Wireless Networking II

Kapitulli 7

Çfarë kemi trajtuar

- Kapitulli 1-4: Materiale hyrëse
- Kapitulli 5: Switched Networks
- Kapitulli 6: Standardet 802.11 dhe funksioni
- Kapitulli 7: 802.11 siguria, 802.11 menaxhimi, teknologji të tjera të rrjetave lokale wireless, teknologjitë celulare

802.11 Siguria

802.11 LAN Menaxhimi

Teknologji të tjera wireless

1.1: Kërcënimet ndaj Sigurisë në WLAN

- **Makinat-Hackers** (Drive-by Hackers)
  - Qëndron jashtë ambjenteve të kompanisë dhe lexon trafikun në rrjetin e kompanisë
  - Mund të dërgojnë trafik të dëmshëm në rrjet
  - Realizohen lehtë me software të gatshëm që mund të dowload-ohen nga interneti
- **Makinat e luftës** (War Drive)
  - Thjesht zbulojnë pika e aksesit të pambrojtura — bëhen makina-hacker vetëm nqs e thyejnë
  - Makinat e luftës në vetvete nuk janë veprim ilegal

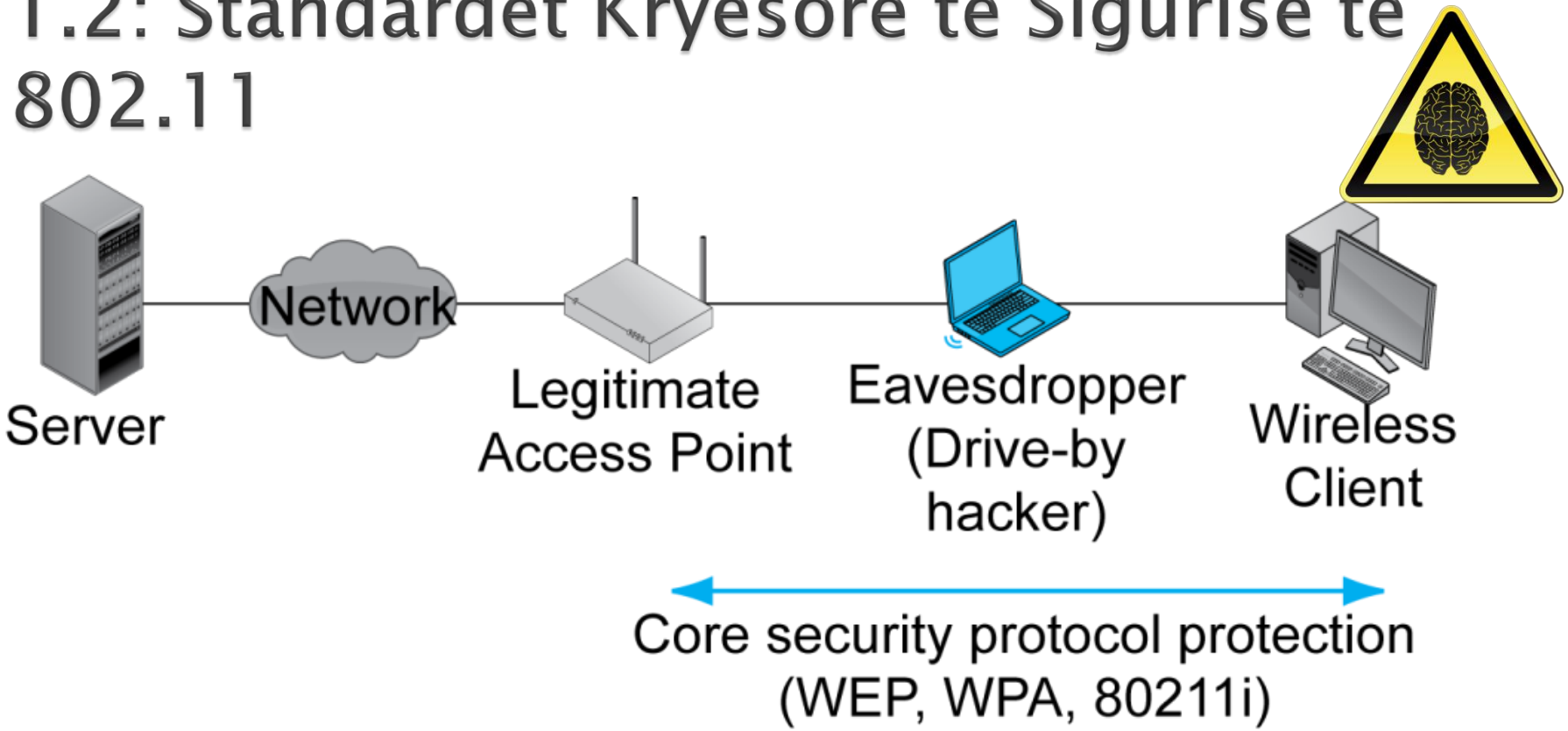
1.1: Kërcënimet ndaj Sigurisë WLAN

- **Pikat e Aksesit të Pambrojtura**
  - Makinat-Hacker (Drive-by Hackers) mund të lidhen në çdo pikë aksesi të pambrojtur.
  - Ata fitojnë akses në LAN duke anashkaluar firewall mbrojtës të rrjetit.

1.1: Kërcënimet ndaj Sigurisë WLAN

- **Rogue Access Points** – Pikat e aksesit të kuqe
  - Pika aksesi të paautorizuara që krijohen nga departamente ose individë
  - Shpesh kanë siguri të dobët, gjë që e bën shumë të lehtë thyerjen nga makinat-hacker (*drive-by hacking)*
  - Shpesh operojnë në fuqi të lartë, duke tërhequr shumë hoste tek shërbimi i tyre me siguri të vogël

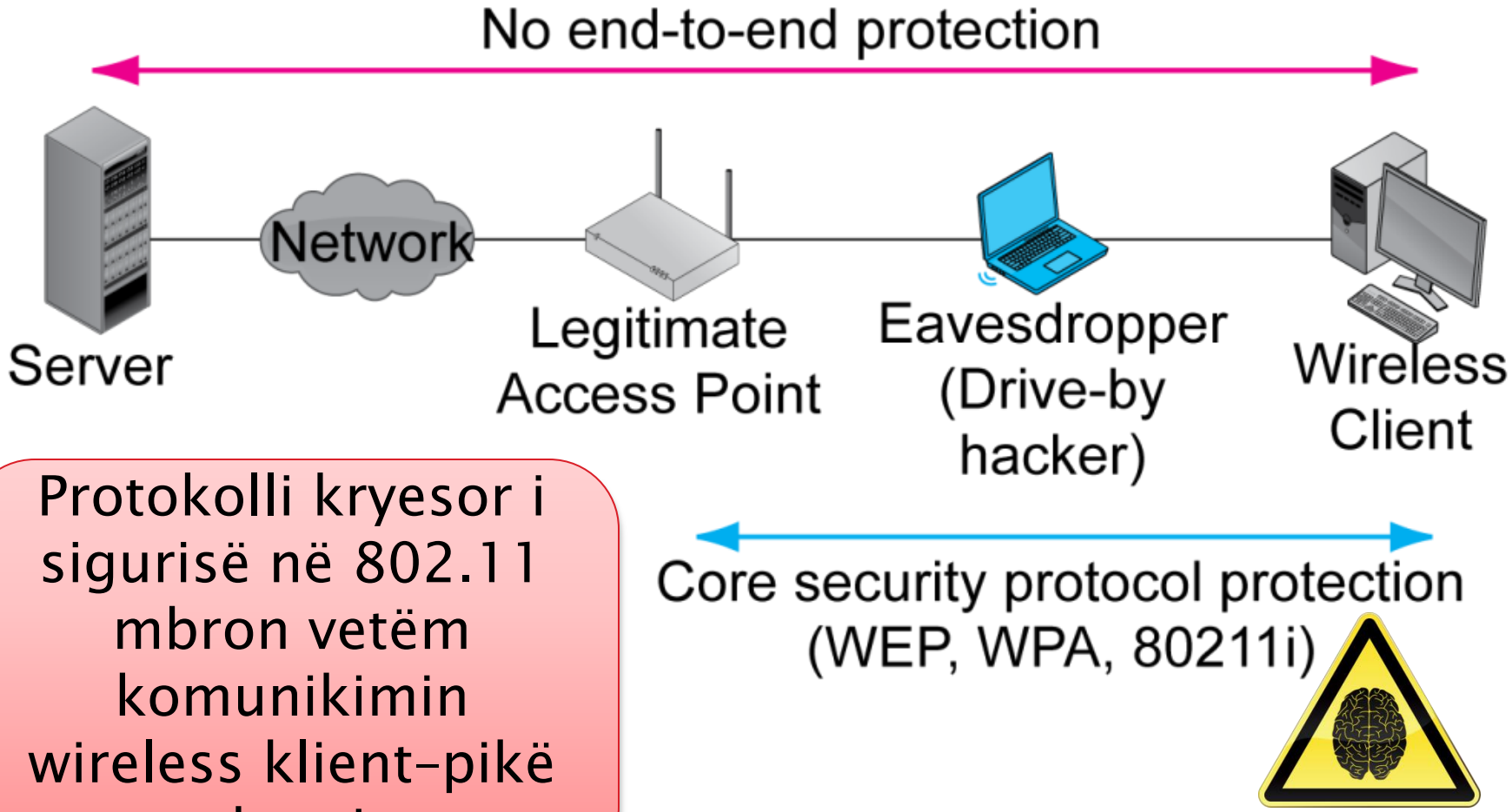
1.2: Standardet Kryesore të Sigurisë të 802.11



Protokolli Kryesor i Sigurisë mbron komunikimin midis një klienti wireless dhe një pike aksesi legjitime.

