DECOIT

CAST-Workshop

Technologie-Entwicklung: grenzenlose Bandbreiten und Dienste für alle?

Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
detken@decoit.de

© Consultancy & Internet Technologies

Kurzvorstellung der DECOIT GmbH

- Fokus: Herstellerneutrale, ganzheitliche Beratung
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
- Bereich Systemmanagement: Anbieten von Herstellerlösungen oder stabilen Open-Source-Lösungen
- Bereich Software-Entwicklung: Anbieten von selbst entwickelten Individuallösungen mit hohem Innovationscharakter oder Produktlösungen
- Sitz: Technologiepark an der Universität Bremen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen bzw. Universitäten
- Zur Know-how-Bildung und Prototypenentwicklung: regelmäßige Teilnahme an Forschungsprojekten

DECOIT

Inhalte

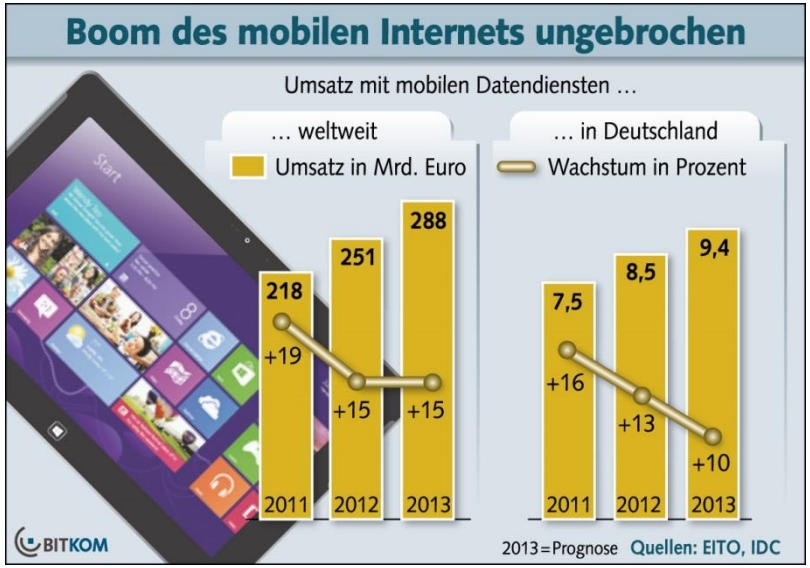
- Von Ethernet zu 100GBit/s-Datenraten
- Mobilfunknetze der nächsten Generation: 4G und LTE
- Entwicklung der Wireless-Technologien in Unternehmensnetzen
- Ausblick und Trends

Steigende Breitbandanschlüsse

- Breitband-Boom in Deutschland setzt sich fort
- 4 von 5 Haushalten nutzen einen schnellen Internet-Zugang (78%)
- Zahl der Anschlüsse hat sich seit 2004 vervierfacht
- Günstige Anschlüsse sind durch Kombination von Telefonie, Fernsehen und Internet verfügbar
- Durch LTE sollen die letzten „weißen Flecken“ bereinigt werden

Das mobile Internet boomt

- Umsatz mit mobilen Datendiensten hat sich seit 2005 verdoppelt
- Weltweit wächst der Markt für mobile Datendienste voraussichtlich um 15% auf 288 Milliarden Euro
- In 2013 nutzen in Deutschland 44% mobile Datendienste
- Treiber sind die steigende Nachfrage nach Smartphones und Tablets sowie die schnelleren Übertragungsraten



Neue Dienste durch wachsende Bandbreite?

- Jahrelang hatten Carrier und Provider das Problem, dass zwar immer mehr Bandbreite zur Verfügung stand, aber die Dienste dafür fehlten
- Auch heute werden fast nur traditionelle Dienste im Festnetzumfeld angeboten wie Videostreaming, VoIP, Internet (sog. Triple Play)
- Allerdings lassen sich neue Geschäftsmodelle erkennen
  - Cloud Computing
  - Collaboration Platforms
  - Remote Services
- Zudem schaffen mobile Zugangsmöglichkeiten neue Dienste

Ethernet (IEEE 802.3)

