# PhD Course

Lecture on

# 802.11 and Mesh Networking

## Paal E. Engelstad

# Outline

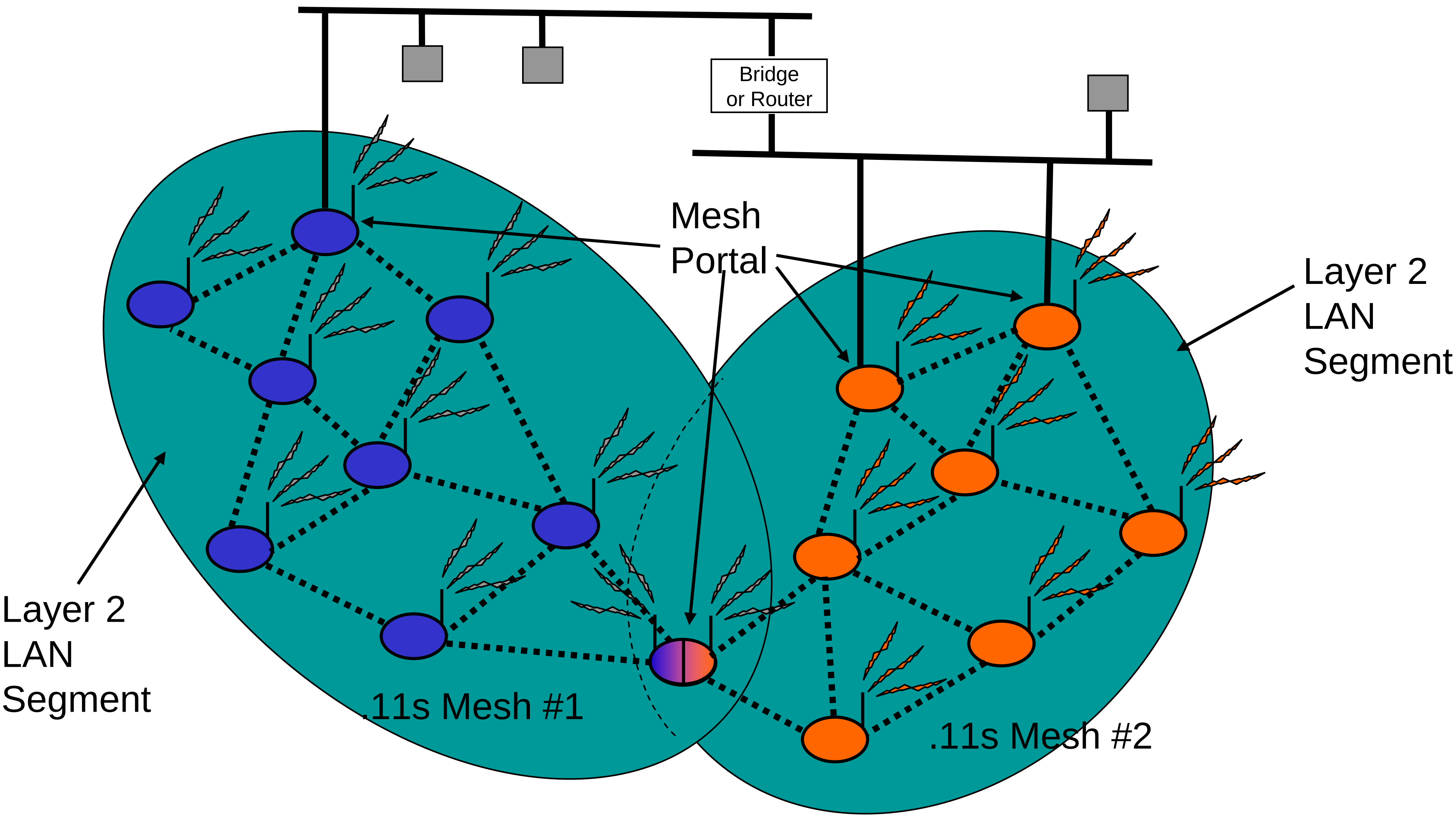
| | |
|---|---|
| **Basic 802.11 WLAN** | **(802.11a/b/g)** |
| **[Security in WLAN** | **(WEP, 802.11i/w)]** |
| **QoS in WLAN** | **(802.11e)** |
| **Markov Modeling** | **(Article)** |
| **Mesh networking** | **(802.11s)** |

This part now!

# Agenda for 802.11s / Mesh

- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

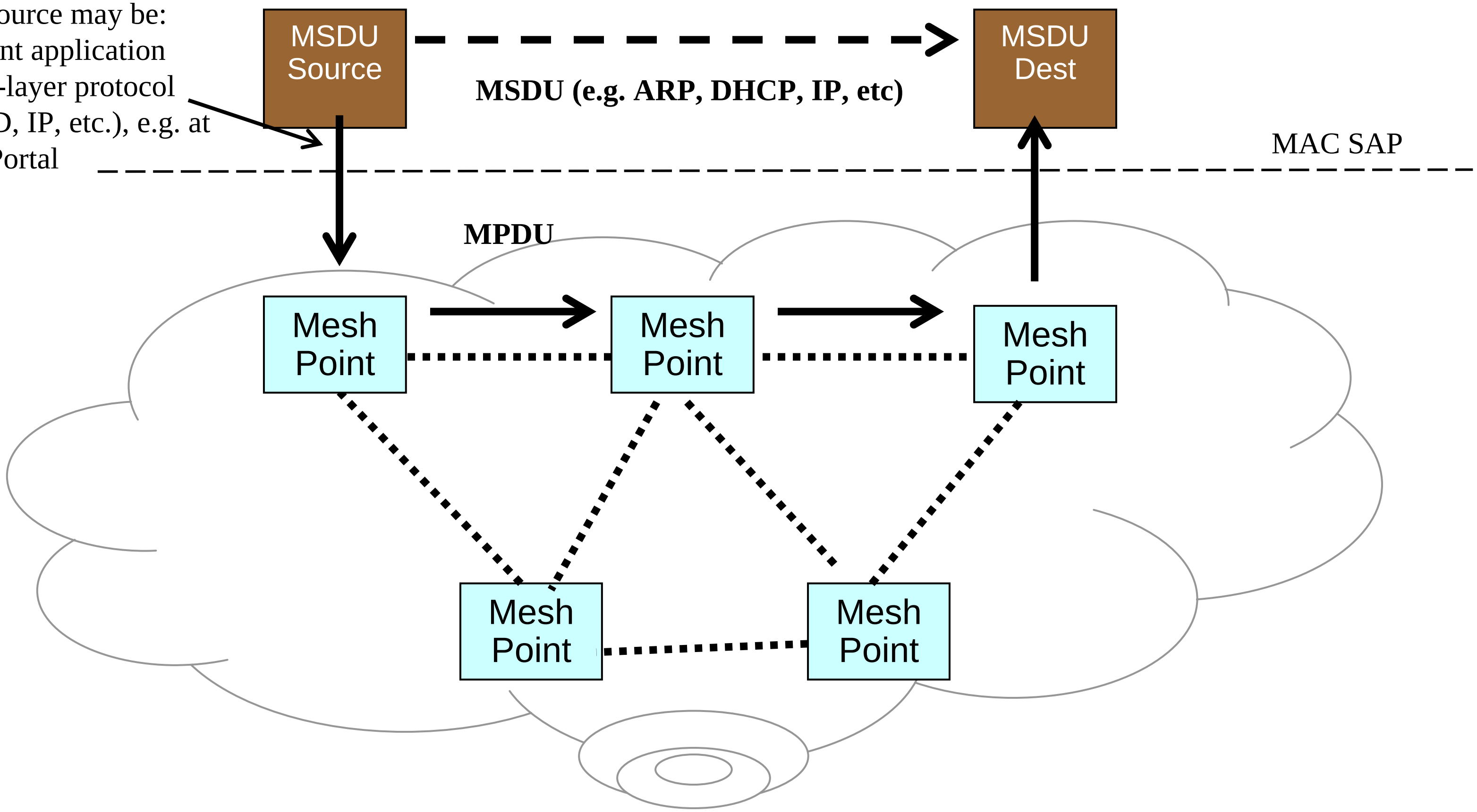
# So what is a Mesh Network?



