Wi-Fi Technology Overview

Abdus Salam ICTP, February 2004

School on Digital Radio Communications for Research and Training in Developing Countries

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

Wi-Fi Technology Overview
Agenda

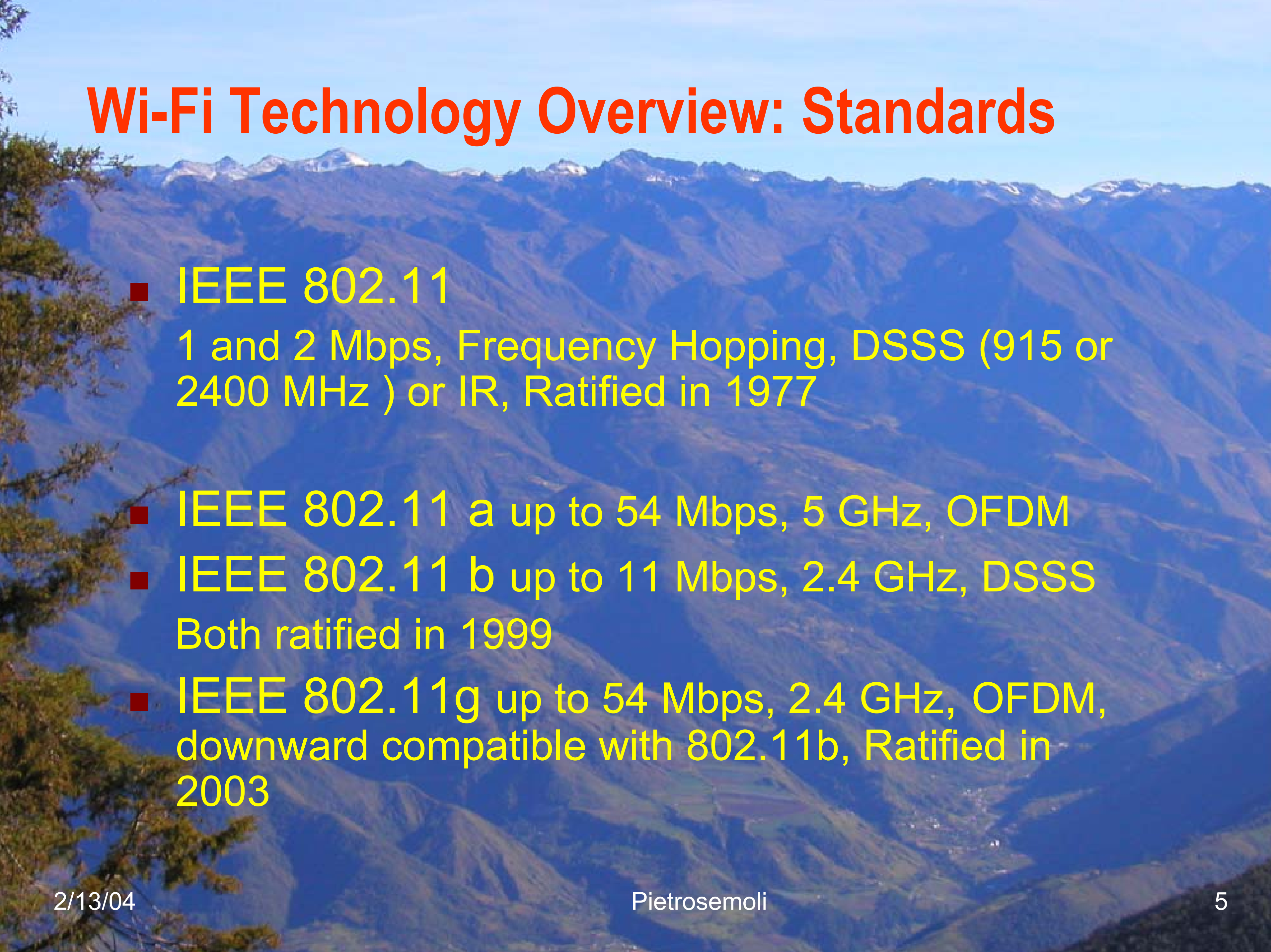
- 802.11 Standards
- 802.11 Terminology
- DSSS Channel Allocation
- Medium Access Control
- It’s all about Power!
- Scanning

Wireless Data Transmission flavors

- Packet Radio
- 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, from $750 in 1992 to $30 in 2004, while transmission speed has increased up to 74 Mbps on the same 20 MHz channel



Wi-Fi Technology Overview: Standards

- IEEE 802.11

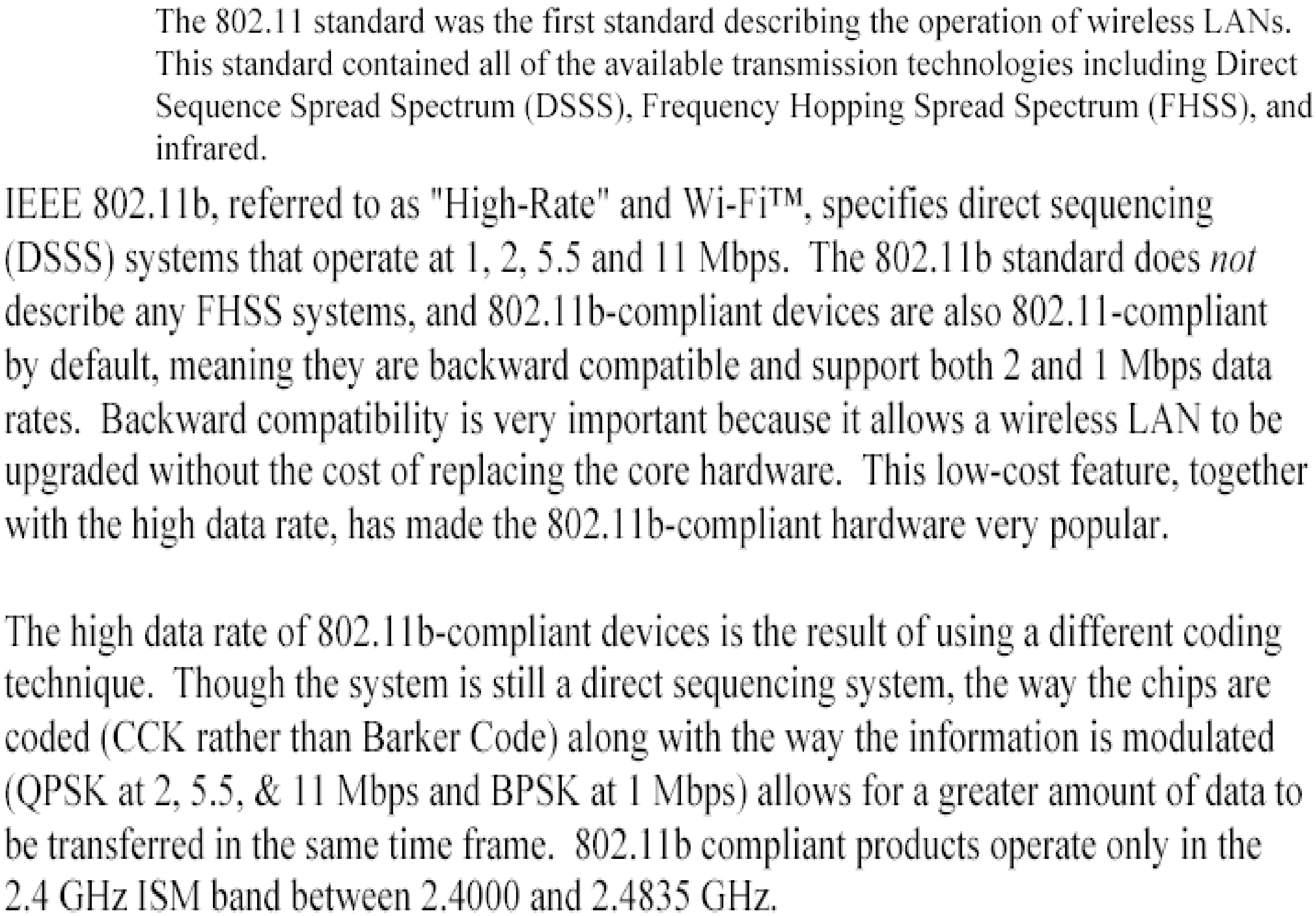
  1 and 2 Mbps, Frequency Hopping, DSSS (915 or 2400 MHz) or IR, Ratified in 1977

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

IEEE 802.11

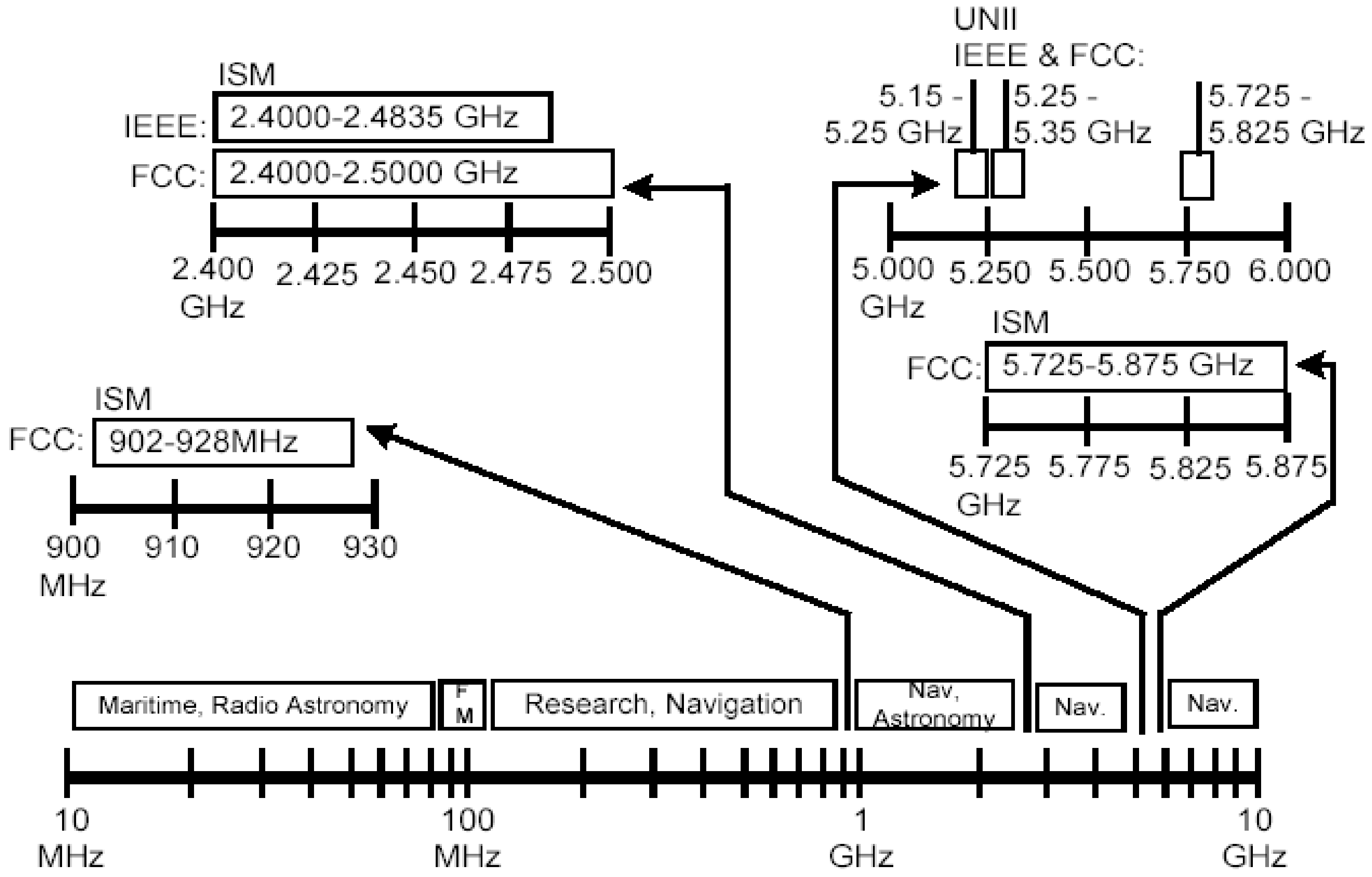


The 802.11 standard was the first standard describing the operation of wireless LANs. This standard contained all of the available transmission technologies including Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and infrared.

IEEE 802.11b, referred to as "High-Rate" and Wi-Fi™, specifies direct sequencing (DSSS) systems that operate at 1, 2, 5.5 and 11 Mbps. The 802.11b standard does *not* describe any FHSS systems, and 802.11b-compliant devices are also 802.11-compliant by default, meaning they are backward compatible and support both 2 and 1 Mbps data rates. Backward compatibility is very important because it allows a wireless LAN to be upgraded without the cost of replacing the core hardware. This low-cost feature, together with the high data rate, has made the 802.11b-compliant hardware very popular.

The high data rate of 802.11b-compliant devices is the result of using a different coding technique. Though the system is still a direct sequencing system, the way the chips are coded (CCK rather than Barker Code) along with the way the information is modulated (QPSK at 2, 5.5, & 11 Mbps and BPSK at 1 Mbps) allows for a greater amount of data to be transferred in the same time frame. 802.11b compliant products operate only in the 2.4 GHz ISM band between 2.4000 and 2.4835 GHz.

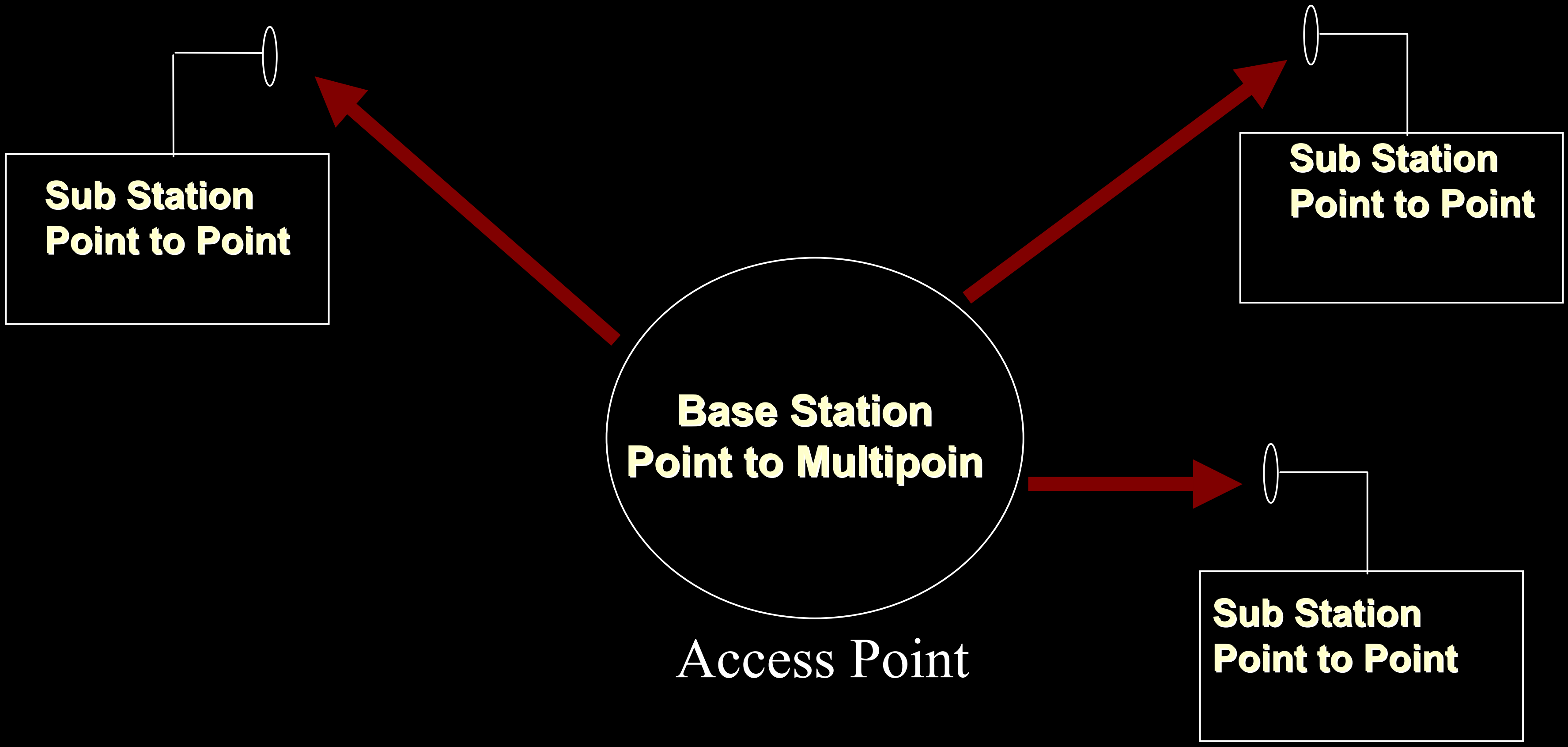
ISM and UNII Spectra



Elements of a Transmission System

- Transmitter
- Connecting cable or waveguide
- Antennas
- Receiver
- Power Supply, Grounding and Lightning Protection

System Configuration



Sub Station
Point to Point

Sub Station
Point to Point

Base Station
Point to Multipoin

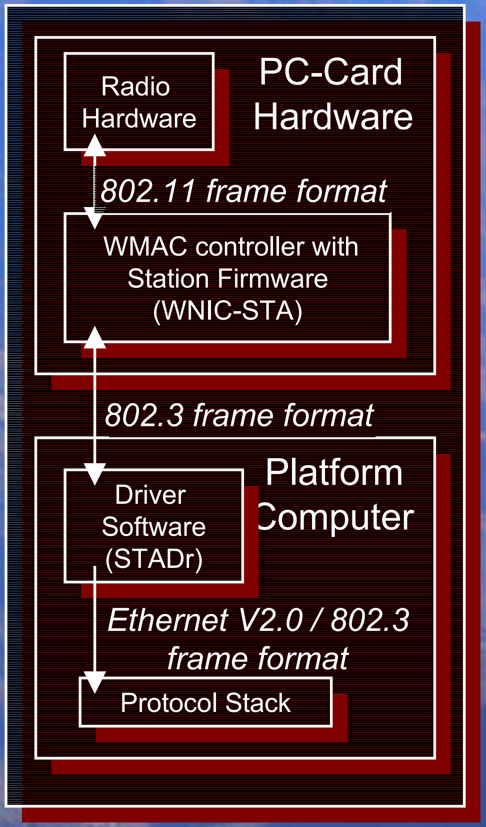
Access Point

Sub Station
Point to Point

IEEE 802 .11 Terminology

Station (STA) Architecture:

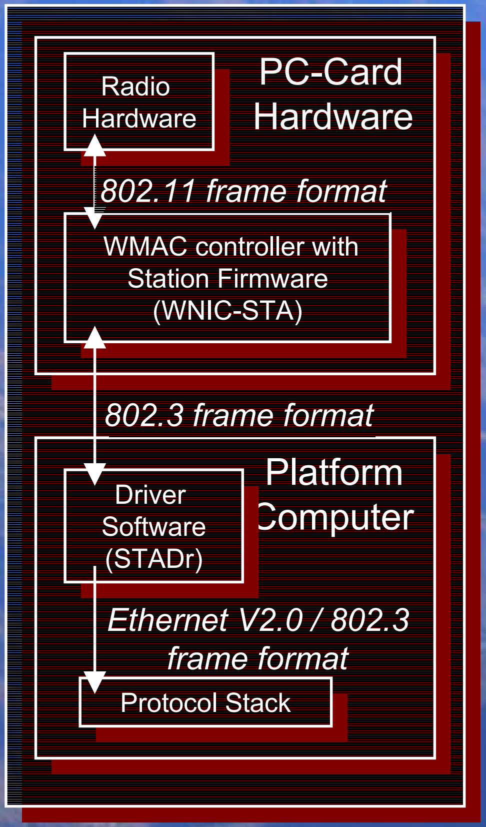
- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system
- Most often end-stations available in terminals (work-stations, laptops etc.)

