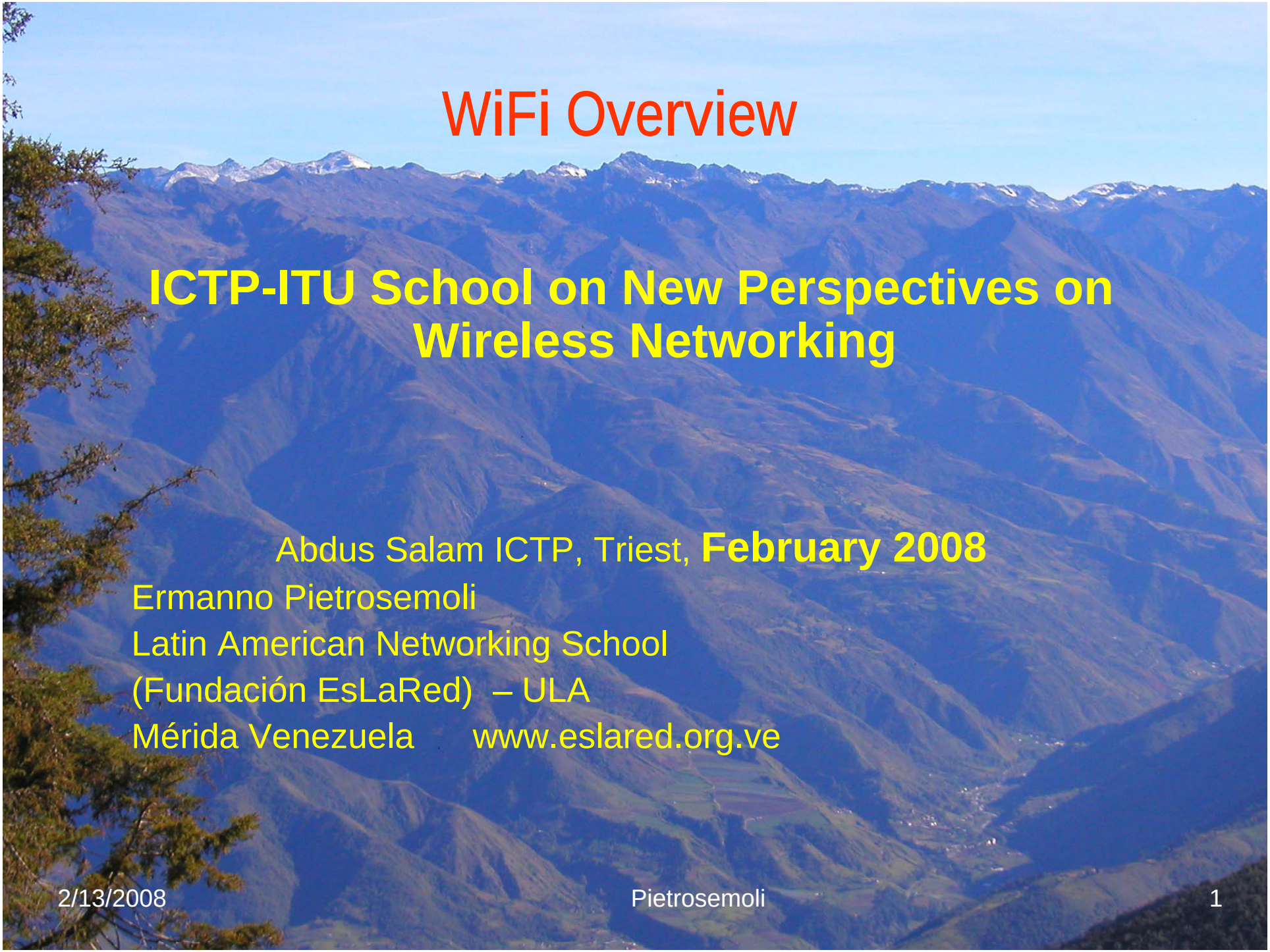


WiFi Overview

ICTP-ITU School on New Perspectives on Wireless Networking

Abdus Salam ICTP, Triest, **February 2008**

Ermanno Pietrosemoli
Latin American Networking School
(Fundación EsLaRed) – ULA
Mérida Venezuela www.eslared.org.ve

WiFi Overview
Agenda

- 802.11 Standards
- 802.11 Terminology
- DSSS Channel Allocation
- Medium Access Control
- Power Considerations
- Scanning
- Configuration
- Interference

Wireless Data Transmission flavors

- Packet Radio over VHF or HF
- Wireless Local Area Networks (WLAN)
- Wireless Local Loop (WLL, LMDS)
- Free Space Optics
- Satellite Transmission

Wi-Fi Technology Overview

- Wireless networks where borne as LANs, but for developing countries' applications they are more useful as MANs or even WANs
- The enormous success of this technology has led to a dramatic price reduction of the radios +modem, from $750 in 1992 to $20 in 2007, while transmission speed has increased from 1 Mbps to more than100 Mbps on the same 20 MHz channel

Wi-Fi Technology Overview: Standards

- IEEE 802.11 1 and 2 Mbps, Frequency Hopping, DSSS (915 or 2400 MHz) or IR, ratified in 1977

As far as the IEEE is concerned there is only one standard - **IEEE 802.11**. This standard is continuously updated by means of amendments:

- IEEE 802.11a up to 54 Mbps, 5 GHz, OFDM
- IEEE 802.11b up to 11 Mbps, 2.4 GHz, DSSS

Both ratified in 1999

- IEEE 802.11g up to 54 Mbps, 2.4 GHz, OFDM, downward compatible with 802.11b, ratified in 2003

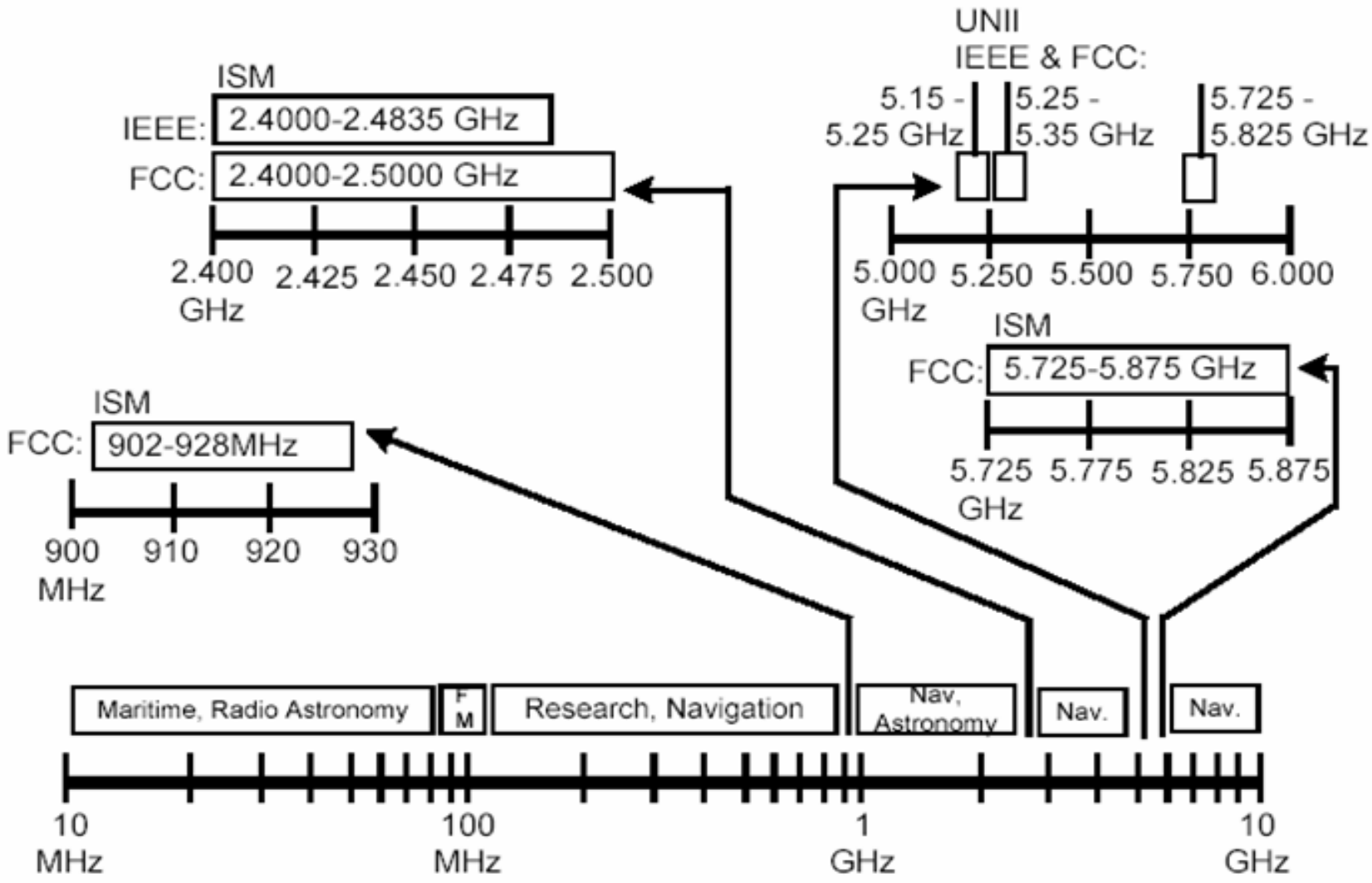
Wi-Fi Technology Overview: Standards

- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003) **Withdrawn February 2006**
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved and will not be used)

Wi-Fi Technology Overview: Standards

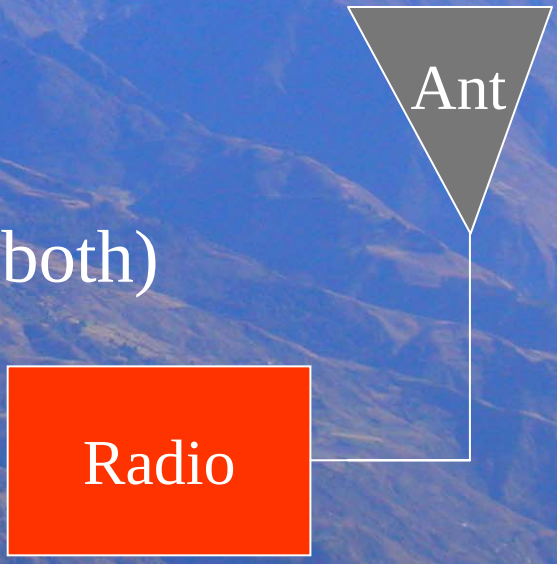
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved and will not be used)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved and will not be used, can be confused with 802.1Q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames
- IEEE 802.11x - (reserved and will not be used)
- IEEE 802.11y - 3650-3700 Operation in USA

ISM and UNII Spectra

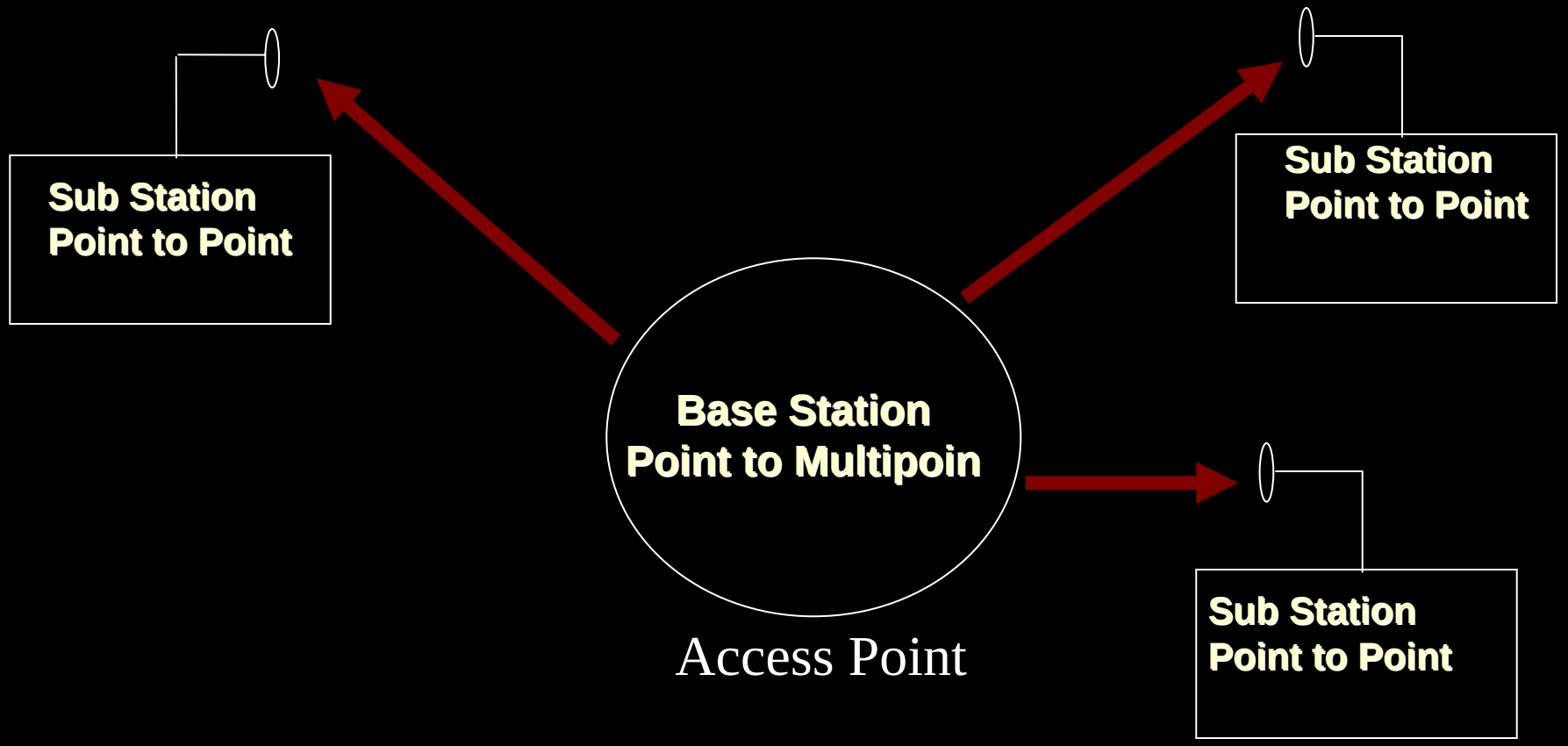


Elements of a Transmission System

- Antennas
- Connecting cable or waveguide
- Radio (Transmitter, Receiver or both)
- Power Supply, Grounding and Lightning Protection



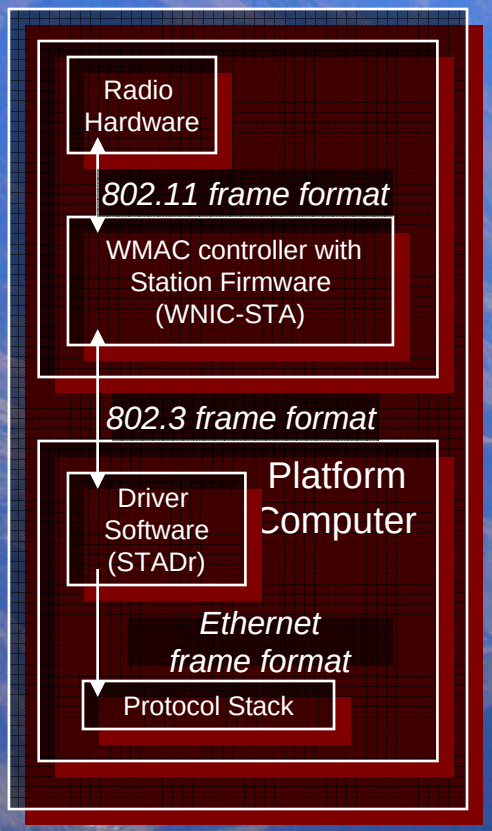
System Configuration



IEEE 802 .11 Terminology

Station (STA) Architecture:

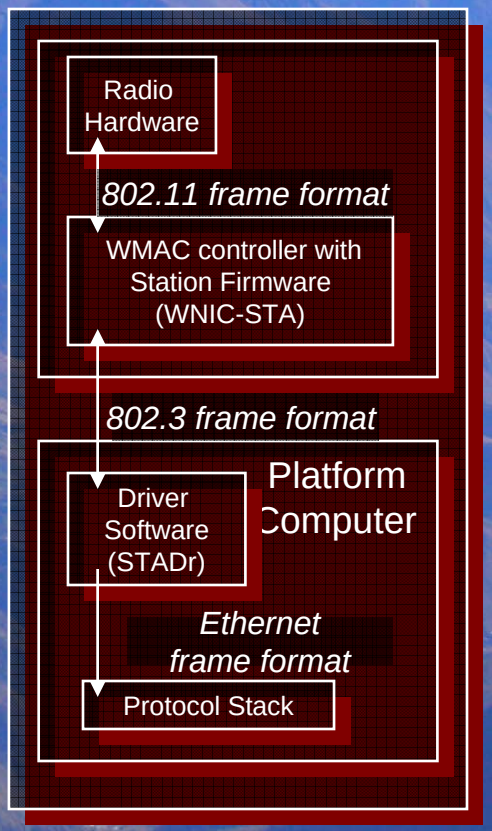
- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system
- Most often end-stations available in terminals (work-stations, laptops etc.)



