Kreativität und Technik

Vorlesung im Modul 10-201-2334 im Wahlbereich Bachelor GSW sowie im Modul 10-201-2333 im Bachelor Informatik

Sommersemester 2016

Prof. Dr. Hans-Gert Gräbe

http://bis.informatik.uni-leipzig.de/HansGertGraebe

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Privatsphäre im Internet

- Privatsphäre im Internet (als Teil eines durch die allgemeinen Persönlichkeitsrechte garantierten Schutzraums gegen äußeren Durchgriff) ist Teil der allgemeinen Privatsphäre und kann ohne Berücksichtigung dieser Einbindung nicht sinnvoll erklärt werden.
- Privatsphäre im Internet spielt heute vor allem im Außen- und Mittelbereich eine Rolle. Eine entsprechende Abstufung der Sicherheitsmaßnahmen gegen äußeren Durchgriff ist sinnvoll.
- Bei der Gestaltung der Privatsphäre im Internet sind Subjekte in hohem Maße auf technische Dienstleistungen und damit auf externe Institutionen angewiesen, deren *Vertrauenswürdigkeit* sie angemessen einschätzen müssen.
- Es ist zwischen privaten *Daten* (Zustand) und zur Ausführung gelangenden *Algorithmen* (Zustandsänderung) zu unterscheiden, die für die Privatsphäre relevant sind.

Digitale Privatsphäre

- Ordnungsrechtliche Regelungen der Privatsphäre im Internet existieren erst in Ansätzen, so dass *angemessenes praktisches Handeln* sowie *kooperative Gestaltung* auf vertragsrechtlicher Basis Hauptformen der Ausformung eines Begriffs „Privatsphäre im Internet“ sind.
- Ein *angemessenes* Verständnis der technischen Bedingtheiten, Möglichkeiten und Restriktionen des Internets ist für die qualifizierte Gestaltung der eigenen Privatsphäre (verstanden als ein durch die allgemeinen Persönlichkeitsrechte garantierter Schutzraum) im Internet unerlässlich.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Internet Basics