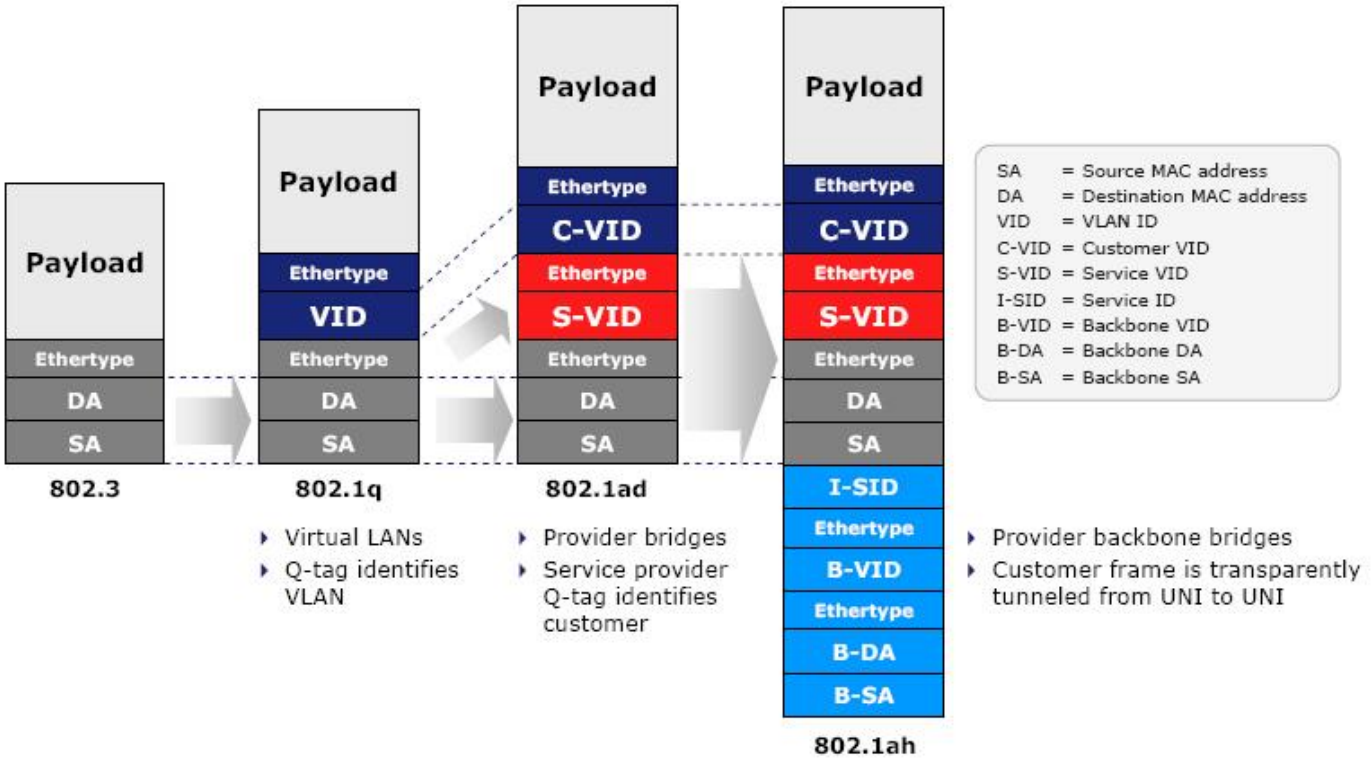
- Erste Gemeinschaftsentwicklung 1973 von Digital, Intel und Xerox (DIX) mit Datenrate von 10 MBit/s
- Einsatz unterschiedlichster Übertragungsmedien (Telefonkabel, IBM TR-Kabel, Koaxkabel und LWL)
- Funktionalität auf die ersten beiden OSI-Schichten begrenzt
- CSMA/CD-Verfahren mit Kollisionserkennung
- Thick-Ethernet und Thin-Ethernet (Cheapernet) für Reichweiten von 500 m (10Base-5) 200 m (10Base-2) konzipiert
- Zugriff auf physikalisches Medium erfolgt über Transceiver
- Max. Rahmengröße ist 1.518 Byte (1.500 Byte Nutzdaten)
- Konzipiert für reine Datenübertragungen, ohne jegliche Quality-of-Service-Mechanismen

Ethernet-Evolution

- Im Dezember 2007 wurde von IEEE die Entscheidung getroffen, die 10-Gigabit-Ethernet-Technik weiter zu entwickeln
  - P802.3ba 40 GBit/s
  - 100 Gbit/s Task Force
- Zum Schutz bestehender Investitionen wird der Grundstandard 802.3 weiterhin als Basis verwendet
  - Unterstützung des Full-Duplex-Betriebs
  - Beibehaltung der bestehenden Frame-Formate aus CSMA/CD und Ethernet V2.0
  - Volle Unterstützung für bestehende Standards 802.1D (Spanning Tree) und 802.1Q (VLAN)
  - Übernahme der bisherigen minimalen (64 Byte) und maximalen (1.518 Byte) Rahmenlänge
  - Eine Bitfehlerrate (Bit Error Rate) von besser als 10^{-12} wird notwendig