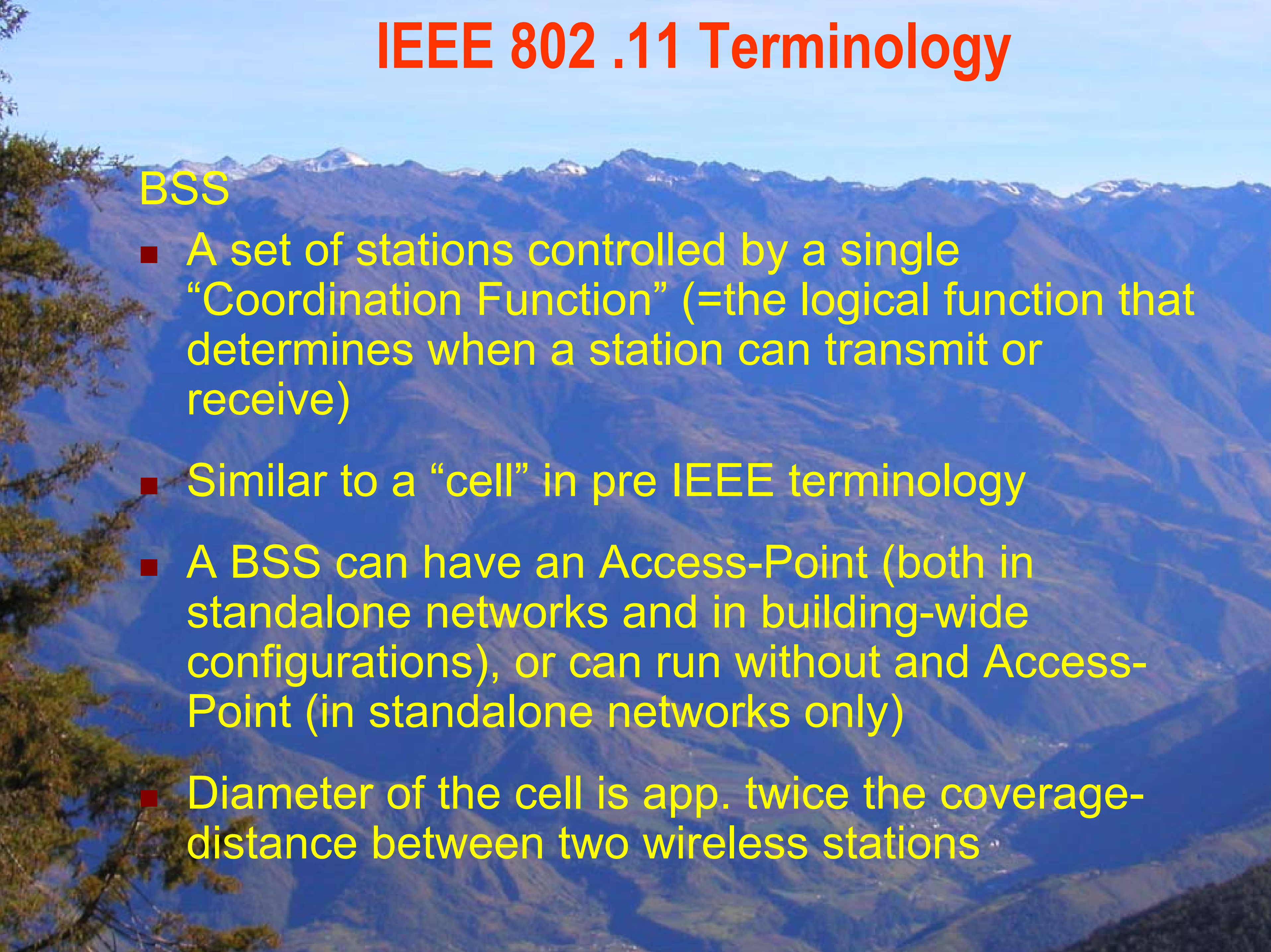


IEEE 802 .11 Terminology

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



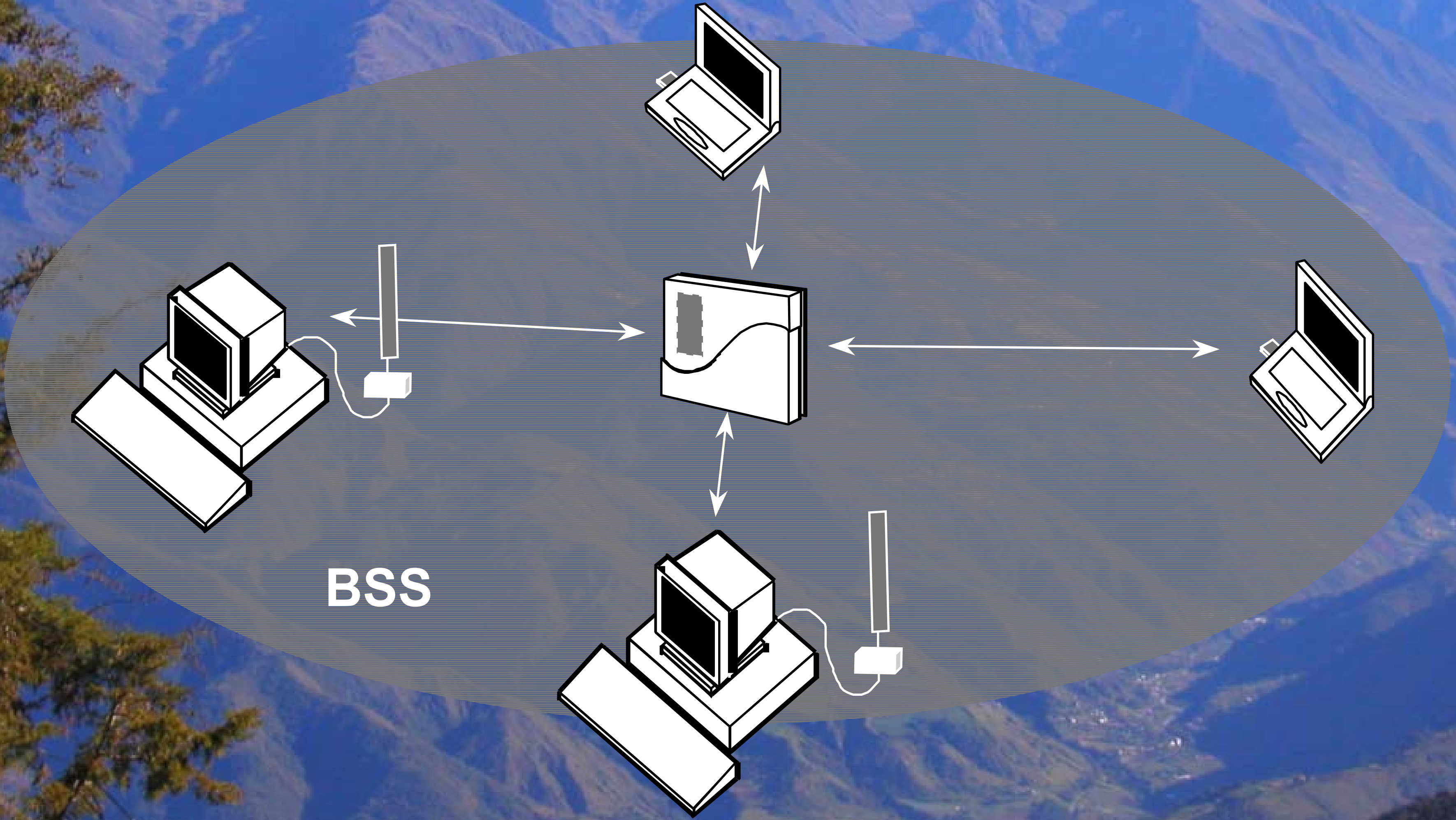


IEEE 802 .11 Terminology

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 pre IEEE 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)

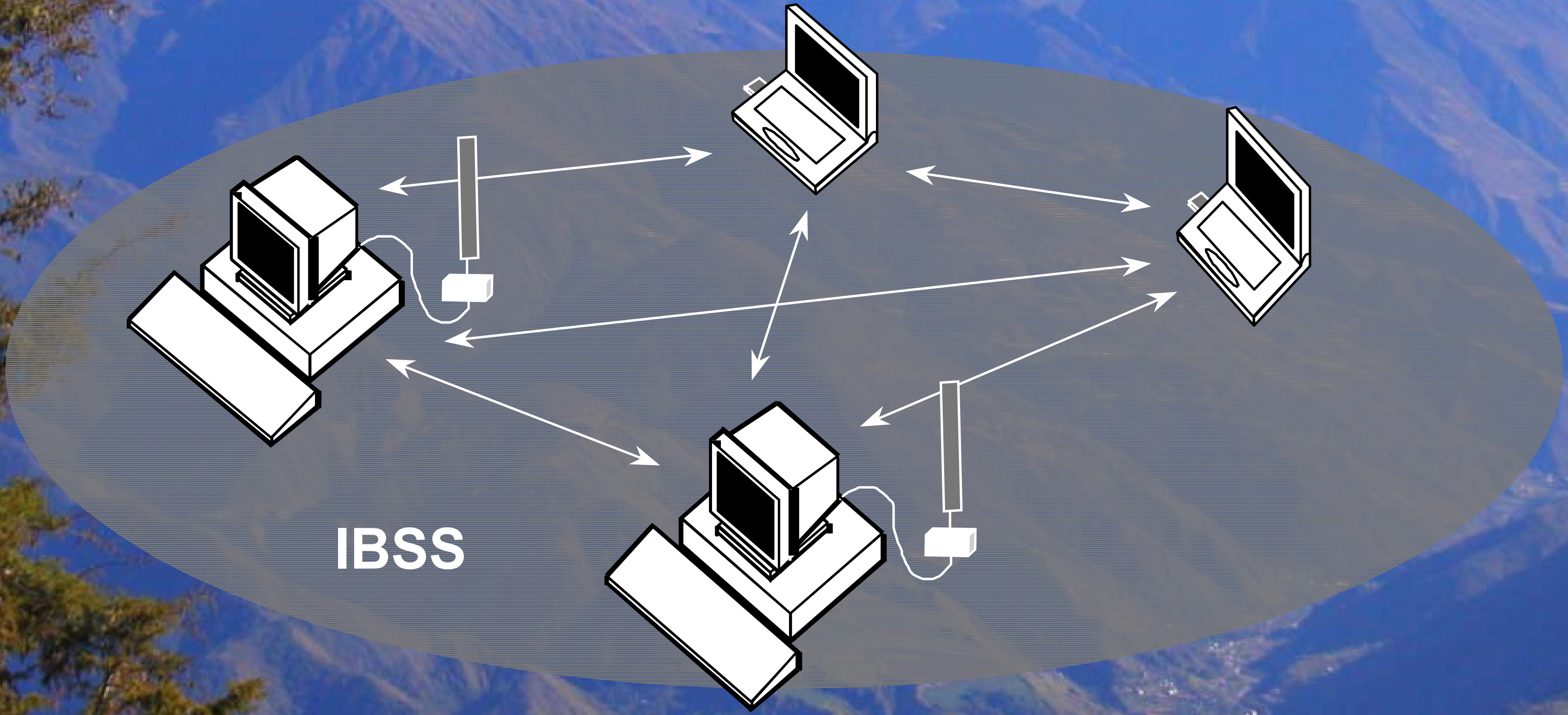


IEEE 802 .11 Terminology

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):

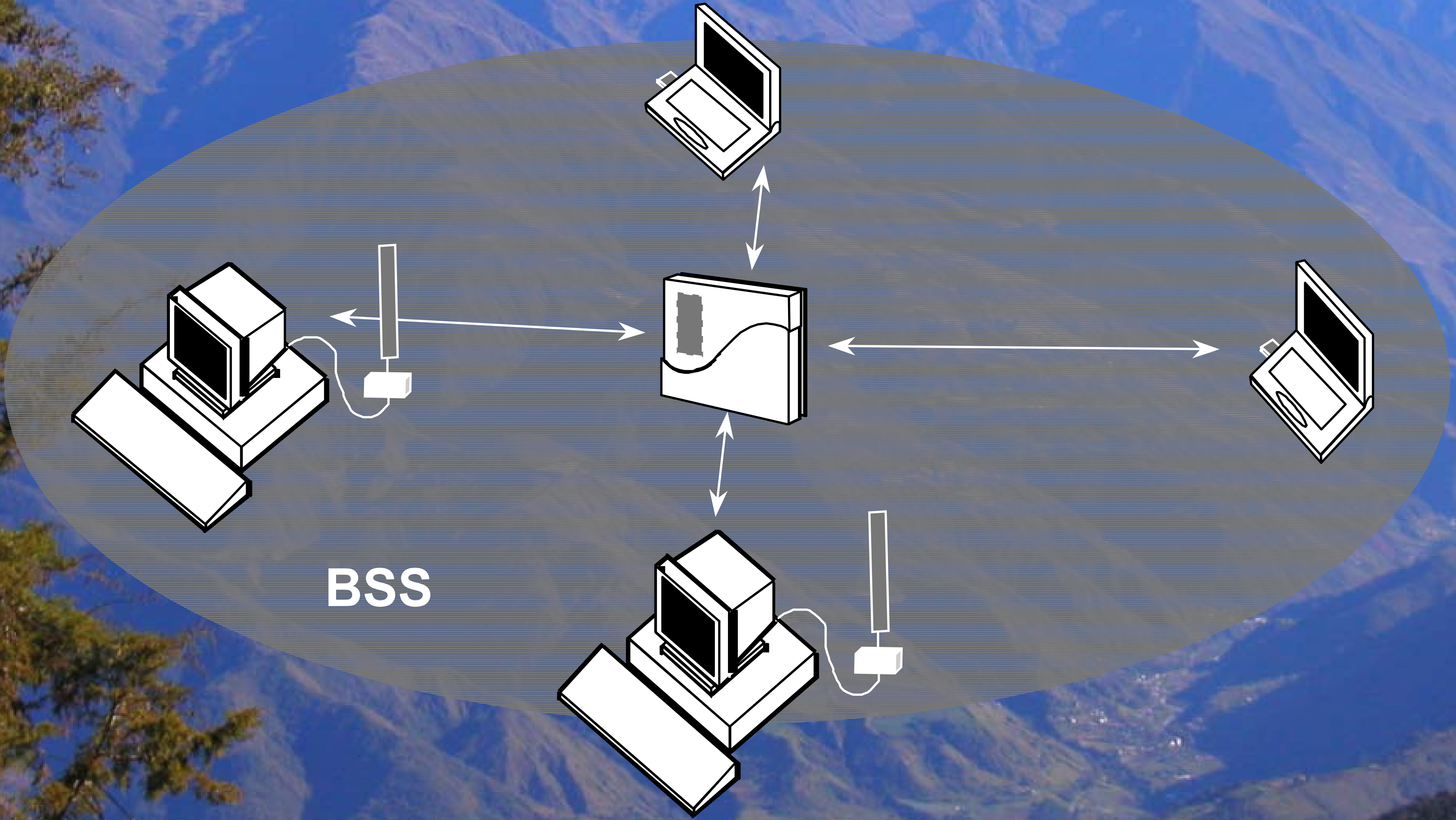
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point

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

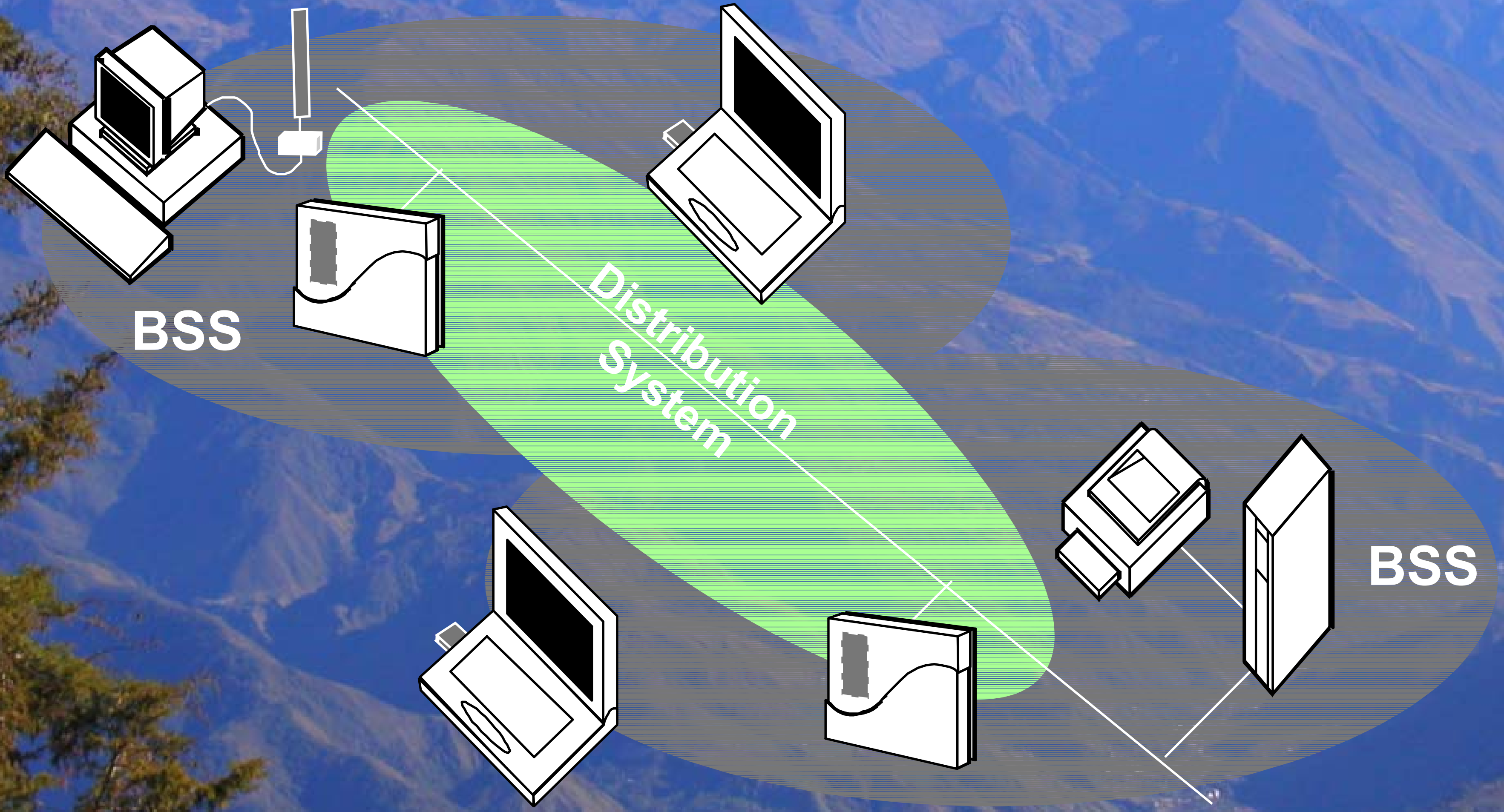
Extended Service Set (ESS)

single BSS (with integrated DS)