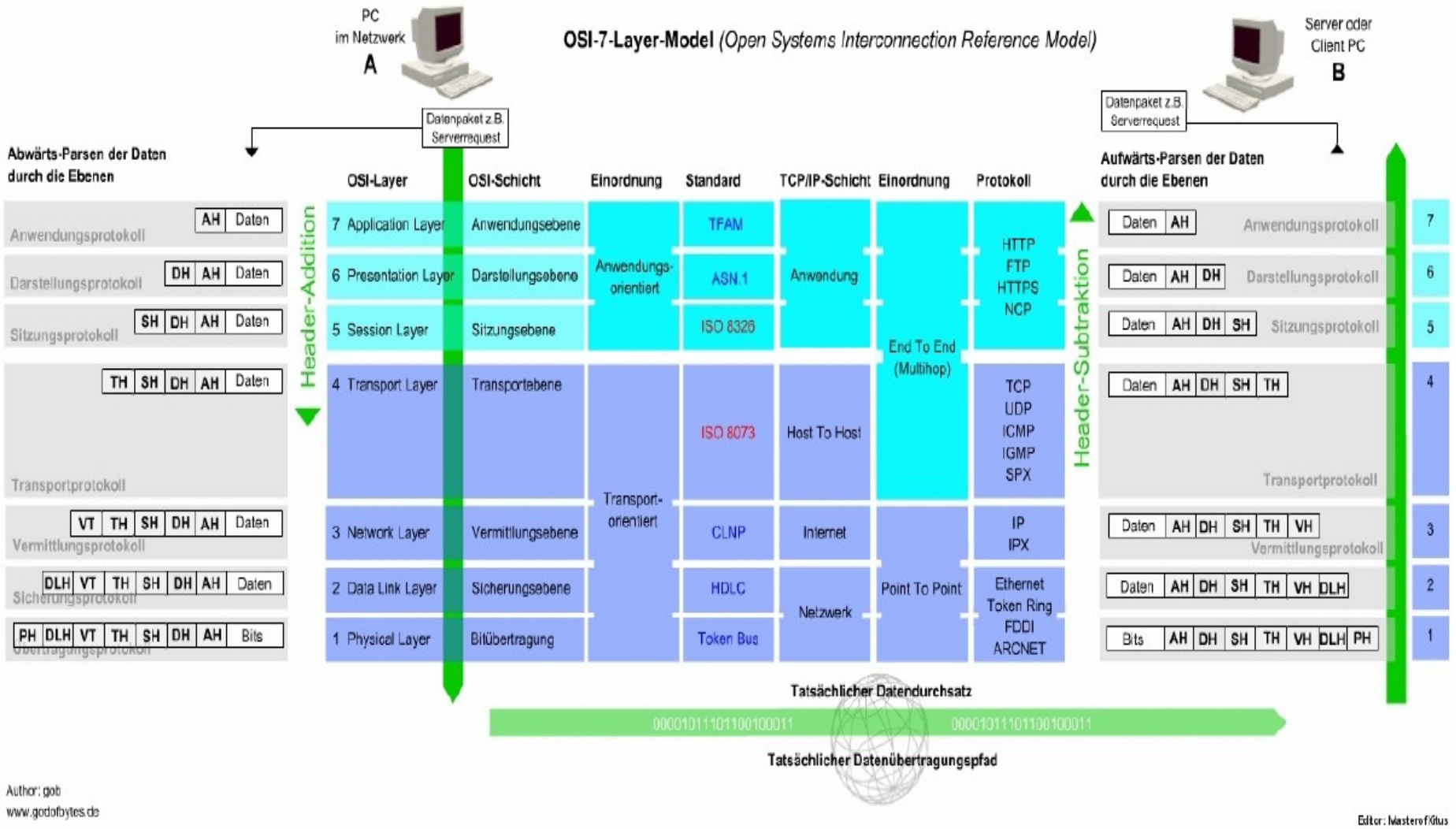
Wir wollen im Weiteren den Begriff der *Rolle* als partielle Identität zu Grunde legen, wenn wir nun die technischen Gegebenheiten des Agierens digitaler Identitäten (genauer: *als* digitale Identitäten) betrachten wollen.

Im Internet werden *Beschreibungen* ausgetauscht

- Auch z.B. Bilder sind Beschreibungen, die dem Computer Anweisungen geben, wie das Bild zu rendern ist.
- Austausch von *Beschreibungen* zwischen Computern erfolgt, indem diese in *Pakete* vorgegebener Struktur und Größe zerlegt werden.