Cisco CRS-3: 1-Port 100 Gigabit Ethernet Interface Module

Provider Backbone Bridging (802.1ah)

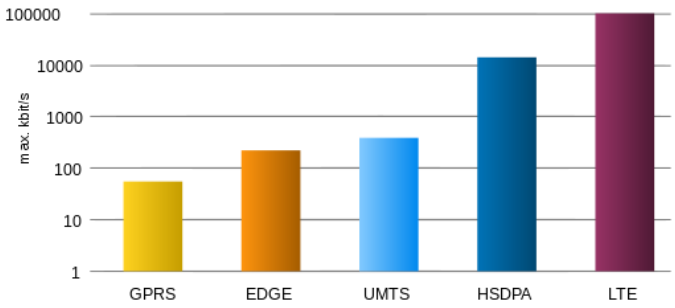


Ausblick zu Ethernet

- Nicht nur die Gerätehersteller, sondern auch die Chip- und Kartenhersteller waren aktiv an der Entwicklung des Standards beteiligt
- Anwendungen sind im Bereich der Hochleistungsserver, Grid Computing, Blade-Controller/-Server, Storage Area Networks (SAN) vorhanden
- Die Technik der Wählnetze und TDM-Verfahren sowie von SONET/SDH wird weiter durch Ethernet abgelöst werden
- Eine garantierte Bandbreite kann immer noch nicht abgegeben werden – nur eine hohe Wahrscheinlichkeit für Qualitätsparameter
- Besser geeignete Netztechnologien wie ATM, sind leider auf der Strecke geblieben
- IT-Sicherheit wurde im Standard nach wie vor nicht berücksichtigt und muss von höheren Schichten übernommen werden

Von GSM zu LTE

- Das GSM-Netz (2G) wurde als reines Sprachnetz konzipiert
- Datenübertragungen waren kaum vorgesehen (Ausnahme: Faxmodem und SMS-Nachrichten)
- Die Umsetzung des mobilen Internet wurde durch ein zweites Netz auf Basis von General Packet Radio Service (GPRS) vorangetrieben
- Enhanced Data Rates for GSM Evolution (EDGE) ermöglicht die Erhöhung der Datenübertragungsrate in GSM-Mobilfunknetzen durch neues Modulationsverfahren
- Vorhandene Bandbreite von GSM wird mehrfach ausgenutzt (max. 220 kBit/s)
- Aufrüstung der Basisstationen ist möglich



Universal Mobile Telecommunications System (UMTS)

- Das UMTS der dritten Generation (3G) hat Daten und Sprache zu einem Netz zusammengeführt
- Zuerst waren max. 2 MBit/s vorgesehen, die aber durch HSPA+ (HSDPA und HSUPA) heute auf bis zu 42 MBit/s erhöht werden können
- Neue Funkzugriffstechnik Wideband CDMA ermöglicht die höheren Übertragungsraten
- Bündelung der Kapazität der Basisstationen führt allerdings zu schnellerer Auslastung
- Es sind unterschiedliche Releases standardisiert worden, die das Kernnetz und die Schnittstellen unterschiedlich definieren

GSM und UMTS – die IT-Sicherheit

- GSM
  - Angreifer können sich als Basisstation ausgeben (keine Authentifizierung der Basisstation vorgesehen)
  - Schlüssellängen sind zu kurz für Brute-Force-Attacken
  - Schlüssel werden unverschlüsselt im Kernnetz übertragen
  - Sicherheitsalgorithmen wurden geheim gehalten
- UMTS
  - Es wird auf Standardverfahren zur Absicherung gesetzt
  - Hauptschlüssel wird niemals über das Netz übertragen
  - Angreifer kann sich nicht mehr einfach als Basisstation ausgeben
  - Sicheres Kernnetz kann nicht mehr angenommen werden, da das Backbone durch unterschiedliche ISP bereitgestellt werden kann
  - IPsec kann man zur Authentifizierung/Verschlüsselung verwenden
  - Unterschiedliche Release-Stände können sich negativ auswirken