Ato sigurojnë enkriptimin për të ofruar konfidencialitet dhe mbrojtje të tjera kriptografike.

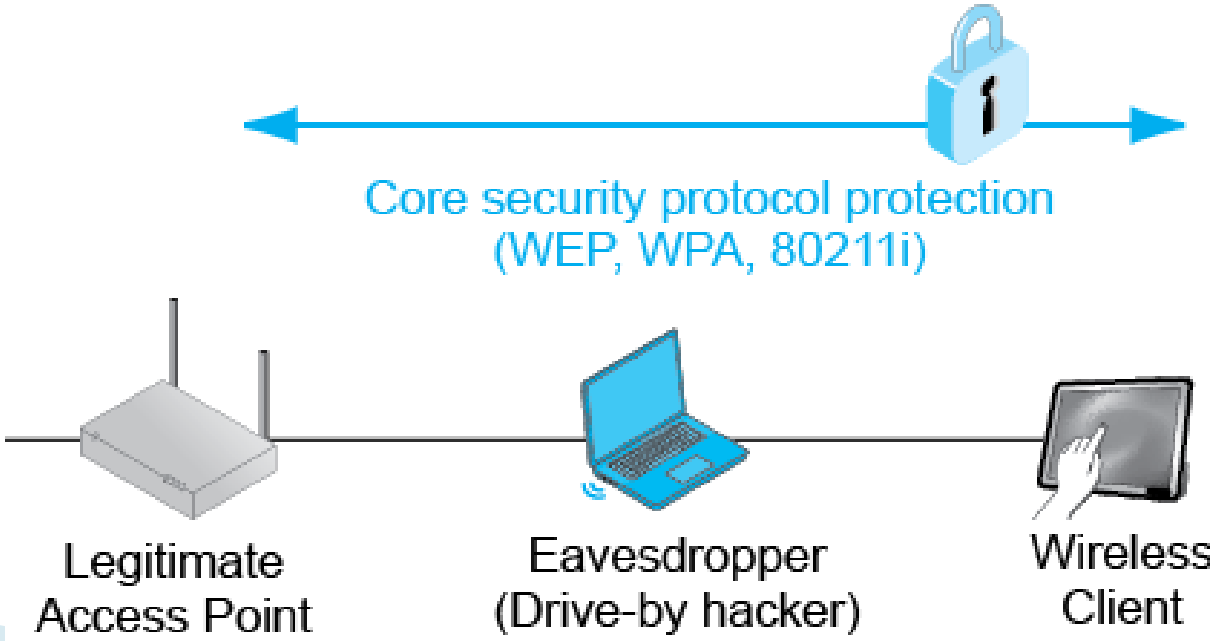
1.2: Standardet Kryesore të Sigurisë të 802.11



Protokolli kryesor i sigurisë në 802.11 mbron vetëm komunikimin wireless klient-pikë aksesi.

7.3: Standardet Kryesore të Sigurisë të 802.11

- Prodhojnë Sigurinë midis Stacionit Wireless dhe Wireless Access Point
  - Autentikim i (ndoshta dhe pikës së aksesit) klientit
  - Enkriptim i mesazheve për konfidencialitet



1.3: Standardet Kryesore të Sigurisë të 802.11

- **Wired Equivalent Privacy (WEP)**
  - Si fillim në 1997 ofrohej një siguri minimale bazë me 802.11.
  - Çdo njeri ndante të njëjtin çelës sekret enkriptimi, dhe ky çelës nuk mund të ndryshohej automatikisht.
  - Meqë çelësi sekret ndahej, ai s'mund të ishte sekret.
    - Përdoruesit shpesh e shpërndanin atë falas.
  - Çelësi fillimisht mund të thyhej në 1-2 orë; tani mund të thyhet në 3-10 minuta duke përdorur software që janë të disponueshëm.

1.3: Standardet Kryesore të Sigurisë të 802.11

- **Wireless Protected Access (WPA)**
  - Aleanca Wi-Fi
    - Normalisht çertifikon ndërveprimin midis pajisjeve 802.11
    - Pajisjet e çertifikuara mbajnë emrin Wi-Fi të shkruar
    - WPA krijuar si një standard sigurie për të mbyllur të çarat e sigurisë derisa përfundoi 802.11i në 2002

1.3: Standardet Kryesore të Sigurisë të 802.11

- **Wireless Protected Access (WPA)**
  - Dizenjuar për të përmirësuar pajisjet e vjetra
    - WPA përdor një nëngrup të 802.11i që mund të ekzekutohen në kartat e vjetra wireless NIC dhe pikat e aksesit.
    - WPA shton algoritma të thjeshtë sigurie për funksionet që nuk mund të ekzekutohen në makinat e vjetra.
  - Pajisjet që nuk mund të përmirësohen (upgrade) me WPA nuk do të përdoren.

1.3: Standardet Kryesore të Sigurisë të 802.11

- **802.11i (WPA2)**
  - Përdor AES-CCMP (algoritëm enkriptimi) me çelës 128-bit për konfidencialitetin dhe menaxhimin
  - 802.11i **është standardi i artë** në sigurinë e 802.11
  - Por kompanitë kanë baza të mëdha të instaluara të pajisjeve WPA, kështu që ata hezitojnë të bëjnë përmirësime (upgrade).
  - WPA tashmë ka qenë pjesërisht e thyer (krakuar) kështu që ka bërë që firmat të pranojnë të bëjnë përmirësime në pajisje.

1.3: Standardet Kryesore të Sigurisë të 802.11

WEP	Standardi kryesor fillestar për sigurinë. Lehtësisht i thyeshëm sot.
WPA	Ka qenë pjesërisht i thyeshëm. Baza shumë e gjerë e instaluar e bën përmirësimin e gjithë rrjetit në 802.11i të shtrenjtë.
802.11i (WPA2)	Standardi i preferuar sot. Ekstremisht i fortë.

8.4: Modelet 802.1X dhe PSK

- Si WPA dhe 802.11i kanë dy modele operimi.
  - **Modeli 802.1X**
  - **Modeli Pre-Shared Key**

7.4: Modelet 802.1X dhe PSK

- **Modeli 802.1X**
  - Për organizata të mëdha
  - Përdor një server qendror autentikimi për konsistencë
  - Serveri i autentikimi gjithashtu ofron dhe menaxhim kyç
  - Aleanca Wi-Fi e quan gjithashtu *Modeli i Organizatës*

7.4: Modelet 802.1X dhe PSK

- **Modeli Pre-Shared Key për shtëpi ose firma të vogla**
  - Për shtëpitë ose firmat e vogla me një pikë të vetme aksesi.
  - Pika e aksesit bën gjithë autentikimin dhe menaxhimin kyç.
  - Të gjithë përdoruesit duhet të njohin një çelës fillestar pre-shared key (PSK).
  - Secilit, më vonë i jepet një çelës unik.

7.4: Modelet 802.1X dhe PSK

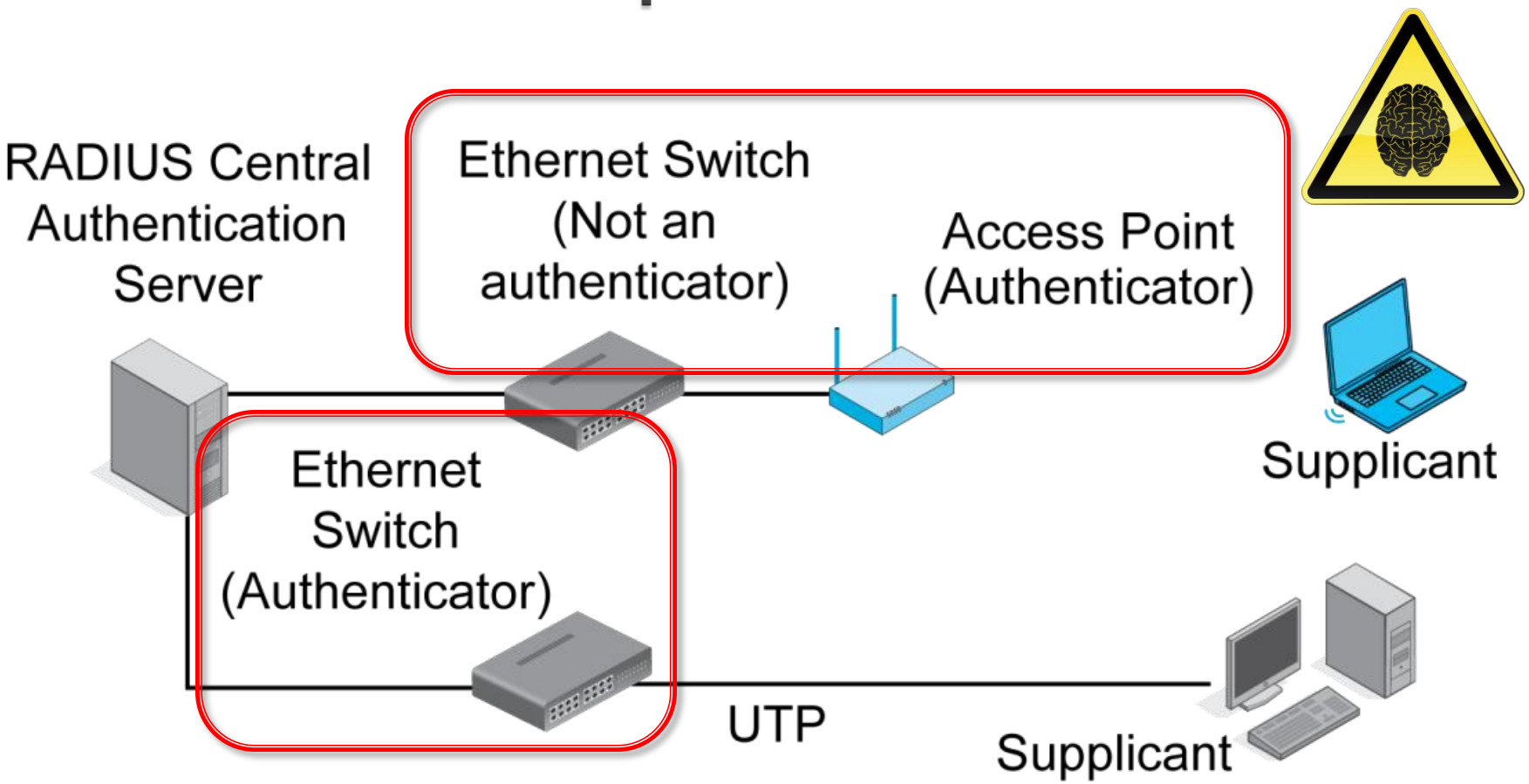
- **Modeli Pre-Shared Key**
  - Nëse pre-shared key është i dobët, ai mund të krakohet lehtë.
  - Fjalëkalimet që gjenerojnë çelësat duhet të jenë të paktën 20 karaktere të gjatë.
  - Aleanca Wi-Fi Alliance e quan këtë *Modeli Personal.*