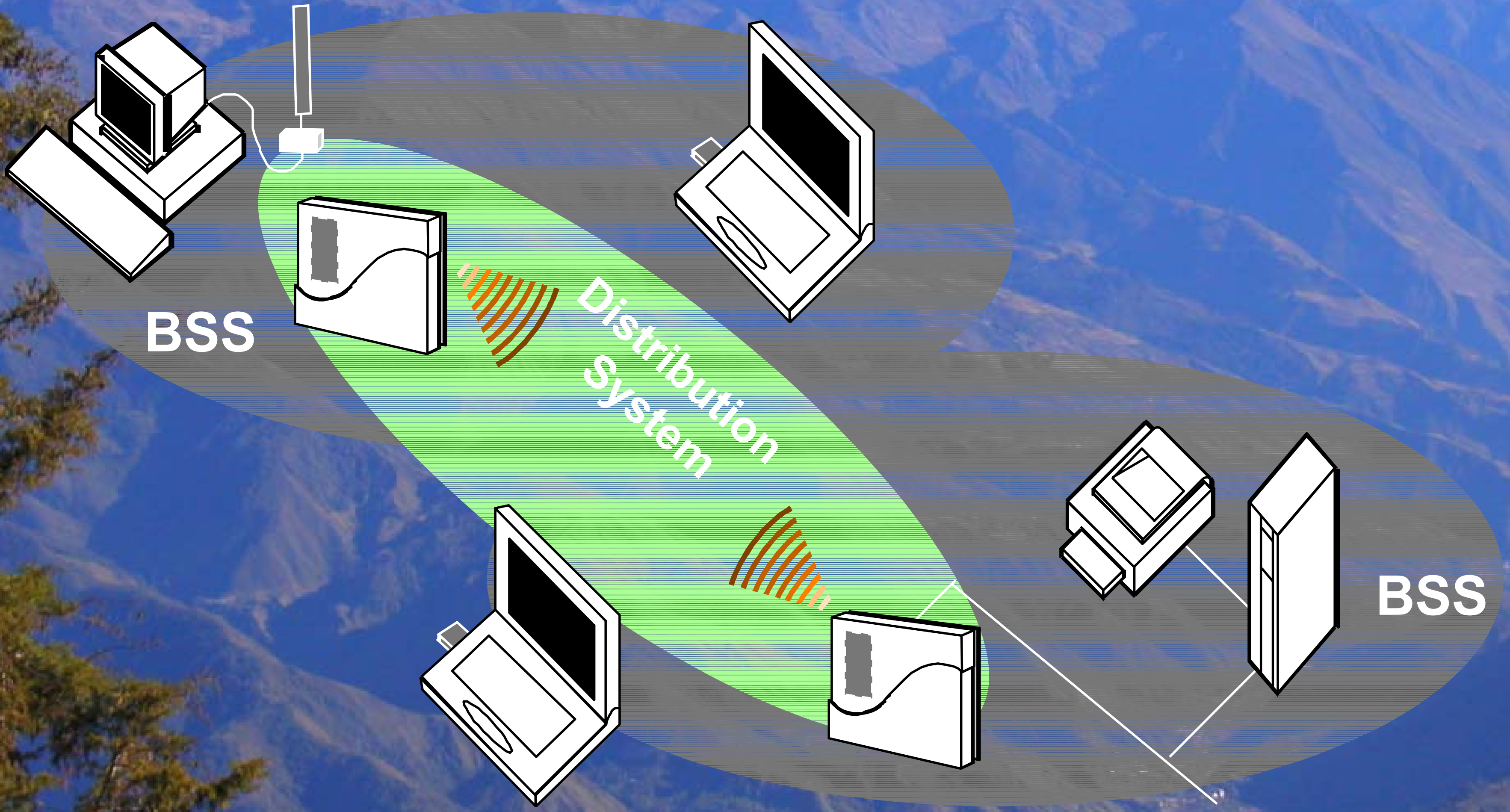
Extended Service Set (ESS)

BSS's with wired Distribution System (DS)



Extended Service Set (ESS)

BSS's 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

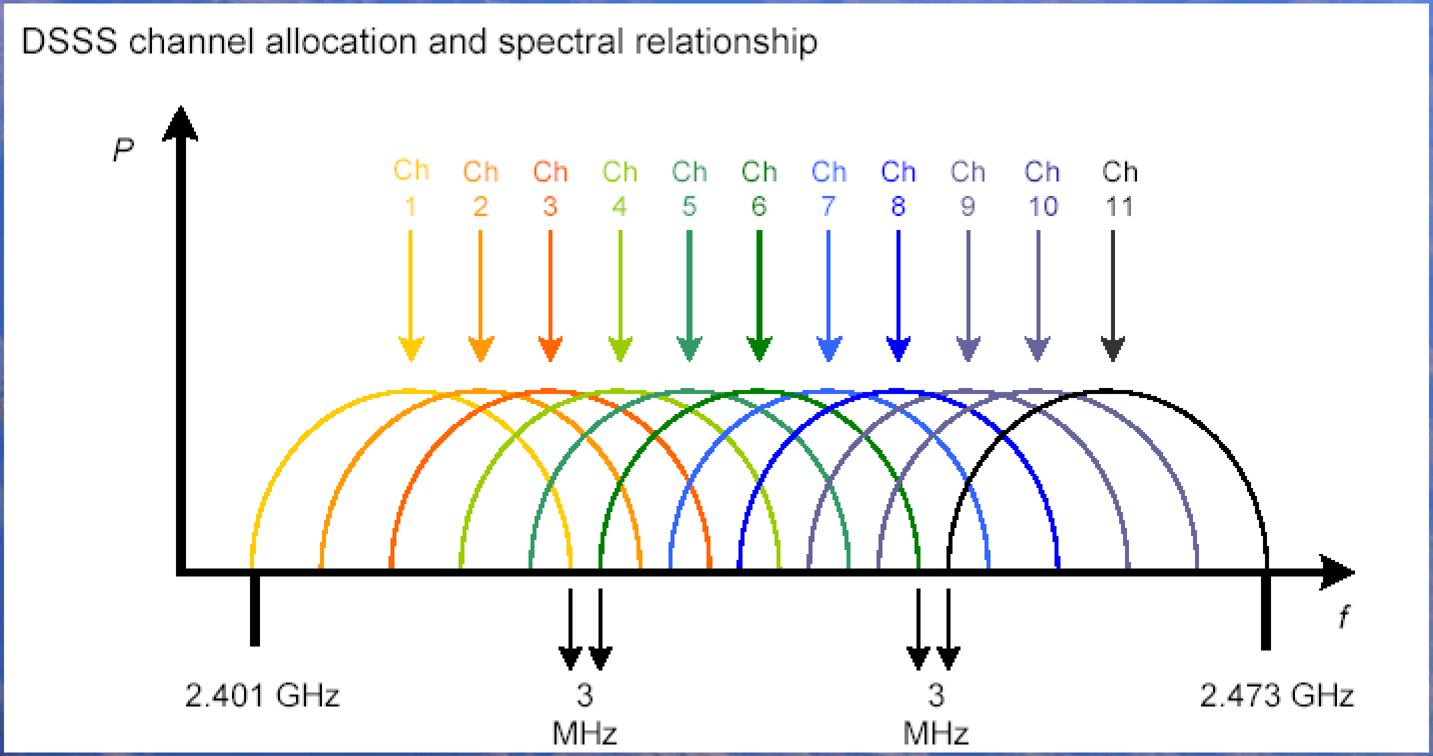
MAC Management Frames

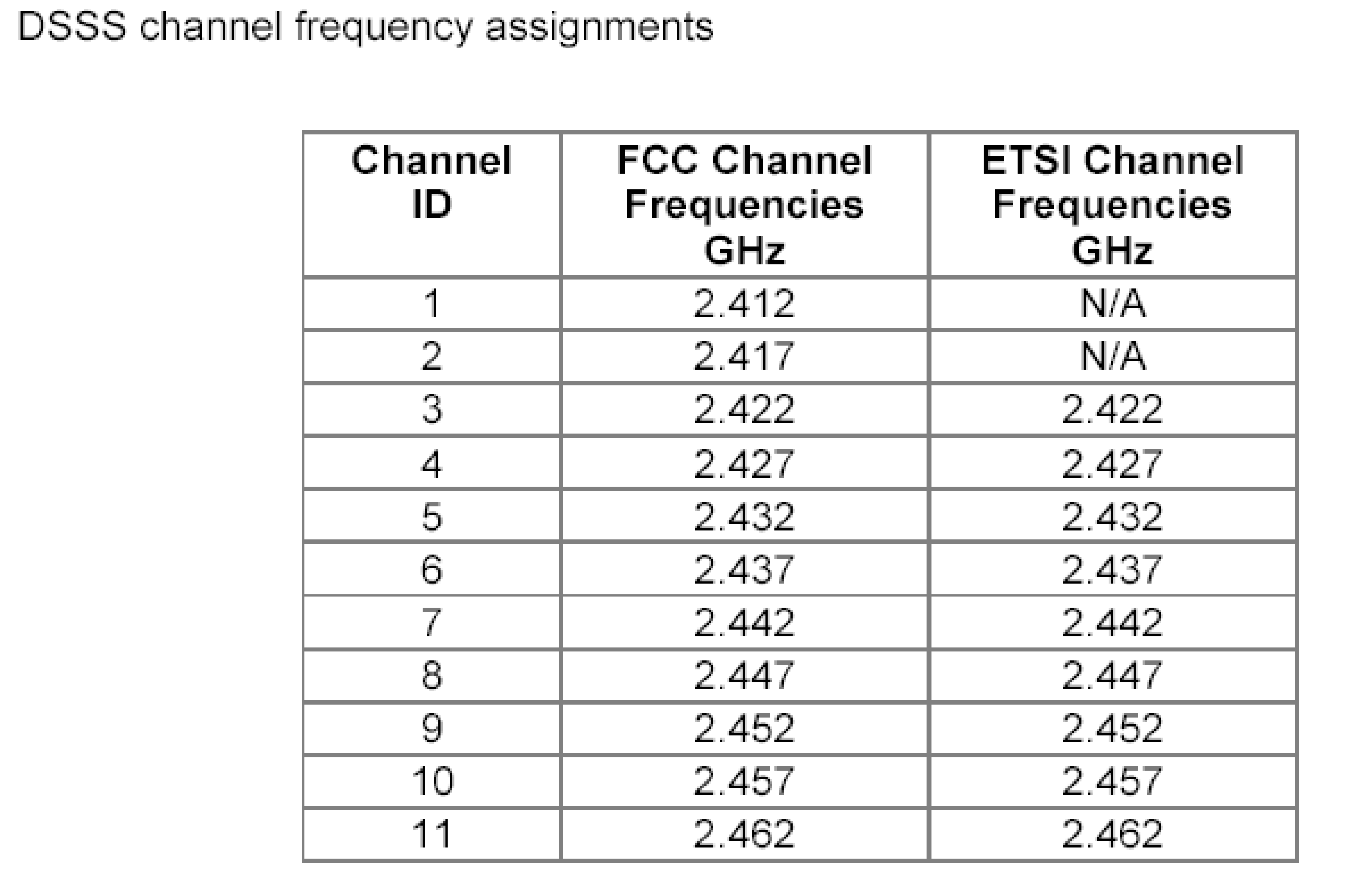
- Beacon
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - Traffic Indication Map
- Probe
  - SSID, Capabilities, Supported Rates
- Probe Response
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - same for Beacon except for TIM

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

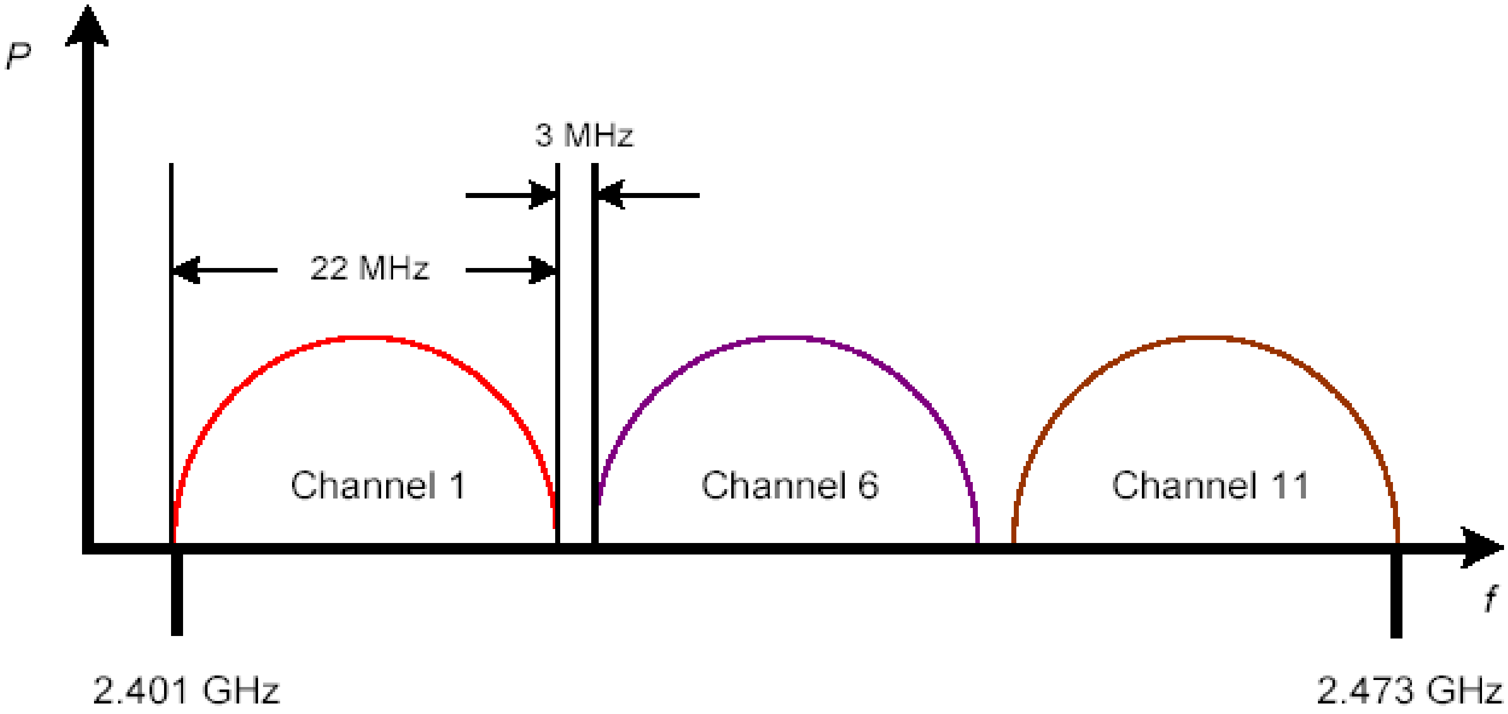




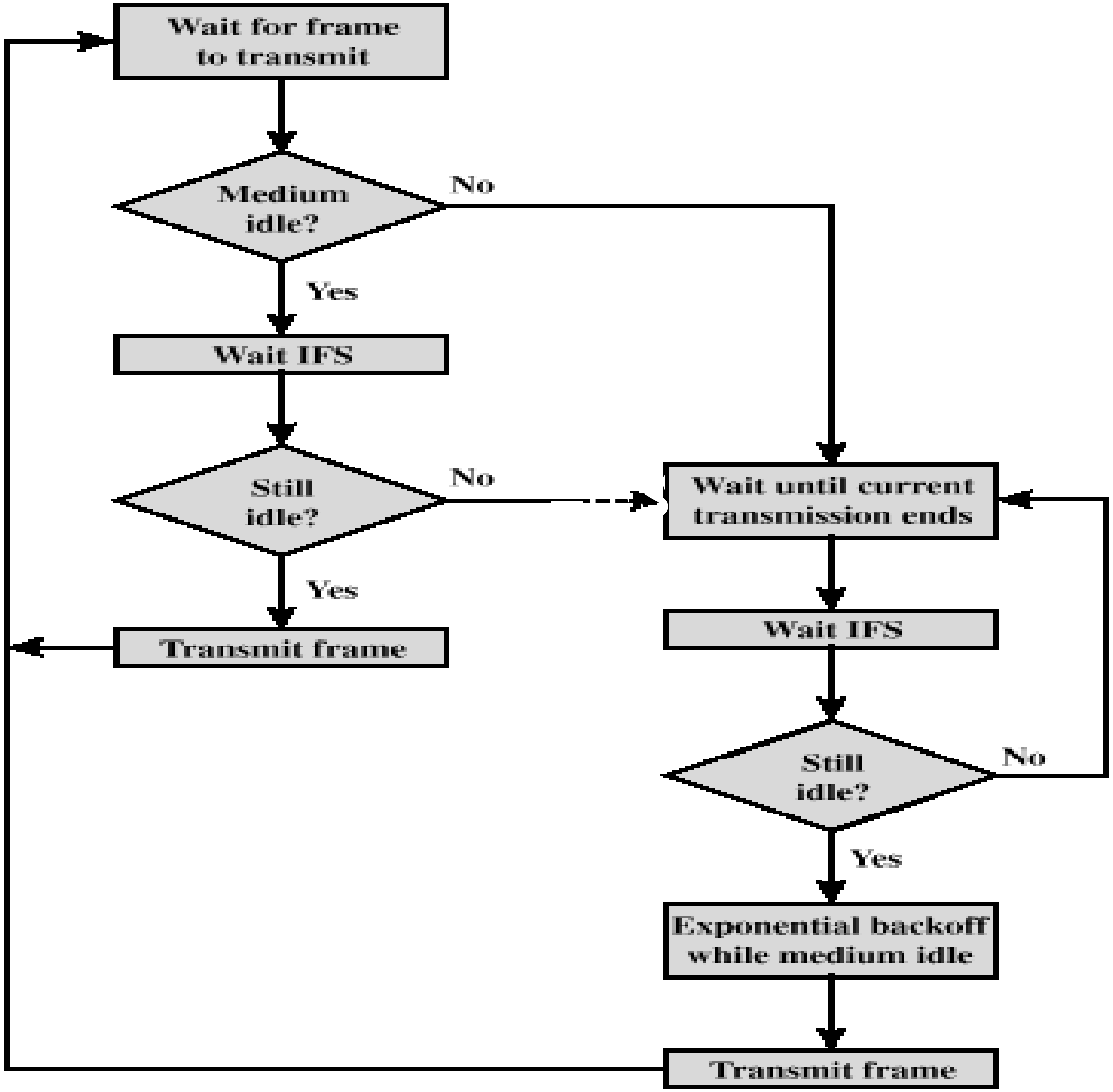
DSSS channel frequency assignments

Channel ID	FCC Channel Frequencies GHz	ETSI Channel Frequencies GHz
1	2.412	N/A
2	2.417	N/A
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

