IEEE 802.11s Tutorial

Overview of the Amendment for Wireless Local Area Mesh Networking

IEEE 802 Plenary, Dallas
Monday, Nov 13, 2006, 6:30 PM

W. Steven Conner, Intel Corp.

Jan Kruys, Cisco Systems

Kyeongsoo (Joseph) Kim, STMicroelectronics

Juan Carlos Zuniga, InterDigital Comm. Corp.

Key Contributors

- **Donald E. Eastlake 3rd, Motorola**
- **Susan Hares, NextHop**
- **Guido Hiertz, Philips**
- **Meiyuan Zhao, Intel**

Abstract

- **Network communications with end devices is increasingly wireless. Many standards for wireless networking are now taking the next step to support mesh architectures in which data is commonly forwarded on paths consisting of multiple wireless hops .**
- **This tutorial will explore the 802.11s amendment being developed to add mesh capabilities to the wireless local area networking (WLAN) standard.**

Outline

- **Part 1, W. Steven Conner**
  - 802.11s Overview
  - 802.11s Extensible Framework
- **Part 2, Jan Kruys**
  - 802.11s Security
  - 802.11s Routing
- **Part 3, Joseph Kim**
  - 802.11s Interworking
  - 802.11s Data Frame Format and 6 Address Scheme
- **Part 4, Juan Carlos Zuniga**
  - 802.11s MAC Enhancements
  - 802.11s Beaconing, Synchronization, and Powersave

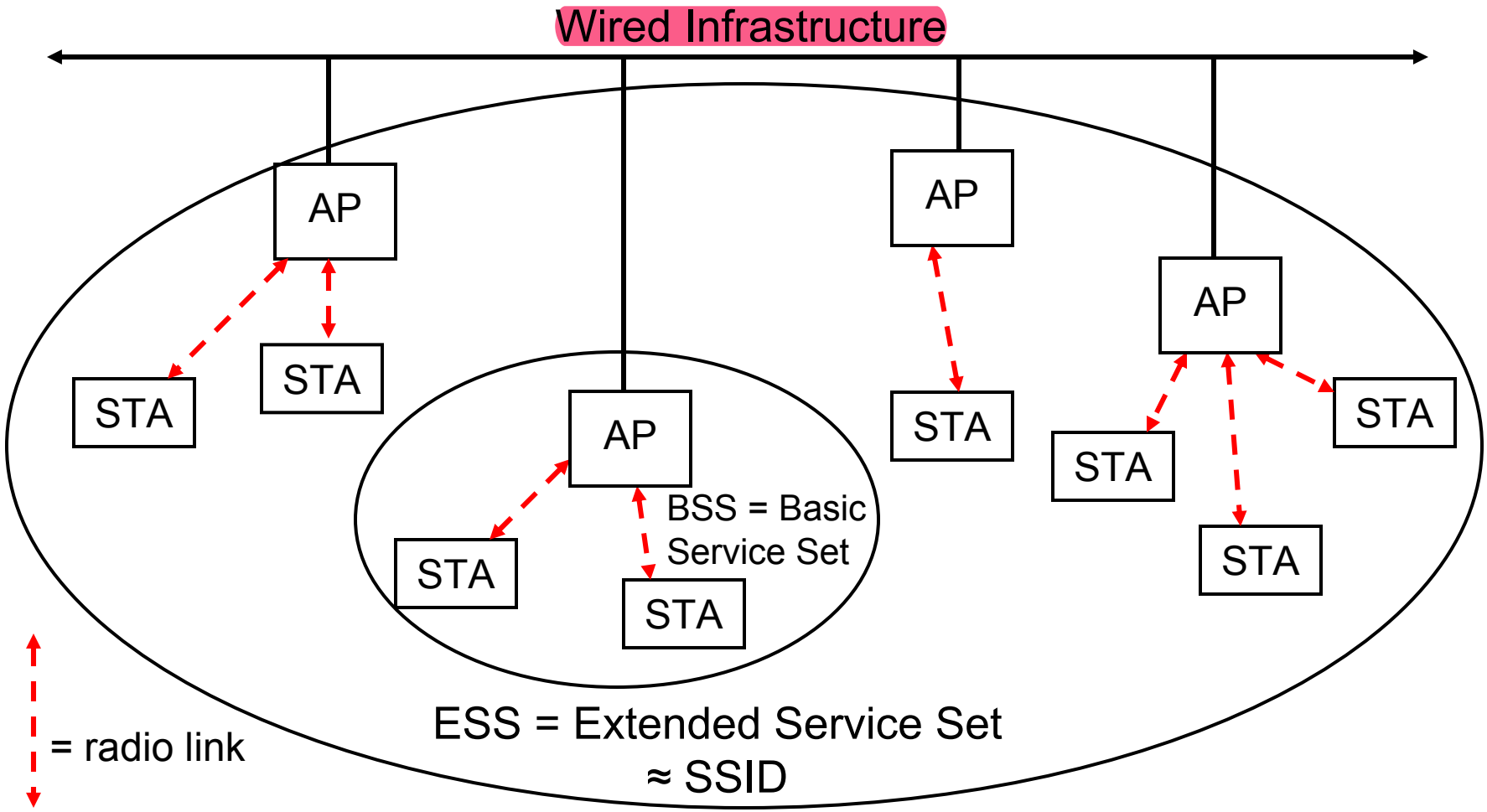
Part 1: Overview

W. Steven Conner, Intel Corp.

- **802.11s Overview**
- **802.11s Extensible Framework**

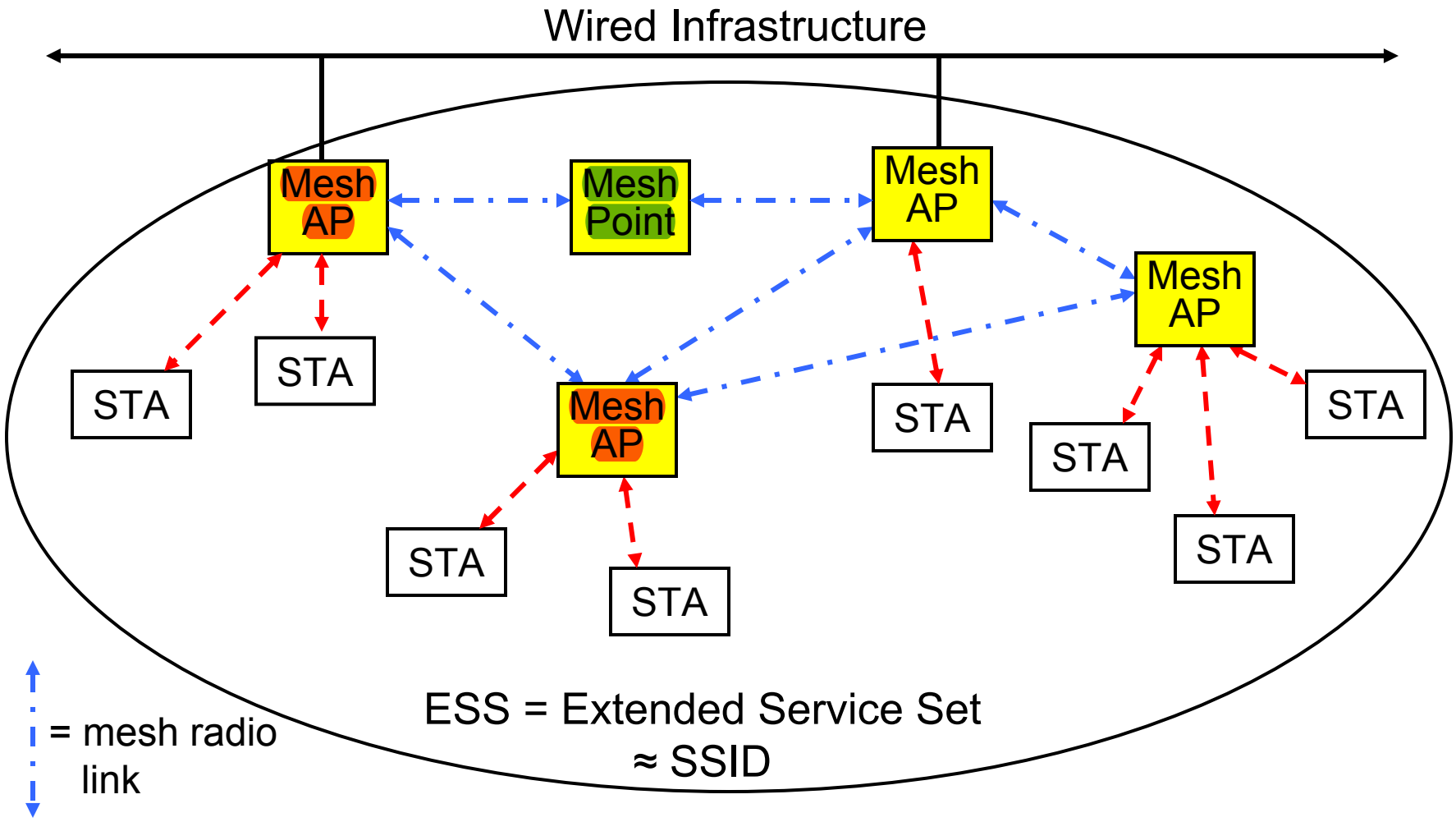
Why, What, How?

Classic 802.11 WLAN



Wireless Paradox: WLAN Access Points are Typically Wired

Unwire the WLAN with Mesh



Why Mesh?

- **What's so good about Mesh?**
  - Enables rapid deployment with lower-cost backhaul
  - Easy to provide coverage in hard-to-wire areas
  - Self-healing, resilient, extensible
  - Under the right circumstances:
    - Greater range due to multi-hop forwarding
    - Higher bandwidth due to shorter hops
    - Better battery life due to lower power transmission

What is IEEE 802.11s?

- **802.11s is an amendment being developed to the IEEE 802.11 WLAN (Wireless Local Area Networks) standard.**
- **The current standard is IEEE 802.11-1999 plus the following ratified amendments (available for download from http://standards.ieee.org/getieee802/):**
  - 802.11a, 802.11b, 802.11g
  - 802.11e, MAC Quality of Service Enhancements
  - 802.11h, Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe
  - 802.11i, MAC Security Enhancements
  - 802.11j, 4.9 GHz–5 GHz Operation in Japan

802.11s Scope

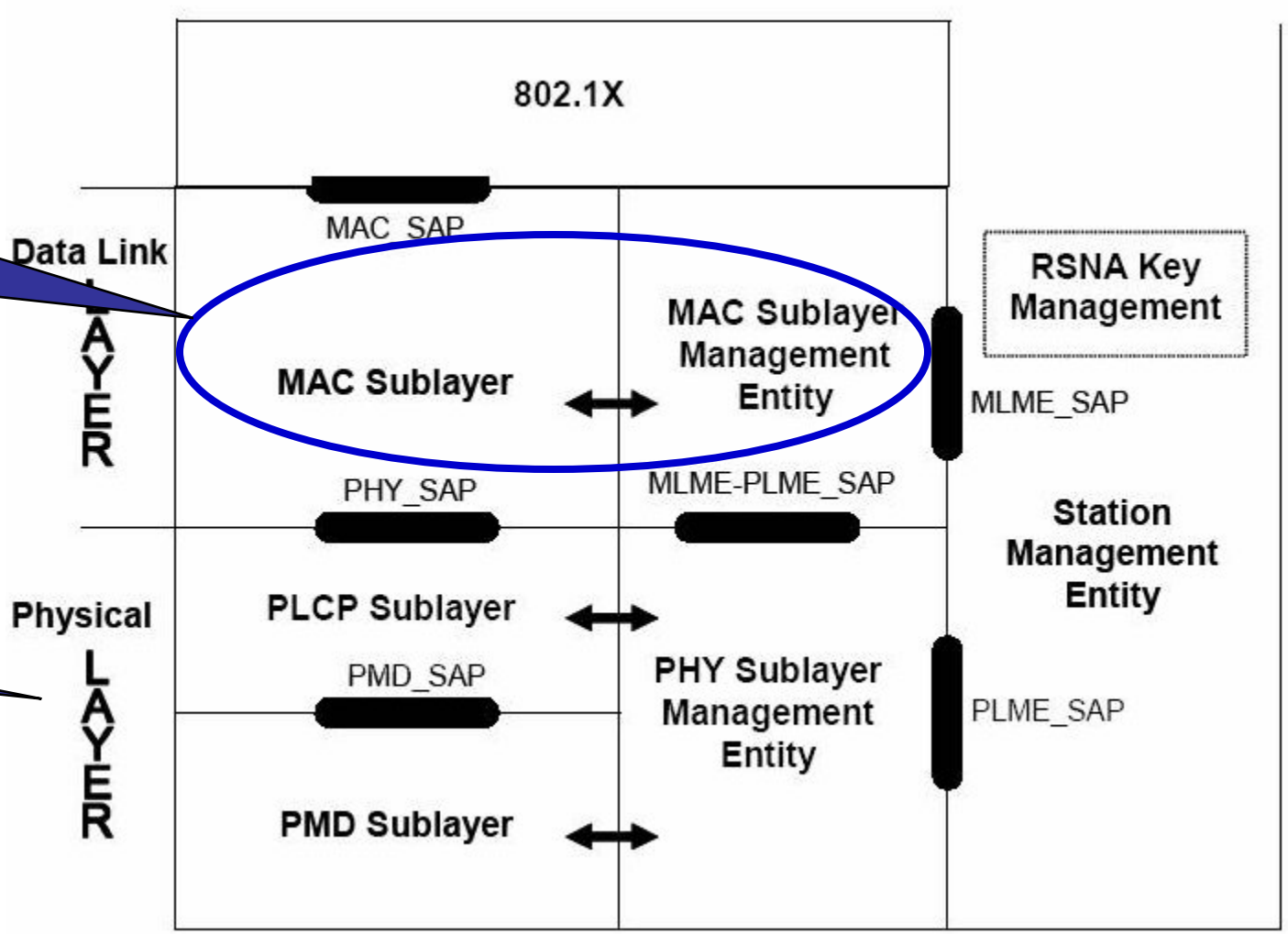
- **802.11s WLAN Mesh Networking**
  - Integrates mesh networking services and protocols with 802.11 at the MAC Layer

- **Primary Scope:**
  - Amendment to IEEE 802.11 to create a Wireless Distribution System with automatic topology learning and wireless path configuration
  - Small/medium mesh networks (~32 forwarding nodes) – can be larger
  - Dynamic, *radio-aware* path selection in the mesh, enabling data delivery on single-hop and multi-hop paths (unicast and broadcast/multicast)
  - Extensible to allow support for diverse applications and future innovation
  - Use 802.11i security or an extension thereof
  - Compatible with higher layer protocols (broadcast LAN metaphor)

802.11s Scope (cont.)

802.11s is an amendment to the 802.11 MAC

No Redesign of Existing PHY (.11a/b/g/n)



Structure of the 802.11 WG

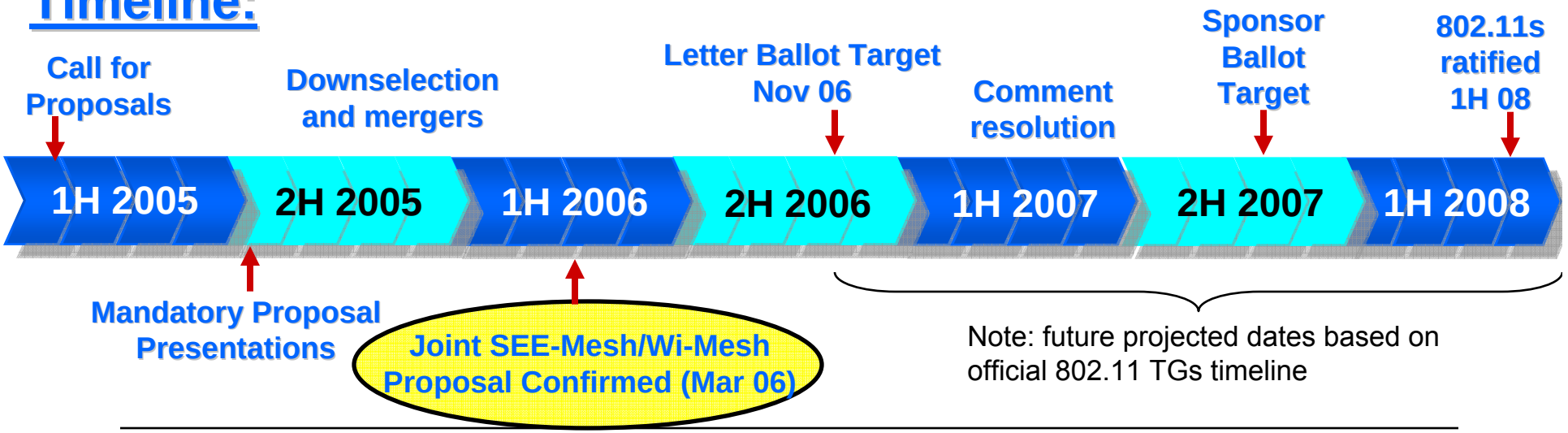
- **Active Task Groups in the Wireless Local Area Network Working Group, 802.11:**
  - 802.11k, TGk, Radio Resources Measurement
  - 802.11REV-ma, TGm, Maintenance
  - 802.11n, TGn, High Throughput
  - 802.11p, TGp, Wireless Access in the Vehicle Environment
  - 802.11r, TGr, Fast Roaming
  - **802.11s, TGs, Mesh Networking**
  - 802.11.2, TGT, Wireless Performance Prediction
  - 802.11u, TGu, Interworking with External Networks
  - 802.11v, TGv, Wireless Network Management
  - 802.11w, TGw, Protected Management Frames
  - 802.11y, TGy, 3850-3700 MHz Operation in the USA

