UNIVERSITÄT BIELEFELD

BITS

Schnittstelle zum Datennetz im Access-Bereich

Inhalt

Einführung

Die Universität Bielefeld betreibt ein Datennetz, das auf dem Ethernet Protokoll und dem Internet Protokoll (IPv4 und IPv6) basiert. Nutzer haben die Möglichkeit Endgeräte an das Datennetz anzuschließen und die dort angebotenen Dienste zu nutzen. Es ist die Nutzungsordnung zu beachten. Zuständig für Planung, Entwicklung, Betrieb und Verwaltung des Datennetzes ist die Abteilung Netze.
Der Anschluss von Endgeräten erfolgt an Datendosen, die in der gesamten Universität verteilt sind. Technisch werden über die Datendosen sogenannte Daten-Ports realisiert. In diesem Dokument sollen der Begriff Daten-Port und Datendose nicht weiter unterschieden werden und ihre Verwendung erfolgt gleichwertig. Der Übergabepunkt zum Datennetz ist immer die Datendose bzw. der Daten-Port. In diesem Dokument werden die Eigenschaften und technischen Parameter des Übergabepunktes beschrieben. Es ist somit eine Schnittstellenbeschreibung. Die hier beschriebenen Parameter sind beim Anschluss eines Endgerätes zu beachten und können nicht geändert werden. Die Parameter werden wenn notwendig neuen Anforderungen und technischen Möglichkeiten angepasst.
Hinweis: Schnittstellen im Data Center werden durch dieses Dokument nicht beschrieben oder erfasst.

Schnittstelle zum Datennetz im Access Bereich

Schnittstelle der Datenkommunikation

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
Datenrate Alter Stecker (EC7)	▪ 10 MBit/s ▪ 100 MBit/s 1000 MBit/s (Gigabit Ethernet) kann **kostenpflichtig** als Upgrade bezogen werden.
Datenrate Neuer Stecker (RJ45)	▪ 10 MBit/s ▪ 100 MBit/s ▪ 1000 MBit/s
Duplexverfahren	▪ Vollduplex Bei einer Datenrate von 10Mbit/s ist zusätzlich Halbduplex möglich.
Autonegotiation	▪ Autonegotiation ist aktiv Datenrate und Duplexverfahren müssen immer per Autonegotiation ausgehandelt werden. Eine statische Konfiguration von Bandbreite und Duplex führt zu Störungen.
MTU	▪ 1500 Byte (Maximum Transmission Unit)
CDP	▪ CDP ist aktiv CDP wird für VoIP Endgeräte benötigt. Über CDP wird das Subnetz für VoIP Endgeräte ausgehandelt. (Cisco Discovery Protocol)
LLDP-MED	▪ LLDP-MED **nicht** ist aktiv (Link Layer Discovery Protokoll - Media Endpoint Devices)
POE	▪ POE ist aktiv ▪ Maximale Leistung ist 7W (Power over Ethernet, IEEE 802.3af, Class 2)
802.1Q	▪ 802.1Q ist **nicht** aktiv 802.1Q wird im Data Center angeboten (IEEE 802.1Q, Cisco:Vlan-Trunking, HP:Vlan-Tagging)
Link Aggregation	▪ Link Aggregation ist **nicht** aktiv ▪ LACP ist **nicht** aktiv Link Aggregation und LACP werden im Data Center angeboten. (LACP nach IEEE 802.3ad, Cisco:Etherchannel, HP:Trunking, Linux:Bonding)
Ethernet Flow Control	Ethernet Flow Control ist **nicht** aktiv.

