RoboCup SSL 5Ghz Wi-Fi Specification

Draft Proposal

The goal of the document is to describe the first prototype version of a shared 5GHz Wi-Fi network for the RoboCup Small Size League. This network is intended to support all teams using 5GHz Wi-Fi for robot command and control.

Background
- Motivation
- Requirements
- Technical Considerations
  - Static vs Dynamic Address Allocation
  - Channel Allocation
  - Non-802.11a/ac/n 5GHz Radios
  - Security
  - Reserved Network Ranges

Physical Network Architecture

IP Network Architecture
- Address Blocks

Standard Discovery Protocol
- Packet Structure

Suggested Equipment
- Access Points
- Embedded Radios

Background

Motivation

The motivation behind this initiative is two fold:

1. **5GHz Wi-Fi channels are a limited commodity**. Currently, all teams using 5GHz Wi-Fi bring their own router and pick or are assigned a unique channel. This means the SSL needs a large allocation of the spectrum, which creates challenges for interference within the league and across the venue. Using a unified network will reduce the channel allocation alleviating this concern.
2. Communication between the coach computer and robots is often a sticking point for new (and returning) teams. Debugging unreliable communications at a unique venue every year is unconstructive in progressing the league. A league standardized network and optional standardized discovery protocol would provide teams with a high confidence

option for communications allowing teams to focus on problems relevant to league advancement.

Requirements

Before proposing an architecture, we first propose requirements.

- **Performance - Latency** - Teams are expected to be concerned about performance on a shared network, specifically the transmission latency of control packets. High packet loss or high delay between the coach and robot can cause control stability and general performance problems. We assume most teams are running the on-board top-level control at around 100Hz, meaning the arrival of a packet within a 10ms timeframe is treated approximately the same. With a baseline time granularity established, a reliability index to meet this latency is created. We target a Z-Score z=2.5 threshold for on-time arrival, or permit approximately 1-in-100 packets to be lost, meaning they arrive outside of this timing threshold or are lost all together.
- **Performance - Throughput** - Sometimes called bandwidth, we expect teams to be concerned that the network can actually offload enough data to be a viable solution. For 5GHz Wi-Fi in particular, this is assumed to be a non-issue given the substantial baseline throughput the standard supports.
- **Implementation Support** - 5GHz Wi-Fi is just a physical access medium (PHY) to a traditional computer IP network. Just as there are a substantial number of ways to architect computer to computer communications on IP networks, different teams have architected different ways to have their coach computer(s) and robots communicate. Any league solution needs to support whatever teams want to do to encourage adoption. Some known network implementations are included in the list below:
    - Full Self Discovery - Neither the coach computer(s) nor the robots have fixed IP addresses or networks. Coaches and robots discover each other via agreed-upon IGMP/Multicast groups, similar to how League software messages are distributed. Coaches and robots are allocated addresses via a DHCP server hosted by the router.
        - Pros: Avoids per-robot hardcoded networking parameters
        - Cons: more sophisticated implementation
        - Team Usage: The A-Team
    - Static Coach IP - The coach computer has a fixed IP address but the robots do not. The firmware must know the coach computer IP address. When the robots turn on they initiate communication with the coach computer and in doing so the coach computer now knows where to reply.
        - Pros: Simpler code and setup
        - Cons: coach computer IP changes or network address changes require a firmware update on all robots
        - Team Usage: RoboJackets (~2019-present)
    - Static Robot IP - The robots have static IP addresses but the coach(es) do not. The coach must know the expected robot ip addresses and attempt

communication to know when the robots are turned on. In receiving communication from the coach, the robots know where to reply.
        - Pros: robot addresses are always known, simpler code
        - Cons: robots need unique addresses and therefore unique firmware (or switch set by a user which can cause address conflicts), a change to network subnet requires robot firmware updates
        - Team Usage: Thunderbots
    - Static Coach and Static Robot IP - The robots and coach all have static IP addresses. Either side can initiate communication because all sides know the addresses of everyone.
        - Pros: all addresses are known, simplest code
        - Cons: any network changes (addresses or subnet) requires reconfiguring both the coach and robot firmware
        - Team Usage: Thunderbots
    - High Level Protocol Communication - Some teams may also optionally use high level protocols as utilities. A common example might be the use of SSH to access Linux Single Board Computers (SBCs) like Nvidia Jetsons or Raspberry PIs. If static IPs are used, then the team knows where the device is. Alternatively, a mDNS (multicast DNS) hostname lookup is performed by the local network and the machine can be connected to by hostname.
        - Team Usage: Thunderbots