IEEE 802 .11 Terminology

Access-Point (AP) Architecture:

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations
- Most often infra-structure products that connect to wired backbones

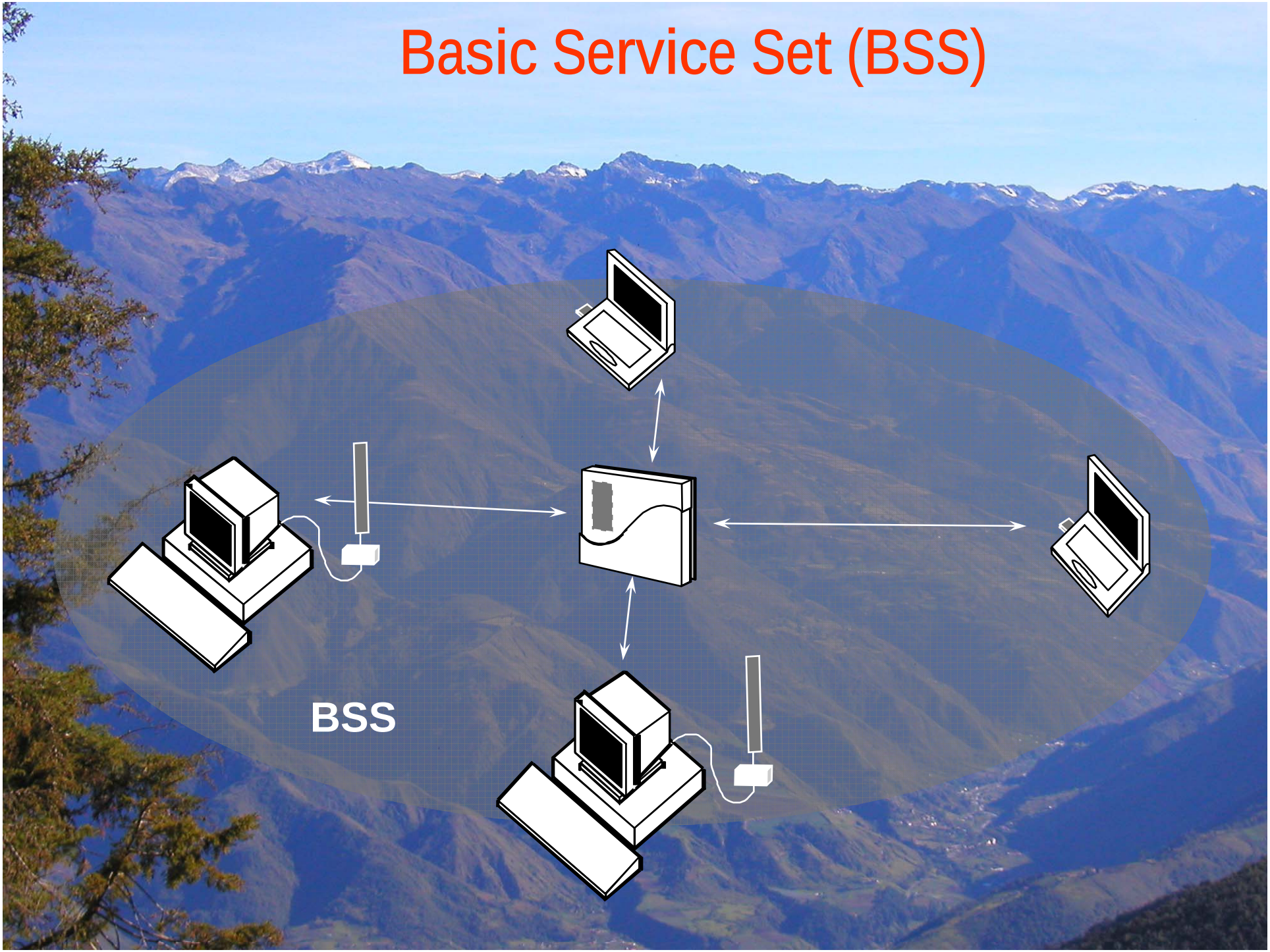


IEEE 802 .11 Terminology

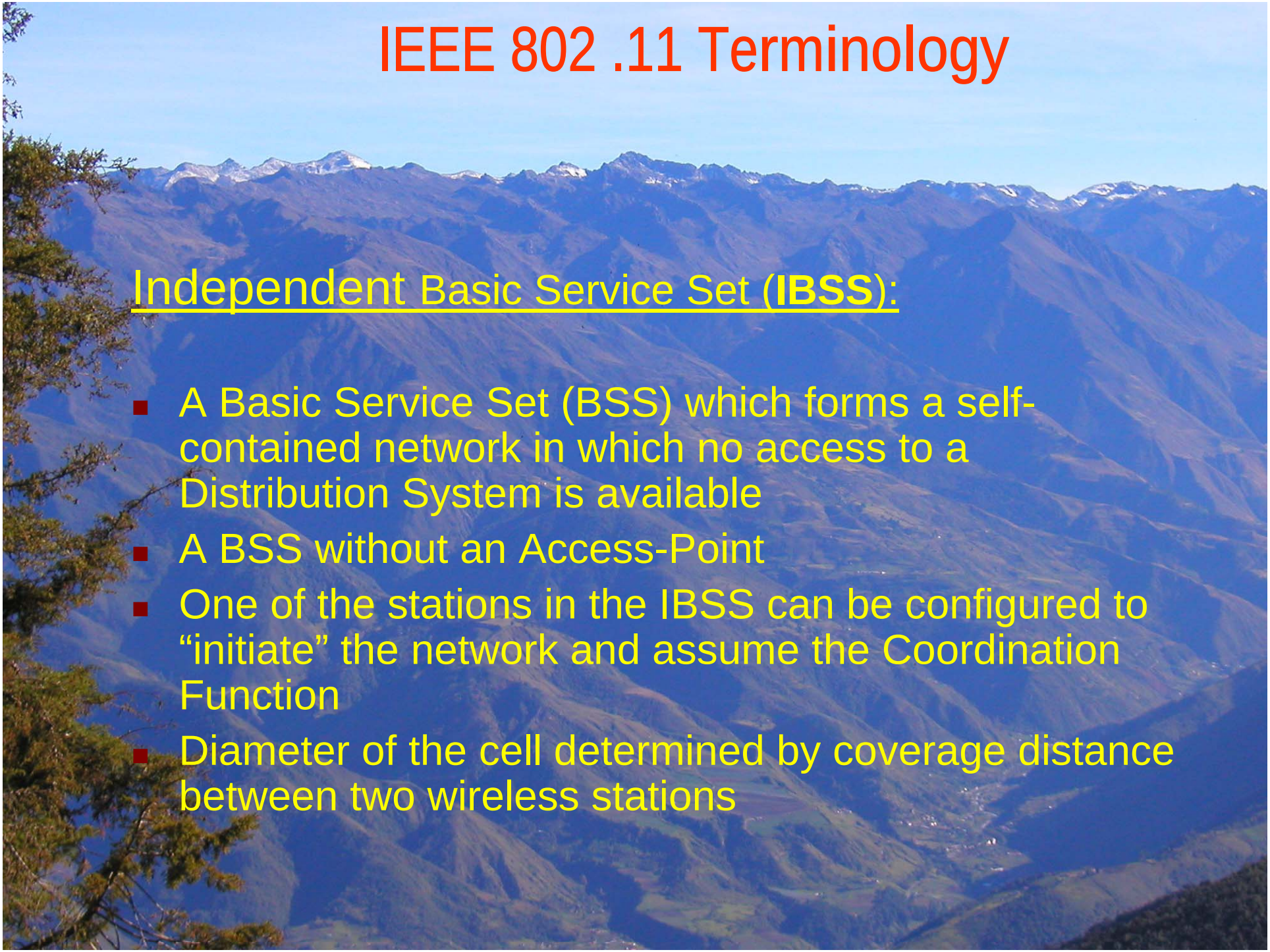
BSS

- A set of stations controlled by a single "Coordination Function" (the logical function that determines when a station can transmit or receive)
- Similar to a "cell" in mobile phone terminology
- A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only)
- Diameter of the cell is app. twice the coverage-distance between two wireless stations

Basic Service Set (BSS)



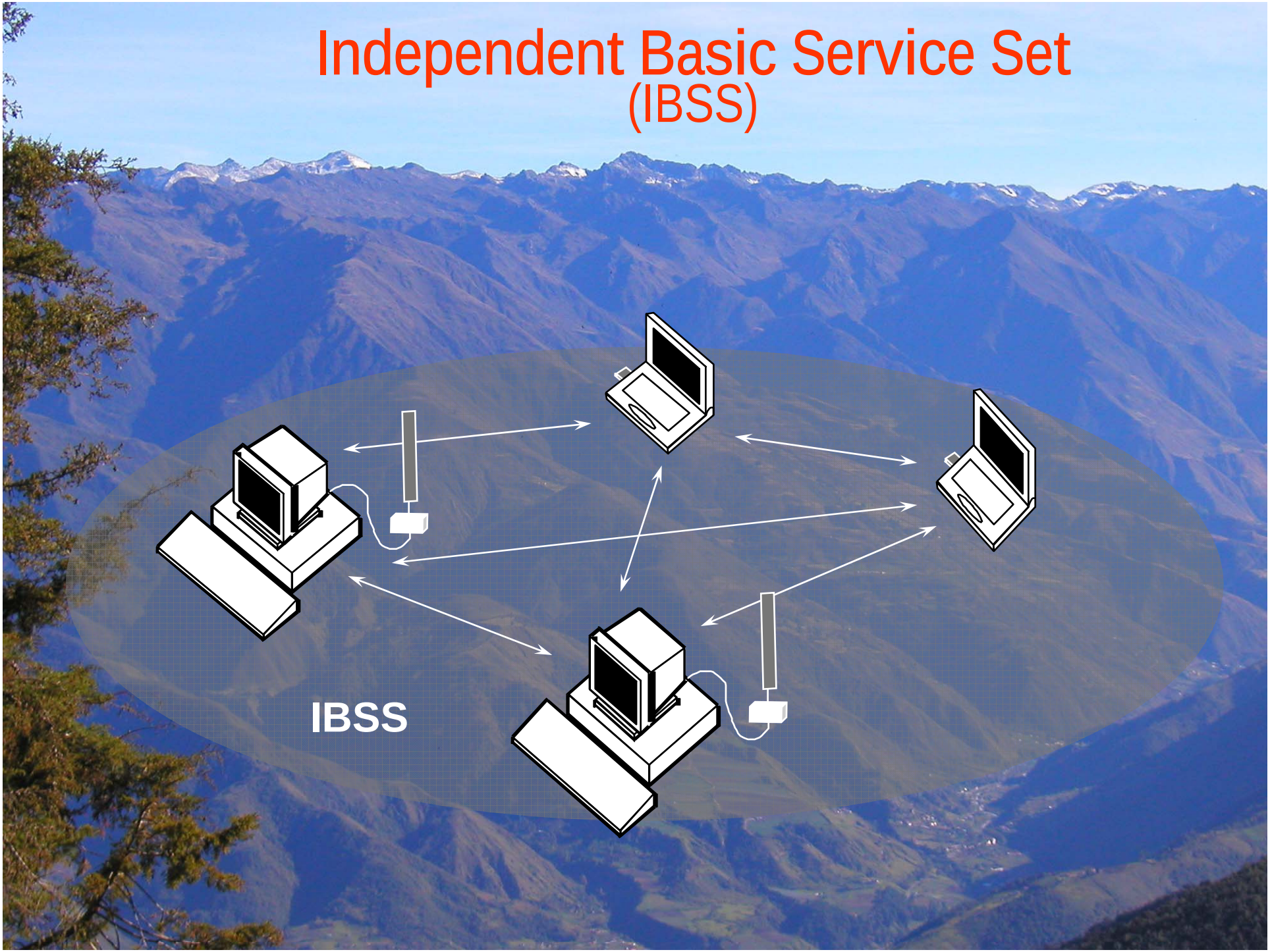
IEEE 802 .11 Terminology



Independent Basic Service Set (**IBSS**):

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function
- Diameter of the cell determined by coverage distance between two wireless stations

Independent Basic Service Set (IBSS)



IEEE 802 .11 Terminology

Extended Service Set (**ESS**):

- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access Point

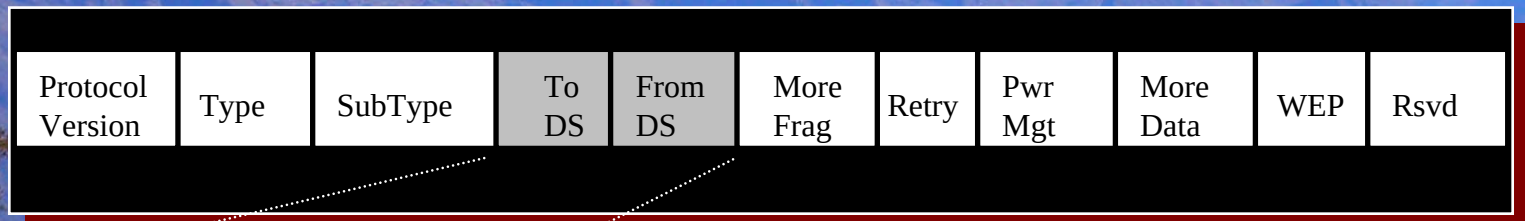
Distribution System (**DS**):

- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access Point in a standalone network
  - Wired; Using cable to interconnect the Access Points
  - Wireless; Using wireless to interconnect the Access Points

Wireless Distribution System

- In IEEE 802.11, **WDS** means
  - Multiple wireless “ports” inside the access-point, to wirelessly interconnect cells (access-points connecting to other access-points)
  - One wireless backbone extension can be made (using two radio modules in the access-point)
- WDS allows:
  - Extending the existing infrastructure with wireless backbone links
  - Totally wireless system without any wired backbones

Address Field Description



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

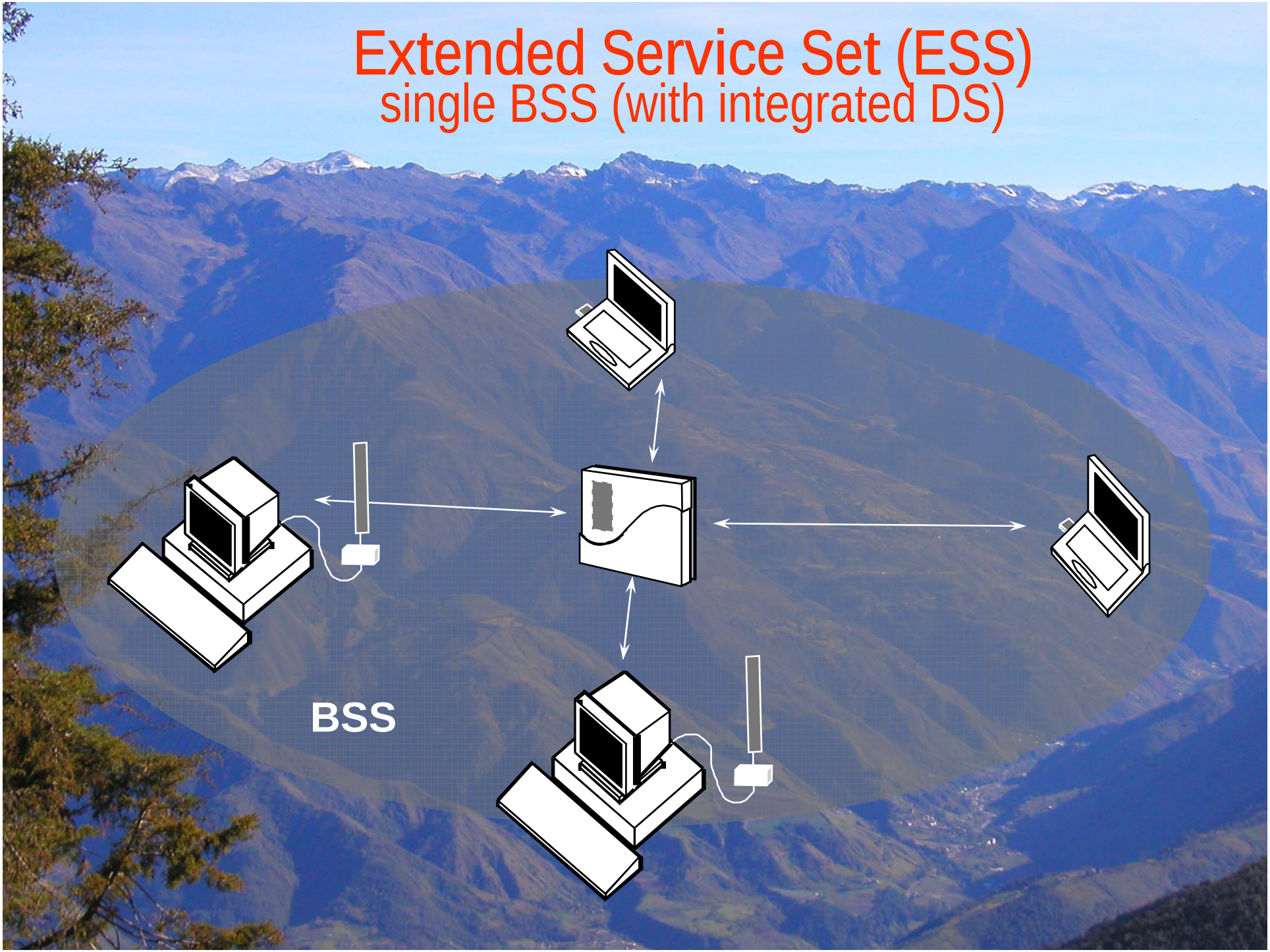
Addr. 1 = All stations filter on this address.

Addr. 2 = Transmitter Address (TA), Identifies transmitter to address the ACK frame to.

Addr. 3 = Dependent on *To* and *From DS* bits.

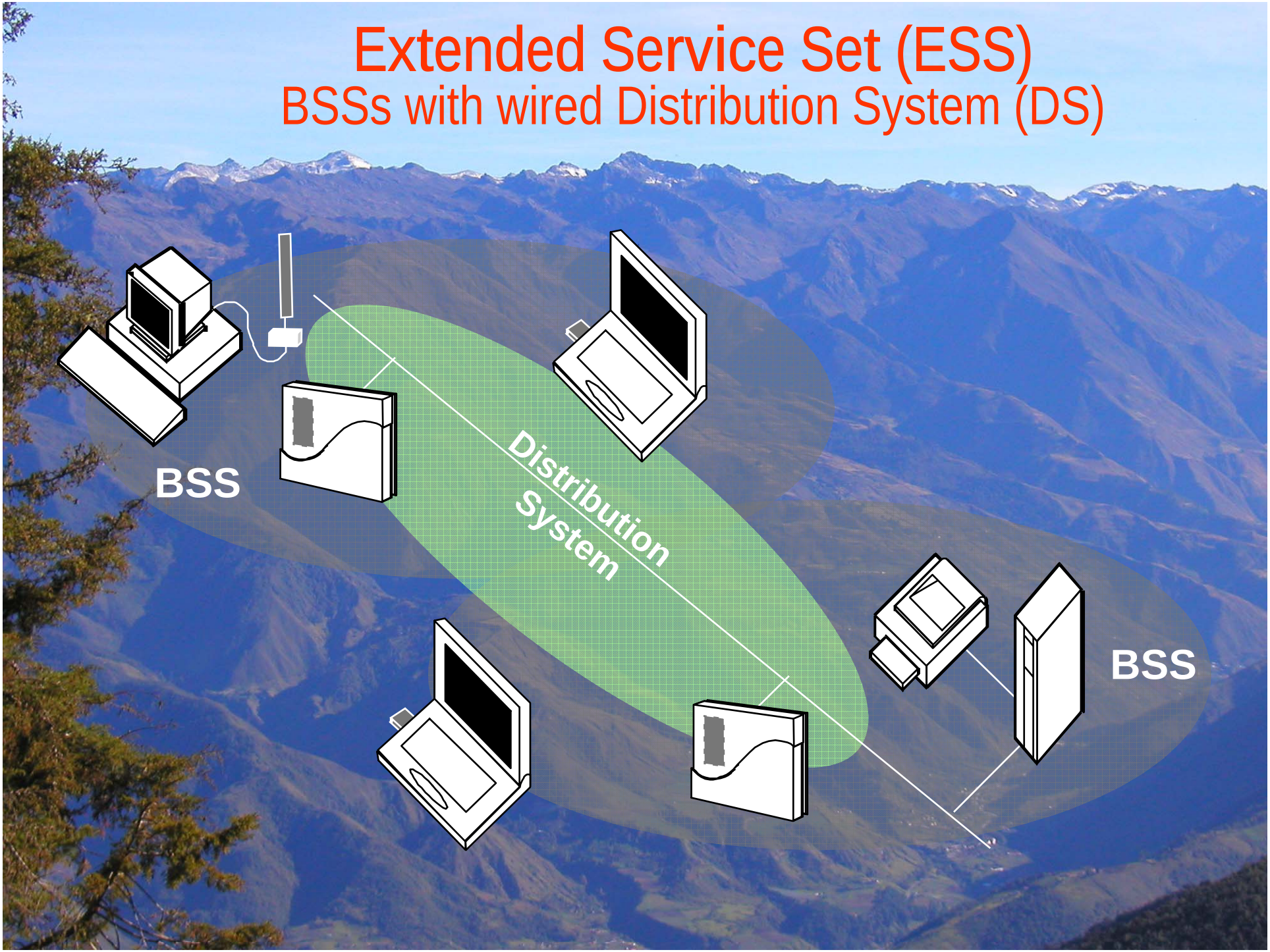
Addr. 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames

Extended Service Set (ESS)
single BSS (with integrated DS)



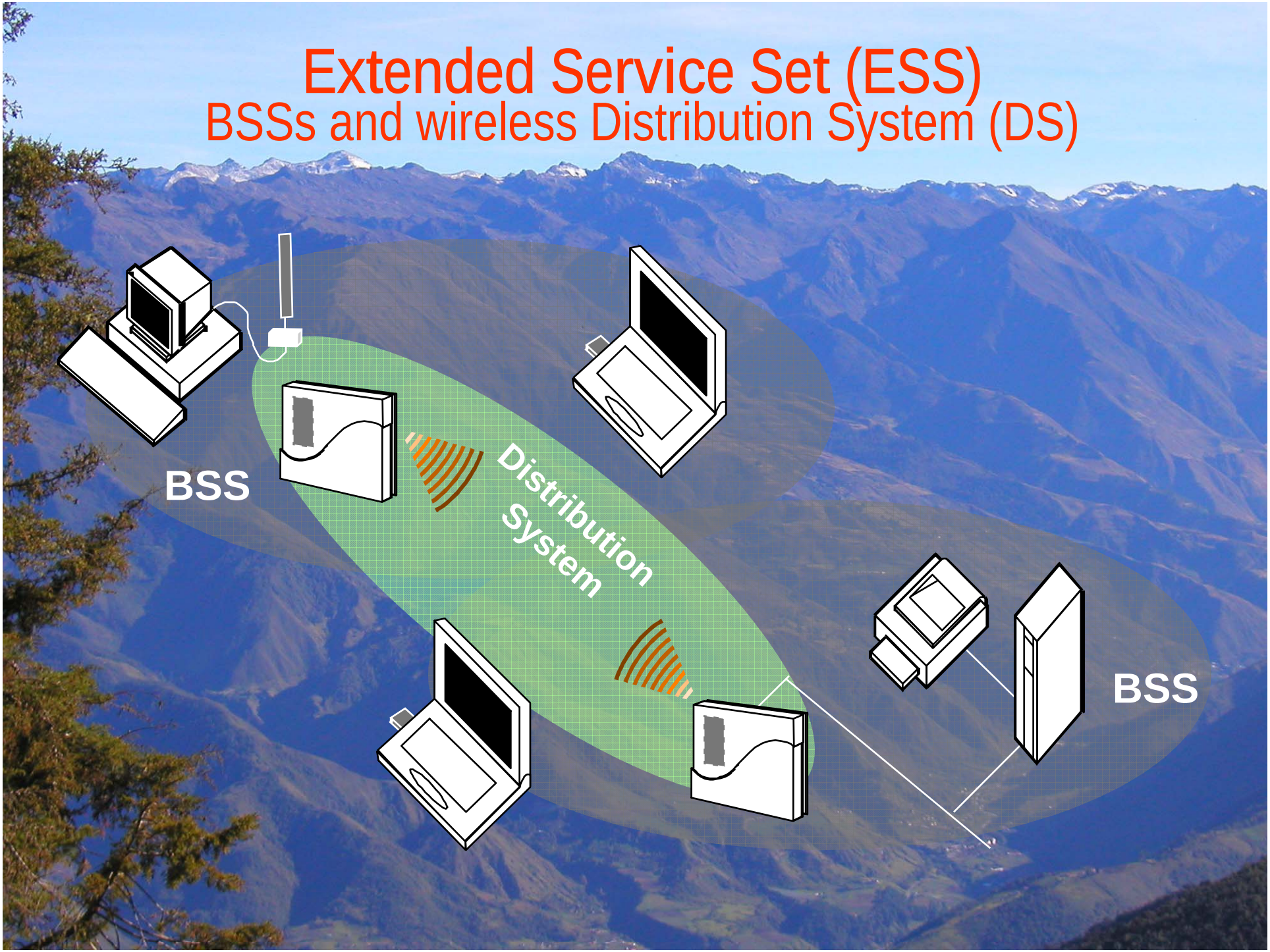
Extended Service Set (ESS)

BSSs with wired Distribution System (DS)

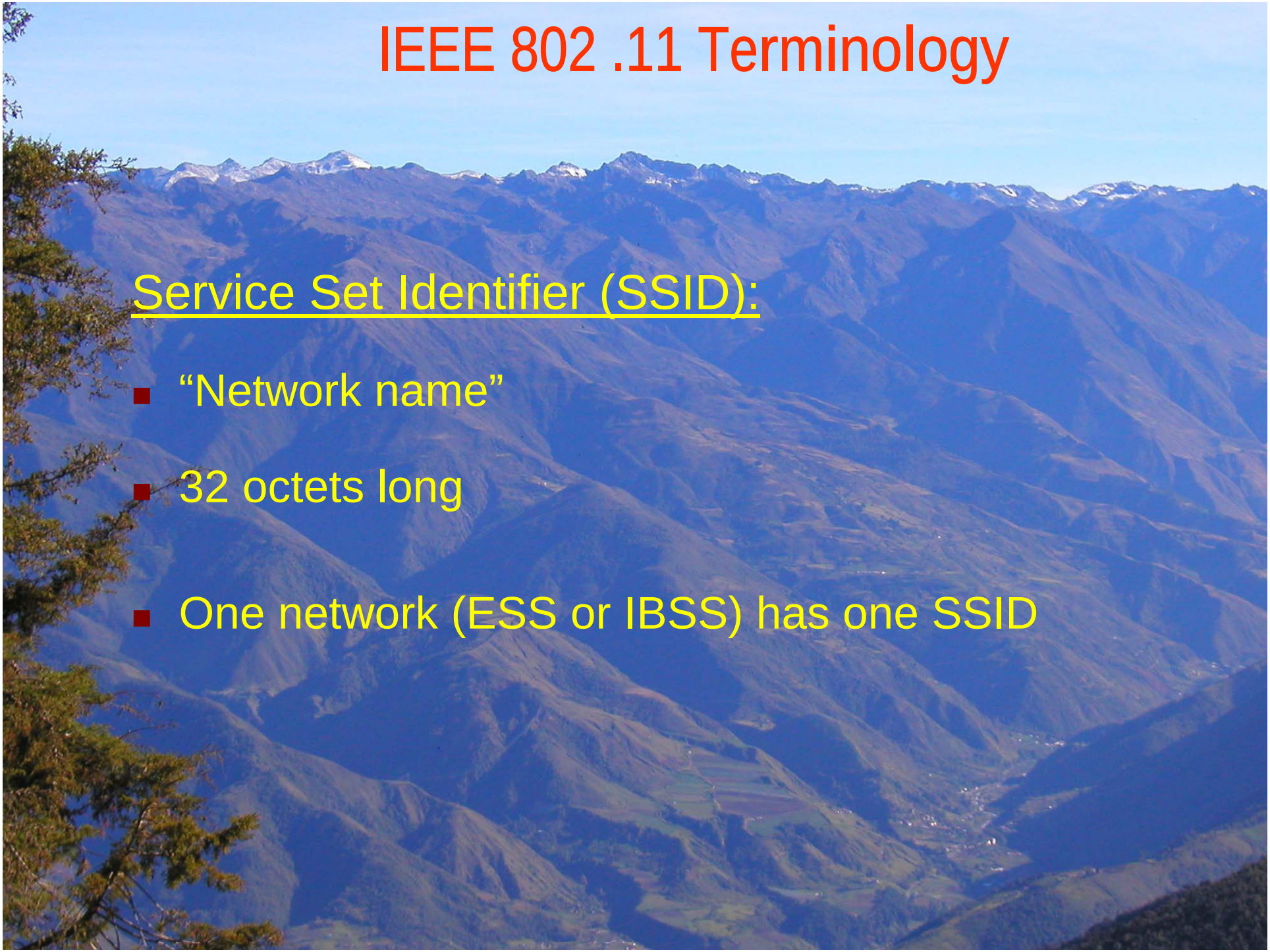


Extended Service Set (ESS)