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
Address Policy	▪ IPv4-Adressen für alle Endgeräte ▪ IPv6-Adressen für alle Endgeräte ▪ IP-MAC-Binding erfolgt über Manual DHCP. Die Vergabe von IPv4-Adressen erfolgt über DHCP. Die Vergabe von IPv6-Adressen erfolgt über SLAAC (Stateless Address Autoconfiguration). ▪ **Keine** statisch konfigurierten IP-Adressen. ▪ Datenpakete mit statisch konfigurierten IP-Adressen werden **nicht** weitergeleitet. ▪ Feste IP Adressen für Endgeräte nur über IP-MAC-Binding in Verbindung mit Manual DHCP Die Abteilung Netze verwaltet sämtliche IP-Adressen der Universität Bielefeld. Vergabe von IP-Adressen ausschließlich durch die Abteilung Netze.
Routing Policy	▪ Routing von IPv4 im gesamten Datennetz ▪ Routing von IPv6 im gesamten Datennetz Für Protokolle die über IPv4 und IPv6 transportiert werden gibt es keine Beschränkung. ▪ Mit Endgeräten werden keine Routing-Informationen ausgetauscht.
Multicast Routing Policy	▪ **Kein** Multicast Routing für IPv4 ▪ **Kein** Multicast Routing für IPv6 ▪ Multicast innerhalb eines Segments bzw. in einem Vlan ist aber dennoch möglich.
Internet Policy	▪ Gehende IP Verbindung zum Internet sind möglich ▪ Kommende IP Verbindung vom Internet werden blockiert Mit gehender Verbindung ist der Verbindungsaufbau vom Endgerät zum Internet gemeint. Mit kommender Verbindung ist der Verbindungsaufbau vom Internet zum Endgerät gemeint. Liegt das Endgerät in einem Gruppen Vlan, legt der zugeordnete EDV Administrator die Policy fest.
Intranet Policy	▪ Gehende IP Verbindung zu Intranet sind möglich ▪ Kommende IP Verbindung vom Intranet sind möglich Mit gehender Verbindung ist der Verbindungsaufbau vom Endgerät zum Intranet gemeint. Mit kommender Verbindung ist der Verbindungsaufbau vom Intranet zum Endgerät gemeint. Liegt das Endgerät in einem Gruppen Vlan, legt der zugeordnete EDV Administrator die Policy fest.
Port Policy	▪ Keine Restriktionen auf Daten-Ports (Datendosen) ▪ Keine Access Liste auf Daten-Ports (Datendosen)

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
DHCP	▪ Dynamische Adressvergabe im gesamten Datennetz ▪ Alle am Datennetz angeschlossen Endgeräte müssen DHCP unterstützen. Der Dienst DHCP gehört zu den IP Services die zentral erbracht werden. DHCP kann von jedem Endgerät verwendet werden. Über DHCP werden folgende Parameter zugewiesen: ▪ IPv4-Adresse ▪ IPv4 Subnetzmaske ▪ IPv4 Standardgateway ▪ IPv4-Adresse des DNS Servers (Dynamic Host Configuration Protocol nach RFC 2131)
IP-MAC-Binding	Unter IP-MAC-Binding versteht man die feste Zuordnung bzw. die feste Bindung einer MAC-Adresse zu einer IP-Adresse. Diese Bindung wird in einem Switch bzw. Router hinterlegt. Das IP-MAC-Binding ist die Grundlage diverser Sicherheitsverfahren. ▪ Dynamische Zuordnung über DHCP ▪ Feste Zuordnung einer IP4-Adresse zu einer MAC-Adresse nur über Manual DHCP Für Manual DHCP wird die MAC-Adresse eines Endgerätes in die DHCP-Datenbasis eingetragen und einer IPv4-Adresse fest zugeordnet. Daher erhält das Endgerät immer diese fest zugeordnete IPv4-Adresse über DHCP zugeteilt. Die Nutzung von Manual DHCP ist optional. Hinweis: Diese Funktion wird oft verwendet um Endgeräten, wie beispielsweise Druckern, eine feste IP-Adresse zuzuordnen
DNS	▪ Im gesamten Datennetz ist DNS verfügbar Der Dienst DNS gehört zu den IP Services die zentral erbracht werden. Die Verteilung der DNS Server erfolgt über DHCP. DNS kann von jedem Endgerät verwendet werden. (Domain Name System)
NTP	▪ Im gesamten Datennetz ist NTP verfügbar Der Dienst NTP gehört zu den IP Services die zentral erbracht werden. Er wird über Broadcast verteilt. NTP kann von jedem Endgerät verwendet werden. (Network Time Protocol)
SNMP	▪ SNMP Anfragen an Netzgeräte wie Router, Switches, usw. werden blockiert. ▪ SNMP Anfragen werden als Angriff gewertet. (Simple Network Management Protocol)