8.4: Modelet 802.1X dhe PSK

	Mund të përdorë 802.1X?	Mund të përdorë PSK?
WPA	Po	Po
802.11i	Po	Po

Si WPA dhe 802.11i përdorin të dyja modelet.
Kjo nuk është çudi sepse WPA ka derivuar nga 802.11i.

Modeli 802.1X për 802.11i dhe WPA

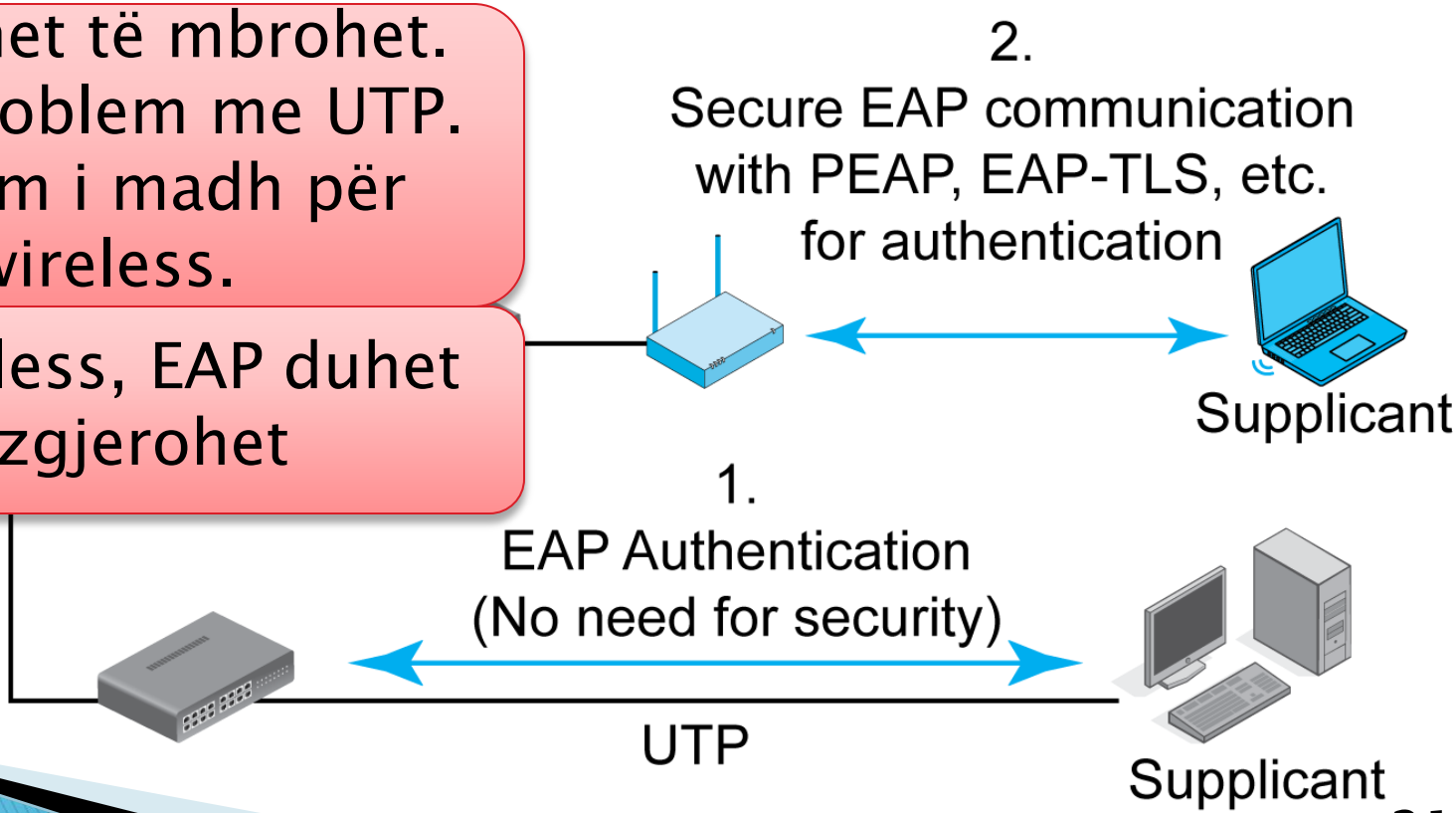


8.4: Modeli 802.1X dhe PSK

- **Modeli 802.1X** (shiko figurën 8-5)
  - Modeli 802.1X në WPA dhe 802.11i mbron komunikimin klient-pikë aksesi me një protokoll të gjerë autentikimi (**Extensible Authentication Protocol**).

EAP duhet të mbrohet. Asnjë problem me UTP. Problem i madh për wireless.

