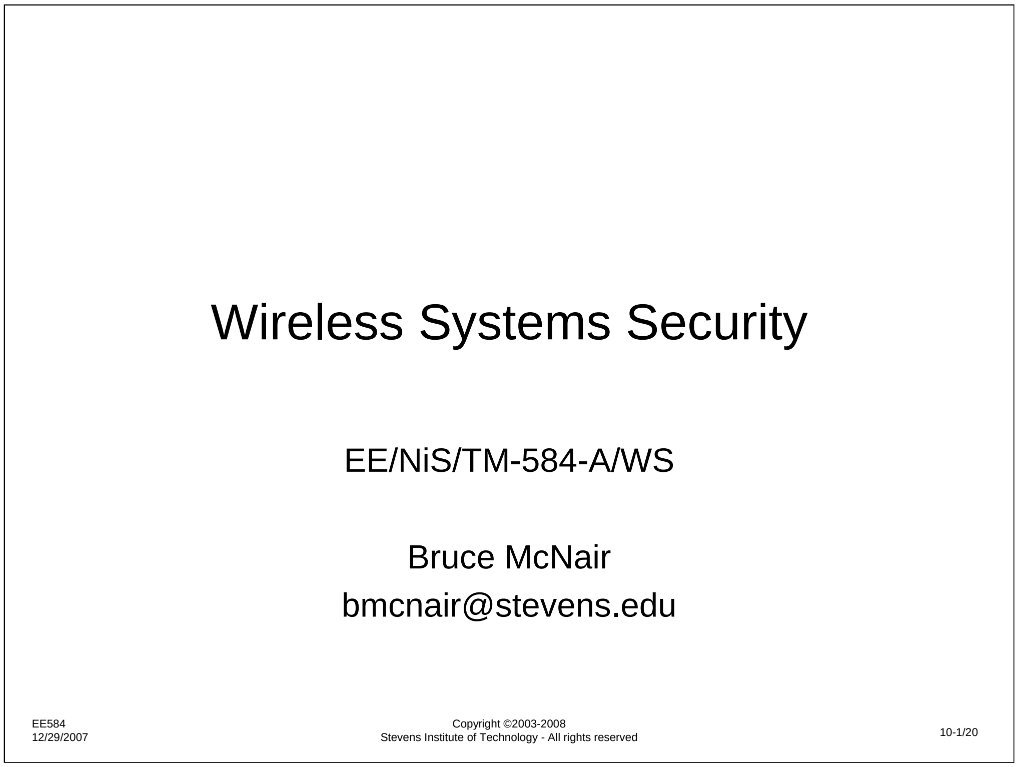
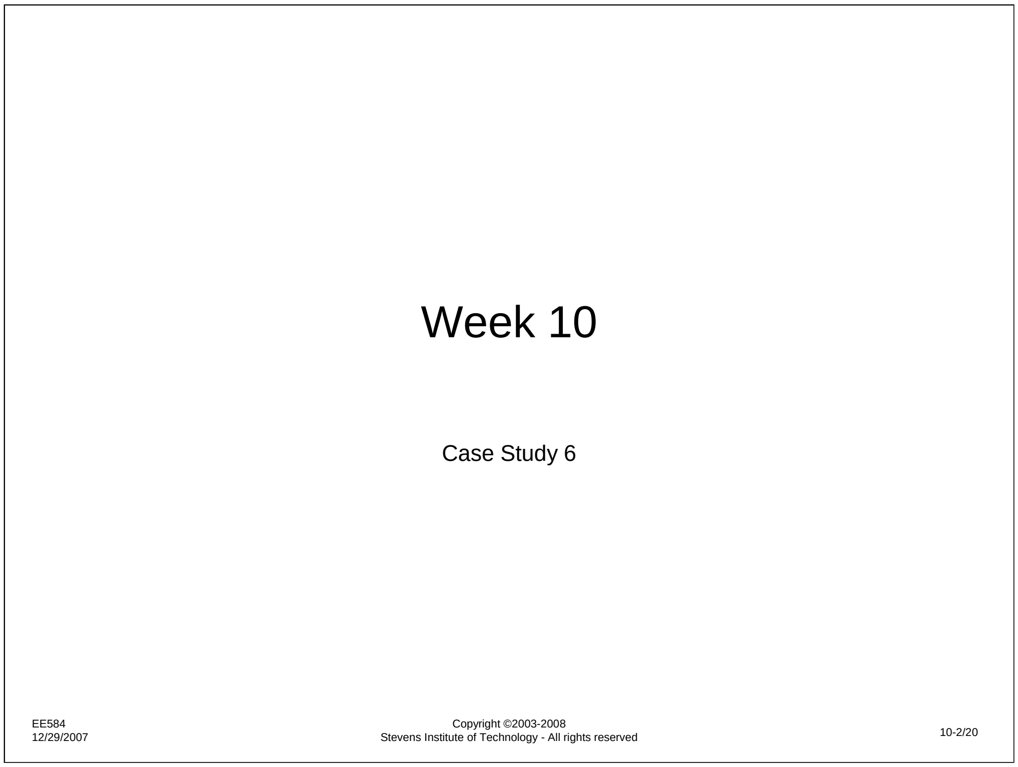


Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

.

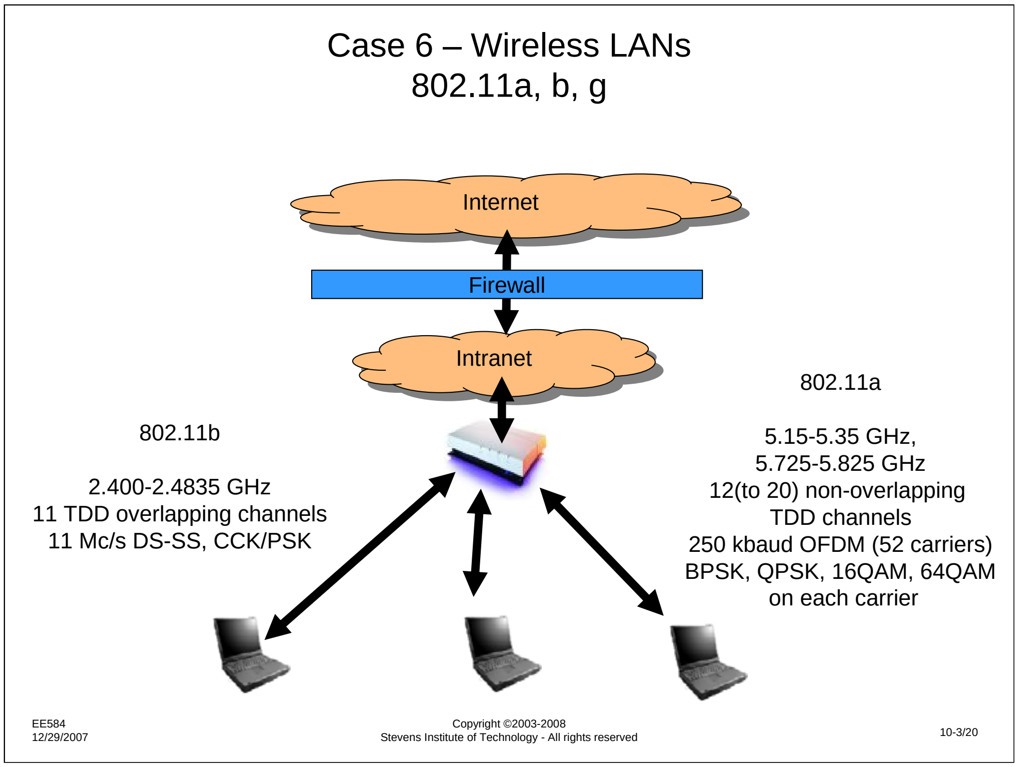


Week 10

Case Study 6

This week we will address the sixth case study. As it was for the previous weeks, you should discuss the security issues in the WebCT discussion groups I have set up. These are labeled Red Team 6 and Blue Team 6. DO NOT POST THIS WEEK'S DISCUSSION TO THE TEAM 2, 3, 4, or 5 GROUPS. It may not be read by other students and will certainly be confusing. Don't post items that should be in your group's discussion to other discussion groups, such as Main, either, since (a) we are trying to keep the Red and Blue team perspective different and (b) other students may not go looking for the assessment discussions there.

This week, I again randomized the teams as I did for the first assessment. I will continue to do this for the rest of the assessments.



