What is Multicast?

- **Multicast**: Delivery from one source to many end stations that are part of a defined multicast group or “subnet of machines”

- The sender transmits only *one copy* of a message to a “multicast address”. That message is replicated within the network and delivered to multiple recipients.

---

**Quote of the day**

“To steal ideas from one person is plagiarism;

To steal from many is research.”

-Unknown

“The Internet is a great way to get on the Net.”

- Bob Dole

---

**What is Multicast (cont)**

![Multicast Diagram]
Multicast Uses

- Multiparty Videoconferencing
- Multiparty Audioconferencing
- Shared Whiteboards (Distance Learning)
- Networked Games
- Distributed Interactive Simulations
- Networked news, sports, weather, stock tickers

Benefits of Multicast

- Efficiency
  - Reduces the sender’s transmission overhead
  - Reduces network bandwidth usage
  - Reduces latency observed by receivers

- Scalability
  - Sender only has to send the packet ONE time, to a virtually unlimited number of receivers

Benefits of Multicast (cont)

- Example: Suppose you are a stock quote ticker update service with 1000 clients. A set of stock updates requires 26 packets to transmit.

  - Traditional “Replicated Unicast” would require 26 * 1000 = 26000 packets. If average packets size is 200 bytes, you are generating 5.2 MB of traffic for each update. (Consider 100,000 clients)
  - If the same service was using multicast, it would send exactly 26 packets for an unlimited number of clients.

How does it work?

- **Host Group Model**: Fundamental architecture under which all multicast protocols have been developed

  - Host group represented by a group address
  - Traffic destined for group are addressed to its group address
  - Up to the routers to determine how to reach group members
  - *Senders need not* be a member of the group to which they are sending
  - *Group membership receiver initiated*
### Why do I care about Multicasting?

- Multicasting is ideal for wireless communications, where bandwidth is limited.
- My research involves “Wireless Ad-Hoc Tactical Networks” and this may be a part of the solution.
- In “Wireless Ad-Hoc Tactical Networks” traditional multicasting is not sufficient. We need **Secure Multicasting**.

### Secure Multicasting

**Secure Multicasting (cont)**

- For secure multicasting we will need:
  - **Cryptography & Key management scheme**
    - Cryptographic keys must to used to encrypt and decrypt messages.
    - The Cryptographic keys must be recalculated and redistributed upon certain events such as a member joining/leaving the group.
  - **Group management scheme**
    - Who is or is not part of the group?
    - What happens if the group changes?
    - What does the group look like?

---

#### Secure Multicasting

- **A Secure multicast protocol** must:
  - Ensure that participants to the group may access the distributed information only when they are **authorized** to do so.
  - Ensure that only authorized participants to the group may distribute information to the group.
  - How can we do this ???

#### Secure Multicasting (cont)

- These issues have been research in the past, but primarily for use in a *wired* environment.
- For Secure Multicasting in a *wireless* environment, we must consider other factors:
  - Power and airtime constraints
  - Bandwidth constraints
  - Host mobility
  - Wireless security issues
In Conclusion

- Secure Multicasting in a wireless environment is a complex problem
- Solutions will require extending previous research that focused on wired systems, taking wireless factors into consideration

802.11b Wireless Network Security

- *802.11* refers to a family of specifications developed by the IEEE for wireless LAN technology
- Three methods to secure an 802.11 Wireless Network
  - Service Set Identifier (SSID)
  - Media Access Control (MAC) address filtering
  - Wired Equivalent Privacy (WEP)

SSID

- A mechanism to segment a wireless network into multiple networks serviced by one or more Access Points (AP)
- Each AP is programmed with a SSID corresponding to a specific wireless network
- To access the network, a client must present the correct SSID
SSID Problems

- Most AP’s come with a default setting “Broadcast SSID” (in the clear)
- Because users typically configure their own client systems, SSID are widely know and easily shared
- Once an attacker has discovered the SSID, he has access to the network

WEP

- 802.11 standard specifies the WEP security protocol to provide encrypted communication between the client and an access point
- WEP employs symmetric key cryptography and the RC4 stream cipher
- All clients and the AP use the same key (64 or 128 bits) to encrypt and decrypt data
- The key is input into RC4 and the resulting sequence is used to encrypt the data to be transmitted

MAC Address Filtering

- Each AP can be programmed with a list of MAC addresses associated clients authorized to use the network
- The administrative overhead of maintaining the list limits the scalability of this approach
- What if the Network Card is lost, stolen, loaned, etc…?

WEP Problems

- Keys must be changed manually by an administrator. In practice keys are rarely, if ever, changed
- Most AP’s come with WEP turned off by default
- Recently WEP has been proven to be vulnerable to many attacks
Final Comments

- The industry and IEE are working on solutions to the problems, and the Advanced Encryption Standard (AES) has been identified as a possible replacement for WEP.
- Despite the weaknesses of current 802.11 security, a combination of 128 bit WEP, SSID, and Mac level filtering is probably sufficient for many small networks with low-to-medium level security requirements.
- For high security networks, a VPN solution may exist.