Për wireless, EAP duhet të zgjerohet

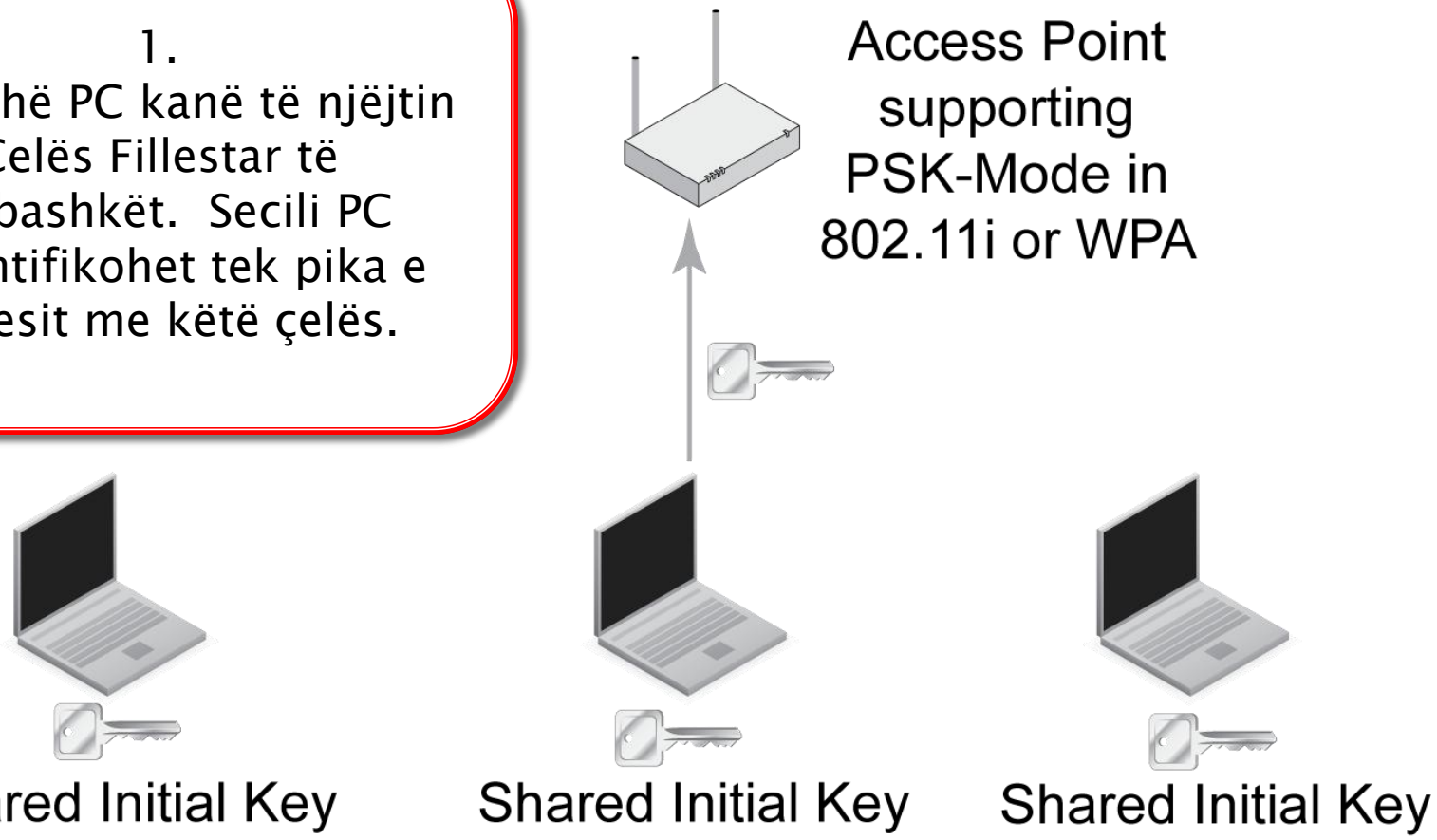


8.4: Modelet 802.1X dhe PSK

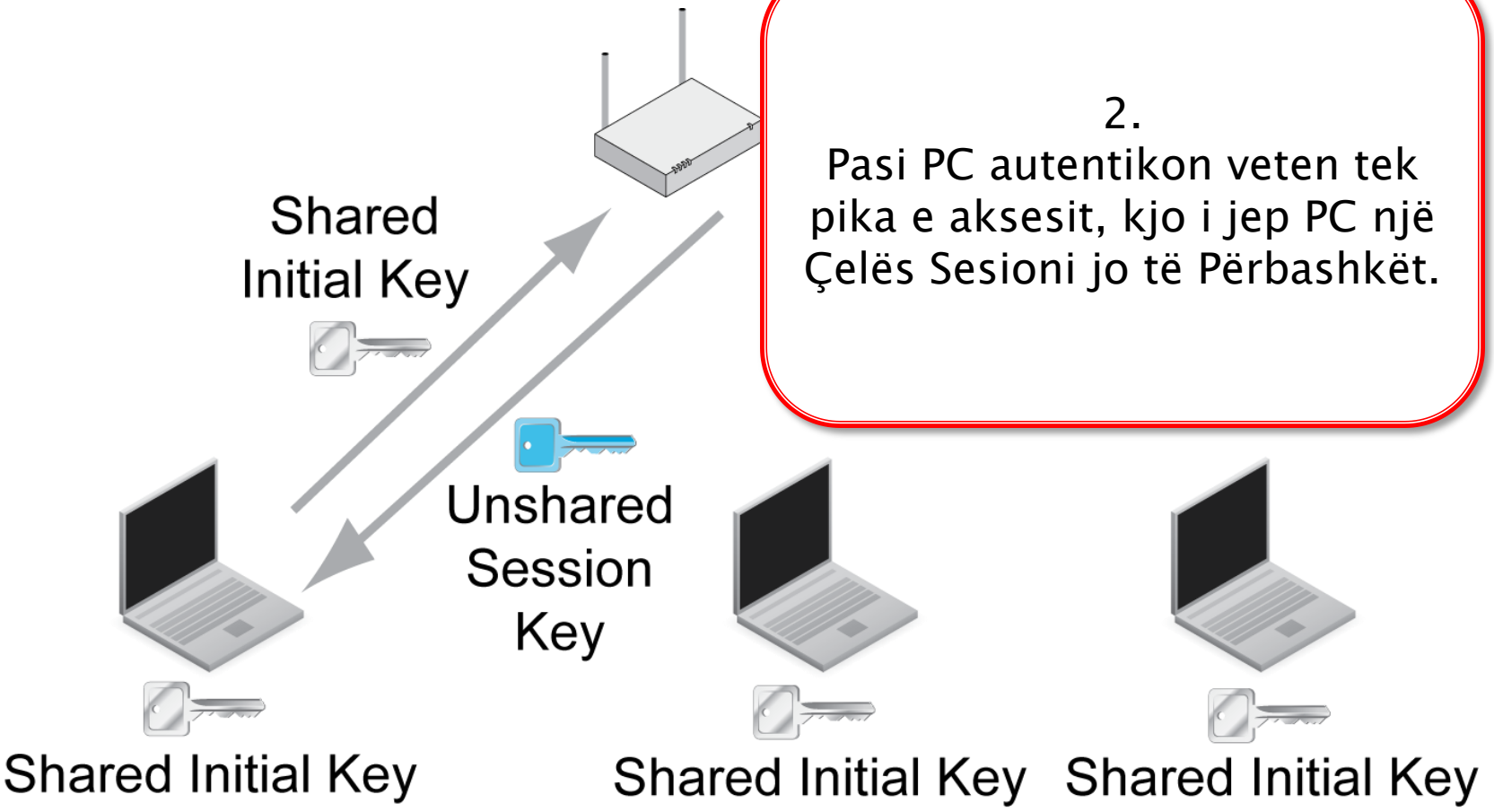
- **Modeli 802.1X** (shiko figurën 8-5)
  - Standardi 802.1X mbron komunikimin me një Extensible Authentication Protocol (protokoll të gjerë autentikimi).
    - Ekzistojnë **disa versione të EAP** me mbrojtje të ndryshme të sigurisë.
    - Firmat që implementojnë 802.1X duhet të zgjedhin një.
    - EAP i Mbrojtur (**PEAP** – Protected EAP) është më popullori sepse Microsoft e favorizon atë.

8.6: 802.11i dhe WPA në modelin Pre-Shared Key

1.
Të gjithë PC kanë të njëjtin Çelës Fillestar të Përbashkët. Secili PC autentifikohet tek pika e aksesit me këtë çelës.



8.6: 802.11i dhe WPA në modelin Pre-Shared Key



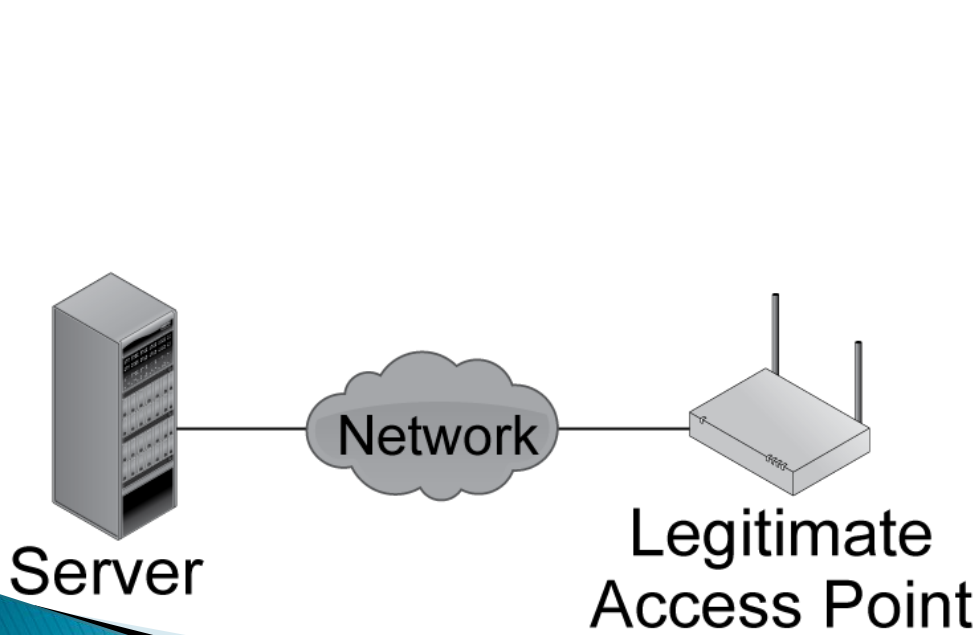
2.
Pasi PC autentikon veten tek pika e aksesit, kjo i jep PC një Çelës Sesioni jo të Përbashkët.

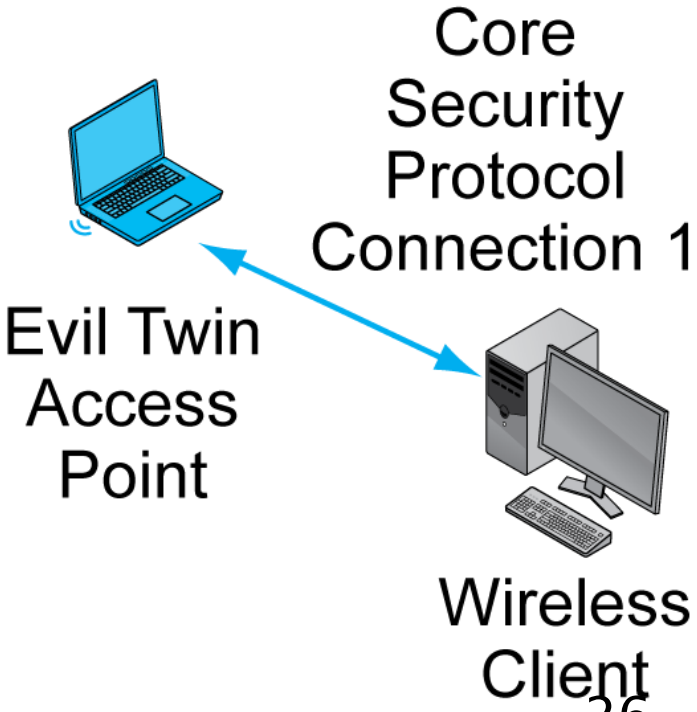
8.6: 802.11i dhe WPA në modelin Pre-Shared Key

- **WEP**
  - Përdor të njëjtin çelës të përbashkët për çdo njeri
  - Ai përdoret për sasi të madhe trafiku
  - Kjo e bën çelësin lehtësisht të thyeshëm
- **Modeli PSK në 802.11i**
  - E përdor çelësin iniciues të përbashkët vetëm për komunikimin fillestar, kështu që nuk mund të thyhet
  - Vetëm pak njerëz e ndajnë atë çelës kështu që nuk do ta japin tek të tjerët
  - Çdo host pastaj merr një çelës të ndryshëm
  - Shumë pak trafik dërgohet me këtë çelës për tu thyer

