FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Erläuterungen zur Richtlinie für die Nutzung des FAU-Datennetzes

Inhalt

1 Zu Kapitel 1, Einleitung

Das RRZE hält das Netzwerk bezüglich Konzeption, Ausbau, Ausgestaltung oder Betrieb im Rahmen gegebener Möglichkeiten auf dem Stand aktueller Anforderungen und Technologien. Unter diesem Gesichtspunkt sind verbindliche, allgemein gültige Richtlinien unerlässlich.

Auf Grund der starken geografischen Verteilung hat das Datennetz der FAU sowohl LAN- (Local Area Network) als auch WAN- (Wide Area Network) Charakter. Dennoch folgt es in seiner Gesamt-architektur einem umfassenden, hierarchisch gegliederten Strukturmodell (Core, Distribution, Access). In der Umsetzung spielen in derzeitiger Ausprägung das Internet Netzwerkprotokoll (IP) und damit verbundene Technologien eine bestimmende Rolle. Die Infrastruktur des Datennetzes erlaubt den Anschluss einzelner Endgeräte über definierte Schnittstellen.

Das Netzwerk besteht aus aktiven Komponenten (LAN-Switches, Router), die über passive Elemente (z.B. Glasfaserkabel, Kupferkabel, Richtfunkstrecken) in einer hierarchischen, baumartigen Struktur untereinander verbunden („vernetzt“) sind. Es ist nach geografischen und funktionalen Gesichtspunkten grob gegliedert in Core-, Distribution- und Access- Bereiche. Der Core fasst regionale Einheiten zusammen und verknüpft sie miteinander (z.B. „Erlangen-Süd“, „Erlangen-Innenstadt“, „Nürnberg“). Distribution- Bereiche gehören jeweils zu einem Core und sind verschiedenen Stand-orten (z.B. „Tennenlohe“, „EWF“), Gebäudekomplexen (z.B. „Biologie/Physik“, „PhilFak“) oder funktionalen Einheiten (z.B. „Datacenter“: Bereich zentraler Server) zugeordnet. Verknüpft über den Core verteilen sie ihrerseits auf mehrere, zugehörige Access- Bereiche, die das Netzwerk in lokalen Einheiten (z.B. Gebäuden, Etagen) verbreiten und schließlich die Zugangspunkte für die Endgeräte bereit-stellen.

Obwohl dieses Architekturkonzept bis auf weiteres die Grundlage der Netzgestaltung darstellt, ist das FAU-Netzwerk kein starres Gebilde, sondern befindet sich in fortwährendem Anpassungs- und Erweiterungsprozess. Dazu gehören das Einbeziehen neuer Gebäude oder ganzer Standorte ebenso, wie das Einbringen neuer Technologien (höhere Übertragungsgeschwindigkeiten) oder auch das Ermöglichen neuartiger Anwendungen (Videodienste, Telefonie).

Neben der flächendeckenden, internen Vernetzung der FAU ist das Datennetz auch mit der international verbreiteten Struktur des Internets verbunden bzw. darin integriert. Dies eröffnet den Universitätsangehörigen vielfältige Möglichkeiten zur Kommunikation mit Partnern außerhalb der Universität, zur Nutzung weltweit angebotener Dienste oder auch des Fernzugriffs auf Systeme innerhalb Universität (z.B. „von zu Hause“ oder „auf Forschungsreisen“). Umgekehrt bietet auch die FAU verschiedene Dienste zur allgemeinen Nutzung durch die Internetgemeinschaft an (z.B. Informationsdienste, Datenbanken).

Die Verknüpfung zwischen FAU- und Internet erfolgt über einen leistungsstarken, redundant ausgelegten Anschluss an das vom DFN-Verein (Verein zur Förderung eines Deutschen Forschungs-netzes e. V.) betriebene Wissenschaftsnetz, das als Schwerpunkt die deutschen Forschungs-einrichtungen untereinander verbindet und seinerseits Austauschpunkte zu Netzen anderer Internet-provider besitzt. Übrigens arbeitet das RRZE eng mit dem DFN-Verein zusammen und beherbergt wichtige Komponenten des Wissenschaftsnetzes als so genannter Kernnetz-Standort.

