv6 shall be used at the network layer to comply with 1451.5 802.11 sub-specification.

IPv4 Datagram Header



IPv4 Datagram Header

Within the IPv4 header, the fields include:

Version (4 bits), Internet Header Length (4 bits), Type of Service (8 bits), Total Length (16 bits), Identification (16 bits), Flags (3 bits), Fragment Offset (13 bits), Time to Live (8 bits), Protocol (8 bits), Header Checksum (16 bits), Source Address (32 bits), Destination Address (32 bits), Options (variable width), and Padding (variable width). The IPv4 header is always 32-bit aligned due to the variable width zero-padding.

IPv6 (optional) at Network Layer

- IETF **RFC 1752**: The Recommendation for the IP Next Generation Protocol, January 1995
- There are several important features of IPv6, which include:
  - Expanded addressing and routing capabilities - The IP address size is increased from 32 bits to 128 bits.
    - much greater number of addressable nodes
    - more levels of addressing hierarchy
    - simpler auto-configuration of addresses
  - Scaleability of **multicast routing** is improved by adding a "scope" field to multicast addresses.
  - A new type of address, called a "cluster address" is defined to identify topological regions rather than individual nodes. The use of cluster addresses in conjunction with the IPv6 source route capability allows nodes additional control over the path their traffic takes.
- Support for IPv6 is optional; however, either IPv4 or IPv6 shall be used at the network layer to comply with 1451.5 802.11 sub-specification.

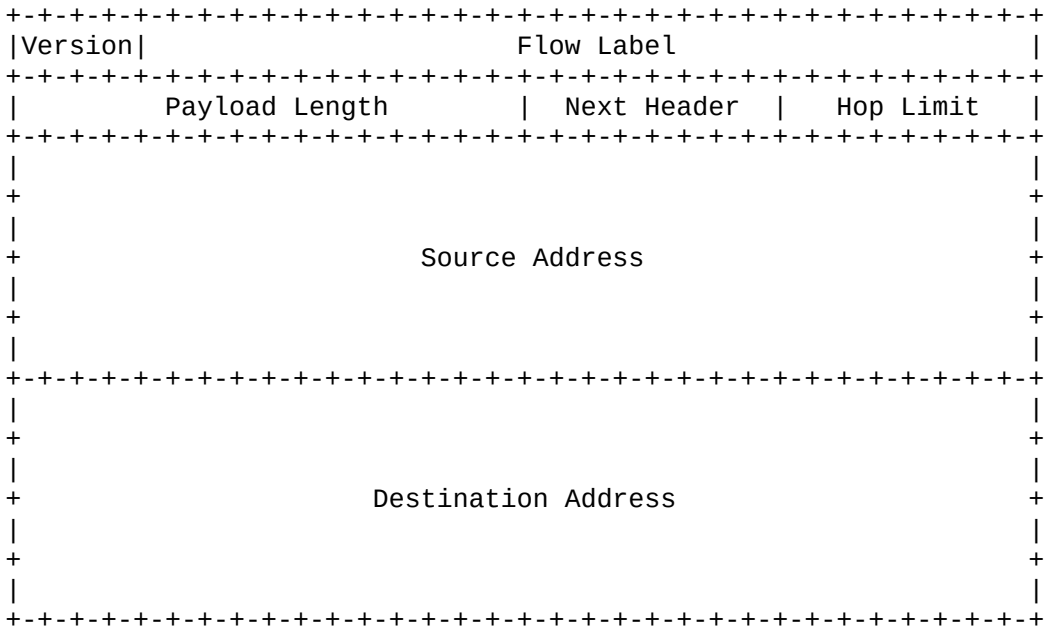
IPv6 Simplified Header & Extension Headers

- **Simplified header format** - Some IPv4 header fields have been dropped or made optional to reduce the common-case processing cost of packet handling and to keep the bandwidth overhead of the IPv6 header as low as possible. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.
- **Support for extension headers and options** - IPv6 options are placed in separate headers located in the packet between the IPv6 header and the transport-layer header. Since most IPv6 option headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination, this organization facilitates a major improvement in router performance for packets containing options. Another improvement is that unlike IPv4, IPv6 options can be of arbitrary length and not limited to 40 bytes.

IPv6 Authentication & Privacy, Autoconfiguration, QoS Support

- **Support for authentication and privacy** - IPv6 includes the definition of an extension which provides support for authentication and data integrity. IPv6 also includes the definition of an extension to support confidentiality by means of encryption.
- **Support for autoconfiguration** - IPv6 supports multiple forms of autoconfiguration, from "plug and play" configuration of node addresses on an isolated network to the full-featured facilities offered by DHCP.
- **Quality of service capabilities** - A new capability is added to IPv6 to enable the labeling of packets belonging to particular traffic "flows" for which the sender has requested special handling, such as non-default quality of service or "real-time" service.