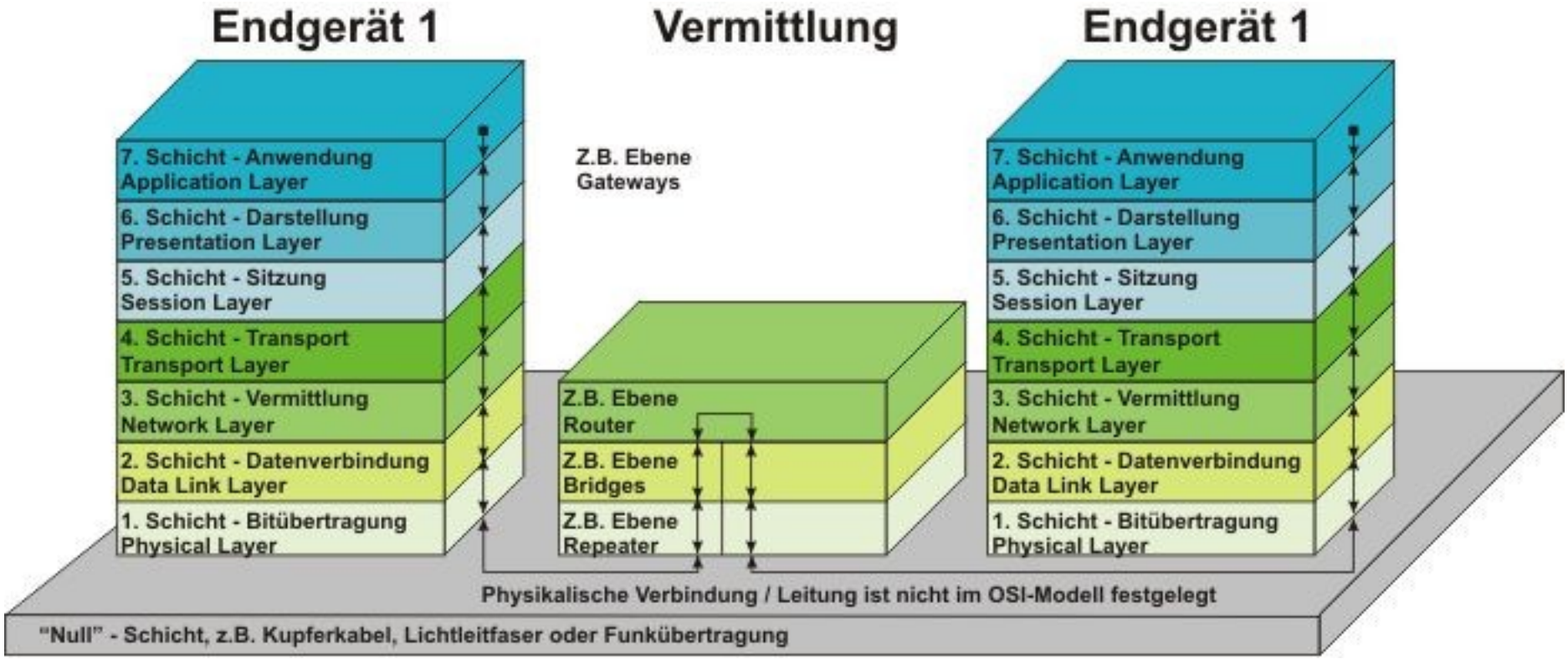
Paketübertragung im Internet, das OSI 7-Schichten-Modell

- http://de.wikipedia.org/wiki/OSI-Modell
- Schichten und Protokolle
- Protokolle und Sprache



Quelle: Wikipedia, http://prima-it.de/images/osi7layermodell.jpg

Internet Basics



Quelle: http://www.hbernstaedt.de/knowhow/ether/osi.jpg

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Texte bestehen aus Zeichen (Buchstaben, Zahlen usw.)

- Bits und Bytes
- Reduktion auf standardisierte Bitfolgen und damit Zahlen
- Erstes beständiges Alphabet: ASCII (7 Bit) = 0..127
  - 0..31 – Steuerzeichen
  - 32..127 – Zahlen und Buchstaben des englischen Alphabets
- Mehrere Standardisierungswellen für weitere Alphabete und Zeichensysteme (latin-1, Windows-Zeichensatz)
- Bedarf, sich zu einigen → Unicode
  - Beginn der Bemühungen um 1988
  - Erster Standard 1991 enthielt $2^{16} = 65.536$ Zeichen

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Unicode

- Internationaler Standard, in dem langfristig für jedes Sinn tragende Schriftzeichen oder Textelement aller bekannten Schriftkulturen und Zeichensysteme ein digitaler Code festgelegt wird, um den Austausch textueller Information weltweit zu vereinheitlichen. Unicode wird ständig um Zeichen weiterer Schriftsysteme ergänzt.
- Hexadezimale Darstellung, etwa U+01FA (2 Byte)

UTF-8 als sich entwickelnder de-facto-Standard

- Kodierung von Zeichen in bis zu 4 Byte (variable Länge)
- Kodierung der ASCII-Zeichen in 1 Byte