Abgesehen von verschiedenen, hauptsächlich unter Sicherheitsaspekten durchgeführten Prüfungen an der Anschlussstelle zum Wissenschaftsnetz, etwa zur Abwehr gewisser Attacken oder der Verhinderung des Einschleppens von Schadsoftware, ist zwischen FAU und Außenwelt eine weitgehend freie Internetkommunikation möglich.

2 Zu Kapitel 2, Verantwortungsbereiche

Das RRZE wird in Bezug auf die Richtlinien für die Nutzung des FAU-Datennetzes von seiner Abteilung Kommunikationssysteme vertreten. Die FAU-Organisationseinheiten (alle Einrichtungen der FAU, wie z.B. Lehrstühle, Institute, Fakultäten, zentrale Einrichtungen) können Ihre Verantwortung selbst wahrnehmen oder auch delegieren, indem sie dem RRZE als IT-Betreuer z.B. eines der RRZE-Betreuungszentren benennen, mit denen sie einen Betreuungsvertrag haben.

2.1 Infrastruktur

In Bezug auf die Infrastruktur des Datennetzes ergibt sich aus der Abgrenzung der Verantwortlichkeiten zwischen RRZE, FAU-Organisationseinheiten und Endgerätenutzern, dass nur vom RRZE eingerichtet / angeschlossen / betrieben werden dürfen:

- Gebäudeübergreifende Verkabelung
- Gebäude-interne Verkabelung
- Rangierungen in den Verteilerschränken des Datennetzes
- Funk- (WLAN-) Komponenten (Access Points)
- LAN-Switches zur Vervielfachung der Anschlussschnittstelle oder Verlängerung der Netzwerkstruktur
- Routende Netzkomponenten (Software-Router oder dedizierte Router) zwischen Endgerät und FAU-Datennetz
- Externe Anbindung über Internetanschlüsse an „fremde“ Provider (z.B. per DSL)

In Hinblick auf die wachsende Migration von ehemals offline betriebenen Geräten in das Datennetz der FAU werden nicht mehr nur Arbeitsplatzgeräte und mobile Geräte mit Netz versorgt, sondern zunehmend auch ursprünglich datennetzfremde Geräte. Speziell bei der Integration von Geräten stationärer sowie raum- bzw. gebäudebezogener Natur (z.B. gebäudeeigene Leit- und Medientechnik, Verkaufsautomaten, Infodisplays oder Beamer) in das Datennetz der FAU gilt dabei:

- Aus der technischen und organisatorischen Ausrichtung sowie der Finanzierung des FAU WLANs speziell zur mobilen Versorgung von Endgeräten der Studierenden und Beschäftigten ergibt sich, dass die Nutzung des FAU WLANs zur Versorgung derartiger Geräte unabhängig von Qualität und Ausbau der WLAN-Infrastruktur vor Ort ausdrücklich nicht gestattet ist
- Derartige Geräte können grundsätzlich nur nach voriger Konzeption durch die Verantwortlichen von RRZE sowie ggf. ZUV Abt. G nach den jeweils geltenden Vorgaben mit einer Festanbindung in das Datennetz integriert werden.

2.2 Grundlegende netzbezogene Dienste

Das Zusammenspiel zwischen Endsystemen und Netzwerk sowie netzinternen Operationen wird durch die vom RRZE betriebenen grundlegenden Netzdienste geregelt, welche im Folgenden aufgeführt werden.

2.2.1 Symbolische Adressen (DNS)

Neben den numerischen IP-Adressen werden vor allem von den Endgerätenutzern symbolische Adressen zur Benennung von Kommunikationspartnern verwandt. Diese im Internet definierten symbolischen Adressen oder Gerätenamen sind nach einem hierarchischen Schema aufgebaut. Die Schreibweise gibt die Hierarchie von „rechts nach links“ wieder und lautet z.B. für den WEB-Server des RRZE: www.rrze.fau.de (de: „Top Level Domain“).