Sicherheitseinstellungen der Schnittstelle

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
Broadcast Limitierung	▪ Broadcast Limitierung ist aktiv ▪ Limit ist 5MBit/s Die Datenrate des eingehenden Broadcast Traffic wird gemessen. Liegt die Datenrate für Broadcast Traffic unter dem Limit, werden die Broadcast Pakete weitergeleitet. Übersteigt die Datenrate das Limit, so werden die folgenden Broadcast Pakete verworfen. Recovery: Unterschreitet die Datenrate für Broadcast Traffic wieder das Limit, werden die dann folgenden Broadcast Pakete weitergeleitet. Hinweis: Der restliche Datenverkehr ist davon nicht betroffen. Hinweis: Technisch wird Broadcast Traffic und Multicast Traffic gemessen und zur Datenrate für Broadcast addiert (Cisco:storm-control, HP:rate-limit)
Multicast Limitierung	▪ Multicast Limitierung ist aktiv ▪ Limit ist 1MBit/s Die Datenrate des eingehenden Multicast Traffic wird gemessen. Liegt die Datenrate für Multicast Traffic unter dem Limit, werden die Multicast Pakete weitergeleitet. Übersteigt die Datenrate für Multicast Traffic das Limit, so werden die folgenden Multicast Pakete verworfen. Recovery: Unterschreitet die Datenrate für Multicast Traffic wieder das Limit, werden die dann folgenden Multicast Pakete weitergeleitet. Hinweis: Der restliche Datenverkehr ist davon nicht betroffen. Hinweis: Technisch wird nur Multicast Traffic gemessen. (Cisco:storm-control, HP:rate-limit)
BPDU Guard	▪ BPDU Guard ist aktiv Der eingehende Traffic wird auf Datenpakete des Spanning Tree Protokolle (BPDUs) untersucht. Wird ein solches Paket gefunden, wird der Daten-Port (Datendose) automatisch deaktiviert. Recovery: Händisch durch die Abteilung Netze. Vorher muss die Fehlerquelle beseitigt werden. (Cisco:guard root, HP:bpdu-protection)

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
Port Security	▪ Port Security ist aktiv ▪ Limit ist 15 MAC-Adressen ▪ Aging Time ist 60s Port Security führt für jeden Daten-Port (Datendose) eine Liste von erlaubten MAC-Adressen. Datenpakete werden nur weitergeleitet, wenn ihre MAC-Adresse in der Liste enthalten ist. Für Port Security werden der eingehende Traffic bzw. die eingehenden Datenpakete untersucht. Die in den Datenpaketen eingetragenen MAC-Adressen werden gelernt und in die Liste der erlaubten MACs eingetragen. Gelernte MAC-Adressen werden automatisch nach der Aging Time wieder aus der Liste gelöscht. Wird das Limit (Anzahl) der gelernten MAC-Adressen an einem Daten-Port (Datendose) überschritten, so wird der Daten-Port (Datendose) deaktiviert und die Liste wird geleert. Port Security untersucht den eingehenden IPv4-Traffic auch nach Kollisionen von MAC-Adressen. Wurde eine empfangene MAC-Adresse bereits an einem anderen Daten-Port (Datendose) gelernt, liegt eine Kollision vor. In diesem Fall wird der Daten-Port (Datendose) über den die MAC-Adressen empfangen wurde deaktiviert. Hinweis: In der Regel gehört zu jedem Endgerät eine MAC-Adresse. Durch Port Security wird daher praktisch die Anzahl der anschließbaren Endgeräte festgelegt. Hinweis: Wird ein Gerät umgesteckt, so muss die aging time abgewartet werden. Erst nach Ablauf der aging time ist ein neuer Verbindungsaufbau möglich. Recovery: Deaktivierte Daten-Ports (Datendosen) werden automatisch nach einer Minute wieder aktiviert. (Cisco:port-security, HP:port-security)