8.7: Evil Twin Access Point

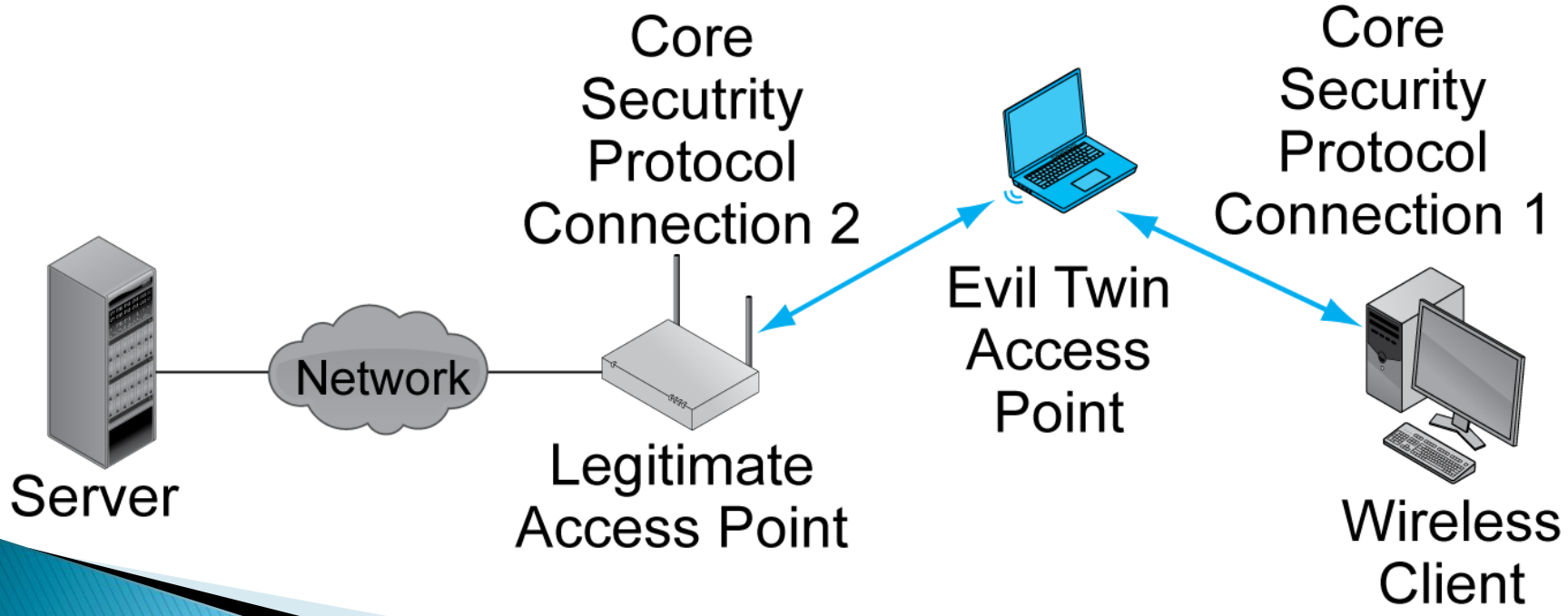
- Vendoset jashtë vendndodhjeve ose në një ***wireless hot spot***
  - Një PC me software për të rivalizuar një pikë aksesi
  - Ndjell një klient wireless për tu shoqëruar me të





8.7: Evil Twin Access Point

- Ndërton një lidhje të dytë me një pikë aksesi legjitime
  - Gjithë trafiku midis klientit wireless dhe serverave të rrjetit kalon nëpërmjet ***evil twin***.

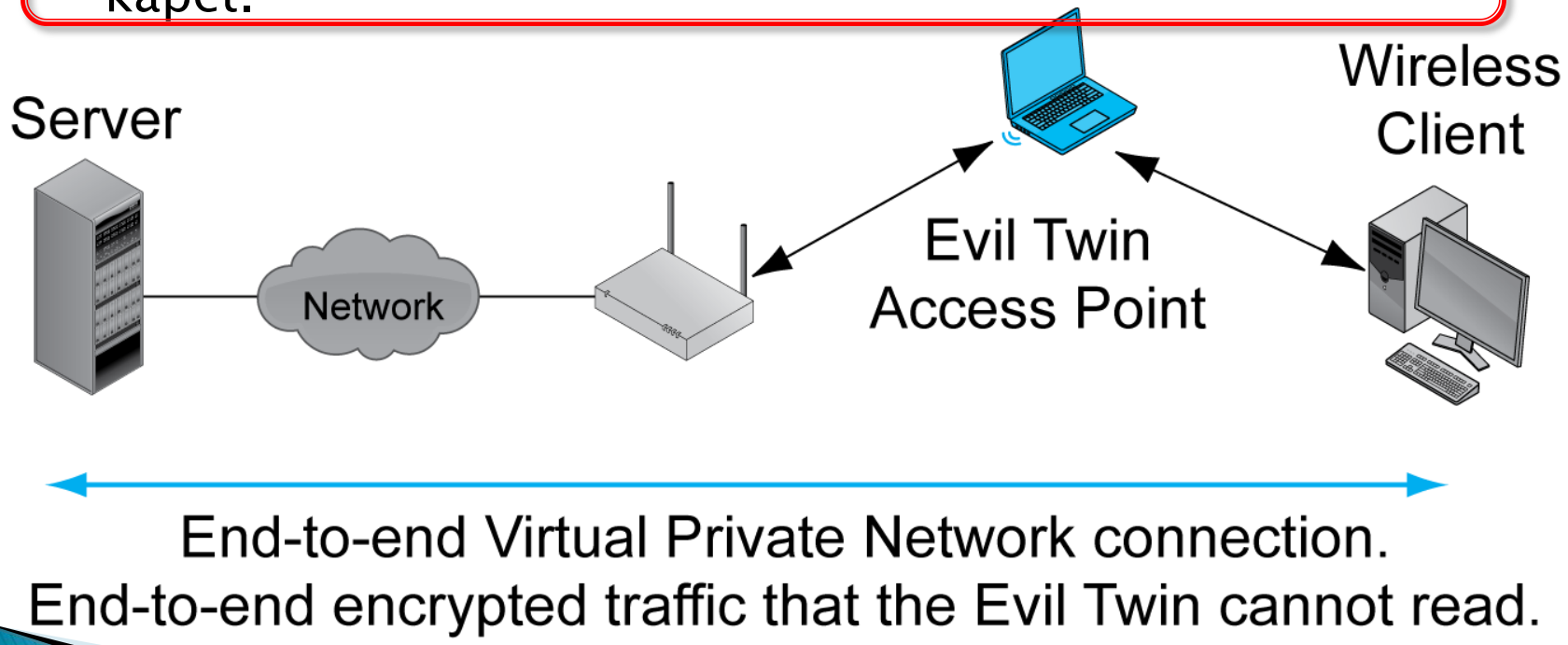


8.7: Evil Twin Access Point

- Ky është një sulm klasik ***man-in-the-middle*** (një njeri ndërmjet)
- Sulme mbi konfidencialitetin sepse *evil twin* lexon gjithë trafikun
  - Klienti enkripton trafikun.
  - *Evil twin* e dekripton atë dhe e lexon.
  - *Evil twin* e rienkripton dhe e dërgon.
- *Evil twin* gjithashtu mund të dërgojë paketa sulmi, të cilat nuk kalojnë kufirin e firewall-it.

8.8: Përdorimi i VPN kundër Evil Twins

- **Virtual Private Networks (VPNs)**
  - Enkriptim skaj më skaj me një sekret të përcaktuar paraprakisht midis client-server
  - Sekreti nuk transmetohet kurrë kështu që nuk mund të kapet.



Wi-Fi Protected Setup

- Zakonisht quhet thjesht WPS
- Protokoll i krijuar për të bërë më lehtë lidhjen midis klientit dhe pikës së aksesit
- Shumë popullor
- Krijuar nga Aleanca Wi-Fi, nuk është pjesë e Komitetit 802

Wi-Fi Protected Setup

- Dizajn i varfër
- Pre-shared keys mund të krakohen me afro 5,500 tentativa
  - E lehtë për tu bërë me sulme automatike
- Zgjidhja e vetme është të fiket WPS tek router
  - Shumë routera madje nuk mund ta fikin atë
- Ky është një problem për PSK por jo për 802.1X

Sulmet Denial-of-Service (DoS)

- Mbingarkojnë pikën e aksesit me trafik
- Ose dërgojnë komanda për të kapur një klient për ta larguar nga një pikë aksesi
- Jo të zakonshëm por të rezikshëm

802.11 Siguria

802.11 LAN Menaxhimi

Teknologji të tjera lokale wireless

8.9: Menaxhimi i WLAN

- **Vendosja e Pikës së Aksesit në një Ndërtesë**
  - Duhet të bëhet me kujdes për një mbulim të mirë dhe për të minimizuar interferencën midis pikave të aksesit.
  - Shtrihet në një reze nga 30-metra në 50-metra në projekt.
  - Rregullohet për probleme të dukshme potenciale të tilla si muret me tulla.
  - Në ndërtesat me disa kate, interferenca duhet të konsiderohet në të tre dimensionet.