Die Verwaltung der Namen und automatische Adressauflösungen von Namen (Angabe der numerischen Adresse nach Anforderung mit symbolischer Adresse) leistet der „Domain Name Service“ (DNS) und wird von sich untereinander austauschenden, dedizierten Servern erbracht.

Im Datennetz der FAU müssen die IT-Betreuer für ihren Bereich jedem Internetgerät bzw. jeder IP-Adresse die Zuordnung eines eindeutigen symbolischen Namens veranlassen durch Meldung. Die Kommunikation von Komponenten mit nicht im DNS eingetragenen Adressen ins Internet wird blockiert. http://dlp.rrze.fau.de/dns/ .

2.2.2 Dynamische Adresszuteilung (DHCP)

Dieser Dienst ermöglicht es Endgeräten, über ein spezielles Protokoll (DHCP: Dynamic Host Configuration Protocol) eine Hostadresse zur aktuellen Nutzung dynamisch anzufragen. Das kann zur Vereinfachung der Konfiguration auf den Endsystemen beitragen, aber auch über Engpässe zur Verfügung stehender IP-Adressen hinweghelfen (Adresszuteilung nur an jeweils aktive Systeme). Je nach Handhabung ist eine Zuordnung von Absenderadresse und Endsystem dann nicht mehr direkt möglich. Das RRZE bietet diesen Dienst unter bestimmten Voraussetzungen an, http://dlp.rrze.fau.de/dhcp/ .

2.3 Adresstransformation (NAT)

Mit Hilfe der Adresstransformation (NAT: Network Address Translation) können an der Außenschnittstelle eines IP-Netzes Absender- oder Zieladressen umgeschrieben werden. Das wird z.B. verwendet, um Netzen mit „privaten“, also im weltweiten Internet nicht gerouteten IP-Adressen, durch dynamische Zuordnung „öffentlicher“ Absender externe Kommunikation zu ermöglichen. Dieser Mechanismus erhöht die Komplexität und macht je nach Handhabung eine Identifizierung des ursprünglichen Absenders eines Datenpaketes schwer bis unmöglich. NAT wird deshalb ausschließlich vom RRZE betrieben und das nicht innerhalb des FAU-Netzes, sondern nur zwischen FAU-Datennetz und Internet.

2.4 Gesicherte Verbindungen (VPN)

Der VPN-Service (VPN: Virtual Private Network) ermöglicht einzelnen Endgerätenutzern kontrollierten, gesicherten Zugang aus dem Internet in das Netz der FAU, d.h. z.B. Zugriffe von Heimarbeitsplätzen auf sonst nur innerhalb der Universität verfügbare Systeme und Dienste. Benötigt wird eine Entsprechende Zugangssoftware (VPN-Client, beziehbar vom RRZE) sowie eine für VPN freigeschaltete IdM-Kennung an der FAU.

Eine andere Variante der VPN-Technik ermöglicht den Aufbau sogenannter Tunnel aus dem oder in das FAU-Datennetz („Site-to-Site“). Über solche Tunnel können etwa auf Rechnerebene IP-Verbindungen hergestellt werden, die von dem darunterliegenden Netzwerk unabhängig sind, und so die homogene, hierarchische Struktur durchbrechen, also damit Routing und Kontrollmechanismen des Datennetzes unterlaufen. Die Einrichtung eines Site-to-Site-Tunnels ist ausschließlich dem RRZE vorbehalten. Siehe http://dlp.rrze.fau.de/vpn/

2.4.1 Firewalling / ACL

Der Datenverkehr zwischen einem Subnetz und seiner Umgebung kann durch Prüfungen auf dem betreffenden (Distribution-) Router nach individuellen Sicherheitsvorgaben eingeschränkt werden. Dies geschieht über sogenannte Access-Listen (ACL: Access Control List), die in Absprache mit dem RRZE bedarfsgerecht implementiert werden, etwa um den Zugriff auf institutsinterne Server mit schützenswerten Daten nur Angehörigen der betreffenden FAU-Organisationseinheit zu erlauben. Unabhängig davon gibt es an der FAU gewisse Standardregeln, die zum Beispiel das sogenannte Spoofing verhindern, d.h. Datenpakete mit unzulässigen Absenderadressen verwerfen (Absender nicht zum sendenden Netz gehörend oder von außen kommendes Paket mit Absender aus dem Zielnetz).