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
DHCP Snooping (IP-MAC-Port-Binding)	▪ DHCP Snooping ist aktiv DHCP Snooping untersucht den eingehenden Traffic auf Datenpakete von DHCP Servern. Werden eingehende Datenpakete von DHCP Servern erkannt, so werden diese verworfen (drop). Damit wird der Betrieb von "wilden" DHCP Servern unterbunden. Ausgehende Datenpakete von DHCP Servern, beispielsweise Datenpakete des zentralen DHCP Servers, sind davon nicht betroffen. Der eingehende IPv4-Traffic wird untersucht, um die Zuordnung von MAC-Adressen zu IPv4-Adressen für einen Daten-Port (Datendose) dynamisch zu lernen. Dazu werden die DHCP Pakete ausgewertet, die zwischen DHCP Client und DHCP Server ausgetauscht werden. Die vom DHCP Server vergebene IPv4-Adresse und die MAC-Adresse des Clients werden in eine Liste eingetragen. Jeder Listeneintrag besteht aus einem Tripel (IPv4, MAC, Port), das auch IP-MAC-Port-Binding genannt wird. Für jeden Daten-Port (Datendose) wird diese Liste geführt. Zusätzlich wird die Lease Time der via DHCP vergebenen IPv4-Adresse eingetragen. Listeneinträge werden automatisch nach Ablauf der Lease Time aus der Liste gelöscht. Die erstellten Listen werden von anderen Security Features verwendet. Recovery: DHCP Server im Access Bereich sind verboten. Daher ist ein Recovery auch nicht vorgesehen. Hinweis: Traffic von DHCP Clients wird durch DHCP Snooping nicht behindert. Es werden keine DHCP-Client Pakete verworfen Hinweis: Der restliche Datenverkehr ist davon **nicht** betroffen. (Cisco:dhcp snooping, HP:dhcp-snooping)
DAI Dynamic ARP Inspection	▪ DAI (Dynamic ARP Inspection) ist akiv Der eingehende und ausgehende IPv4-Traffic wird untersucht. Für jedes Datenpaket wird untersucht, ob die dort eingetragene IPv4 Adresse bekannt ist. Ist die Adresse bekannt, wird das ARP Paket weitergeleitet. Ist die Adresse unbekannt, wird das ARP Paket verworfen (drop). Eine Adresse ist dann bekannt, wenn sie in der Liste mit dem IP-MAC-PORT-Bindings enthalten ist. Es wird überprüft, ob die IPv4-Adresse für den Port eingetragen wurde, über den das Paket empfangen wurde oder gesendet werden soll. Die MAC Adresse wird nicht überprüft. DAI erkennt ARP Anfragen mit gefälschten IPv4-Adressen (Spoofing) und unterbindet sie. Voraussetzung: IPv4-Adresse wurde über DHCP bezogen (Cisco:arp inspection, HP:arp-protect)