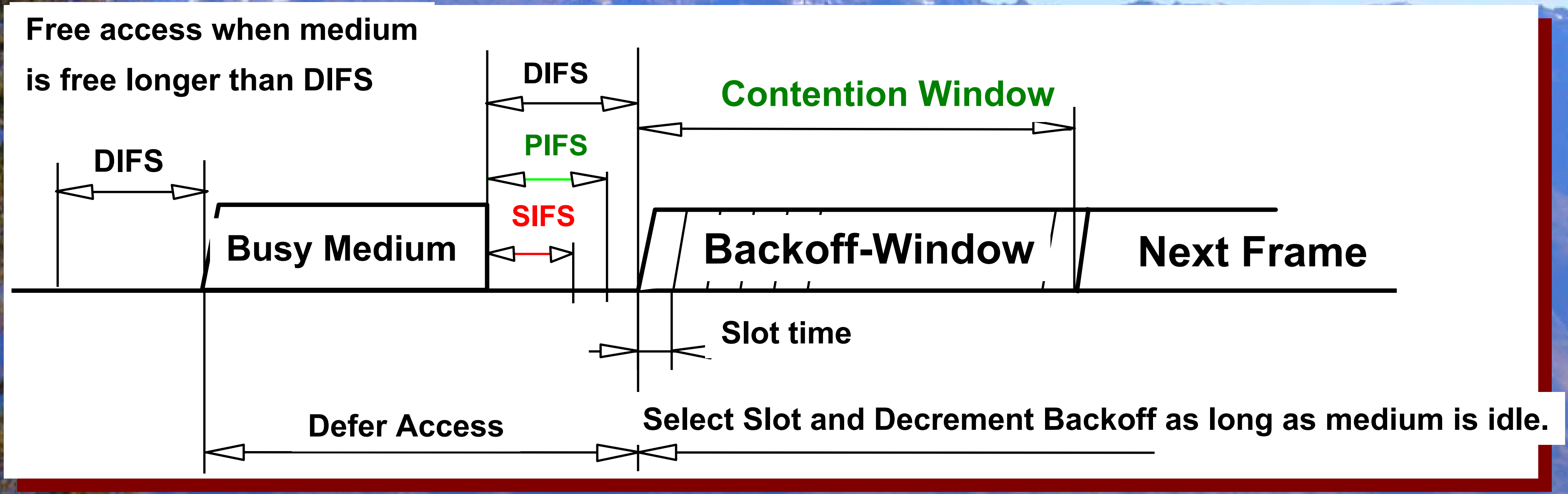
DSSS non-overlapping channels



Medium Access Control Logic

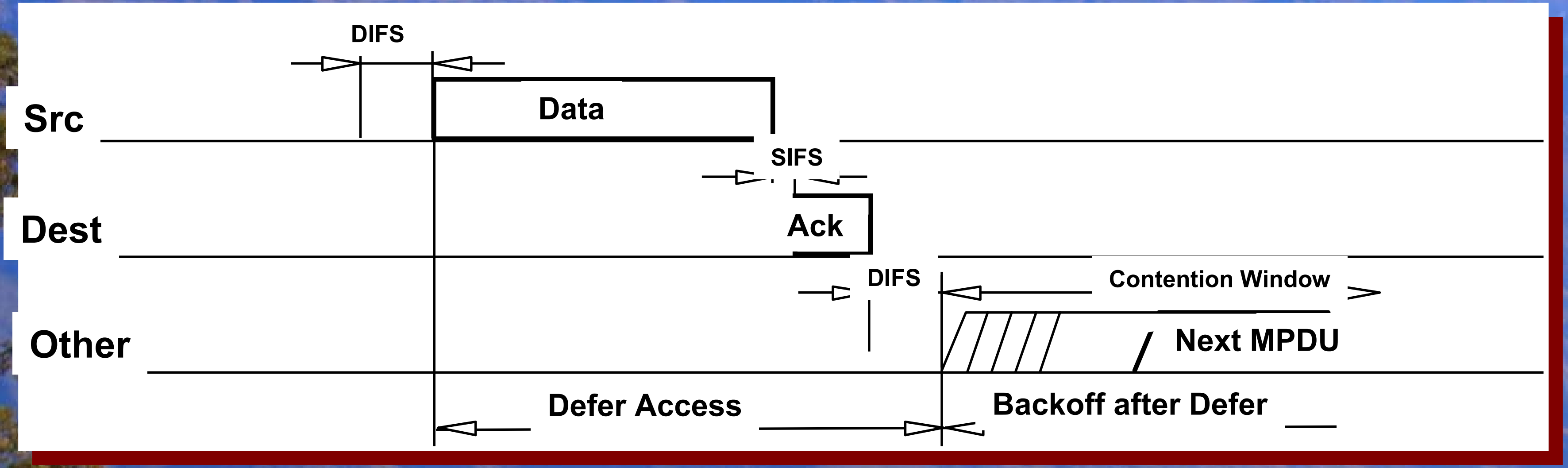

Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

Operational processes
Inter-Frame Spacing



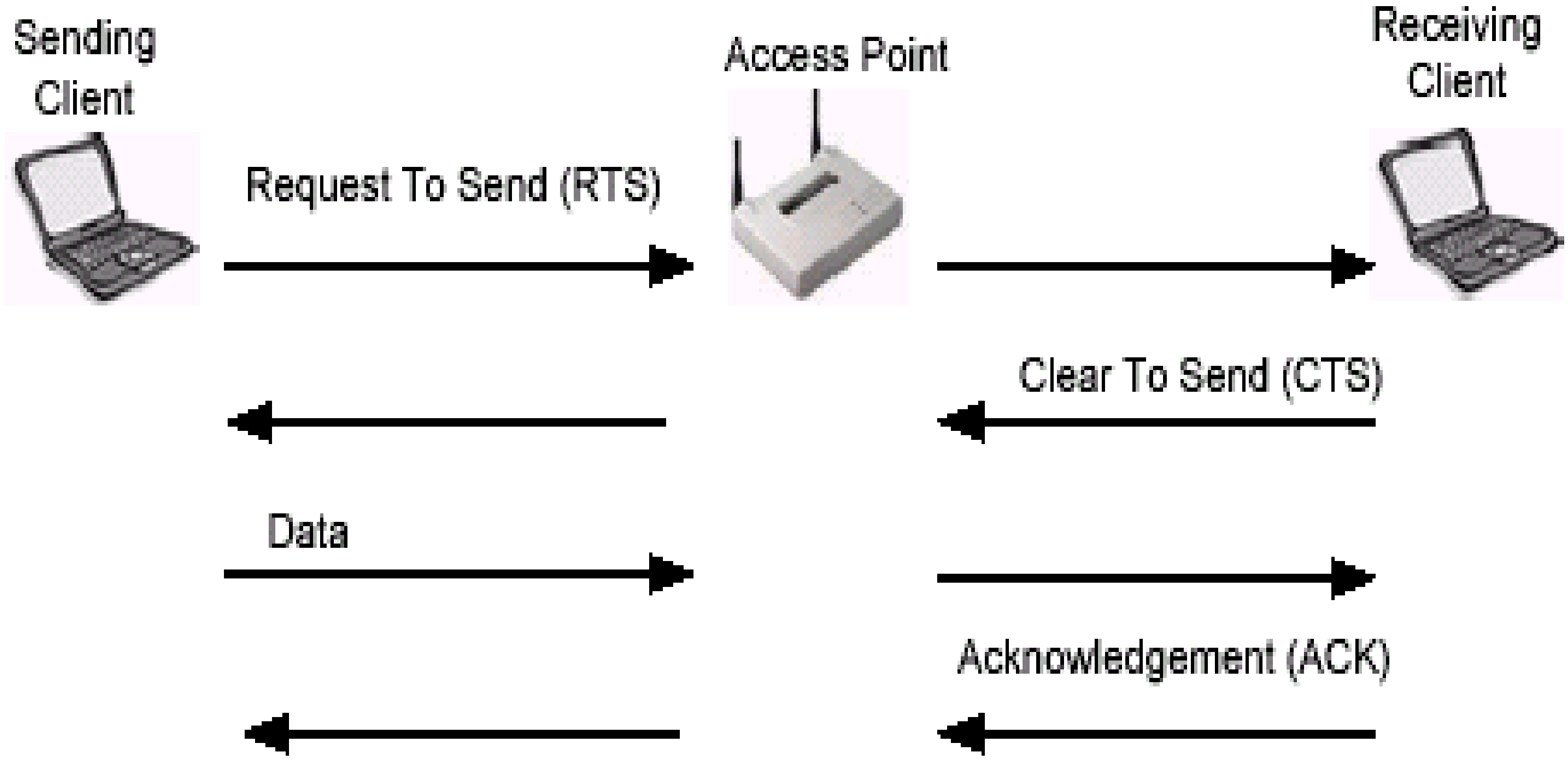
- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = PCF interframe space
  - DIFS = DCF interframe space
- Back-off timer expressed in terms of number of time slots

Operational processes
Data Frames and their ACK

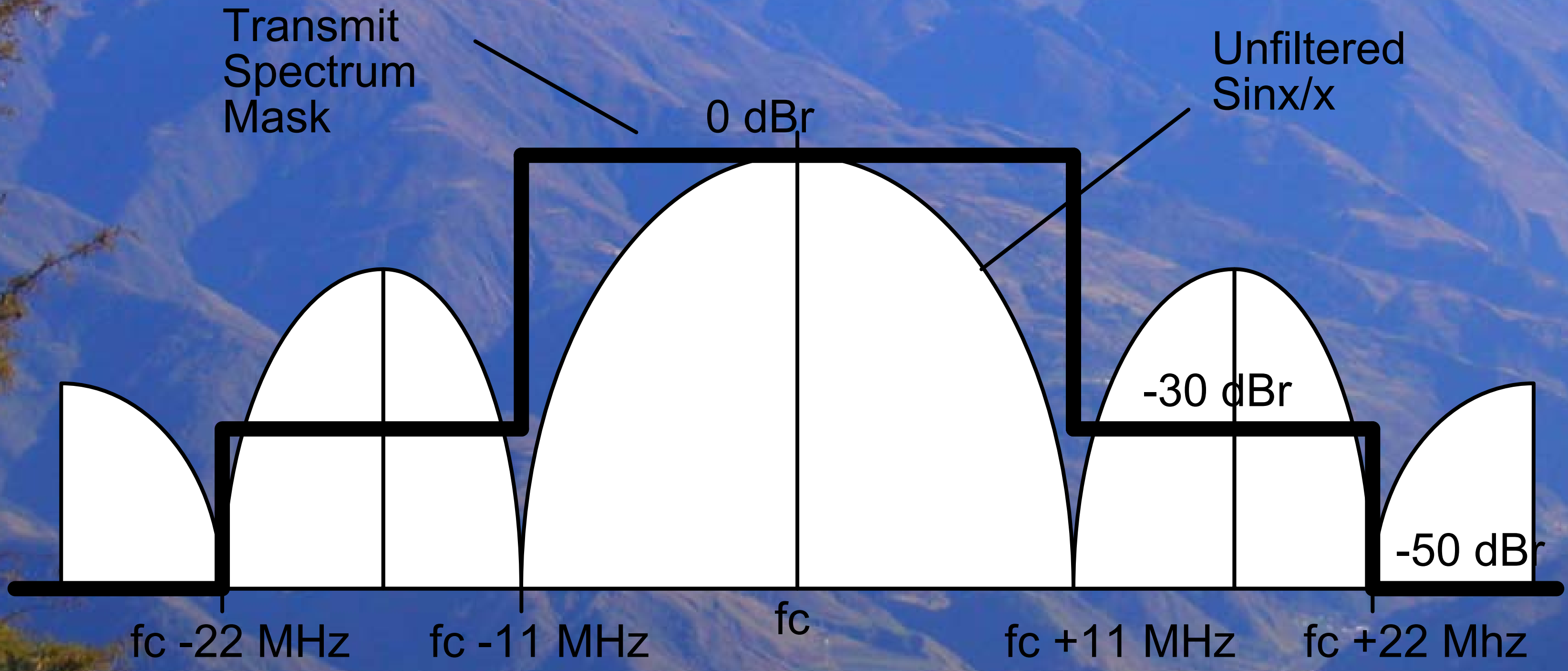


- Acknowledgment are to arrive at within the SIFS
- The DCF interframe space is observed before medium is considered free for use

RTS/CTS handshaking



802.11b spectral mask

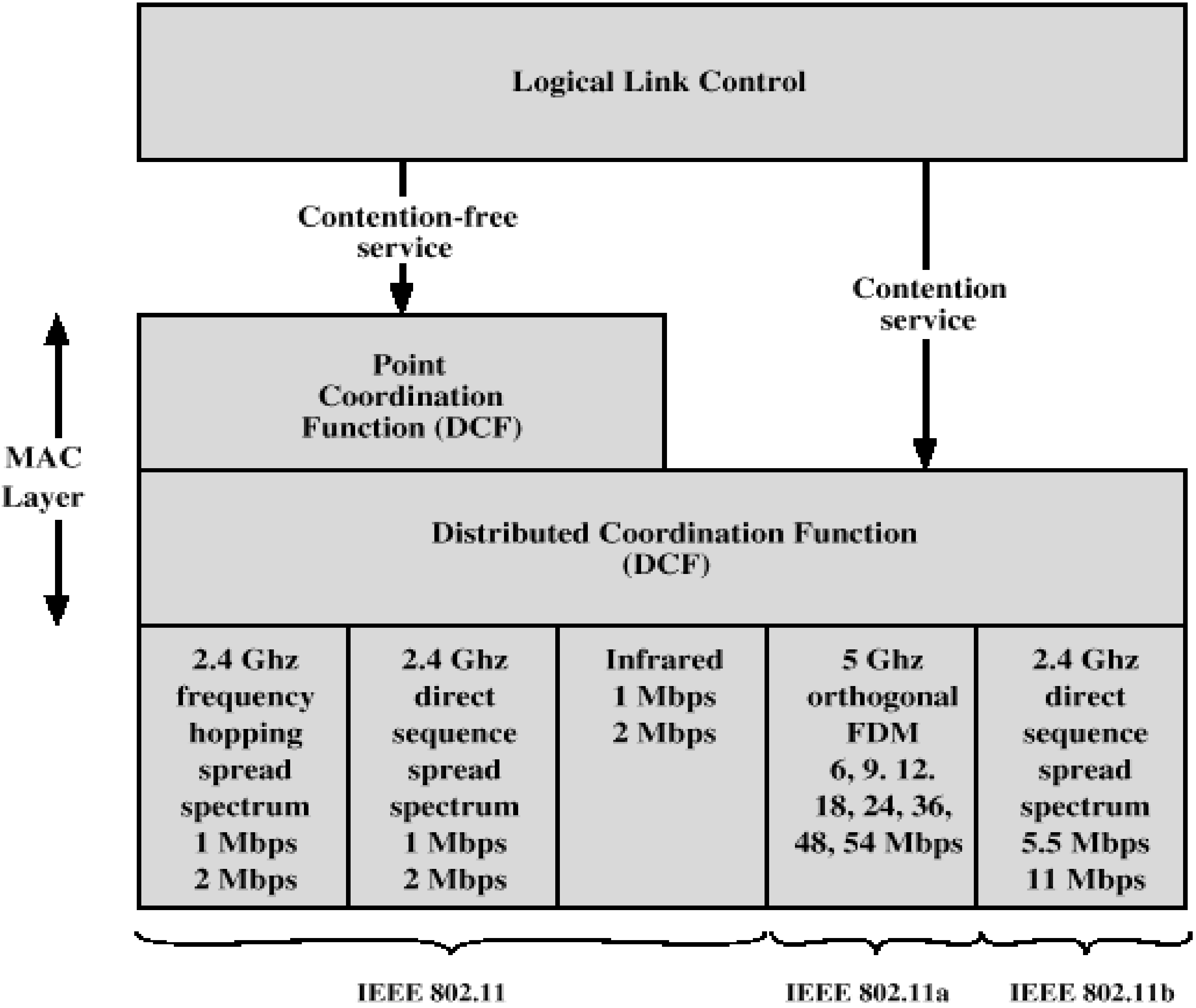


Control Frames

- 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



Logical Link Control

Contention-free service

Contention service

MAC Layer

Point Coordination Function (DCF)

Distributed Coordination Function (DCF)

2.4 Ghz frequency hopping spread spectrum 1 Mbps 2 Mbps

2.4 Ghz direct sequence spread spectrum 1 Mbps 2 Mbps

Infrared 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

IEEE 802.11

IEEE 802.11a

IEEE 802.11b

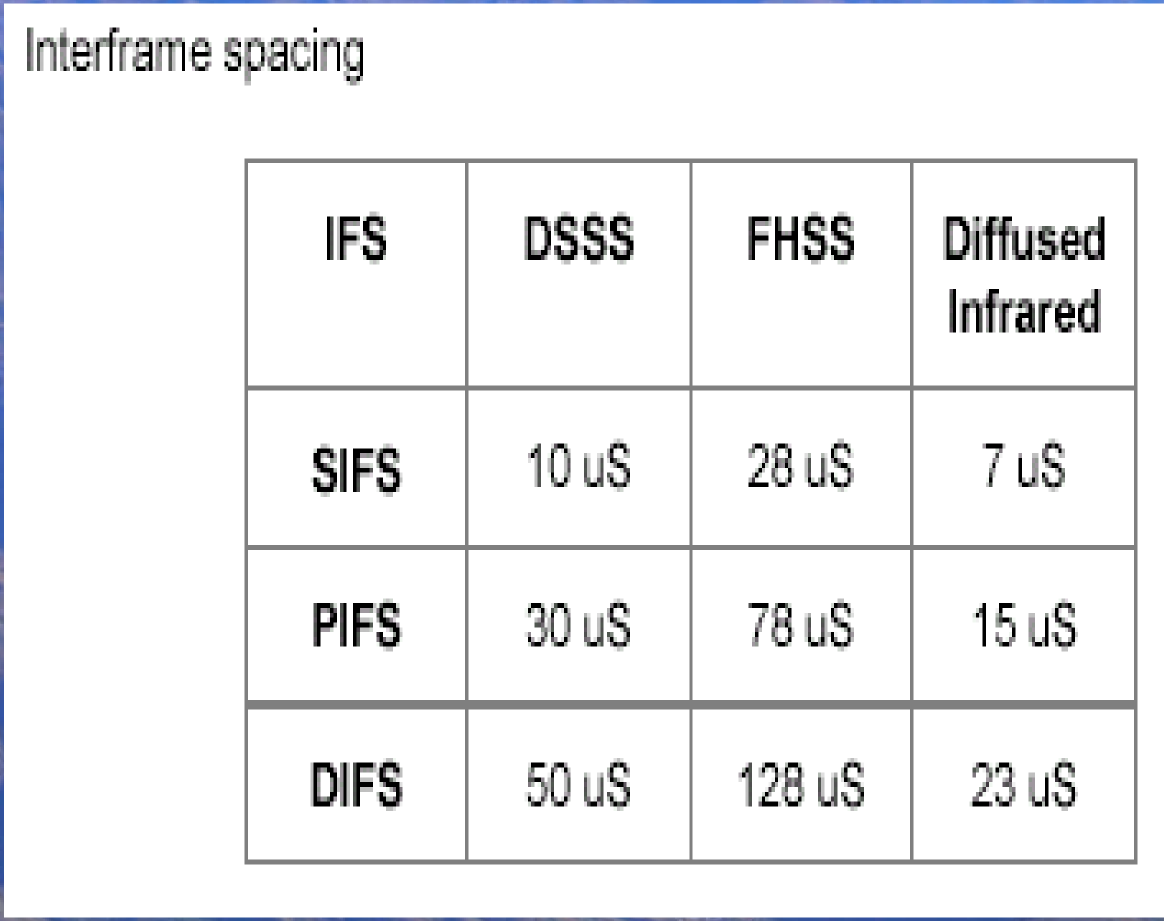
IEEE 802.11 Protocol Architecture

IFS FLAVORS

- SIFS
  - Acknowledgment (ACK)
  - Clear to send (CTS)
  - Poll response
- PIFS
  - Used by centralized controller in issuing polls
  - Takes precedence over normal contention traffic
- DIFS
  - Used for all ordinary asynchronous traffic