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Datenübertragung im Internet

- Serielle Übertragung als Bitfolge, für menschenlesbare Zwecke meist im Oktal- oder (häufiger) Hexadezimal-system (Basis 16) dargestellt (x1FA = 0001.1111.1010)
- Bitstrom wird in Pakete konstanter Länge zerteilt und mit Sender/Empfänger-Informationen (Routing) losgeschickt
- Pakete werden von Rechner zu Rechner weitergeleitet, bis sie ihren Empfänger erreicht haben
  - Integritätsprüfung mit einer Hash-Funktion
- Empfänger setzt aus den Paketen den Bitstrom wieder zusammen
- Damit dies für den Nutzer transparent ist, werden standardisierte Protokolle verwendet

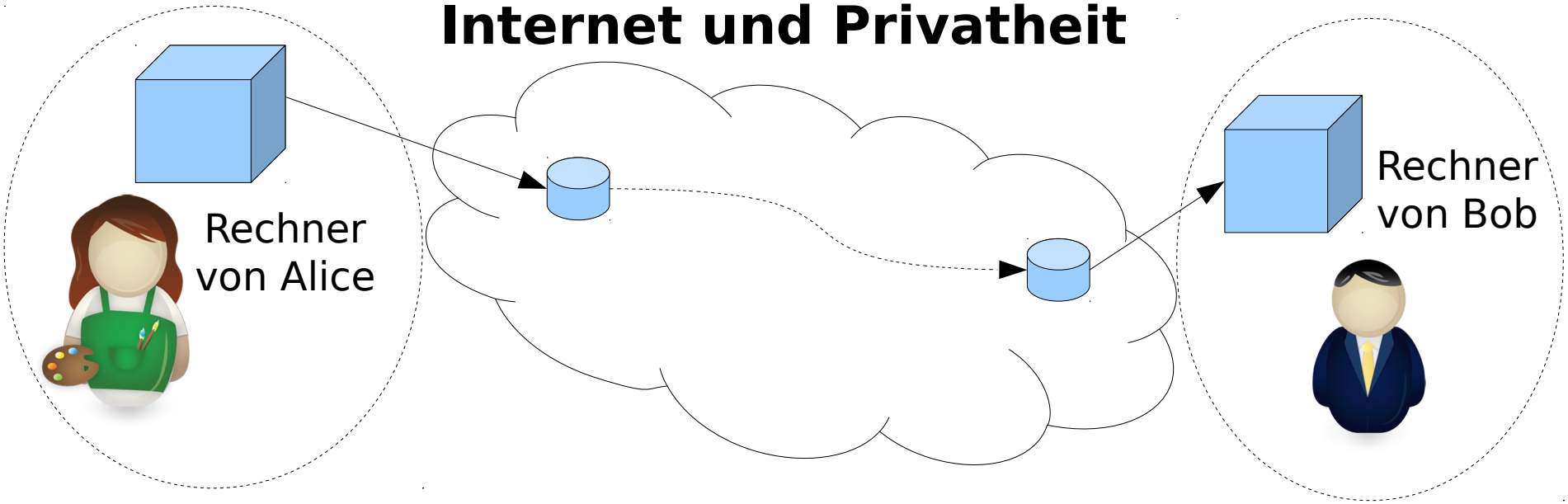
UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Funktion	OSI Schichtenmodell	Protokolle (Auswahl)
Anwendungen	Anwendungsschicht Darstellungsschicht Sitzungsschicht	HTTP HTTPS SSH
Netzübertragung	Transportschicht Vermittlungsschicht	TCP/IP SSL/TLS
Netzzugang	Sicherungsschicht Übertragungsschicht	WLAN PPP Ethernet