Eigenschaft	Verhalten auf Datendose bzw. Daten-Port
DAI Rate Limit	▪ DAI Rate Limit ist aktiv ▪ Limit ist 128 pps (Pakets per Second) Die Datenrate des eingehenden ARP Traffic wird gemessen. Liegt die Datenrate für ARP Traffic unter dem Limit, werden die ARP Pakete weitergeleitet. Übersteigt die Datenrate das Limit wird der Daten-Port (Datendose) automatisch deaktiviert. Recovery: Deaktivierte Daten-Ports (Datendosen) werden automatisch nach einer Minute wieder aktiviert (Cisco:ip arp inspection limit,)
IP Source Guard	▪ IP Source Guard ist aktiv Der eingehende IPv4 Traffic wird untersucht. Für jedes Datenpaket wird überprüft, ob die dort eingetragene IPv4-Source-Adresse bekannt ist. Ist die Adresse bekannt, wird das Paket weitergeleitet. Ist die Adresse unbekannt, wird das Paket verworfen (drop). Eine Adresse ist dann bekannt, wenn sie in der Liste mit dem IP-MAC-PORT-Bindings enthalten ist. Es wird überprüft, ob die IPv4-Source-Adresse für den Port eingetragen wurde, über den das Paket empfangen wurde. Die MAC Adresse wird nicht überprüft. Auch werden ausgehende Pakete nicht überprüft. Voraussetzung: IPv4-Adresse wurde über DHCP bezogen. Hinweis: IP Source Guard lässt DHCP-Traffic transparent passieren. (Cisco:verify source, HP:dynamic ip lockdown)

Mechanische Schnittstelle

Kupferkabel sind die Standardverbindung zwischen Endgeräten und dem Datennetz im Access Bereich. Sie sind auf beiden Enden mit Datendosen versehen. Historisch wurden in der Universität Datendosen vom Typ EC7 verbaut. Im Rahmen der Sanierung der Universität Bielefeld wurde die Umstellung des Steckersystems beschlossenen. Zukünftig kommt der RJ45 Stecker zum Einsatz. Daher wird in diesem Dokument zwischen den beiden folgenden Varianten unterschieden:

- Alter Stecker
  - EC7 Stecker
  - Findet sich vor allem in noch nicht sanierten Gebäuden des UHG
- Neuer Stecker
  - RJ45 Stecker
  - Findet sich vor allem in Verkabelungen neueren Datums.

Mechanische Schnittstelle alter Stecker (EC7)

Die bestehende, alte Kupferverkabelung entspricht ISO/IEC Linkklasse Class F_a mit ISO/IEC Kategorie $Cat7_a$ Komponenten. Sie hat eine EC7 Kupplung (Stecker, Steckdose) und beruht auf der Systemlösung ELine 1200 der Firma Leoni Kerpen. Der mechanische Anschluss von Endgeräten erfolgt über Patchkabel in den beiden folgenden Varianten:

- Der Anschluss von Endgeräten erfolgt über ein Patchkabel mit bis zu 5m Länge. Es kommen 4-Draht Patchkabel mit EC7 Stecker an einem Ende und RJ45 Stecker am anderen Ende zum Einsatz. Über eine 4-Draht Verbindung sind Bandbreiten mit bis zu 100MBit/s möglich.
- Der Anschluss von Endgeräten erfolgt über ein Patchkabel mit bis zu 5m Länge. Es kommen 8-Draht Patchkabel mit EC7 Stecker an einem Ende und RJ45 Stecker am anderen Ende zum Einsatz. Über eine 8-Draht Verbindung sind Bandbreiten mit bis zu 1GBit/s möglich.

 EC7 Datendose	 EC7 Patchkabel, 4-Draht	 EC7 Patchkabel, 8-Draht

Mechanische Schnittstelle neuer Stecker (RJ45)

Die neue Kupferverkabelung entspricht der Link Klasse ISO/IEC Class E_a mit ISO/IEC Kategorie $Cat6_a$ Komponenten. Sie hat eine RJ45 Kupplung (Stecker, Steckdose). Es sind immer alle 8 Adern belegt und es kommt kein Cablesharing zum Einsatz.
Der Anschluss von Endgeräten erfolgt über ein Patchkabel mit bis zu 5m Länge. Es kommen 8-Draht Patchkabel mit RJ45 Steckern an beiden Enden zum Einsatz.

 RJ45 Datendose	 RJ45 Patchkabel, 8-Draht	