802.11s Standardization Progress and Status

IEEE 802.11s Timeline

- January 04: Formation of 802.11 Mesh Study Group
- July 04: First 802.11 TGs Meeting
- January 05: Call for Proposals Issued
- July 05: Mandatory Proposal Presentations
- March 06: First 802.11s Draft Spec Adopted

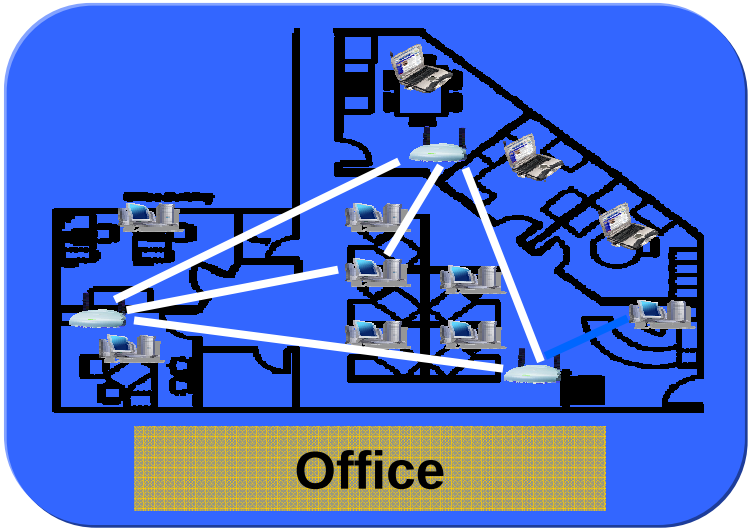
Timeline:

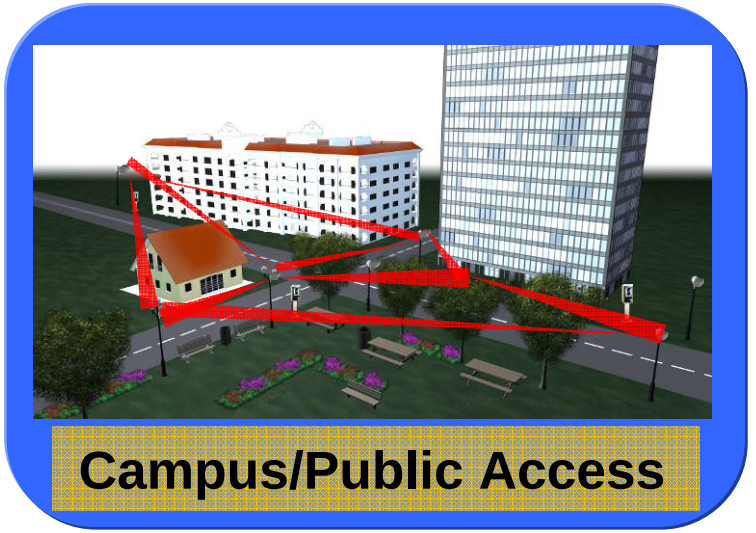


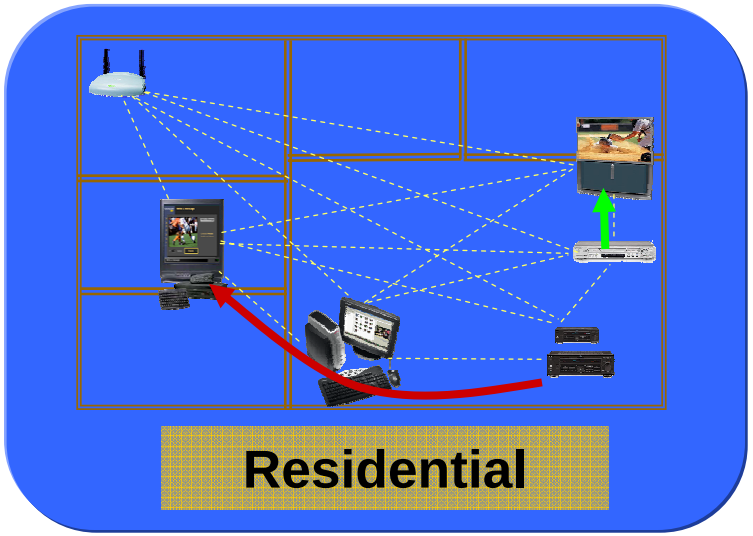
Proposal Evaluation Basis

- **Mandatory conformance documents**
  - 11-04/54r2 “PAR for IEEE 802.11 ESS Mesh”
  - 11-04/56r1 “Five Criteria for IEEE 802.11 ESS Mesh”
- **Evaluation documents**
  - 11-04/1174r13 “Functional Requirements and Scope”
  - 11-04/1175r10 “Comparison Categories and Informative Checklists”
  - **11-04/662r16 “Usage Models”**
  - 11-04/1477r4 “Terms and Definitions for 802.11s”
- **Informational documents**
  - 11-04/968r13 “Issues for Mesh Media Access Coordination Component in 11s”
  - 11-04/981r1 “TGs Reference Architecture Considerations”
  - 11-04/1462r0 “Routing and Rbridges”
  - 11-04/1543r4 “Informative Reference Bibliography for 802.11s”

Example 802.11s Mesh Networking Deployment Scenarios





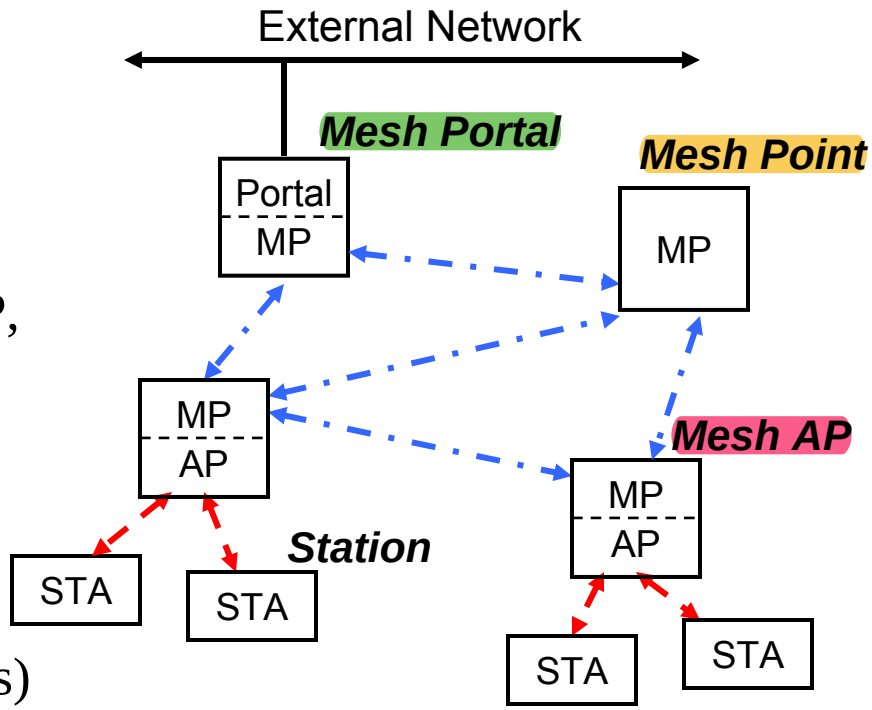


802.11s Expected to be Used Across Many Diverse Usage Models

802.11s Topology, Discovery, and Extensible Framework

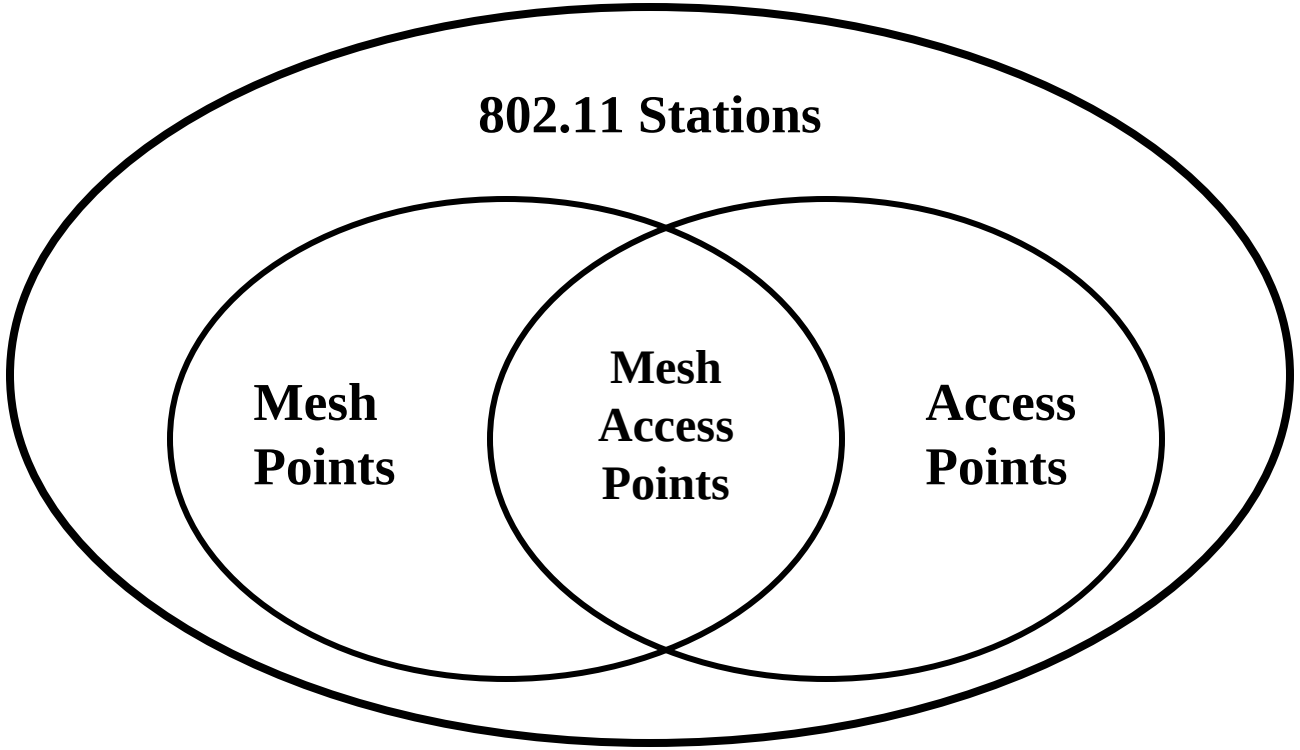
Device Classes in a WLAN Mesh Network

- **Mesh Point (MP):** establishes peer links with MP neighbors, full participant in WLAN Mesh services
  - Light Weight MP participates only in 1-hop communication with immediate neighbors (routing=NULL)
- **Mesh AP (MAP):** functionality of a MP, collocated with AP which provides BSS services to support communication with STAs
- **Mesh Portal (MPP):** point at which MSDUs exit and enter a WLAN Mesh (relies on higher layer bridging functions)
- **Station (STA):** outside of the WLAN Mesh, connected via Mesh AP



Mesh Points / Mesh APs

Set diagram of terms:

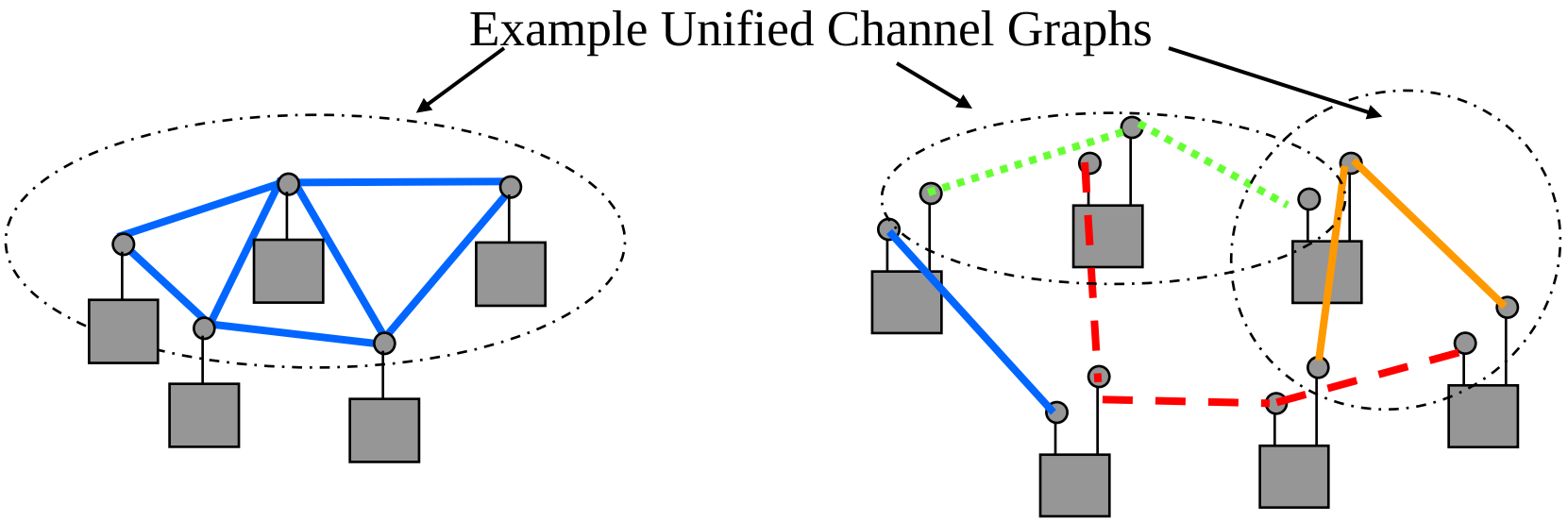


Topology Formation: Membership in a WLAN Mesh Network

- **Mesh Points (MPs) discover candidate neighbors based on new IEs in beacons and probe response frames**
  - **WLAN Mesh Capability Element**
    - Summary of active protocol/metric
    - Channel coalescence mode and Channel precedence indicators
  - **Mesh ID**
    - Name of the mesh
- **Mesh Services are supported by new IEs (in action frames), exchanged between MP neighbors**
- **Membership in a WLAN Mesh Network is determined by secure peer links with neighbors**

Topology Formation: Support for Single & Multi-Channel Meshes

- **Each Mesh Point may have one or more logical radio interface:**
  - Each logical interface on one (infrequently changing) RF channel, belongs to one “Unified Channel Graph”
  - Each Unified Channel Graph shares a channel precedence value
    - Channel precedence indicator – used to coalesce disjoint graphs and support channel switching for DFS



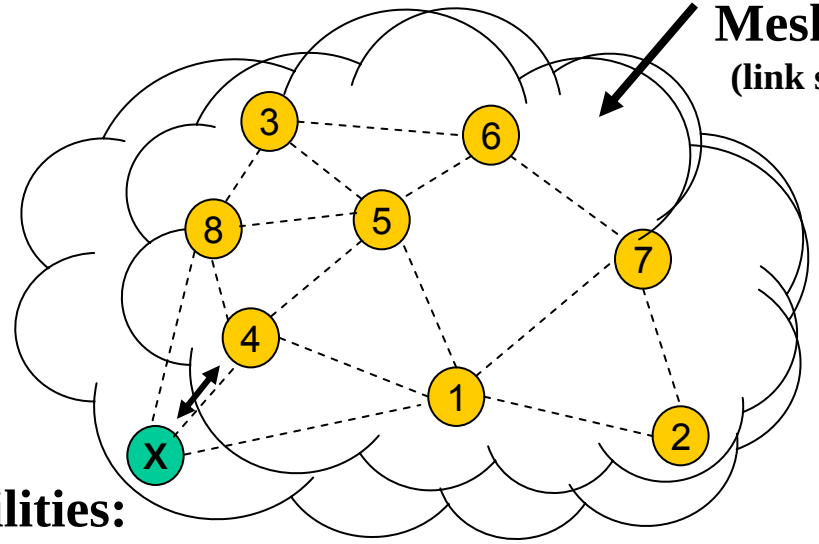
Extensible Framework Support for Mandatory and Alternative Path Selection Protocols

- **Draft defines one mandatory protocol and metric**
  - ***Any vendor may implement any protocol and/or metric*** within the framework
  - A particular mesh will have only one active protocol
  - Only one protocol/metric will be active on a particular link at a time
- **Mesh Points use the WLAN Mesh Capability IE to indicate which protocol is in use**
- **A mesh that is using other than mandatory protocol is not required to change its protocol when a new MP joins**
  - Algorithm to coordinate such a reconfiguration is out of scope

Example: Enabling Extensible Protocol and Metric Implementation

1. **Mesh Point *X* discovers Mesh (WLANMesh_Home) with Profile (link state, airtime metric)**
2. **Mesh Point *X* establishes peer link / authenticates with neighbors in the mesh, since it is capable of supporting the Profile**
3. **Mesh Point *X* begins participating in link state path selection and data forwarding protocol**

Mesh Identifier:
WLANMesh_Home
Mesh Profile:
(link state, airtime metric)



Capabilities:
Path Selection: distance vector, link state
Metrics: airtime, latency

One active protocol/metric in one mesh, but allow for alternative protocols/ metrics in different meshes