Technical Considerations

Static vs Dynamic Address Allocation

Generally, simultaneous static and dynamic address allocation can cause problems. Devices using static addresses cannot pick a static IP address guaranteed to have not been allocated by DHCP or taken by another device. These limitations can be mitigated by restricting the two allocation paradigms to different subnets. DHCP and static devices can comfortably operate in ranges they know won't be used by the other.

Channel Allocation

5GHz Wi-Fi channels are allocated per *access point*, not per subnet, VLAN, or SSID. This is a function of how the PHY standard works and isn't negotiable.

Non-802.11a/ac/n 5GHz Radios

This specification does not cover non-Wi-Fi radios in any way. The 5GHz Wi-Fi standards are 802.11a, 802.11n, and 802.11ac. Non Wi-Fi radios are allowed to operate here under what is generally described as the Industrial Scientific and Medical (ISM) band. Efforts will be taken to deconflict channel selections from any teams operating non-Wi-Fi radios in the ISM band.

Security

This specification largely leaves network security to the individual teams. It's expected that teams ask questions about security. For ease of operation and support of multiple types of team connection architectures, team subnets are not firewalled off. This would greatly complicate the interaction between DHCP and static ranges, as well as advanced protocols which are 4 of 5 of possible architectures. If teams are concerned about other teams snooping on their robot commands, they can choose to encrypt their traffic. As for denial of service attacks and flooding, the coach computers are already vulnerable to this via the shared league network for vision/ref and so this is not a novel concern. Additionally, no teams have a public key registered with the SSL game controller (on the Test Team public key is there) so it appears the general level of trust is high. Any traffic snooping or attacks would be considered unsportsmanlike conduct and grounds for an immediate disqualification from a policy standpoint.

Reserved Network Ranges

ipv4 reserves three major network blocks for internal and debug use:

- 172.16.0.0/12
- 192.168.0.0/16
- 10.0.0.0/8

The host venue will use one of these three networks for internet drops and internet connect Wi-Fi. We will pick one that is not used by the venue.

Physical Network Architecture

The physical network architecture for standardized 5GHz Wi-Fi in SSL minimally extends the existing league network architecture.

Each field has a wired network to connect team coach computers to the game controller and vision server. To enable 5GHz Wi-Fi for robot communication, one Wi-Fi access point is added to the field network. Each field access point is configured with a unique SSID, such as "SslDivA".

Optionally, an additional access point can be provided for teams to use when they are away from the field.

TODO: network diagram

IP Network Architecture

The IP address space of the field network will be divided into multiple subnets to provide ranges of usable addresses for different purposes. This allows us to comfortably support different equipment and team needs without having to worry about address conflicts. In particular, teams are free to use any combination of statically and dynamically allocated addresses within the constraints described below.

The overall address space will be chosen from one of the three reserved private network blocks. The driving factor in the choice for each event will be avoiding conflict with the upstream venue network. Thus the entire field network will live in one of the following three address spaces:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

In practice, a /16 address space will be chosen such that the first two octets are the same for all devices in the network.

It is highly recommended the network operator use the router firewall to block internet access, even though the router may be connected to an internet connected upstream network for remote monitoring and administration. It is expected that with many users, anything like a video stream or large file download could degrade robot communication performance.

Address Blocks

Within the field network address space, the following blocks will be reserved for specific uses.

Address Block	**Address Range**	**Address Count**	**Purpose**
192.168.0.0/18	192.168.0.0 - 192.168.63.255	16,384	League equipment.
192.168.64.0/18	192.168.64.0 - 192.168.127.255	16,384	Static allocation range for teams. Each team gets a /24 block.
192.168.128.0/18	192.168.128.0 - 192.168.191.255	16,384	Dynamic allocation range for teams.
192.168.192.0/18	192.168.192.0 - 192.168.192.255	16,384	Unused. Reserved for future use.