# 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.



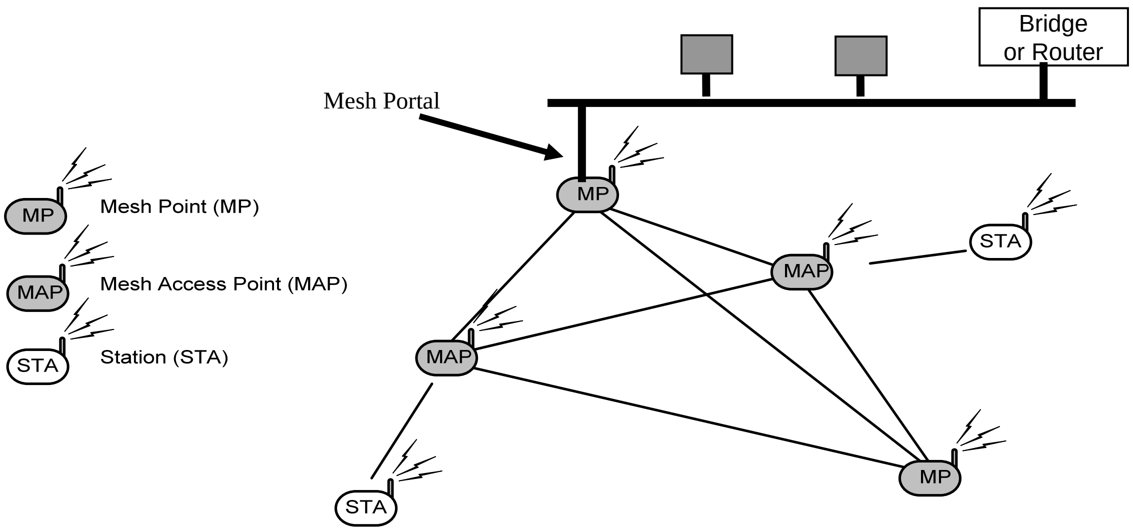

**802.11s Transparent to Higher-Layers: Internal L2 behavior of WLAN Mesh is hidden from higher-layer protocols under MAC-SAP**

# Agenda for 802.11s / Mesh

- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

# Device Classes in a WLAN Mesh Network

- **Mesh Point (MP):** establishes links with other MP neighbors, full participant in WLAN Mesh services
- **Mesh AP (MAP):** all functionality of a MP, plus provides BSS services to support communication with STAs
- **Mesh Portal (MPP):** point at which MSDUs exit and enter a WLAN Mesh
- **Light Weight MP (LWMP):** participate in subset of WLAN Mesh services primarily for neighbor-link communication
- **Station (STA):** outside of the WLAN Mesh, connected via Mesh AP (no new BSS functionality specified)

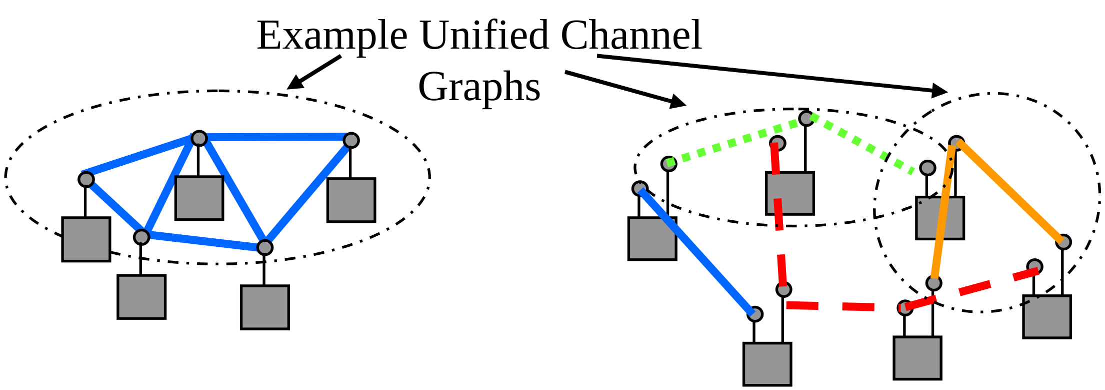


# Topology Formation: Membership in a WLAN Mesh Network

- Mesh Points 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 associated MP neighbors
  - E.g. Link state announcement, path selection information etc.
- Membership in a WLAN Mesh Network is determined by secure association with neighbors

# Topology Formation: Support for Single & Multi-Channel Meshes

- Each MP may have one or more logical radio interface:
  - Each logical interface on one (infrequently changing) RF channel, belongs to one “Unified Channel Graph”
  - Two possible modes for each interface:
    - Simple channel unification mode (follow rules to coalesce into a common, fully connected graph on one channel)
    - Advanced mode (framework for flexible channel selection, algorithms/ policy beyond scope of this proposal)
  - Each Unified Channel Graph shares a channel precedence value
    - Channel precedence indicator – used to coalesce disjoint graphs and support channel switching for DFS
  - Provides foundation for the optional Common Channel Framework



# Agenda for 802.11s / Mesh

- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

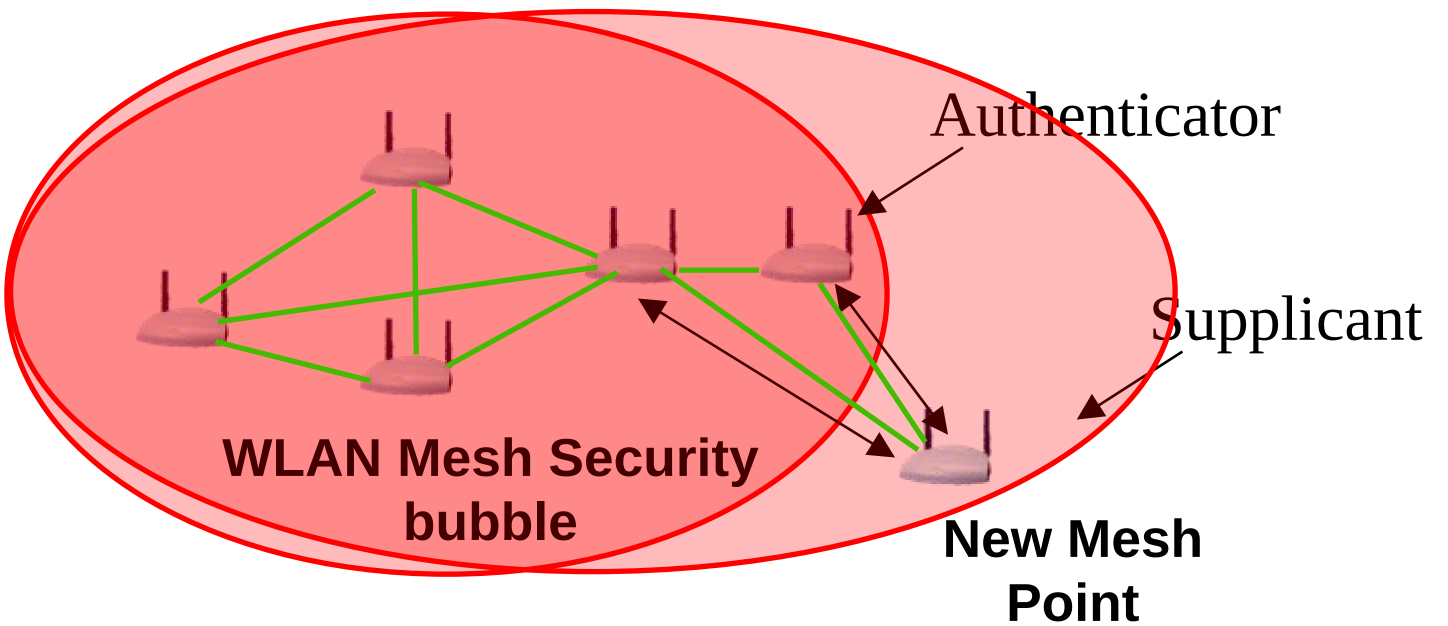
# Security Goals and Requirements

- Reuse/build on top of current 802.11i techniques
  - Leverage extensibility already built in to 802.11i – e.g., allow for both distributed and centralized authentication schemes
  - *Note that 802.11i provides link-security*
    - *End-to-end security could be layered on top, e.g. using IPSEC. This is beyond the scope of 802.11s*
- What new functionality beyond 11i?
  - Allow association/authentication between neighboring Mesh Points/ Mesh APs
  - Protect mesh management and control messages exchanged between Mesh Points/Mesh APs (e.g. routing and topology info)
    - *Goal: Align with TGw mgmt frame security*

# Security Basic Model

- Authenticated mesh points are trustworthy participants in WLAN Mesh services (path selection protocol, data forwarding, etc.)
  - Aligned with TGs security scope: all Mesh Points belong to single logical administrative domain – not targeted at secure mesh between un-trusted devices
- Each mesh point acts as supplicant and authenticator for each of its neighbors
  - Similar to IBSS security model in 802.11i
- Each MP uses 4-way handshake with each neighbor to establish session keys
  - Each MP uses its own group session key to broadcast/multicast and pair-wise session keys for unicast
- Number of keys is O (num_neighbors)

# Basic Security Model




- Pair-wise keys are used for unicast communications
- Group key is used for broadcast/multicast communications
- Authentication can be distributed or centralized