Case 6 – Wireless LANs
802.11a, b, g

Internet

Firewall

Intranet

802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK

802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
12(to 20) non-overlapping
TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier

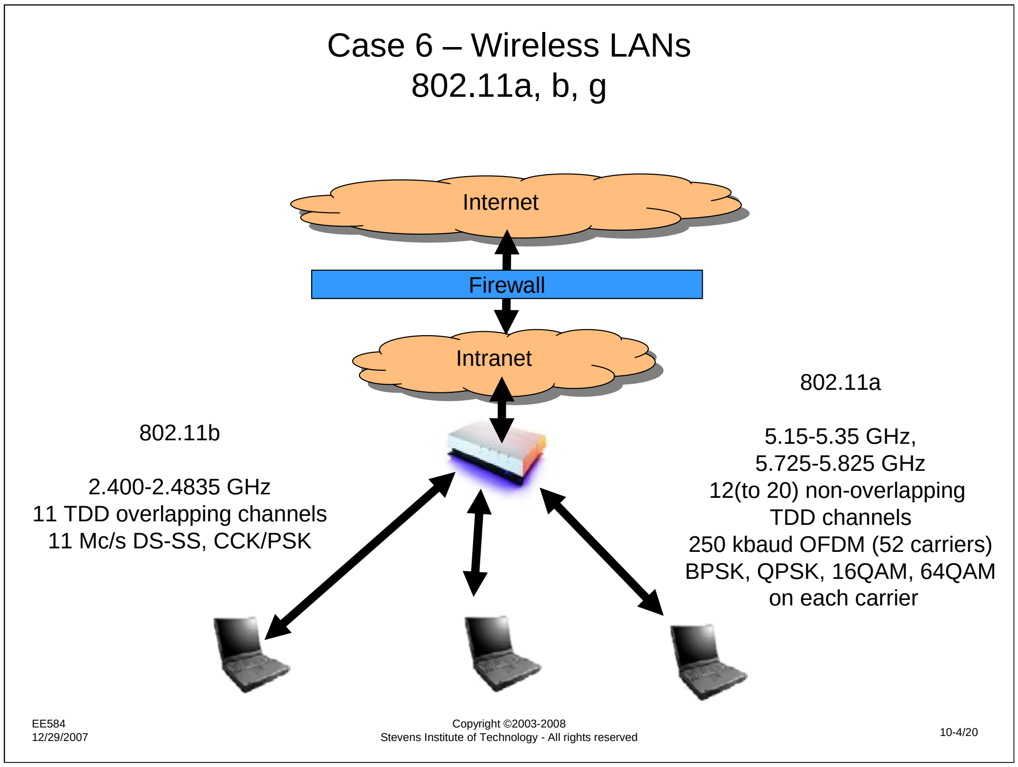
EE584
12/29/2007

10-3/20

For this week's assessment, we will be dealing with a set of wireless systems that have been something of a technical and market phenomena – the wireless LANs.

In the span of about 6 years, wireless LANs went from initial deployment to a central part of data networking. In 1998-1999, some of the first WLAN products operated in the 900 MHz ISM band and were capable of 1-2 Mb/s. With the growing popularity of the Internet and corporate intranets, plus the rapid evolution of portable PCs, all providing relatively user friendly browsers and operating systems, the rapid growth of wireless in-building networking is almost a model for other technologies deployments. Although the initial WLANs were not completely standardized, the development of the IEEE 802.11 standards helped to change that, which was a major factor in the rapid growth.

As I will discuss later, there have been various fundamental versions of the 802.11 standard, but the most significant have been 802.11a and 802.11b. 802.11(no suffix letter) standardized the initial WLAN deployments with 1-2 Mb/s direct sequence spread spectrum. In this case, the DS-SS was not to allow multiple user sharing or avoid jamming or detection, but was rather an FCC requirement. Any system using the ISM unlicensed spectrum had to spread its signal power, obstensively to reduce interference to other users of the band. Through a technicality in interpretation of the rules, 802.11b was able to offer 11 Mb/s operation in the same spectrum using phase shift keying with a coding technique known as complementary code keying. What is important to consider for 802.11b systems is that they share the 2.4 GHz ISM band with other systems – microwave ovens, cordless telephones, wireless baby monitors, cordless video cameras, among others. In addition, although 11 two-way alternate time division duplex channels are defined for 802.11b, there are only three channels available that do not overlap – channel spacing is 5 MHz, but the emission bandwidth is about 11 MHz.



Case 6 – Wireless LANs 802.11a, b, g

802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK

802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
12(to 20) non-overlapping
TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier

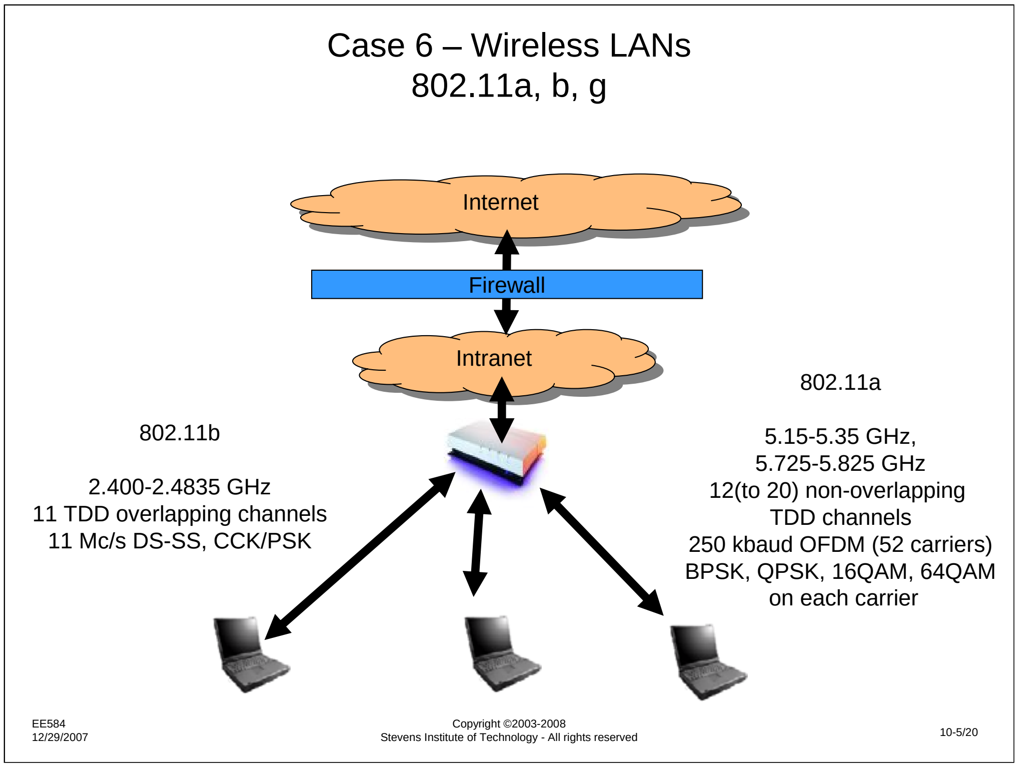
EE584
12/29/2007

10-4/20

Although the standards committee was formed first, 802.11a was not deployed until after 802.11b had established itself in the market. Unlike 802.11b, the 802.11a systems operate in the 5 GHz ISM and UNII bands – there are far fewer other ISM users at 5 GHz, and the 5 GHz UNII band is intended only for data networking applications (i.e., there are no microwave ovens to share the band with). Although antennas are half the size at 5 GHz, compared to 2.4 GHz, and despite the fact that there is less interference, there are a few issues with 802.11a systems that limit their capabilities – it is inherently more difficult to build RF devices that operate at higher frequencies with the same efficiency, and RF path loss is higher at higher frequencies, all other things being equal.

Despite these issues, 802.11a systems are being deployed, in many cases with PC cards and access points that are capable of switching between bands. The major attractions of 802.11a are bandwidth and throughput. Compared to the 3 non-overlapping channels of the 2.4 GHz band, there are 20 non-overlapping channels at 5 GHz, but most importantly, the maximum data rate of 802.11a is 54 Mb/s, compared to 11 Mb/s for 802.11b. As we will see later, the modulation format of 802.11a is what makes the difference in throughput. Instead of using a variant of single carrier PSK, like 802.11b, 802.11a sends data on 52 parallel carriers using a very effective technique known as orthogonal frequency division multiplexing (OFDM), the same technique used in DSL, European digital video broadcasting for terrestrial (DVB-T), satellite digital audio broadcasting (DAB), and cable modems.

One hybrid of 802.11a and b that is now being widely deployed is 802.11g – using the modulation techniques of 802.11a on the 2.4 GHz band. Despite the increased throughput of this approach, it is not a clean alternative, since the bandwidth requirements of 802.11a are slightly greater than 802.11b. This makes frequency planning for coexistence of the two systems a bit difficult, something that has not been widely discussed, even for simple 802.11b systems. Research that I did with a group of summer students at AT&T Labs showed that to get the best system performance, slight overlap of the operating frequencies of individual access points had to be avoided entirely. With coexisting 802.11b and g systems, this reduces the 2.4 GHz band to providing 2 non-overlapping channels.