Wenn in besonderen Fällen spezielle Sicherheitsanforderungen nicht über derartige Filterung erfüllt werden können, kommen auch dedizierte Firewall-Komponenten zum Einsatz (so z.B. am Übergang zum Netz der zentralen Universitätsverwaltung).

3 Zu Kapitel 3, Anschluss von Endgeräten

Die internationale Normungsorganisation ISO/OSI beschreibt die Kommunikation zwischen Rechnersystemen über ein 7-schichtiges Referenzmodell. Während ab der 4. Schicht (Ende-zu-Ende-Kontrolle) die entsprechenden Protokolle für Endsysteme definiert sind und dort abgewickelt werden, sind die unteren 3 Schichten innerhalb eines Netzwerkes, d.h. zwischen den Netzkomponenten sowie an den Schnittstellen zu den Endgeräten von Bedeutung. Sie sollen daher im Folgenden allgemein erläutert und in Bezug auf das Datennetz der FAU konkret beschrieben werden.

3.1 Bitübertragungsschicht (Schicht 1 - Physical Layer)

3.1.1 Allgemeine Beschreibung

Die physikalische Schicht beschreibt technische Eigenschaften und Nutzungsart von Medien zum Datentransfer zwischen kommunizierenden Geräten. Sie ist an der FAU durch das passive Netz repräsentiert, das nach dem Konzept einer universellen Gebäudeverkabelung aufgebaut ist. Diese strukturierte Verkabelung ist in Primär, Sekundär- und Tertiärbereich eingeteilt:

Primärbereich

Der Primärbereich verbindet verschiede Gebäude oder Gebäudegruppen miteinander. Im günstigen Fall geschieht dies über mehrere, in Trassen verlegte Glasfaserkabel. Dabei können auch einzelne Glasfasern mit Hilfe von Multiplexern (DWDM) für mehrere Verbindungen genutzt werden. Dort, wo keine Glasfasern zur Verfügung stehen oder verlegt werden können (Entfernung, Geländehoheit, Kosten) kommen stattdessen dedizierte Übertragungswege, wie Richtfunkstrecken (RiFu) oder geschlossene Pfade in Providernetzen (z.B. über DSL) zum Einsatz. Auch diese, z.B. durch Strombedarf oder Verwendung spezifischer Komponenten über rein passive Gestaltung hinausgehenden Verbindungsarten, sind funktional dem Bereich der primären strukturierten Verkabelung zuzuordnen.

Sekundärbereich

Der Sekundärbereich verbindet Stockwerke eines Gebäudes (vertikale Steigbereichsverkabelung) oder kleinere Gebäude eines begrenzten Komplexes. Die Verkabelung ist in der Regel mit Glasfasern ausgelegt, mitunter werden auch Kupferkabel dazu verwendet.

Tertiärbereich

Der Tertiärbereich enthält die horizontalen Verbindungen vom Etagenverteiler in die Räume der Endgeräte (Büros, Gruppenräume, Labore, Hörsäle, usw.). Sie bestehen in der Regel aus Kupferkabeln unterschiedlichen Typs („älter“: 4-drahtig, Übertragungen bis 100 mbps / „aktuell“: 8-drahtig, Übertragungen bis 1000 bps bzw. 1 gbps) und enden mit entsprechenden Anschlussdosen für zu versorgende Endgeräte.

Die Kabelenden in den Gebäuden und Etagen auf zugehörigen Rangierverteilern (Patchfeldern), über die benötigten Verbindungen zwischen Netzwerkkomponenten (primär, sekundär) oder Netzwerkkomponenten und Endgeräten (tertiär) bedarfsgerecht geschaltet werden können (Patchung).