BSSs and wireless Distribution System (DS)



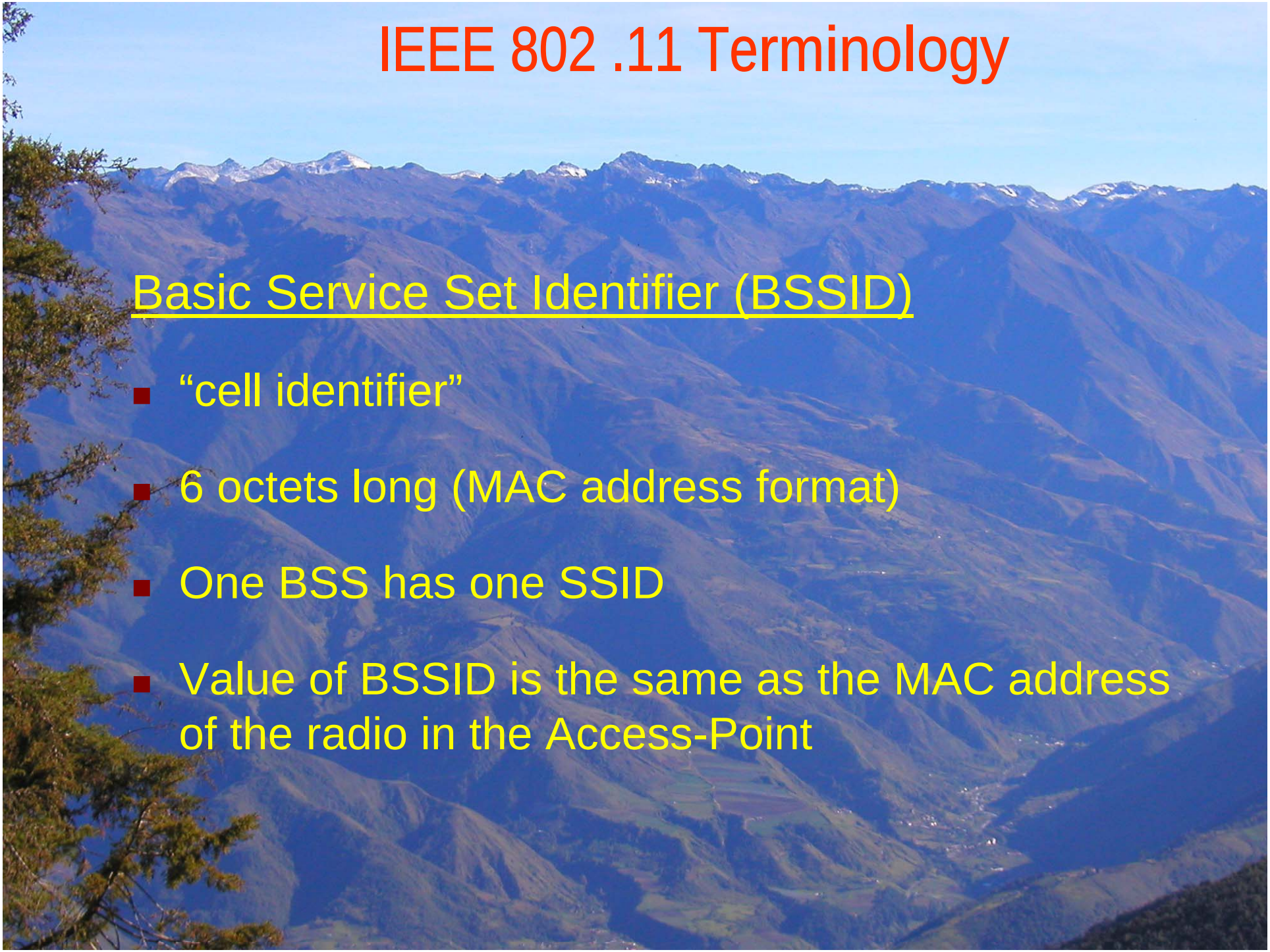
IEEE 802 .11 Terminology



Service Set Identifier (SSID):

- "Network name"
- 32 octets long
- One network (ESS or IBSS) has one SSID

IEEE 802 .11 Terminology



Basic Service Set Identifier (BSSID)

- "cell identifier"
- 6 octets long (MAC address format)
- One BSS has one SSID
- Value of BSSID is the same as the MAC address of the radio in the Access-Point

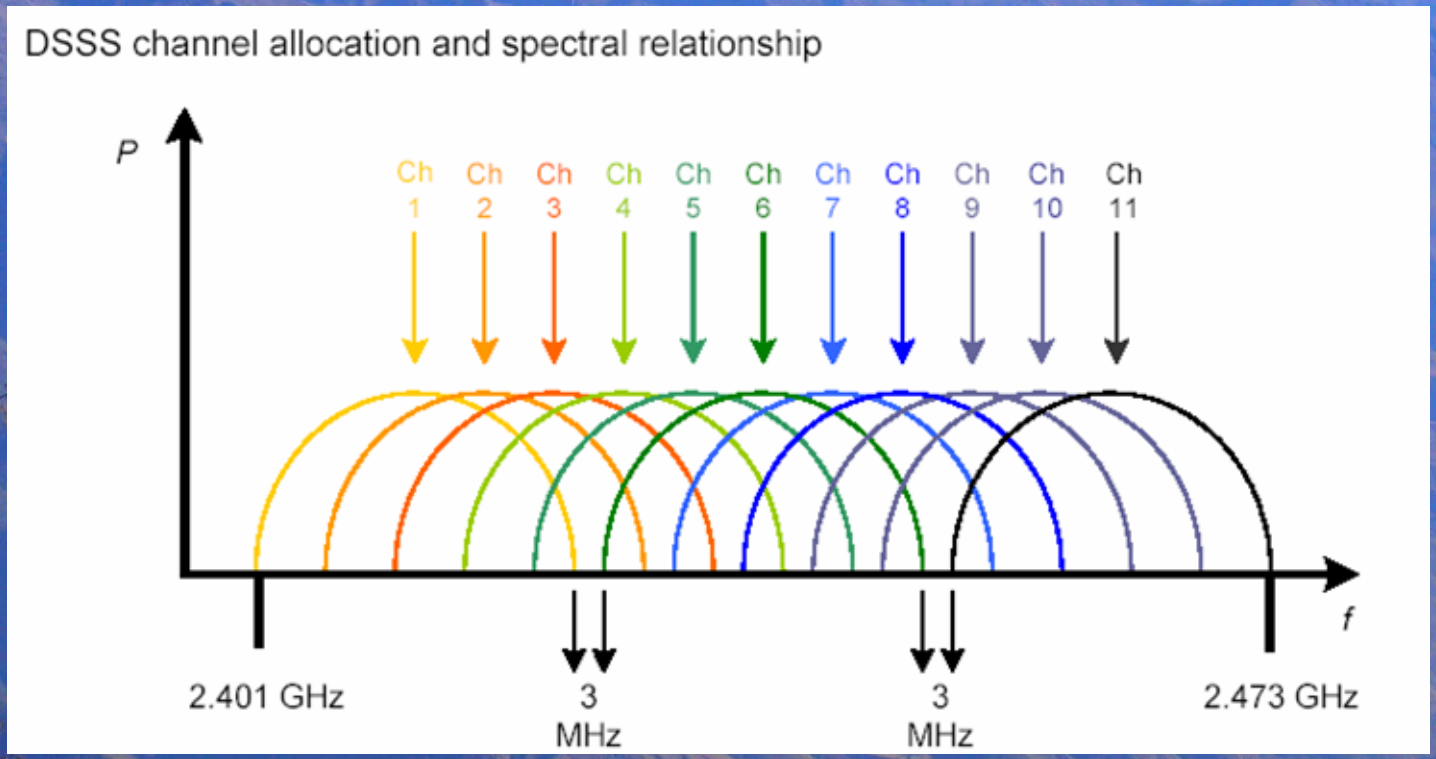
MAC Management Frames

- **Beacon**
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - Traffic Indication Map
- **Probe**
  - SSID, Capabilities, Supported Rates
- **Probe Response**
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - same for Beacon except for TIM

MAC Management Frames (cont'd)

- **Association Request**
  - Capability, Listen Interval, SSID, Supported Rates
- **Association Response**
  - Capability, Status Code, Station ID, Supported Rates
- **Re-association Request**
  - Capability, Listen Interval, SSID, Supported Rates, Current AP Address
- **Re-association Response**
  - Capability, Status Code, Station ID, Supported Rates