IPv6 Datagram Header



IPv6 Datagram Header

Within the IPv6 header, the fields include:
Version (4 bits), Flow Label (28 bits), Payload Length (16 bits), Next Header (8 bits), Hop Limit (8 bits), Source Address (128 bits), and Destination Address (128 bits).

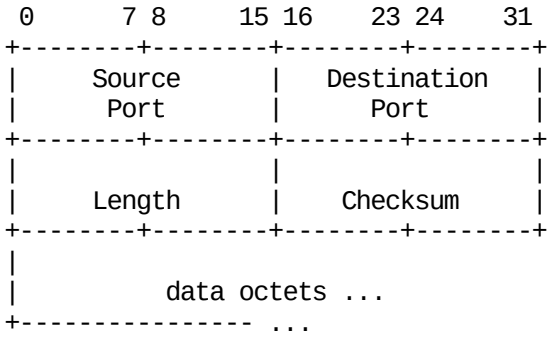
IPv6 Extension Headers

- In IPv6, optional network-layer information is encoded in separate headers that may be placed between the IPv6 header and the transport-layer header in a packet.
- There are a small number of such **extension headers**, each identified by a distinct Next Header value.
- Refer to **RFC 1752 section 12.2** “Extension Headers” for additional specification
- Extension Headers include:
  - (12.2.1) **Hop-by-Hop Option Header**
  - (12.2.2) **IPv6 Header Options**
  - (12.2.3) **Routing Header**
  - (12.2.4) **Fragment Header**
  - (12.2.5) **Authentication Header**
  - (12.2.6) **Privacy Header**
  - (12.2.7) **End-to-End Option Header**

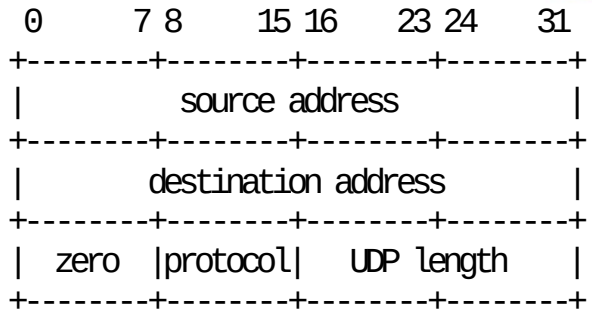
UDP (optional) at Transport Layer

- IETF **RFC 768**: User Datagram Protocol, August 1980 (UDP)
- UDP provides a procedure for application programs to send messages to other programs with a **minimum of protocol mechanism**. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed.
- The (Layer-5—UDP) “user” interface should allow:
  - the creation of new receive ports
  - receive operations on the receive ports that return the data octets and an indication of source port and source address
  - an operation that allows a datagram to be sent, specifying the data, source and destination ports and addresses to be sent.
- Support for TCP is optional; however, either TCP or UDP shall be used at the transport layer to comply with 1451.5 802.11 sub-specification.

UDP Header Format



UDP Header Format



UDP Pseudo Header Format

Within the UDP header, the fields include:

Source Port (16 bits) Destination Port (16 bits) Length (16 bits) – Length is the length in octets of this user datagram including this header and the data. Checksum (16 bits) – Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header.

UDP Pseudo Header:

The pseudo header conceptually prefixed to the UDP header contains the source address, the destination address, the protocol, and the UDP length. This information gives protection against misrouted datagrams.