Part 2: Security and Routing

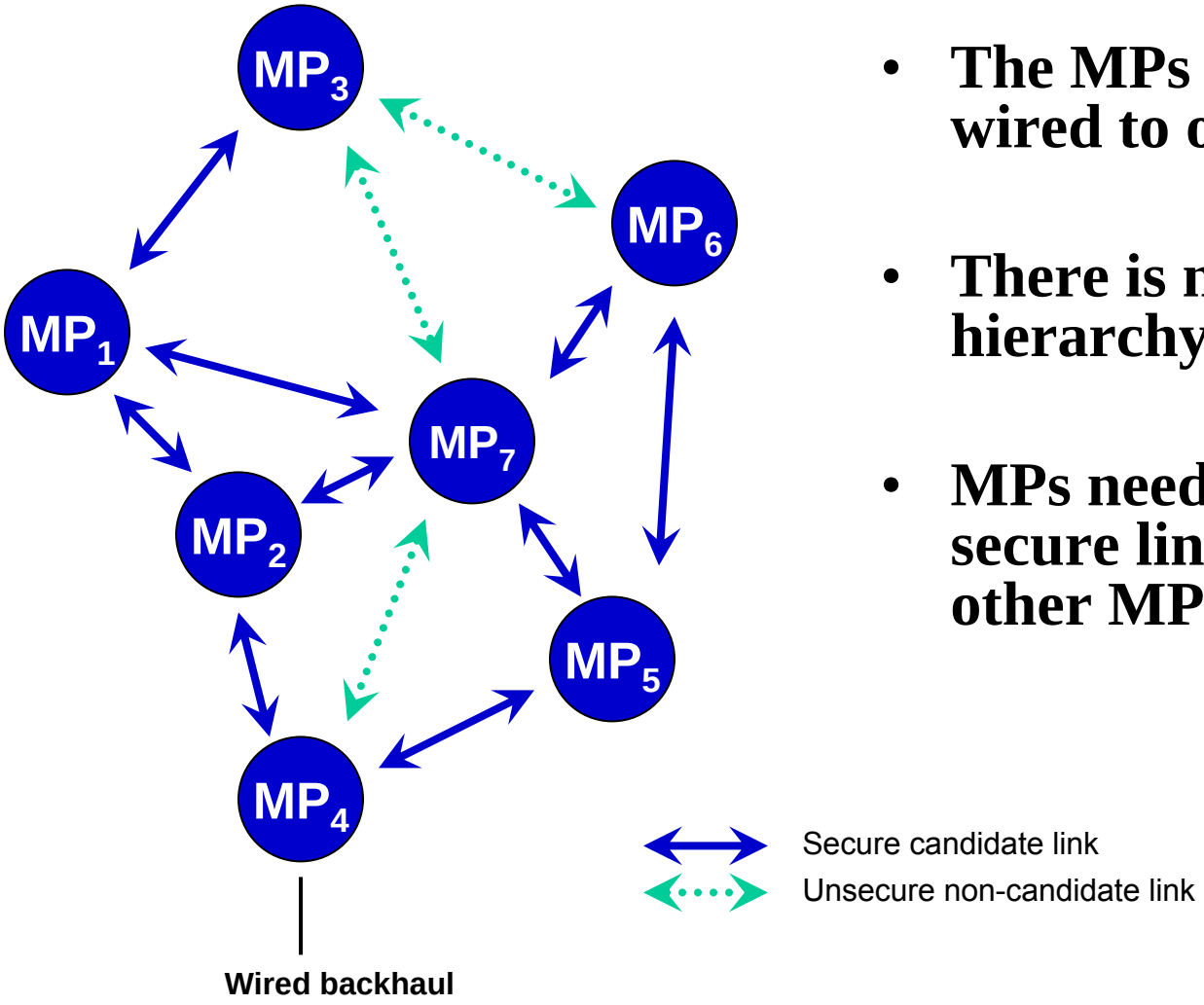
Jan Kruys, Cisco Systems

- **802.11s Security**
- **802.11s Path Selection and Forwarding**

802.11s Security

- **Objectives**
- **Scope**
- **Role Negotiation**
- **Authentication**
- **Key Management**

11s Security Situation

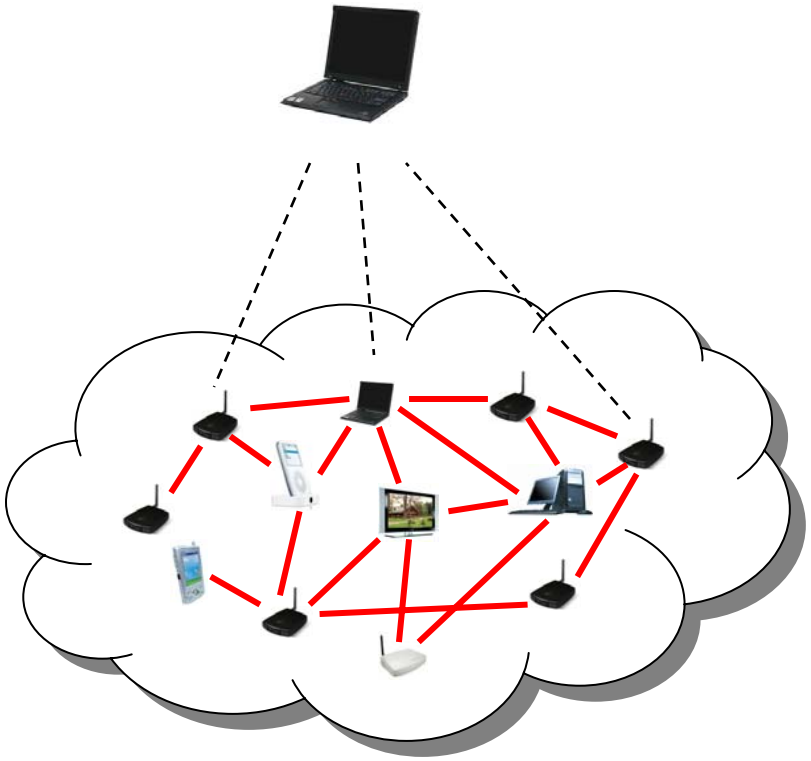


- The MPs are no longer wired to one another
- There is no intrinsic node hierarchy
- MPs need to maintain secure links with many other MPs

Mesh Security Considerations

- **Functions in the scope**
  - Transport
    (Access point covered by 11i)
- **Functions out of the scope**
  - Internal routing
  - External routing
  - Forwarding
- **Rationale**
  - Current technology is not mature enough to address all vulnerabilities from routing and forwarding
  - There are still research questions

Transport Security



- **Prevent unauthorized devices from directly sending and receiving traffic via the mesh**
  - Protect unicast traffic between neighbor MPs
  - Protect broadcast traffic between neighbor MPs
- **We need**
  - Mutually authenticate neighbor MPs
  - Generate and manage session keys and broadcast keys
  - Data confidentiality over a link
  - Detect message forgeries and replays received on a link

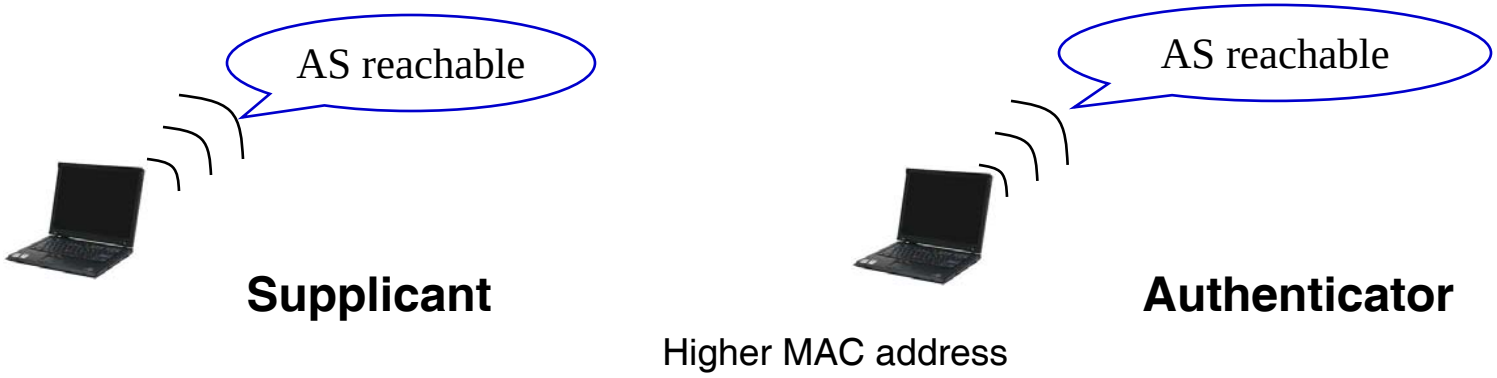
Authentication and Initial Key Management

- **Basic approach is to re-use 802.11i/802.1X**
  - Re-use of 802.11i facilitates implementation
  - Allows other AKM schemes
- **802.1X is widely used and is suitable for many mesh scenarios**
  - but can be replaced with small scale alternatives if required
- **Provides a basis for secure key distribution (PMK)**
- **In a mesh, PMK is treated as token of authorization for a MP to join the mesh**
  - Authorized to send and receive messages to/from mesh neighbors

Discovery and Role Negotiation

- **Discovery**
  - Discover the available mesh for joining
  - What Authenticated Key Management (AKM) Protocol, Unicast and Multicast Ciphersuites are available?
- **Negotiation—Enable parties to agree on the security roles and security policy to use with a peer link**
  - Who's the authenticator, who's the supplicant?
  - Agree on which of those options enabled to use

Role Negotiation



Key Management Goals

Given a "good" PMK

- **Guarantee fresh session key**
- **Demonstrate liveness of peer PMK holder**
- **Bind session key to the communicating MPs**
- **Synchronize session key use**
- **Distribute the Group Keys**
  - Both party needs to distribute its group key for broadcast/multicast protection

TGs Security: initial contact

Supplicant

Authenticator

Authentication Server

Link state and security capabilities discovery

Peer link establishment, Security and Role negotiation

Authentication

4 way handshake (PTK/GTK distribution)

Data protection

PMK distribution

TGs Security subsequent contact (new feature under discussion)

PMK-MA-n

PMK-MA-m
PMK-MA-n
etc

Authentication Server

Supplicant n

Authenticator

Robust Peer link establishment, Security Role negotiation

4 way handshake (PTK/GTK distribution)

Data protection

PMKs generated in previous authentications (based on TGr key hierarchy)

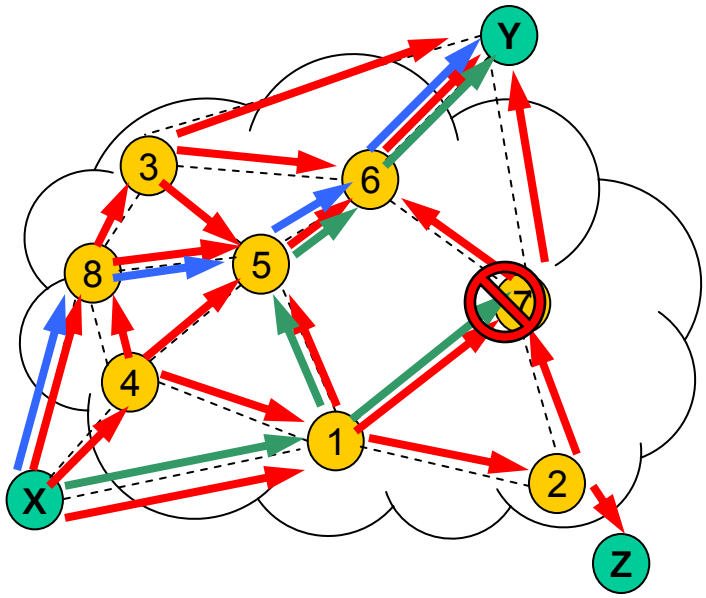
TGs Security Summary

- **TGs makes extensive re-use of 11i features**
  - Including the 802.1X “initial Authentication”
- **Fitted into a peer to peer environment**
  - With the aid of role negotiation prior to starting the security protocol exchange
- **New extension for “fast re-connect” under discussion**
  - based on the key hierarchy developed by TGr
  - modified for robust peer-to-peer link establishment

802.11s Routing

- **HWMP: Default Routing Protocol**
- **RA-OLSR: Optional Routing Protocol**

Routing = Path Calculation for Forwarding



- **Routing optimizes Unicast Forwarding of frames**
  - Between Mesh Points
  - To Associated stations
- **Nodes Participating in routing calculate best paths**
  - Paths may change as link state changes
- **Routing may include support for broadcast/multicast**

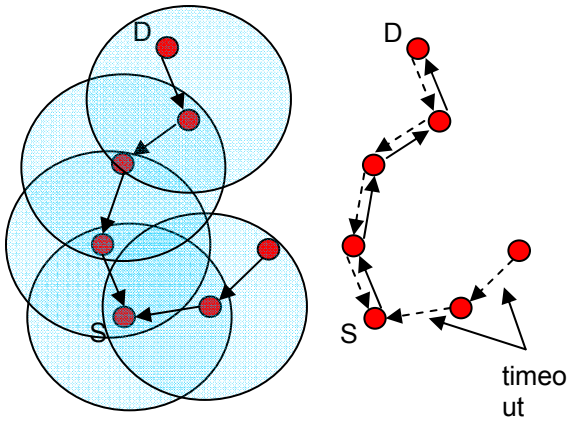
Default Routing protocol for Interoperability
Hybrid Wireless Mesh Protocol (HWMP)

- **Combines the flexibility of on-demand route discovery with efficient proactive routing to a mesh portal**
  - On demand routing offers great flexibility in changing environments
  - Pro-active tree based routing is very efficient in fixed mesh deployments
  - The combination makes it suitable for implementation on a variety of different devices under consideration in TGs usage models
    - from CE devices to APs and servers
- **Simple mandatory metric based on airtime as default, with support for other metrics**
  - Extensibility framework allows any path selection metric (QoS, load balancing, power-aware, etc)

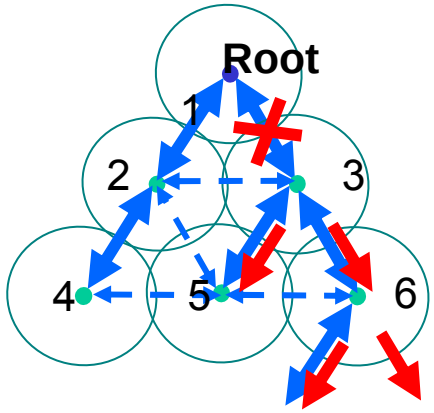
Hybrid Wireless Mesh Protocol (HWMP)

- **On demand routing is based on Radio Metric AODV (RM-AODV)**
  - Based on basic mandatory features of AODV (RFC 3561)
  - Extensions to identify best-metric path with arbitrary path metrics
  - Destinations may be discovered in the mesh on-demand

Ad hoc On-Demand Distance Vector Routing (AODV)



- **Pro-active routing is based on tree based routing**
  - If a Root portal is present, a distance vector routing tree is built and maintained
  - Tree based routing is efficient for hierarchical networks
  - Tree based routing avoids unnecessary discovery flooding during discovery and recovery

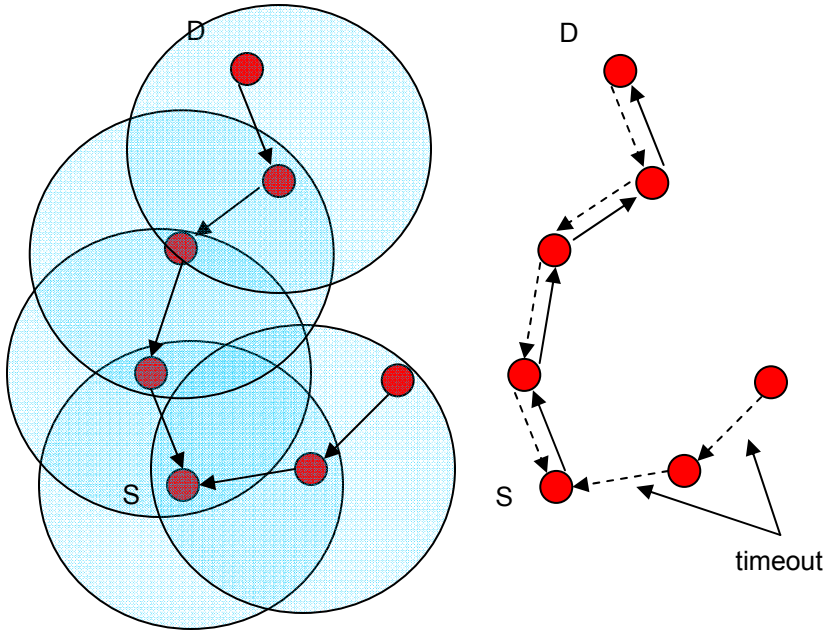


HWMP Protocol Elements

- **Root Announcement (broadcast)**
- **Tells MPs about presence and distance of Root MP**
- **Route Request (broadcast/unicast)**
- **Asks destination MP(s) to form a *reverse* route to the originator**
- **Route Reply (unicast)**
- **Forms a *forward* route to the originator and confirms the reverse route**
- **Route Error (broadcast)**
- **Tells receiving MPs that the originator no longer supports certain routes**

On-demand Routing in HWMP– Key Features

- **On Demand Routing**
  - Allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication.
- **Route Discovery**
  - Uses Expanding Ring Search to limit the flood of routing packets
  - Reverse Paths are setup by Route Request packets broadcast (or unicast) from Originator
  - Forward Paths are setup by Route Reply packet sent from destination node or any intermediate node with a valid route to the destination



Reverse Path Formation

Forward Path Formation

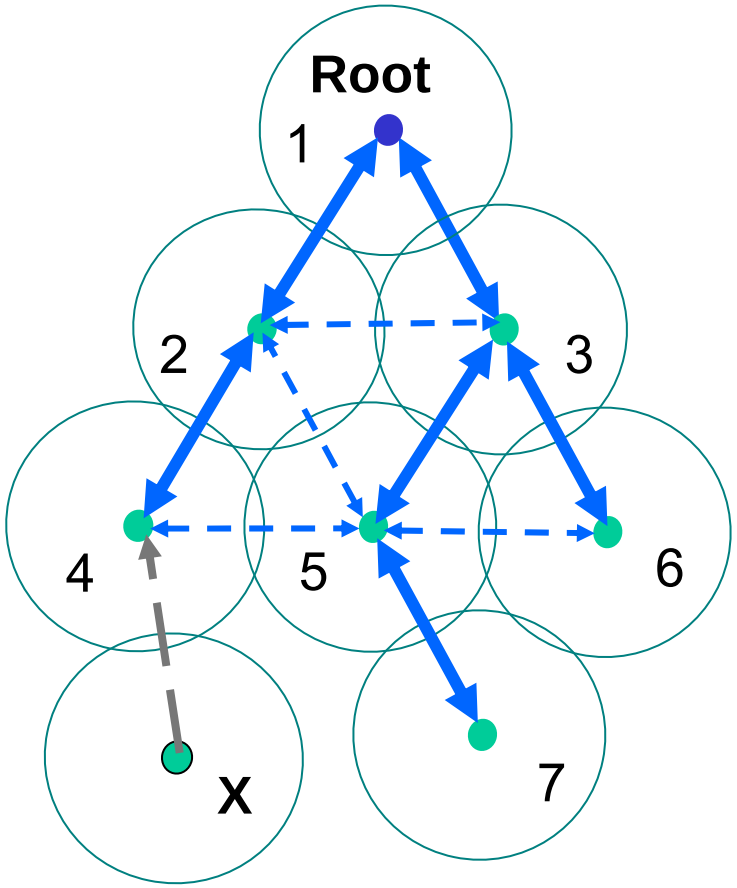
Figure From:
C. E. Perkins and E. M. Royer., Ad-hoc On-Demand Distance Vector Routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90-100.