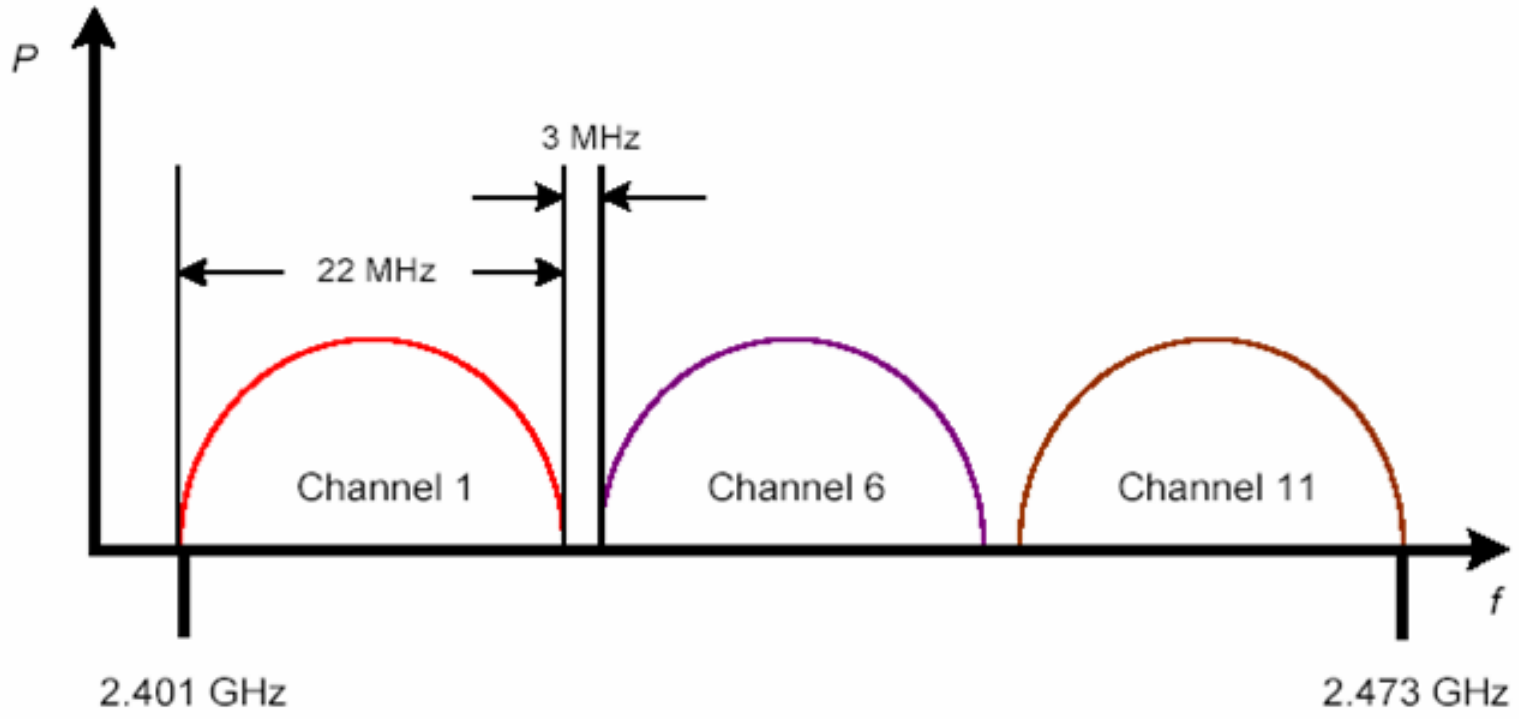
Channel Overlapping



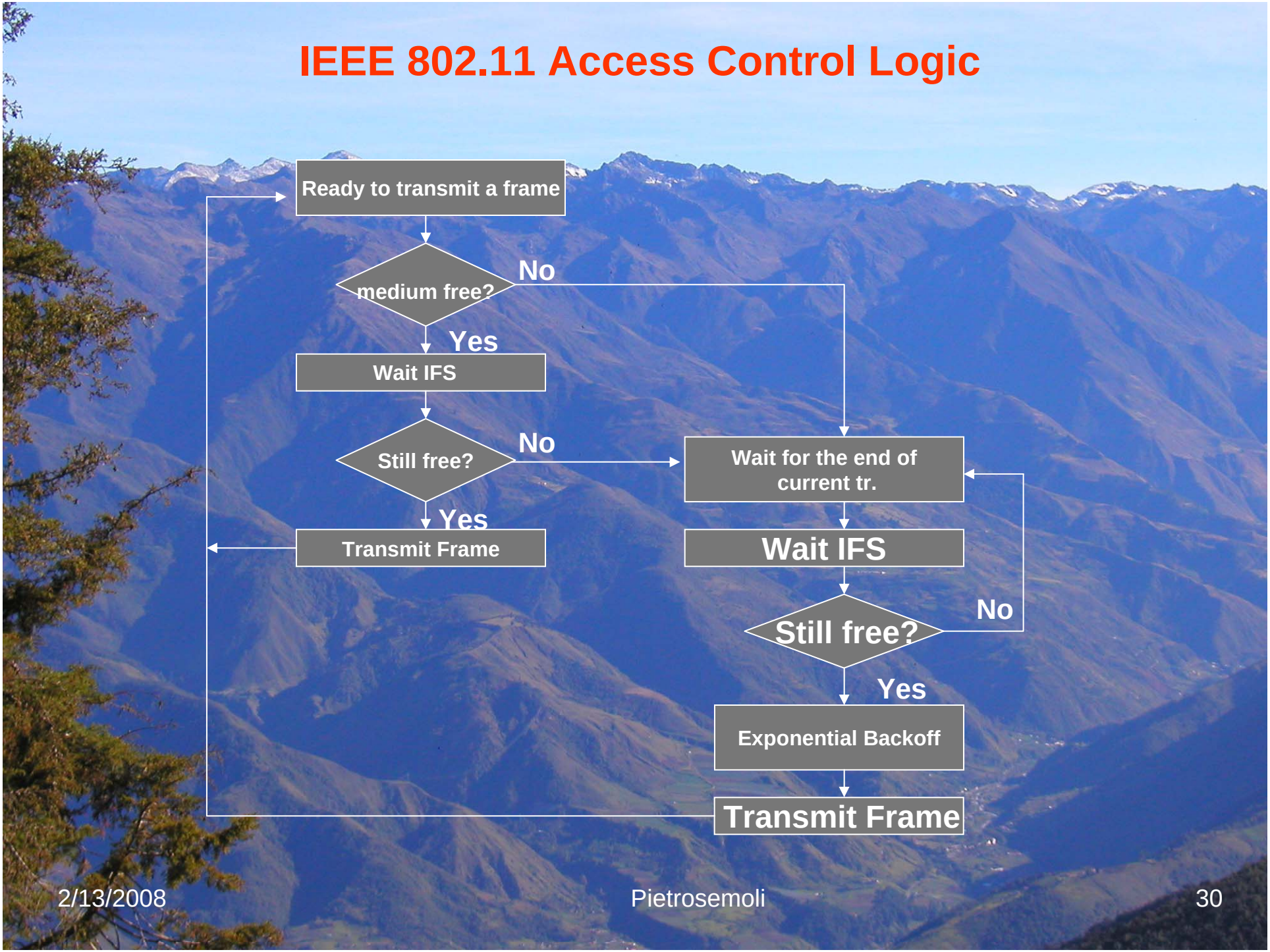
Some Channels Assignments

Channel ID	FCC (worldcard)	ETSI	France	Japan
1	2412	2412	-	2412
2	2417	2417	-	2417
3	2422	2422	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11	2462	2462	2462	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14	-	-	-	2484

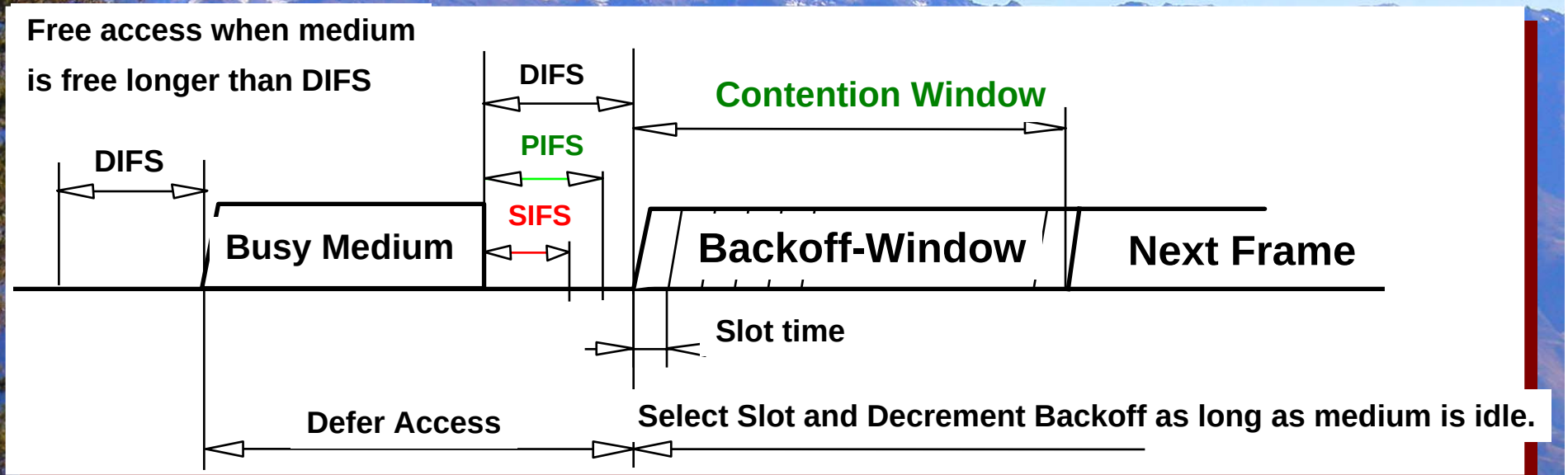
DSSS non-overlapping channels



IEEE 802.11 Access Control Logic

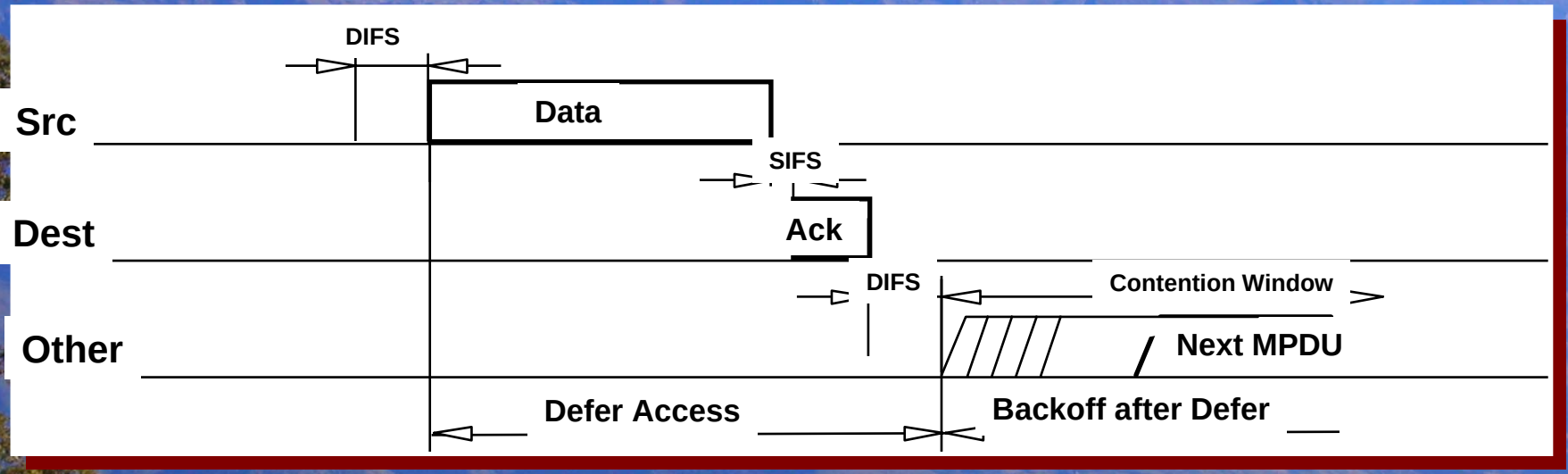


Operational processes
Inter-Frame Spacing



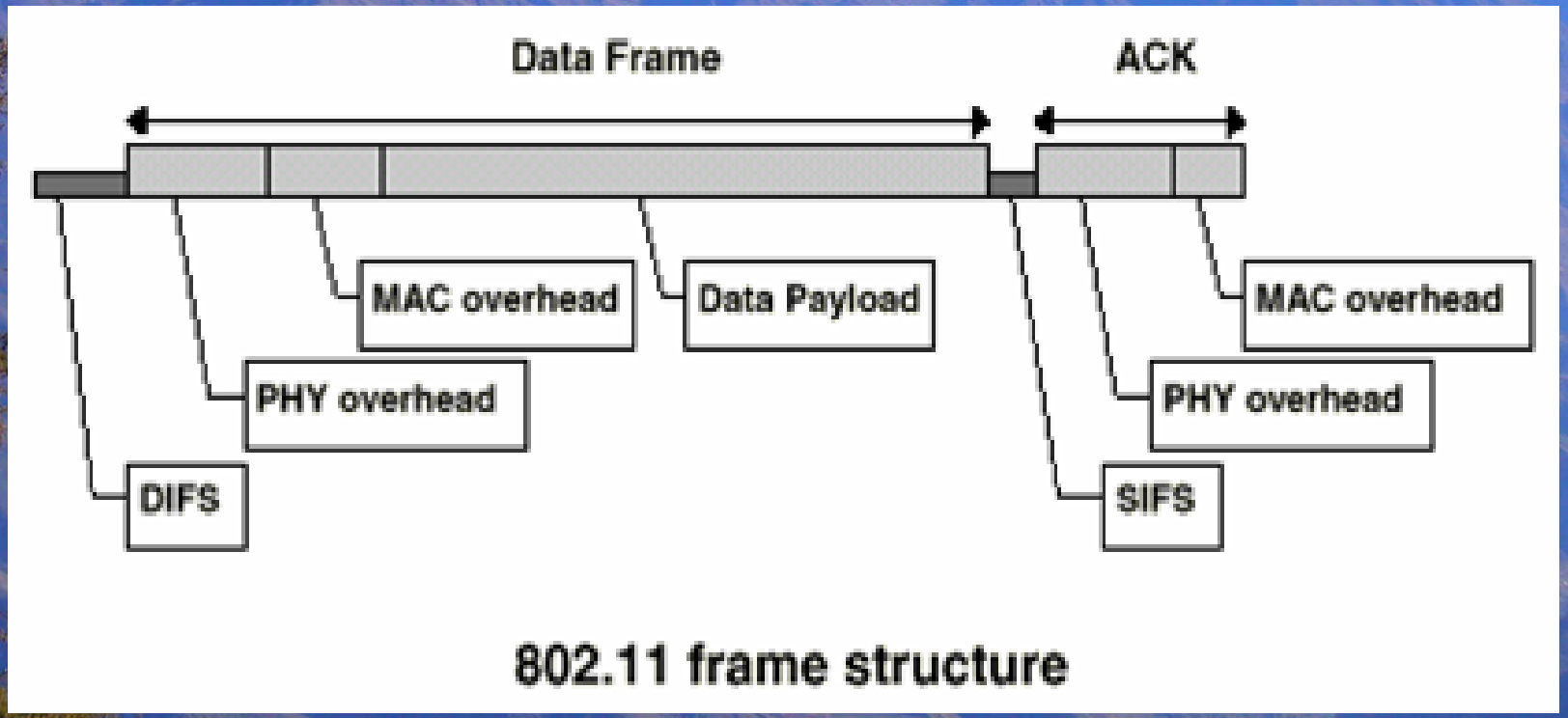
- Inter frame spacing required for MAC protocol traffic
  - **SIFS** = Short interframe space
  - **PIFS** = **PCF** slots
  - interframe space
  - **DIFS** = **DCF** interframe space
- Back-off timer expressed in terms of number of time slots

Operational processes
Data Frames and their ACK



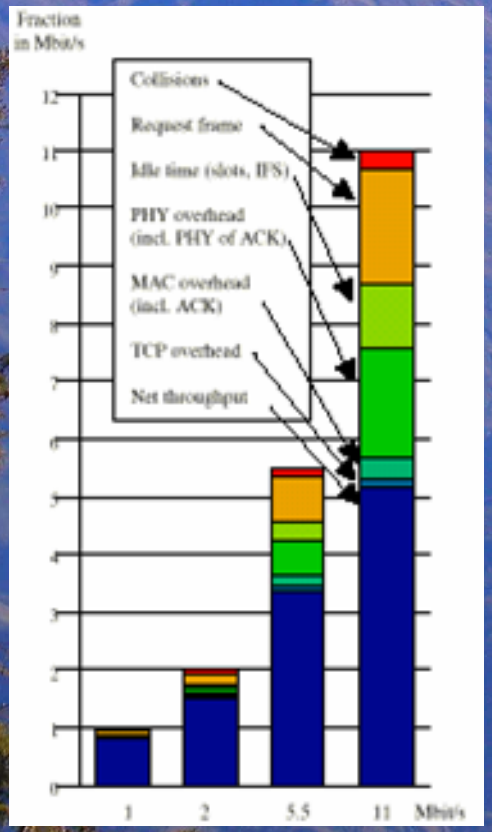
- Acknowledgment are to arrive within the SIFS
- The DCF interframe space is observed before medium is considered free for use

Throughput
Impact of IEEE 802.11 MAC



802.11 frame structure

Throughput
Impact of IEEE 802.11 MAC



IEEE 802.11b, 802.11a AND 802.3 FRAME STRUCTURE AND OVERHEAD RELATED PARAMETERS

	802.11b	802.11a	802.3
Bit rates	1, 2, 5.5, 11 Mbit/s	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	10, 100 Mbit/s (1000 Mbit/s is not shown)
DIFS	50 µs	25 µs	IFS 9.6 µs, 0.96 µs
Slot time	20 µs	6 µs	51.2 µs , 5.12 µs
Preamble and PHY header	192 µs	10, 7, 6, 5, 4, 3, 3, 3 µs	6.4 µs, 0.64 µs
MAC overhead	34 byte	34 byte	18 byte
Payload data	46 – 1500 byte (0 – 2312 byte without 802.3 infrastructure)	46 – 1500 byte (0 – 2312 byte without 802.3 infrastructure)	46 – 1500 byte
Short IFS	10 µs	13 µs	N.A.
Preamble and PHY header	192 µs	10, 7, 6, 5, 4, 3, 3, 3 µs	N.A.
MAC overhead per ACK	14 byte	14 byte	N.A.