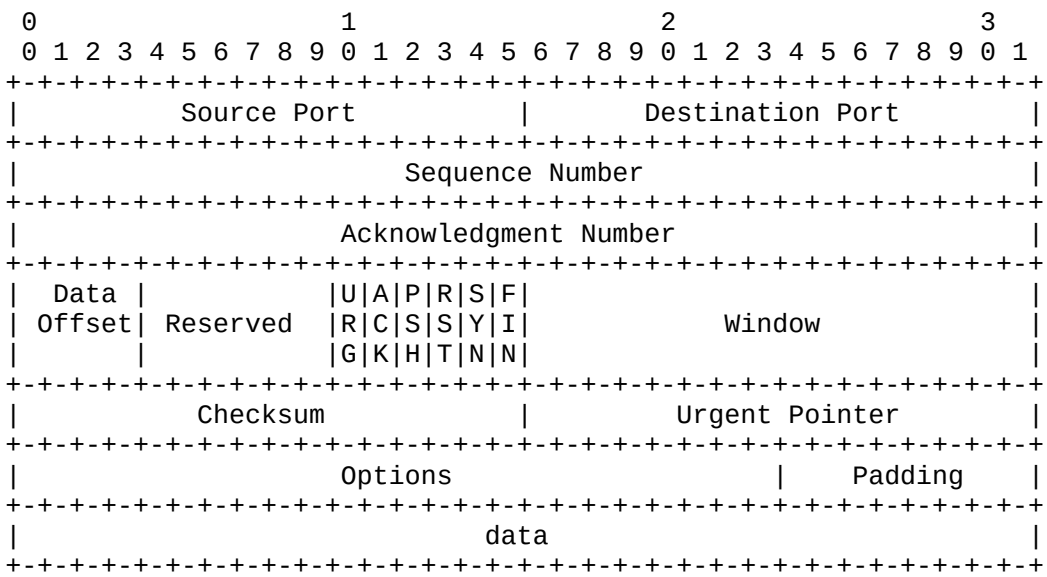
TCP (optional) at Transport Layer

- IETF **RFC 793**: Transmission Control Protocol, DARPA Internet Program, Protocol Specification, September 1981
- TCP is intended for use as a highly reliable host-to-host transport-layer protocol between NCAPs and WTIMs in the packet-switched “802.11 p1451.5” communication network, and in interconnected systems of such networks.
- TCP is a **connection-oriented, end-to-end reliable protocol** designed to fit into a layered hierarchy of protocols which support multi-network applications.
- TCP provides for reliable inter-process communication between pairs of processes in host NCAPs or WTIMs. To provide its services, TCP specifies facilities in the following areas:
  - Basic Data Transfer
  - Reliability
  - Flow Control
  - Multiplexing
  - Connections
  - Precedence
  - Security
- Support for TCP is optional; however, either TCP or UDP shall be used at the transport layer to comply with 1451.5 802.11 sub-specification.

Salient Properties of TCP

- A stream of data sent on a TCP connection is delivered **reliably** and **in order** at the destination. Transmission is made reliable via the use of sequence numbers and acknowledgments.
  - Because segments may be lost due to errors (checksum test failure), or network congestion, TCP uses retransmission (after a timeout) to ensure delivery of every segment.
- To provide for unique addresses within each TCP, an internet address identifying the TCP is concatenated with a port identifier to create a **socket** which will be unique throughout all networks connected together. A connection is fully specified by the pair of sockets at the ends.
- TCP makes use of the IP type of service field and security option to provide **precedence** and **security** on a per connection basis to TCP users.
  - The intent is that connection be allowed only between ports operating with exactly the same security and compartment values and at the higher of the precedence level requested by the two ports. The precedence and security parameters used in TCP are exactly those defined in the Internet Protocol (IPv4 or IPv6).

TCP Header Format



TCP Header Format

Within the TCP header, the fields include:

Source Port (16 bits), Destination Port (16 bits), Sequence Number (32 bits), Acknowledgment Number (32 bits), Data Offset (4 bits), Reserved (6 bits), Control Bits (6 bits), Window (16 bits), Checksum (16 bits), Urgent Pointer (16 bits), Options (variable), Padding (variable), and Data (variable).

Layer 5 (Dot0) Interface to TCP

- The activity of the TCP can be characterized as responding to events. The events that occur can be cast into three categories: user calls, arriving segments, and timeouts.

- User (i.e. Layer-5) Calls
- **OPEN**
- **SEND**
- **RECEIVE**
- **CLOSE**
- **ABORT**
- **STATUS**

- Arriving Segments
- SEGMENT ARRIVES

- Timeouts
- USER TIMEOUT
- RETRANSMISSION TIMEOUT
- TIME-WAIT TIMEOUT

Envisioned API with Dot0

- **Open**
  - Format: OPEN (local port, foreign socket, active/passive [, timeout] [, precedence] [, security/compartment] [, options]) -> local connection name
- **Send**
  - Format: SEND (local connection name, buffer address, byte count, PUSH flag, URGENT flag [,timeout])
- **Receive**
  - Format: RECEIVE (local connection name, buffer address, byte count) -> byte count, urgent flag, push flag
- **Close**
  - Format: CLOSE (local connection name)
- **Status**
  - Format: STATUS (local connection name) -> status data
- **Abort**
  - Format: ABORT (local connection name)

Next Steps

- Establish & Finalize API with Dot0 this week at Sensors Expo
  - QoS Parameters
  - Multicast, Publish/Subscribe Group Identification
- Work out any convergence layer issues to make the (3) radio subgroups look more uniform to Dot0
- Establish any 802.11-specific PHY TEDS
- Publish 1451.5 802.11 draft sub-specification

Thank You!