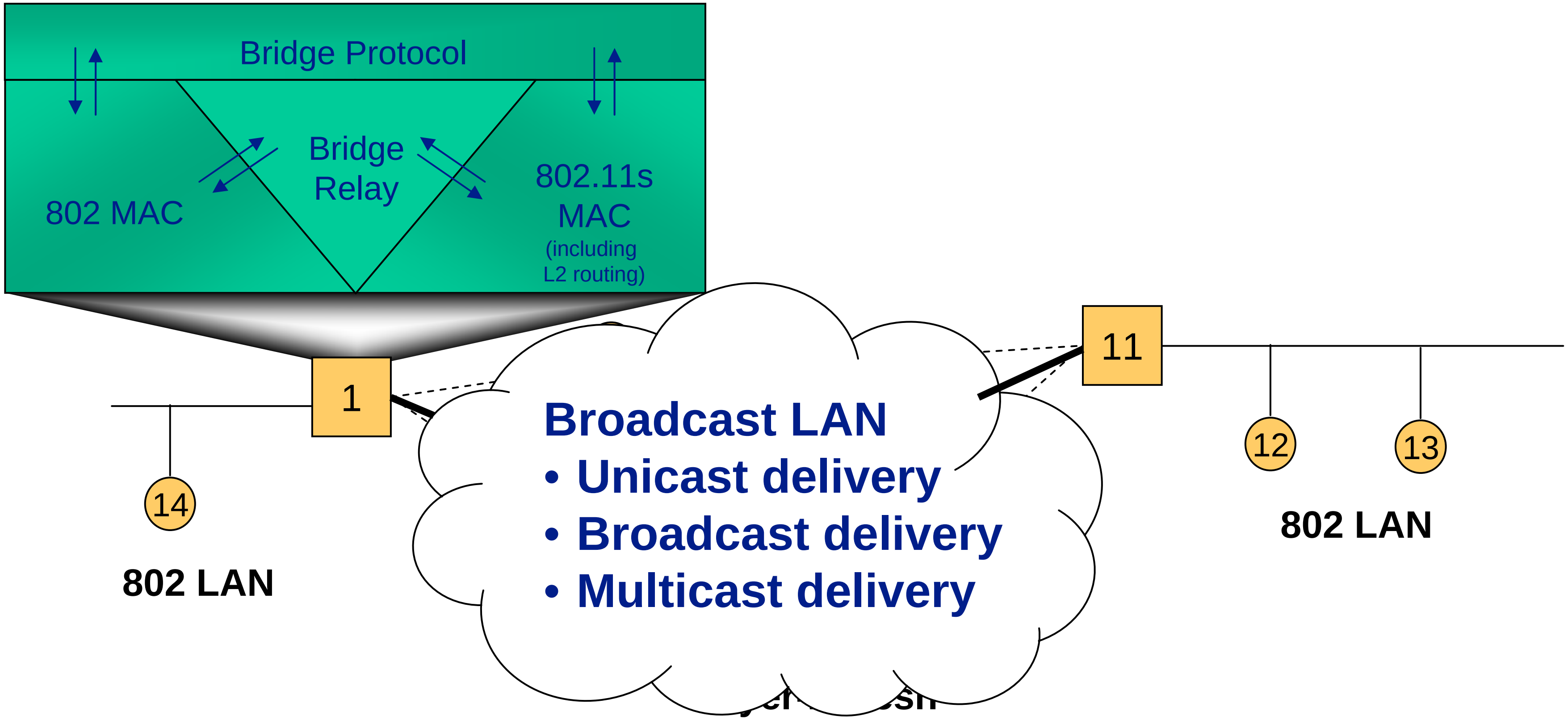
# Security of Management Frames

- Security of management frames is important for 802.11s
  - E.g., allow routing information to be authenticated
- Goal:
  - Rather than defining a unique solution for management frame security in 802.11s, work with TGw to ensure that general management frame security covers requirements for TGs
  - Adapt TGw framework to 802.11s
- A liason should be appointed

# Agenda for 802.11s / Mesh

- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

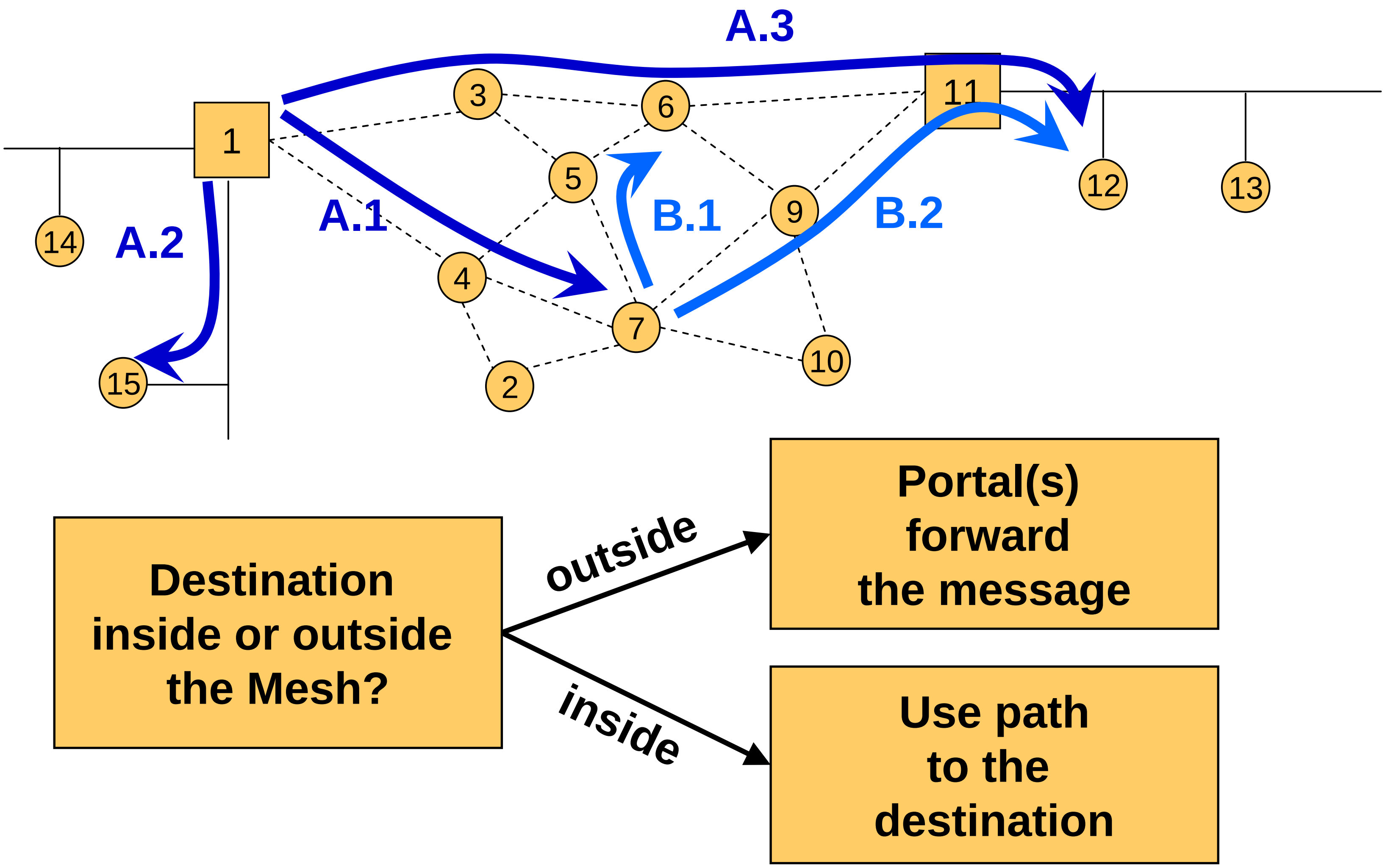
# Achieving 802 LAN Segment Behavior




**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

# Agenda for 802.11s / Mesh

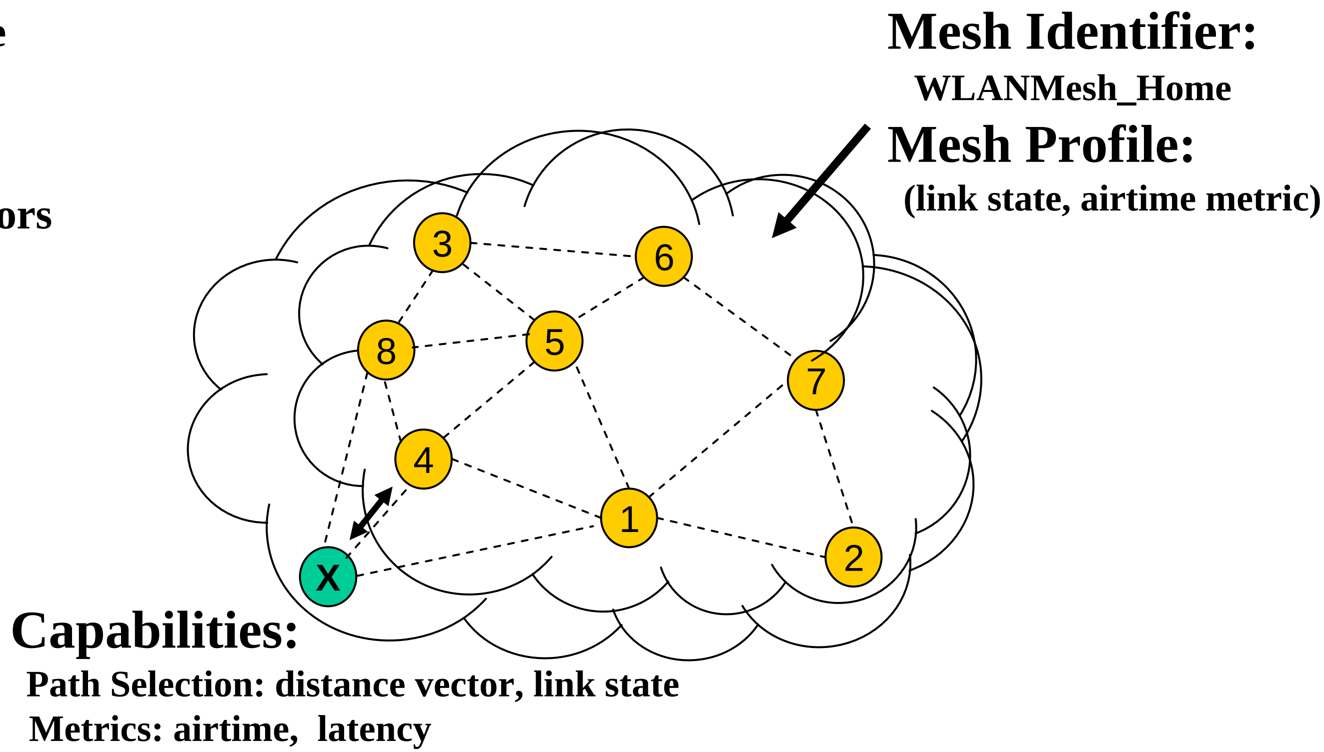
- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