On-demand routing in HWMP – Key Features

- **Route Maintenance**
  - Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a Route Error message is used to notify other nodes that the loss of that link has occurred.
  - Route Error message is a unicast message, resulting in quick notification of route failure.
- **Loop Freedom**
  - All nodes in the network own and maintain a destination sequence number which guarantees the loop-freedom of all routes towards that node.

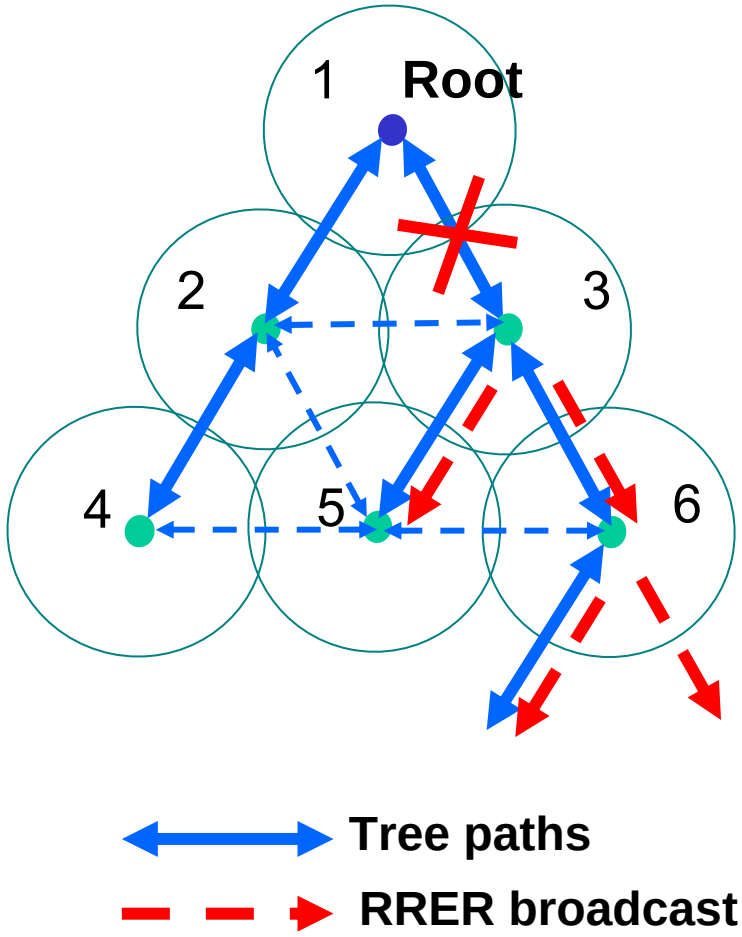
Tree-based routing in HWMP – Key Features

- **Topology Creation**
  - Root MP may issue a "broadcast" RREQ
    - MPs may respond with RREP
  - The Root MP may issue "Root Announcements"
    - MPs may respond by a unicast RREQ to the Root (answered by RREP)
  - MPs select next hop to Root based on best path metric
    - Best path propagates down from the Root (e.g. X-4-2-1)
  - "Registration" of subtrees by MPs facilitates outward message routing



Tree-based routing in HWMP – Key Features

- **Topology Maintenance**
  - MPs monitor their upstream links and may switch to back up links using RREP (3-1 >> 3-2)
    - This avoids "re-building" the tree
  - Loss of upstream link ✕ causes RRER to sent down
    - Allows nodes to decide/select own back-up paths
    - Signals route holders that some route is broken

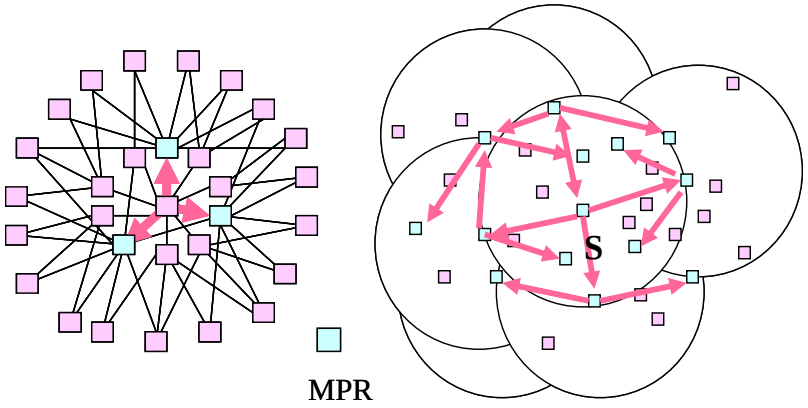


Example Optional Path Selection Protocol *Radio Aware OLSR (RA-OLSR)*

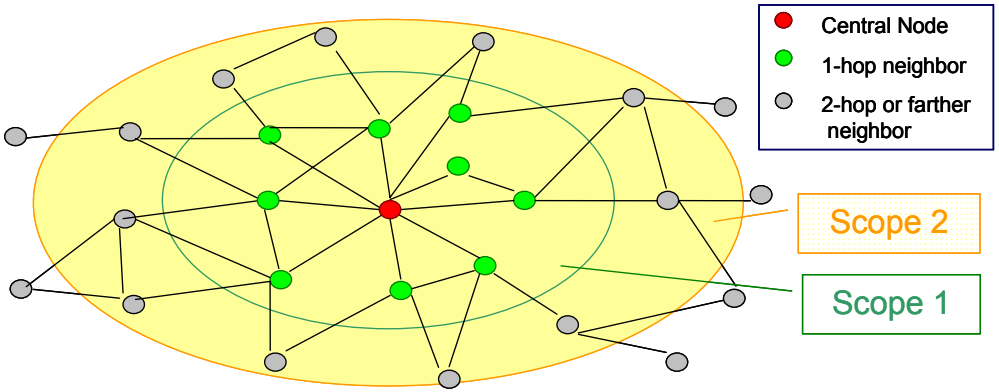
- **Proactively maintains link-state for routing**
  - Changes in link state are communicated to “neighborhood” nodes
- **Extensible routing scheme based on the two link-state routing protocols:**
  - OLSR (RFC 3626)
  - (Optional) Fisheye State Routing (FSR)
- **Extended with:**
  - Use of a radio aware metric in MPR selection and routing path selection
  - Efficient association discovery and dissemination protocol to support 802.11 stations

RA-OLSR – Key Features

- **Multi Point Relays (MPRs)**
  - A set of 1-hop neighbor nodes covering 2-hop neighborhood
  - Only MPRs emit topology information and retransmit packets
    - Reduces retransmission overhead in flooding process ***in space***.



- **(Optional) message exchange frequency control (fish-eye state routing)**
  - Lower frequency for nodes within larger scope
    - Reduce message exchange overhead ***in time***.



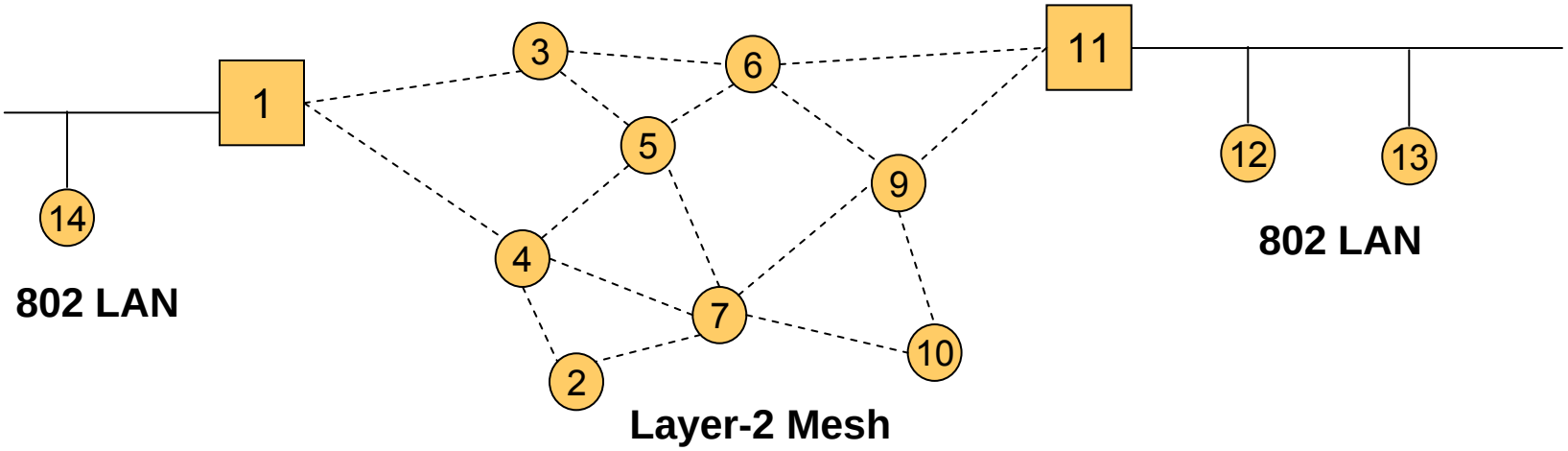
Part 3: Interworking and Frame Formats

Joseph Kim, STMicroelectronics

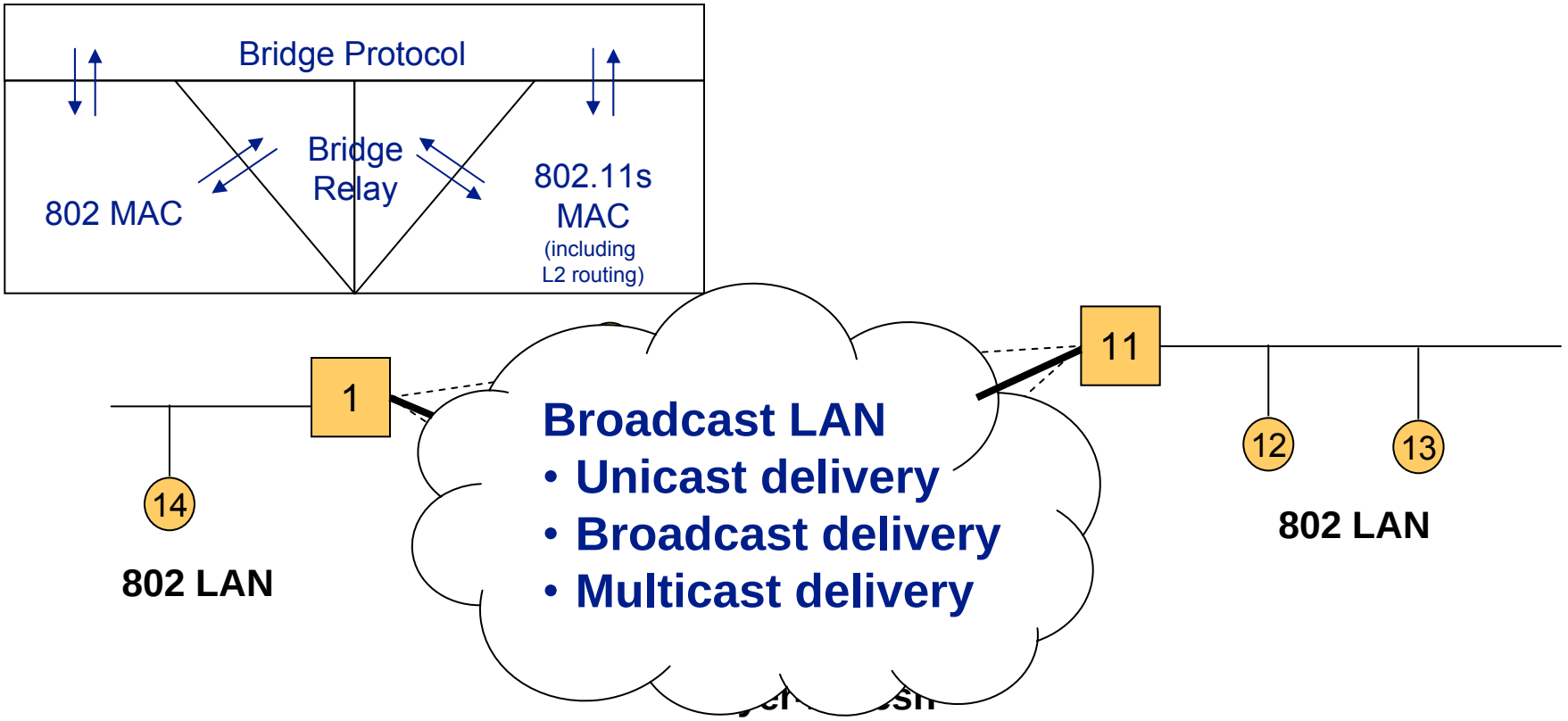
- **802.11s Interworking**
- **802.11s Data Frame Format and 6 Address Scheme**

802.11s Interworking Approach

Achieving 802 LAN Segment Behavior



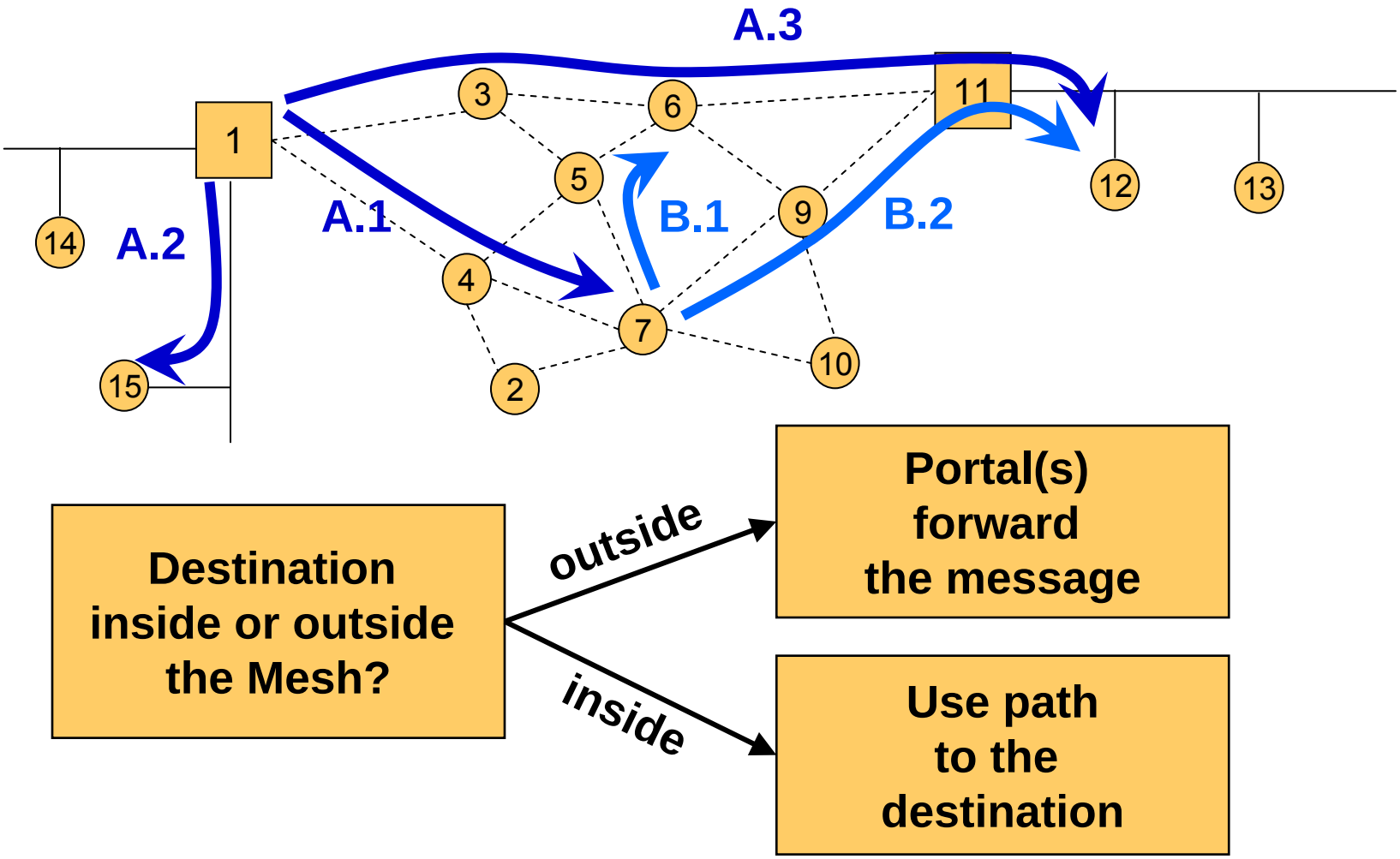
Achieving 802 LAN Segment Behavior



Support for connecting an 802.11s mesh to an 802.1D bridged LAN

- Broadcast LAN (transparent forwarding)
- Overhearing of packets (bridge learning)
- Support for bridge-to-bridge communications (e.g. allowing Mesh Portal devices to participate in STP)