Frames spacing intervals

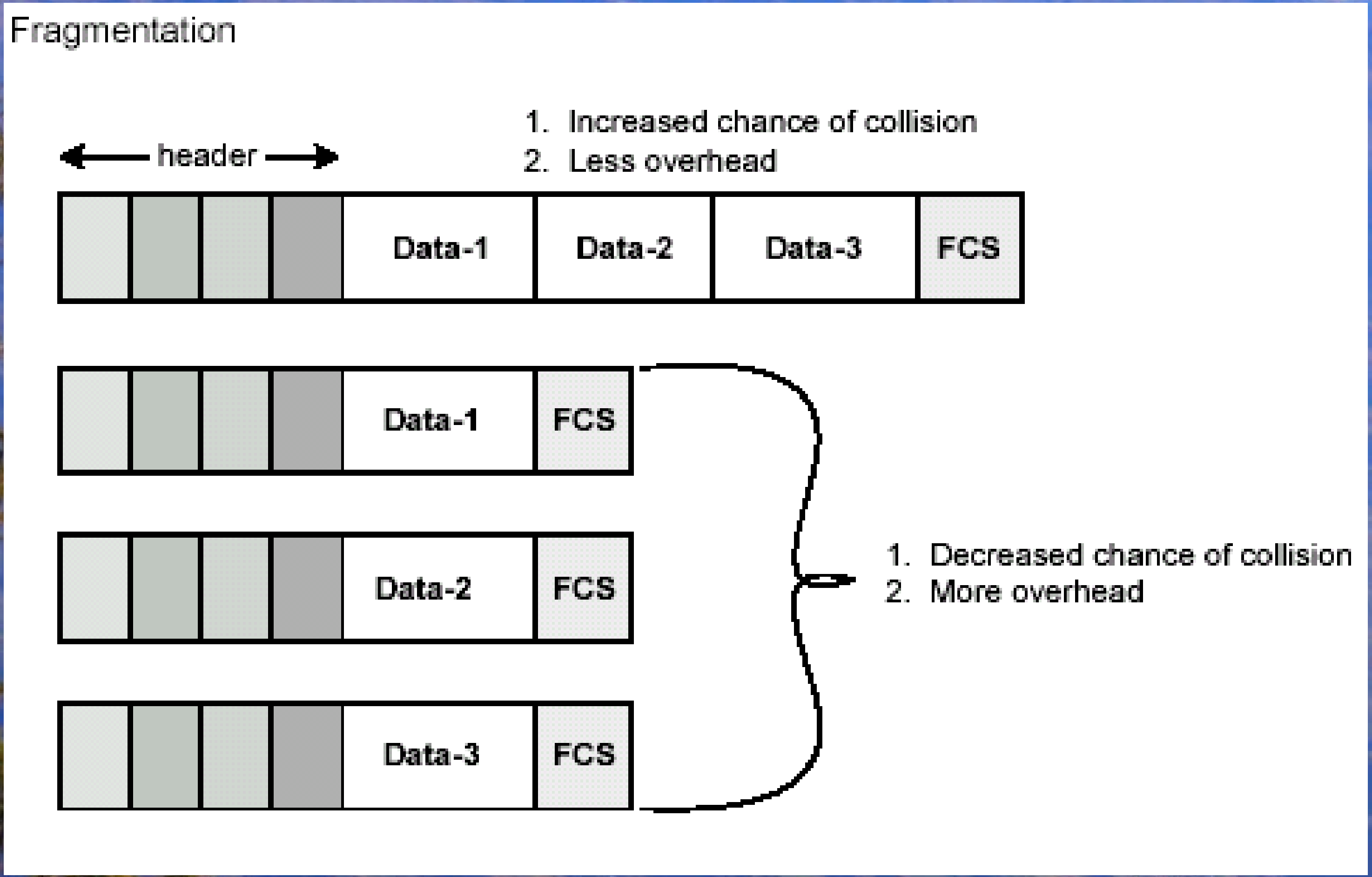
Short Interframe Spacing (SIFS)
Point Coordination Function Interframe Space (PIFS)
Distributed Coordination Function Interframe Space (DIFS)



Interframe spacing

IFS	DSSS	FHSS	Diffused Infrared
SIFS	10 uS	28 uS	7 uS
PIFS	30 uS	78 uS	15 uS
DIFS	50 uS	128 uS	23 uS

Fragmentation

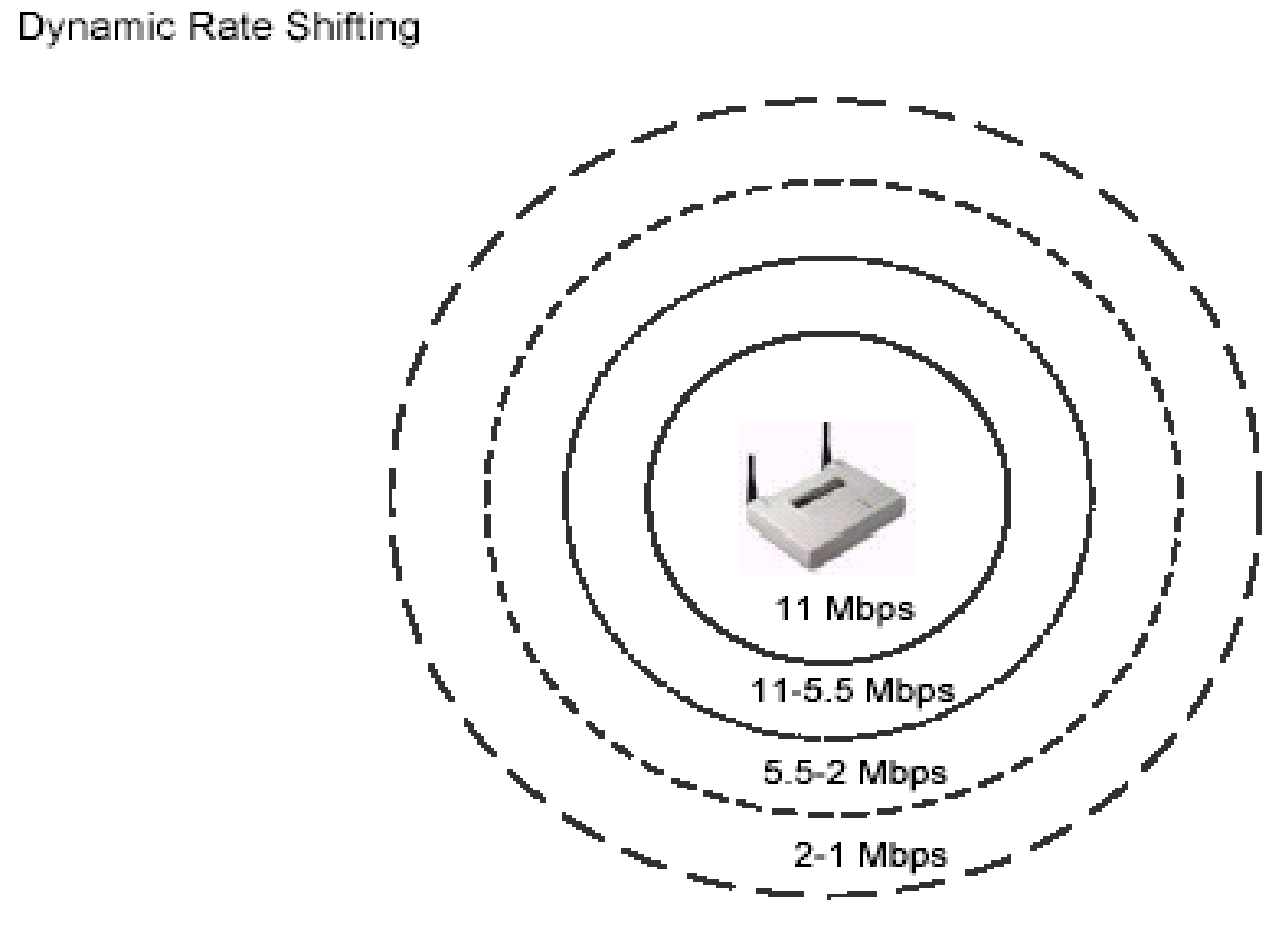


Fragmentation

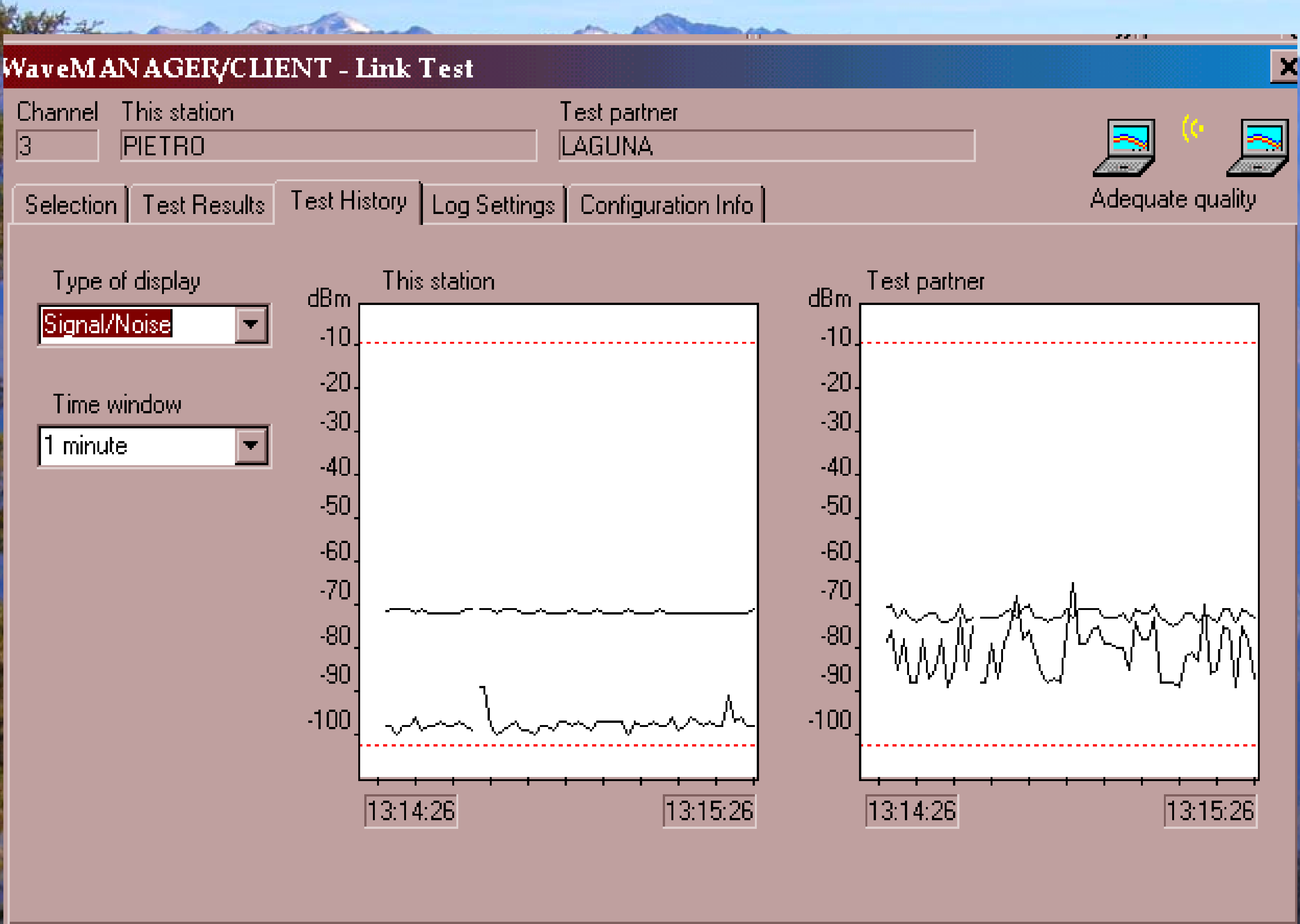
1. Increased chance of collision
2. Less overhead