# Extensible Framework Support for Mandatory and Alternative Path Selection Protocols

- **All implementations support 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**
- **MIB objects provide a standard management interface to the mandatory and alternative path selection protocols**
- **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 Mesh Association Enabling Extensible Protocol and Metric Implementation

1. **Mesh Point *X* discovers Mesh (WLANMesh_Home) with Profile (link state, airtime metric)**
2. **Mesh Point *X* associates / 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**




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

# Hybrid Wireless Mesh Protocol (HWMP)

## *Default Path Selection for Interoperability*

- Combines the flexibility of on-demand route discovery with the option for efficient proactive routing to a mesh portal
  - Supports any path selection metric (QoS, load balancing, power-aware, etc)
  - Simple mandatory metric based on airtime as default, with support for other metrics

- On demand service 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

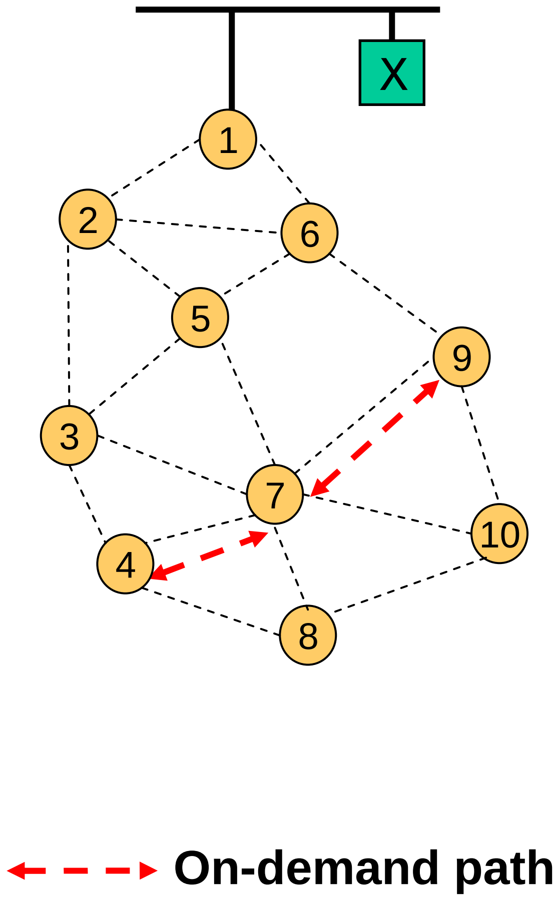
- Pro-active services based on tree based routing
  - If a Root portal is present, a distance vector routing tree is built and maintained
  - Tree based routing is efficient for hierarchical networks
  - Tree based routing avoids unnecessary discovery flooding during discovery and recovery

- HWMP resource demands vary with Mesh functionality
  - Makes it suitable for implementation on a variety of different devices under consideration in TGs usage models from CE devices to APs and servers

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

<u>Example: MP 4 wants to communicate with MP 9</u>

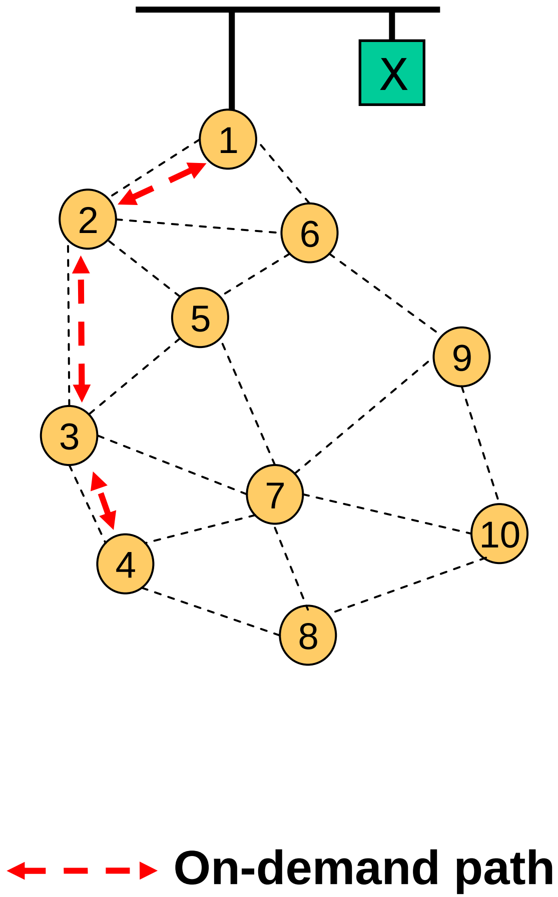
1. **MP 4 first checks its local forwarding table for an active forwarding entry to MP 9**
2. **If no active path exists, MP 4 sends a broadcast RREQ to discover the best path to MP 9**
3. **MP 9 replies to the RREQ with a unicast RREP to establish a bi-directional path for data forwarding**
4. **MP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



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

Example: 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 forwards messages to other LAN segments according to locally implemented interworking**

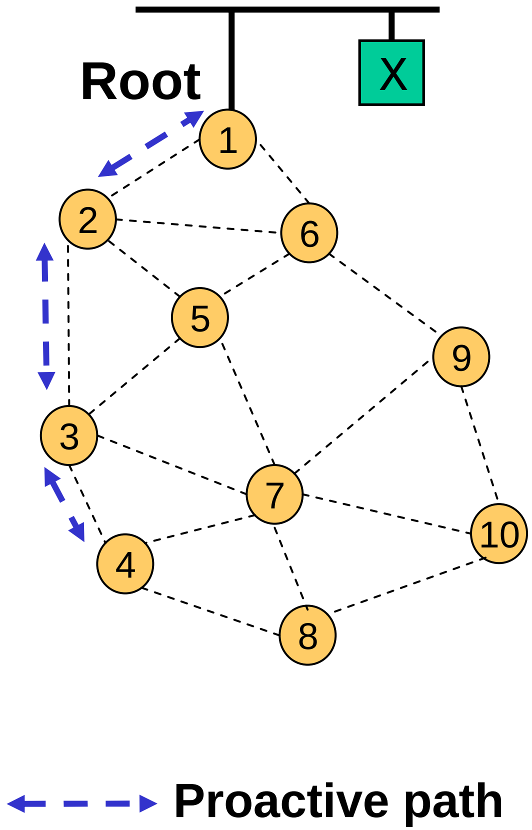


# HWMP Example #3: Root Portal, Destination Outside the Mesh

<u>Example: MP 4 wants to communicate with X</u>

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**

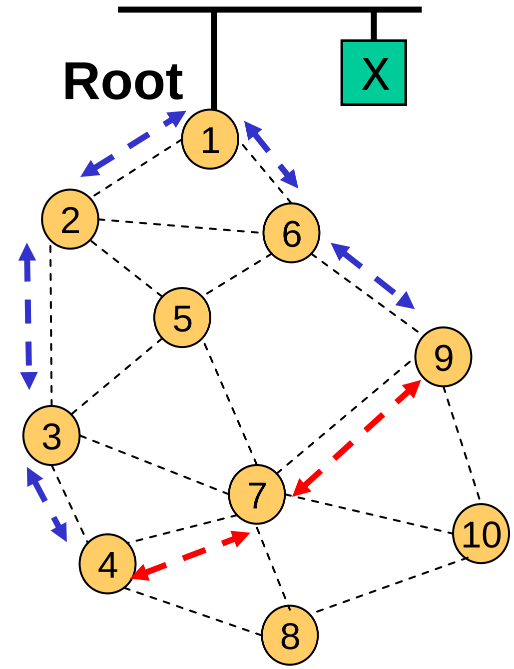
***Note: No broadcast discovery required when destination is outside of the mesh***



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

Example: 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**




**Proactive path**

**On-demand path**

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

- A unified and extensible routing framework based on the two link-state routing protocols:
  - OLSR (RFC 3626)
  - (Optional) Fisheye State Routing (FSR)

- RA-OLSR, proactively maintains link-state for routing

- With the following extensions:
  - Use of radio aware metric in MPR and routing path selection
  - Efficient association discovery and dissemination protocol to support 802.11 stations

# Agenda for 802.11s / Mesh

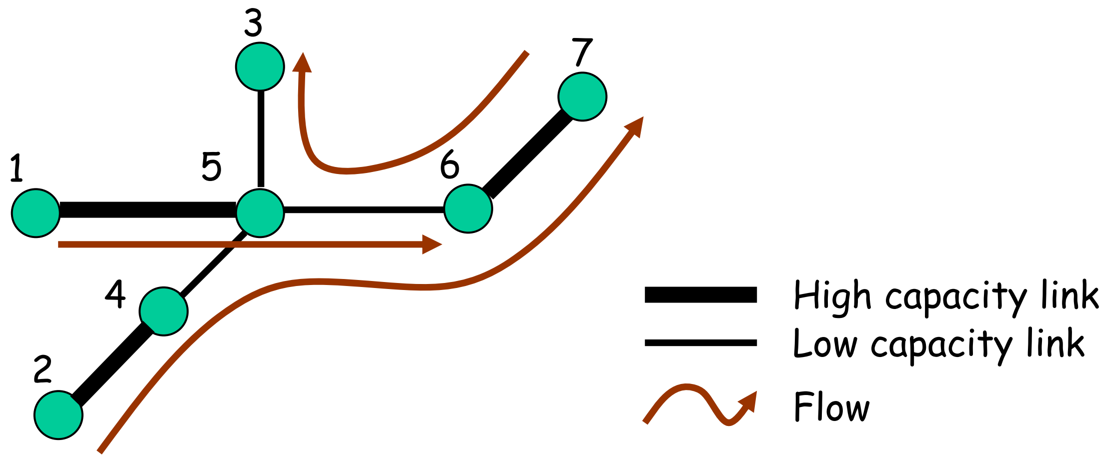
- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

