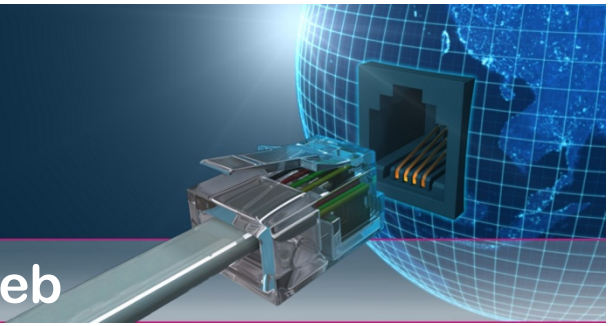
Kommunikationsnetze in Betrieb (1)





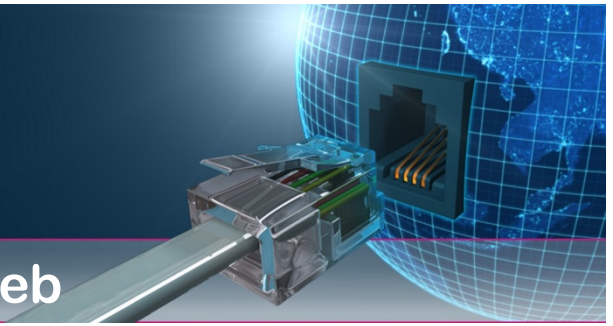



V 17-02 vom 19.03.2017



Inhalt

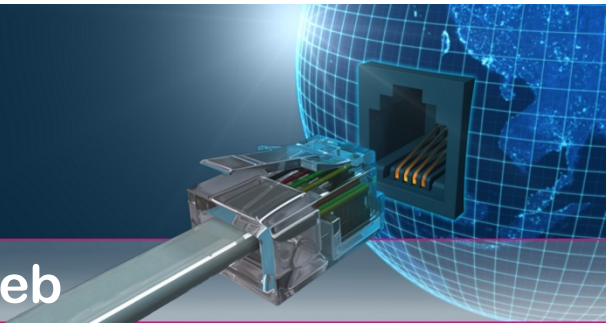
- Nächste Schritte
- IP-Adressierung
- Sicherheit in IP-basierenden Netzen
- Schwachstellen in Fernwirknetzen
- Kommunikationsnetze Anwendungen
- Konzept DigiComm



Kommunikationsnetze in Betrieb

Nächste Schritte

- Anforderungen an Übertragungstechnik
- Entscheidung Layer 2, VLAN …
- Entscheidung Layer 3 Routing, MPLS …
- IP-Adressschema



Kommunikationsnetze in Betrieb

Anforderungen an Übertragungstechnik

- Einfache Bedienung und Handhabbarkeit
- Überwachung per SNMP oder Kontakte
- Fernkonfiguration
- Besondere Maßnahmen für Sicherheit und Datenschutz

Kommunikationsnetze in Betrieb

Anforderungen an Übertragungstechnik

- Einfache Konfiguration über Browser, CLI und SSH/Telnet
- Konfigurationsdaten können lokal oder Remote gespeichert werden
- Management über SNMP v1/2/3 und Alarmkontakte
- Alle Ports (Ethernet/WAN) einzeln konfigurier- uns abschaltbar
- Bridge & Router & Firewall

Bausteine für wirtschaftliche Datenübertragung

Kommunikationsnetze in Betrieb

DigiComm

- Home
- Quick Setup
- Network
- Advanced
- Security
- Management
- Show
- Status
- Utilities

© 2016 Digicomm GmbH

Dsl Status

Item	Local Side				Remote Side			
	Channel A	Channel B	Channel C	Channel D	Channel A	Channel B	Channel C	Channel D
Mode	Master	Master	Master	Master	Slave	Slave	Slave	Slave
State	CONNECTED	CONNECTED	CONNECTED	CONNECTED	CONNECTED	CONNECTED	CONNECTED	CONNECTED
Line Rate	15288Kbps	15288Kbps	15288Kbps	15288Kbps	15288Kbps	15288Kbps	15288Kbps	15288Kbps
Attenuation	0dB	0dB	0dB	0dB	1dB	0dB	0dB	0dB
SNR	9dB	8dB	11dB	11dB	11dB	11dB	11dB	11dB
CRC	0	0	0	3	0	0	0	0

ClearCRC

Interface Statistics

Port	InOctets	OutOctets	InPackets	OutPackets	InDrops	OutDrops	Active
LAN	1668932	3222019	14410	14410	0	0	UP
WAN1	0	574	0	0	0	0	UP

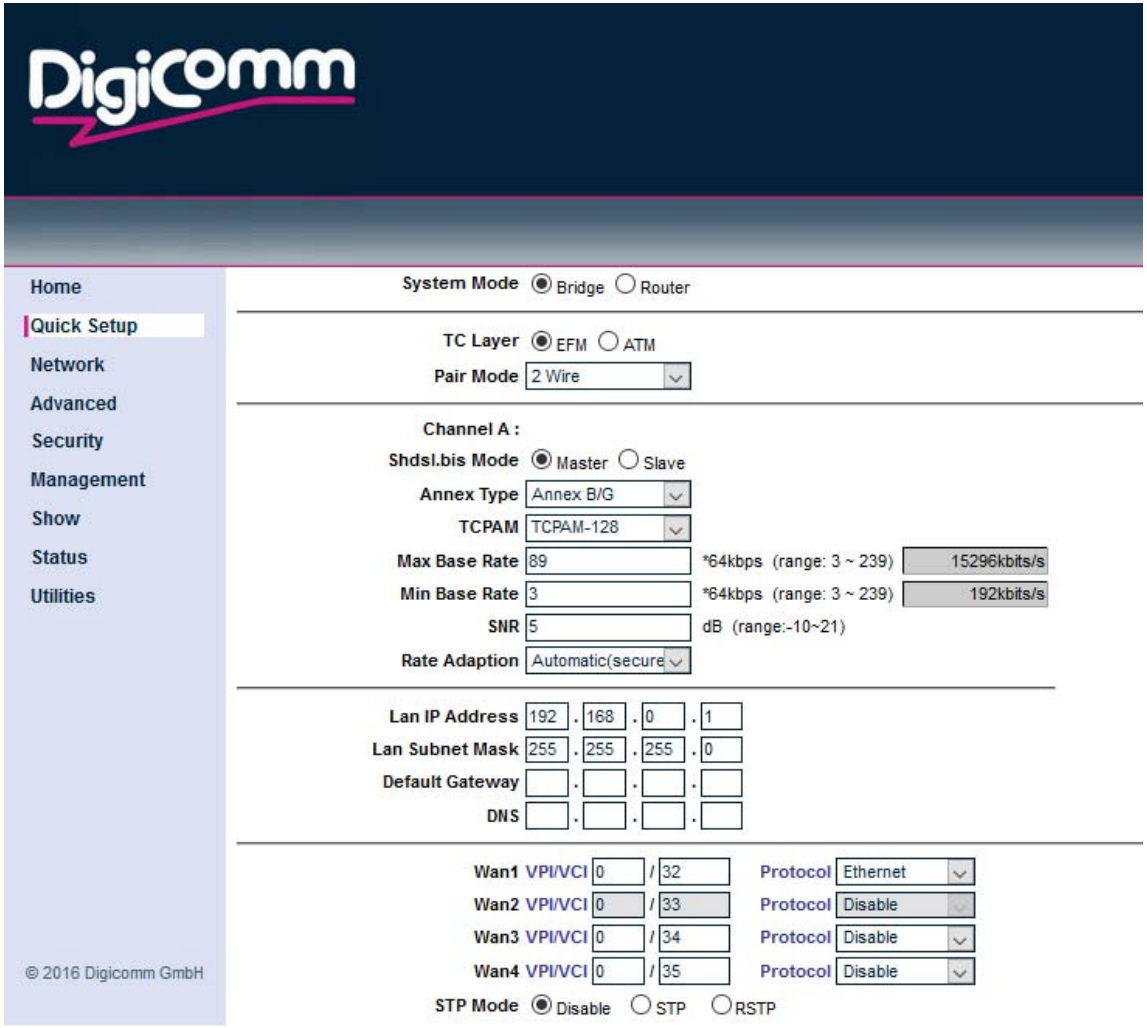
Switch Status

Port 1	Port 2	Port 3	Port 4

DigiComm

Bausteine für wirtschaftliche Datenübertragung

Kommunikationsnetze in Betrieb

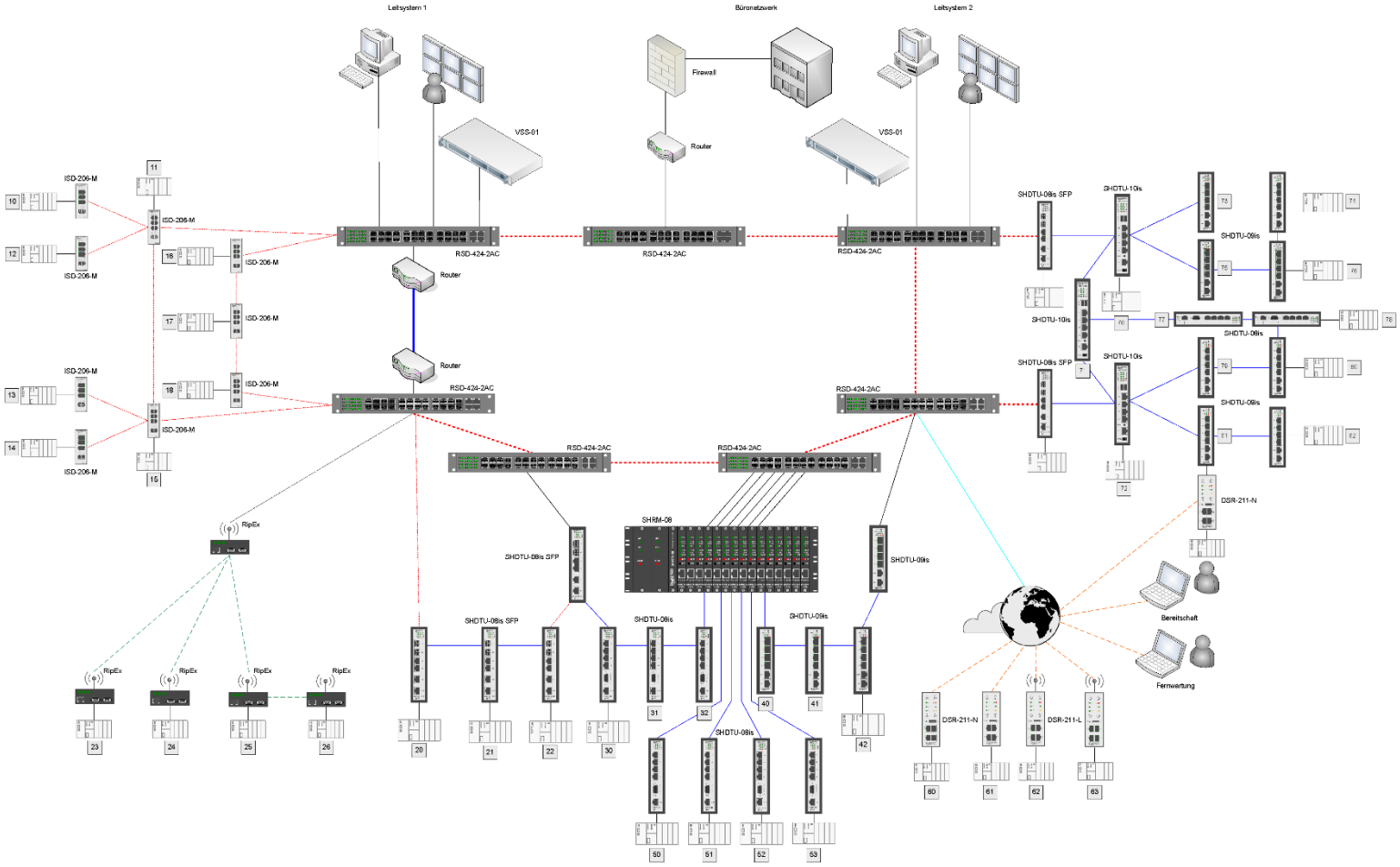


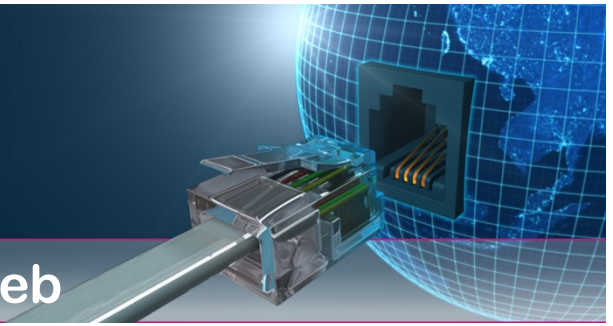
SHDTU - Konfigurationsmöglichkeiten

Einfache Inbetriebnahme oder Austausch

- Voreingestellt für den Punkt-zu-Punkt Betrieb oder Kundenspezifisch
- Für beide Seiten identische Geräte (Einstellung: Master / Slave)
- Vorkonfiguriert auf Master/Slave, Bridgemode und automatische Anpassung der Geschwindigkeit an die Qualität der Leitung (Plug and Play)
- Die Konfiguration kann lokal oder auf einem Server abgespeichert werden

Kommunikationsnetze in Betrieb





Kommunikationsnetze in Betrieb

Layer 2 = Bridge/Switch Infrastruktur

Vorteile

- Einfache Infrastruktur
- Ein IP-Netzwerk
- Trennung von Diensten über VLAN
- Unterschiedliche Netze können parallel übertragen werden

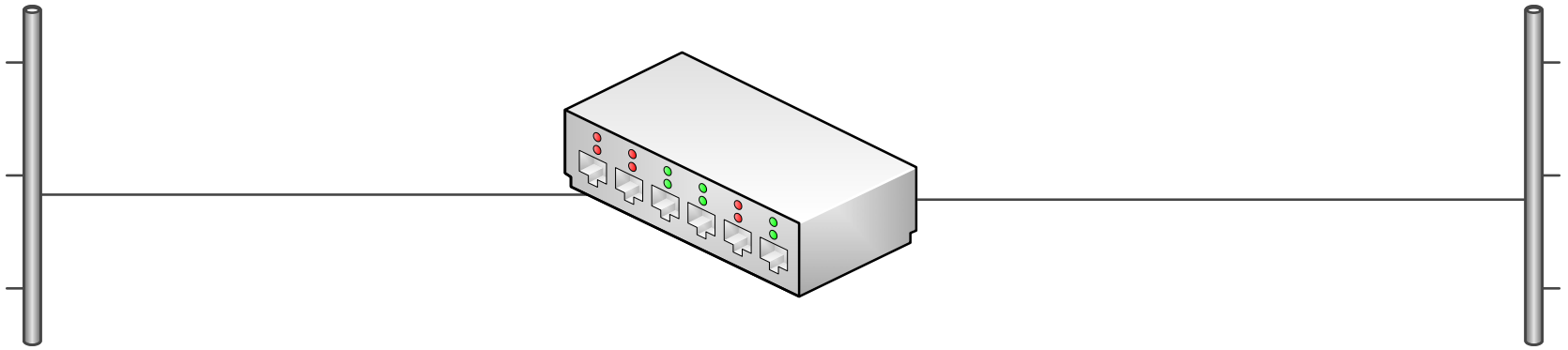
Nachteile

- Ein IP-Netzwerk (eine Broadcastdomäne)
- Leichter angreifbar
- Höhere Last als bei Layer-3 Netzwerken