Während also Primär- und Sekundärbereich hauptsächlich zum Aufbau einer ortsübergreifenden Netzinfrastruktur, d.h. der Verbindung aktiver Netzkomponenten untereinander, genutzt werden, dient der Tertiärbereich vornehmlich der Heranführung von Endgeräten an das Datennetz. Neben dieser „drahtgebundenen“ Anbindung fest installierter Geräte, besteht aber auch die Möglichkeit des Netzzuganges für mobile Endgeräte (LapTops, Tablets, Smartphones, usw.) über „nicht drahtgebundene“ Funktechnik (WLANs). Die entsprechenden Zugangspunkte (Access Points, APs) gliedern sich in das drahtgebundene Netzwerk ein und können funktional dem Tertiärbereich der strukturierten Verkabelung zugeordnet werden. Durch ihre weite Verteilung steht diese Nutzungsart für Mitarbeiter, Studenten oder Gäste unter Zuordnung entsprechender Berechtigungen in fast allen öffentlichen Bereichen der FAU zur Verfügung.

3.1.2 Schnittstelle zwischen FAU-Datennetz und Endgerät

Die Schnittstelle zwischen Datennetz der FAU und Endgerät ist auf der Bitübertragungsschicht konkret wie folgt charakterisiert:

- Port an LAN-Switch mit definierter Charakteristik (z.B. feste oder automatisch eingestellte Geschwindigkeit)
- Verlängerung im Tertiärbereich über Rangierung / Patchung vom Switchport zur (TP-) Anschluss-dose (am Arbeitsplatz)
- Im Falle mobiler Endgeräte Verbindung über örtliches WLAN zu nächstgelegenem AccessPoint
- Im Falle hochverfügbarer Server im RRZE-Data-Center mit Spezialverkabelung und deutlich höheren Zugangsgeschwindigkeiten (z.B. 10 gbps)

Grundsätzlich darf ein Endgerät nur an einem Port angeschlossen sein. Die Anschlüsse von sogenannten multihomed Hosts (Endgeräte, welche über mehrere Ports angeschlossen sind) sowie Endgeräten, die ihrerseits mehrere virtuelle Instanzen auf demselben Port anbinden, bedürfen der Zustimmung des RRZE.

3.2 Sicherungsschicht (Schicht 2 - Data Link Layer)

3.2.1 Allgemeine Beschreibung

Aufgabe der Sicherungsschicht ist es, eine zuverlässige, das heißt weitgehend fehlerfreie Über-tragung zu gewährleisten und den Zugriff auf das jeweilige Übertragungsmedium zu regeln. Im FAU-Netz ist sie durch virtuelle Ethernet LANs (VLANs) realisiert, die über strukturiert verknüpfte, aktive Komponenten (LAN-Switches) definiert und verbreitet werden. Die VLANs sind naturgemäß räumlich begrenzt und nach geografischen und nutzungsspezifischen Gesichtspunkten gebildet. Gemäß der Ethernet-Technologie sind sie unabhängig vom jeweiligen Übertragungsmedium (Schicht 1, z.B. Glasfaserkabel, Kupferkabel, Funk) charakterisiert durch:

- Zugriffsmethode (z.B. CSMA/CD)
- Datenformate (Ethernet-Frames)
- Einzel-Adressierung (lokale MAC-Adressen, global eindeutige Vergabe durch Hersteller)
- Sammel-Adressierung (Broadcasts, Multicasts)

Im Vergleich zum ursprünglich auf spezifischen Koaxialkabeln definierten Ethernet verhindert der Einsatz von LAN-Switches weitgehend Zugriffskonflikte (Kollisionen) und ermöglicht das Mischen von Anschlüssen unterschiedlicher Geschwindigkeiten (10, 100, 1000, 10000 mbps) im einem LAN. Unter den über die strukturierte Verkabelung verknüpften LAN-Switches gibt es solche mit reinen strukturellen Aufgaben (Verteil-Switches) und solche zur Bereitstellung von Endgeräteanschlüssen (End-Switches). Die Ports an den End-Switches sind je eindeutig einem VLAN zugeordnet und definieren so die LAN-Zugehörigkeit der angeschlossenen Endgeräte.