Case 6 – Wireless LANs
802.11a, b, g

Internet

Firewall

Intranet

802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK

802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
12(to 20) non-overlapping
TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier

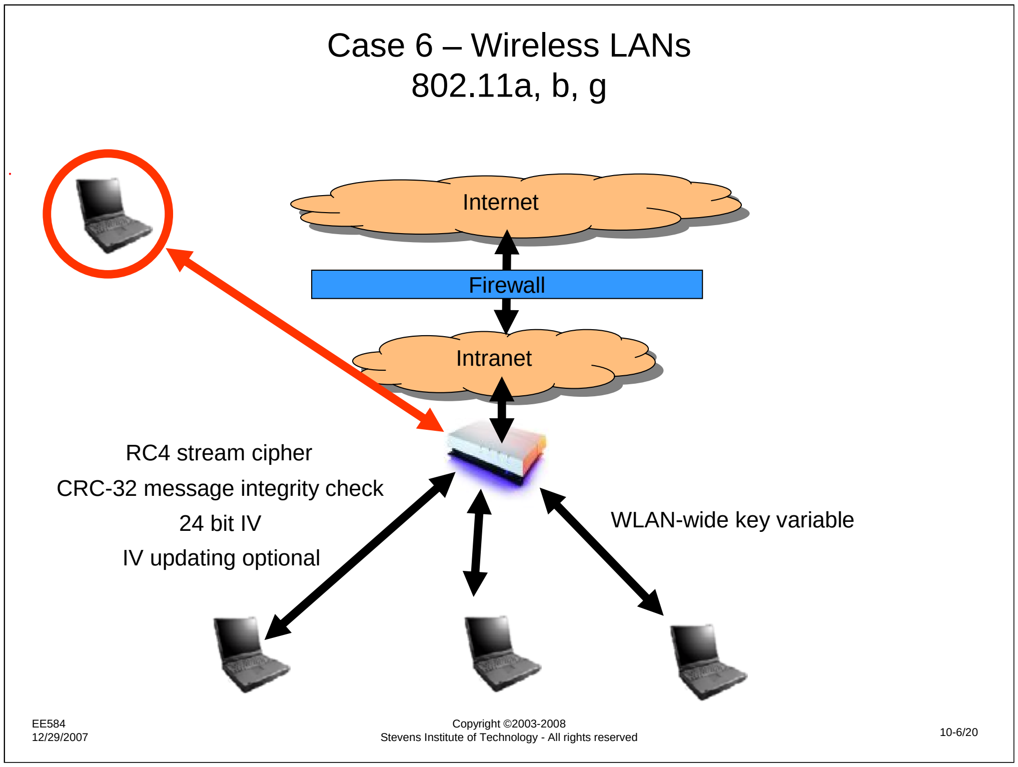
EE584
12/29/2007

10-5/20

Finally, let's discuss the networking arrangement one might use with an 802.11 WLAN within a corporate intranet.

If we assume that proprietary information is going to be sent on the intranet, we will need some sort of barrier between the intranet and the Internet. This is the role of the firewall shown in blue in the middle of the diagram. We probably have a variety of wired and wireless users using the intranet – this gets at the real draw of wireless networking: With fixed PCs and workstations and new building construction, it is relatively easy to plan for building wiring to handle networking needs. However, with the growing popularity of laptops and other mobile computing devices, it is not always easy to wire the portable PCs to the network. Further, as organizations change and people move, network connectivity may change. Finally, in older existing buildings, it is very difficult to pull wires through walls. It is not unusual for an electrician to charge $100 to install an outlet in a residence with plasterboard walls and wooden framing. Consider how hard it would be to install the same outlet in a late 1800's vintage building like the Edwin A. Stevens building, constructed with plaster walls before the advent of AC wiring. When an access point that can support dozens of users is $150 and a network card for a PC is $50, it isn't too difficult to see how soon the WLAN proves in over rewiring a building for only a few users.

Still, we need to consider the protection of data on the corporate intranet. We can assume the firewall protects most of the internal wiring, but what if an outsider can use the WLAN to get into the intranet, bypassing the firewall?



Case 6 – Wireless LANs
802.11a, b, g

RC4 stream cipher

CRC-32 message integrity check

24 bit IV

IV updating optional

WLAN-wide key variable

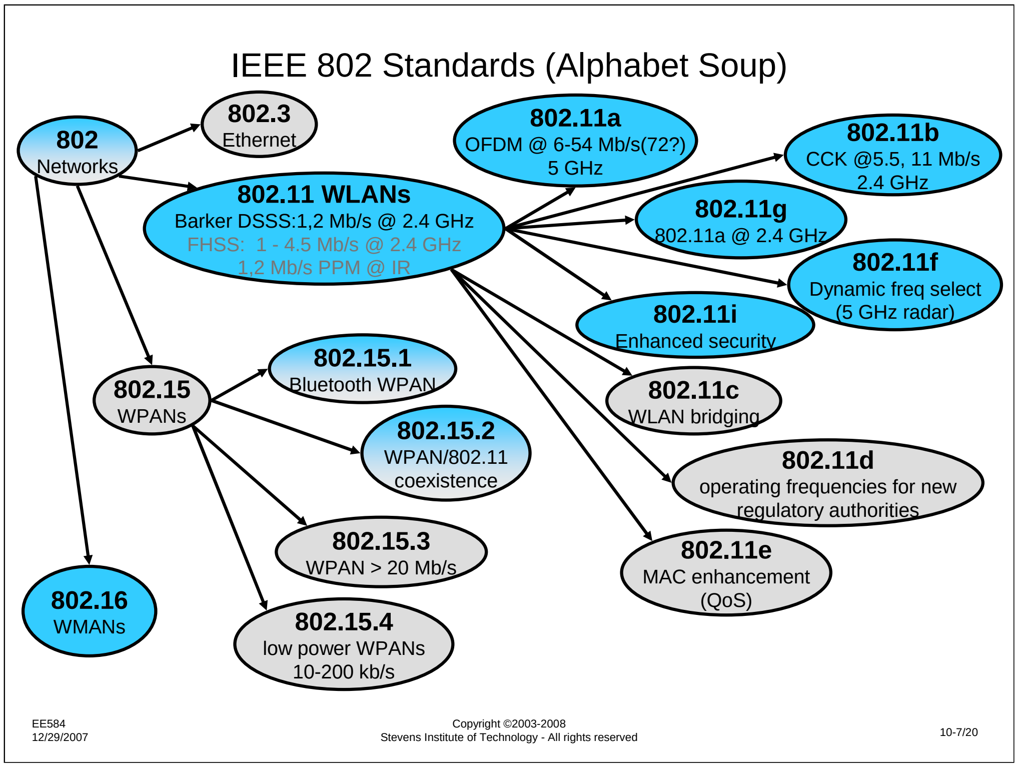
EE584
12/29/2007

10-6/20

Some of the characteristics of the 802.11 networks intended to deal with wireless attacks are shown above. For now, I'll leave it to the Red and Blue teams to decide which of the protections are adequate and which are not. I'll list the most important characteristics here, but will go into some of the background during the wrap-up for this week's case study after the assessment week.

First, communications on the WLAN are (optionally) encrypted using the RC-4 stream cipher. At the time the standards were being set, other encryption algorithms were considered, but the US government's restrictions on export of cryptographic technology restricted the choices. RC-4 was one of the algorithms that were approved for export without special permission. [Side note: There are some interesting laws that deal with export of "munitions" – items that can be used in warfare. While one might generally think of munitions as guns, bombs, and ammunitions, the International Trafficking in Arms Regulations (ITAR) defines cryptography and some other technology as a munition. This means that software and other intellectual property can be restricted from export. Interestingly, books and other publications are not restricted under the First Amendment, so there have been cases where a book that describes an encryption algorithm by a source code listing was not restricted, but the CD-ROM that had the same source code in machine readable code was restricted…] The wired equivalent privacy (WEP) encryption can operate in 64-bit or 128-bit encryption mode. Most systems that use encryption are operated with a system-wide key variable that is generally static for long periods of time, due to the difficulty in securely coordinating a key change to all the users.

For each transmission, the transmit and receive key generator that implement the RC-4 algorithm must be initialized to the same value to be able to transfer the cleartext. For this, a 24-bit initialization vector (IV) is sent along with the packet. The means of choosing the IV for each packet is left open in the standard. The IV could be left constant, or it could be generated sequentially or randomly. Finally, to detect damage to the packet over the RF link, a 32-bit cyclic redundancy check is added to the plaintext packet before encryption.