Kommunikationsnetze in Betrieb

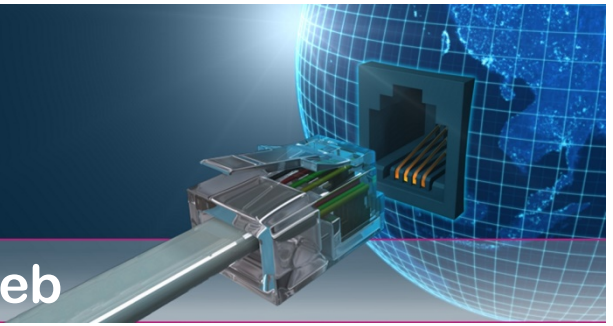
Layer 2 = Bridge/Switch Infrastruktur

Funktionsprinzip



192.168.0.0

192.168.0.0



Kommunikationsnetze in Betrieb

Layer 3 = Routing Infrastruktur

Vorteile

- Jede Station ein eigenes Netzwerk
- Trennung von Diensten über VPN
- Gezielte Zuweisung
- Unterschiedliche Netze können mit Router verbunden werden

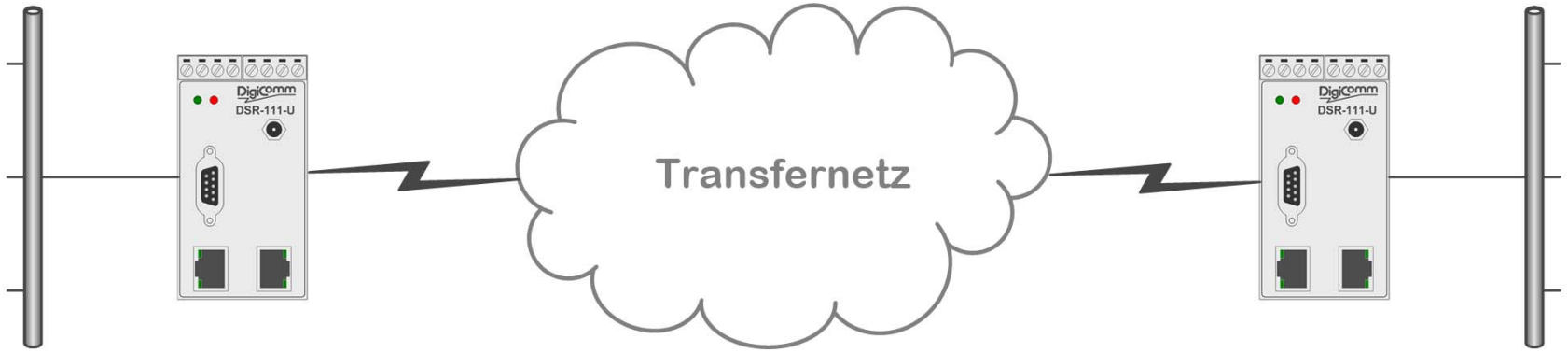
Nachteile

- IT Kenntnisse erforderlich
- Höherer Konfigurationsaufwand
- Kompliziertere Handhabung

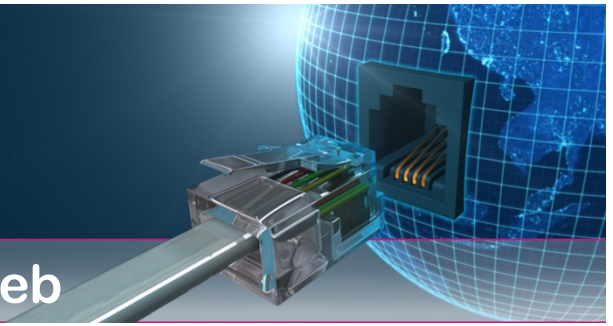
Kommunikationsnetze in Betrieb

Layer 3 = Routing Infrastruktur

Standardkonfiguration VPN



192.168.0.0 10.1.1.0 172.5.5.0



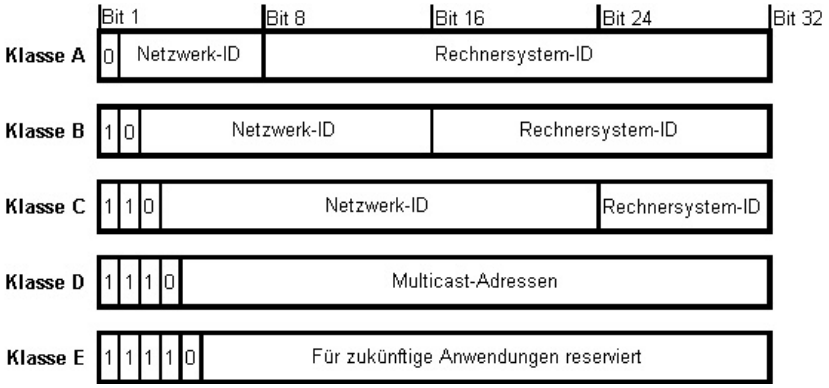
Kommunikationsnetze in Betrieb

IP-Adressierung

- Jedes End- und Übertragungsgerät hat eine 32 Bit lange IP-Adresse
- Eine IP-Adresse ist eindeutig
- Geräte die an verschiedene Netze angeschlossen sind, haben in jedem Netz eine eigene IP-Adresse
- IP-Adressen werden in einem Unternehmen zentral verwaltet um Adresskonflikte zu vermeiden

Kommunikationsnetze in Betrieb

IP-Adressierung



IP-Adresse nach IPv4

192.168.178.135

8 Bit großer Zahlenblock

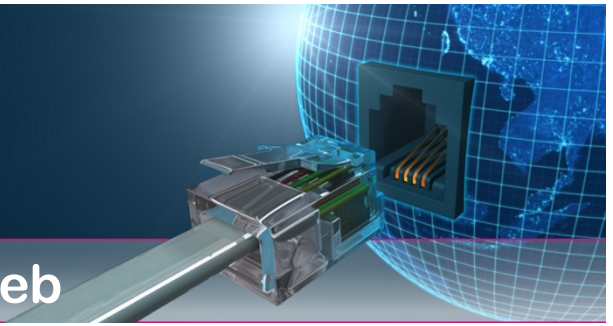
Dezimal im Bereich zwischen 0 – 255

Insgesamt bestehend aus 4 Zahlenblöcken

?

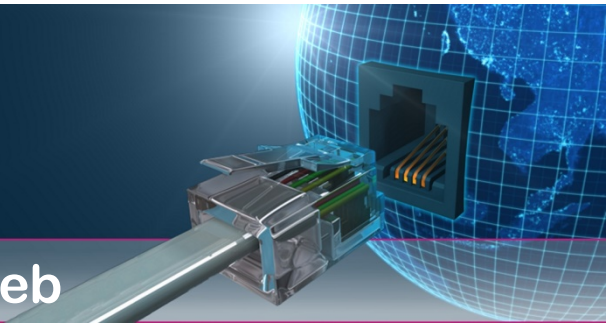
Klasse	Werte der ersten Bits	Dezimalwerte für das erste Byte	Verfügbarer Adressbereich (für Hosts)
A	**0**	0 - 127	1.0.0.1 - 126.255.255.254
B	**10**	128 - 191	128.0.0.1 - 191.255.255.254
C	**110**	192 - 223	192.0.0.1 - 223.255.255.254
D	**1110**	224 - 239	224.0.0.0 - 239.255.255.255
E	**1111**	240 - 255	240.0.0.0 - 255.255.255.255

Sicherheit in IP-basierenden Netzen



Sicherheit in IP-basierenden Netzen

- Der Wechsel von serieller zu IP-basierender Übertragung bringt zahlreiche Vorteile mit sich, wie z. B. einfacher Zugriff, schnelle Verbindungen, unterschiedliche Dienste über eine Verbindung usw.
- Dadurch werden aber auch bisher abgesicherte Produktions-prozesse von außen und innen angreifbar
- Das Thema Sicherheit wurde in der Fernwirktechnik bisher nachrangig behandelt oder vernachlässigt
- Angriffe durch „Stuxnet“ oder die „Snowden Affäre“ schärfen den Sinn für Sicherheit



Sicherheit in IP-basierenden Netzen

- Mit der Veröffentlichung im Bundesanzeiger am 24.07.2015 ist das IT-Sicherheitsgesetz in Kraft getreten und bringt spezielle Anforderungen für Betreiber kritischer Infrastrukturen mit sich
- Betroffen sind vor allem die Sektoren Energie, Wasser, Transport und Verkehr, sowie Informationstechnik und Telekommunikation, die die Mindeststandards zur IT-Sicherheit aus dem am 12.08.2015 veröffentlichten IT-Sicherheitskatalog umsetzen, einhalten und zertifizieren müssen
- Die Zertifizierung muss der Bundesnetzagentur bis zum 31.01.2018 nachgewiesen werden

Sicherheit in IP-basierenden Netzen

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden

Sicherheit in IP-basierenden Netzen

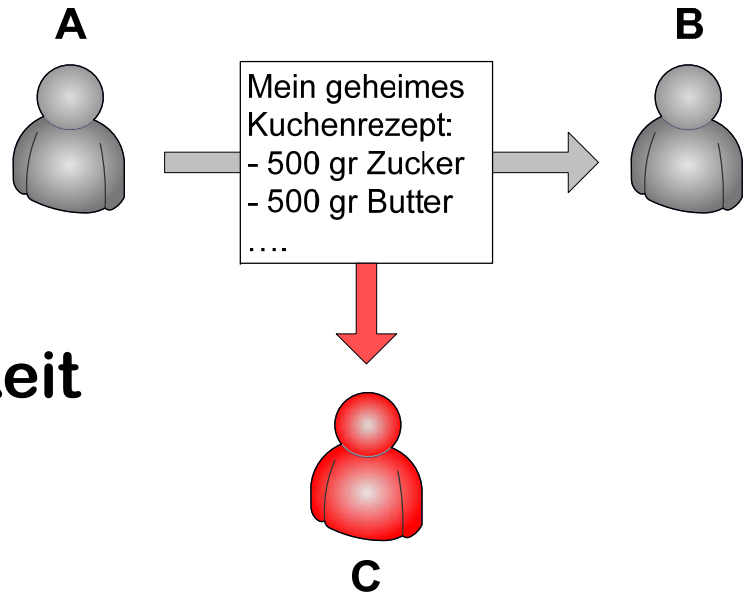
Sicherheit ist kein Produkt,

sondern ein Prozess, mit drei Zielen:

Sicherheit in IP-basierenden Netzen

Vertraulichkeit

- A möchte B bei der Gründung einer Konditorei helfen und stellt ihm sein geheimes Kuchenrezept zur Verfügung
- Konkurrent C kann das Dokument ebenfalls lesen



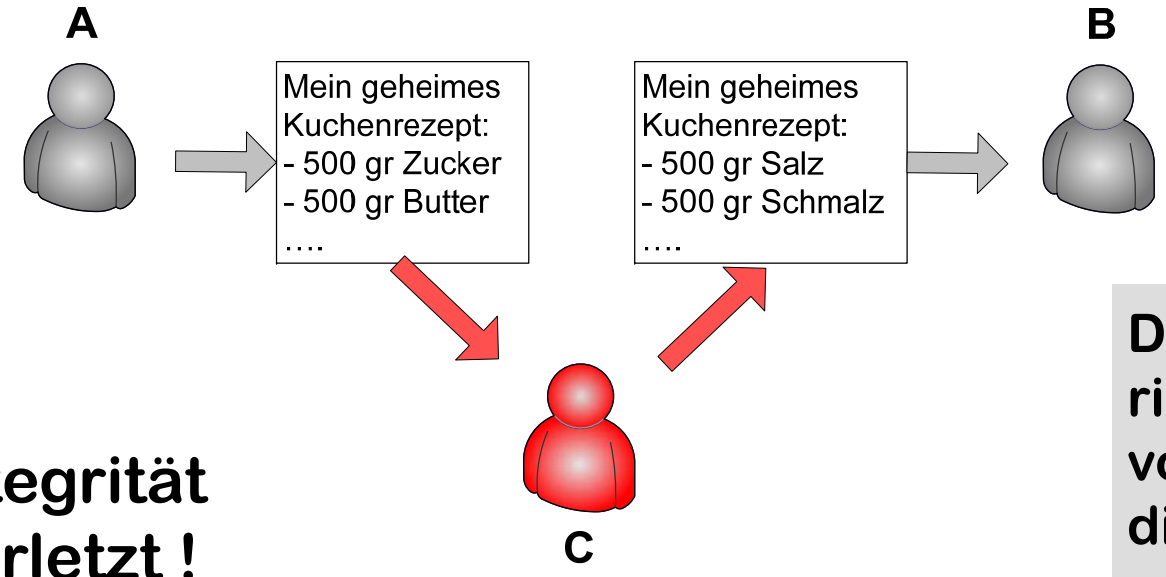
Vertraulichkeit verletzt !

Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse

Sicherheit in IP-basierenden Netzen

Integrität

- C manipuliert das Dokument unbemerkt



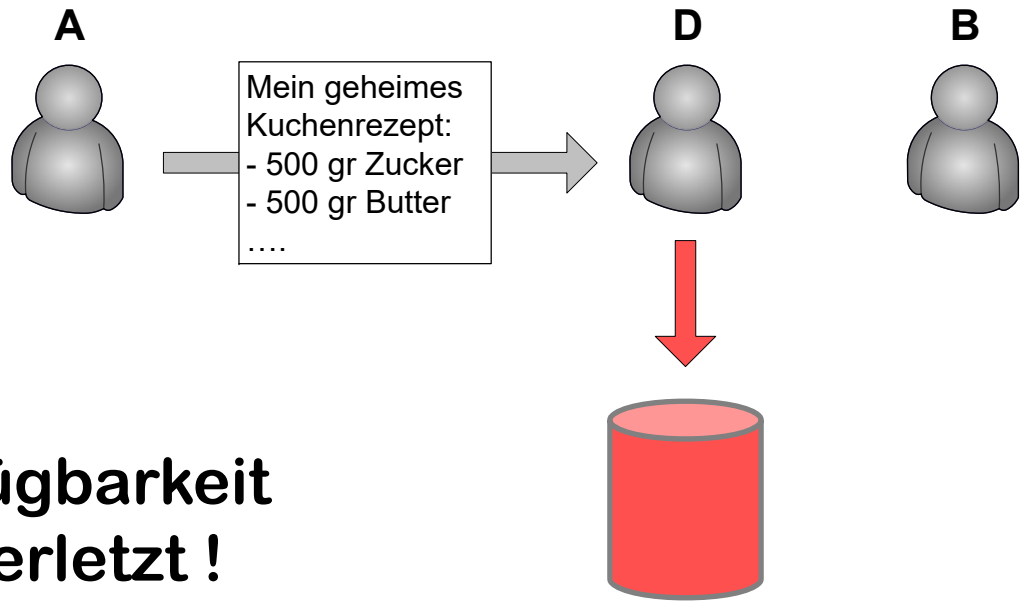
Integrität verletzt !

Die Daten müssen richtig und vollständig sein und die Systeme müssen korrekt funktionieren

Sicherheit in IP-basierenden Netzen

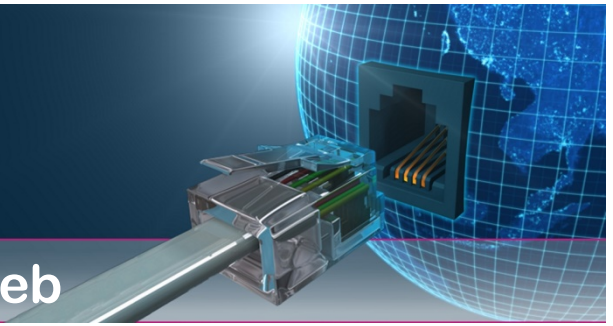
Verfügbarkeit

- D leitet das für B bestimmte Dokument nicht weiter oder löscht es



Verfügbarkeit verletzt !