Channel Reservation

Sending Client

Access Point

Receiving Client

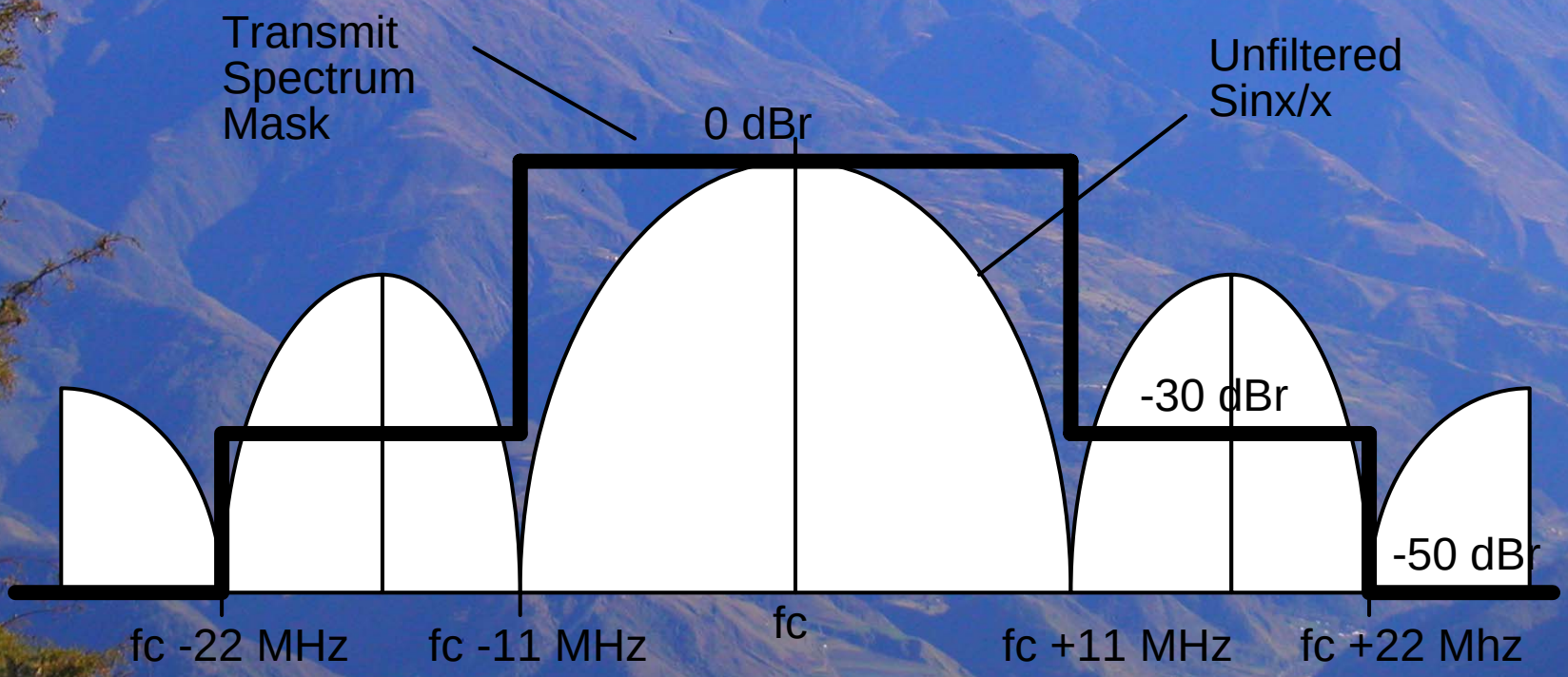
Request to send (RTS)

data

Clear to send (CTS)

Acknowledgment (ACK)

802.11b spectral mask

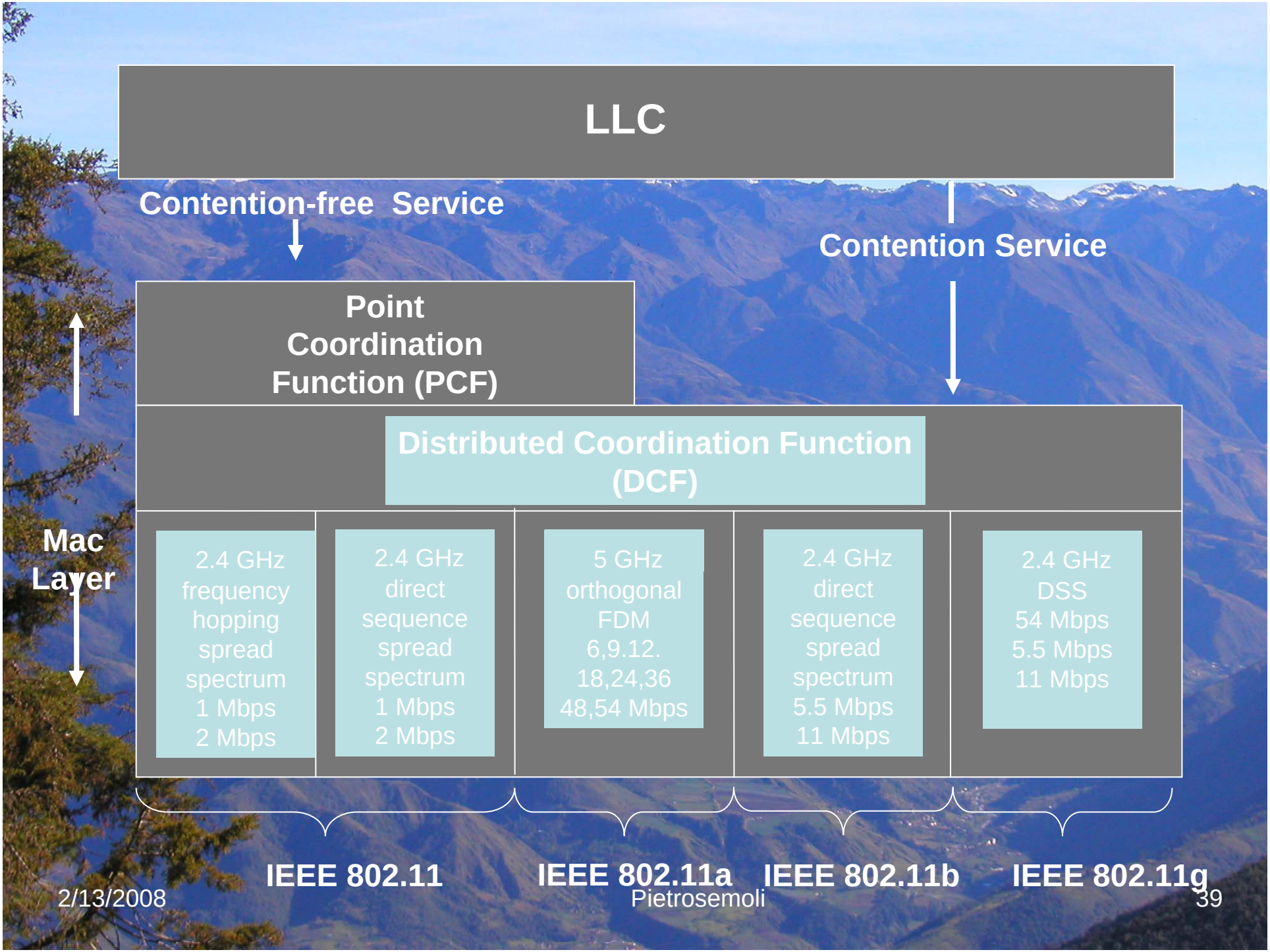


Control Frames

- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgement (ACK)
- Power-Save Poll (PS Poll)
- Contention-Free End (CF End)
- CF End + CF Ack

Management Frames

- Association request frame
- Association response frame
- Reassociation request frame
- Reassociation response frame
- Probe request frame
- Probe response frame
- Beacon frame
- ATIM frame
- Disassociation frame
- Authentication frame
- Deauthentication frame


LLC
Contention-free Service
Contention Service
Point Coordination Function (PCF)
Distributed Coordination Function (DCF)
Mac Layer
2.4 GHz frequency hopping spread spectrum 1 Mbps 2 Mbps
2.4 GHz direct sequence spread spectrum 1 Mbps 2 Mbps
5 GHz orthogonal FDM 6,9.12. 18,24,36 48,54 Mbps
2.4 GHz direct sequence spread spectrum 5.5 Mbps 11 Mbps
2.4 GHz DSS 54 Mbps 5.5 Mbps 11 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

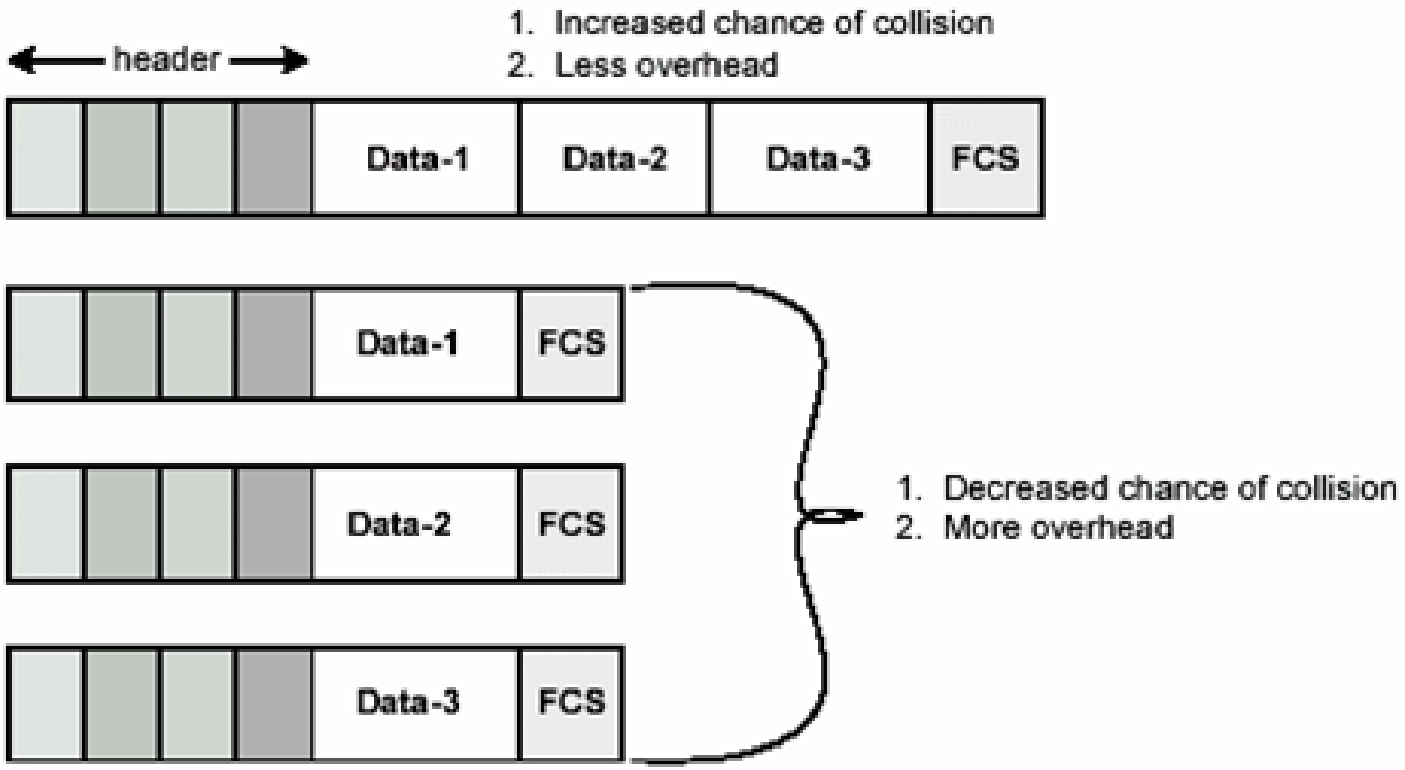
Frames spacing intervals for DSSS

Short Interframe Spacing (SIFS) 10 μs

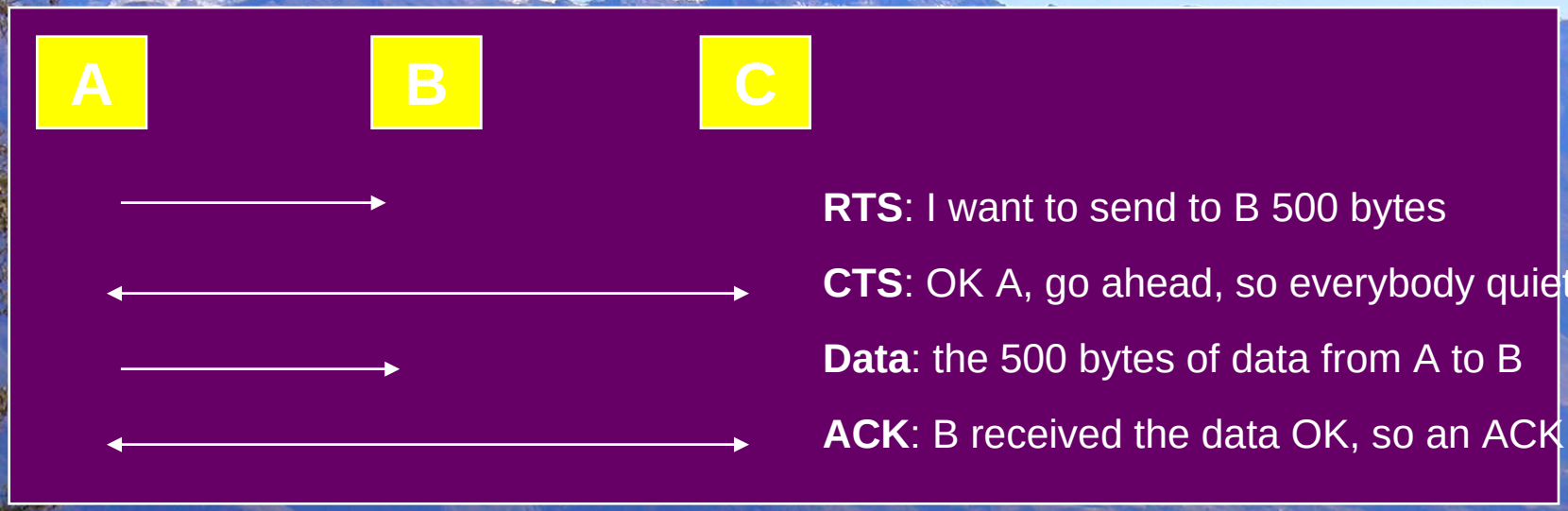
Point Coordination Function Interframe Space (PIFS) 30 μs

Distributed Coordination Function Interframe Space (DIFS) 50 μs

Fragmentation

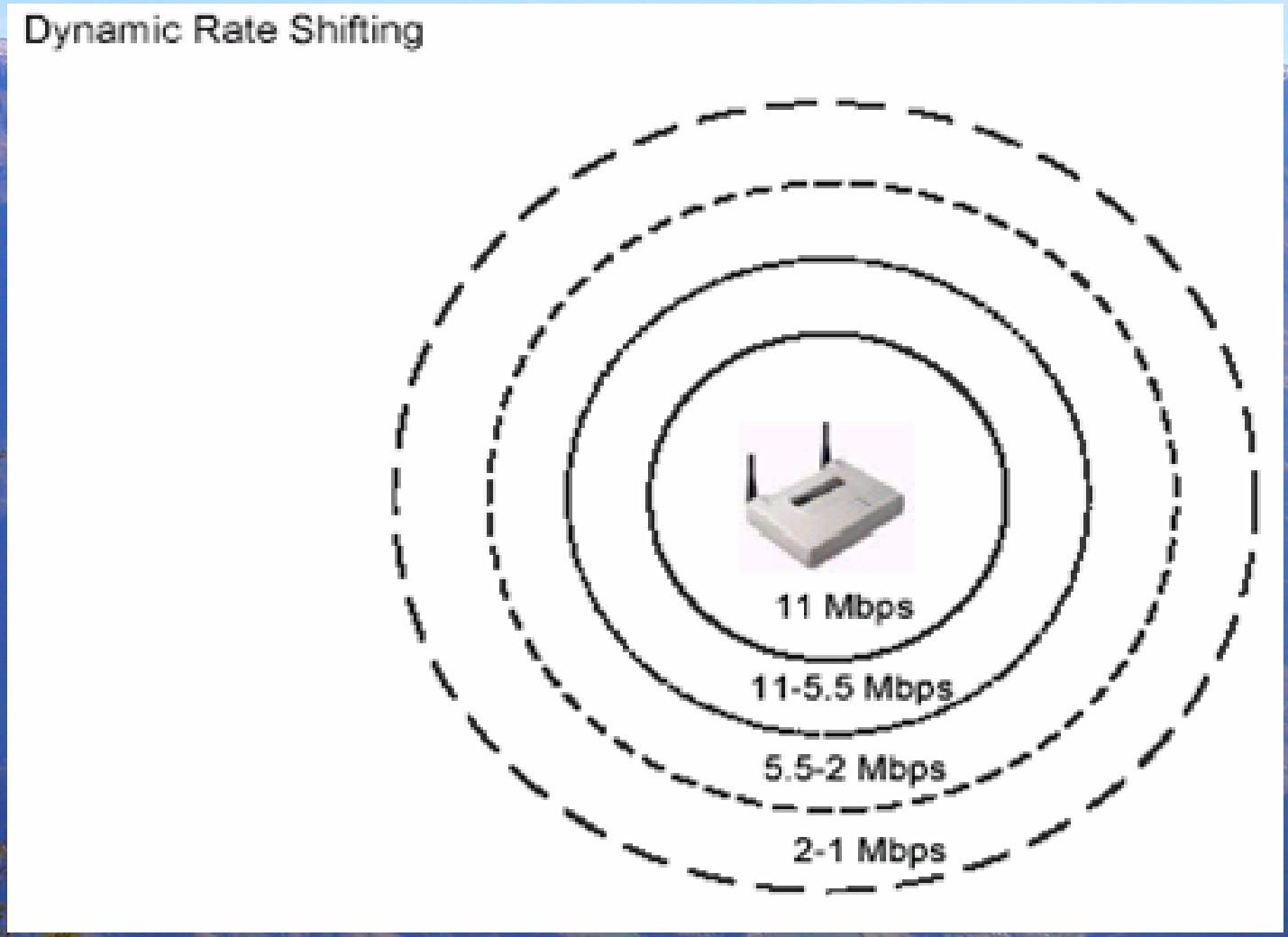


“Hidden stations”