1. Decreased chance of collision
2. More overhead

Dynamic transmission rate



Interference



WaveMANAGER/CLIENT - Link Test

Channel: 3

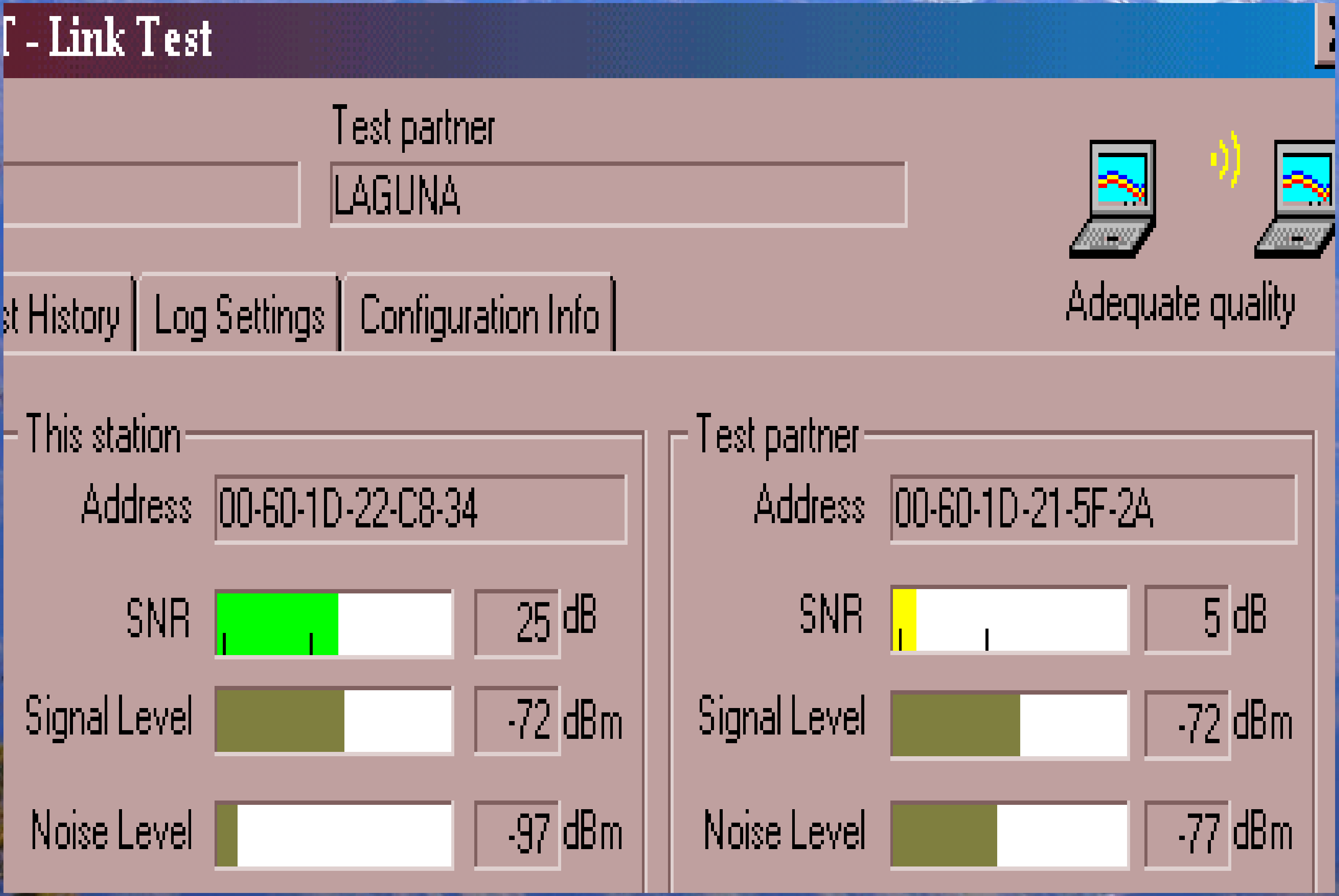
This station: PIETRO

Test partner: LAGUNA

Type of display: Signal/Noise

Time window: 1 minute

Interference



T - Link Test

Test partner: LAGUNA

Adequate quality

This station

Address: 00-60-1D-22-C8-34

SNR: 25 dB

Signal Level: -72 dBm

Noise Level: -97 dBm

Test partner

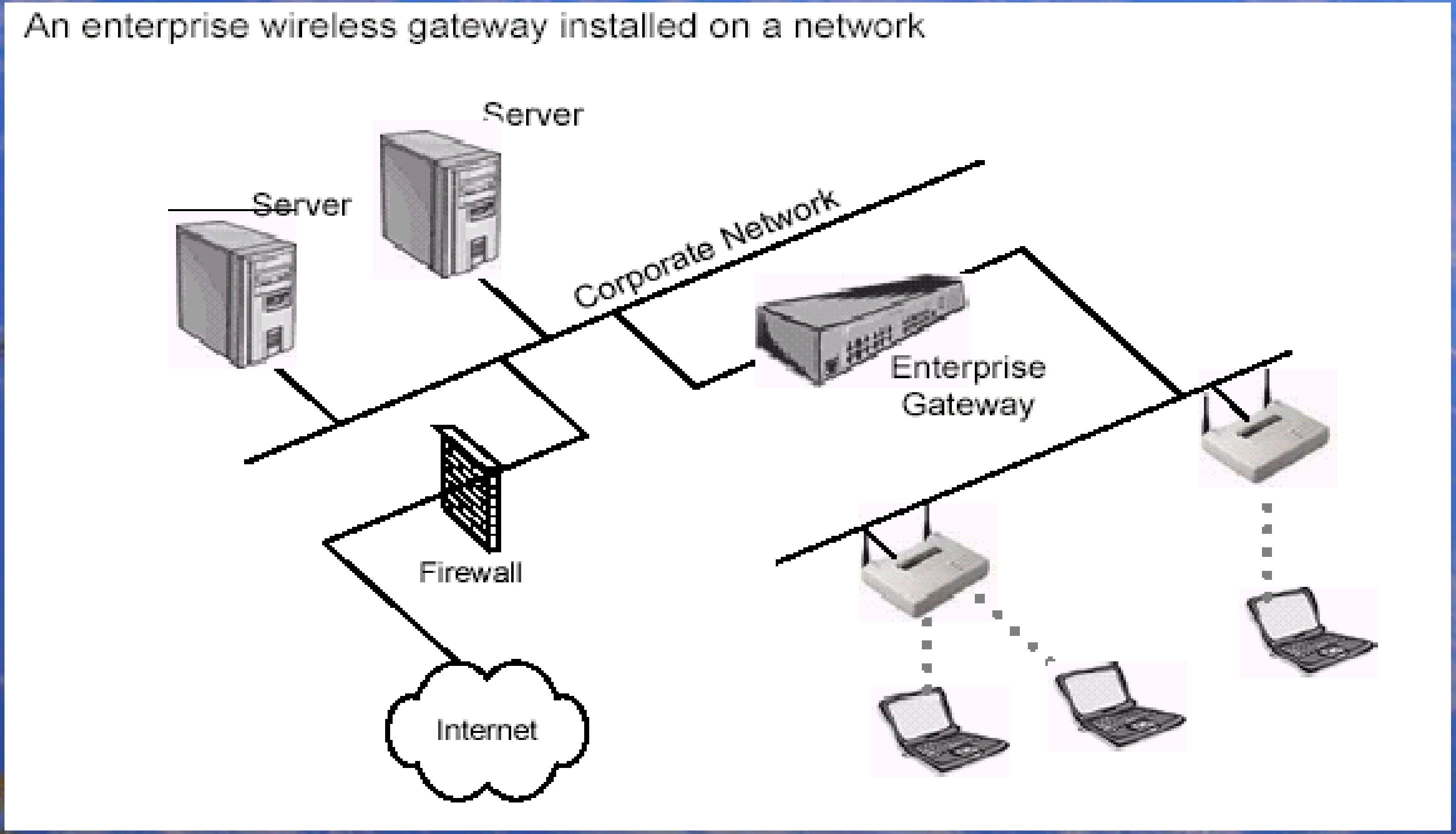
Address: 00-60-1D-21-5F-2A

SNR: 5 dB

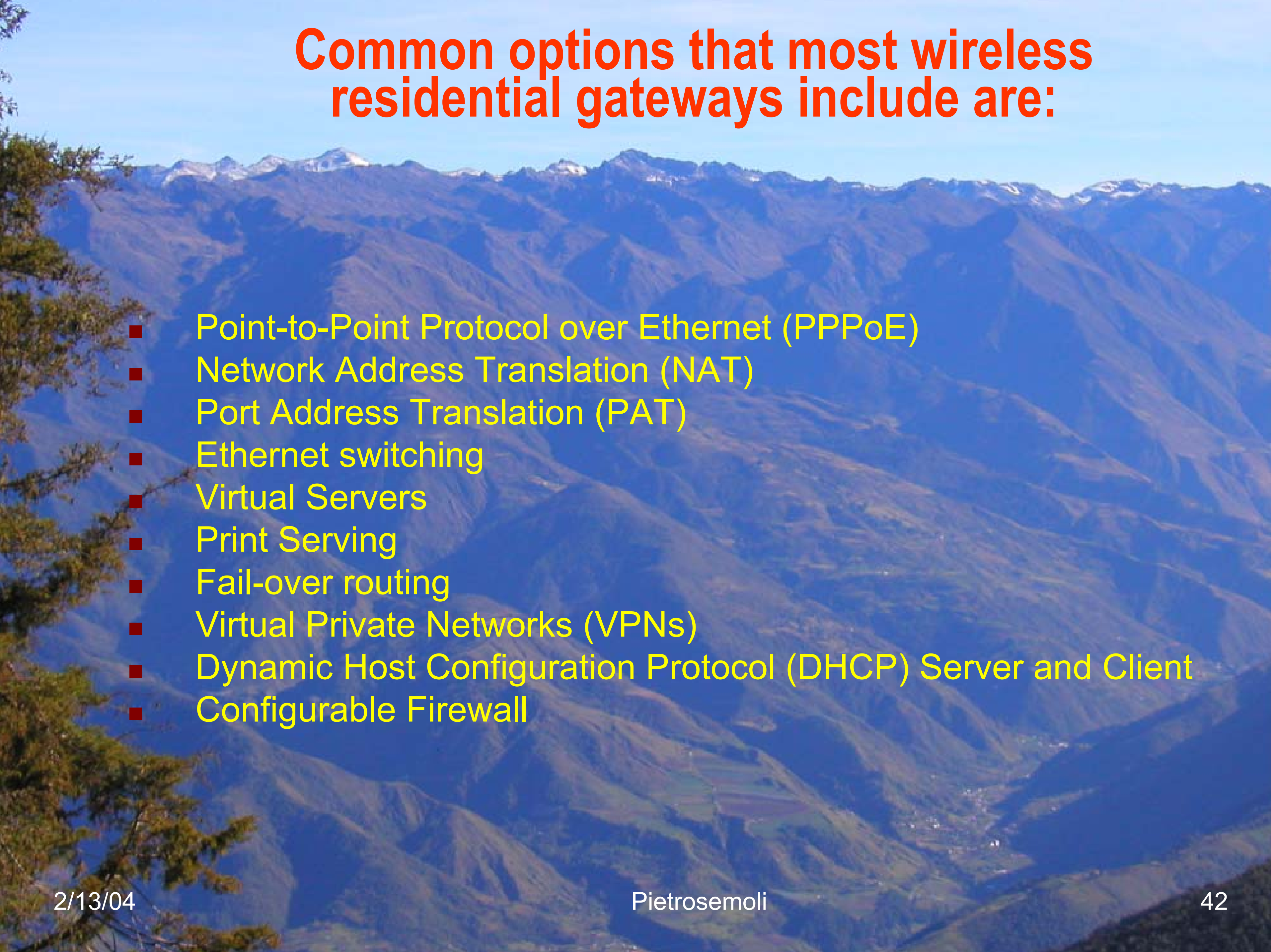
Signal Level: -72 dBm

Noise Level: -77 dBm

Enterprise Gateway



Common options that most wireless residential gateways include are:

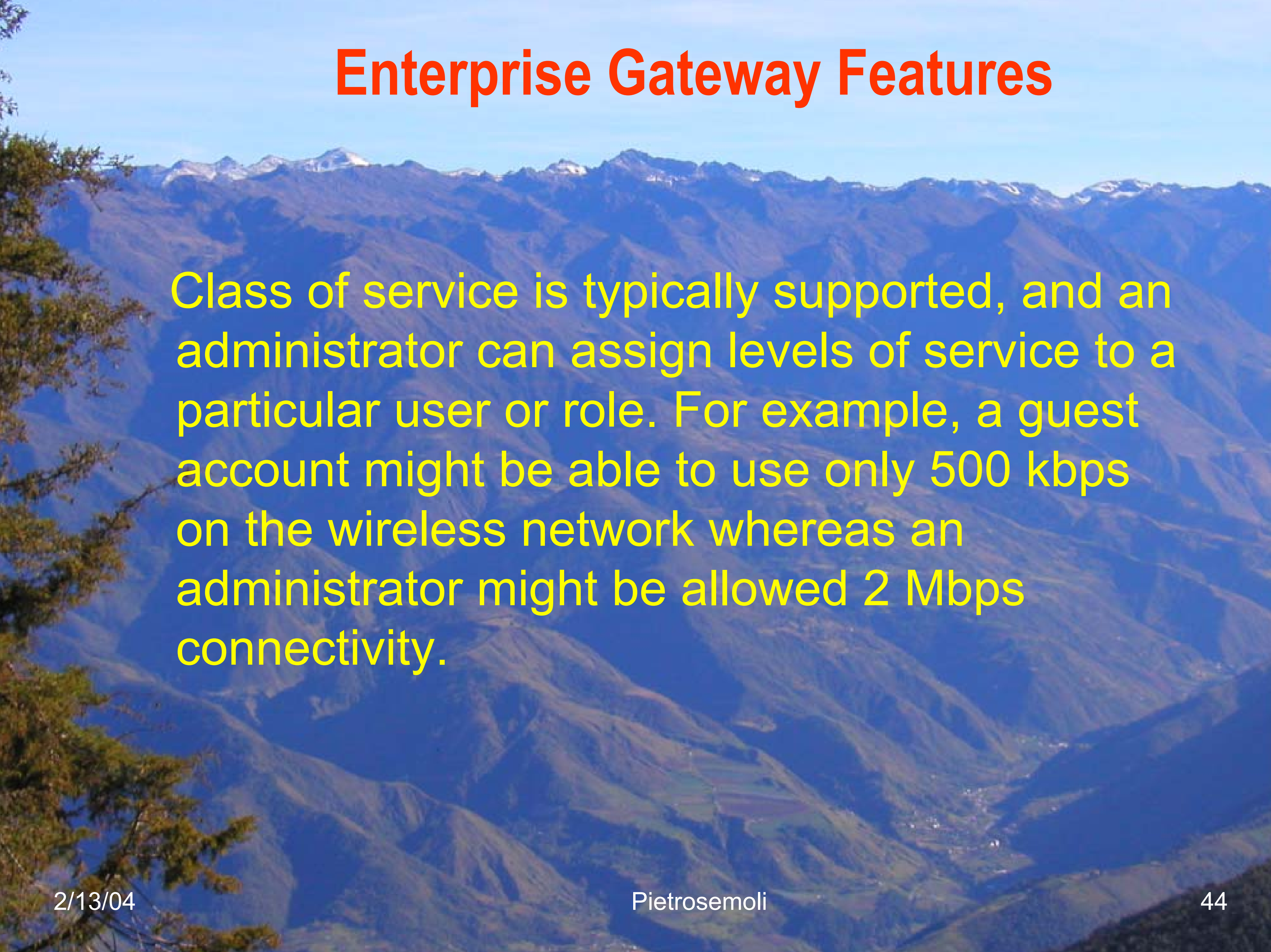


- Point-to-Point Protocol over Ethernet (PPPoE)
- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Ethernet switching
- Virtual Servers
- Print Serving
- Fail-over routing
- Virtual Private Networks (VPNs)
- Dynamic Host Configuration Protocol (DHCP) Server and Client
- Configurable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

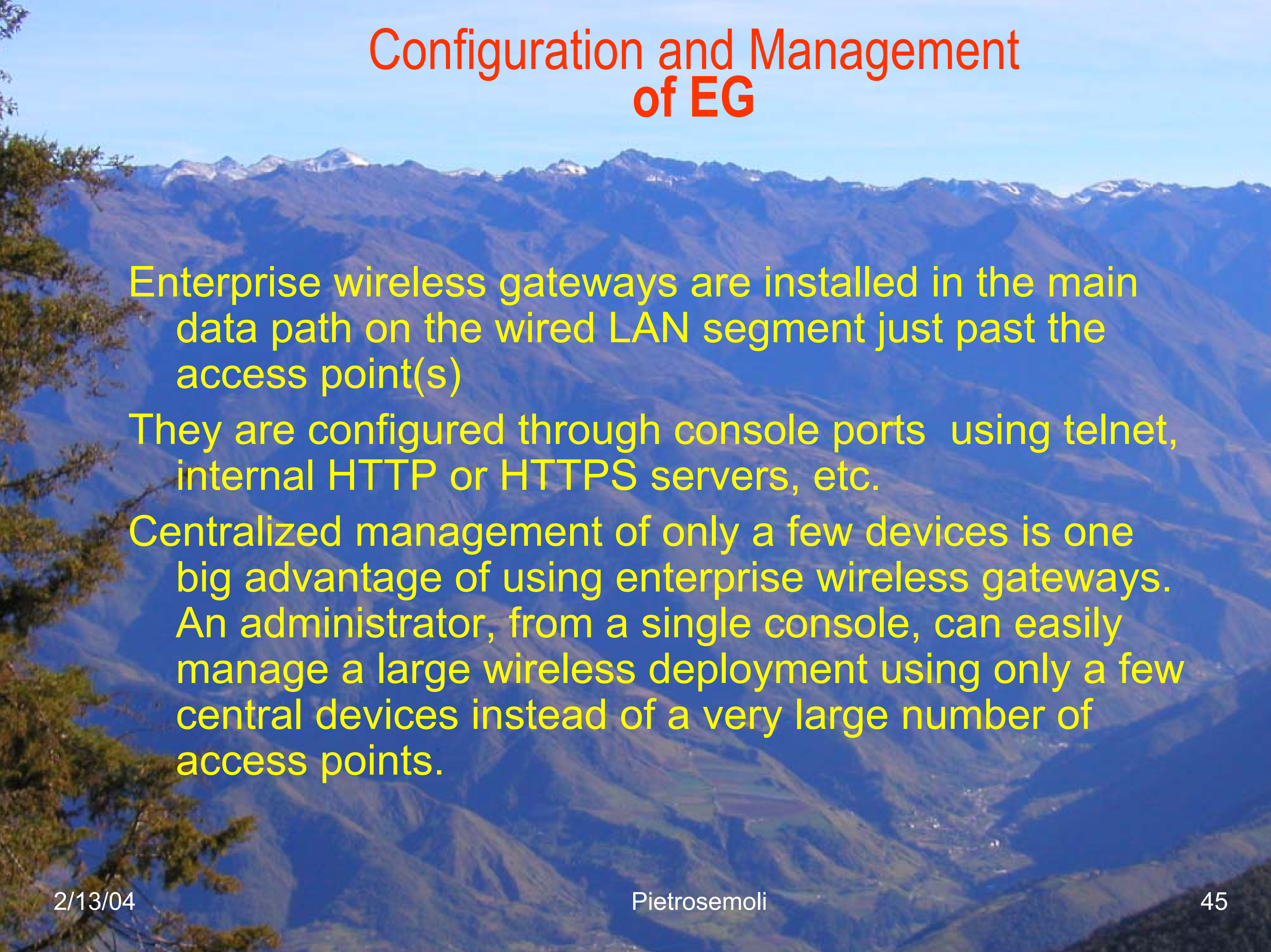
Enterprise Gateway Features

Enterprise wireless gateways do have features, such as Role-Based Access Control (RBAC), that are not found in any access points. RBAC allows an administrator to assign a certain level of wireless network access to a particular job position in the company. If the person doing that job is replaced, the new person automatically gains the same network rights as the replaced person. Having the ability to limit a wireless user's access to corporate resources, as part of the "role", can be a useful security feature.

Enterprise Gateway Features



Class of service is typically supported, and an administrator can assign levels of service to a particular user or role. For example, a guest account might be able to use only 500 kbps on the wireless network whereas an administrator might be allowed 2 Mbps connectivity.



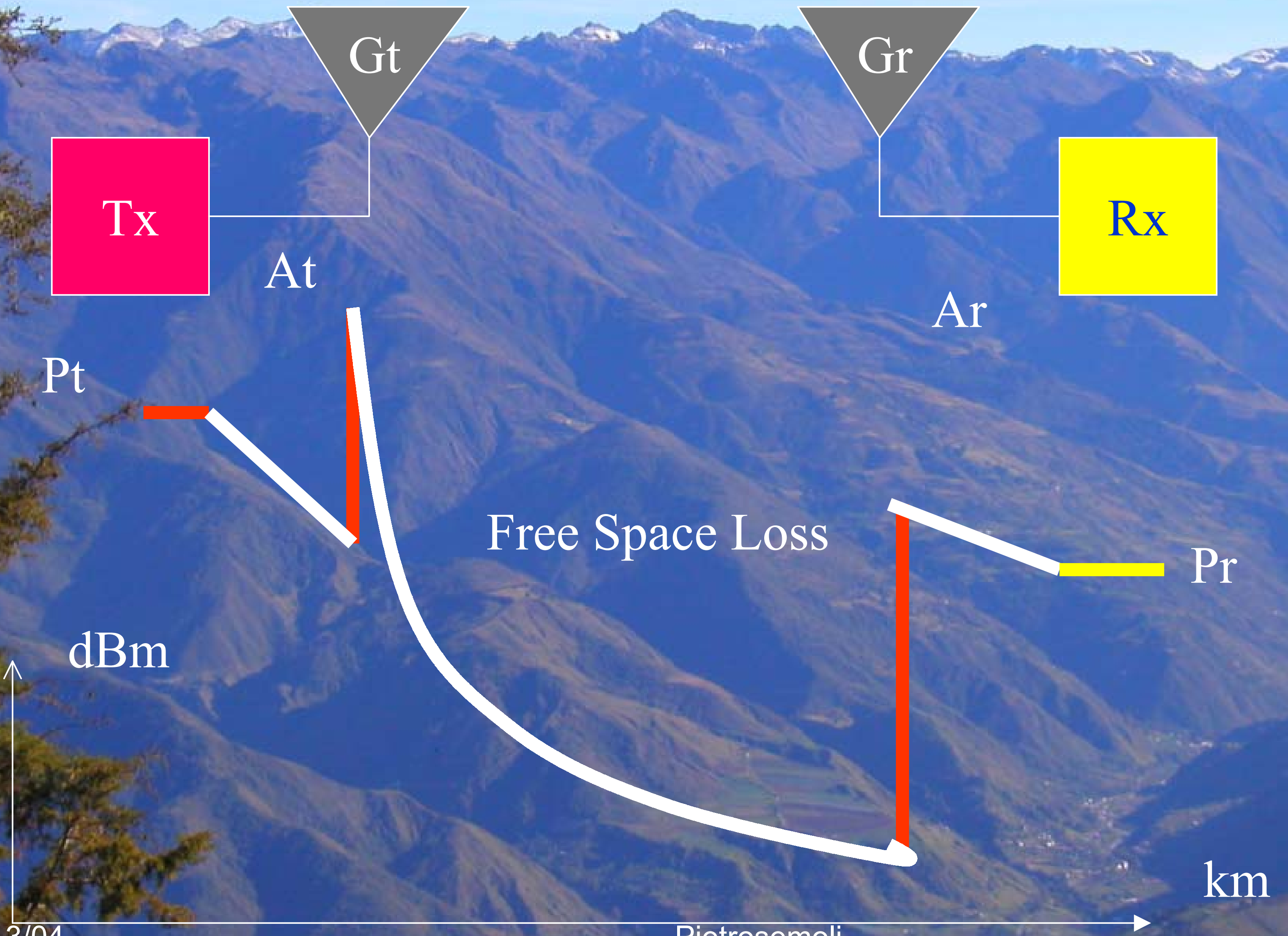
Configuration and Management **of EG**

- 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.

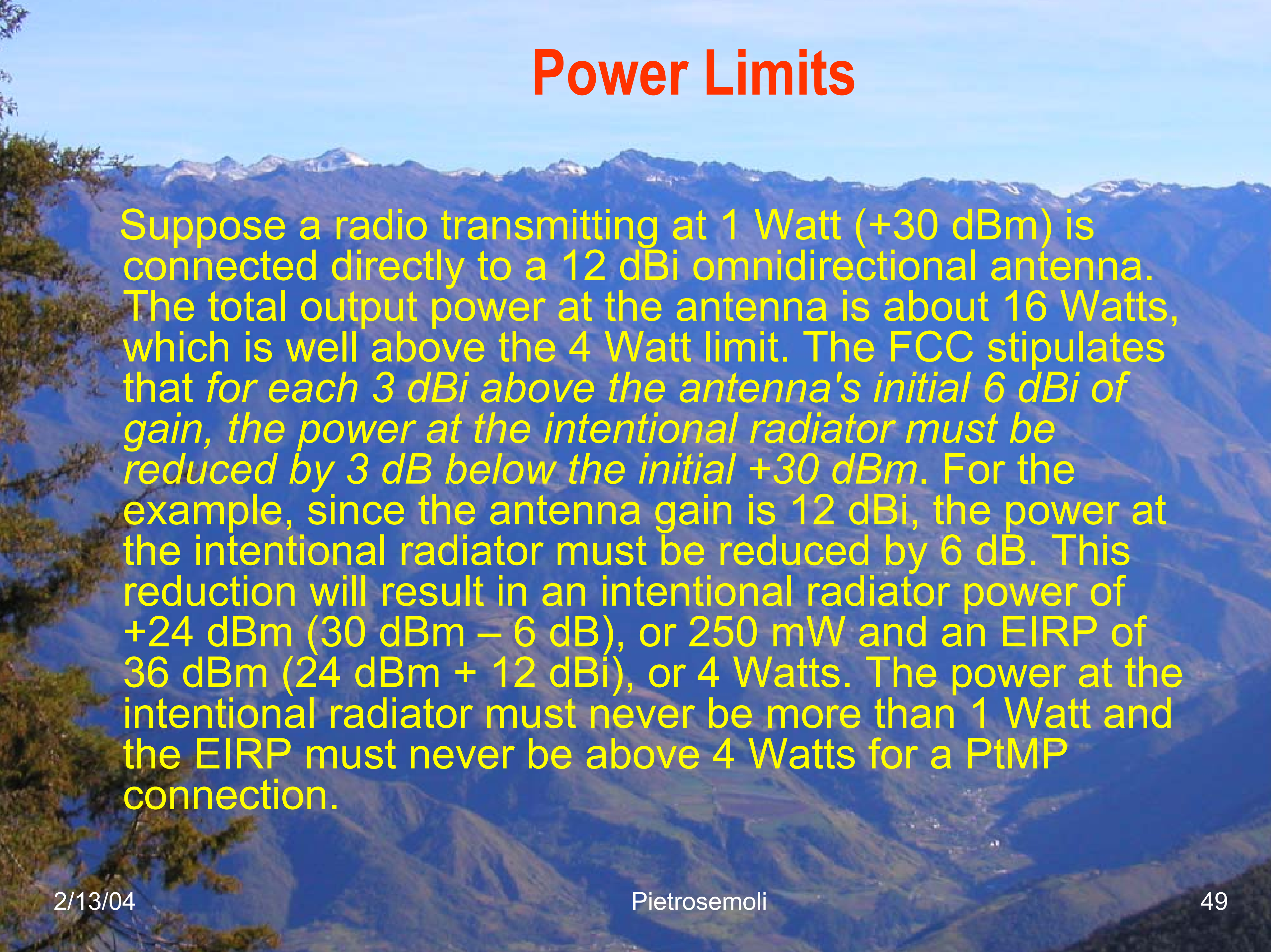
Power over distance



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.