Die zu schützenden Systeme müssen jederzeit betriebsbereit und über berechtigte Teilnehmer nutzbar und zugänglich sein



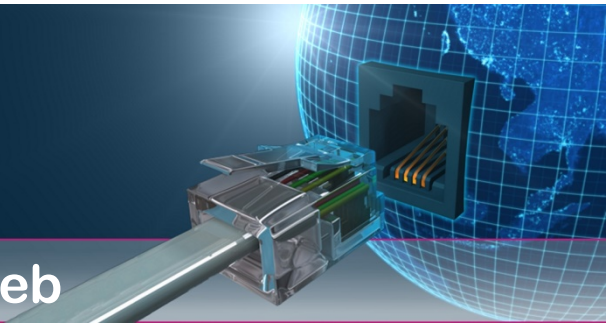
Sicherheit in IP-basierenden Netzen

Relevante Standards für Sicherheit im industriellen Umfeld

- **ISO-Standard 27001**
  inklusive der ergänzenden Standards mit den fortlaufenden Nummern 270xx
  Die Anforderungen der ISO 27001 beschreiben WAS im Bereich Sicherheit gemacht werden muss

- **IT-Grundschutz Katalog (BSI)**
  Der IT-Grundschutz beschreibt darüber hinaus auch, WIE es gemacht werden kann

(BSI = Bundesamt für Sicherheit und Informationstechnik)



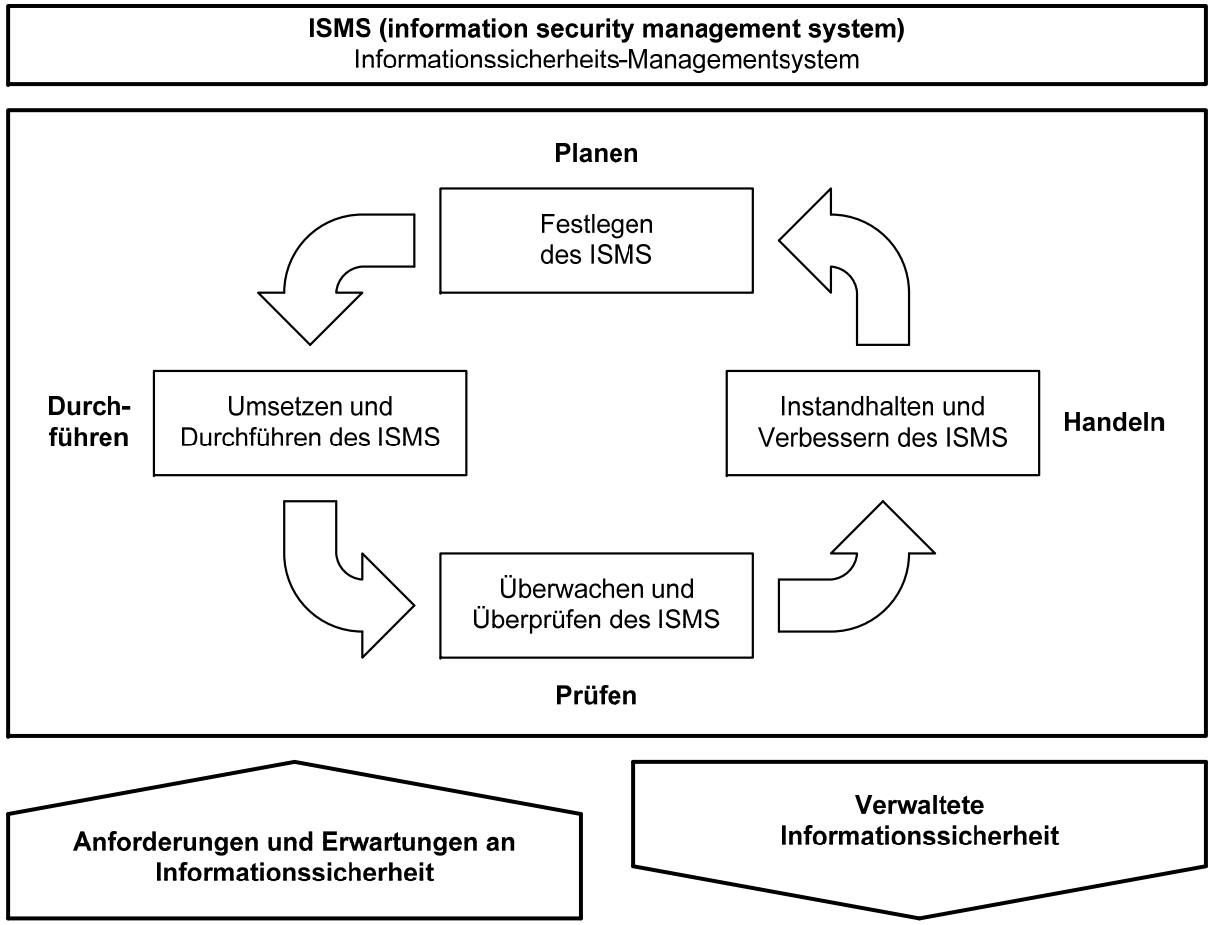
Sicherheit in IP-basierenden Netzen

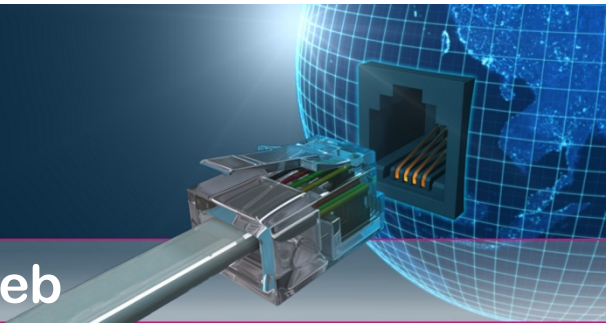
Ziel: Zertifizierung nach ISO 27001 bis zum 31.01.2018

Einsatz eines Sicherheitsmanagers

- Dokumentation laufender Prozesse
- Bewertung von Risikofällen
- Vorschläge zur Optimierung
- Koordination von Maßnahmen
- Überprüfen der Ergebnisse

Sicherheit in IP-basierenden Netzen

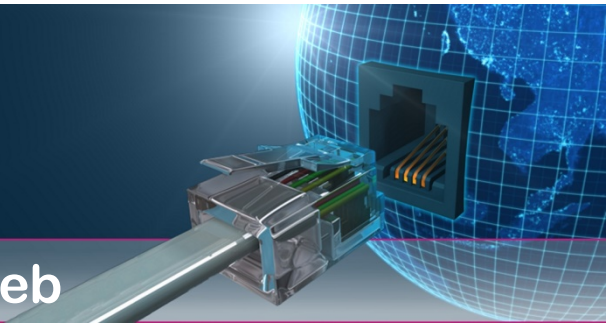




Sicherheit in IP-basierenden Netzen

Risikofälle können eine Vielzahl von Ursachen haben, die in folgende Kategorien unterteilt werden:

- **Elementare Gefährdung**
- **Höhere Gewalt**
- **Organisatorische Mängel**
- **Menschliches Fehlverhalten**
- **Technisches Versagen**
- **Vorsätzliche Handlungen**



Sicherheit in IP-basierenden Netzen

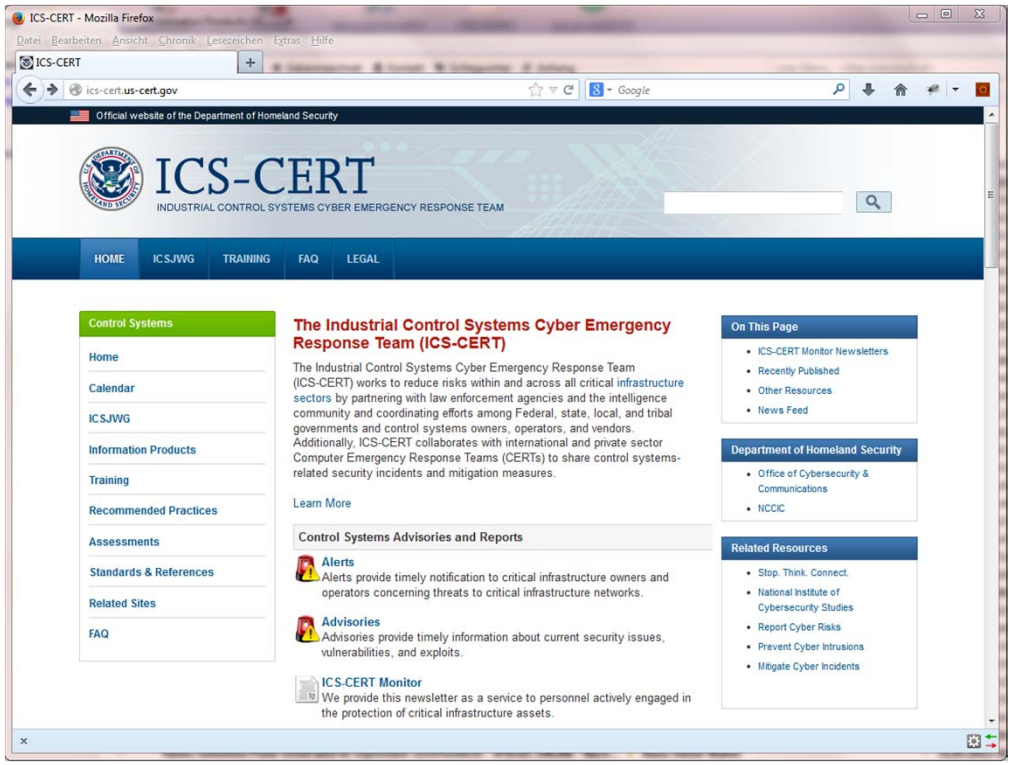
Beispiele:

- **Zutrittskontrolle und Objektsicherung**
- **Trennung von Diensten**
- **Überwachung der Infrastruktur und der Geräte**
- **Klares Konzept für Passworte (Password, Geheim, 11111, admin, qwertz usw. sollten der Vergangenheit angehören)**

Sicherheit in IP-basierenden Netzen

In den USA existiert ein öffentlich zugängliches „ICS-CERT“.

Siehe auch „Allianz für Cyber-Sicherheit“ des BSI …

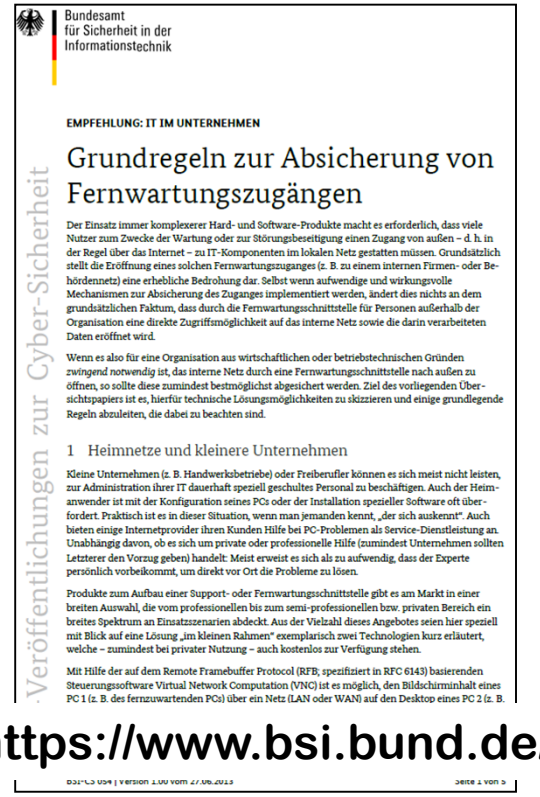


https://ics-cert.us-cert.gov/

https://www.allianz-fuer-cybersicherheit.de

Sicherheit in IP-basierenden Netzen

Bei der Entwicklung orientieren wir uns an den BSI-Empfehlungen IT-Grundschutz und an ISO 27001



Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Grundregeln zur Absicherung von Fernwartungszugängen

Der Einsatz immer komplexerer Hard- und Software-Produkte macht es erforderlich, dass viele Nutzer zum Zwecke der Wartung oder zur Störungsbeseitigung einen Zugang von außen – d. h. in der Regel über das Internet – zu IT-Komponenten im lokalen Netz gestatten müssen. Grundsätzlich stellt die Eröffnung eines solchen Fernwartungszuganges (z. B. zu einem internen Firmen- oder Behördennetz) eine erhebliche Bedrohung dar. Selbst wenn aufwendige und wirkungsvolle Mechanismen zur Absicherung des Zuganges implementiert werden, ändert dies nichts an dem grundsätzlichen Faktum, dass durch die Fernwartungsschnittstelle für Personen außerhalb der Organisation eine direkte Zugriffsmöglichkeit auf das interne Netz sowie die darin verarbeiteten Daten eröffnet wird.

Wenn es also für eine Organisation aus wirtschaftlichen oder betriebstechnischen Gründen *zwingend notwendig* ist, das interne Netz durch eine Fernwartungsschnittstelle nach außen zu öffnen, so sollte diese zumindest bestmöglichst abgesichert werden. Ziel des vorliegenden Übersichtspapiers ist es, hierfür technische Lösungsmöglichkeiten zu skizzieren und einige grundlegende Regeln abzuleiten, die dabei zu beachten sind.

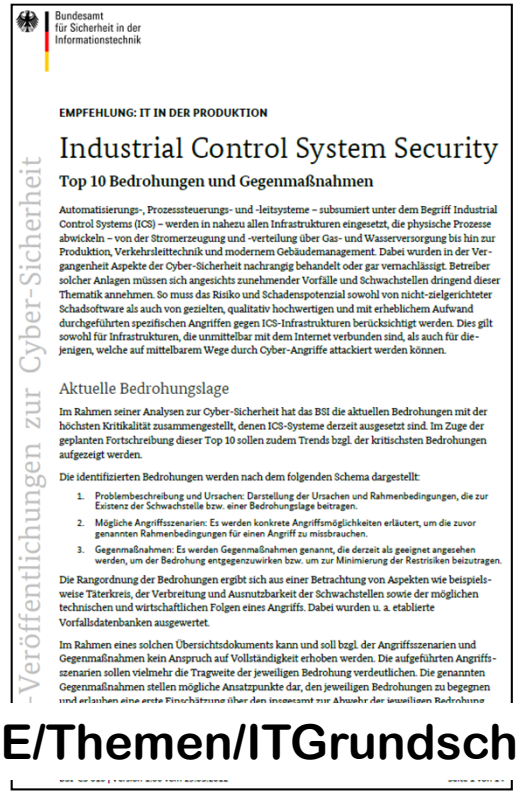
1 Heimnetze und kleinere Unternehmen

Kleine Unternehmen (z. B. Handwerksbetriebe) oder Freiberufler können es sich meist nicht leisten, zur Administration ihrer IT dauerhaft speziell geschultes Personal zu beschäftigen. Auch der Heimanwender ist mit der Konfiguration seines PCs oder der Installation spezieller Software oft überfordert. Praktisch ist es in dieser Situation, wenn man jemanden kennt, „der sich auskennt". Auch bieten einige Internetprovider ihren Kunden Hilfe bei PC-Problemen als Service-Dienstleistung an. Unabhängig davon, ob es sich um private oder professionelle Hilfe (zumindest Unternehmen sollten Letzterer den Vorzug geben) handelt: Meist erweist es sich als zu aufwendig, dass der Experte persönlich vorbeikommt, um direkt vor Ort die Probleme zu lösen.

Produkte zum Aufbau einer Support- oder Fernwartungsschnittstelle gibt es am Markt in einer breiten Auswahl, die vom professionellen bis zum semi-professionellen bzw. privaten Bereich ein breites Spektrum an Einsatzszenarien abdeckt. Aus der Vielzahl dieses Angebotes seien hier speziell mit Blick auf eine Lösung „im kleinen Rahmen" exemplarisch zwei Technologien kurz erläutert, welche – zumindest bei privater Nutzung – auch kostenlos zur Verfügung stehen.

Mit Hilfe der auf dem Remote Framebuffer Protocol (RFB, spezifiziert in RFC 6143) basierenden Steuerungssoftware Virtual Network Computation (VNC) ist es möglich, den Bildschirminhalt eines PC 1 (z. B. des fernzuwartenden PCs) über ein Netz (LAN oder WAN) auf den Desktop eines PC 2 (z. B.