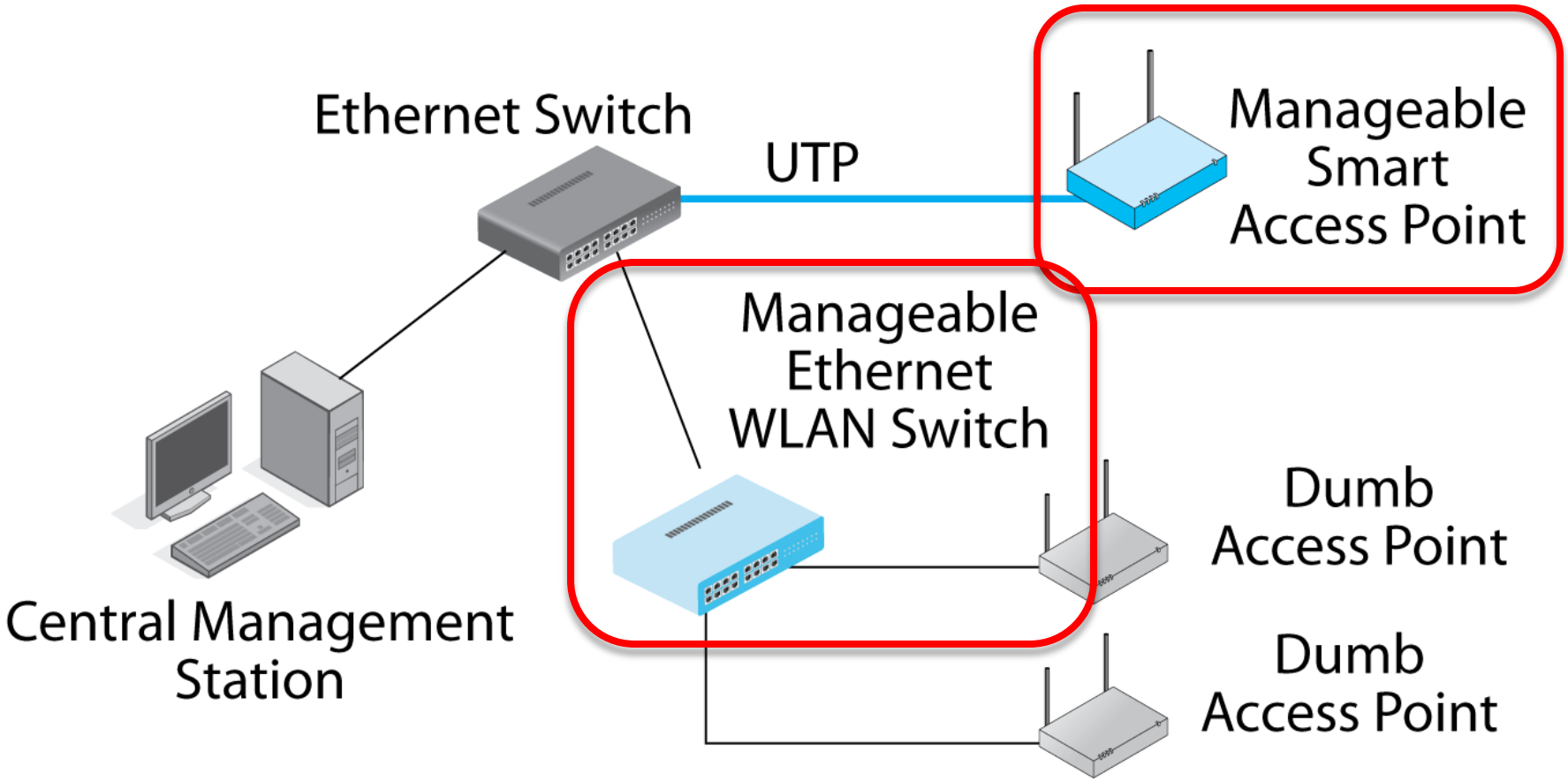
8.9: Menaxhimi i WLAN

- **Vendosja e Pikës së Aksesit në një Ndërtesë**
  - Instalohet pika e aksesit dhe bëhet survejim i ndërtesës për të përcaktuar cilësinë e sinjalit.
  - Rregullohet pozicioni dhe fortësia e sinjalit siç nevojitet.
  - Në pikat e aksesit komerciale, fortësia e sinjalit dhe informacione të tjera të konfigurimit mund të kontrollohen në mënyrë aktive.

8.9: Menaxhimi i WLAN

- **Menaxhimi i Pikave të Aksesit në Distancë**
  - Puna që duhet bërë për të menaxhuar shumë pika aksesi mund të jetë shumë e madhe.
  - Ato patjetër duhen menaxhuar.

8.10: Alternativa të Menaxhimit të Pikave të Aksesit Wireless



8.9: Menaxhimi i WLAN

- **Menaxhimi i Pikave të Aksesit në Distancë**
  - **Funksionaliteti i dëshiruar për rrjetin:**
    - Të informojnë menjëherë administratorin e WLAN për dëmtimet.
    - Të mbështesin rregullimin e pikës së aksesit në distancë.
    - Duhet të sigurojnë monitorim të vazhdueshëm të cilësisë së transmetimit.
    - Të lejojnë përditësim të softwareve tek të gjitha pikat e aksesit ose switche-t e WLAN.
    - Të funksionojnë automatikisht sa herë të jetë e mundur.

7.9: Menaxhimi i WLAN

- **Menaxhimi i pikave të aksesit në distancë**
  - Funksionaliteti i dëshiruar për sigurinë:
    - Të njoftojë administratorin për *rogue access points.*
    - Të njoftojë administratorin për *evil twin access points.*
    - Të njoftojë administratorin për rjedhën e sulmeve *denial-of-service*.
    - Të njoftojë administratorin për sulmet me mesashe larguese *denial-of-service attacks*.
    - Menjëherë të mohojë aksesin në stacione të tilla me kushtet e përcaktuara më sipër.

802.11 Siguria

802.11 LAN Menaxhimi

Teknologji të tjera lokale wireless

7.12: Teknologji të tjera Wireless

	802.11i	Bluetooth	Near Field Communi-cation (NFC)	Ultrawideband (UWB)
Përdorimi	Infrastrukturë tipike e LAN-eve lidhurme Ethernet switches; Wi-Fi Direct jep komunikim direkt midis dy pajisjeve wireless	Personal area networks (PANs) në një tavolinë ose rreth një personi	Komunikim shumë i afërt midis dy hosteve wireless	Shpejtësi ekstremisht e lartë, distancë shumë e shkurtër komunikimi

7.12: Teknologji të tjera Wireless

	802.11i	Bluetooth	Near Field Communi-cation (NFC)	Ultrawideband (UWB)
Shpejtësia tipike	20–300 Mbps	2 Mbps	106, 212, ose 424 kbps	100 Mbps
Shtrirja e shërbimit	30–50 m	10 m	10 cm	10 m
Energjia e kërkuar	Po	Jo	Jo	Po
Banda e shërbimit	2.4 and 5 GHz	2.4 GHz	13.56 kHz	Kanalet UWB zakonisht shtrihen në shumë banda shërbimi

8.11: Bluetooth

- **Për Personal Area Networks (PAN)**
  - Pajisje në trupin e njeriut ose pranë tij (kufje, telefona mobile, netbook kompjuter, etj.)
  - Pajisje në një tavolinë (kompjuter, mouse, tastjerë, printer)

8.11: Bluetooth

- **Teknologjia e Zëvendësimit të Kabllit**
  - Për shembull, me një telefon Bluetooth, mund të printoni pa pasur kabëll, tek një printer pranë që ka Bluetooth
  - Nuk përdor pikë aksesi
  - Përdor komunikim direkt pajisje me pajisje

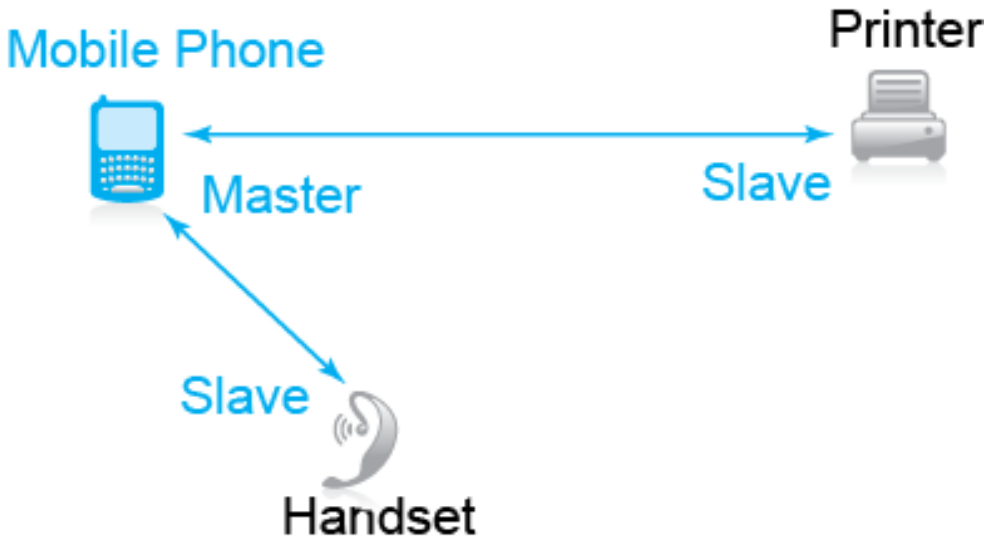
7.13 Modelet e operimit të Bluetooth

	Classic Bluetooth	High-Speed Bluetooth	Low-Energy Bluetooth
Përfitimi kryesor	Performancë e mirë me energji të ulët	Transferim me shpejtësi të lartë kur është e nevojshmë	Jetëgjatësi baterie dhe kohë shumë e shpejtë lidhje
Shpejtësia	Deri në 3 Mbps	Deri në rreth 24 Mbps	Deri në 200 kbps
Cikli i detyrës i pritshëm	Nga i ulët tek i lartë	Nga i ulët tek i lartë	Shumë i ulët
Energjia e kërkuar	E ulët	E lartë	Shumë e ulët
distanca	~10 m	~30 m	~15 m
Koha e lidhjes	< 6 s	Nuk jepet	< 3 ms