LTE – die vierte Generation

- Long Term Evolution (LTE) wird als 3,9G-Mobilfunkstandard bezeichnet
- Grundschema von UMTS bleibt erhalten, weshalb vorhandene Basisstationen relativ einfach erweitert werden können
- Frequenzvergabe war mit der Auflage verbunden, Regionen mit schlechter Abdeckung zuerst anzugehen
- Datenraten von bis zu 300 MBit/s sollen zwischen 800 MHz und 2.600 MHz ermöglicht werden
- Nutzinformation mit hoher Datenrate wird auf mehrere Datenströme mit niedrigerer Datenrate per OFDM-Modulationsverfahren aufgeteilt
- Alternativ kann SC-FDMA mit geringerer Leistungsaufnahme verwendet werden
- Multiple Input Multiple Output (MIMO) Technik ermöglicht die gleichzeitige Übertragung unabhängiger Datenströme über den selben Kanal, wodurch höhere Bandbreiten abgedeckt werden können
- Für MIMO sind mindestens zwei Antennen notwendig (2x2 oder 4x4)

LTE – die IT-Sicherheit

- Bei den Schnittstellenvorgaben wird physikalisch auf Ethernet gesetzt
- In der Architektur ist der Diameter-Standard (Nachfolger von RADIUS) enthalten
- Das heißt, es können Einwahlprofile und Verschlüsselungsparamater (AAA) hinterlegt werden
- Für die Verschlüsselung der Verbindungen über Diameter wird TLS oder IPsec verwendet
- Zusätzlich wird als Transportprotokoll SCTP verwendet, welches resistent gegenüber SYN-Flooding und DoS-Attacken ist
- SCTP vereint die Vorteile von TCP und UDP auf Layer 4
- IT-Sicherheit (Abhörsicherheit) ist damit integraler Bestandteil – problematisch ist allerdings die Vielfalt der mobilen Endgeräte (Betriebssystem + Schnittstellen)

Ausblick Mobilfunktechnik

- LTE Advanced erweitert LTE, um weitere Datenraten von bis zu 1 GBit/s
- Bestehende Basisstationen benötigen dann nur noch nur ein Software-Upgrade
- LTE nutzt im Gegensatz zu UMTS verschiedene Spektren (1,4/3/5/10/15/20 MHz)
- Durch die höhere Datenrate am mobilen Endgerät müssen auch die Backbone-Netze mit angepasst werden
- Häufige Nutzung von HSPA bei UMTS beinhaltet oftmals ein Überbuchen der Mobilfunkzelle
- Durch Carrier Aggregation bei LTE kann die MIMO-Technik effizienter genutzt werden und weniger Interferenzen treten auf
- LTE führt den Weg nach mehr Bandbreite konsequent weiter fort – anfangs werden aber geringere Datenraten nur möglich sein
- LTE ermöglicht „neue“ Mobilfunkdienste wie HD-Radio, MMS, Mobile TV und DVB+
- Sprache wird nur noch als „minimaler Service“ bezeichnet

WLAN-Technologien: von „b“ bis „h“

- 1999:
  - 802.11b: Weltweiter Standard (2.4 GHz)
  - 802.11a: 5 GHz, 54 MBit/s, in Deutschland legalisiert
- 2002:
  - 802.11g: Höhere Geschwindigkeit für 802.11b
  - 802.11h: als 802.11a in Europa legalisiert
- 2003
  - Dual-Mode/Dual-Band 802.11g/h
- 2009
  - 802.11n: 600 MBit/s durch MIMO-Technik
- Heute
  - 802.11s: vermaschte Netze
  - 802.11ac: 1,3 GBit/s

Arbeitsgruppe	Arbeitsgebiet
802.11a	54-MBit/s-WLAN im 5-GHz-Band
802.11b	11-MBit/s-WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging
802.11d	"World Mode", Anpassung an regionsspezifische Regulatorien
802.11e	QoS- und Streaming-Erweiterung für 802.11a/g/h
802.11f	Handover für 802.11a/g/h (Inter Access Point Protocol - IAPP)
802.11g	54-MBit/s-WLAN im 2,4-GHz-Band
802.11h	54-MBit/s-WLAN im 5-GHz-Band mit DFS und TPC
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES, 802.1x)
802.11n	600-MBit/s-WLAN durch MIMO-Technik im 2,4- und 5-GHz-Band
802.11r	Fast Handover: Erweiterung für VoIP