IEEE 802 Standards (Alphabet Soup)

802
Networks

802.3
Ethernet

802.11 WLANs
Barker DSSS:1,2 Mb/s @ 2.4 GHz
FHSS: 1 - 4.5 Mb/s @ 2.4 GHz
1,2 Mb/s PPM @ IR

802.11a
OFDM @ 6-54 Mb/s(72?)
5 GHz

802.11b
CCK @5.5, 11 Mb/s
2.4 GHz

802.11g
802.11a @ 2.4 GHz

802.11f
Dynamic freq select
(5 GHz radar)

802.11i
Enhanced security

802.11c
WLAN bridging

802.11d
operating frequencies for new regulatory authorities

802.11e
MAC enhancement
(QoS)

802.15
WPANs

802.15.1
Bluetooth WPAN

802.15.2
WPAN/802.11
coexistence

802.15.3
WPAN > 20 Mb/s

802.15.4
low power WPANs
10-200 kb/s

802.16
WMANs

EE584
12/29/2007

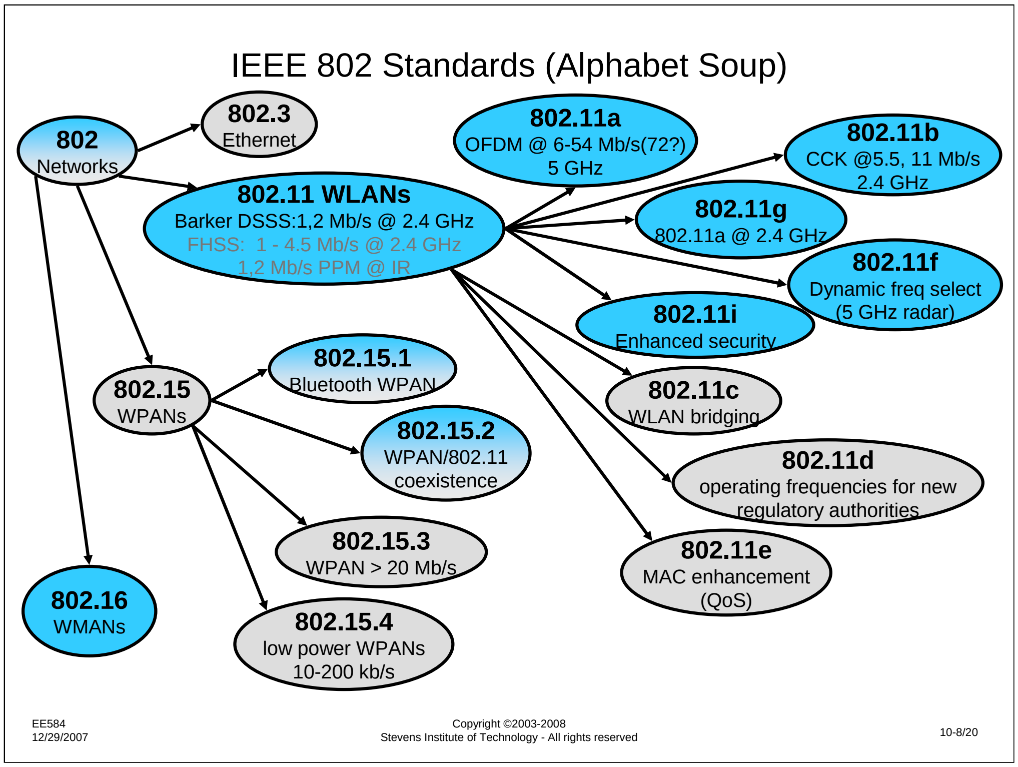
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

10-7/20

I have mentioned several 802.11 standards. When I was working on this area in Bell Labs and AT&T Labs, I felt I needed a score card to keep them all separate. Shown above is a diagram to sort out some of the alphabet soup.

IEEE 802 generally deals with “networks.” While 802.11 wireless LANs is one subcommittee, others like 802.3, which deals with Ethernet, 802.15, which deals with Bluetooth™ and other personal area networks, and 802.16, which deals with wireless metropolitan area networks, exist. The ones in grey will not be discussed in this course, but we will, at least, touch on the ones in blue. In particular, we will discuss 802.16 as next week’s last case study.

First, let’s discuss Bluetooth™. The original concept was to use wireless to make connections the last few feet between various devices that are now handled with dozens of specialized cables – RS-232 cables, printer cables, USB cables, etc. Bluetooth™ interfaces would everywhere and, thus, would be very cheap. Printers, computers, cellular phones, and just about everything else one could imagine connecting with a cable would be connected with Bluetooth™. As it happens, there are several devices that have incorporated Bluetooth™, but it has not happed as widely or as quickly as the people who were pushing it hoped. This might be a good thing, since Bluetooth™ also operates on the 2.4 GHz ISM band. Worse, to avoid interference, it hops over the band. Where are we most likely to see a Bluetooth™ interface? In the same laptop that has an 802.11b WLAN! What happens when they are both operating at the same time? From my 802.11b interference research (which were *supposed* to be Bluetooth™ compatibility tests, except that we couldn’t get working Bluetooth™ devices at the time), I inferred a lot of interference to the 802.11b system while the Bluetooth™ devices worked away merrily.



IEEE 802 Standards (Alphabet Soup)

802
Networks

802.3
Ethernet

802.11 WLANs
Barker DSSS:1,2 Mb/s @ 2.4 GHz
FHSS: 1 - 4.5 Mb/s @ 2.4 GHz
1,2 Mb/s PPM @ IR

802.11a
OFDM @ 6-54 Mb/s(72?)
5 GHz

802.11b
CCK @5.5, 11 Mb/s
2.4 GHz

802.11g
802.11a @ 2.4 GHz

802.11f
Dynamic freq select
(5 GHz radar)

802.11i
Enhanced security

802.11c
WLAN bridging

802.11d
operating frequencies for new regulatory authorities

802.11e
MAC enhancement
(QoS)

802.15
WPANs

802.15.1
Bluetooth WPAN

802.15.2
WPAN/802.11
coexistence

802.15.3
WPAN > 20 Mb/s

802.15.4
low power WPANs
10-200 kb/s

802.16
WMANs

EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

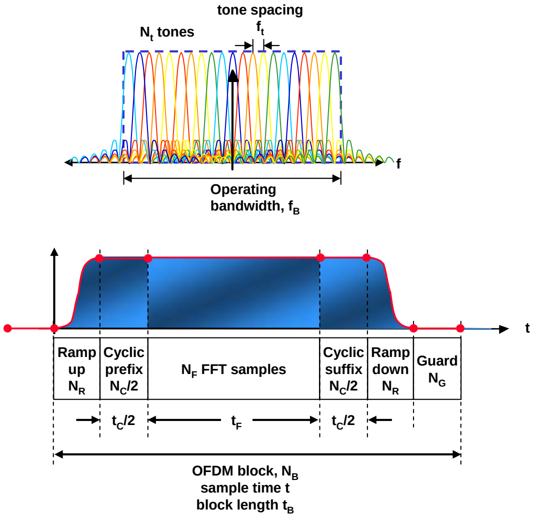
10-8/20

Let’s discuss the rest of the blue bubbles above. We have touched on 802.11, 11a, 11b, and 11g. There are two more standards committees that need to be mentioned: 802.11f and 11i.

In Europe, their flavor of 802.11a, known as Hyperlan II, was fielded a bit in advance of 802.11a in the US. They saw the potential for problems that have not become apparent here yet due to the frequencies they use for radar landing systems, which share their 5 GHz band. 802.11f investigates techniques that would allow a 802.11a system to detect the presence of radar systems on an operating channel and shift to another channel to avoid creating interference. Bluetooth™ *could* do the same thing as it hops from channel to channel, upon detection of an 802.11 network, but it doesn’t.

Unless you have been living in a cave for the last few years, you have probably heard discussions about security issues in 802.11 systems, which, combined with the popularity of the systems, is the main reason I picked this for one of the case studies. I won’t go into what the real issues are until the wrap-up week, but suffice it to say that the IEEE and the WLAN industry is responding to these issues by enhancements to the standard. This is the role of the 802.11i committee. This work has also spawned other 802.11 committees, looking at particular aspects of 802.11 security, but this has been a changing landscape, compared to the rest of the 802 committees.