Interworking: Packet Forwarding

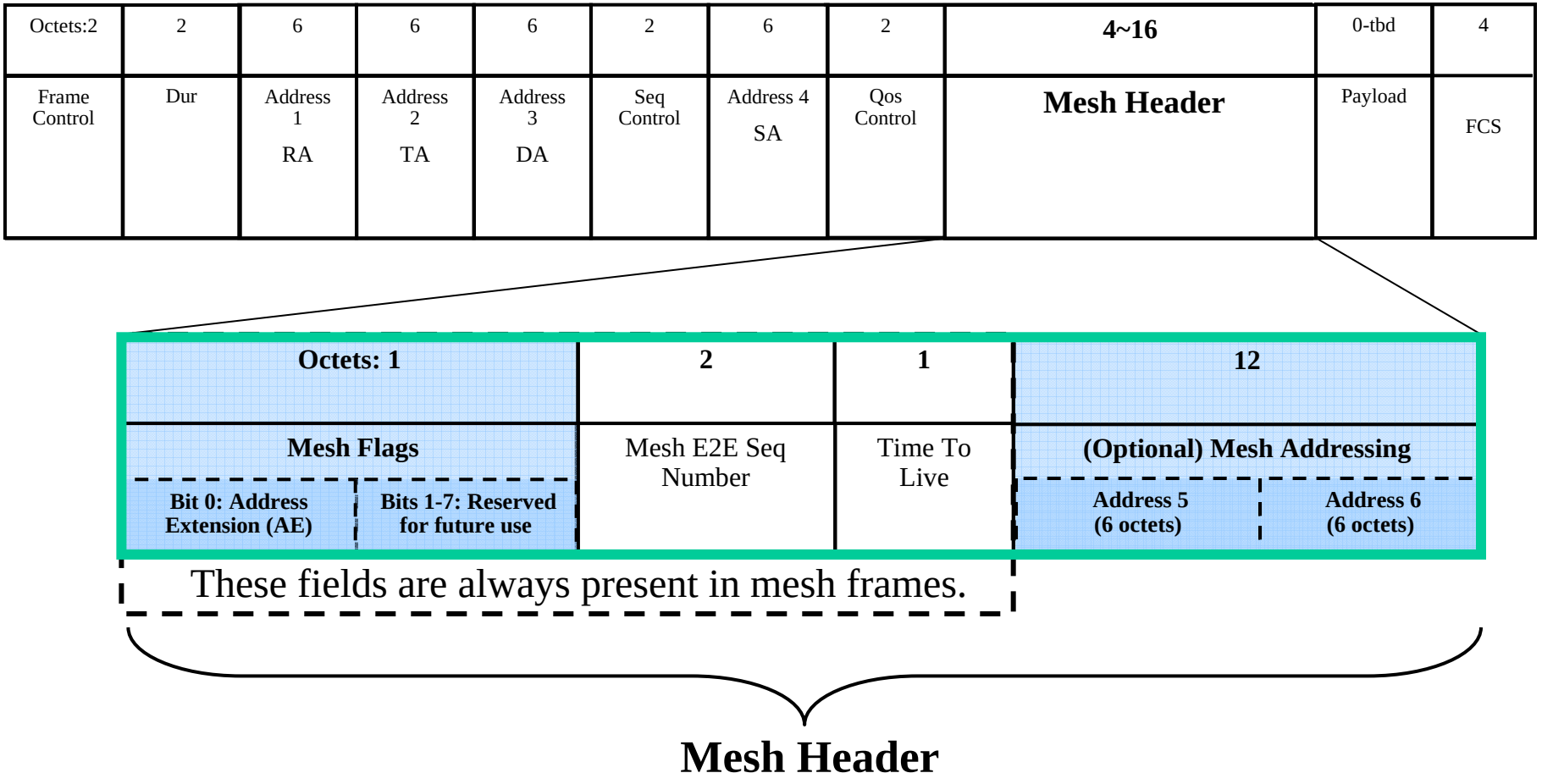


Interworking: MP view

1. **Determine if the destination is inside or outside of the Mesh**
   a. Leverage layer-2 mesh path discovery
2. **For a destination inside the Mesh,**
   a. Use layer-2 mesh path discovery/forwarding
3. **For a destination outside the Mesh,**
   a. Identify the “right” portal, and deliver packets via unicast
   b. If not known, deliver to all mesh portals

802.11s Data Frame Format and 6-Address Scheme

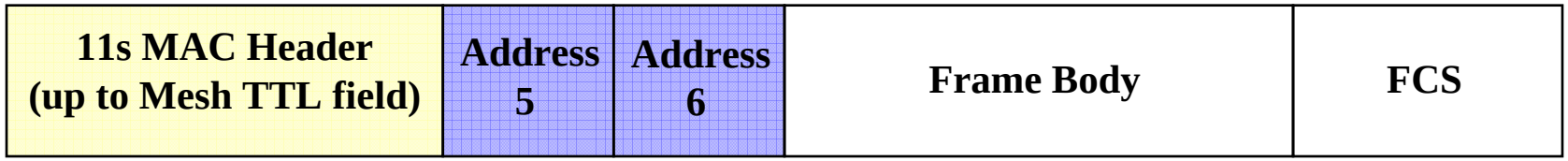
Mesh Data Frame Format



6-Address Scheme

To DS	From DS	AE Flag	Address 1	Address 2	Address 3	Address 4	Address 5	Address 6
0	0	0	RA=DA	TA=SA	BSSID	N/A	N/P*	N/P
0	1	0	RA=DA	TA=BSSID	SA	N/A	N/P	N/P
1	0	0	RA=BSSID	TA=SA	DA	N/A	N/P	N/P
1	1	0	RA	TA	DA	SA	N/P	N/P
1	1	1	RA	TA	Mesh DA	Mesh SA	DA	SA

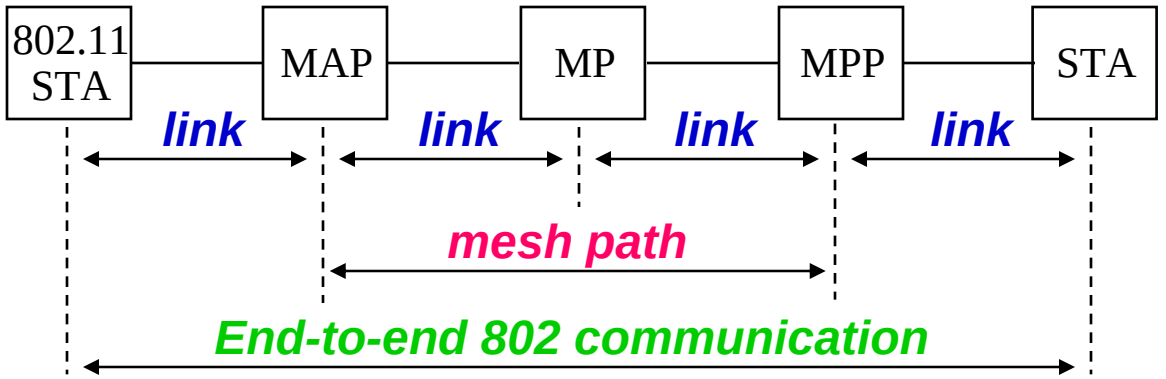
** N/P = Not Present*



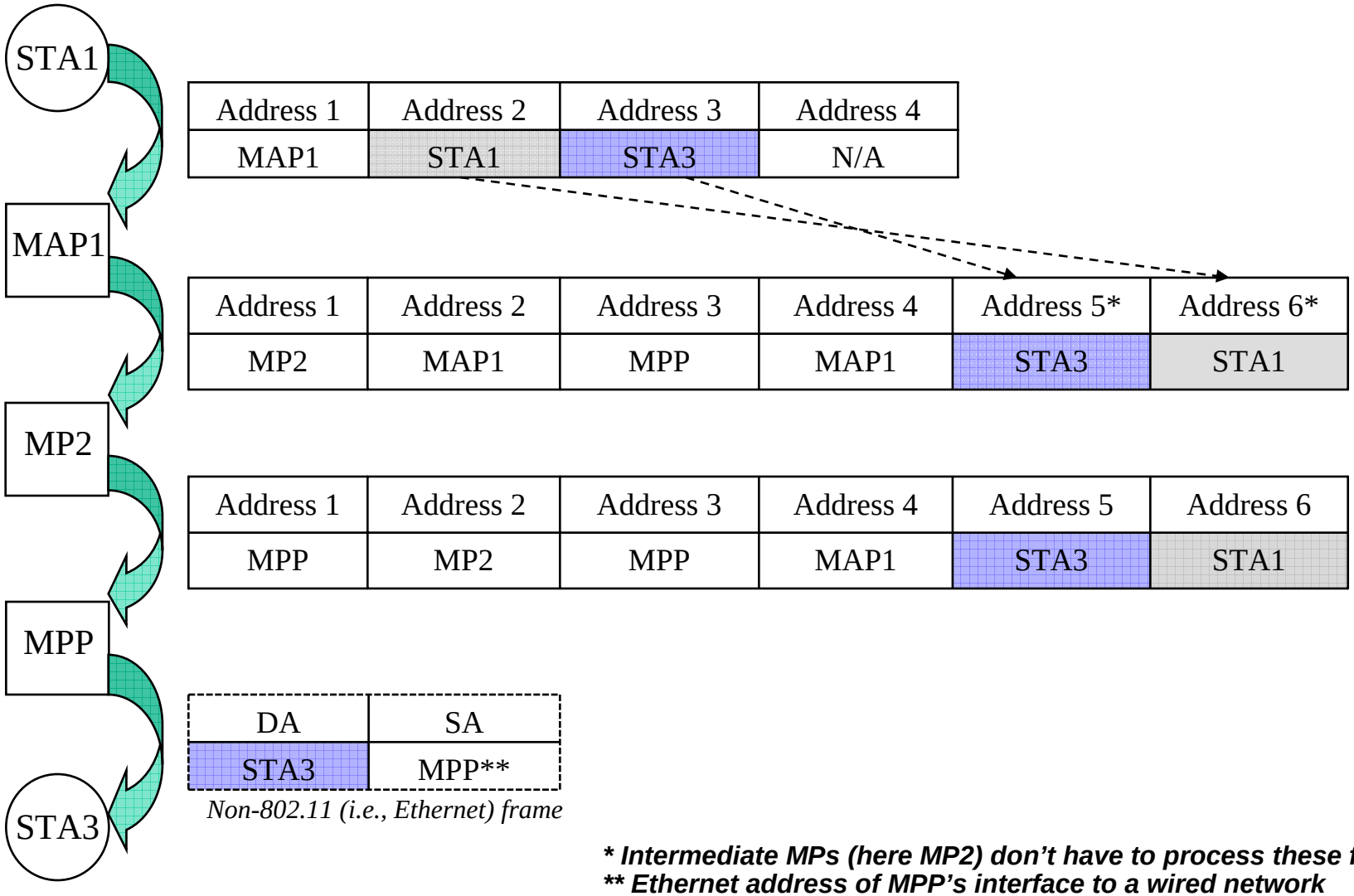
When the AE flag = 0, all fields have their existing meaning, and there exist no “Address 5” and “Address 6” fields – this assures compatibility with existing hardware and/or firmware.

6-Address Scheme – Address Mapping Principle

- **The ordering of the addresses should be from the innermost to the outermost "connections"**
  - ***Address 1 & 2*** for endpoints of a ***link*** between RX and TX
  - ***Address 3 & 4*** for endpoints of a ***mesh path*** between a destination and a source MP
    - Including MPPs and MAPs
  - ***Address 5 & 6*** for endpoints of an (end-to-end) ***802 communication***
    - A series of mesh paths connected at MPPs (*e.g.*, TBR in HWMP) or
    - An 802 path between legacy STAs (including nodes outside the mesh) or
    - Any mixture of them (*e.g.*, an MP to an STA or vice versa).

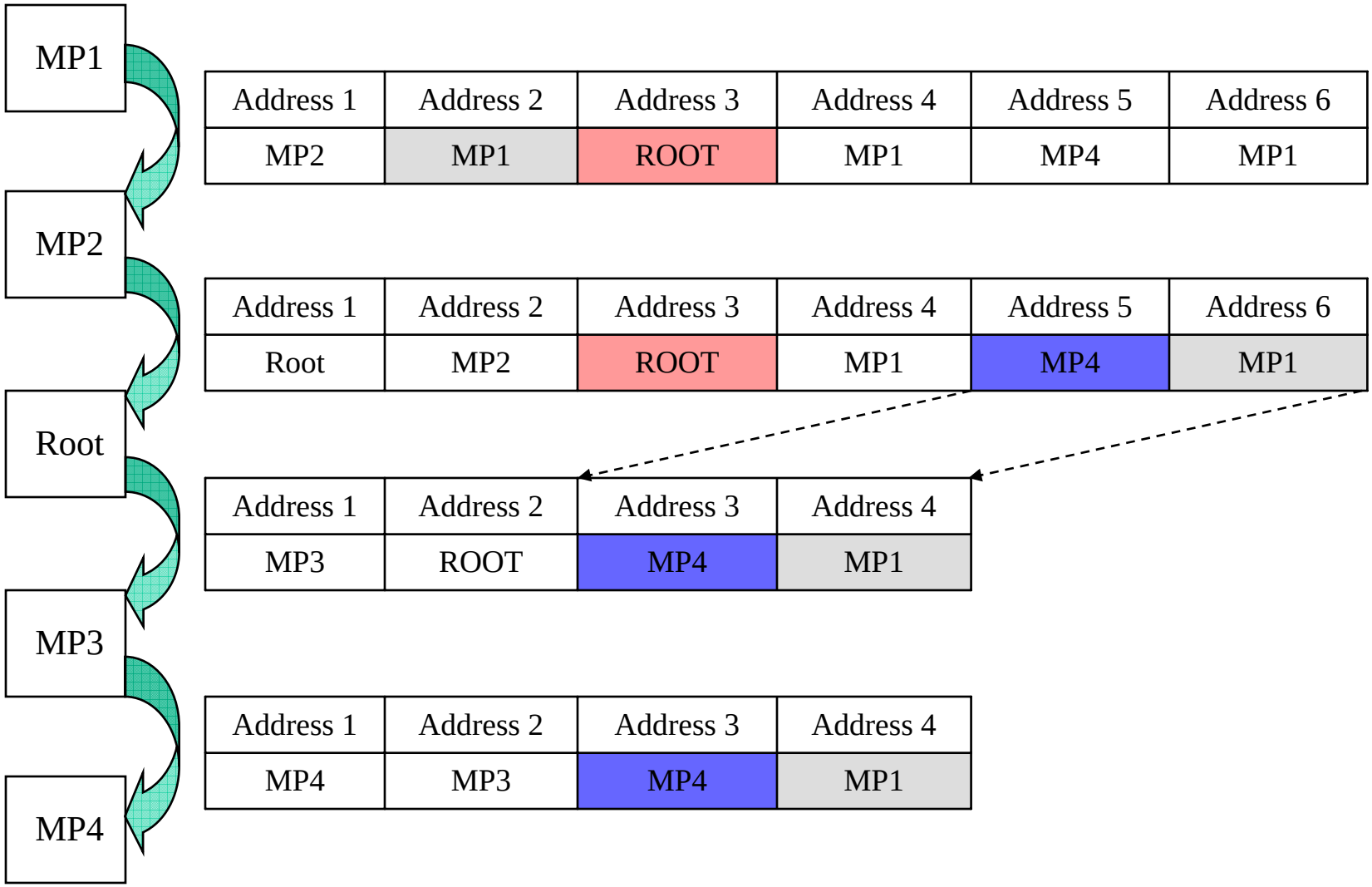


Example #1: 802.11 STA to External STA



**** Intermediate MPs (here MP2) don't have to process these fields.***
***** Ethernet address of MPP's interface to a wired network***