# MAC Based on 802.11e EDCA

- EDCA as the basis for the .11s media access mechanism
  - Re-use of latest MAC enhancement from 802.11
  - Compatibility with legacy devices
  - Interaction of forwarding and BSS traffic
    - Handling of multi-hop mesh traffic and single-hop BSS traffic within one device treated as implementation choice
- MAC Enhancement for mesh
  - Intra-mesh Congestion Control
  - Common Channel Framework (Optional)
  - Mesh Deterministic Access (Optional)

# Need for Congestion Control

- Mesh characteristics
  - Heterogeneous link capacities along the path of a flow
  - Traffic aggregation: Multi-hop flows sharing intermediate links
- 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 Mechanisms

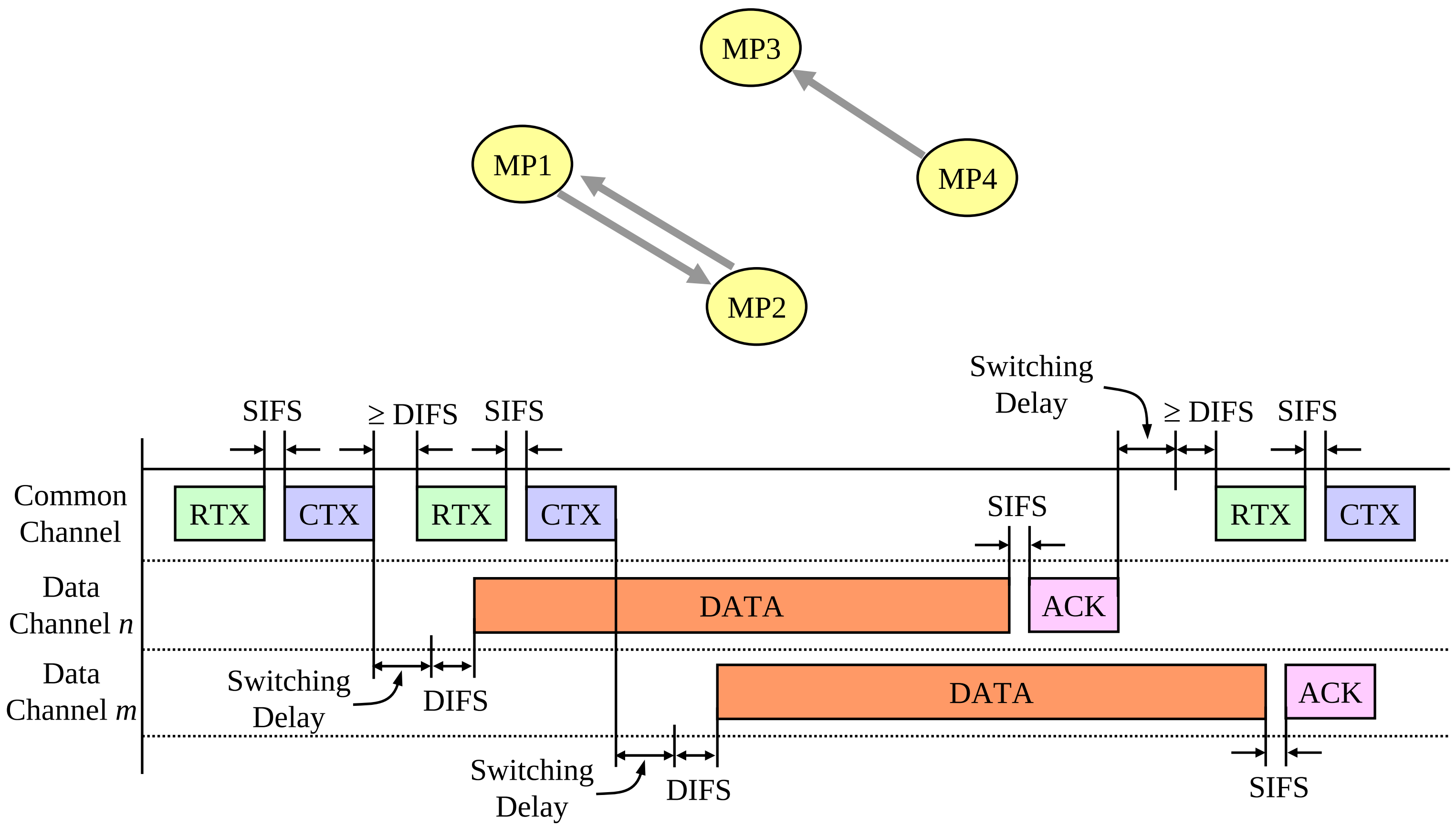
- Local congestion monitoring *(informative)*
  - Each node actively monitors local channel utilization
  - If congestion detected, notifies previous-hop neighbors and/or the neighborhood
- Congestion control signaling
  - Congestion Control Request (unicast)
  - Congestion Control Response (unicast)
  - Neighborhood Congestion Announcement (broadcast)
- Local rate control *(informative)*
  - Each node that receives either a unicast or broadcast congestion notification message should adjust its traffic generation rate accordingly
  - Rate control (and signaling) 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 STAs

* *Informative sections provide recommendations for efficient mesh network implementation but are not normative specifications and are not strictly required for interoperability.*

# Common Channel Framework (CCF) for Multi-Channel MAC Operation (Optional)

- A framework that enables single and multi-channel MAC operation for devices with single and multiple radios.
  - Common channel is:
    - Unified Channel Graph (see UCG slide) on which MPs and MAPs operate.
    - The channel from which MPs switch to a destination channel and return back.
  - MPs with multiple radios may use a separate common channel for each interface
  - CCF supports optional channel switching in different forms
    - After RTX/CTX exchange on common channel, MP pairs switch to a destination channel and then switch back
    - Groups of MPs may switch to a negotiated destination channel
- Neighbors discover support for CCF during association.
  - Using the Mesh Capability IE in the beacon

# Multi-Channel CCF for Single Radio: Channel Switching

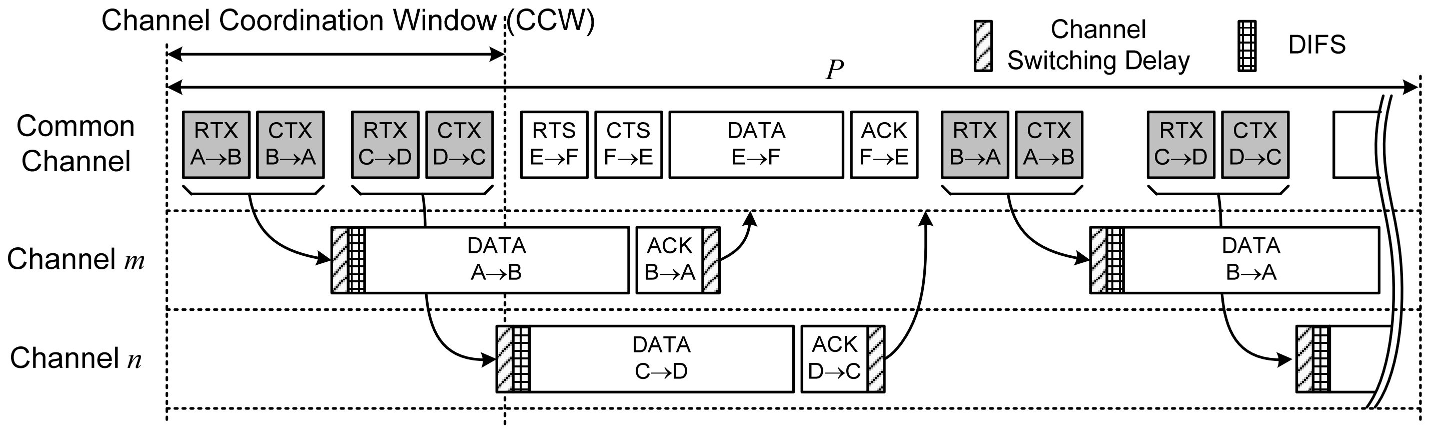


# MAC Mechanism for the CCF

- Using RTX, the transmitter suggests a destination channel.
- 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.

# Channel Coordination

- A channel coordination window (CCW) is defined on the common channel
- At the start of CCW, CCF enabled MPs tune to the common channel.
  - This facilitates arbitrary MPs to get connected.
  - Channel Utilization Vector (**U**) of each MP is reset.
  - MPs mark the channel as unavailable based on channel information read from RTX/CTX frames.
- *P* is the period with which CCW is repeated.
  - CCF enabled MPs initiate transmissions that end before *P.*
  - MPs can stay tuned to the CC beyond CCW duration.
- *P* and CCW are carried in beacons.