OFDM Basics



Total bandwidth $f_B = N_t f_t$

Tone spacing vs active block time $f_t = \frac{1}{t_F}$

$$N_B = 2N_R + N_C + N_G + N_F$$

Block efficiency $\eta = \frac{N_F}{N_B} = \frac{N_F}{N_F + N_C + 2N_R + N_G}$

Tolerance to delay spread $\approx t_C \propto N_C$

Raw capacity for M-ary tone modulation $N_t M$

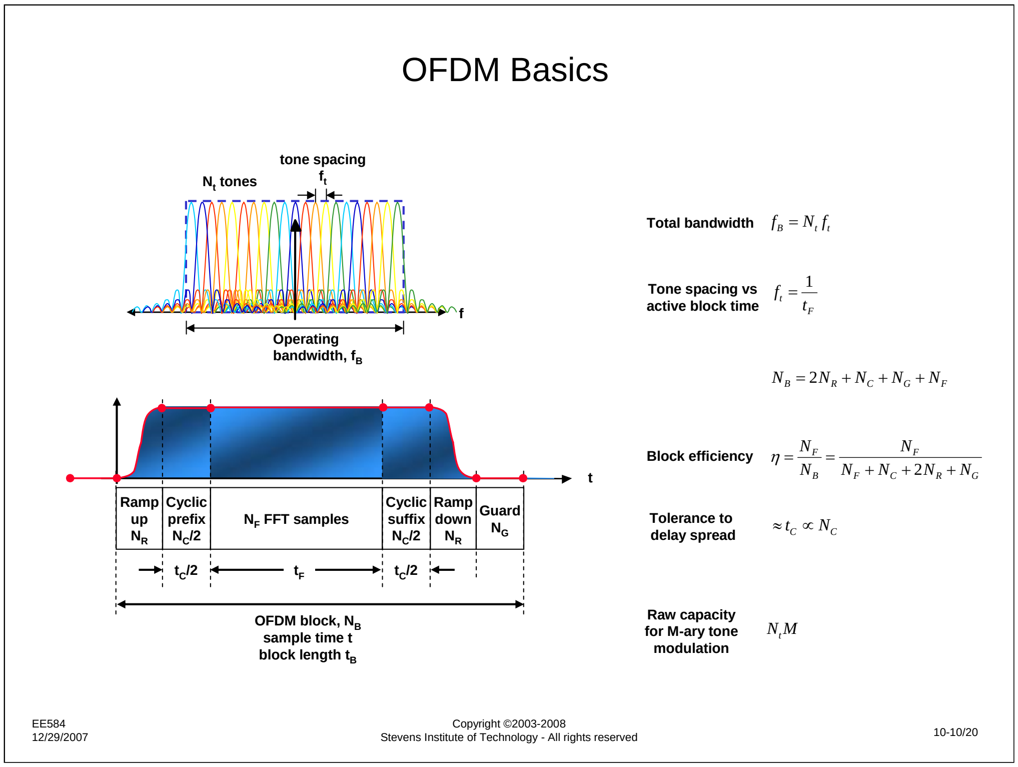
EE584
12/29/2007

10-9/20

Since it is so central to the operation of 802.11a, g, and the WMAN standards we will discuss next week, I wanted to provide some background on the OFDM technology that is used in these standards. I will present a high level discussion here, but if you want some more details, see: http://www.novidesic.com/papers.htm and http://www.novidesic.com/talks.htm, where there are several references.

Here's the essential problem of transmitting data at high speeds, particularly over a wireless network. You could send a carrier that is modulated at a very high symbol rate, but with a small (perhaps, 2) levels. It would be easy to detect each symbol and decide a value, but since the symbol rate is very high, the system would be subject to multipath distortion on the channel. For instance, to send 10 Mb/s, using binary signaling, this would mean a symbol rate of 10 Mbaud (1 baud = 1 symbol/second). This is a symbol duration of 100 ns, which means that a multipath signal that travels 50 feet longer than the main signal will interfere with half of the symbol. This is not good, since we typically see a few hundred nanoseconds of multipath inside a large building and several microseconds of multipath outside. So, what happens if we send at a lower symbol rate, but increase the number of levels? To deal with 200 ns of "delay spread," we could signal with a symbol period of 2 microseconds. This way, the multipath would be no more than 1/10th of the symbol period. This is 500 kbaud, which would also reduce the bandwidth needed from ~10 MHz to about 500 kHz. If we still want to be able to send 10 Mb/s, this means we have to convey 20 bits per symbol. Since the number of bits per symbol is the base 2 logarithm of the number of levels, this means we have to signal with 1000000 possible levels per signal. Even using quadrature modulation, this requires 1000 levels per phase, which means that the smallest signal step is 30 dB below the peak excursion. Noise would kill such system – we would need much more than a 30 dB signal to noise ratio, so this isn't going to work.

So, how can we send information at high data rates over a channel that is dispersive (multipath) and noisy. And, oh, by the way, is a fading channel, which makes it harder to discern small changes in amplitude from a fade?



OFDM Basics

N_t tones

tone spacing f_t

f

Operating bandwidth, f_B

t

Ramp up N_R	Cyclic prefix $N_C/2$	N_F FFT samples	Cyclic suffix $N_C/2$	Ramp down N_R	Guard N_G
	$t_C/2$	t_F	$t_C/2$		

OFDM block, N_B sample time t block length t_B

Total bandwidth $f_B = N_t f_t$

Tone spacing vs active block time $f_t = \frac{1}{t_F}$

$$N_B = 2N_R + N_C + N_G + N_F$$

Block efficiency $\eta = \frac{N_F}{N_B} = \frac{N_F}{N_F + N_C + 2N_R + N_G}$

Tolerance to delay spread $\approx t_C \propto N_C$

Raw capacity for M-ary tone modulation $N_t M$

EE584
12/29/2007

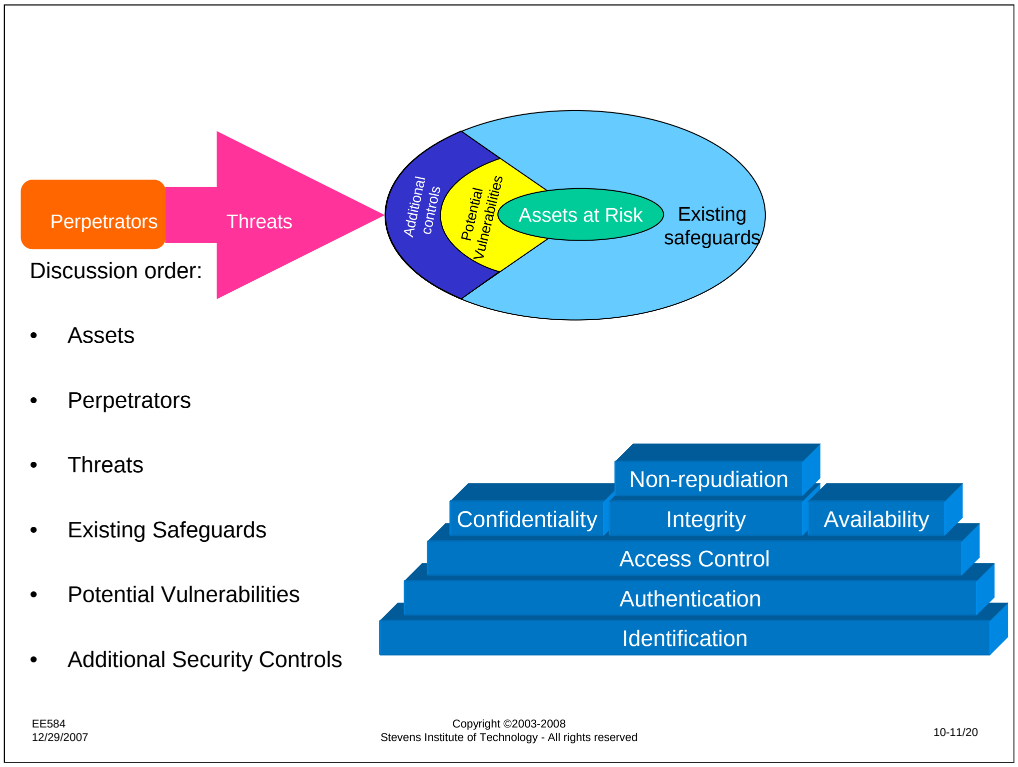
10-10/20

Obviously, the answer has to be OFDM, or I wouldn't be using this slide.

The concept of OFDM is to avoid the problem of too many levels and too fast a signaling rate, by restricting ***both***. But that would seem to mean that it isn't possible to signal at a high data rate! What is unique about OFDM is that, while a single carrier is only carrying the low data rate it is restricted to, by intelligently packaging together a number of carriers, we can achieve a high aggregate data rate.

Using 802.11a as an example, the symbol period is 4 microseconds, with a 800 ns guard interval (something specific to OFDM, because of the way signals are generated). As a result of this, 802.11a can tolerate up to 800 ns of delay spread, more than enough for the interior of a large, open factory floor. This means that the symbol rate is 250 kbaud. To support the 54 Mb/s data rate, 802.11a supports modulation up to 64 QAM, although it can fall back to BPSK if channel conditions require it. With 64 levels per symbol (8 in each phase – in-phase and quadrature), this means that levels that are 1/8th of the maximum variation need to be discerned, which is easily doable on a decent wireless channel. However, with 64 levels per symbol, this means that log2(64)=6 bits can be transmitted per symbol. This means that 6*250k=1.5 Mb/s is the maximum capacity of the 802.11a carrier. The earliest WLANs did better than this! However, 802.11a uses 52 parallel carriers, each of which could carry independent data. This means that the aggregate data rate is 1.5*52=78 Mb/s. With coding to protect against channel errors, and other overhead, this easily delivers 54 Mb/s.

The technology that makes the OFDM system possible in the first place is the ability to perform a Fast Fourier Transform (FFT) to convert between the time and frequency domain quickly and easily. It happens that the most efficient FFTs use a transform size that is a power of two. In this case, a 64 point FFT is computed 250,000 times per second, with 12 "virtual carriers" transformed but not used for modulation. At the transmitter, modulation is simply determining which complex value to input into each frequency bin, followed by an inverse FFT (IFFT) to create the time domain signal. At the receiver, the time domain signal is processed by the FFT to recreate the complex modulation on each carrier, which requires simple decisions to detect the data. Of course, I am leaving off issues like synchronization. etc., but you can find more than you want to know about this in the references.