Veröffentlichungen zur Cyber-Sicherheit



Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

Top 10 Bedrohungen und Gegenmaßnahmen

Automatisierungs-, Prozesssteuerungs- und -leitsysteme – subsumiert unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln – von der Stromerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Produktion, Verkehrsleittechnik und modernem Gebäudemanagement. Dabei wurden in der Vergangenheit Aspekte der Cyber-Sicherheit nachrangig behandelt oder gar vernachlässigt. Betreiber solcher Anlagen müssen sich angesichts zunehmender Vorfälle und Schwachstellen dringend dieser Thematik annehmen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit erheblichem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Aktuelle Bedrohungslage

Im Rahmen seiner Analysen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS-Systeme derzeit ausgesetzt sind. Im Zuge der geplanten Fortschreibung dieser Top 10 sollen zudem Trends bzgl. der kritischsten Bedrohungen aufgezeigt werden.

Die identifizierten Bedrohungen werden nach dem folgenden Schema dargestellt:

1. Problembeschreibung und Ursachen: Darstellung der Ursachen und Rahmenbedingungen, die zur Existenz der Schwachstelle bzw. einer Bedrohungslage beitragen.
2. Mögliche Angriffsszenarien: Es werden konkrete Angriffsmöglichkeiten erläutert, um die zuvor genannten Rahmenbedingungen für einen Angriff zu missbrauchen.
3. Gegenmaßnahmen: Es werden Gegenmaßnahmen genannt, die derzeit als geeignet angesehen werden, um der Bedrohung entgegenzuwirken bzw. um zur Minimierung der Restrisiken beizutragen.

Die Rangordnung der Bedrohungen ergibt sich aus einer Betrachtung von Aspekten wie beispielsweise Täterkreis, der Verbreitung und Ausnutzbarkeit der Schwachstellen sowie der möglichen technischen und wirtschaftlichen Folgen eines Angriffs. Dabei wurden u. a. etablierte Vorfallsdatenbanken ausgewertet.

Im Rahmen eines solchen Übersichtsdokuments kann und soll bzgl. der Angriffsszenarien und Gegenmaßnahmen kein Anspruch auf Vollständigkeit erhoben werden. Die aufgeführten Angriffsszenarien sollen vielmehr die Tragweite der jeweiligen Bedrohung verdeutlichen. Die genannten Gegenmaßnahmen stellen mögliche Ansatzpunkte dar, den jeweiligen Bedrohungen zu begegnen

Veröffentlichungen zur Cyber-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: HERSTELLER

Anforderungen an netzwerkfähige Industriekomponenten

Speicher-programmierbare Steuerungen (SPS) und ähnliche industriell genutzte, netzwerkfähige Komponenten verfügen zunehmend über Dienste, die auch bei Serversystemen zu finden sind. Zusätzlich zu diesen Standarddiensten gibt es bei solchen Geräten eine Reihe von Prinzipien zu beachten, um als Hersteller ein sicheres Produkt anbieten zu können. Dieses Dokument gibt Herstellern einen Überblick über die zentralen Best Practices für solche Komponenten. In Ergänzung hierzu stellt das BSI einen Leitfaden für Hersteller von Industriekomponenten zur Verfügung, der bei dem Aufbau von Produkttests und Sicherheitsanalysen unterstützen soll.

Organisatorische Maßnahmen

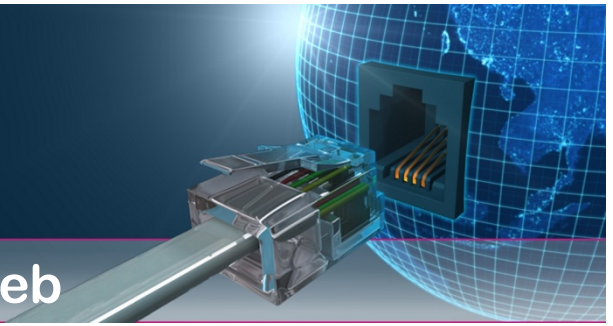
Product Lifecycle & interne Prozesse

Eine grundlegende Verbesserung der Sicherheit eines Produkts kann durch das Etablieren eines sicheren Entwicklungszyklus (Secure Software Development Lifecycle) erzielt werden. Hierzu kann man sich u. a. an den folgenden Fragen orientieren.

- Gibt es einheitliche und verbindliche, dem aktuellen Stand der Technik entsprechende Vorgaben zur sicheren Implementierung (Development Policies)?
- Sind im Entwicklungszyklus verbindliche Prüfphasen (Security Gates) vorgeschrieben, in denen beispielsweise ein Review der Anwendungslogik oder eine ganzheitliche Sicherheitsbetrachtung erfolgt?
- Sind – sofern technisch und wirtschaftlich möglich – automatisierte Codeanalysen fester Bestandteil des Entwicklungszyklus?
- Werden im Entwicklungszyklus Sicherheitsanalysen zu Bedrohungen und Risiken durchgeführt und Gegenmaßnahmen festgelegt?
- Werden Produkte einer technischen Sicherheitsanalyse (Penetrations- oder Schwachstellentests) unterzogen, bei denen nicht nur auf bekannte Schwachstellen, sondern auch auf neue Verwundbarkeiten (z. B. durch Fuzzing-Tests) untersucht wird?
- Werden flankierende Sicherheitsmechanismen, wie Antivirus-Produkte, gefördert (z. B. Zertifizierung) statt deren Einsatz z. B. durch einen Ausschluss der Gewährleistung zu untersagen?

Veröffentlichungen zur Cyber-Sicherheit

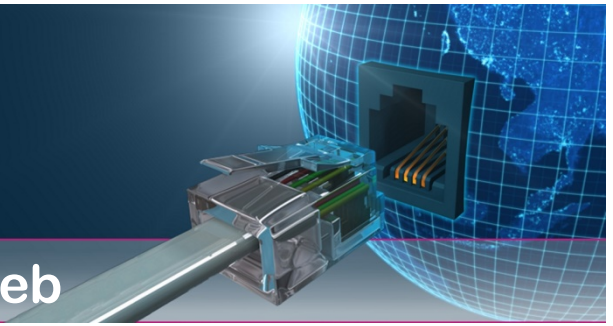
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html



Sicherheit in IP-basierenden Netzen

- Sichere Datenübertragung besteht aus vielen Einzelelementen, die nur als Gesamtkonzept die angestrebte Sicherheit ermöglichen
- Sicherheitsmaßnahmen sind nicht einmalig, sondern ein andauernder Prozess
- Alle Lösungen der DigiComm unterstützen die notwendigen Sicherheitsfunktionen

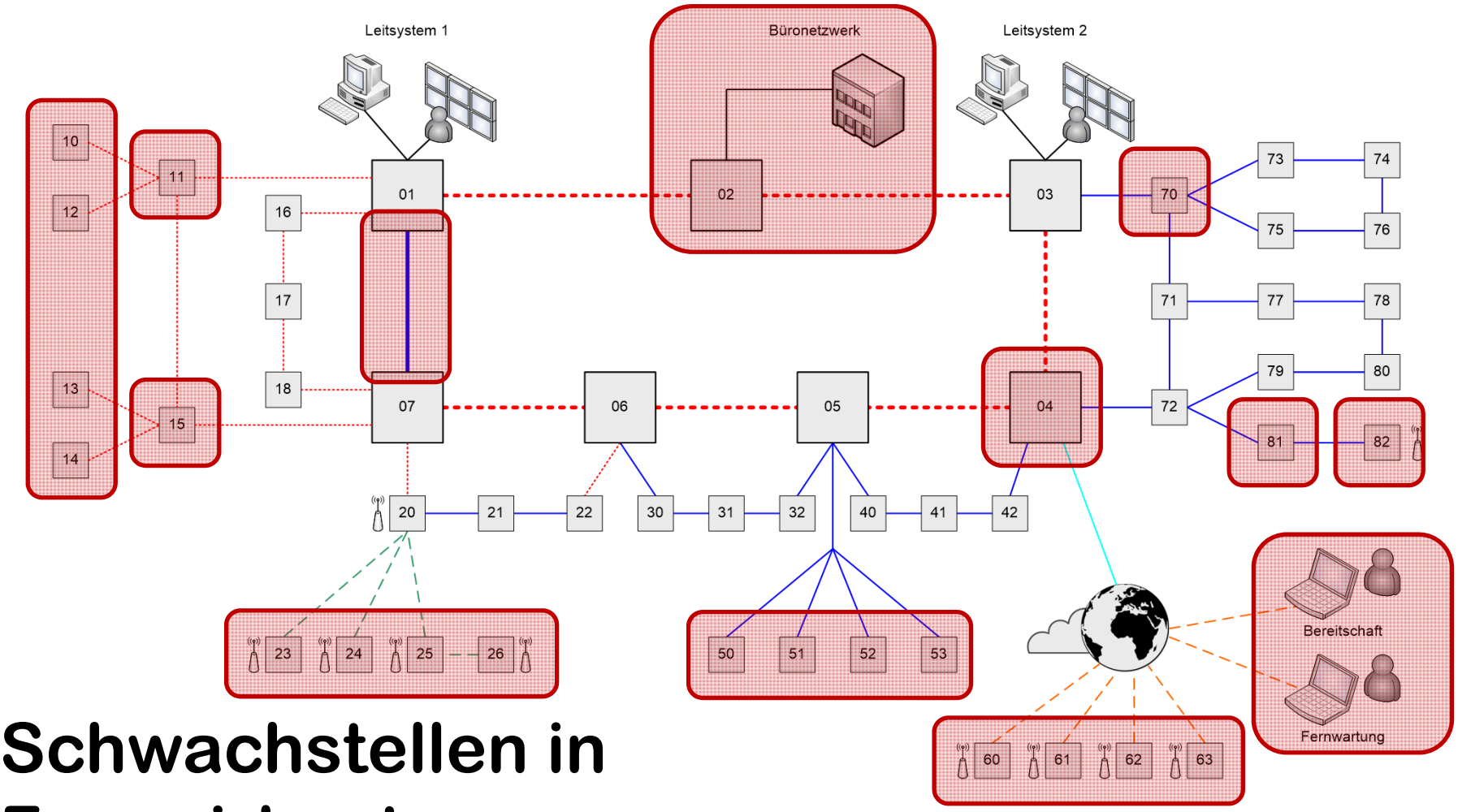
Schwachstellen in Fernwirknetzen



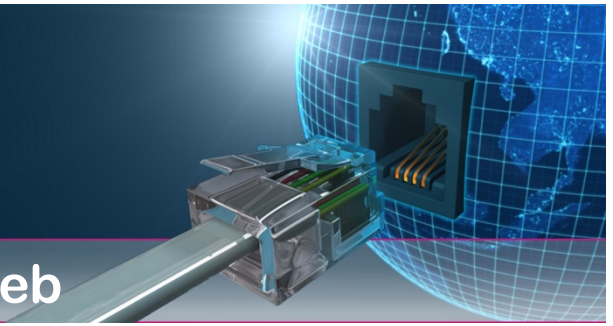
Top 10 Bedrohungen nach BSI

(Bundesamt für Sicherheit und Informationstechnik) (Quelle: BSI-A-CS 004 | Version 1.00 vom 12.04.2012)

1. Unberechtigte Nutzung von Fernwartungszugängen
2. Online-Angriffe über das Firmennetzwerk
3. Angriffe auf eingesetzte Standardkomponenten
4. (D)DOS Angriffe (Distributed Denial of Service)
5. Menschliches Fehlverhalten und Sabotage
6. Einschleusen von Schadcodes über Wechseldatenträger
7. Lesen und Schreiben von Daten / Nachrichten
8. Unberechtigter Zugriff auf Ressourcen
9. Angriffe auf Netzwerkkomponenten
10. Technisches Fehlverhalten und höhere Gewalt



Schwachstellen in Fernwirknetzen

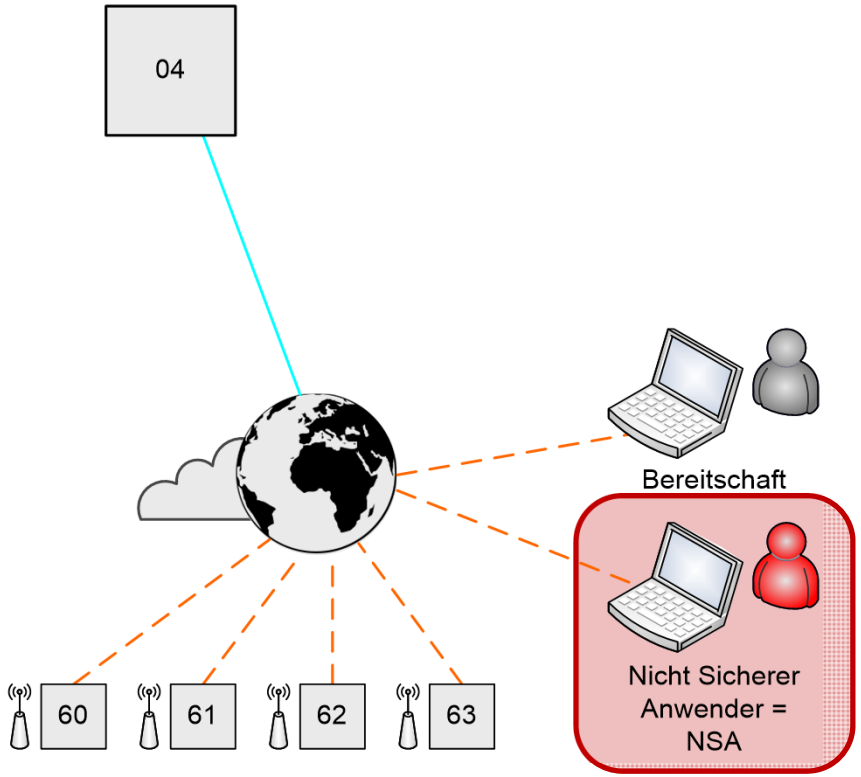


Schwachstellen in Fernwirknetzen

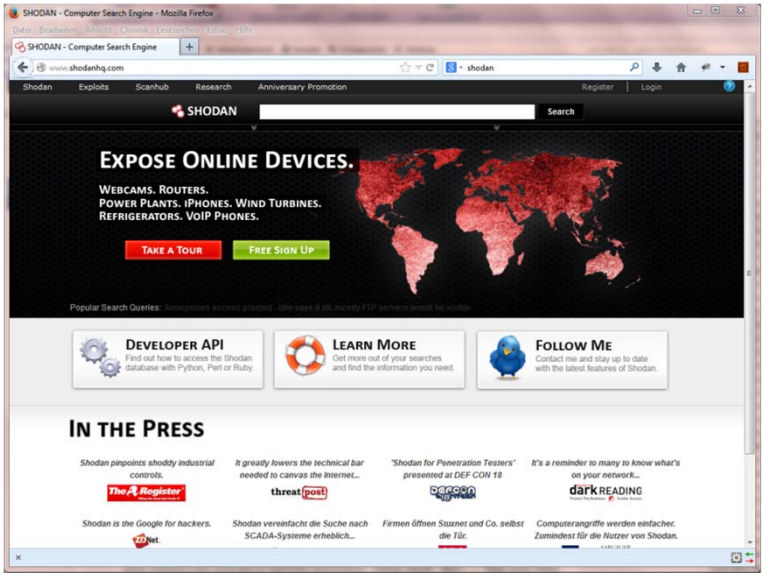
- Fernwartungszugänge
- Anbindung über öffentliche Netze
- Netzübergänge
- Übertragung über Fremdleitungen
- Kommunikationsstruktur und –geräte
- Stations-Technik und -Geräte