Note: The first two octets used in this table (192.168.) are examples and might be different in practice.

The league equipment range is governed by the TC/OC and is intended for devices such as network infrastructure (ie. routers) and league servers (GC and vision). These devices will need to be configured with static addresses.

The static allocation range for teams is further divided into individual team subnets. Each team is allocated a /24 network block. Within this block they will have 256 addresses to do with as they please. These blocks can be assigned and communicated well before the event. This architecture supports up to 64 teams using static IP addresses on the same field simultaneously. For example, an event may assign 192.168.70.0/24 to Team A, 192.168.71.0/24 to Team B, and so on down the team list.

The dynamic allocation range will be controlled by the network's DHCP server (usually built into the router or access point on the network). Devices choosing to use dynamic address allocation may expect to get any address in this block. There is no guarantee that all of a team's devices will land in the same /24 block. With over sixteen thousand addresses available, if all twelve division B teams chose to use dynamic allocation, they would each be able to connect over one thousand devices before running out of addresses.

The final /24 block of the network is reserved but unused. Teams should not depend on this range as the league may extend this specification into that range or use the range for adhoc needs without warning.

Standard Discovery Protocol

To allow teams to discover robots using dynamically allocated addresses, a simple discovery protocol is specified which teams may use. This specification leaves open the option for teams to use other means to discover their robots and only asks that teams choosing not to use the standard protocol avoid using the multicast address and port used by this protocol.

The standard discovery protocol consists of a single packet type that is published to an IGMP multicast group. This packet contains identifying information about the robot that sent it such that team coach computers can recognize their robots and learn their assigned addresses.

Once a robot connects to the field network and is assigned an IP address, it may send a multicast UDP packet to the multicast group with address 224.4.20.69 and port 42069. These discovery packets should not be sent more frequently than 10Hz. Team coach computers join this multicast group and listen for discovery packets. When a packet is found that comes from one of that team's robots, the coach computer can extract the sending IP address from the IPv4 header.

Packet Structure

The standard discovery packet is a simple encoding of key identifying information for a robot. It is worth noting the standard eschews popular serialization frameworks such as Google's Protobuff in favor of a direct byte layout because not all embedded controllers that could be used on a RoboCup robot easily support these more advanced serialization approaches.

The discovery packet encodes the following information:

- Team Name
- Team Color
- Robot ID

These three fields are sufficient to completely identify a robot on the field and allow for teams to scrimmage against themselves by including the team color.

The byte layout of the packet is as follows:

16 bytes	1 byte	1 byte
Team name (<= 16 characters)	Team color (0=Blue, 1=Yellow)	Robot ID (0-15)

Suggested Equipment

No specific equipment requirements are imposed by this standard besides compliance with the 5GHz Wi-Fi standards (802.11a / 802.11n / 802.11ac). The following lists of recommended equipment are provided to help teams who would rather not spend time researching quality Wi-Fi products.

Networking

There are certainly other options, I just know these options fairly well.

- Router/AP Configuration Management: Unifi Cloud Gateway Pro
  - $129.00
  - Quantity: 1
  - Configures Access Points and Switches, provides a DHCP server, provides spectrum analysis for 2.4 and 5GHz Wi-Fi
- Access Points: U6+
  - $129.00
  - Quantity: 3
  - Broadcasts Wi-Fi for each field, 1gbit total bandwidth per field
- Switch: Ultra 60W
  - 159.00 USD
  - Quantity: 3
  - One switch per field power the access point and provides 6 wired connections for team laptops (3 per team for a match)

Total Cost: 993.00 USD + Tax + Shipping

Embedded Radios (on robot radios)

Should collect from teams what they use and if they like it. Perhaps this can be a starting point for new teams.

- Odin-w262
  - Used By: The A-Team
  - Price: 37.93
  - Supports 5GHz Wi-Fi, 2.4GHz Wi-Fi, Bluetooth (all off by default)
  - Interface: UART, RMII
  - Dev Boards? Yes
  - Breadboard Module? No
  - Optional U.FL external antenna connector instead of On-Chip Antenna (OCA)