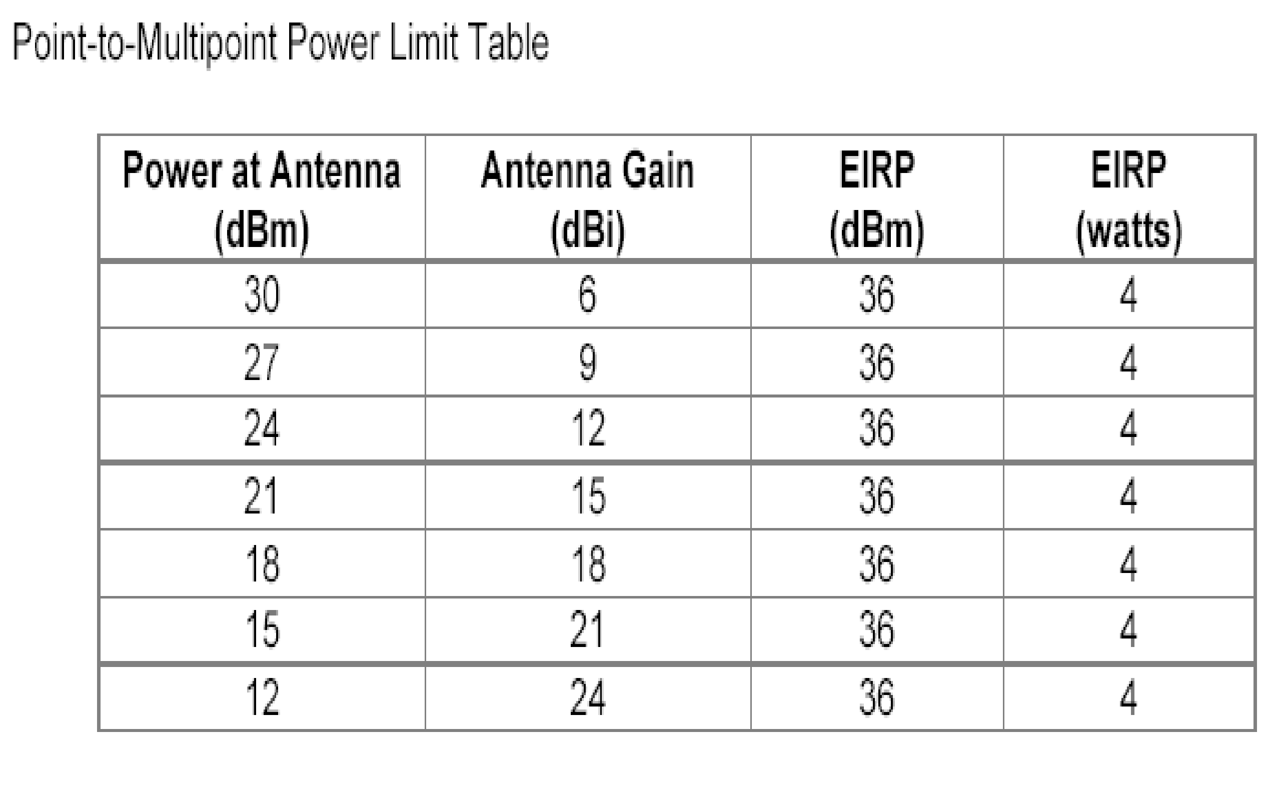
Regarding the setup of a PtMP link, the FCC limits the EIRP to 4 Watts in both the 2.4 GHz ISM band and upper 5 GHz UNII band. The power limit set for the intentional radiator (the device transmitting the RF signal) in each of these bands is 1 Watt. If the transmitting wireless LAN devices are adjustable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

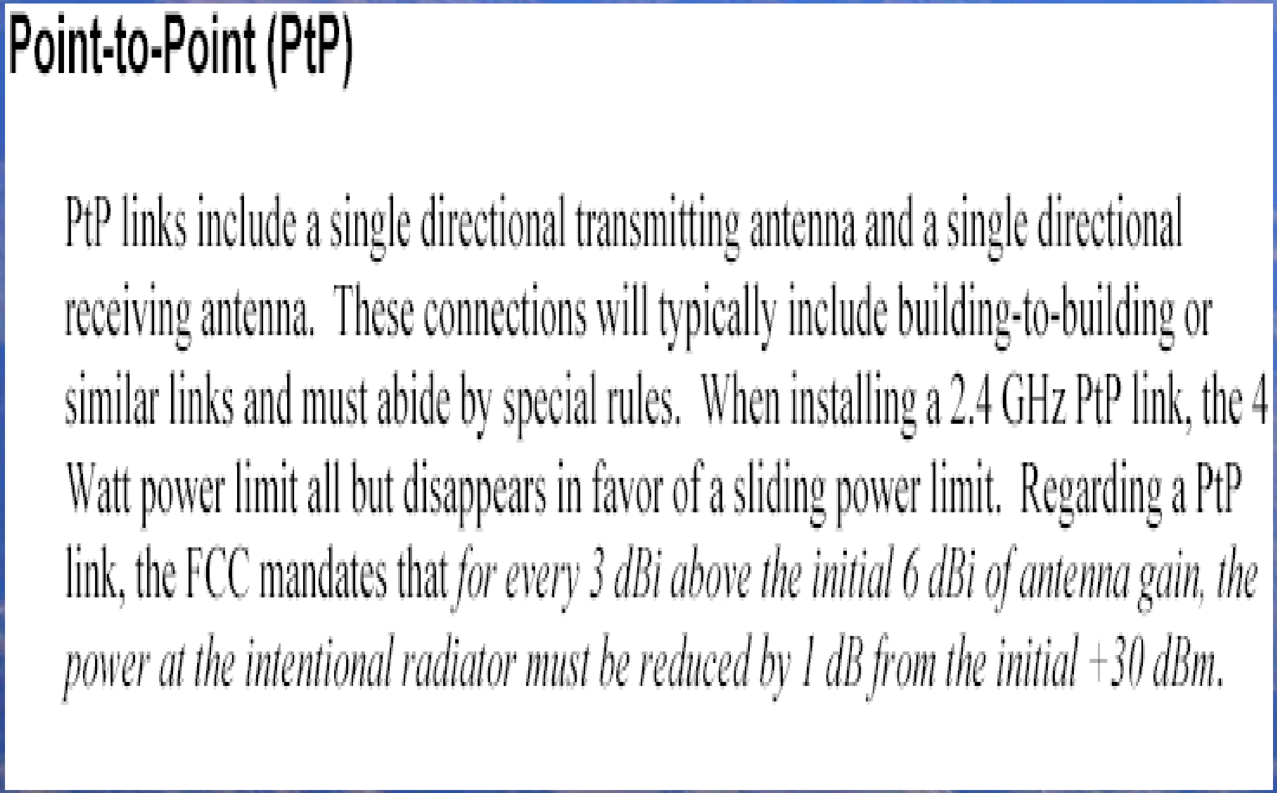
Power Limits



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

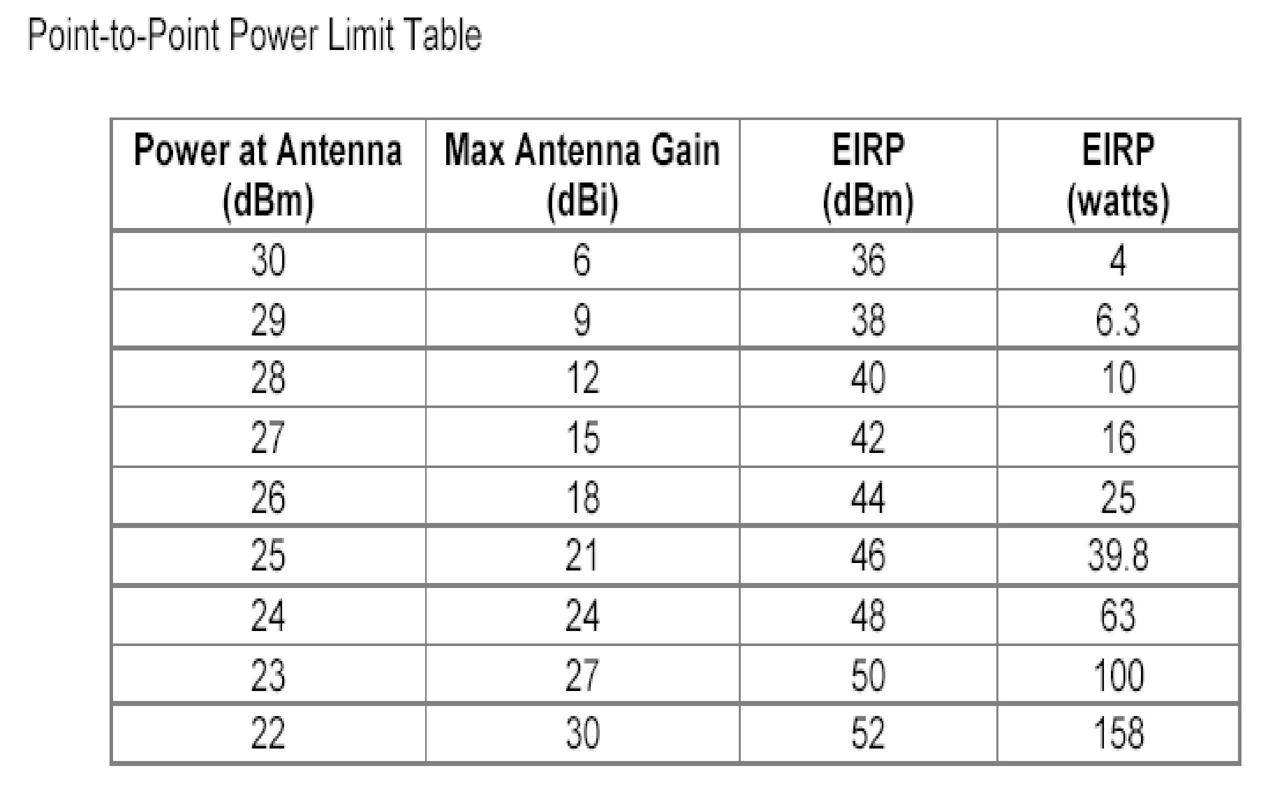
Power Limits



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.*

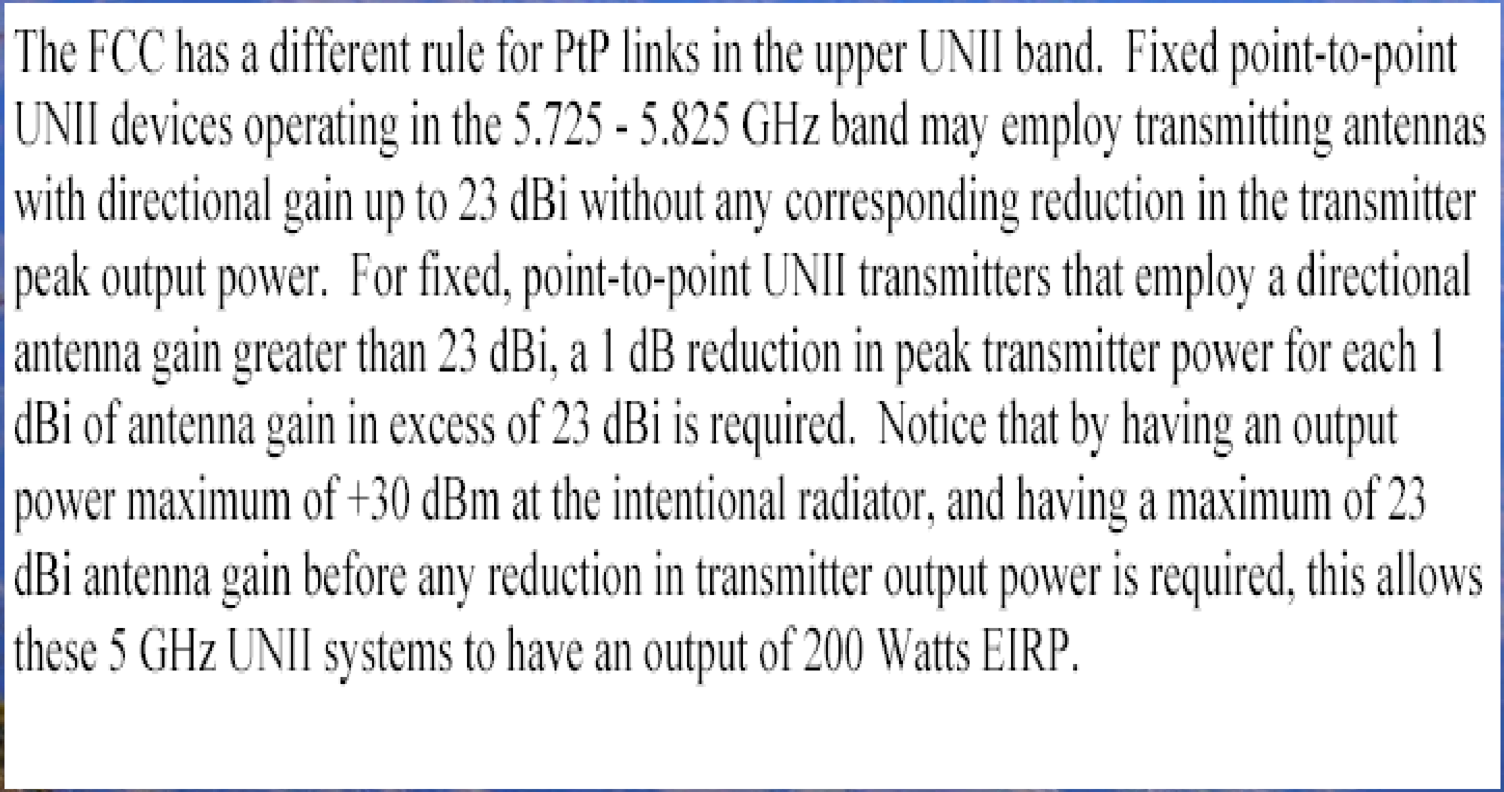
Power Limits



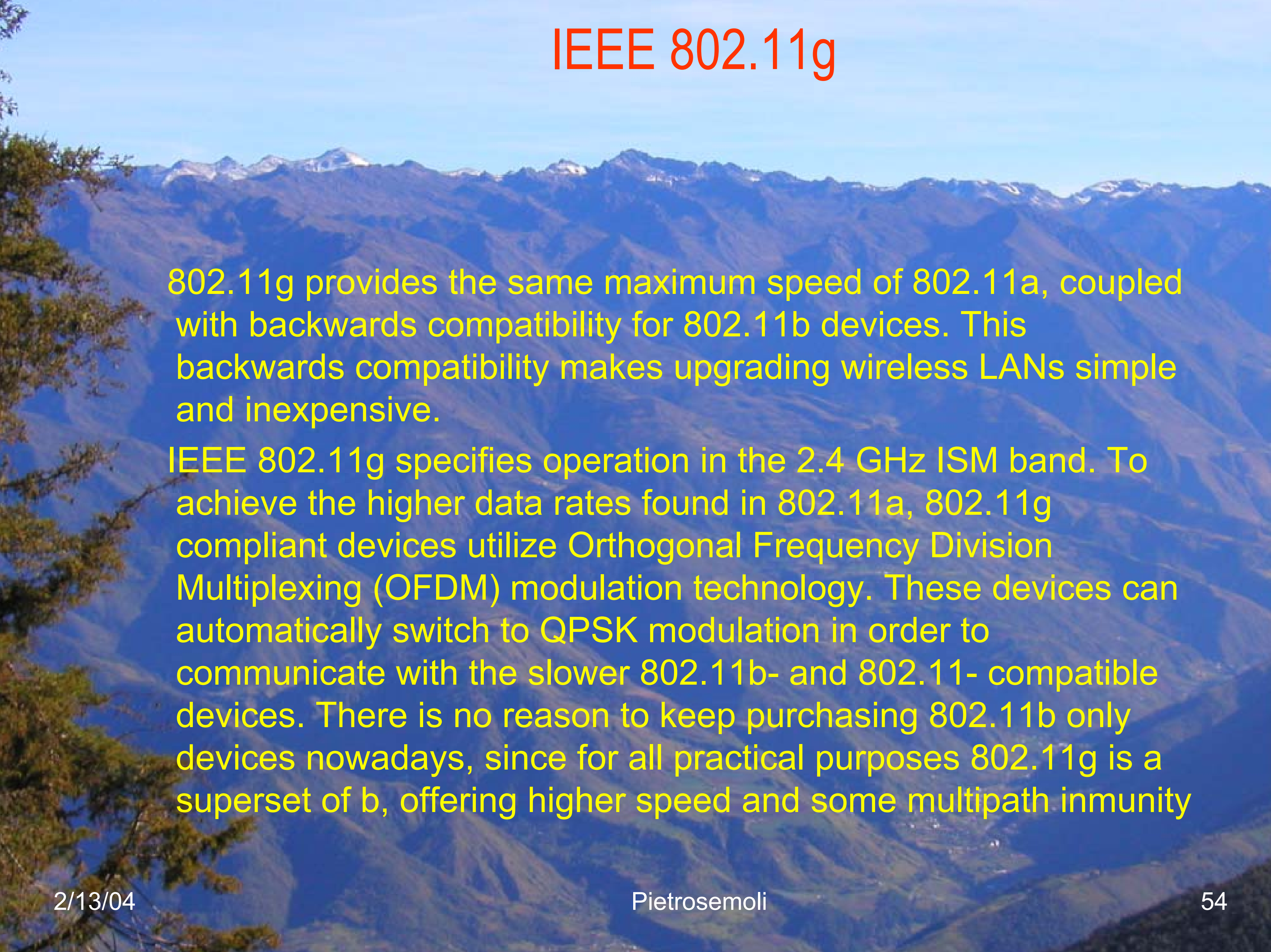
Point-to-Point Power Limit Table

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



The FCC has a different rule for PtP links in the upper UNII band. Fixed point-to-point UNII devices operating in the 5.725 - 5.825 GHz band may employ transmitting antennas with directional gain up to 23 dBi without any corresponding reduction in the transmitter peak output power. For fixed, point-to-point UNII transmitters that employ a directional antenna gain greater than 23 dBi, a 1 dB reduction in peak transmitter power for each 1 dBi of antenna gain in excess of 23 dBi is required. Notice that by having an output power maximum of +30 dBm at the intentional radiator, and having a maximum of 23 dBi antenna gain before any reduction in transmitter output power is required, this allows these 5 GHz UNII systems to have an output of 200 Watts EIRP.