# Accommodating Legacy Behavior

- To devices that do not implement CCF, the common channel appears as a conventional single channel.
- Common channel can be used for data transmission.
- A MAP with a single radio may use the common channel for WDS as well as BSS traffic.
- Dynamic channel selection is restricted to MPs that support CCF.

# Mesh Deterministic Access – MDA (Optional)

- Objective:
  - Lower contention (more deterministic) access mechanism for improved QoS for periodic flows
  - Does not require support from non-implementing MPs

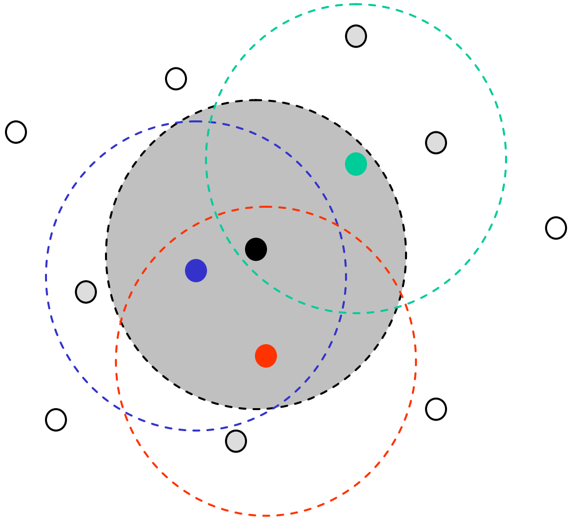
- Mechanism:
  - Simple handshake between transmitter-receiver to set up the deterministic access opportunities called MDAOPs
  - Advertisement and state-keeping of transmitting, receiving, and interfering MDAOPs to ensure non overlap of potentially interfering MDAOPs
  - Two hop neighborhood clearing for low contention
  - Low contention access during MDAOPs

All MPs can use EDCA at all times with the appropriate IFS

# MDA Overview

- Set up periodic MDAOPs for transmissions such that there is no overlap with
  - MDA advertised Transmissions from all neighbors
  - MDA advertised Receptions at all neighbors

  The advertisements may include HCCA, beacon, and other known busy times



Example possibly interfering areas for node •

# MDAOP Setup, Teardown, and Advertisements

- Setup Request: Unicast from a transmitter to a receiver using MDAOP Setup Request IE
- Setup Reply: Unicast from a receiver of Setup Request IE to the sender using the MDAOP Setup Reply IE
  - Accept setup
  - Reject setup, possibly with reasons and alternate suggestions
- MDAOP advertisements: MDAOP and possibly other known busy times are advertised broadcast using MDAOP Advertisements IE
- MDAOP teardown: Either the transmitter or the receiver may indicate a teardown by transmitting the MDAOP Set Teardown IE to the other

# Operation During MDAOP

- 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

- Nodes that own an MDAOP
  - Access the channel using MDA parameters for CWMin, CWMax, and AIFSN
  - Send traffic for one TXOP
  - Use retransmit rules the same as EDCA
  - Relinquish any remaining MDAOP time by sending CF-End or QoS-Poll to self with zero duration

# Agenda for 802.11s / Mesh

- Intro
- Topology and Discovery
- Security
- Interworking Approach
- Path Selection and Forwarding
- MAC enhancements
- Beaconing, Synchronization and Powersave

# Beaconing and Synchronization Overview

- Synchronization
  - Optional capability
  - IBSS method

- Beaconing: Reuse of existing modes
  - IBSS mode
    - Synchronizing non-AP MPs
  - Infrastructure mode
    - All MAPs
    - Unsynchronizing non-AP MPs

- Beacon collision avoidance
  - Synchronizing non-AP MPs: IBSS beaconing mechanism
  - Synchronizing MAPs: offsets and avoidance mechanisms
  - Unsynchronizing MPs: optional avoidance mechanisms

# Synchronization: Salient Features

A Synchronization capable MP

- May choose to be synchronizing
  May request synchronization from peers
- May choose to be unsynchronizing
  If no neighbors are requesting synchronization and do not need synchronization itself

Synchronization and Mesh TSF

- IBSS like synchronization method
  - Adopt the latest TSF
- Timer in MPs
  - Non-AP MPs: Mesh TSF
  - MAPs: Mesh TSF in terms of timer plus offset

# Beacon Collision Avoidance

- Choose or Shift to non-colliding times for its own TBTTs
  - Discover time instants used by potential colliding MPs for beaconing
  - Discover any collisions of its own and other’s beacons
- Beacon Timing information exchange
  - In Beacons at any selected frequency
  - In action frames through a request-response approach
- Beacon Timing information exchange formats
  - Beacon timing IE:
    - From Synchronizing neighbors: with respect to Mesh TSF
    - From Unsynchronizing neighbors: with respect to self TSF
  - 802.11 k beacon reports

# Powersave Mechanisms (Optional)

- Mechanisms focused on powersave between neighbors
  - Sleep wake cycles are not coordinated across multiple hops
  - Supporting of neighbors sleep-wake cycles is optional
  - MPs that support powersave may enter sleep state

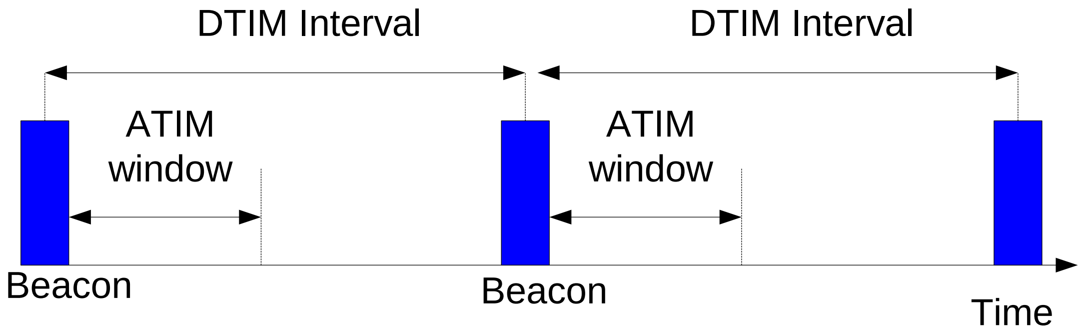
- Two approaches:
  - **The APSD approach**: similar to 802.11e APSD
    - **Periodic APSD**
    - **Aperiodic APSD**
  - **The ATIM / DTIM approach**
    - Well known wake times coordinated with well-known specific beacon times

# APSD based Sleep-Wake Operation

- Similar to 802.11e APSD solution for BSS based WLANs
- Periodic-APSD: Sleep-wake times coordinated with each neighbor separately and independently
  - Used for QoS traffic such as VoIP
  - Pairs of neighbors setup periodic schedules to wake up at set times
- Aperiodic-APSD : MP in powersave state sends a packet to an ‘always awake’ neighbor to indicate it is awake
  - Used only with neighbors that are awake all the time
  - PS state MP sends a packet to the neighbor to indicate it is awake any time it wishes

# ATIM based Sleep-Wake Operation

- Guaranteed window of awake time after periodic DTIM beacons
- DTIM interval is a multiple of beacon intervals; globally unique to the mesh
- Control communication in ATIM window
  - Indicating pending traffic
  - Indicating change in PS state
  - Re-instating of stopped flows
- Remain awake after ATIM window depending on the control communication in it



# Powersave: Salient Features

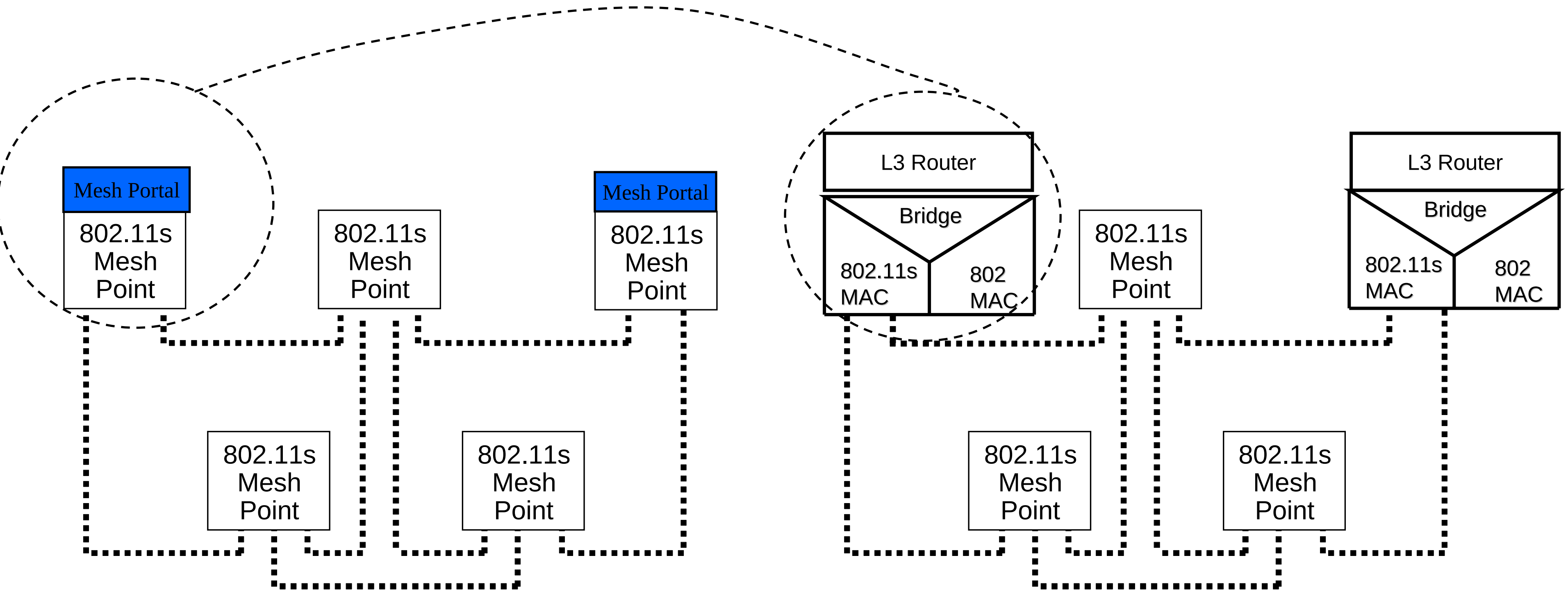
- Reduced beaconing frequency
  - Possibility of DTIM only beacons
  - Efficient sharing of beaconing responsibility
- Efficient power save state advertising
  - In beacons
  - Using QoS Null packets with PS bit indication
- Mechanisms to allow MPs to be awake only for the portion of time required for actual reception
  - Efficient use of “more data bit” and “EOSP”
- Scope for agreed, flexible, and non beacon related periodic transmissions between Mesh Points operating in powersave