Example #2: MP to MP Via Root Portal



Part 4: MAC Extensions

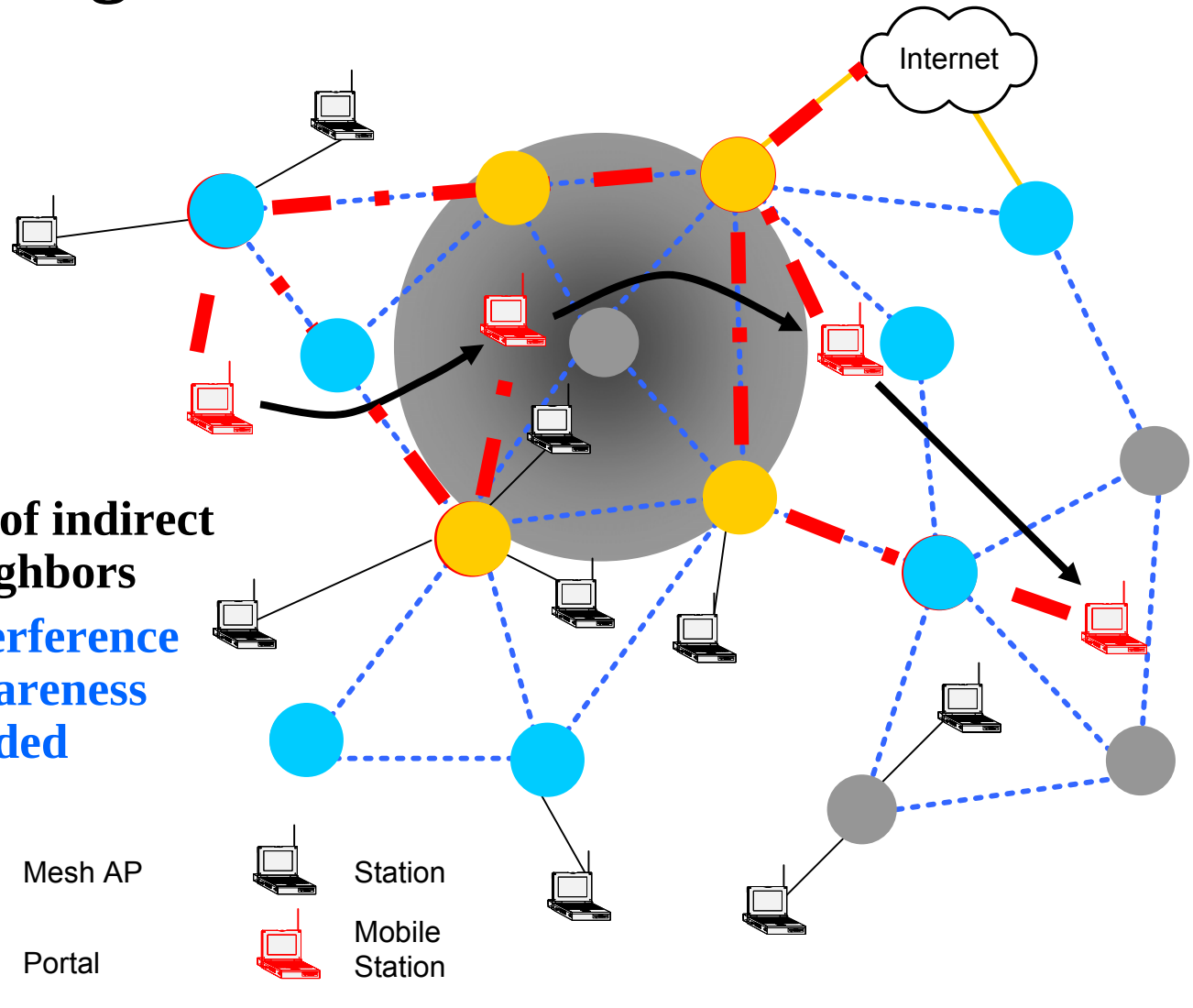
Juan Carlos Zuniga, InterDigital Comm Corp.

- **802.11s MAC Enhancements**
- **802.11s Beaconing, Synchronization, and Powersave**

Some Challenges in Mesh networks

- **Mobility awareness**
  - Client stations
  - Network nodes
- **Dynamical Radio Environment**

- **Set of direct Neighbors** = **Set of indirect Neighbors**
- **Exposed & hidden nodes** → **Interference Awareness needed**

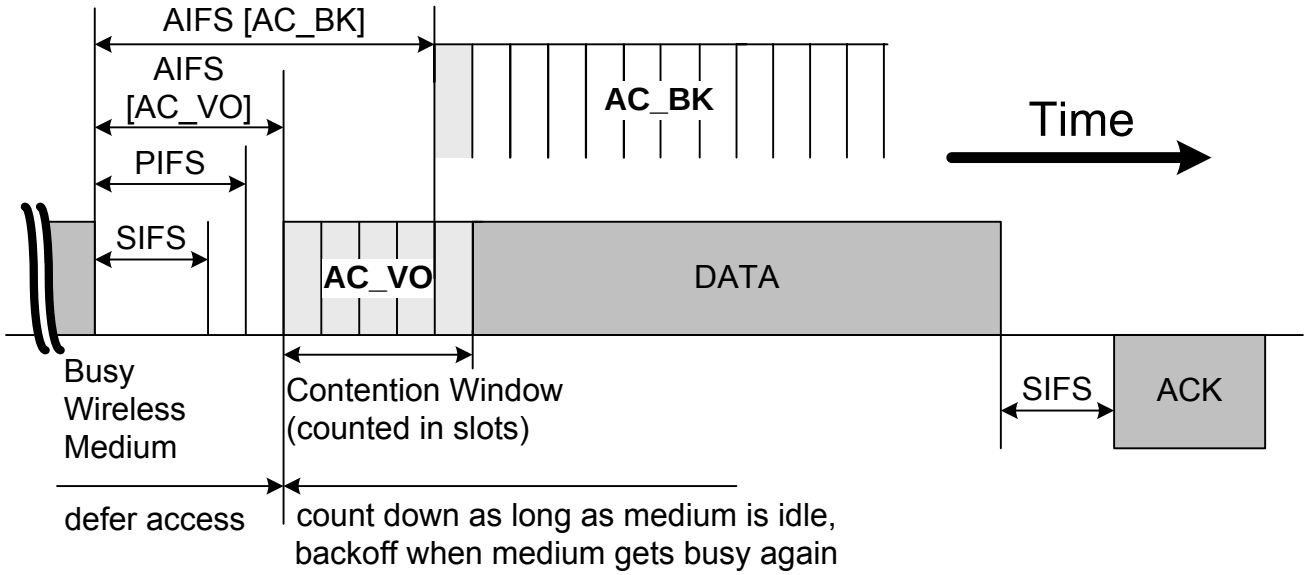


802.11s MAC

- **Mandatory MAC Functions**
  - Enhanced Distributed Channel Access (EDCA)
    - Re-use of latest MAC enhancements from 802.11 (i.e. 802.11e)
    - Compatibility with legacy devices
    - Easy to implement, providing reasonable efficiency in simple Mesh WLAN deployments
- **Optional MAC Enhancements**
  - Mesh Deterministic Access (MDA)
    - Reservation-based deterministic mechanism
  - Common Channel Framework (CCF)
    - Multi-channel operation mechanism
  - Intra-mesh Congestion Control
  - Power Management

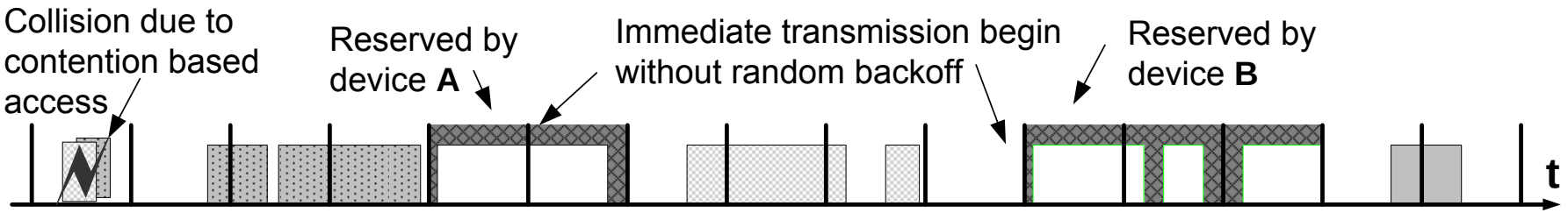
Enhanced Distributed Channel Access (EDCA)

- **MAC QoS enhancement introduced by 802.11e providing prioritized back-off**
- **Used as baseline by 802.11s**



Mesh Deterministic Access (MDA)

- **MAC enhancement based on a reservation protocol**
- **QoS support in large scale distributed Mesh networks**
- **Synchronized operation**
- **Reduced contention (two-hop clearing)**
- **Distributed scheduling**



MDAOP Protocol

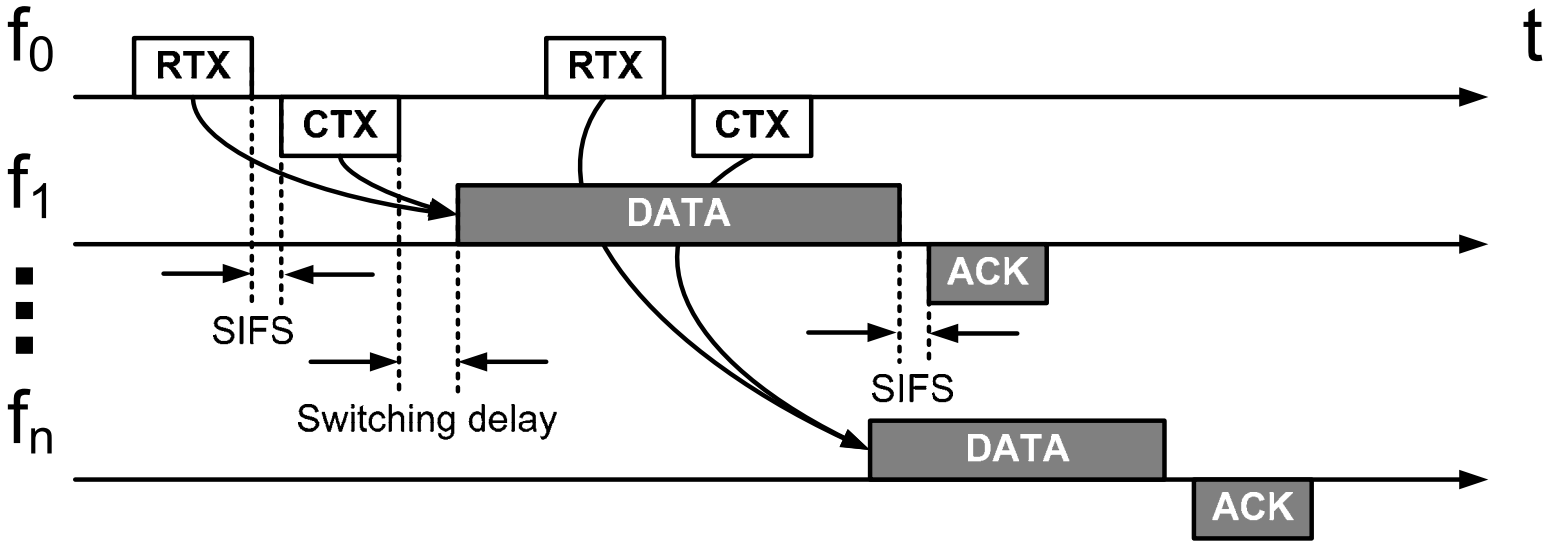
- **Setup Request**
  - Unicast from a transmitter to a receiver using MDAOP Setup Request Information Element (IE)
- **Setup Reply**
  - Unicast from a receiver of Setup Request IE to the sender using the MDAOP Setup Reply IE (Accept or Reject, possibly with reasons and alternate suggestions)
- **MDAOP advertisements**
  - MDAOP and other known busy times (e.g. HCCA, Beacons, etc.) can be broadcast using MDAOP Advertisements IEs
- **MDAOP teardown**
  - Either transmitter or receiver may indicate a teardown at any time by transmitting an MDAOP Set Teardown IE

MDAOP Operation

- **Nodes that own an MDAOP**
  - Access the channel using MDA parameters for CWMin, CWMax, and AIFSN
  - Send traffic for one TXOP
  - Use the same retransmit rules as common EDCA
  - Relinquish any remaining MDAOP time by sending CF-End or QoS-Poll to self with zero duration
- **Nodes that defer during a known MDAOP**
  - Set NAV to the end of the MDAOP
  - Shorten the NAV if CF-End or QoS-Poll with zero duration received

Common Channel Framework (CCF)

- Used for negotiating other channels for data exchange
- Provides means for using orthogonal frequency channels
- Entities periodically switch to common channel

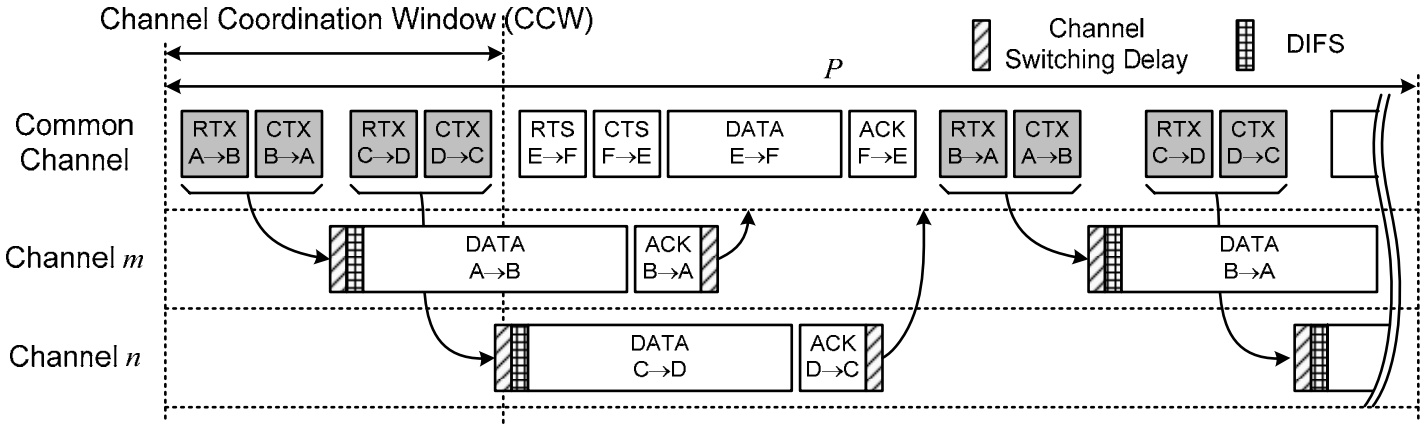


CCF Protocol

- **Simple RTX/CTX protocol**
  - Using RTX, the transmitter suggests a destination channel
  - The receiver accepts/declines the suggested channel using CTX
  - After a successful RTX/CTX exchange, the transmitter and receiver switch to the destination channel
  - Switching is limited to channels with little activity
- **Existing medium access schemes are reused (i.e. EDCA)**
  - To devices that do not implement CCF, the common channel appears as a conventional single channel
  - Common channel can also be used for normal data transmission

CCF Operation

- **Channel Coordination Window (CCW)**
  - Defined for CCF-enabled MPs to tune into the common channel
  - Channel Utilization Vector (**U**) of each MP gets reset
  - Allows MPs marking other channels unavailable based on RTX/CTX exchanges
- **CCW repetition period *P***
  - CCF-enabled MPs initiate transmissions that end before *P*
  - MPs may stay tuned to the common channel beyond CCW

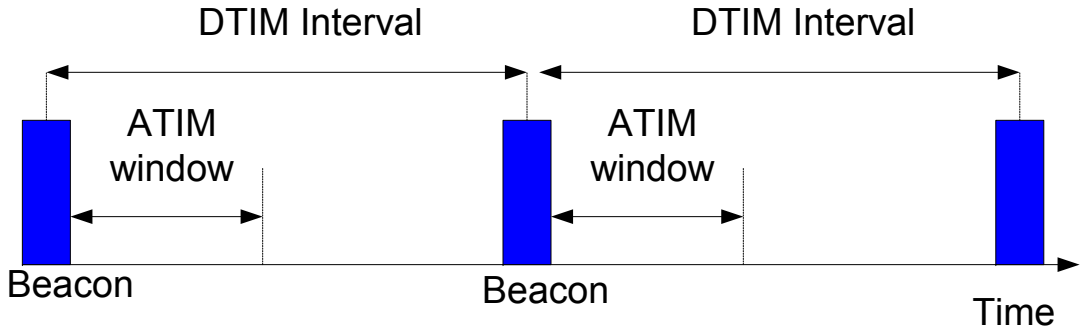


MP Power Management

- **Reuses existing mechanisms defined for BSS/IBSS with some modifications**
  - ATIM window and ATIM frames with some new rules
  - TIM IE in beacon frame and PS-poll frame
  - APSD mechanism
- **Uses reduced beaconing frequency**
  - Possibility of beaconing only at DTIM timing
  - Efficient sharing of Mesh beaconing responsibility
- **Provides efficient Power Save mode advertising**
  - Indicated in beacon frames
  - Indication by PS bit in Frame Control field
- **Defines mechanisms to allow MPs being awake only for the portion of time required for actual reception**
  - Efficient use of “more data bit” and “EOSP”

ATIM-based Sleep-wake Operation

- **Announcement Traffic Indication Message (ATIM)**
  - Guaranteed window of awake time after periodic Delivery Traffic Indication Message (DTIM) beacons
  - DTIM interval defined as a multiple of beacon intervals
  - Globally unique to the mesh
- **Control communication transferred during ATIM window**
  - Indicating pending traffic, change in PS state or re-instating stopped flows
  - Remain awake time after ATIM window dependant on control communication exchanged during ATIM window