IEEE 802.11g

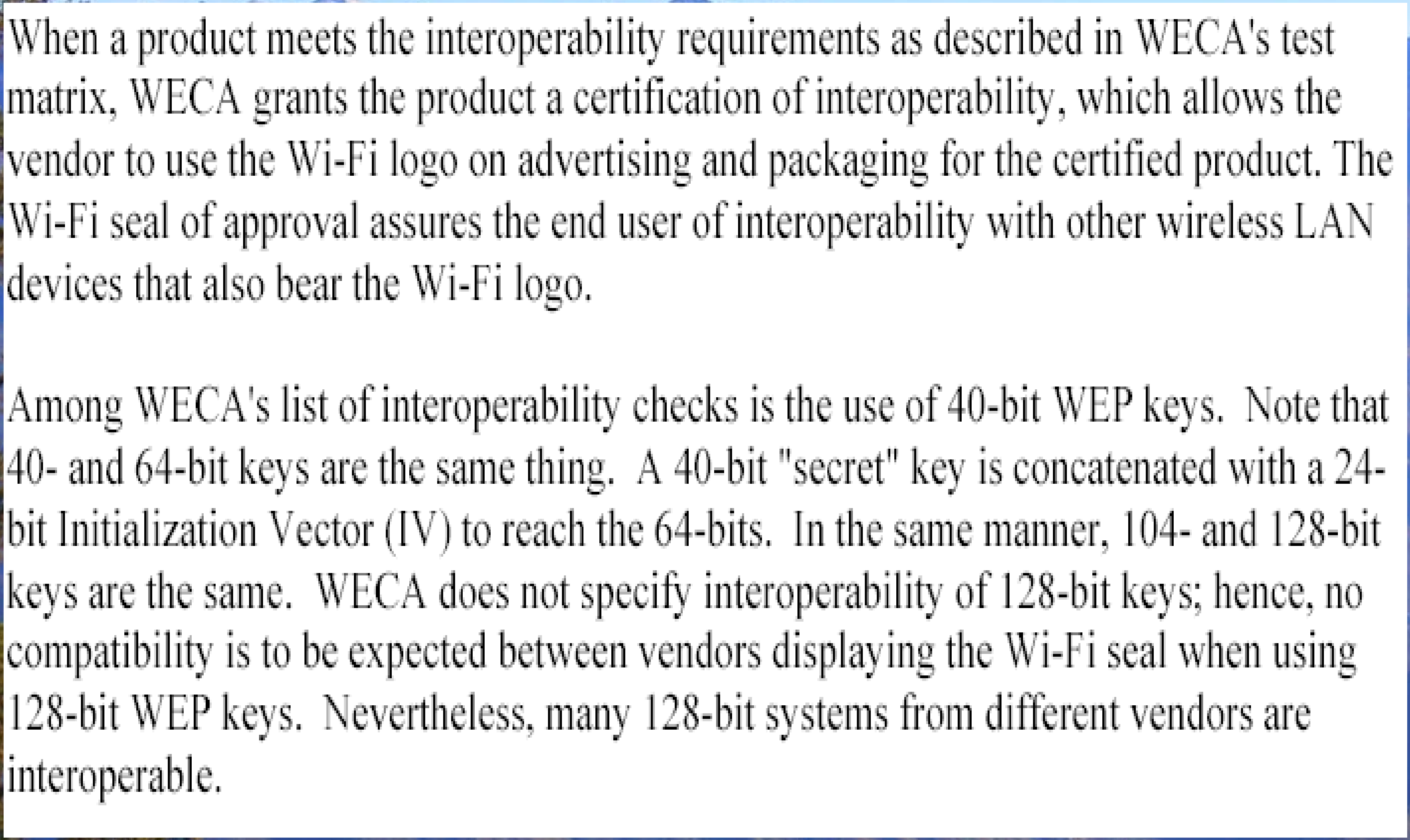
802.11g provides the same maximum speed of 802.11a, coupled with backwards compatibility for 802.11b devices. This backwards compatibility makes upgrading wireless LANs simple and inexpensive.

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

Wireless Ethernet Compatibility Alliance

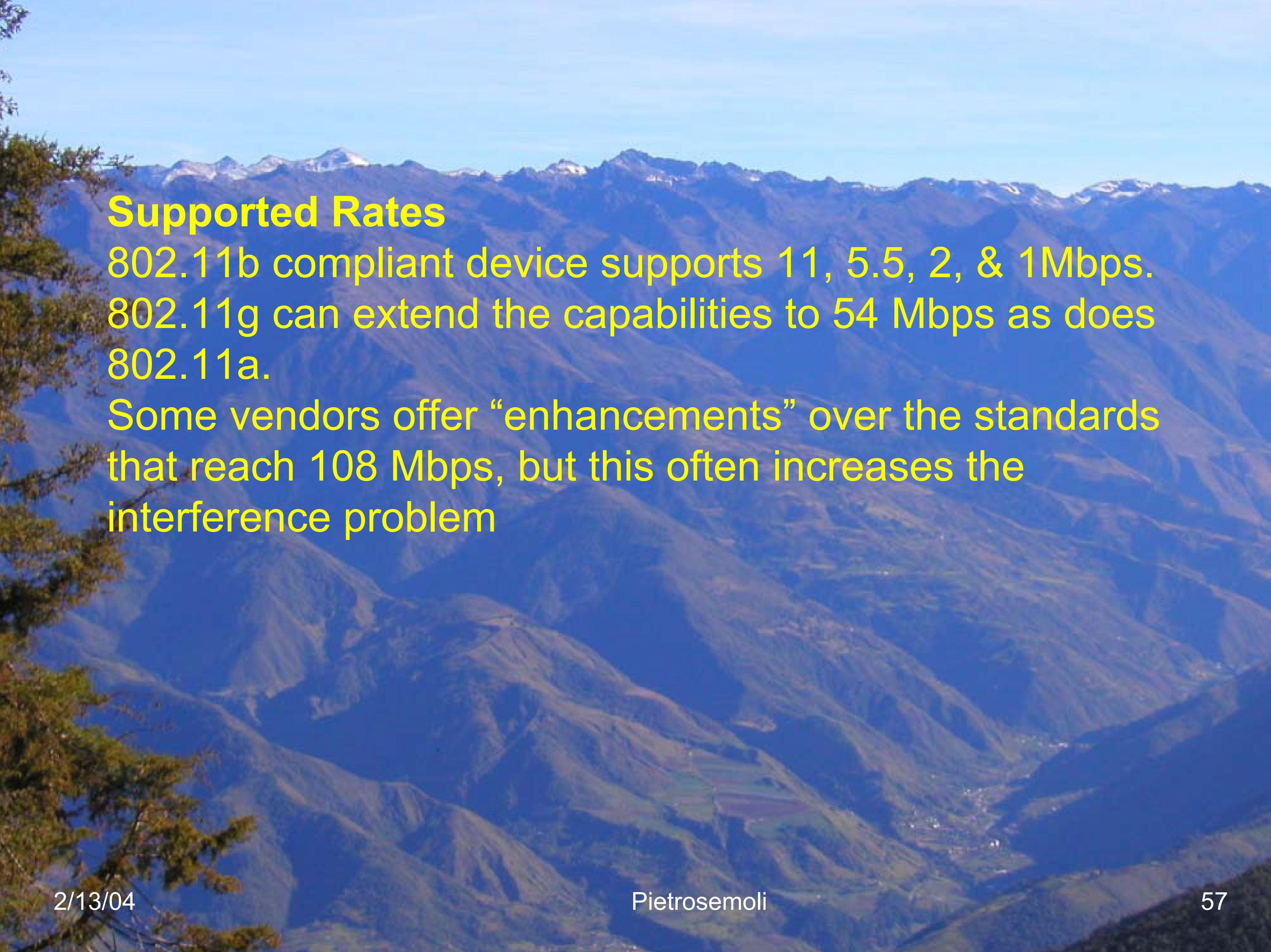
The Wireless Ethernet Compatibility Alliance (*WECA*) promotes and tests for wireless LAN interoperability of 802.11b devices and 802.11a devices. WECA’s mission is *to certify interoperability of Wi-Fi™ (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments*. As an administrator, you must resolve conflicts among wireless LAN devices that result from interference, incompatibility, or other problems.

Wireless Ethernet Compatibility Alliance



When a product meets the interoperability requirements as described in WECA's test matrix, WECA grants the product a certification of interoperability, which allows the vendor to use the Wi-Fi logo on advertising and packaging for the certified product. The Wi-Fi seal of approval assures the end user of interoperability with other wireless LAN devices that also bear the Wi-Fi logo.

Among WECA's list of interoperability checks is the use of 40-bit WEP keys. Note that 40- and 64-bit keys are the same thing. A 40-bit "secret" key is concatenated with a 24-bit Initialization Vector (IV) to reach the 64-bits. In the same manner, 104- and 128-bit keys are the same. WECA does not specify interoperability of 128-bit keys; hence, no compatibility is to be expected between vendors displaying the Wi-Fi seal when using 128-bit WEP keys. Nevertheless, many 128-bit systems from different vendors are interoperable.

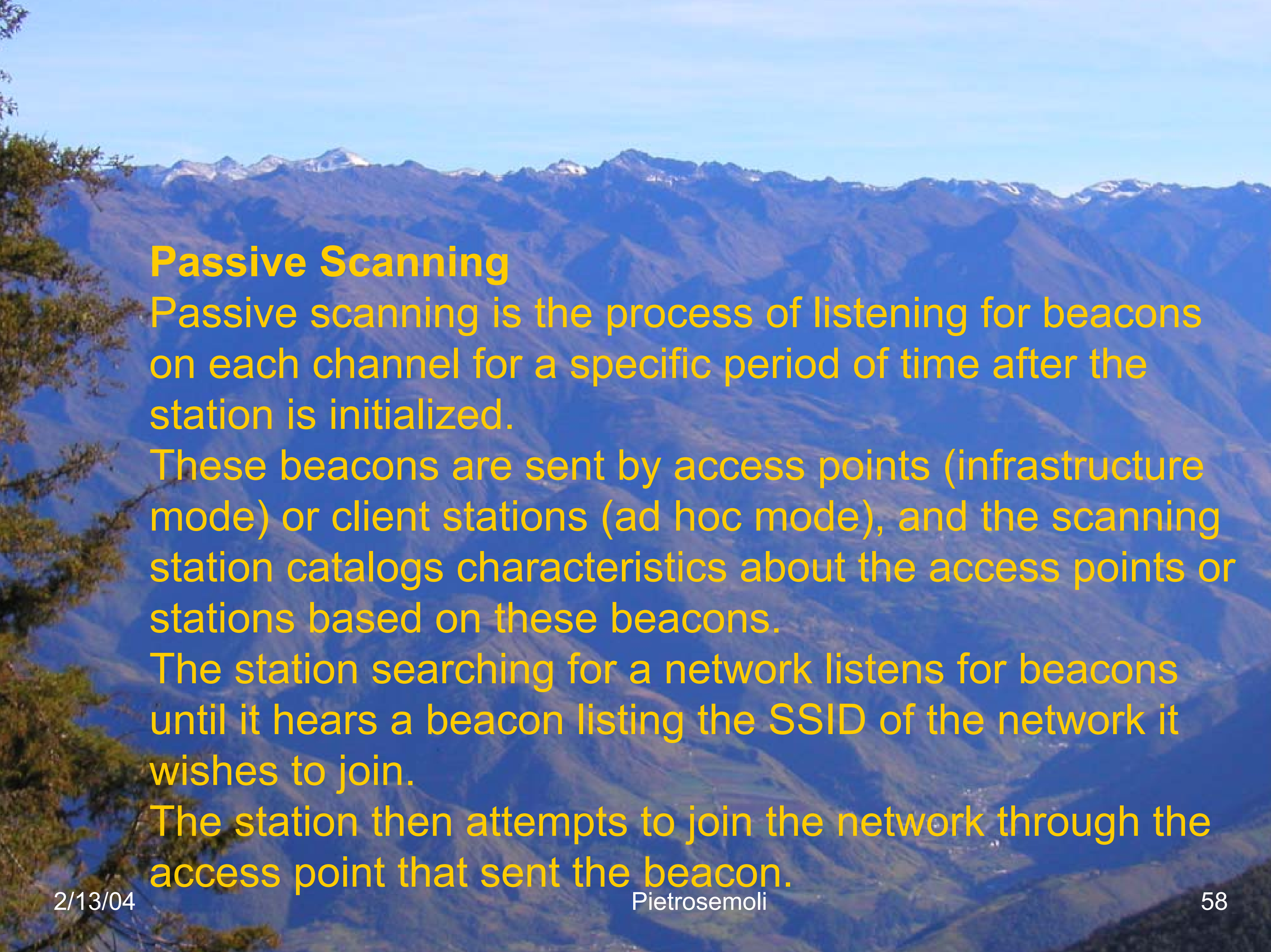


Supported Rates

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



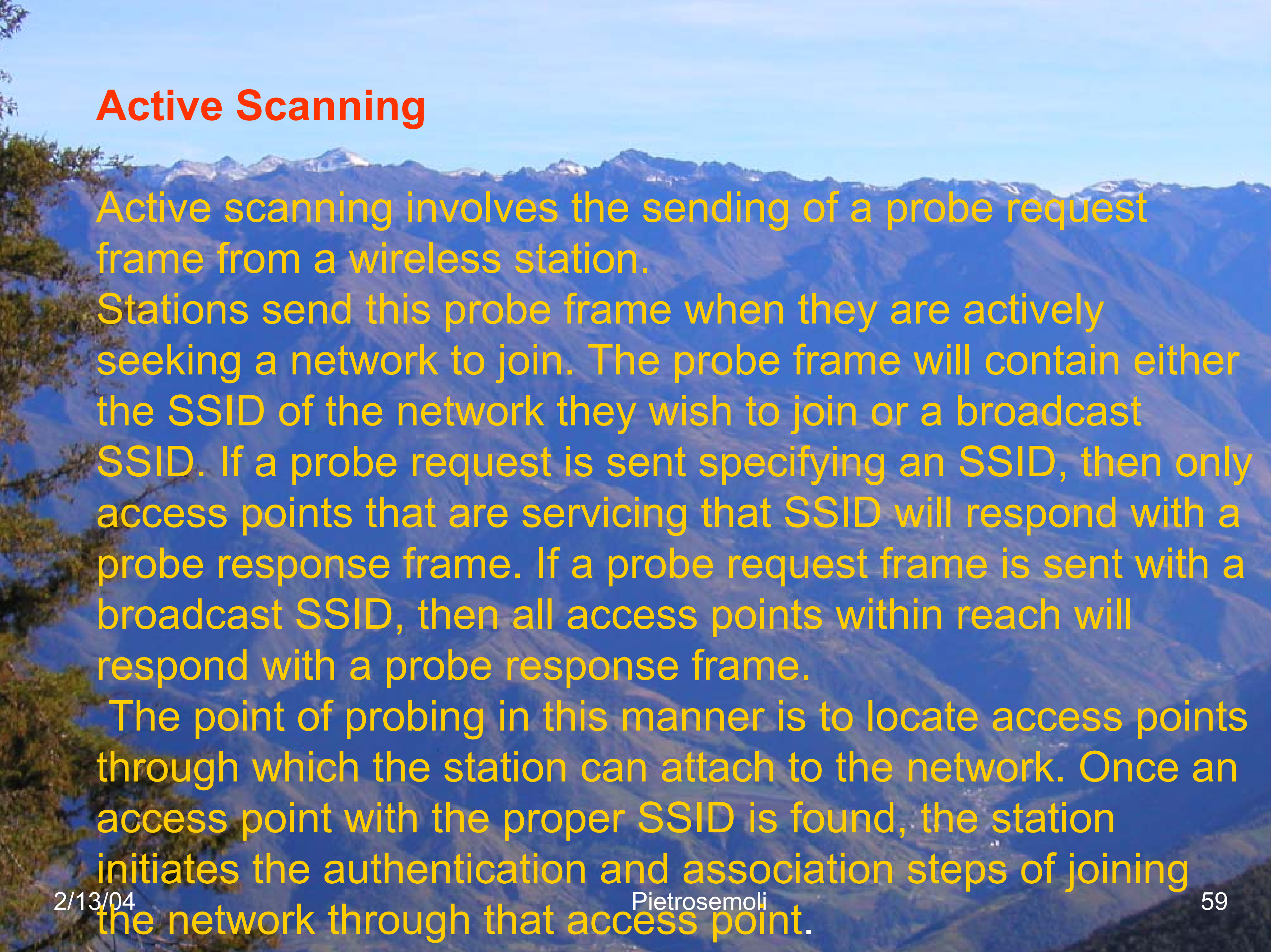
Passive Scanning

Passive scanning is the process of listening for beacons on each channel for a specific period of time after the station is initialized.

These beacons are sent by access points (infrastructure mode) or client stations (ad hoc mode), and the scanning station catalogs characteristics about the access points or stations based on these beacons.

The station searching for a network listens for beacons until it hears a beacon listing the SSID of the network it wishes to join.

The station then attempts to join the network through the access point that sent the beacon.



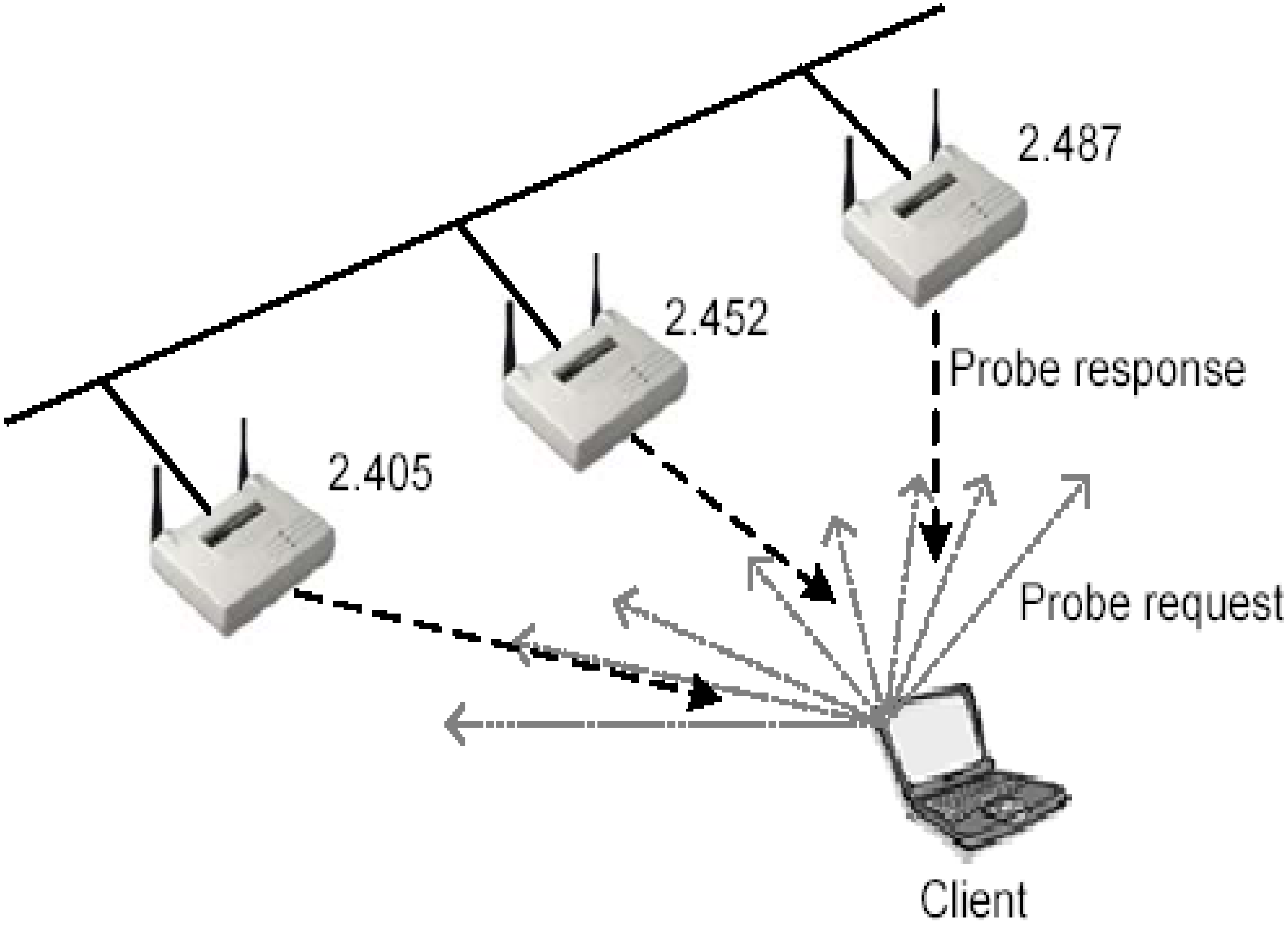
Active Scanning

Active scanning involves the sending of a probe request frame from a wireless station.

Stations send this probe frame when they are actively seeking a network to join. The probe frame will contain either the SSID of the network they wish to join or a broadcast SSID. If a probe request is sent specifying an SSID, then only access points that are servicing that SSID will respond with a probe response frame. If a probe request frame is sent with a broadcast SSID, then all access points within reach will respond with a probe response frame.

The point of probing in this manner is to locate access points through which the station can attach to the network. Once an access point with the proper SSID is found, the station initiates the authentication and association steps of joining the network through that access point.

Active Scanning



Questions?