# Backup Slides
# (With Additional Details)

# Outline of the 802.11s Draft

1 Executive Summary
2 Definitions
3 Abbreviations and Acronyms
4 General Description
5 MAC Frame Formats
6 WLAN Mesh Services
  - **6.1 Use of Mesh Identifier**
  - **6.2 Single and Multiple Radio Devices**
  - **6.3 Mesh Topology Discovery and Formation**
  - **6.4 Mesh Path Selection and Forwarding**
    - **- Extensible Path Selection Framework**
    - **- Path Selection Metrics**
    - **- Path Selection Protocols**
      - **- Hybrid Wireless Mesh Protocol (Default protocol for interoperability)**
      - **- Radio Aware OLSR Path Selection Protocol (Optional)**
    - **- Data Message Forwarding**
  - **6.5 Security**
  - **6.6 Optimizations to EDCA for Mesh Points**
  - **6.7 Intra-Mesh Congestion Control**
  - **6.8 Multi-Channel MAC Using Common Channel Framework (Optional)**
  - **6.9 Mesh Deterministic Access (Optional)**
  - **6.10 Interworking Support in a WLAN Mesh**
  - **6.11 Configuration and Management**
  - **6.12 Mesh Beaconing and Synchronization**
  - **6.13 Power Management in a Mesh (Optional)**
  - **6.14 Layer Management (Informative)**

# Reference Model for 802.11s Interworking



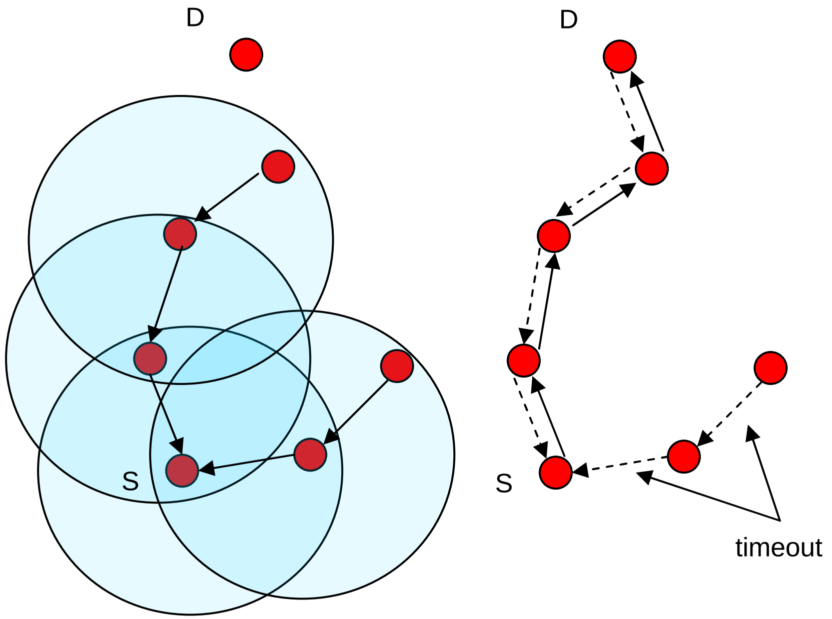

The 802.11s MAC entity appears as a single port to an 802.1 bridging relay or L3 router. 802.11s mesh portals expose the WLAN mesh behavior as an 802-style LAN segment (appears as a single loop-free broadcast LAN segment to the 802.1 bridge relay and higher layers).

*** See IEEE 802.17 Annex F for another example 802 multi-hop L2 standard that used a similar approach.**

# Backup slides on path selection protocols

# On-demand Routing in HWMP (based on AODV) – Key Features

- On Demand Routing Protocol
  - AODV 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 broadcasted from Source node
  - 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**

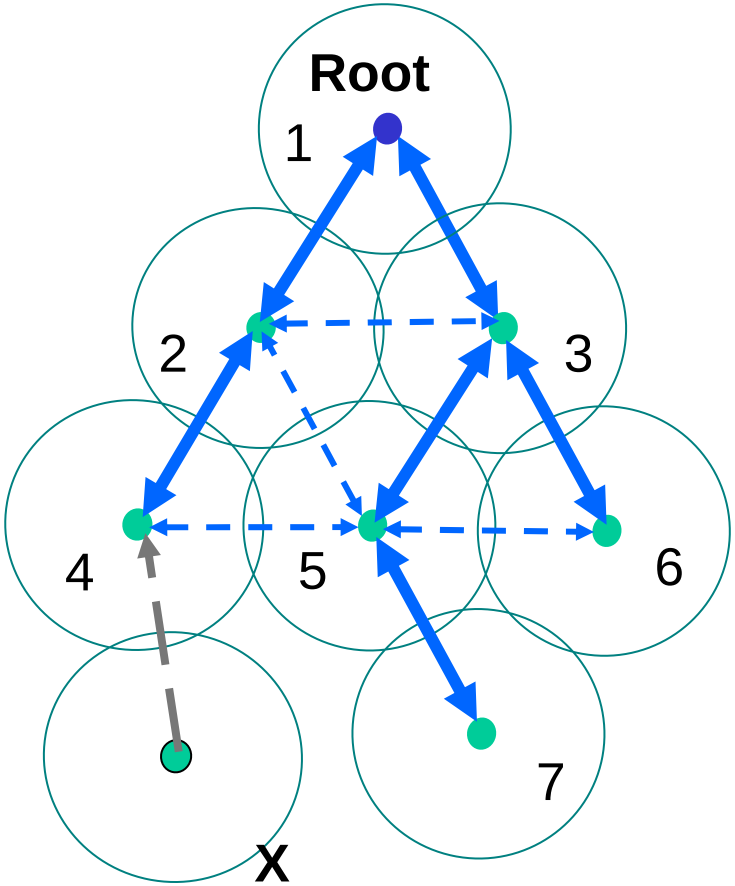
Figure From:
C. E. Perkins and E. M. Royer., Ad-hoc On-Demand Distance Vector Routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90-100.

# On-demand routing in HWMP – Key Features (cont'd)

- 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 its destination sequence number which guarantee the loop-freedom of all routes towards that node. It avoids the Bellman-Ford "counting to infinity" problem by using sequence numbers.

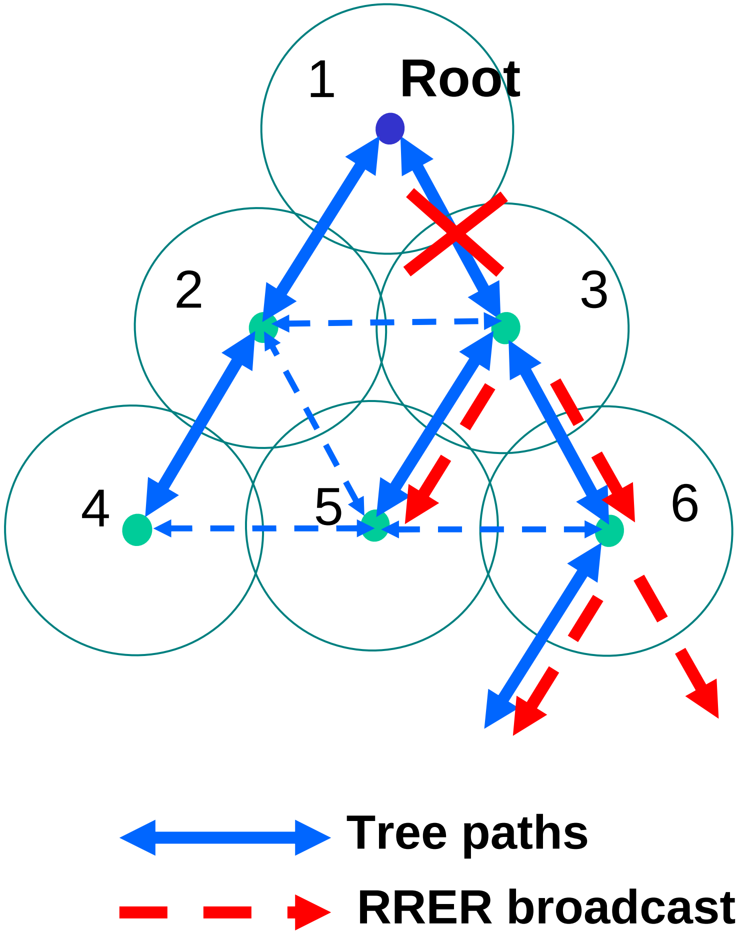
# Tree-based Routing in HWMP – Key Features