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

Non-repudiation

Confidentiality

Integrity

Availability

Access Control

Authentication

Identification

EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

10-11/20

Once again, as for the previous assessments, if you have been assigned to a Red Team, you should be concentrating on the following items:

Assets: What is it about the system that you would be interested in stealing, destroying, disrupting, etc.?

Perpetrators: Who are you? Why do you do the evil things you do? Who is backing you, or what resources are available to you?

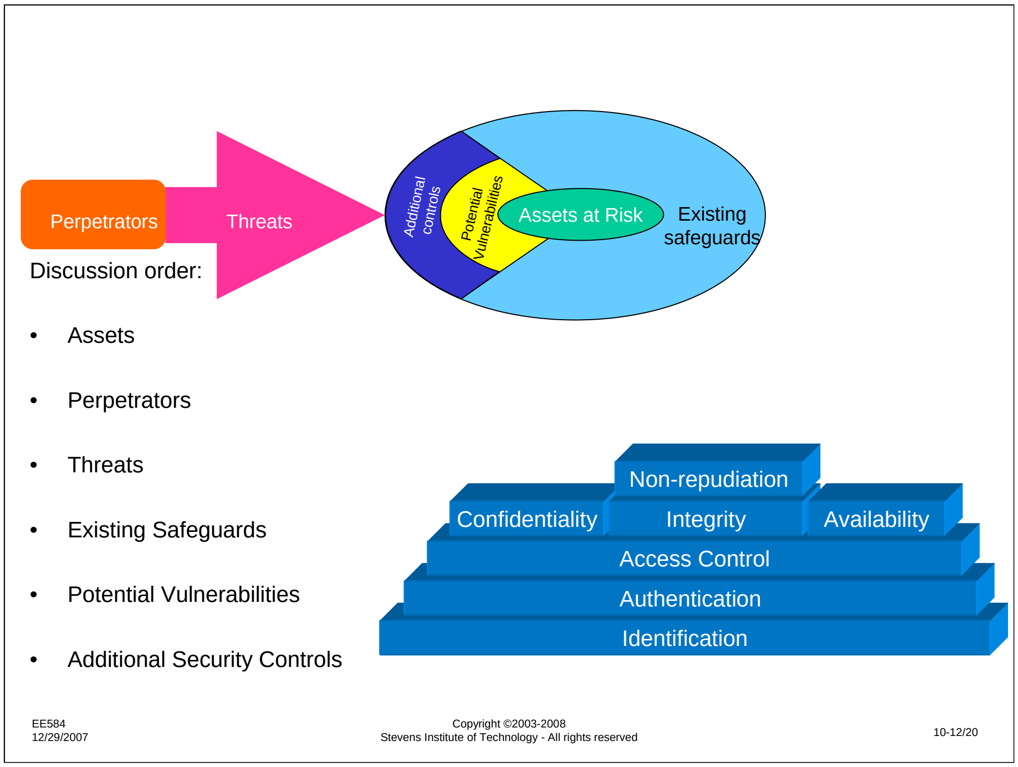
Threats: What mischief can you get into? How would you do it?

Safeguards: What are the things that are, or might be, in your way?

Vulnerabilities: What unlocked doors, open windows, unprotected ways in might exist?

Additional Controls: What might the defender do to make you life harder?

Again, keep in mind the security architecture at the bottom right. For each security service, there might be something that you can do, steal, break, etc.



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

Non-repudiation

Confidentiality

Integrity

Availability

Access Control

Authentication

Identification

EE584
12/29/2007

10-12/20

Likewise, if you have been assigned to a Blue Team, you should be concentrating on the following items:

Assets: What is valuable to you in your system? What might the attacker be after?

Perpetrators: Who should you be on the lookout for? How do they operate? What are they capable of?

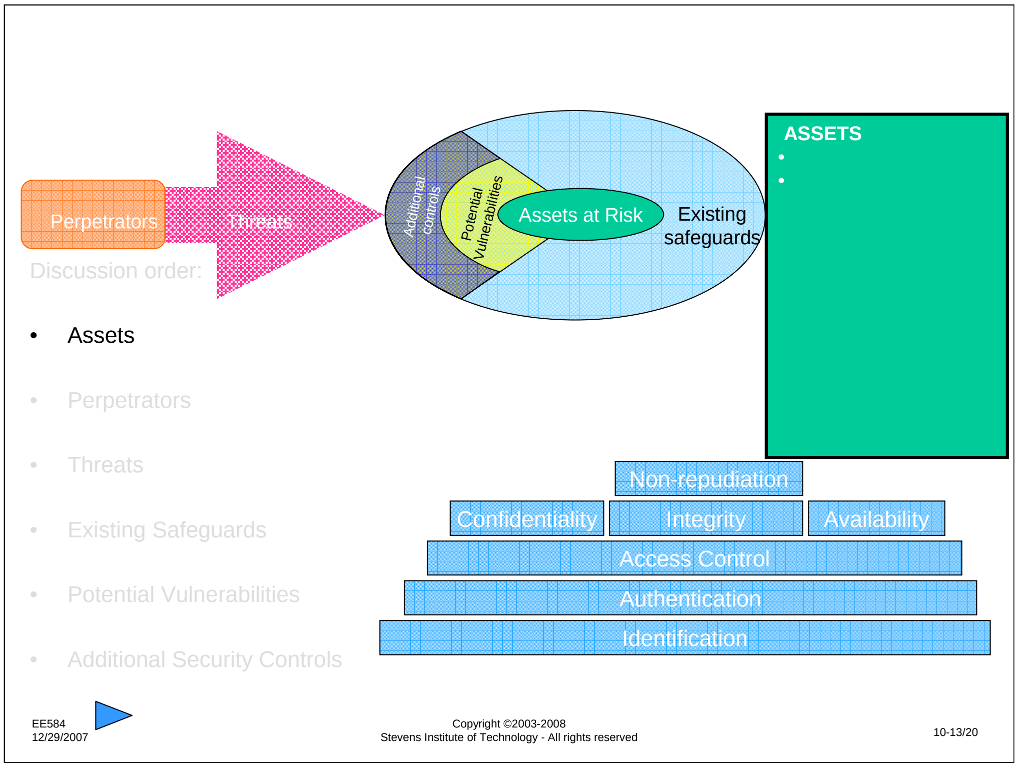
Threats: How might someone try to attack your system?

Safeguards: What protection is already in place?

Vulnerabilities: What might have been missed? Where are they most likely to try to enter?

Additional Controls: How could you make the system stronger? Would it be worth it?

Again, keep in mind the security architecture at the bottom right. For each security service, there might be something in your system that needs protecting.



Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

EE584
12/29/2007

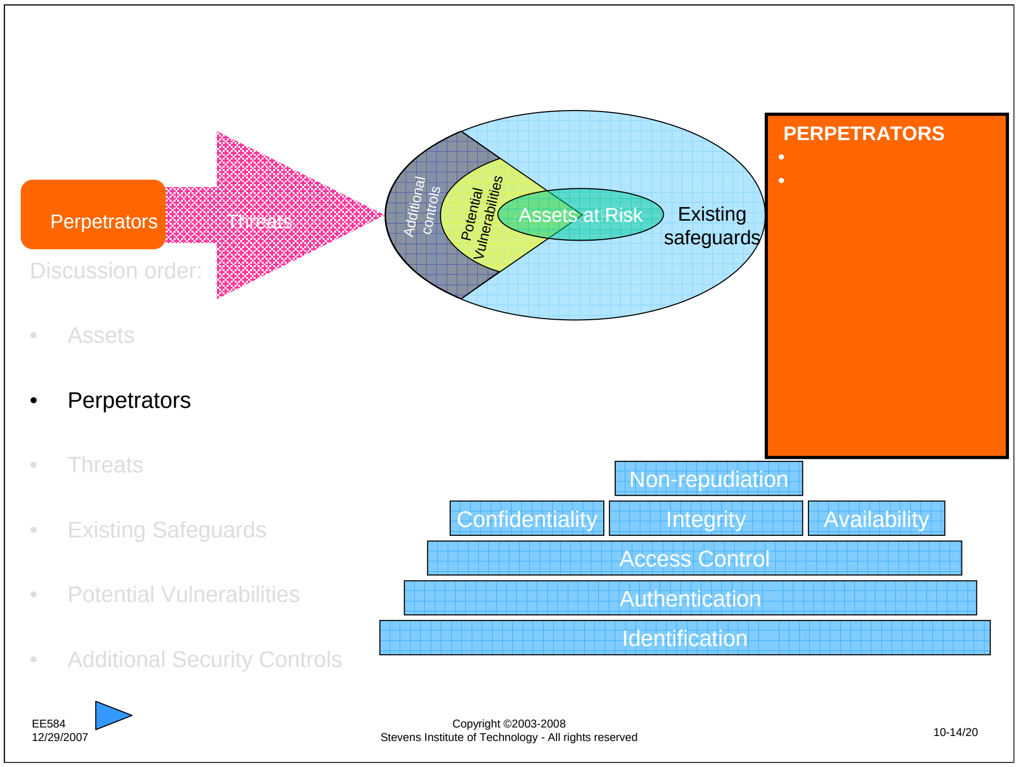
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

10-13/20

Once again, I recommend that as you examine the system under discussion, you create a discussion topic for each aspect of security and/or for each element of the security assessment process.   This is a brainstorming process, so don't worry about silly suggestions or things that are not in the right discussion thread. Post as many ideas as you can think of and respond to the postings of others with more ideas.