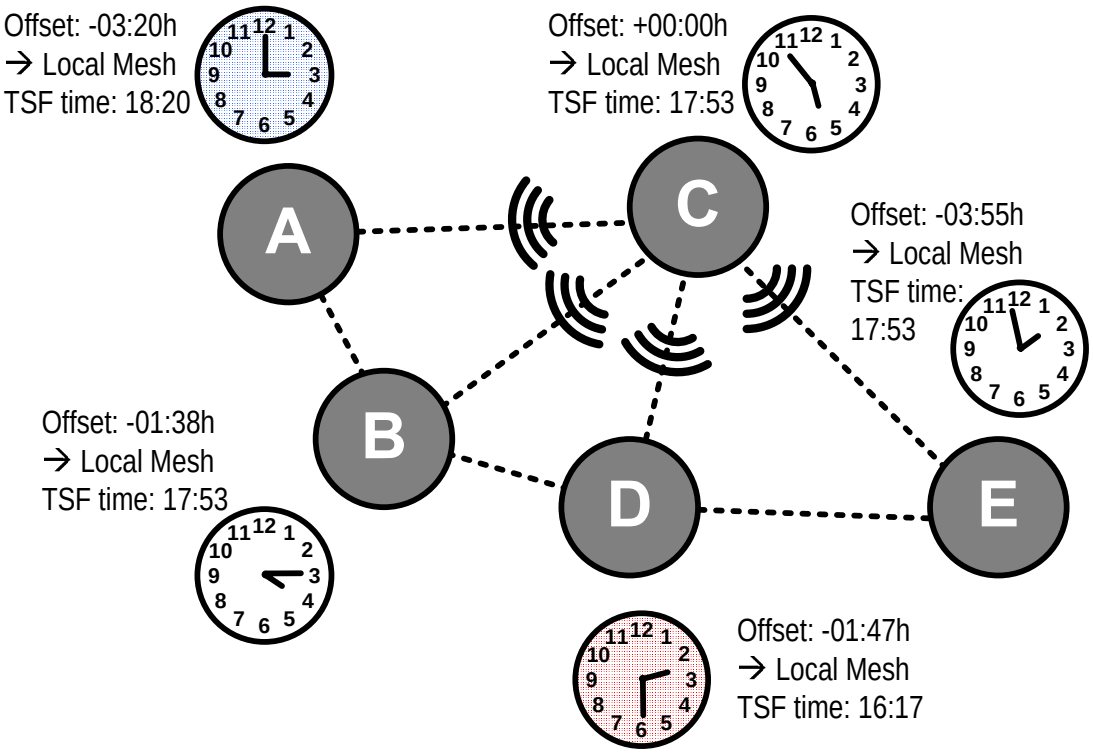


Synchronization

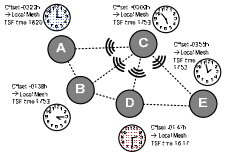
- **Many 802.11s MAC services rely on synchronization**
  - High performance MAC schemes
  - Power saving
- **MPs may have different Beacon Intervals**
  - No requirement to impose a strict beacon time interval
- **Mesh-wide common Timing Synchronization Function (TSF)**
  - MPs calculate local offset between own beacon time and mesh time
  - Local TSF updating rules similar to IBSS (i.e. 802.11 ad-hoc)
    - Adopt fastest TSF timer, or
    - Update local offset to Mesh TSF

Synchronization (1)

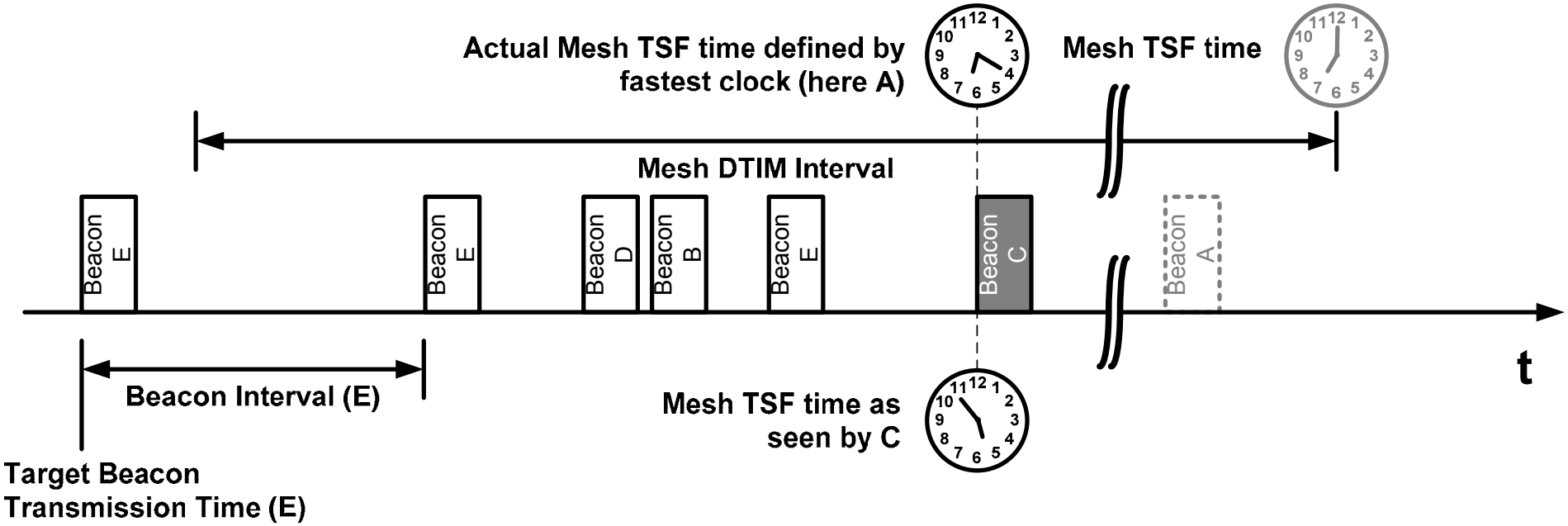
- **B & E are synchronous with C**
  - B, C & E may change their local TSF to become Mesh TSF time
    - → Local offset = 0
- **D has delayed Mesh TSF**
  - D must update
    - Local offset, or
    - Local TSF time
- **A has faster clock**
  - Does not adopt
  - Its next beacon will synchronize B & C



Synchronization (2)

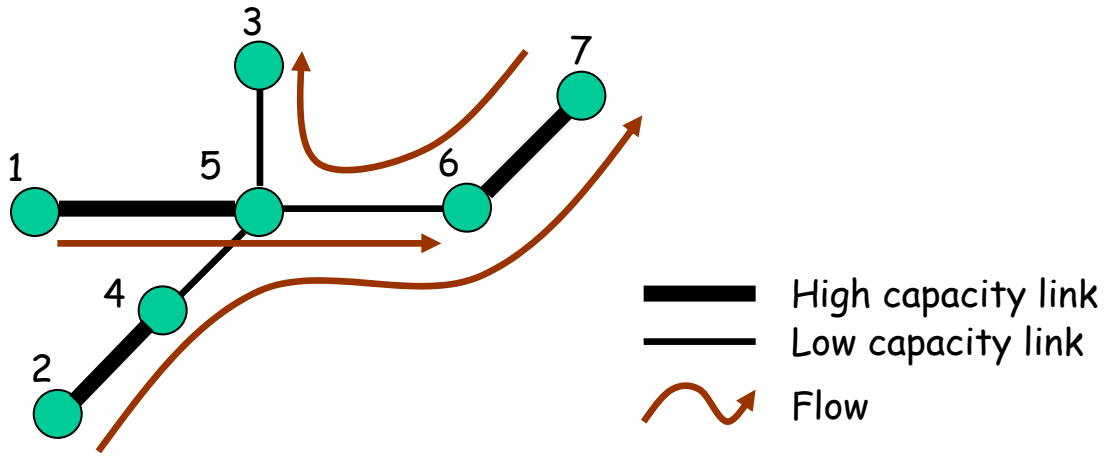


- **Global Mesh DTIM Interval**
  - All MPs generate beacon frames
  - MPs adjust local TSF or local offset
  - Fastest clock determines TSF



Congestion Control

- **Mesh characteristics**
  - Heterogeneous link capacities along the path of a flow
  - Traffic aggregation with multi-hop flows sharing intermediate links
- **Some issues with the 11/11e MAC for mesh**
  - Nodes blindly transmit as many packets as possible, regardless of how many reach the destination
  - Results in throughput degradation and performance inefficiency



Intra-Mesh Congestion Control

- **Local congestion monitoring**
  - Each node actively monitors local channel utilization
  - If congestion detected, notifies previous-hop neighbours and/or the neighbourhood
- **Congestion control signalling**
  - Congestion Control Request (unicast)
  - Congestion Control Response (unicast)
  - Neighbourhood Congestion Announcement (broadcast)
- **Local rate control**
  - Each node that receives either a unicast or broadcast congestion notification message should adjust its traffic generation rate accordingly
  - Rate control (and signalling) on per-AC basis – e.g., data traffic rate may be adjusted without affecting voice traffic
    - Example: MAPs may adjust BSS EDCA parameters to alleviate congestion due to associated stations

Summary

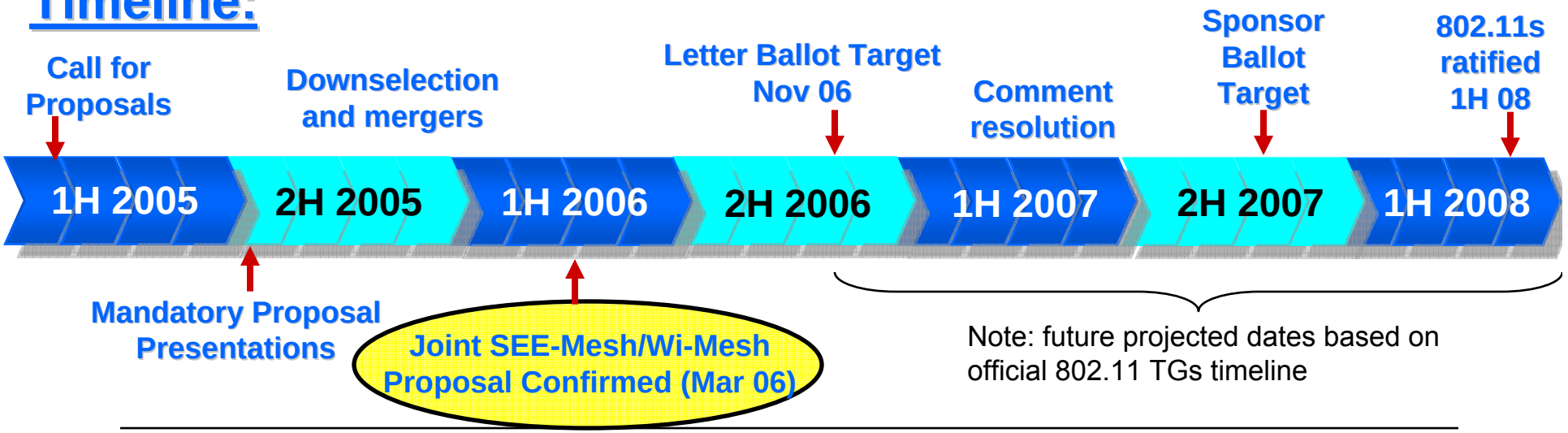
- **Mesh Networking provides a number of benefits to WLAN**
  - Enables rapid deployment with lower-cost backhaul
  - Easy to provide coverage in hard-to-wire areas
  - Self-healing, resilient, extensible
  - Replacement for today's ad-hoc mode
- **IEEE 802.11s amendment enables interoperable WLAN Mesh Networking implementations**
  - Extensible framework enables application across wide range of usage models
    - Office
    - Campus/Public Access
    - Residential
    - Public Safety/Military

Backup Materials

IEEE 802.11s Timeline

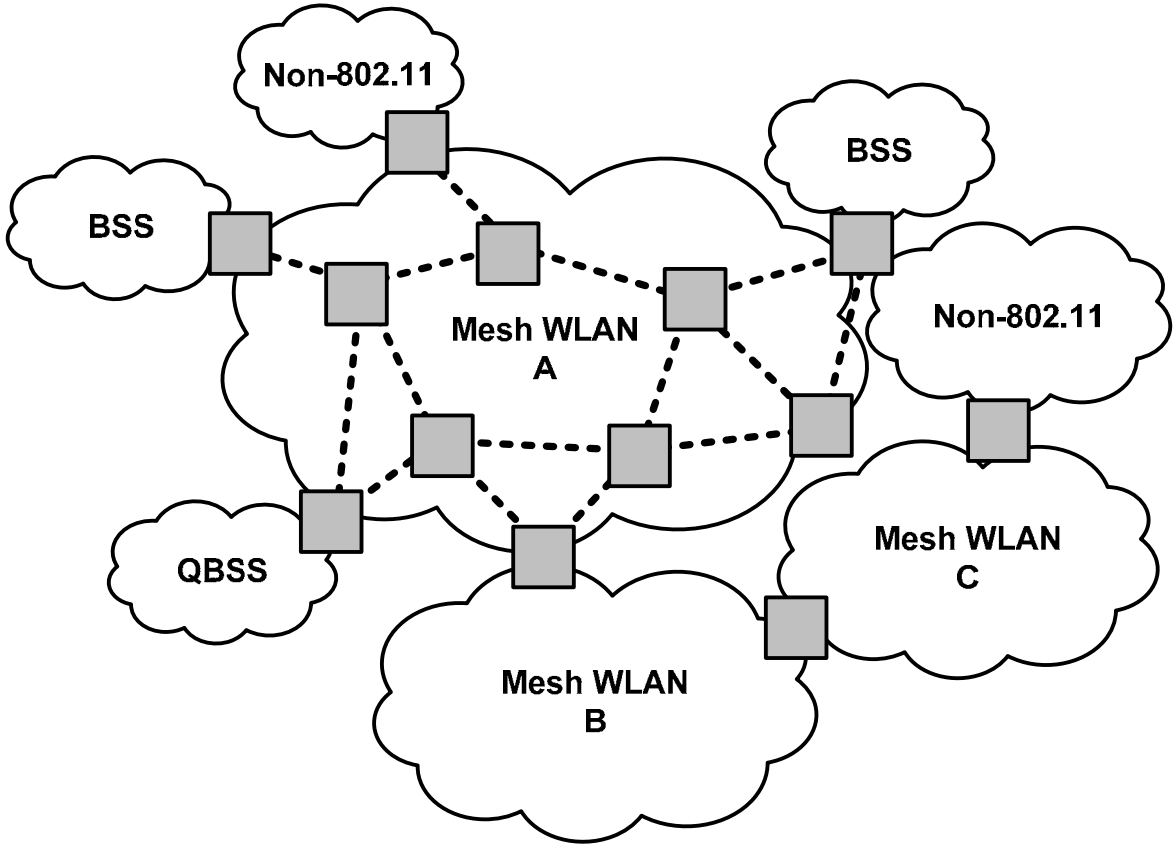
- January 04: Formation of 802.11 Mesh Study Group
- July 04: First 802.11 TGs Meeting
- January 05: Call for Proposals Issued
- July 05: Mandatory Proposal Presentations
- March 06: First 802.11s Draft Spec Adopted

Timeline:



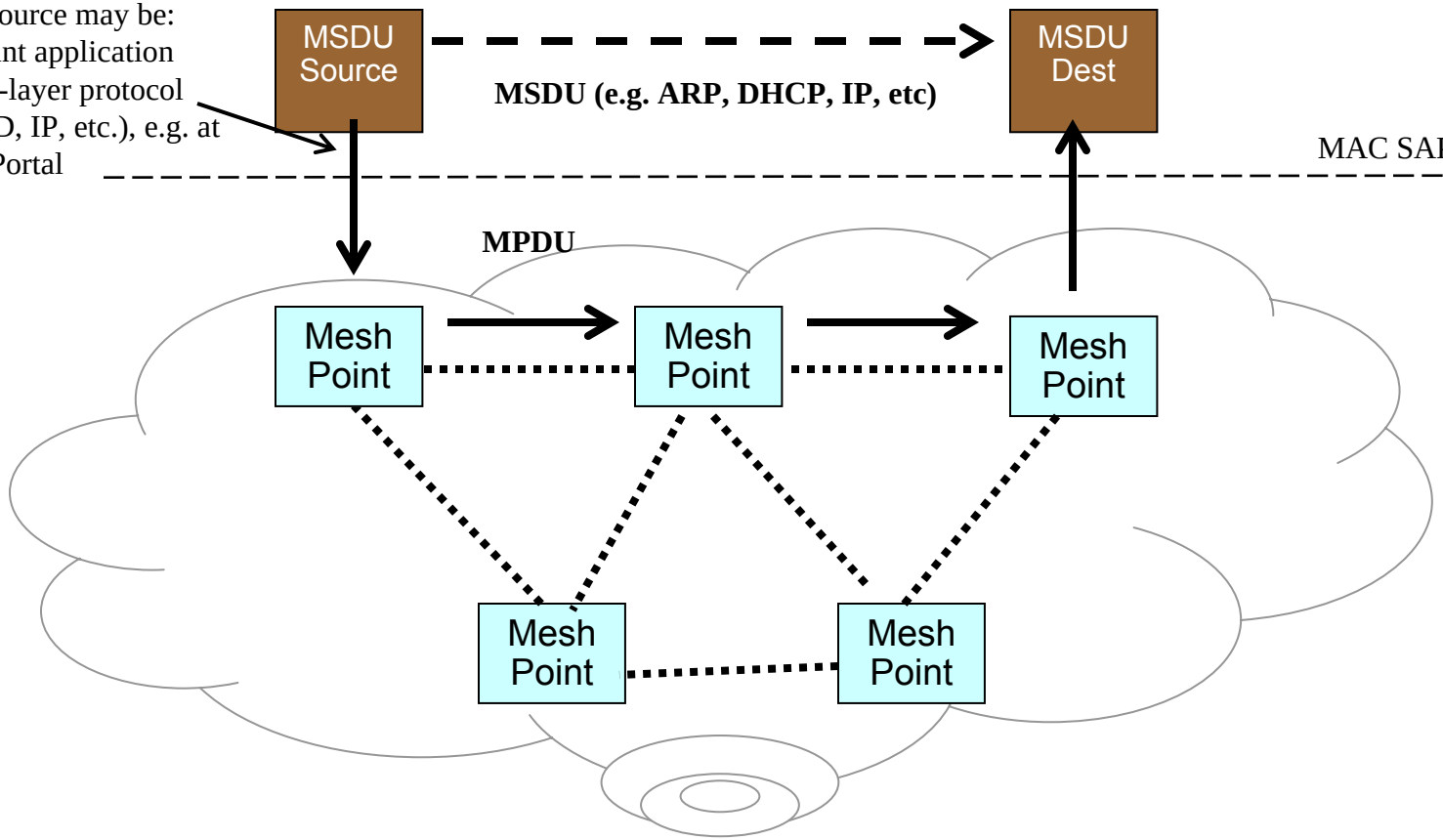
What does 802.11s provide?