3.2.2 Schnittstelle zwischen FAU-Datennetz und Endgerät

Die Schnittstelle zwischen Datennetz der FAU und Endgerät ist auf der Sicherungsschicht konkret wie folgt charakterisiert:

- LAN mit Ethernet-Funktionalität
- Im betreffenden Access-Bereich als virtuelles LAN (d.h. VLAN) realisiert
- Port-VLAN-Zuordnung pro Anschluss
- Verteilung eines LANs auf mehrere Orte (Segmente) innerhalb des betreffenden Bereiches möglich, nicht aber über Bereichsgrenzen hinweg

3.2.3 Vermittlungsschicht (Schicht 3 – Network Layer)

3.2.4 Allgemeine Beschreibung

Die Vermittlungsschicht ermöglicht den Datenaustausch über lokale Grenzen hinweg, d.h. zwischen Teilnehmern in verschiedenen VLANs oder internen und externen Partnern einer Organisation. Hierzu ist ein übergreifendes, einheitliches Netzwerkprotokoll erforderlich, dessen Rolle sowohl an der FAU als auch im nationalen und internationalen Rahmen vorherrschend die Internetprotokolle (IP) der Version 4 (IPv4) und der Version 6 (IPv6) einnehmen. Hauptaufgabe des Netzes ist die Vermittlung von (IP-)Datenpaketen zwischen Netzteilnehmern, also die Bestimmung von Übertragungspfaden, so wie Annahme, Transport und Zustellung, auch als „Routing“ bezeichnet.

Charakteristische Merkmale des IP-Protokolls sind u.a.:

- Verbindungslose Übertragung (Datagramme) ohne Ende-zu-Ende Kontrolle
- Daten- und Steuerpakete
- Datenpakete mit Steuerinformation u.a. (Absender-, Zieladresse) und Nutzdaten
- IP-Versionen v4 und v6 mit unterschiedlicher Adressierung
  IPv4 : 4 Byte- lange Adressen, dezimale Schreibweise pro Byte
  IPv6 : 16 Byte- lange Adressen, hexadezimale Schreibweise in 8 - 2er-Blöcken
- Geräteadressen aufgeteilt in Netz- und Host- Anteil, Grenze durch Netzmaske definiert
- Internationale, zentrale Netzadressenzuordnung durch Internet-Organisation (IANA)
  z.B. 131.188.0.0 (IPv4)
  z.B. 2001:638:a000:: (IPv6)
- Institutionsspezifische Netzadresszuordnung an Netzgruppen durch Aufteilung in Subnetze über Längenangabe oder verlängerter Subnetzmaske
  z.B. 131.188.31.0 / 24, bzw. Netzmaske 255.255.255.0 (IPv4)
  z.B. 2001:638:a000:1001:: / 64 (IPv6)
- Zusätzliche, gemäß RFC1918 nur innerhalb einer am Internet teilnehmenden Organisation zu verwendende Adressen, auch als „private“, oder (im Internet) „nicht geroutete“ Adressen bezeichnet. Z.B. 10.0.0.0 (IPv4)
- Keine Unterscheidung zwischen "privaten" und "öffentlichen" Adressen innerhalb der o.g. Organisation, d.h. Gleichbehandlung im organisationsinternen Routing

3.2.5 Schnittstelle zwischen FAU-Datennetz und Endgerät

Die angeführten Merkmale sollen nur einen prinzipiellen Eindruck vermitteln. Die Schnittstelle zwischen Datennetz der FAU und Endgerät ist auf der Vermittlungsschicht konkret wie folgt charakterisiert:

- IP-Adressraum (bezeichnet als Subnetz)
- Adressraum öffentlich (im Internet geroutet) oder privat (nur innerhalb der FAU gültig)
- Subnetzadresse inkl. Netzmaske (pro Nutzergruppe), eindeutig einem VLAN zugeordnet
- Individuelle Hostadressen (pro Endsystem) innerhalb des zugeteilten Netzadressraumes
- Default Route (Router-Adresse, Next-Hop) zur Kommunikation mit Partnern außerhalb des eigenen Subnetzes
- Subnetzadresszuteilung durch RRZE an IT-Betreuer der FAU-Organisationseinheit
- Hostadresszuteilung durch IT-Betreuer der FAU-Organisationseinheit
- Individuelle, dynamische Adresszuordnung im Falle mobiler Endgeräte