Schwachstellen in Fernwirknetzen

Fernwartungszugänge



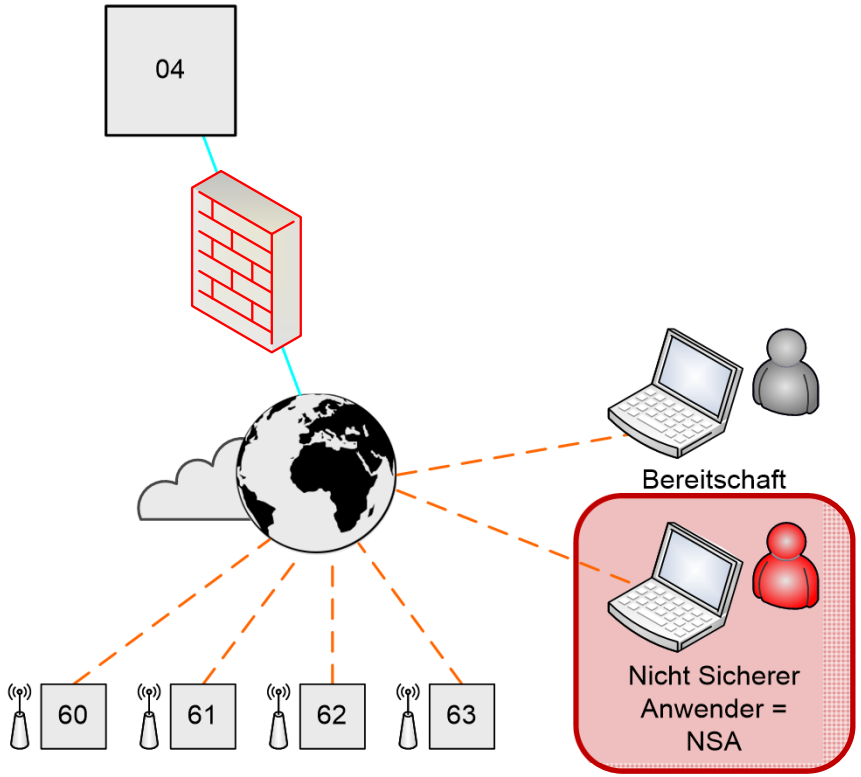
Es gibt spezielle Suchmaschinen, die angreifbare Systeme anzeigen

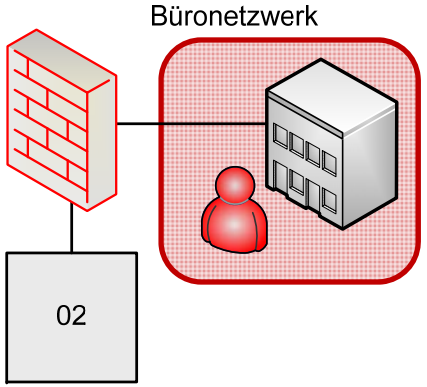


www.shodanhq.com

Schwachstellen in Fernwirknetzen

Netzübergänge

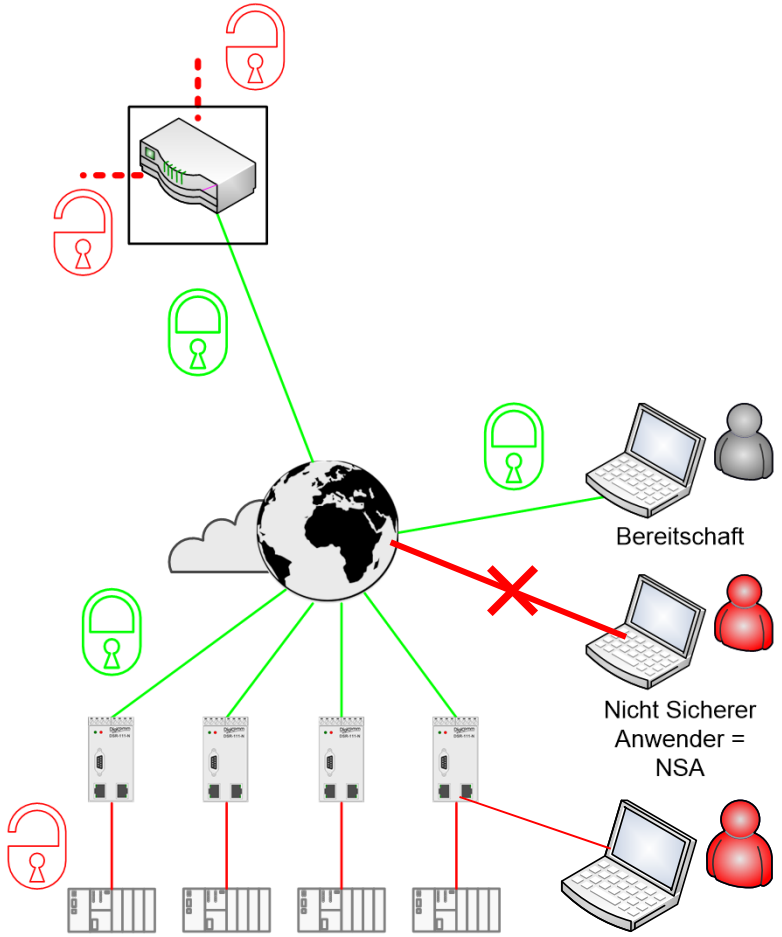




Schwachstellen in Fernwirknetzen

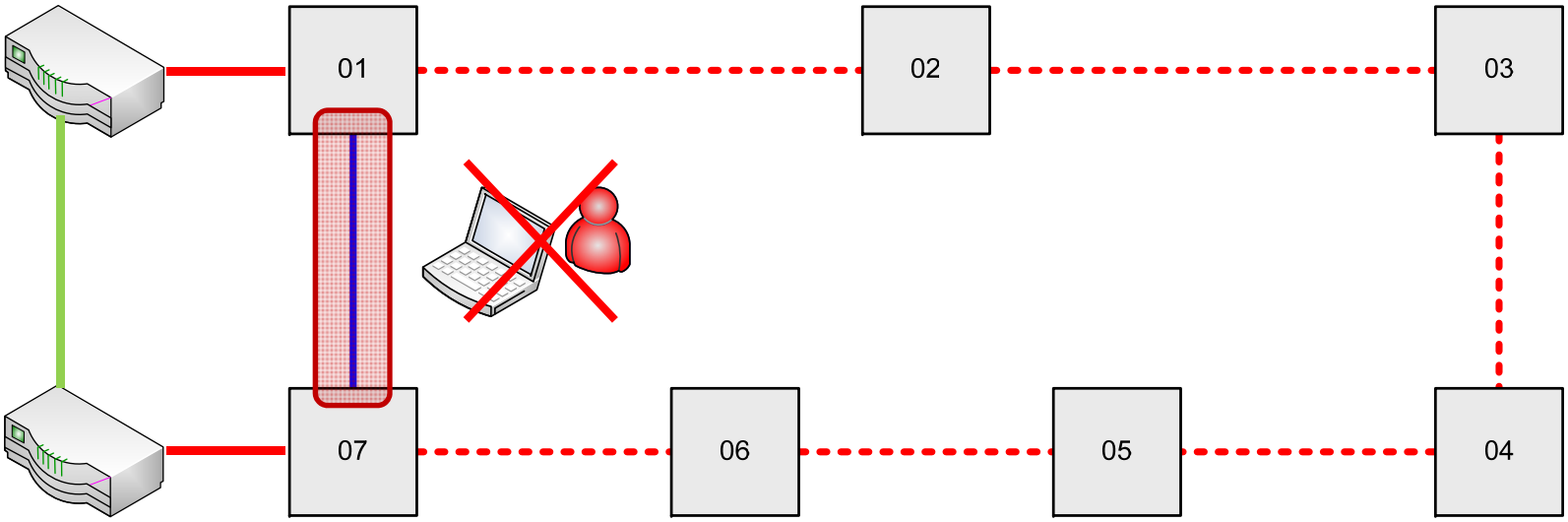
Netzübergänge

Ein VPN (Virtual Private Network) ist ein Lösungsansatz, führt aber nicht automatisch zu einer (hoch)sicheren Lösung …



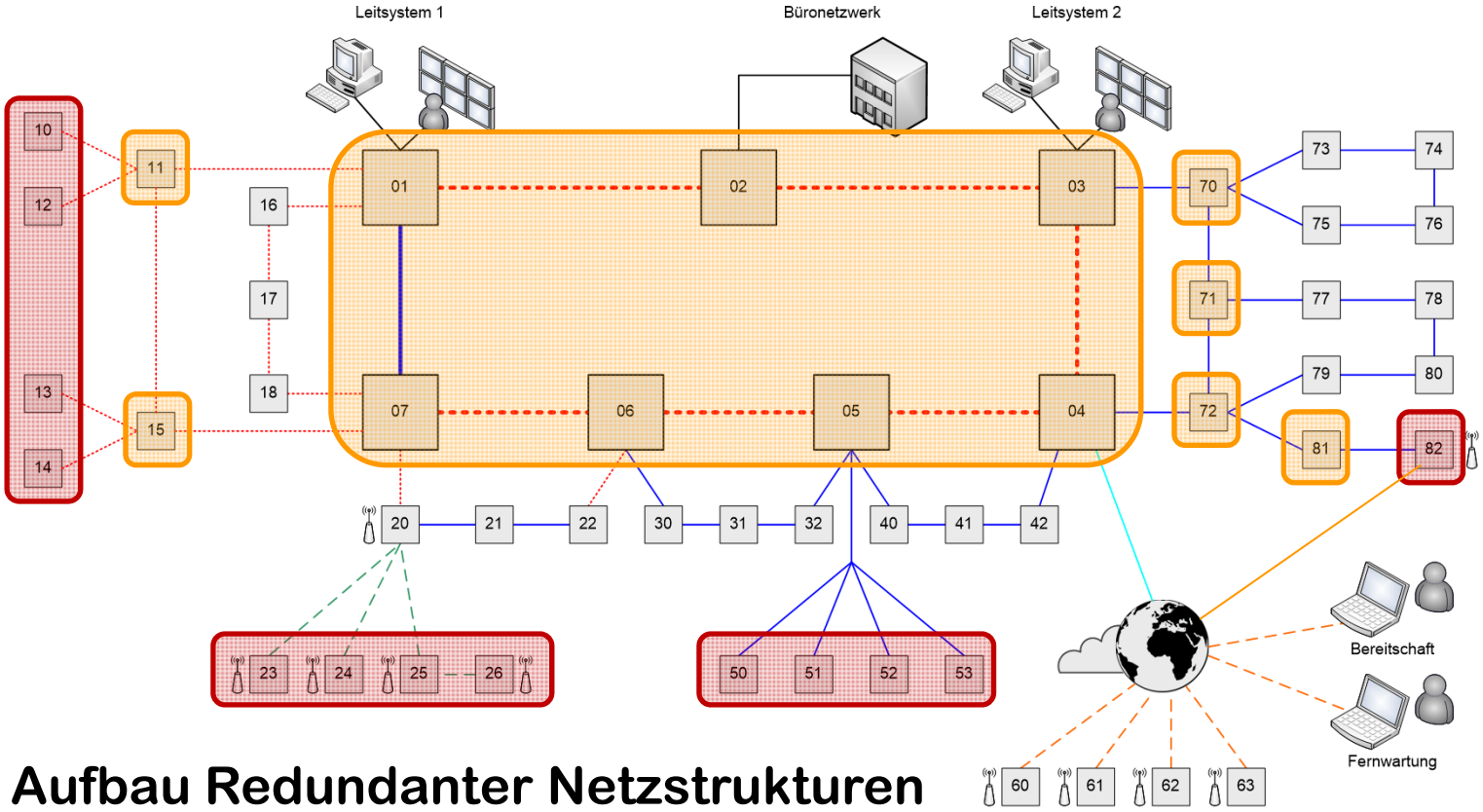
Schwachstellen in Fernwirknetzen

Übertragung über Fremdleitungen



Schwachstellen in Fernwirknetzen

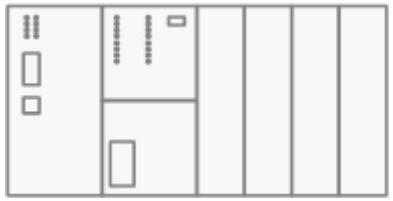
Kommunikationsstruktur und –geräte



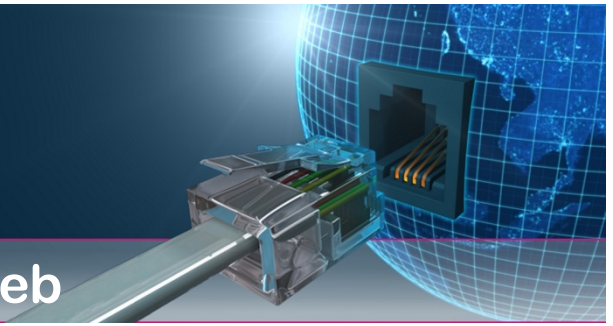
Aufbau Redundanter Netzstrukturen

Schwachstellen in Fernwirknetzen

Stations-Technik und -Geräte



- Security follows function: Durch LAN und Embedded Webserver sind unzählige Systeme angreifbar geworden …
- MSR-Baugruppen besitzen keine fälschungs-sicheren bzw. eindeutige digitalen Identitäten …
- Einseitige Authentifizierung und unverschlüsselt übertragende Benutzernamen/Passwörter sind sehr bedenklich …
- MSR-Architekturen sind nicht DoS-resistent …



Schwachstellen in Fernwirknetzen

Forderungen (Security) an Übertragungstechnik

- Gesicherter Zugriff auf die Geräte mit HTTPS und Username/Passwort – mit unterschiedlichen Berechtigungen
- Trennung von Diensten, z.B. Management / Fernwirken
- VPN-Verbindungen für potentiell unsichere Endgeräte oder Verbindungen über öffentliche Netze

Kommunikationsnetze in Betrieb

Forderungen (Security) an Übertragungstechnik

- ✓ Bridge & Router & Firewall
- ✓ Zugriff über User/Passwort mit unterschiedlichen Berechtigungen
- ✓ VLAN 802.1Q & Port-basierend inkl. Management im eigenen VLAN
- ✓ HTTPS/SSH/SNMPv3 – Zugriff
- ✓ STP/RSTP und MSTP für VLAN im Ring
- ✓ OSPF/RIP – Automatisiertes Routing (mit Verschlüsselung)

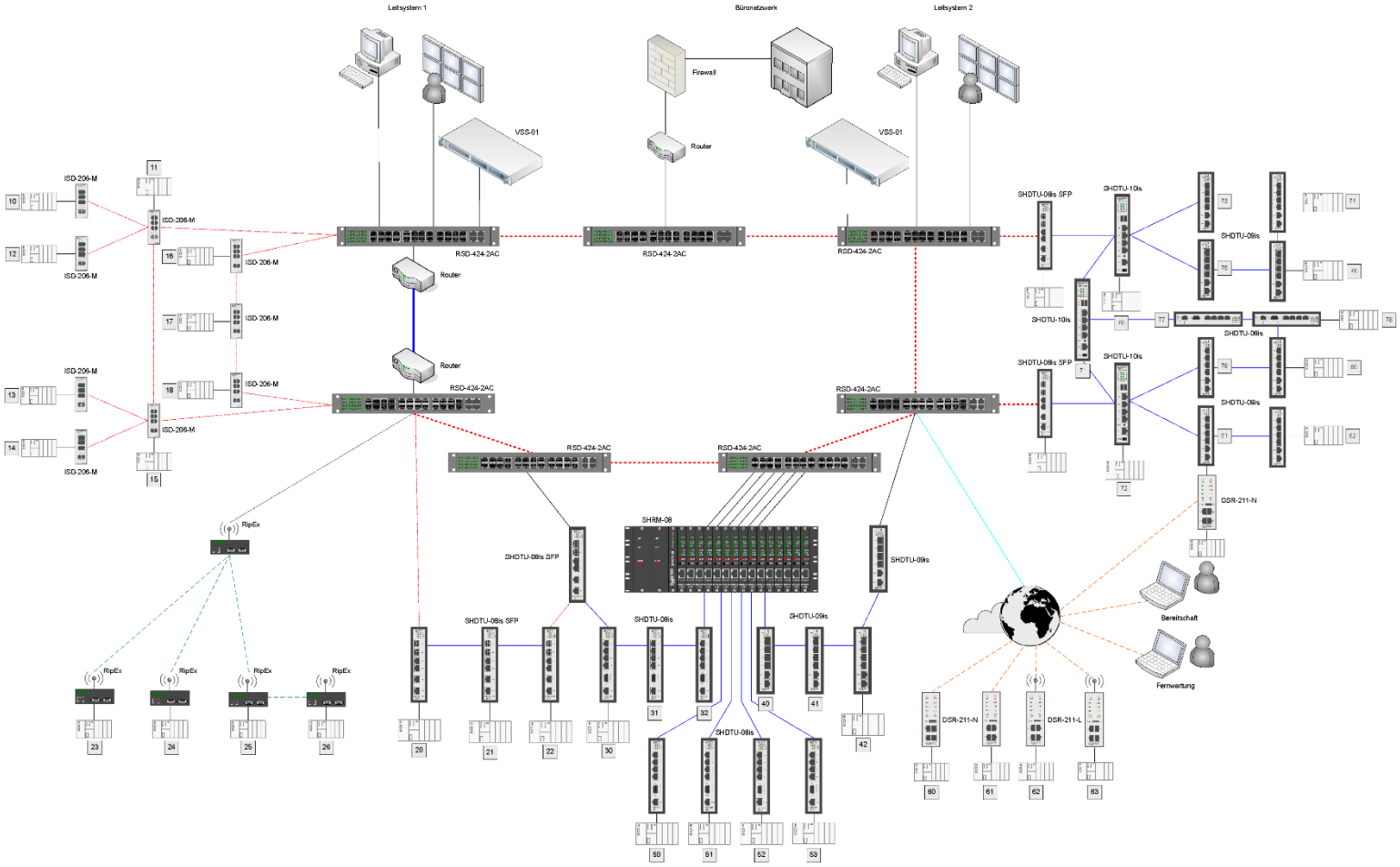
Kommunikationsnetze in Betrieb

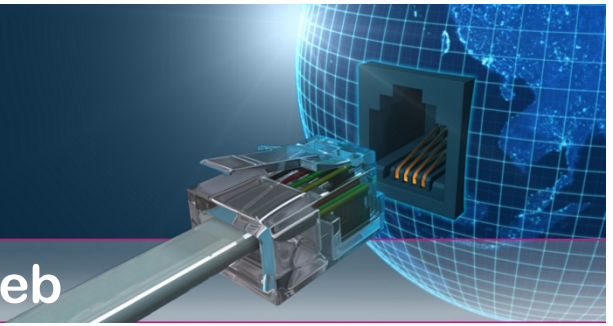
Forderungen (Security) an Übertragungstechnik