- MAC level RTS/CTS protocol (Request to Send / Clear to Send)
- Can be switched off to reduce overhead (when no hidden nodes exist)
- More robustness, and increased reliability
- No interruptions when large files are transmitted

Dynamic transmission rate



Similar behaviour for the 54 Mbps rate adaption

Traffic Indication Map (TIM)

The TIM is used an as indicator of which sleeping stations have packets queued at the access point. This information is passed in each beacon to all associated stations. While sleeping, synchronized stations power up their receivers, listen for the beacon, check the TIM to see if they are listed, then, if they are not listed, they power down their receivers and continue sleeping.

.

Operational processes
Association

- To establish relationship with Access Point
- Stations scan frequency band to and select Access Point with best communications quality
  - Active Scan (sending a “Probe request” on specific channels and assess response)
  - Passive Scan (assessing communications quality from beacon message)
- Access Point maintains list of associate stations in MAC FW
  - Record station capability (data-rate)
  - To allow inter-BSS relay
- Station’s MAC address is also maintained in bridge learn table associated with the port it is located on

Operational processes
Authentication

- To control access to the infrastructure via an authentication
- Stations identify themselves to other stations (or Access-Points) prior to data traffic or association
- Open System Authentication
  - Uses null authentication algorithm
  - Default
- Shared Key Authentication
  - Uses WEP privacy algorithm
  - Optional

Configuration Parameters
Basic parameters (Station)

Network Name (SSID)

- ASCII string to identify the network that the station wants to connect to.

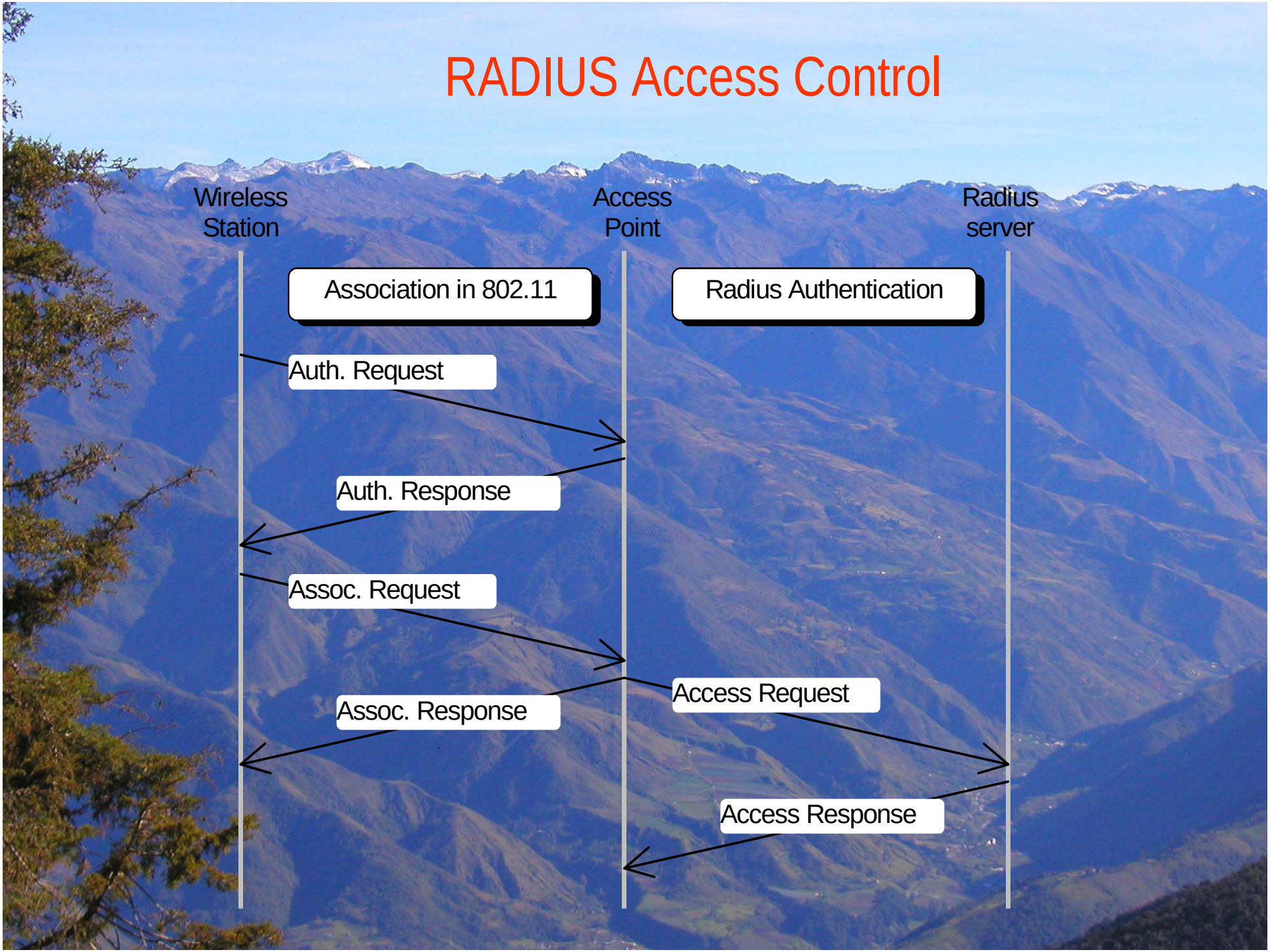
Station Name (SSID)

- ASCII string to provide a user friendly station identification, when used in diagnostic purposes (in Windows systems: equal to “computer name”)

Type of Operation

- To identify the kind of network that the station will be part of
  - Network centered around APs
  - IBSS (peer-to-peer network)

RADIUS Access Control



Configuration Parameters
Basic parameters (AP)

Network Name (SSID)

- ASCII string to identify the network that the Access Point is part of. Only available in “Access Point” mode.

Frequency (channel)

- To indicate the frequency channel that the AP will use for its “cell”. The channel is selected from the set that is allowed in the regulatory domain.

Configuration Parameters
Advanced parameters (AP)

Microwave Oven Robustness

- Check box to enable/disable data-rate fallback delay-mechanism to allow improved performance in presence of microwave ovens

DTIM

- Power Management related parameter to specify the timing of the delivery of multicast traffic to stations that have indicated to receive multicast messages while under power management.

  Example:

  - DTIM=1 means multicast traffic when it arrives at the AP is passed through after every beacon
  - DTIM=3 means multicast traffic is passed through after every 3rd beacon message

Configuration Parameters
Security parameters

Closed System (AP)

- To enable rejection of association requests from stations with *Network Name* set to “ANY”

Enable Encryption

- To enable/disable Encryption

Encryption keys

- Four fields to store up to four different encryption keys

Encryption key index

- Index identifying which of the four keys is the active one

Configuration Parameters
Advanced parameters

Medium Reservation

- To enable/disable the RTS/CTS handshake.
  - Threshold value 0-2346 (value=2347 disables Medium Reservation)

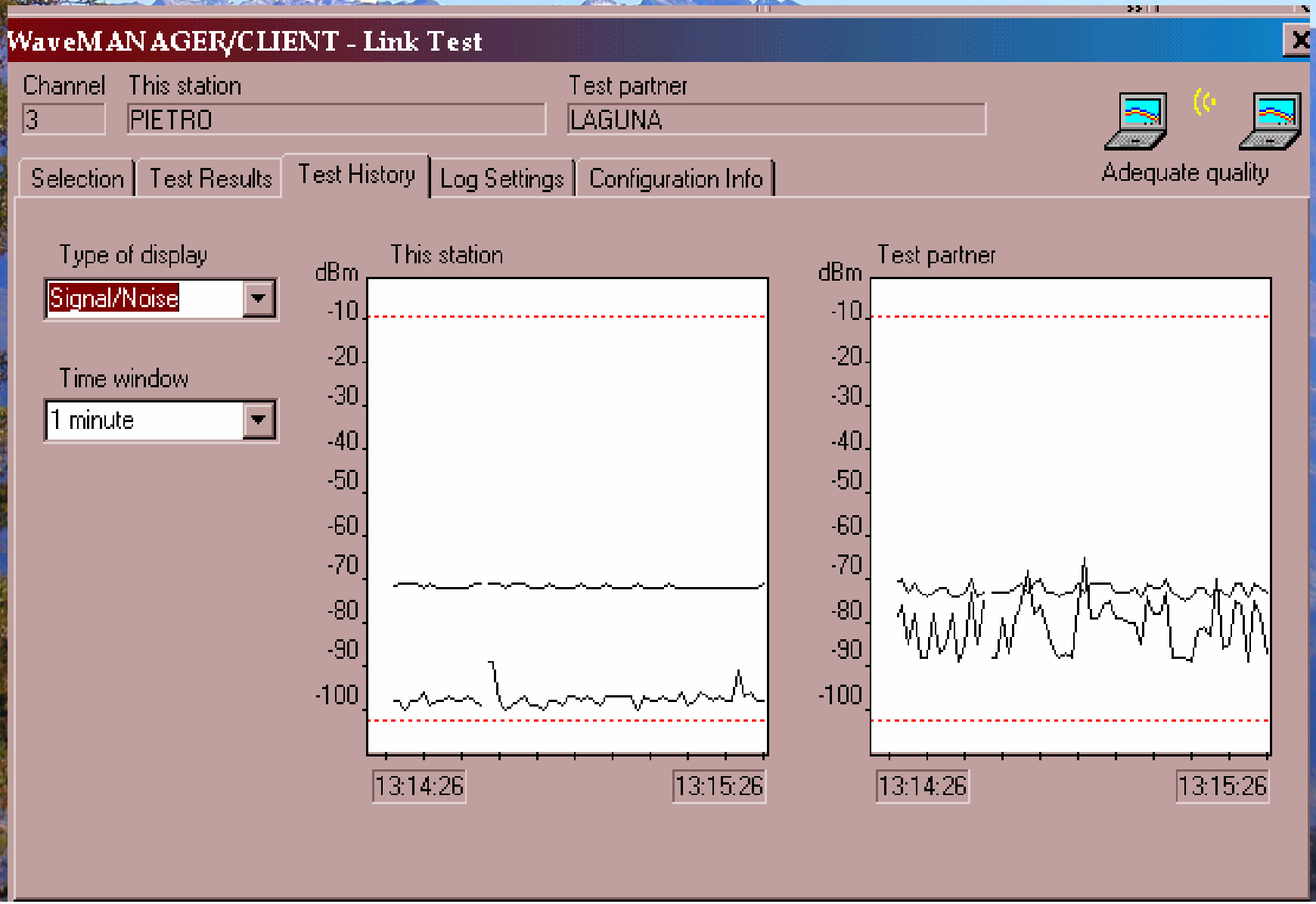
Distance between APs

- To specify the coverage of a “cell” in terms of the distance between the Access Points
  - Large
  - Medium
  - Small

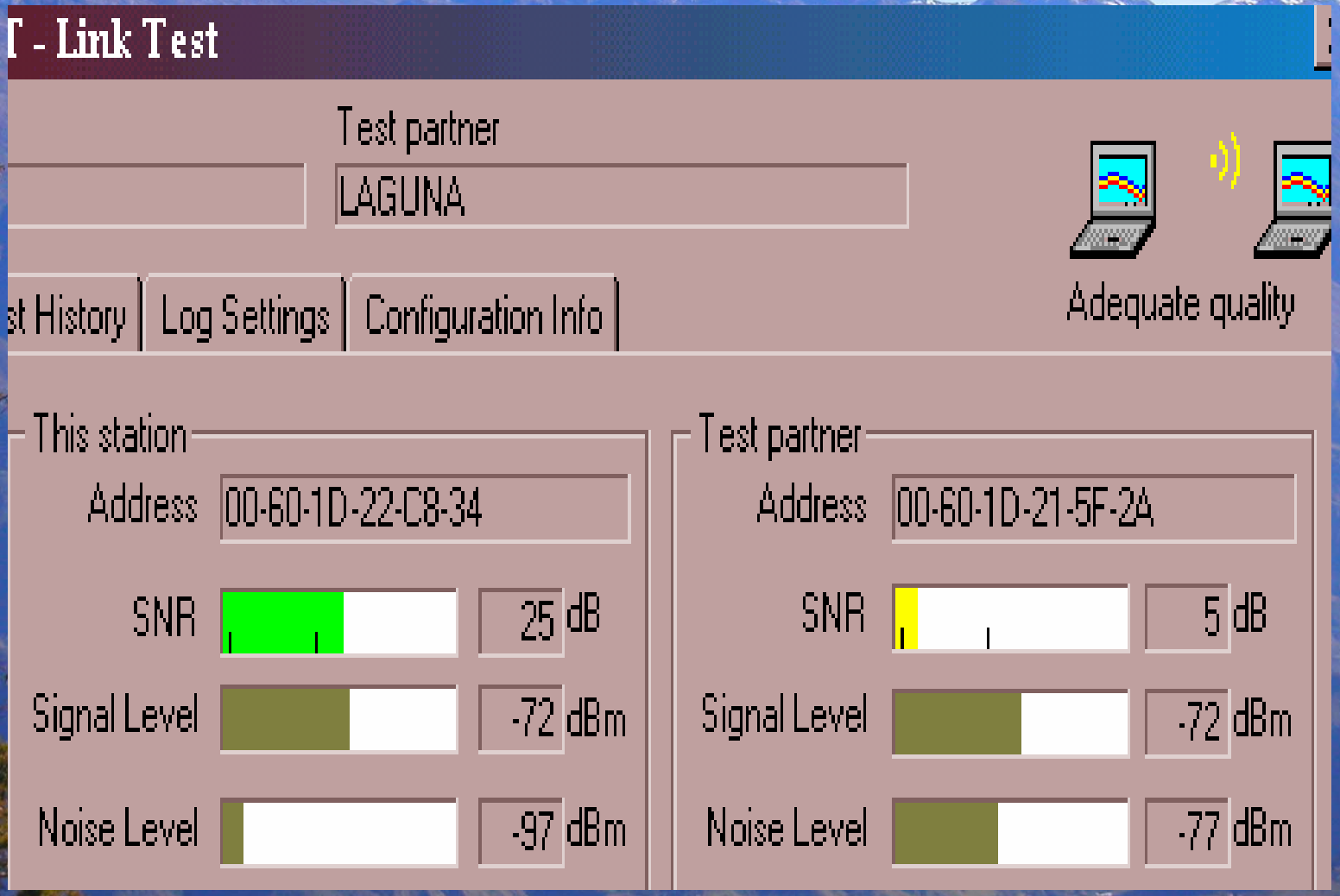
Multicast Rate

- To specify data-rate used for transmitting Multicast frames

Interference



Interference



Supported Channels for 802.11a

Channel ID	FCC	ETSI	Channel ID	FCC	ETSI
52	5.260	–	149	5.745	–
56	5.280	–	153	5.765	–
60	5.300	–	157	5.785	–
64	5.320	–	161	5.805	–
100	–	5.500	165	5.825	–
104	–	5.520			
108	–	5.540			
112	–	5.560			
116	–	5.580			
120	–	5.600			
124	–	5.620			
128	–	5.640			
132	–	5.660			
136	–	5.680			