- **802.11s defines *some* functions of the *grey boxes***
  - Some boxes are simpler than others



Interoperability with Higher Layer Protocols: MAC Data Transport over an 802.11s WLAN Mesh

MSDU source may be:
- Endpoint application
- Higher-layer protocol (802.1D, IP, etc.), e.g. at Mesh Portal
- Etc.



802.11s Transparent to Higher-Layers: Internal L2 behavior of WLAN Mesh is hidden from higher-layer protocols under MAC-SAP

Joint SEE-Mesh/Wi-Mesh Proposal

Documents

- Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs, 11-06/328r0, 27 February 2006
- Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs Overview, 11-06/329r3, March 6, 2006.
- Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs Checklists, 11-06/337r0, 27 February 2006.

Joint SEE-Mesh/Wi-Mesh Proposal

Affiliations of authors of the Joint Proposal

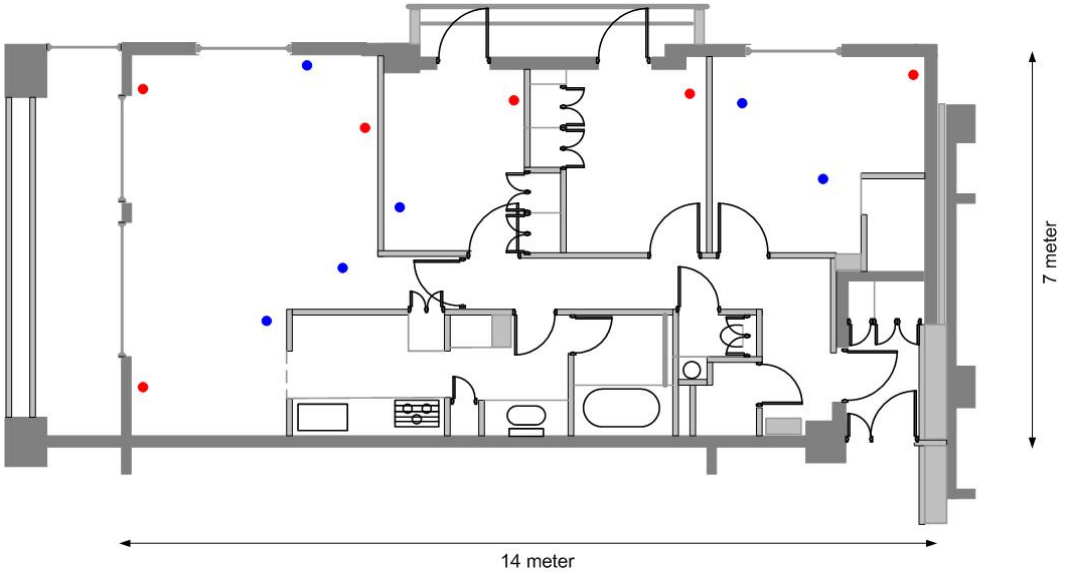
- Airespider
- ATR
- BAE Systems
- BelAir
- Cisco Systems
- ComNets
- NTT DoCoMo
- Firetide
- Fujitsu
- Hewlett Packard
- Huawei
- Intel
- InterDigital
- ITRI
- Kiyon
- Kyushu University
- MITRE
- Mitsubishi Electric
- Motorola
- NextHop
- NICT
- Nokia
- Nortel
- NRL
- NTUST
- Oki Electric
- PacketHop
- Philips
- Qualcomm
- Samsung
- Siemens
- Sony
- STMicroelectronics
- Swisscom
- Texas Instruments
- Thomson
- Tropos
- Wipro

IEEE 802.11s – Project Authorization Request

1. The proposed amendment shall be an extension to the IEEE 802.11 MAC.
2. The amendment will define an architecture and protocol for providing an IEEE 802.11 ESS Mesh […] to create an IEEE 802.11 Wireless Distribution System
3. […] over self-configuring multi-hop topologies.
4. An ESS Mesh is functionally equivalent to a wired ESS, with respect to the STAs relationship with the BSS and ESS.
5. A target configuration is up to 32 devices participating as AP forwarders in the ESS Mesh.
6. The amendment shall utilize IEEE 802.11i security mechanisms, or an extension thereof
7. […] in which all of the APs are controlled by a single logical administrative entity for security.
8. The amendment shall allow the use of one or more IEEE 802.11 radios on each AP in the ESS Mesh.

Residential Usage Case

In the digital home usage model, the primary purposes for the mesh network are to create low-cost, easily deployable, high performance wireless coverage throughout the home. The mesh network should help to eliminate RF dead-spots and areas of low-quality wireless coverage throughout the home. High-bandwidth applications such as video distribution are likely to be used within a home network, thus high bandwidth performance will be very important for residential mesh networks.



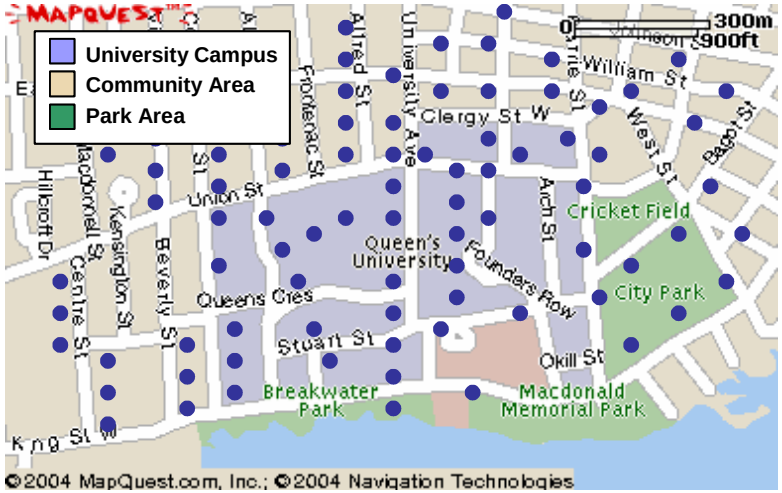
Office Usage Case

In the office usage model, the primary motivation for using mesh network technology is to create low-cost, easily deployable wireless networks that provide reliable coverage and performance.

WLAN Mesh networks are particularly useful in areas where Ethernet cabling does not exist or is cost prohibitive to install. Offices can reduce capital costs associated with cable installation and reduce time required for deployment. They may also benefit from an increase in employee productivity through expanded connectivity to key data network resources.

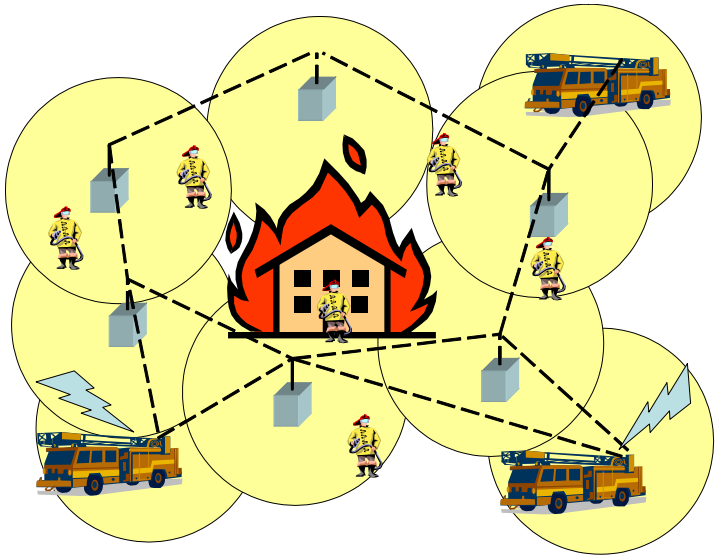
Campus / Community / Public Access Usage Case

• Seamless connectivity over large geographic areas.
• Rapidly provide connectivity to locations where wired infrastructure is not available or is cost prohibitive.
• Lower cost / higher bandwidth alternative to traditional internet access methods (dial up, cable, DSL, fiber).
• Enable advanced applications/services through ubiquitous access & reliable connectivity.
• Enable location based services. Location information is particularly important for public safety services.



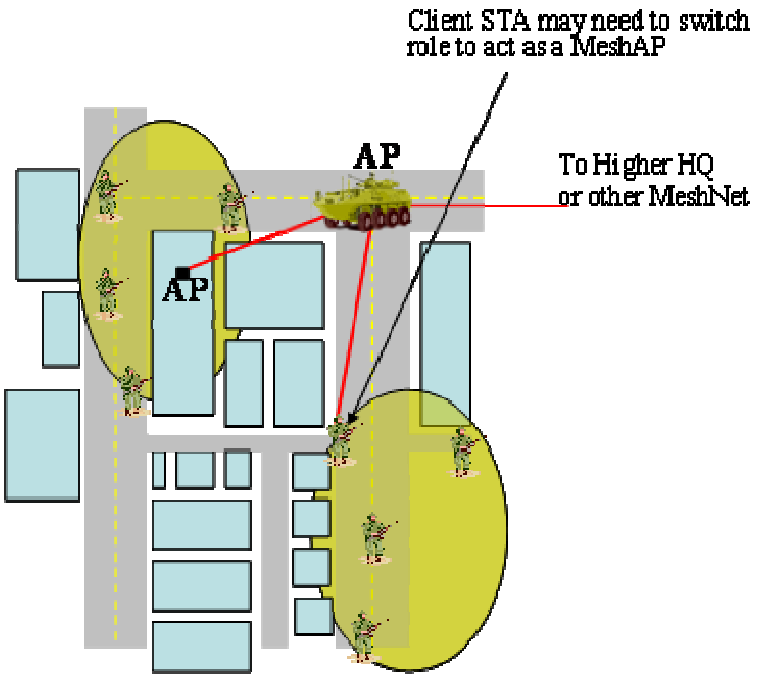
Public Safety Usage Case

Public safety mesh networks provide wireless network access to emergency and municipal safety personnel such as fire, police, and emergency workers responding to an incident scene. The network may be used for video surveillance, tracking emergency workers with bio-sensors, voice and data communication between emergency workers, uploading images, downloading hazmat information, tracking air status, etc.



Military Usage Case

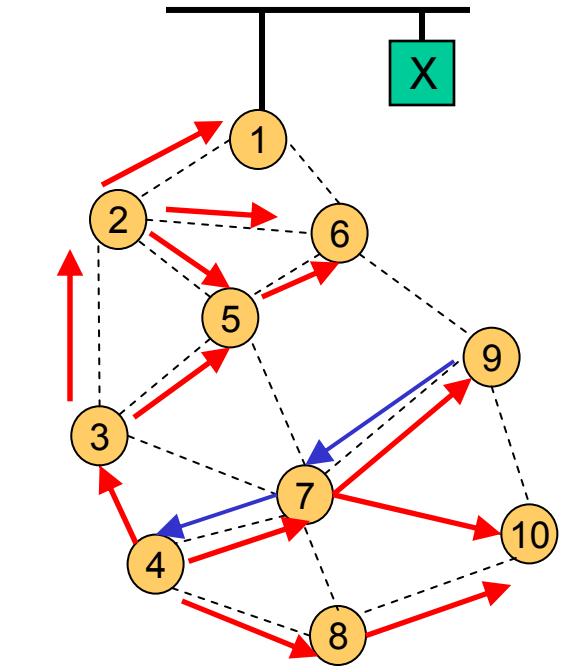
Military usage of mesh networks can be classified into two categories. The first category, non-combat usage, is adequately represented by the usage cases previously described in this document. The second category, combat operational usage, is distinguished by node mobility, a heavy reliance on fully automated network management and, for disadvantaged nodes, e.g., dismounted troops, sensitivity to energy conservation.

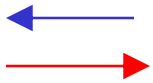


HWMP Example #1:
No Root, Destination Inside the Mesh

MP 4 wants to communicate with MP 9

1. MP 4 first checks its local forwarding table for an active forwarding entry to MP 9
2. If no active path exists, MP 4 sends a broadcast RREQ to discover the best path to MP 9
3. MP 9 replies to the RREQ with a unicast RREP to establish a bi-directional path for data forwarding
4. MP 4 begins data communication with MP 9



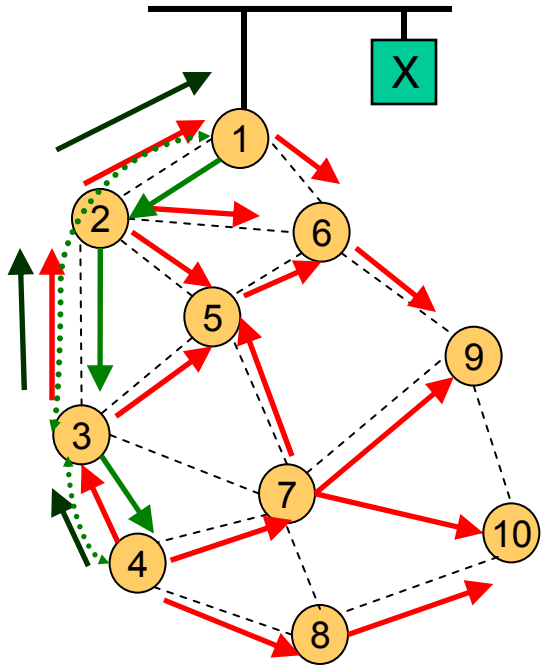


On-demand path

HWMP Example #2:
Non-Root Portal(s), Destination Outside the Mesh

MP 4 wants to communicate with X

1. MP 4 first checks its local forwarding table for an active forwarding entry to X
2. If no active path exists, MP 4 sends a broadcast RREQ to discover the best path to X
3. When no RREP received, MP 4 assumes X is outside the mesh and sends messages destined to X to Mesh Portal(s) for interworking
   - A Mesh Portal that knows X may respond with a unicast RREP
4. Mesh Portal MP 1 ` LAN segments according to locally implemented interworking

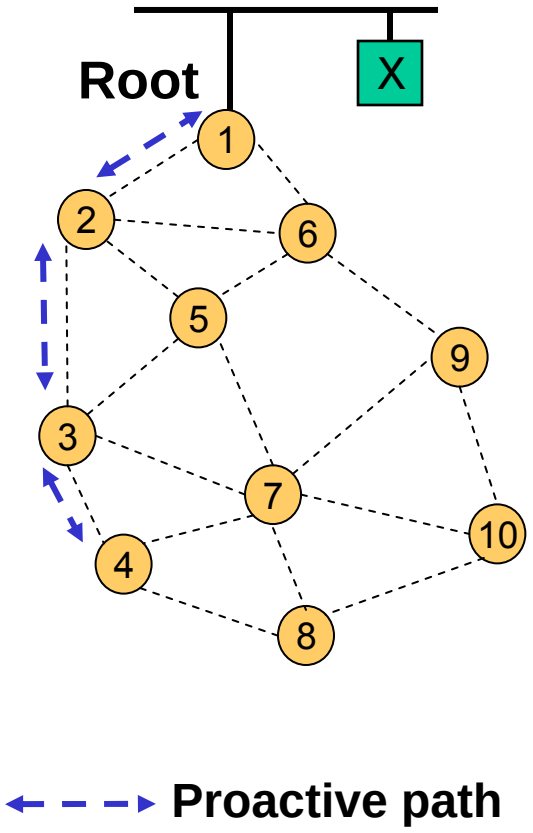


HWMP Example #3:
Root Portal, Destination Outside the Mesh

MP 4 wants to communicate with X

1. MPs learns Root MP 1 through Root Announcement messages
2. If MP 4 has no entry for X in its local forwarding table, MP 4 may immediately forward the message on the proactive path toward the Root MP 1
3. When MP 1 receives the message, if it does not have an active forwarding entry to X it may assume the destination is outside the mesh
4. Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking

Note: No broadcast discovery required when destination is outside of the mesh



HWMP Example #4:
With Root, Destination Inside the Mesh

MP 4 wants to communicate with MP 9

1. MPs learns Root MP 1 through Root Announcement messages
2. MP 4 first checks its local forwarding table for an active forwarding entry to MP 9
3. If no active path exists, MP 4 *may* immediately forward the message on the proactive path toward the Root MP 1
4. When MP 1 receives the message, it flags the message as “intra-mesh” and forwards on the proactive path to MP 9
5. MP 9, receiving the message, *may* issue a RREQ back to MP 4 to establish a path that is more efficient than the path via Root MP 1