7.14: Operimi i Bluetooth

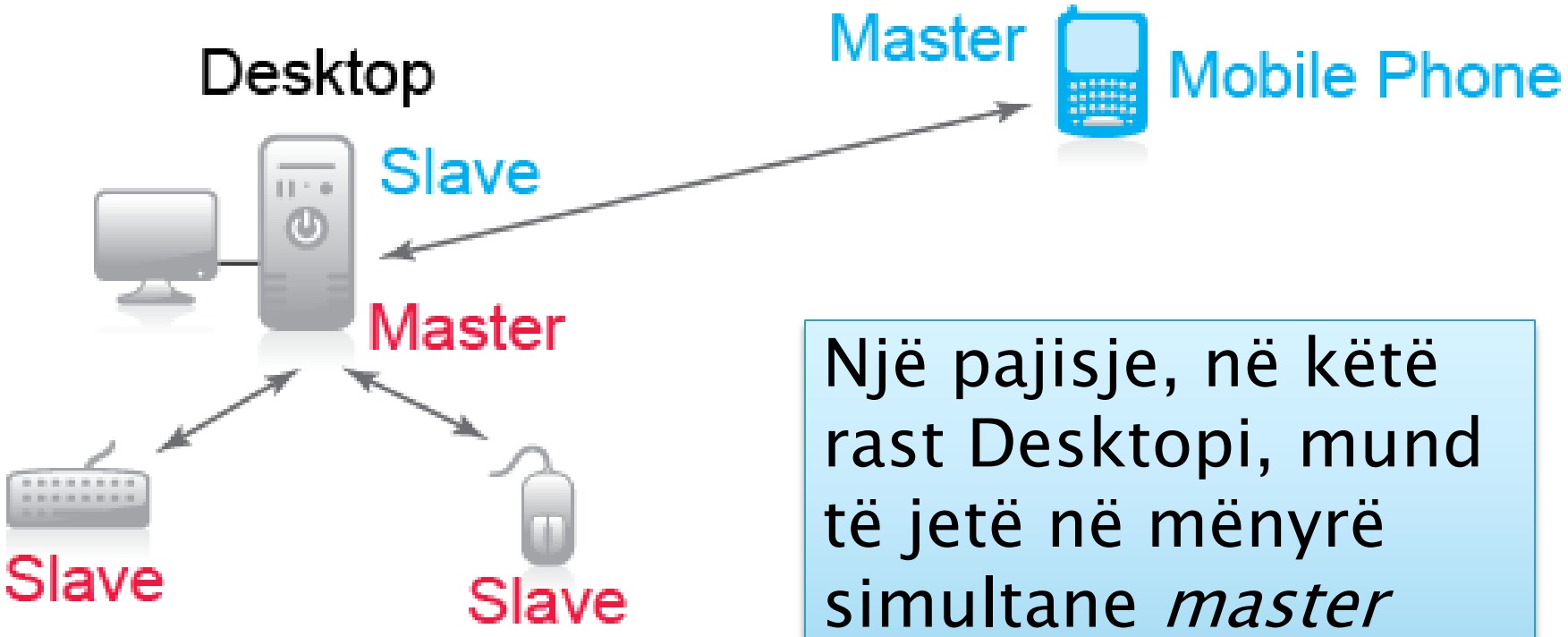
Lidhjet Bluetooth janë lidhje një-me-një

Një *master* dhe një *slave* është quajtur kolektivisht një *piconet*



Një *master* mund të ketë deri në 7 *slave*, kështu që një *piconet* mund tëketë deri në 8 pajisje

7.14: Operimi i Bluetooth

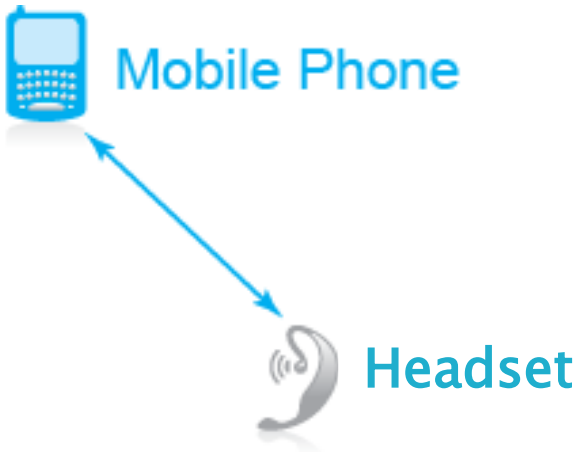


Një pajisje, në këtë rast Desktopi, mund të jetë në mënyrë simultane *master* dhe *slave*.

7.14: Operimi i Bluetooth

Kufja fillon si master nëse telefonata iniciohet nga ajo.

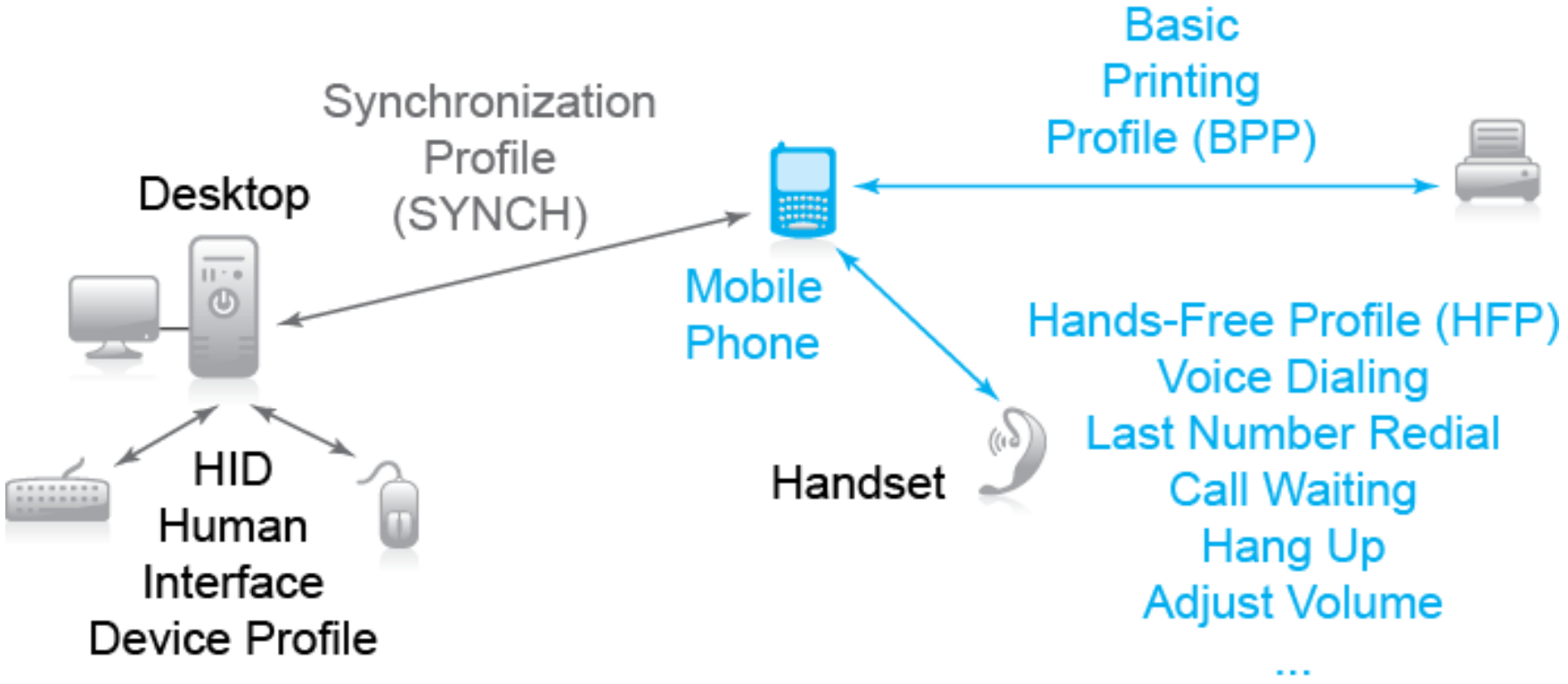
Zakonisht telefoni mobile merr rolin e masterit më vonë.



8.11: Bluetooth

- **Avantazhet krahasuar me 802.11**
  - Harxhon pak bateri, kështu që kohëzgjatja e baterisë midis karrikimeve është e gjatë
  - Profili i Bluetooth (printim, telefon, kufje, tasjerë dhe mouse wireless, etj.)
    - Nuk nevojitet konfigurim specifik për secilën pajisje
  - Disi minimal
  - Pajisjet tipikisht automatizojnë disa profile Bluetooth

7.14: Bluetooth Operation



Bluetooth Profiles

7.15 Bluetooth Peering dhe Binding

- **Peering**
  - Kur dy pajisje së pari takojnë njëra – tjetrën duhet të kalojnë në një proçes negocimi.
  - Ky proçes negocimi quhet *peering*.
  - Ai përfshin shkëmbimin e informacioneve të pajisjeve.
  - Mund të përfshijë autentikim.
  - Gjithashtu përfshin një ose të dy zotëruesit e pajisjeve që të vendosin nëse pajisjet duhet të komunikojnë .