Common options that most wireless residential gateways include are:

- Point-to-Point Protocol over Ethernet (PPPoE)
- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Ethernet switching
- Virtual Servers
- Print Serving
- Fail-over routing
- Virtual Private Networks (VPNs)
- Dynamic Host Configuration Protocol (DHCP) Server and Client
- Configurable Firewall

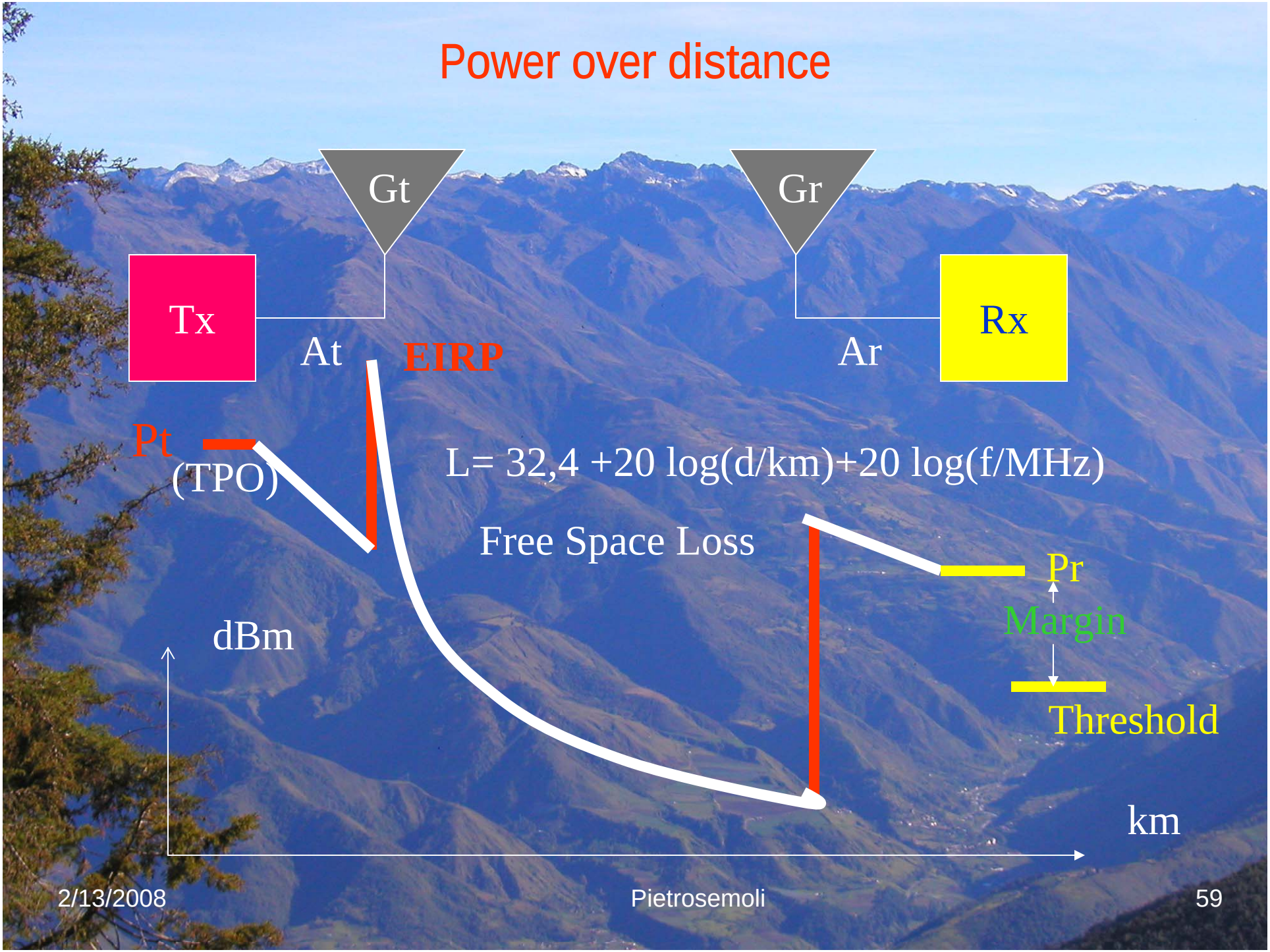
Configuration and Management of EG

- Enterprise wireless gateways are installed in the main data path on the wired LAN segment just past the access point(s)
- They are configured through console ports using telnet, internal HTTP or HTTPS servers, etc.
- Centralized management of only a few devices is one big advantage of using enterprise wireless gateways. An administrator, from a single console, can easily manage a large wireless deployment using only a few central devices instead of a very large number of access points.

Configuration and Management of EWG

Enterprise wireless gateways are normally upgraded through use of TFTP in the same fashion as many switches and routers on the market today. Configuration backups can often be automated so that the administrator won't have to spend additional management time backing up or recovering from lost configuration files. Enterprise wireless gateways are mostly manufactured as rack-mountable 1U or 2U devices that can fit into your existing data center design.

Power over distance



Power Limits

PtMP links have a central point of connection and two or more non-central connection points. PtMP links are typically configured in a star topology. The central connection point may or may not have an omnidirectional antenna. It is important to note that when an omnidirectional antenna is used, the FCC automatically considers the link a PtMP link.

Regarding the setup of a PtMP link, the FCC limits the EIRP to 4 Watts in both the 2.4 GHz ISM band and upper 5 GHz UNII band. The power limit set for the intentional radiator (the device transmitting the RF signal) in each of these bands is 1 Watt. If the transmitting wireless LAN devices are adjustable with respect to their output power, then the system can be customized to the needs of the user.

Power Limits

Suppose a radio transmitting at 1 Watt (+30 dBm) is connected directly to a 12 dBi omnidirectional antenna. The total output power at the antenna is about 16 Watts, which is well above the 4 Watt limit. The FCC stipulates that *for each 3 dBi above the antenna's initial 6 dBi of gain, the power at the intentional radiator must be reduced by 3 dB below the initial +30 dBm*. For the example, since the antenna gain is 12 dBi, the power at the intentional radiator must be reduced by 6 dB. This reduction will result in an intentional radiator power of +24 dBm (30 dBm – 6 dB), or 250 mW and an EIRP of 36 dBm (24 dBm + 12 dBi), or 4 Watts. The power at the intentional radiator must never be more than 1 Watt and the EIRP must never be above 4 Watts for a PtMP connection.

Power Limits

Point-to-Multipoint Power Limit Table

Power at Antenna (dBm)	Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

Power Limits

Point-to-Point (PtP)

PtP links include a single directional transmitting antenna and a single directional receiving antenna. These connections will typically include building-to-building or similar links and must abide by special rules. When installing a 2.4 GHz PtP link, the 4 Watt power limit all but disappears in favor of a sliding power limit. Regarding a PtP link, the FCC mandates that *for every 3 dBi above the initial 6 dBi of antenna gain, the power at the intentional radiator must be reduced by 1 dB from the initial +30 dBm.*

Power Limits

Point-to-Point Power Limit Table

Power at Antenna (dBm)	Max Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
29	9	38	6.3
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39.8
24	24	48	63
23	27	50	100
22	30	52	158

Power Limits

- *(d) Any U-NII device that operates in the 5.15-5.25 GHz band shall use a transmitting antenna that*
- *is an integral part of the device.*
- *(e) Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce*
- *any potential for harmful interference to co-channel MSS operations.*
- The "middle" band runs from 5.25 GHz to 5.35 GHz, with a maximum power limit of 250 mW. Finally
- the "high" band runs from 5.725 GHz to 5.825 GHz, with a maximum transmitter power of 1 watt and
- antenna gain of 6 dBi or 36 dBm or 4 watts EIRP.

FCC 15.247 Revised as of February 11, 2008

- TITLE 47--TELECOMMUNICATION
  CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION
  PART 15--Subpart C--Intentional Radiators
  Sec. 15.247 Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz Maximum Power :
- (3) For systems using digital modulation in the 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz bands: 1 Watt.
- (ii) Systems operating in the 5725–5850 MHz band that are used exclusively for fixed, point-to-point operations may employ transmitting antennas with directional gain greater than 6 dBi without any corresponding reduction in transmitter peak output power.

IEEE 802.11g

802.11g provides the same maximum speed of 802.11a, coupled with backwards compatibility for 802.11b devices. This backwards compatibility makes upgrading wireless LANs simple and inexpensive.

IEEE 802.11g specifies operation in the 2.4 GHz ISM band. To achieve the higher data rates found in 802.11a, 802.11g compliant devices utilize Orthogonal Frequency Division Multiplexing (OFDM) modulation technology. These devices can automatically switch to QPSK modulation in order to communicate with the slower 802.11b- and 802.11- compatible devices. There is no reason to keep purchasing 802.11b only devices nowadays, since for all practical purposes 802.11g is a superset of b, offering higher speed and some multipath inmunity

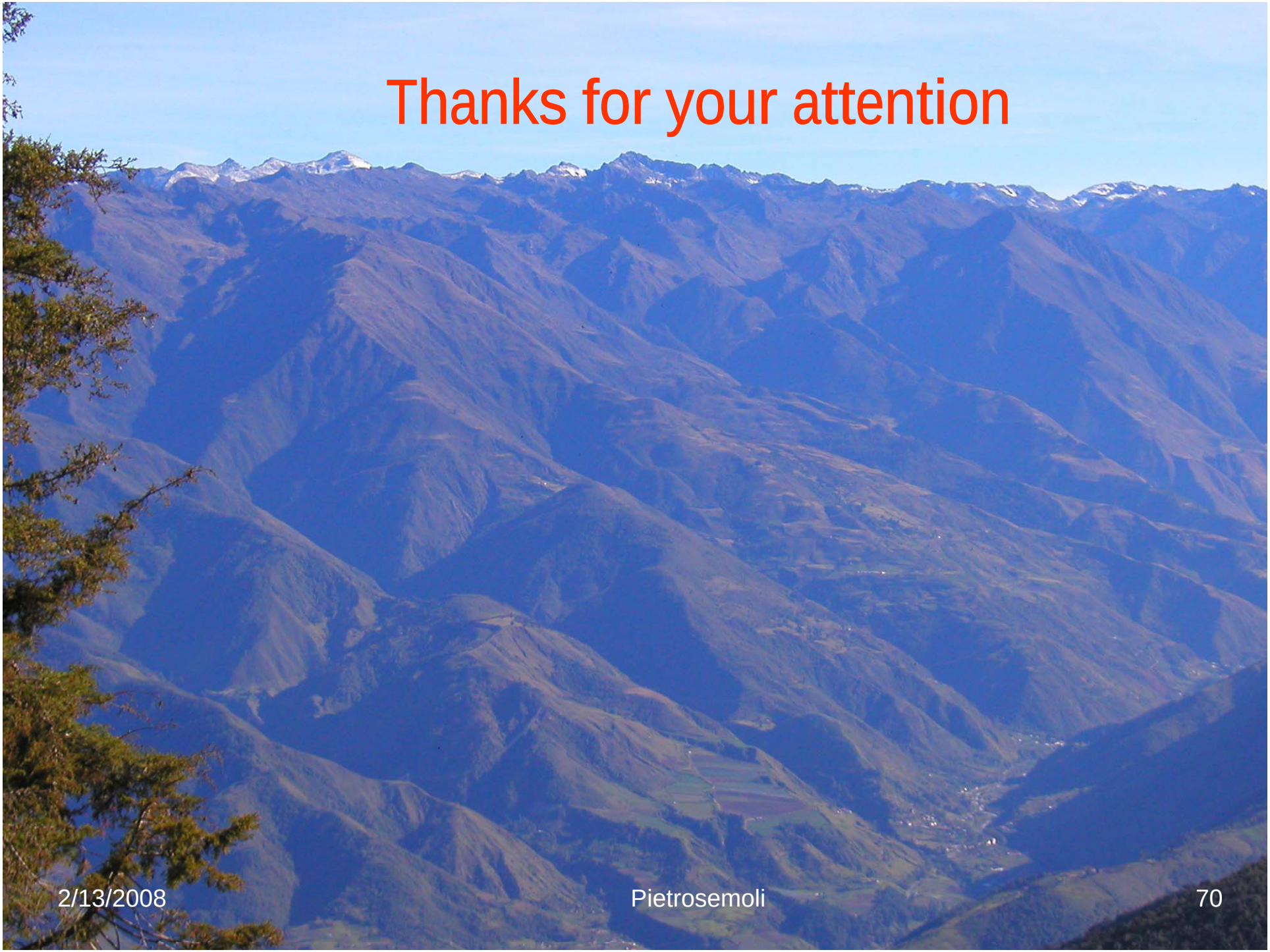
WiFi Compatibility Alliance

The **WiFi Compatibility Alliance** promotes and tests for wireless LAN interoperability of 802.11 devices. WiFi's mission is *to certify interoperability of Wi-Fi™ (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments*.

The certification is done by a vendor-independent laboratory, like CETECOM in Spain.

Supported Rates

802.11b compliant device supports 11, 5.5, 2, & 1Mbps.
802.11g can extend the capabilities to 54 Mbps as does 802.11a.
Some vendors offer “enhancements” over the standards that reach 108 Mbps, but this often increases the interference problem
802.11n (not yet officially approved) offers nominal data rates above 200 Mbps and also the possibility of using 2 adjacent 20 MHz channels to reach a nominal throughput of 400 Mbps


Thanks for your attention