Again, the Red Team will not be able to see the postings of the Blue Team during this week and vice versa. As I did previously, next week, both sets of discussions will be open to the other group. I encourage each group to compare their thought process with the process of the other group. You can, however, look at last week's assessment discussions. In addition, I will have posted summaries of assessments that were performed on last week's topic by previous sessions of this course so you can compare your group's assessment to previous ones. There will be some common items, but I am sure there will be some that one session or the other did not encounter. As this course is repeated, I expect that the cumulative assessment discussion will converge to a common set of issues.

Next week, we perform an assessment on the last system – 802.16 wireless metropolitan area networks (WMAN). At that time, again, I will summarize the discussions and will add some more information about issues in the system that may not have been addressed.

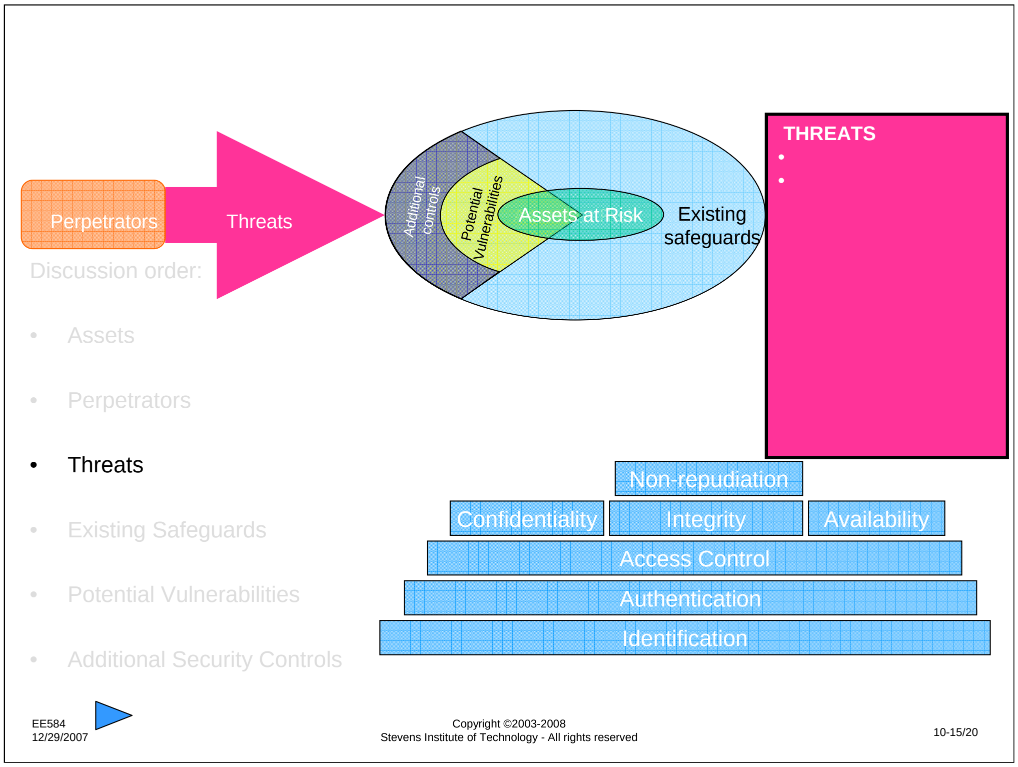


PERPETRATORS

-
-

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

THREATS

-
-

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

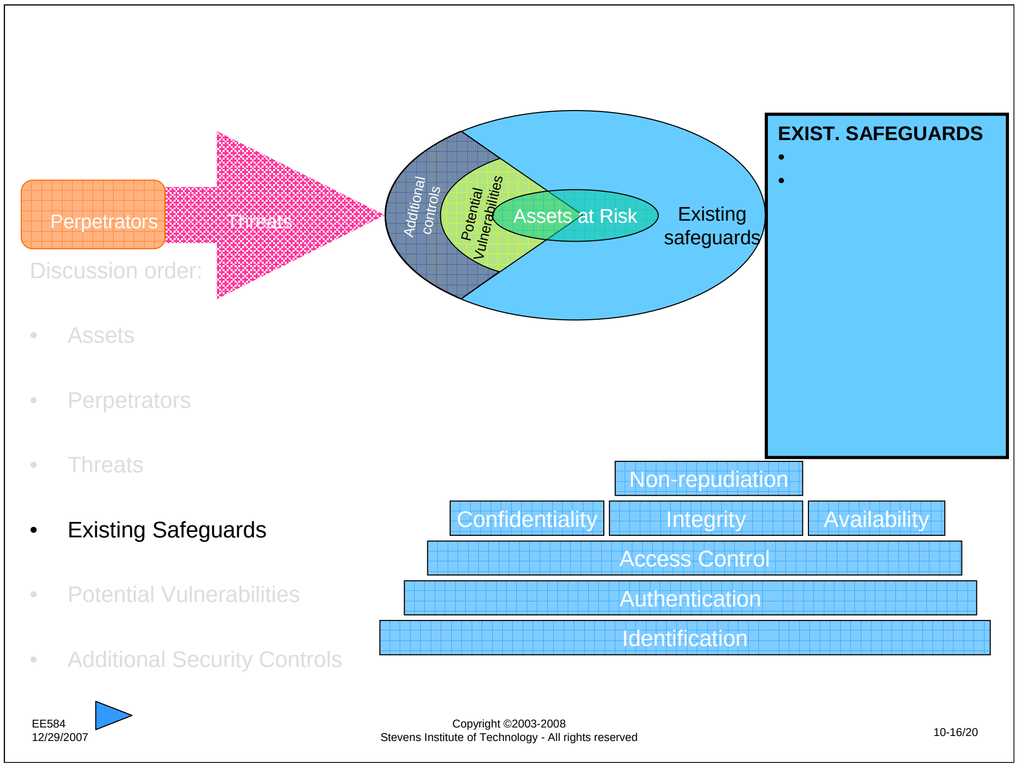
Non-repudiation

Confidentiality | Integrity | Availability

Access Control

Authentication

Identification



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

EXIST. SAFEGUARDS

-
-

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

Non-repudiation