7.15: Bluetooth Peering dhe Binding

- **Service Discovery Profile (SDP)**
  - *Peering* përdor Service Discovery Profile (SDP).
  - Normalisht, një pajisje operon në modelin që mund të arrihet (dedektohet).
  - Nëse ajo merr një kërkesë Service Discovery Protocol, ajo do të dërgojë informacione për veten:
    - Emrin
    - Klasën e pajisjes
    - Profilin e Bluetooth që suporton
    - Informacione teknike si emri i prodhuesit

7.15: Bluetooth Peering dhe Binding

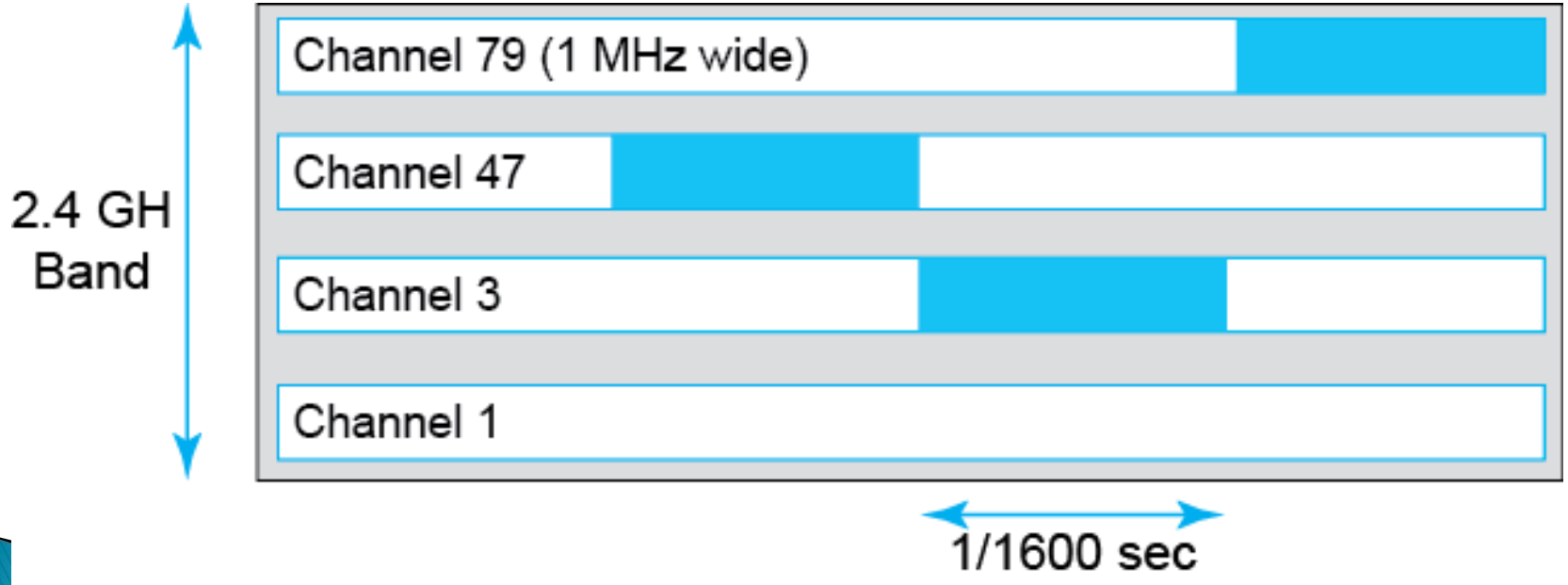
- **Binding**
  - Pasi *peering* ka përfunduar, thuhet se të dy pajisjet janë bashkuar *bound*.
  - Mund të fillojnë të komunikojnë.
  - Edhe nëse do të komunikojnë më vonë ato janë të bashkuara njëherë.
  - Do të fillojnë të komunikojnë pa e bërë proçesin e *peering*.
  - Kjo lejon një lidhje të shpejtë.
  - Zotëruesi i secilës pajisje mund të përfundojë proçesin e bashkimit *binding*.

7.16: Frequency Hopping Spread Spectrum

- 802.11 Wi-Fi përdor kanale 20 MHz ose 40 MHz në bandën 2.4 GHz dhe5 GHz.
- Bluetooth operon në bandën 2.4 GHz.
- Bluetooth e ndan bandën në 79 kanale, secili 1 MHz i gjerë.

7.16: Frequency Hopping Spread Spectrum

- Valët e radios Bluetooth kërkcejnë midis frekuencave deri në 1,600 herë në sekondë.
- Këto valë shmangin kanalet ku janë aktive pajisjet e tjera (përfshi edhe pajisjet 802.11).



7.17: Near Field Communication (NFC)

Radio Power Requirements are Minimized by:

Distancë e shurtër transmetimi (0 deri në 4 cm)ose (0 deri në 2 inç)
Shpejtësi e ulët (106 kbps, 212 kbps, ose 424 kbps) dhe
Operim në banë me frekuencë të ulët 13.56 kHz

7.18: Aplikime të mundshme NFC

- Pagesa shërbim autobuzi (shumë popullore në disa vende)
- Hapja e dyerve të makinave
- Ndezja e makninës
- Kontroll i hyrjes nëpër ndërtesa
- Shkëmbim i kartvizitave

- vazhdon…

7.18: Aplikime të mundshme NFC

- Këmbimi i faqeve web midis pajisjeve mobile
- Pagesa në dyqane me pakicë, përfshi edhe kartat e besnikërisë dhe kuponat (kanë filluar të bëhen popullore)
- NFC postera me pika takmi për komunikim
- Radio Frequency ID (RFID) Tags Pasive

8.13: Teknologjitë Lokale Wireless që po shfaqen

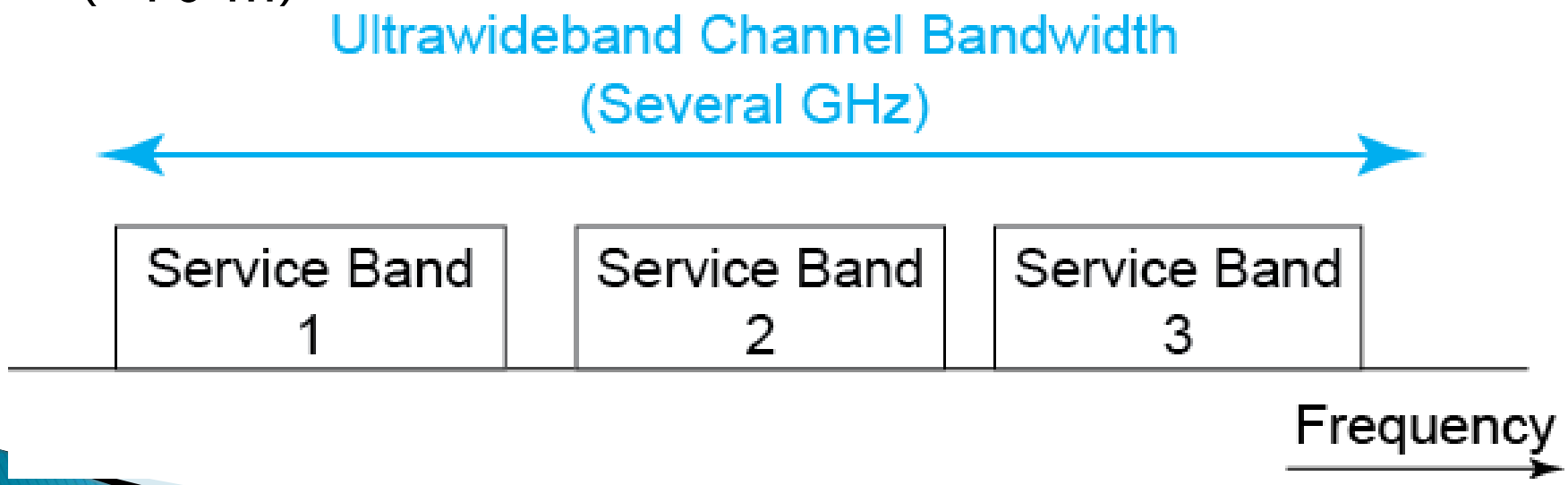
- **RFID**
  - Si etiketat e bar-kodeve por që lexohen në distancë
  - Disa furnizohen nga energjia e skanerit

7.19 Passive Radio Frequency ID Tags

- Radio frequency ID tags përmbajnë informacine për një produkt
- Passive RFID tag nuk ka burim energjie të brendshëm.
- Kur lexohet nga një pajisje NFC, energjia e kërkesës së lexuesit furnizon me energji edhe për përgjigjen.
- 13.56 kHz u specifikuar nga ISO/IEC për passive RFID tags shumë më përpara se të krijoheshin standardet NFC .
- Me antenë sensitive, transmetimet NFC përgjohen nga distanca

7.20 Transmetimet Ultrawideband

- Kanale shumë të gjera
- Energji shumë e ulët për hertz për të shmangur interferencën me transmetimet e tjera
- Shpejtësi shumë e lartë në distancë të shkurtër (~10 m)



7.21 Siguria në Teknologjitë Wireless që po shfaqen

- Kërcënimet
  - Përgjimet
  - Modifikimi i të dhënave
  - Imitimet
  - Sulmet Denial-of-service

7.21 Siguria në Teknologjitë Wireless që po shfaqen

- Siguria kriptologjike
  - Disa teknologji lokale wireless nuk kanë siguri kriptologjikehave .
  - Shembull: NFC për të lexuar passive ID tags.
  - Ato mbështeten mbi transmetimin në distancë të shkurtër për të penguar përgjuesit.
  - Antenat direkte dhe amplifikuesit mund të mbrojnë prej kësaj.

7.21 Siguria në Teknologjitë Wireless që po shfaqen

- Shkalla e sigurisë
  - Disa kanë siguri të mirë.
  - Shembull : Bluetooth
  - Megjithatë , akoma jo aq të fortë sa siguria në 802.11i dhe WPA.

7.21 Siguria në Teknologjitë Wireless që po shfaqen

- Humbja ose vjedhja e pajisjeve
  - Në epokën e *bring your own device* (BYOD) në punë, ky është një problem serioz.
  - Shumica e pajisjeve mbrohen nga një PIN i shkurtër.

7.21 Siguria në Teknologjitë Wireless që po shfaqen

- Pjekuria
  - Në përgjithësi, teknologjitë e reja të sigurisë duan ca kohë të maturohen.
  - Gjatë kësaj periudhe, ato shpesh kanë dobësi që duhet të rregullohen shpejt.
  - Kompanitë përdoruese duhet të forcojnë sigurinë për çdo teknologji të re.