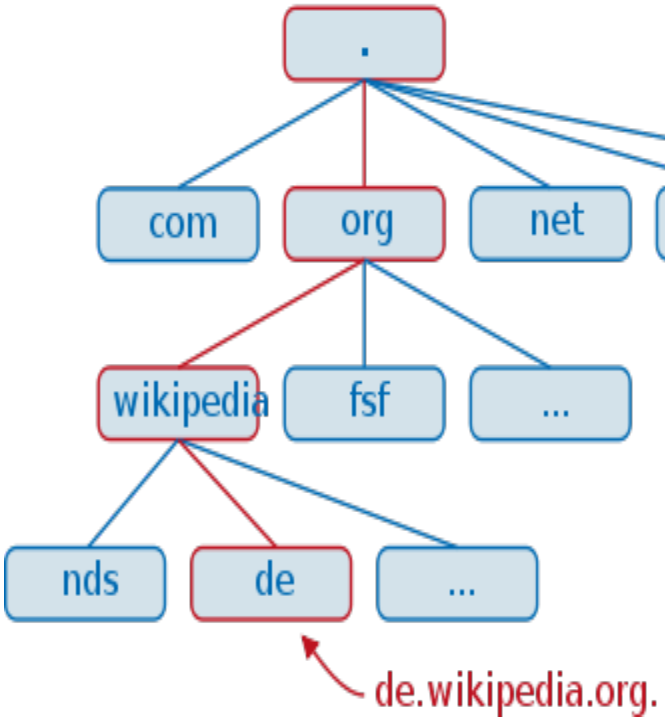
UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Internet und Privatheit



- Fiktion der universellen Ende-zu-Ende-Verbindbarkeit
  - Hohe Ausfallsicherheit gegen zufällige Störungen.
    Das Internet ist ein skalenfreies Netz.
- Pakete haben öffentliche Header und private Inhalte
  - Header-Informationen sind grundsätzlich öffentlich
- Fragen: Sicherheit und Integrität
  - Antwort: Hashfunktionen
- Fragen: Privatheit
  - Antwort: Verschlüsselung

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme



Rechner und Rechnername

- Rechnernamen und Rechneradressen
- IPv4 (32 Bit) und IPv6 (128 Bit) – ping und ifconfig
- Zum Aufbau von Rechnernamen, Domänennamen und Top Level Domänen
- Umrechnung von Namen in Adressen – das Domain Name Service System

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Registrar, Provider, Host

- **Registrar:** Verwalter von Rechnernamen
  - Denic.de – Verwalter der TLD .de ist die DENIC e.G.
  - Zitat Impressum: Eingetragen unter Nr. 770 im Genossenschaftsregister, Amtsgericht Frankfurt am Main
  - Anmerkungen zur Rechtsform
  - URZ verwaltet uni-leipzig.de und Subdomänen
- Welche Domänennamen?
  - Besitz einer Domäne als Rechtstitel
  - Rechnernamen als Handelsware: https://sedo.com/de/wissen/markt-trends/
- **Provider:** Hält Rechner mit IP-Adressen (**Hosts**) vor und kümmert sich um das Umrechnen von Domain-Namen in IP-Adressen sowie das Weiterleiten (Routing) von Datenpaketen.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Vergabe der IP-Adressen

- IP-Adressen werden hierarchisch vergeben: Nutzer bekommen IP-Adressen vom ISP (internet service provider), ISPs von einer local Internet registry (LIR) oder National Internet Registry (NIR) oder Regional Internet Registry (RIR - RIPE NCC for Europe, the Middle East, and Central Asia) und diese von der Internet Assigned Numbers Authority (IANA).
- IANA is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is … free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA. IANA is one of the Internet's oldest institutions, with its activities dating back to the 1970s. → https://www.iana.org/numbers
- *Frage:* Can I buy IP addresses from the RIPE NCC?
  Antwort: No. Internet number resources are a shared public resource and do not have a value. Members are charged fees based on the services that they receive from the RIPE NCC.