Confidentiality | Integrity | Availability

Access Control

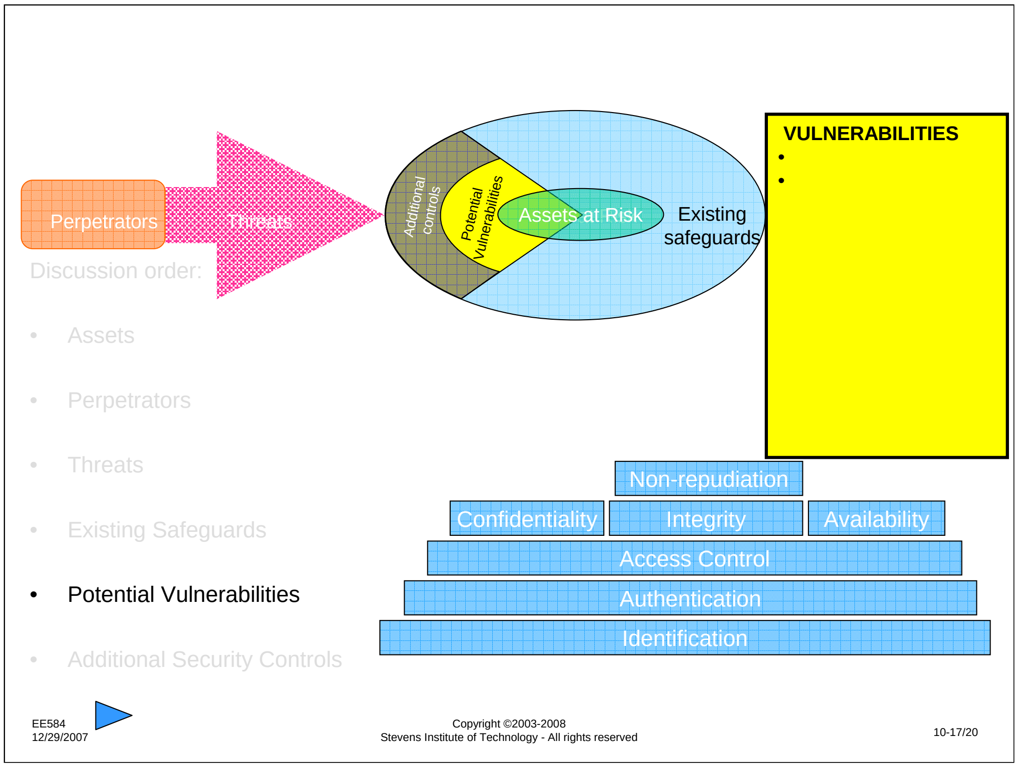
Authentication

Identification

EE584
12/29/2007

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

10-16/20



Perpetrators

Threats

Additional controls

Potential Vulnerabilities

Assets at Risk

Existing safeguards

VULNERABILITIES

-
-

Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

Non-repudiation

Confidentiality | Integrity | Availability

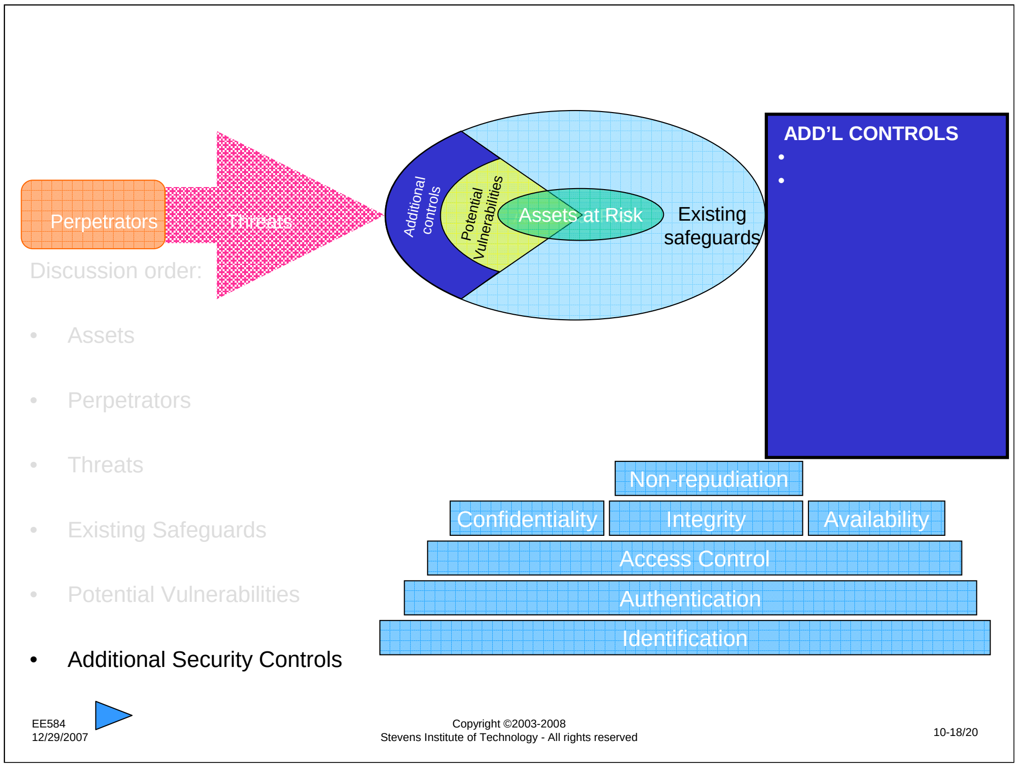
Access Control

Authentication

Identification

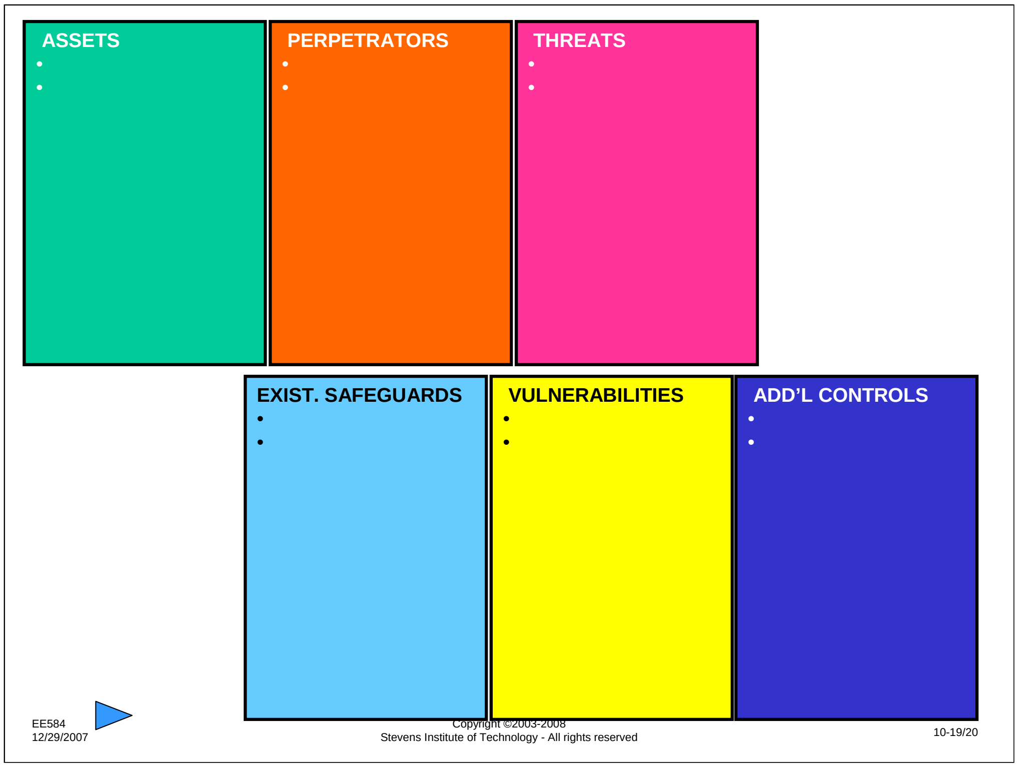
EE584
12/29/2007

10-17/20



Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



ASSETS

•

•

PERPETRATORS

•

•

THREATS

•

•

EXIST. SAFEGUARDS

•

•

VULNERABILITIES

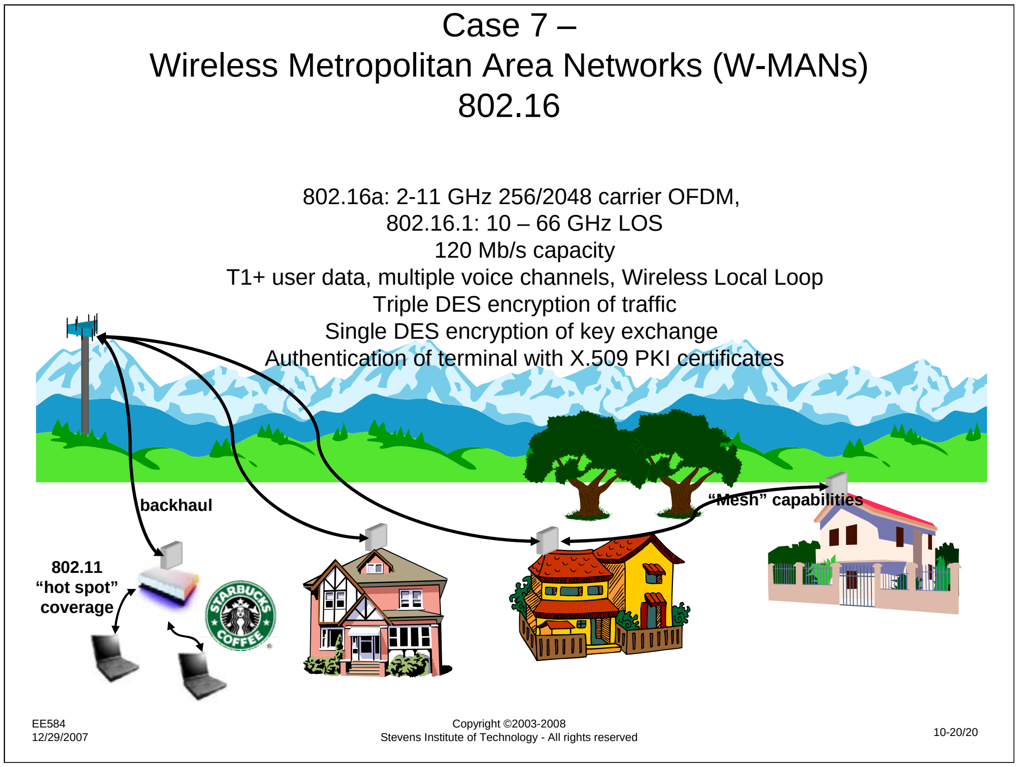
•

•

ADD’L CONTROLS

•

•



Case 7 –
Wireless Metropolitan Area Networks (W-MANs)
802.16

802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates

EE584
12/29/2007

10-20/20

The wireless network for this last case study will be a newly emerging set of standards addressing what are known as wireless MANs – Metropolitan Area Networks. As the name implies, this is a broader coverage area than a WLAN, capable of covering a metropolitan area, perhaps several square miles to dozens of square miles. You might consider the coverage area to be similar to the coverage of a cell site. Research these systems, which are sometimes referred to as WiMAX (a take-off on WiFi,the standard for wireless LANs)