- Topology Creation
  - The Root MP issues “Root Announcements”
    - Arbitration scheme allows for auto-formation and recovery
  - Non-root MPs bind to the Root MP or other MPs based on best path metric
    - Best path propagates down from the Root (e.g. X-4-2-1)
  - “Registration” by MPs facilitates downstream message handling by the Root
    - Applies equally to MPs and STA’s attached to MPs



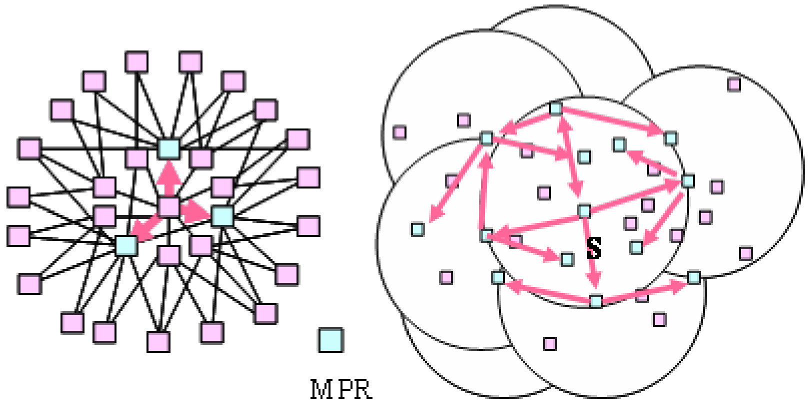
# Tree-based Routing in HWMP – Key Features (cont'd)

- Topology Maintenance
  - Portals monitor the Root and take over if Root fails (Root arbitration)
  - MPs monitor their upstream links and may switch to back up links (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 AODV path holders that some path is broken

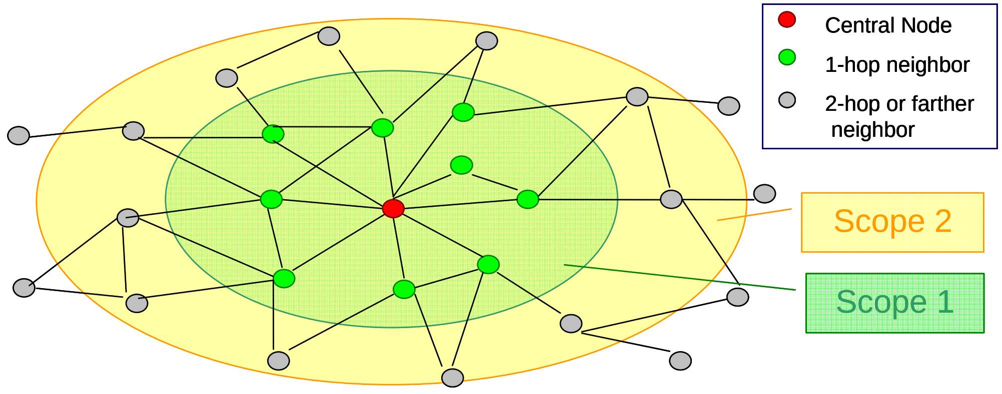


# RA-OLSR – Key Features

- 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***.

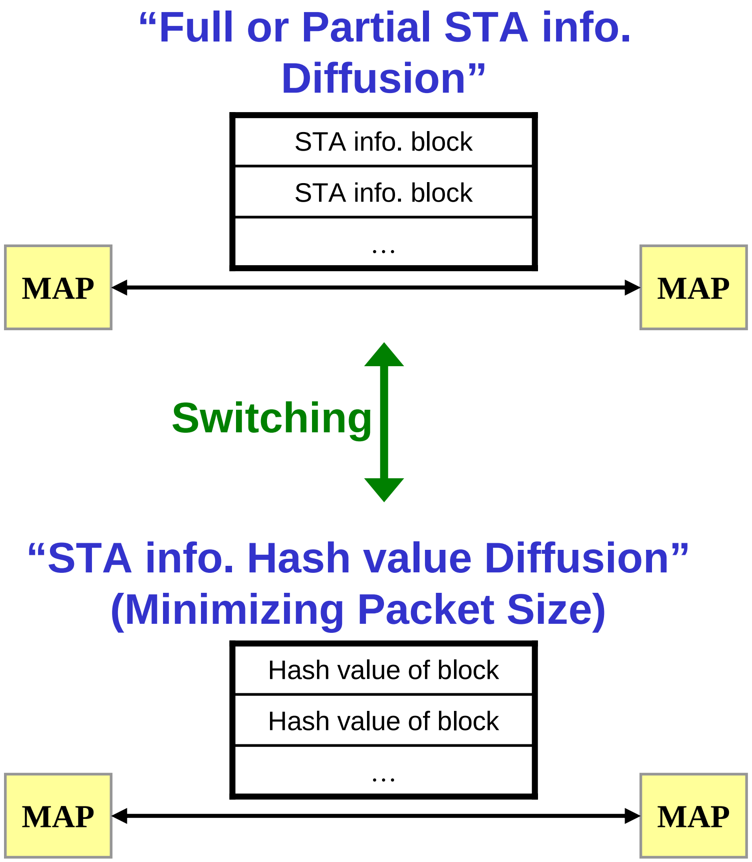



- (Optional) Fisheye-scope-based message exchange frequency control
  - Lower exchange frequency for nodes within larger scope
    - Further reduce message exchange overhead ***in time***.



# RA-OLSR – Optimized Associated Station Discovery

- Adaptive distribution of STA information
  - In initial stage, MAP sends Full STA info. block (Full Diffusion)
  - When the association table doesn’t change frequently, MAP sends only hash values of STA info. Block (Hash value Diffusion)
- Minimizing STA information traffic
  - MAP sends requested STA info. block (Partial Diffusion)
  - Hash values of STA info. block minimize packet size



# Mesh Data Frames (Extensions to 4-Addr Frame Format)

| 2 | 2 | 6 | 6 | 6 | 2 | 6 | 2 | 3 | | 4 |
|---|---|---|---|---|---|---|---|---|---|---|
| Frame Control | Dur | Addr 1 | Addr 2 | Addr 3 | Seq Control | Addr 4 | QoS Control | Mesh Control | Body | FCS |

**MAC Header**

| 0 – 7 | 8 – 23 |
|---|---|
| Mesh TTL | Mesh E2E Seq |

**Mesh Control**

- Data frames transmitted from one MP to another use the 802.11-1999 four address format as a basis, extended with the 802.11e QoS header field and a new Mesh Control header field.

- Mesh Control Field:
  - TTL – eliminates possibility of infinite loops
  - Mesh E2E Seq # – enables controlled broadcast flooding, unicast reliability and ordering services

# Backup slides on Common Channel Framework (CCF) for Multi-Channel MAC

# Control Frames

- Request to Switch (RTX) Frame

| 2 | 2 | 6 | 6 | 2 | 4 |
|---|---|---|---|---|---|
| Frame Control | Duration/ ID | RA | TA | Destination Channel Info. | FCS |

- Clear to Switch (CTX) Frame

| 2 | 2 | 6 | 2 | 4 |
|---|---|---|---|---|
| Frame Control | Duration/ ID | RA | Destination Channel Info. | FCS |

# Backup slides on powersave mechanism

# Quick Return to Sleep from Awake

- The mechanisms support returning to sleep as soon as possible
  - EOSP bit for APSD
  - ‘more bit’ used in the ATIM mode
  - No requirement for keeping awake until next beacon if no indication of further traffic as above

# Efficient power save state advertising

- Broadcast QoS-Null packet with PS bit set to ‘1’ in two consecutive ATIM windows
- Beacon based advertisement
  - Mesh PS IE carries PS state in subsequent beacons
  - Neighbors list with their powersave state is carried in BB beacons
    - No requirement on all MPs to keep track of every neighbor all the time

# IBSS versus Mesh Powersave

- IBSS PS
  - Requires at least a single STA to be awake at any given time; For a P2P link this in effect forces a STA to be awake for over 50% of the time
  - IBSS PS does not include defined method to derive the power save state of other STA
- Mesh PS
  - All powersaving MPs may be asleep between DTIM beacons
  - Mesh PS includes a low complexity mechanism for power save state advertising

# IBSS versus Mesh Powersave (cont’d)

- IBSS PS
  - Requires STA to be awake for a full Beacon period on reception of any traffic from other STA; this is true even if the traffic itself is extremely short; makes PS operation for fixed rate packetized applications (Voice, video conf) complexly useless
  - IBSS PS requires STA to announce intention to transmit to PS STA on defined windows after each beacon
  - IBSS PS requires STA to wakeup for every Beacon interval

- Mesh PS
  - Mesh PS requires mesh points to be awake only for the portion of time required for actual reception; uses EOSP and More bits to indicate that mesh point may return to doze mode
  - Mesh PS allows for setup of agreed flexible and non beacon related schedules for transmission between mesh points operating in PS