WLAN-Standard 802.11n

- Zur Erreichung der höheren Datenrate wird ein höherer Uplink ins Netzwerk benötigt (Gigabit-Ethernet) und mehrere Antennen
- Die Datenrate pro Antenne liegt bei max. 150 MBit/s, wodurch vier Antennen für 600 MBit/s notwendig sind
- Kompatibilität zu älteren WLAN-Systemen wie 802.11b und 802.11g ist gewährleistet
- Multiple Input Multiple Output (MIMO) Technik nutzt mehrere Sende- und Empfangsantennen aus und bündelt den Datenstrom
- Zudem können pro Hz-Bandbreite mehr Bit/s genutzt werden
- MIMO-Technik wird auch in Mobilfunknetzen wie z.B. LTE verwendet

WLAN im Unternehmensnetz

- WLAN-Technologien haben sich im Unternehmensnetz zur Erweiterung der LAN-Umgebung etabliert
- Problematisch waren anfangs die IT-Sicherheit, das Handover-Verhalten und fehlende QoS-Mechanismen
- Zentrale Managementmöglichkeiten sind notwendig sowie eine exakte Planung der Kanäle (Kanalüberlappungen, Sendeleistung, Firmware-Updates)
- Redundanz des zentralen WLAN-Controllers muss ggf. mit eingeplant werden
- Auswahl der Endgeräte sowie Umgebungsmessungen sind ebenfalls relevant

IT-Sicherheit im WLAN-Umfeld

- Anfangs wurde WEP zur Verschlüsselung eingesetzt
  - Dieser konnte nie den Sicherheitsanforderungen gerecht werden, da er den kompromittierbaren RC4-Algorithmus enthielt
  - Zusätzlich wurden nur statische Schlüssel verwendet
- Alternative VPN-Topologien wurden daher eingesetzt
- Wireless Protected Access (WPA) mit Fast Packet Keying, EAP und Kerberos sollten Abhilfe schaffen
  - WPA verwendet dynamische Schlüssel
  - Die Sicherheit hängt aber stark von dem verwendet Passwort ab
  - Außerdem wurde wieder auf den RC4-Algorithmus gesetzt!
- Sicherheitsstandard 802.11i
  - Beinhaltet heute WPA2 und AES-Verschlüsselung
  - RADIUS-Authentifizierung ist integraler Bestandteil

Ausblick Wireless LAN

- Oftmals kommen vor dem Standard proprietäre Lösungen auf den Markt, die keine Kompatibilität besitzen
- Mobile Endgeräte (z.B. Handscanner im Lager) schränken evtl. die IT-Sicherheit ein
- Neue mobile Anwendungen sind denkbar, wie mobile Arbeitsplätze, mobile Datenerfassung, VoIP-Anbindung, Hot-Spots, Vernetzung von Gebäuden ohne IT-Infrastruktur
- Die Bandbreite muss nach wie vor mit anderen Teilnehmern geteilt werden (echtes QoS fehlt – nur Priorisierung ist möglich)
- Weitere Standards werden erarbeitet, um die Datenrate weiter zu erhöhen (1,3 GBit/s und 7 GBit/s)
- IT-Sicherheit ist mit WPA2 und 802.11i inzwischen ausreichend implementiert worden (Endgeräte mussten leistungsfähiger werden)

Zusammenfassung

- Bandbreiten und höhere Datenraten steigen weiter an und werden neue Nutzungsmöglichkeiten schaffen
- Neue Dienste werden durch das mobile Internet maßgeblich beeinflusst
- „Always On“ ist heute durch nahtlose Mobilfunkabdeckung unproblematisch möglich
- WLAN- und Mobilfunkstandards ergänzen sich bzgl. der Abdeckung
- Durch heutige Ethernet-Technologie wächst auch das Backbone entsprechend mit
- Aber:
  - Proprietäre Lösungen erschweren oftmals die Interoperabilität
  - Quality-of-Service (QoS) ist in heutigen Netzen kaum im Einsatz
  - Die IT-Sicherheit wird oftmals vernachlässigt (nachträgliche Integration)
  - Mobile Endgerätevielfalt schafft Sicherheitsprobleme
  - Dienstunterstützung steht im Vordergrund und keine Datensicherheit
  - Der Massenmarkt kennt keine IT-Sicherheit
  - Datenschutz wird durch mobile Massendienste weiter aufgeweicht

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY
CAST

© Consultancy & Internet Technologies