- ✓ VPN-Verschlüsselung über WAN und per Port
- ✓ Abschalten nicht genutzter LAN-Ports
- ✓ Port-Control
- ✓ Abschalten der WEB-Oberfläche
- ✓ Portfreigabe über MAC- / IP-Adresse
- ✓ Freigabe nur für bestimmte Dienste

Kommunikationsnetze Anwendungen

Kommunikationsnetze Anwendungen





Kommunikationsnetze Anwendungen

Netzaufbau - Stand

- ✓ Infrastruktur = Umstellung auf Ethernet
- ✓ Redundante Netzwerkstrukturen
- ✓ Geräte entsprechen den aktuellen Sicherheitsbedürfnissen

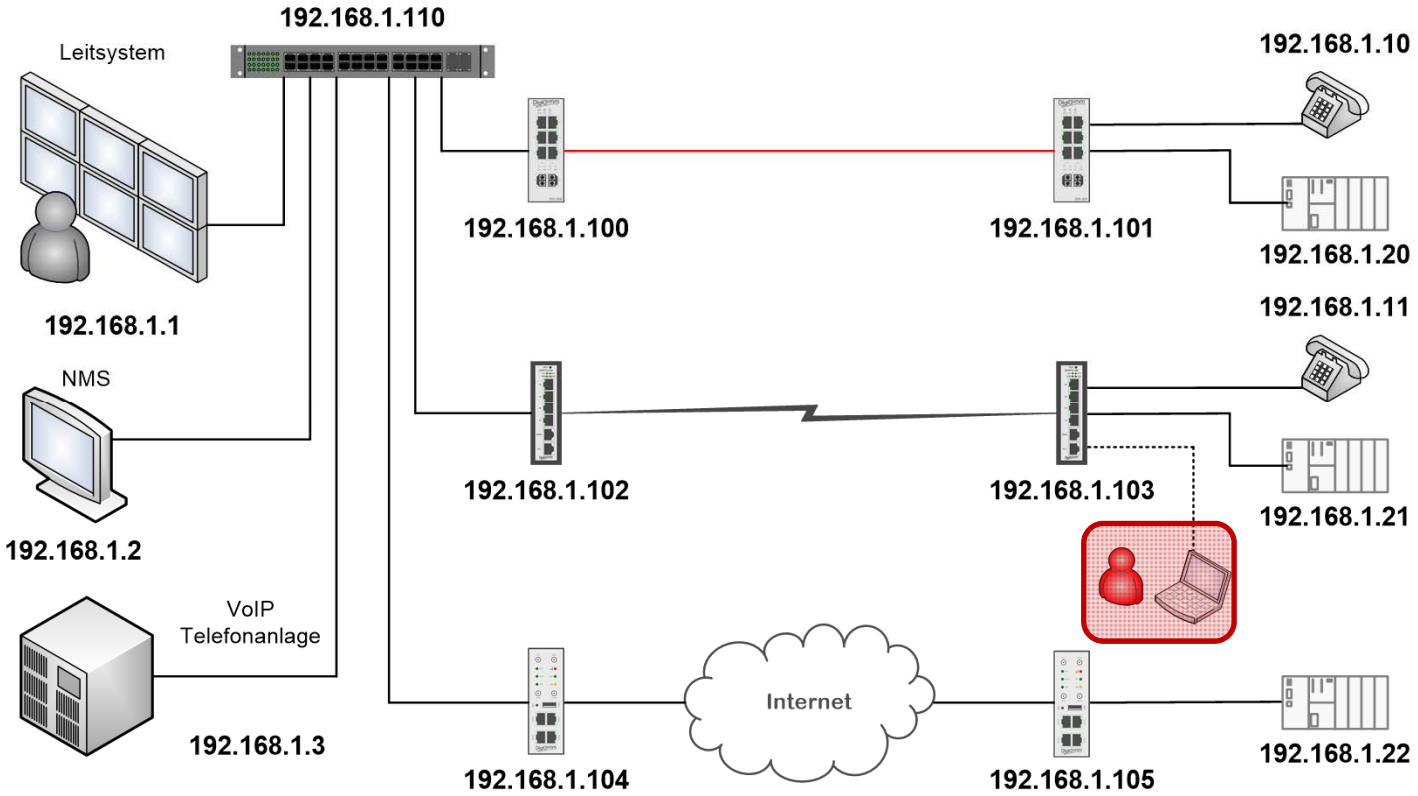
- ? Layer 2 oder 3
- ? Migration von seriell zu Ethernet
- ? Überwachung und Alarmierung

Kommunikationsnetze Anwendungen

Layer – 2 = Bridge / Switch

Kommunikationsnetze Anwendungen

Layer – 2 = Bridge / Switch

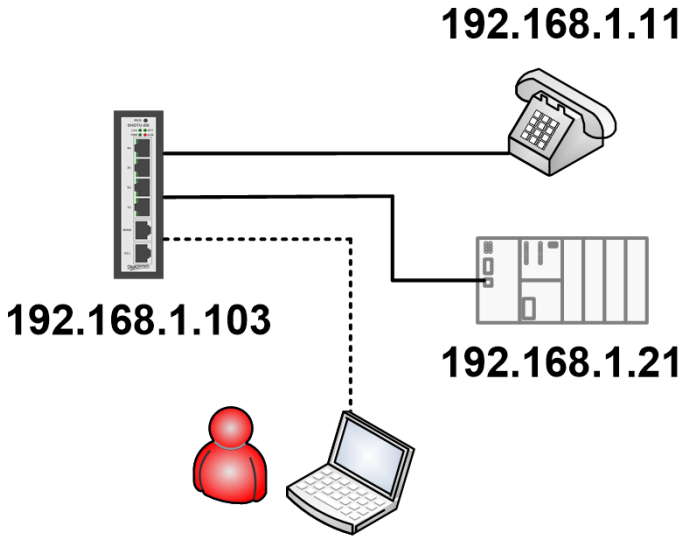


Voraussetzung für Zugriff

- **IP-Adresse**

Kommunikationsnetze Anwendungen

Layer – 2 - Sicherheit



Schutzmaßnahmen

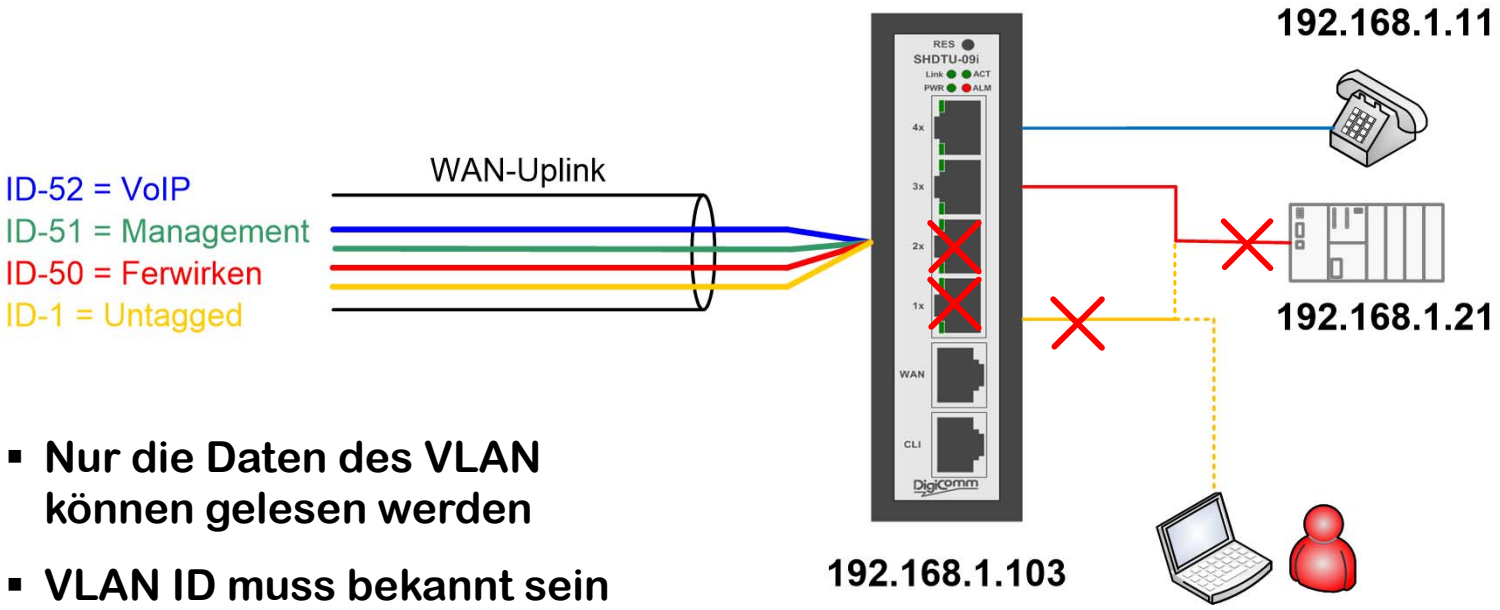
- Nicht genutzte Ports abschalten
- Trennung der Dienste über VLAN
- Port-Control nutzen
- MAC-Filter

Voraussetzung für Zugriff

- IP-Adresse

Kommunikationsnetze Anwendungen

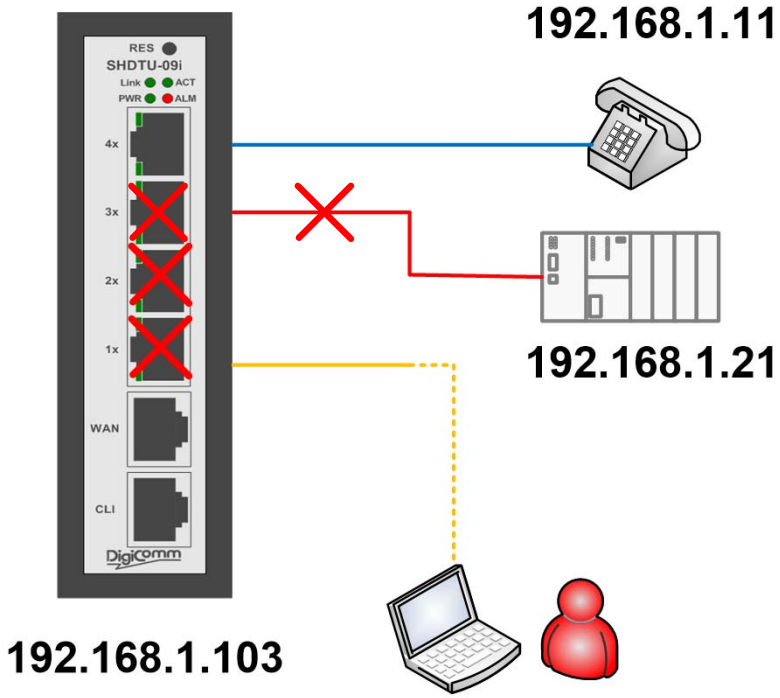
Layer – 2 – Port abschalten & VLAN



- Nur die Daten des VLAN können gelesen werden
- VLAN ID muss bekannt sein um Daten zu lesen

Kommunikationsnetze Anwendungen

Layer – 2 – Port-Control

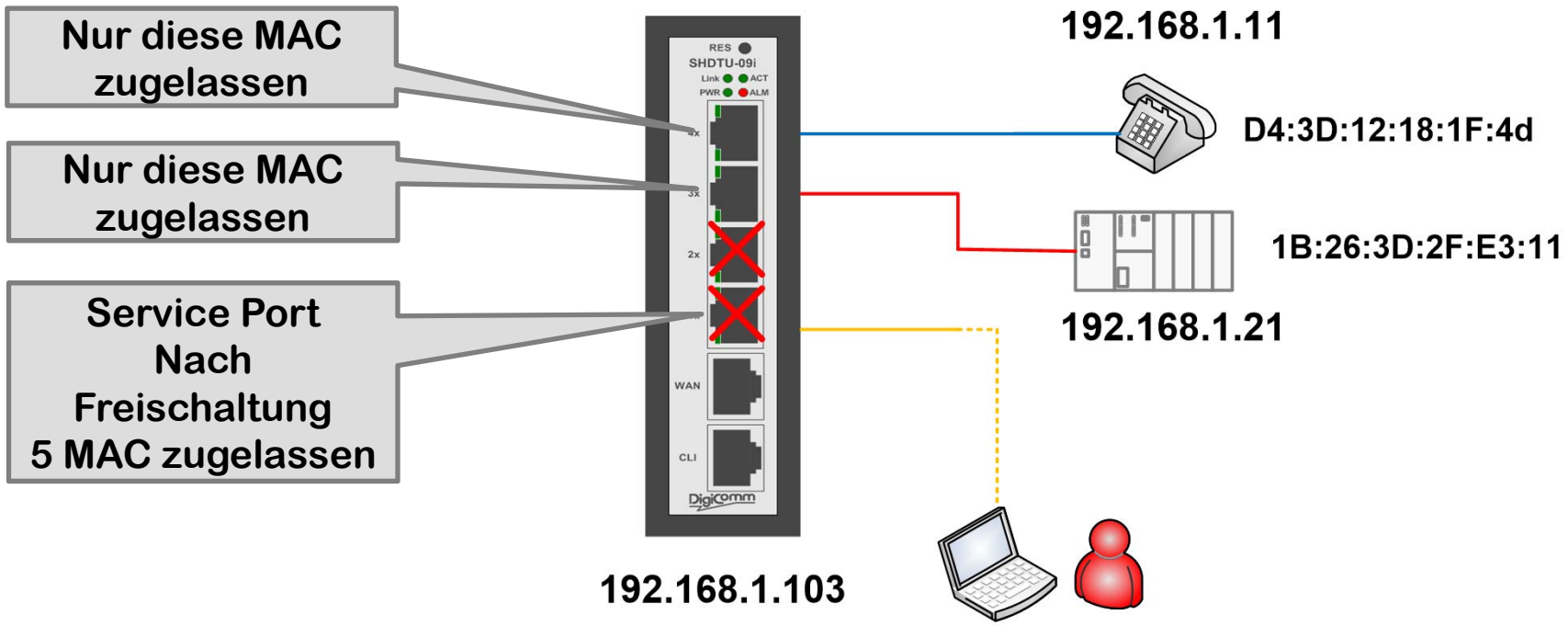


Unterschiedliche Möglichkeiten:

- Standard (verhält sich wie ein normaler Switch)
- Monitor (sendet eine SNMP Nachricht an das Management-System, muss vom Operator quittiert werden)
- Shut down (Port wird abgeschaltet und muss vom Operator freigegeben werden)

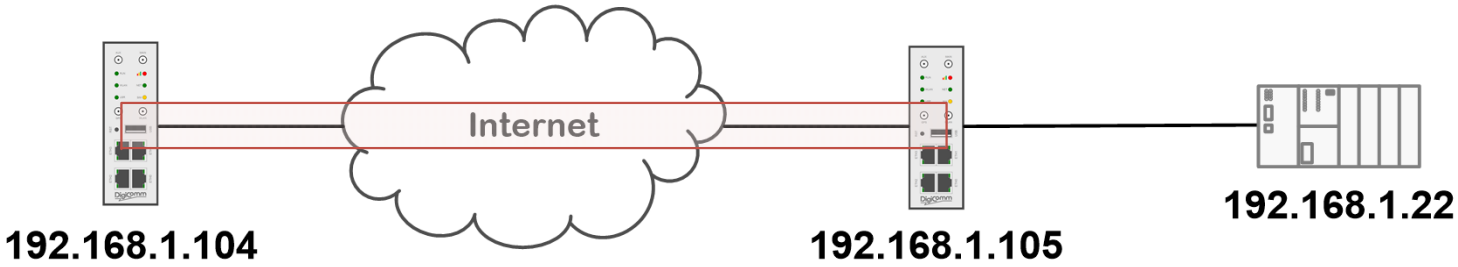
Kommunikationsnetze Anwendungen

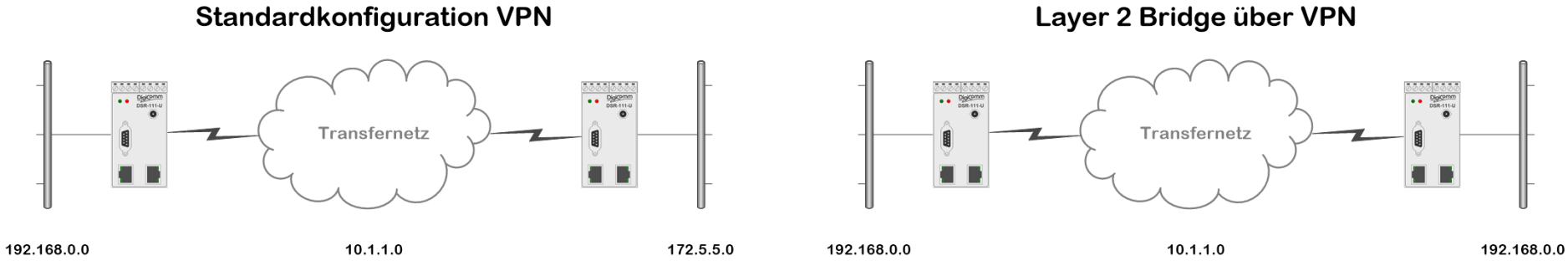
Layer – 2 – MAC-Filter



Kommunikationsnetze Anwendungen

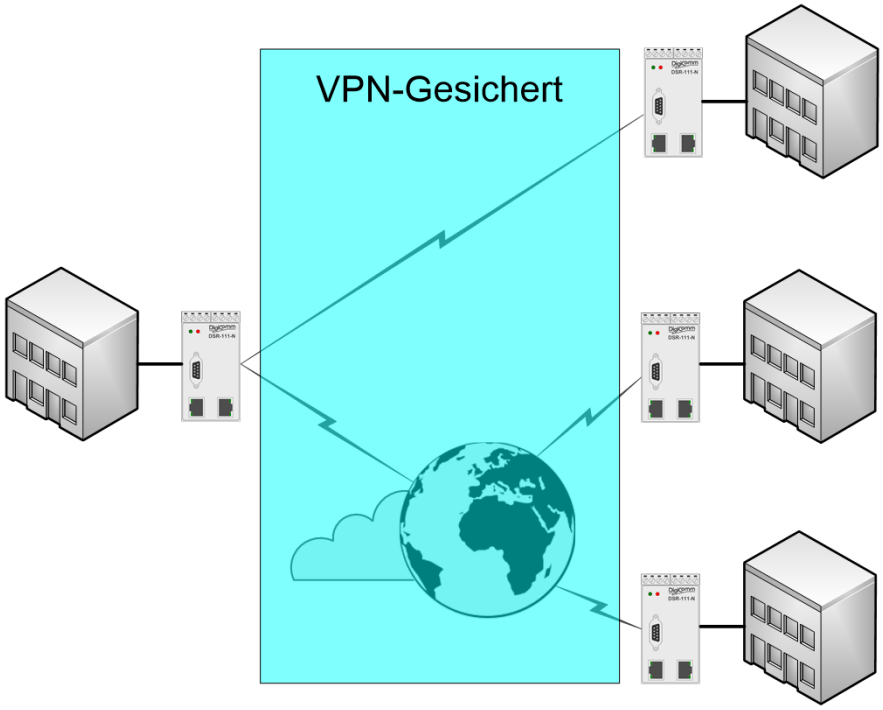
Layer – 2 – VPN-Bridge

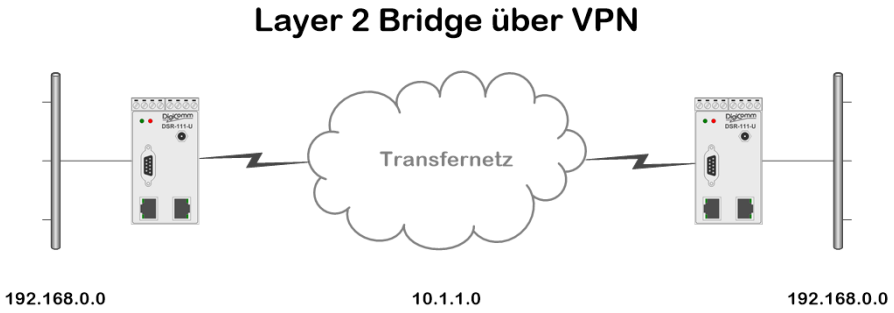


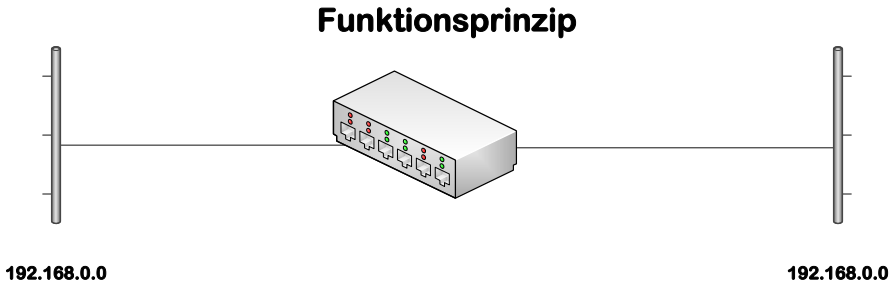


Kommunikationsnetze Anwendungen

Layer – 2 – VPN-Bridge





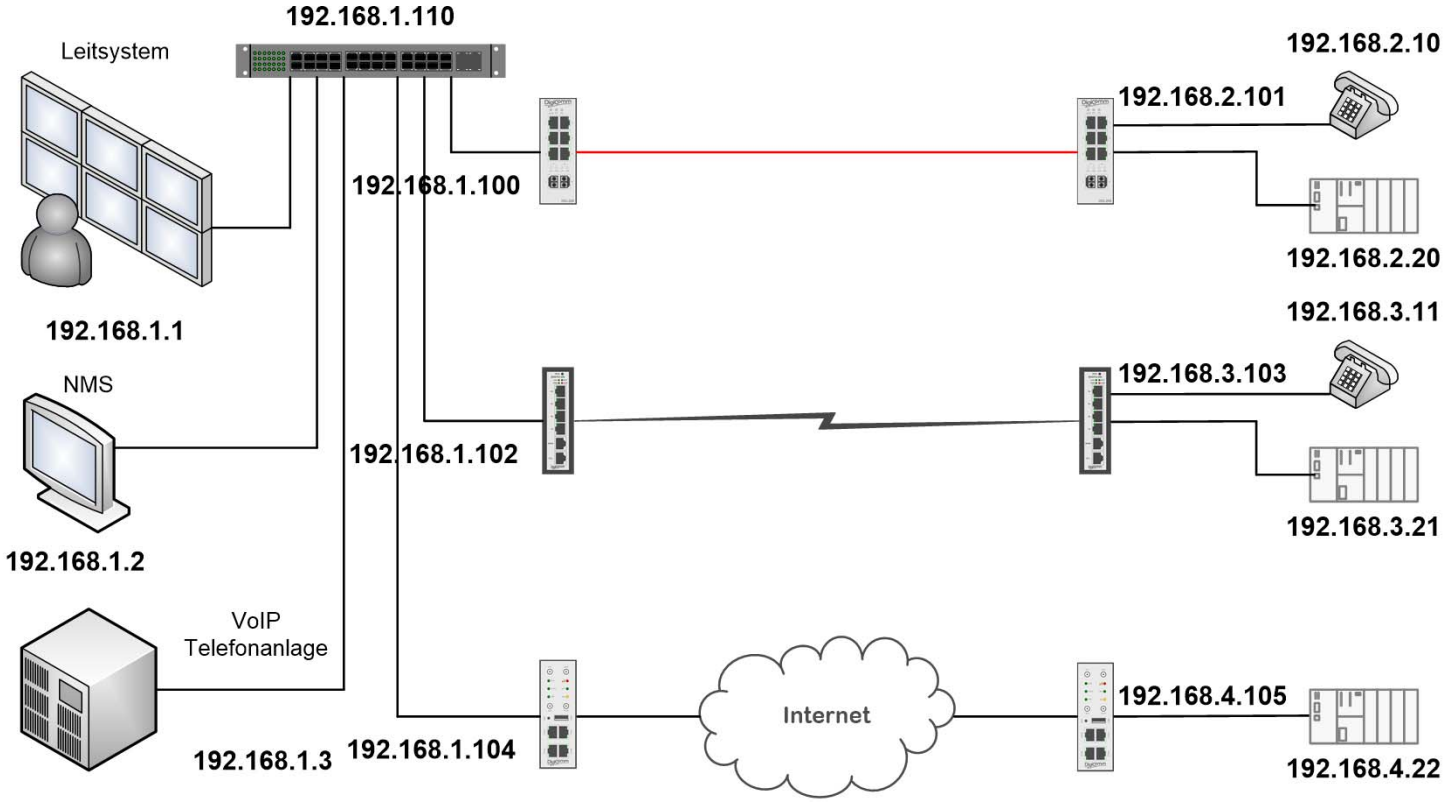


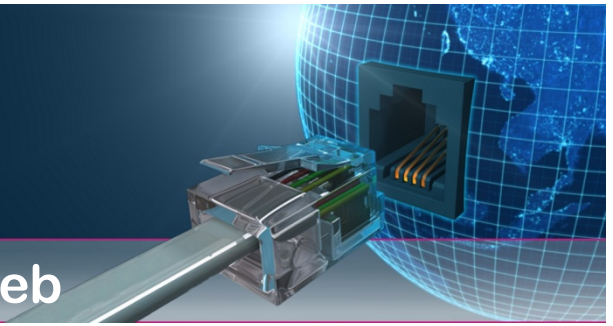
Kommunikationsnetze Anwendungen

Layer – 3 = Routing

Kommunikationsnetze Anwendungen

Layer – 3 = Routing

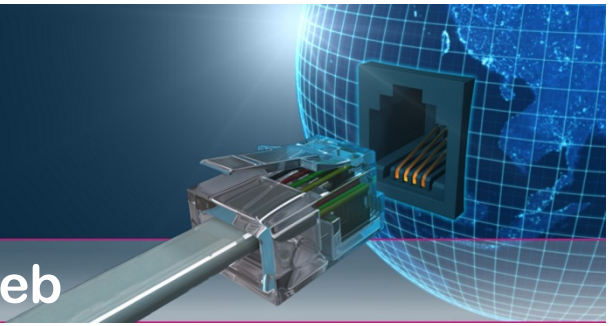




Kommunikationsnetze Anwendungen

Layer – 3 = Routing

- Ein Router ist mit mindestens zwei unterschiedlichen Netzwerken verbunden
- Über die Routing-Tabelle entscheidet ein Router, welchen Weg ein Datenpaket nimmt
- Es ist ein dynamisches Verfahren, das Ausfälle und Engpässe ohne den Eingriff eines Administrators berücksichtigen kann
- Ein Router verschlüsselt Übertragung und verhindert Angriffe von außen und nach innen



Kommunikationsnetze Anwendungen

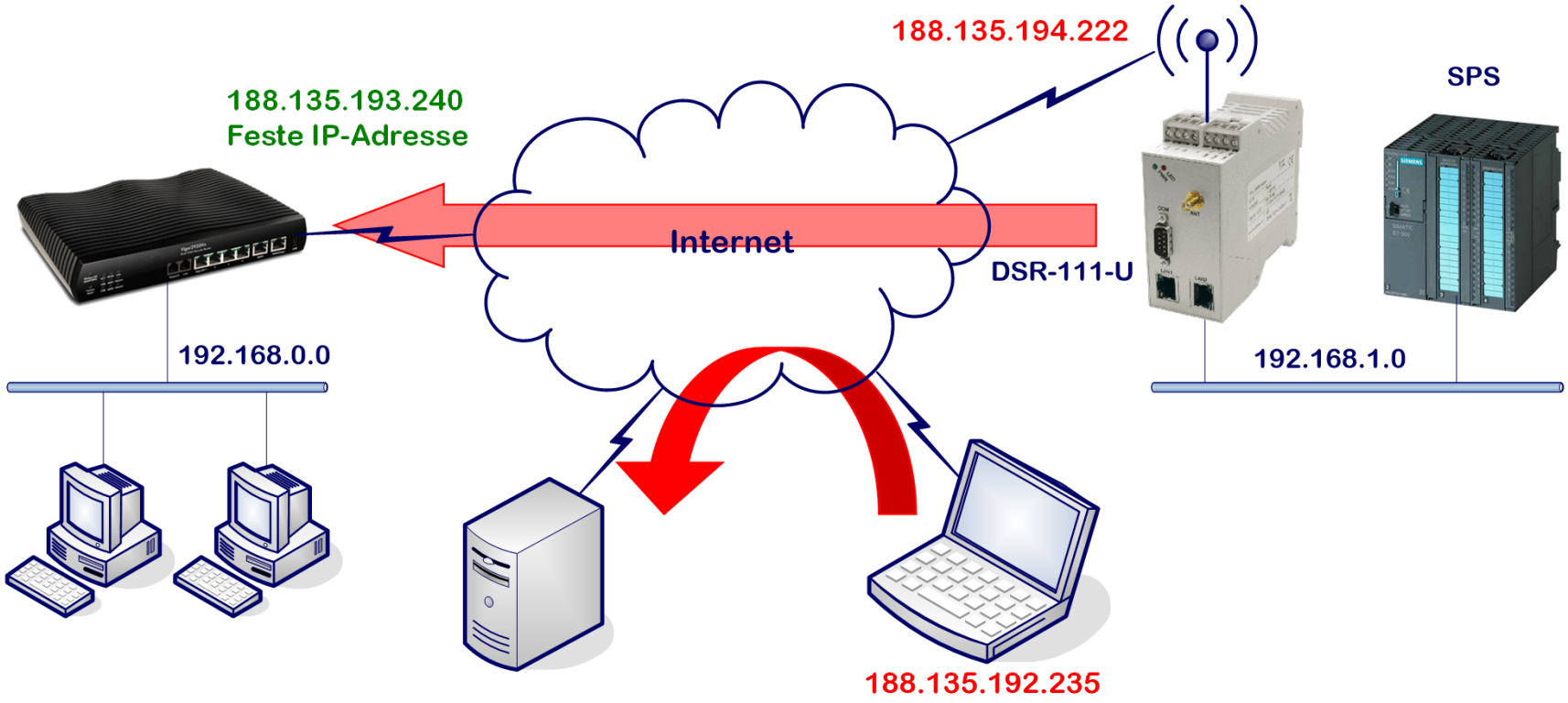
Layer – 3 = Routing

Die Aufgabe eines Routers lässt sich in 4 Schritte einteilen:

- **Ermittlung der verfügbaren Routen**
- **Auswahl der geeignetsten Route**
- **Herstellen der Verbindung**
- **Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung)**

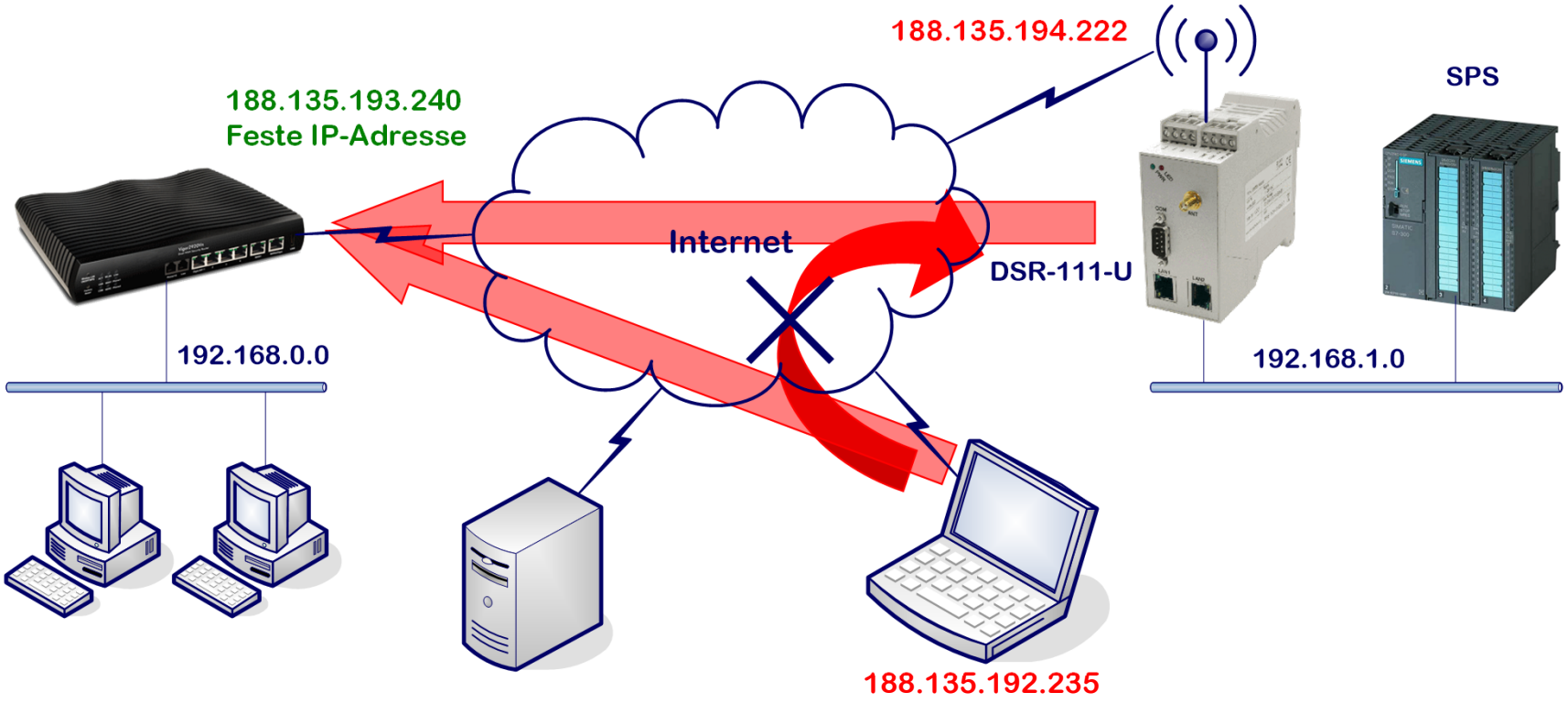
Kommunikationsnetze Anwendungen

Layer – 3 = Routing über öffentliche Netze



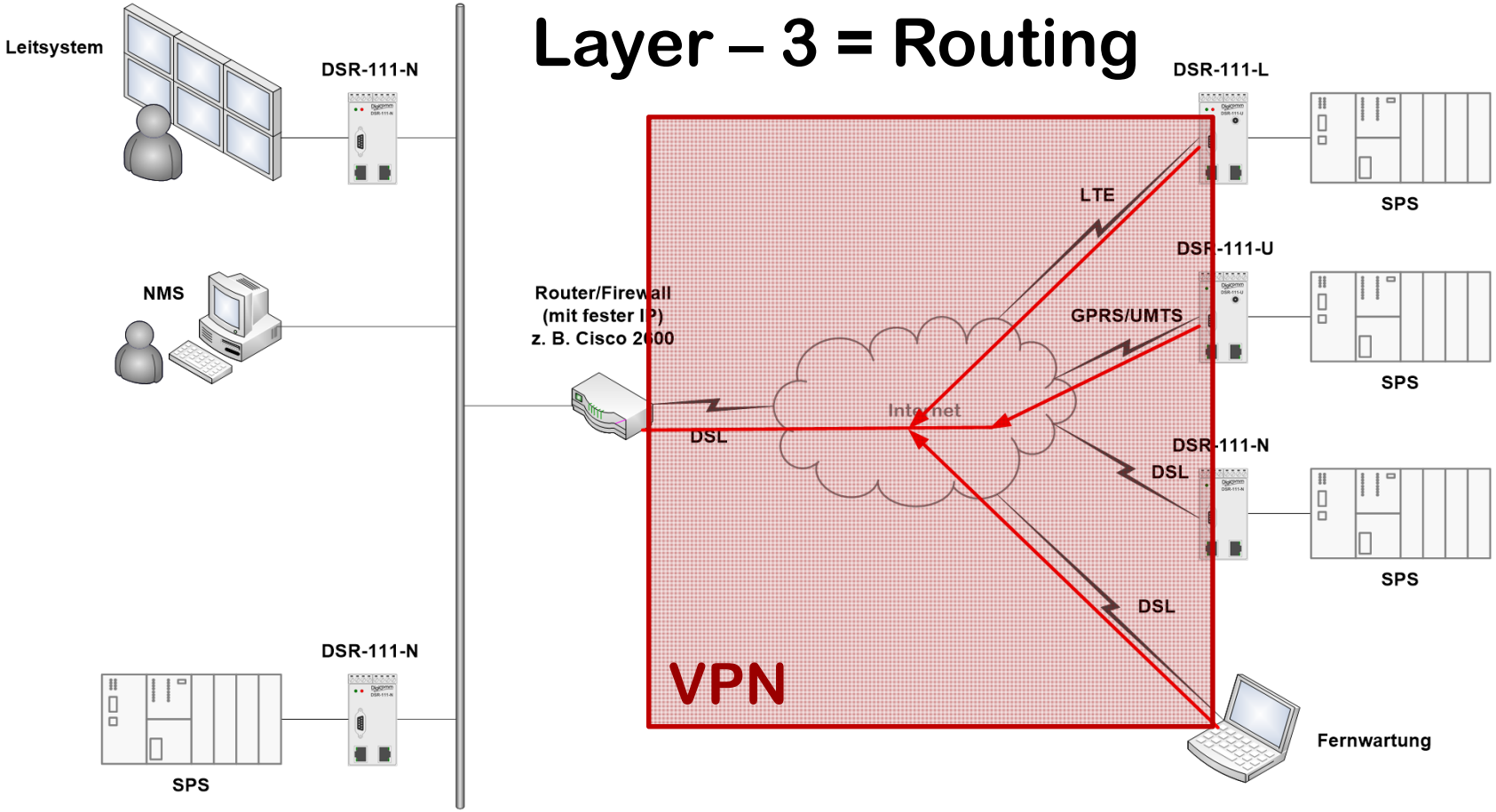
Kommunikationsnetze Anwendungen

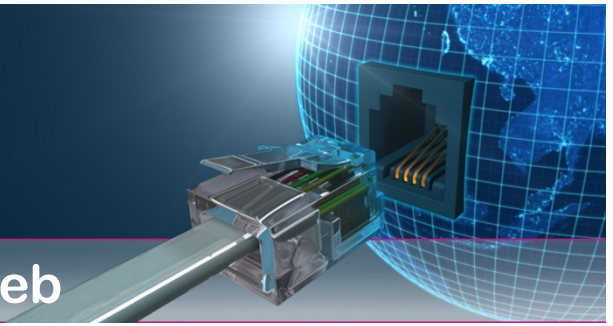
Layer – 3 = Routing über öffentliche Netze



Kommunikationsnetze Anwendungen

Layer – 3 = Routing

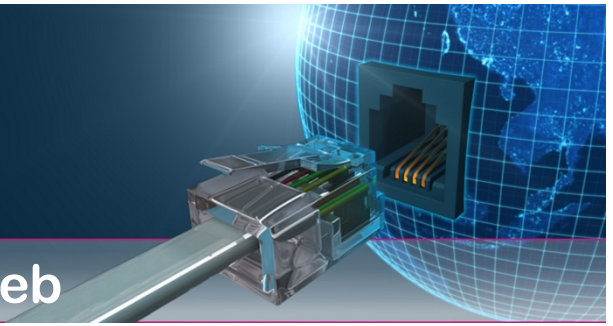




Kommunikationsnetze Anwendungen

Sicherheit durch VPN Tunnel

- Geschützter Datenverkehr durch das ungeschützte Internet
- Protokollunabhängig (es muss lediglich ein IP-Protokoll sein)
- geschützte Portnummern (werden erst nach dem Tunnel aktiv)
- Authentifizierung der Verbindungspartner
- Client- Server-Prinzip (Private-IP beim Client möglich)
- Verbindung zwischen zwei privaten IP-Adressen oder privaten Netzwerken über das Internet



Kommunikationsnetze Anwendungen

Sicherheit durch VPN Tunnel

Abhörsicher:

- **Ein Angreifer kann nur erkennen, dass Daten zwischen zwei Internetteilnehmern ausgetauscht werden, er sieht nicht das tatsächliche Ziel und kann den Dateninhalt nicht lesen**

Manipulationssicher:

- **Ein Angreifer kann den Dateninhalt der ausgetauschten Telegramme nicht verändern, da er das Zertifikat und damit die Verschlüsselung nicht kennt**

Kommunikationsnetze Anwendungen

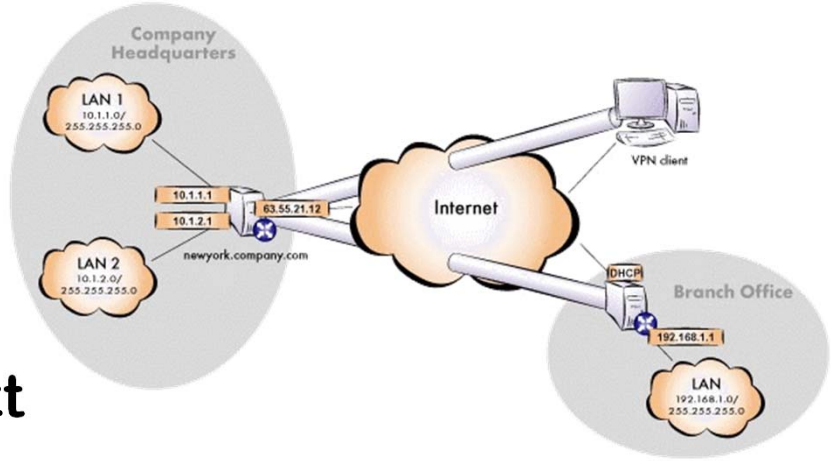
Sicherheit durch VPN Tunnel

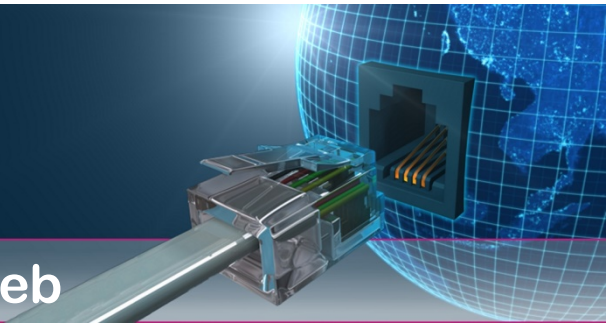
Abgesicherte Einwahl:

Authentifizierung:

Ein Angreifer kann sich nicht anstelle eines berechtigten Users einwählen, da er nicht im Besitz des gültigen Zertifikates ist

Der Server kann auch nicht durch einen manipulierten Server ersetzt werden (man in the middle)





Kommunikationsnetze Anwendungen

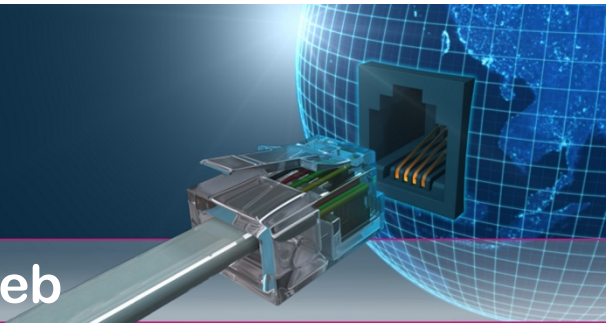
Sicherheit durch VPN Tunnel = Protokolle

- **Point-to-Point-Tunneling-Protocol (PPTP):** PPTP ermöglicht es, Netzwerkverkehr verschiedenster Protokolle zu verschlüsseln und dann mit einem IP-Header zu kapseln und so über ein IP-Netzwerk (zum Beispiel dem Internet) zu übertragen.

- **Layer-Two-Tunneling-Protocol (L2TP):** L2TP ermöglicht die Verschlüsselung und Versendung verschiedenster Netzwerkprotokolle über jedes Medium, das Point-to-Point-Datagram-Delivery unterstützt (zum Beispiel IP, X.25, Frame Relay oder ATM).

- **IPSec-Tunnelmodus:** Der IPSec-Tunnelmodus ermöglicht es, IP-Pakete zu verschlüsseln, diese dann in einen IP-Header zu Kapseln und dann zum Beispiel über ein öffentliches IP-Netzwerk zu versenden.

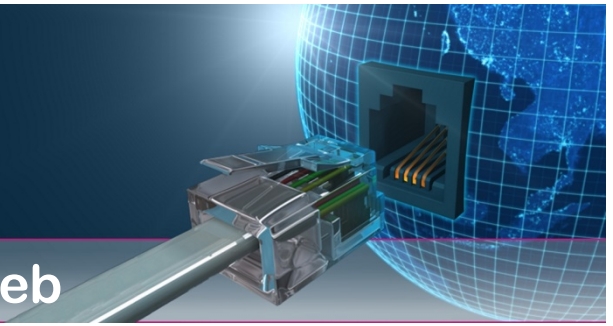
- **Open VPN:** OpenSource Programm zur Herstellung eines VPN's. Es verwendet wahlweise UDP oder TCP Protokoll, dieVerschlüsselung erfolgt mit OpenSSL.



Kommunikationsnetze Anwendungen

Sicherheit durch VPN Tunnel = OpenVPN

- Offenes System und Standard
- Hersteller unabhängig
- Ideales Handling für Industrie
- Subnet Kopplung
- Client to Client Mode auch für Subnets und extrem große Anzahl Clients



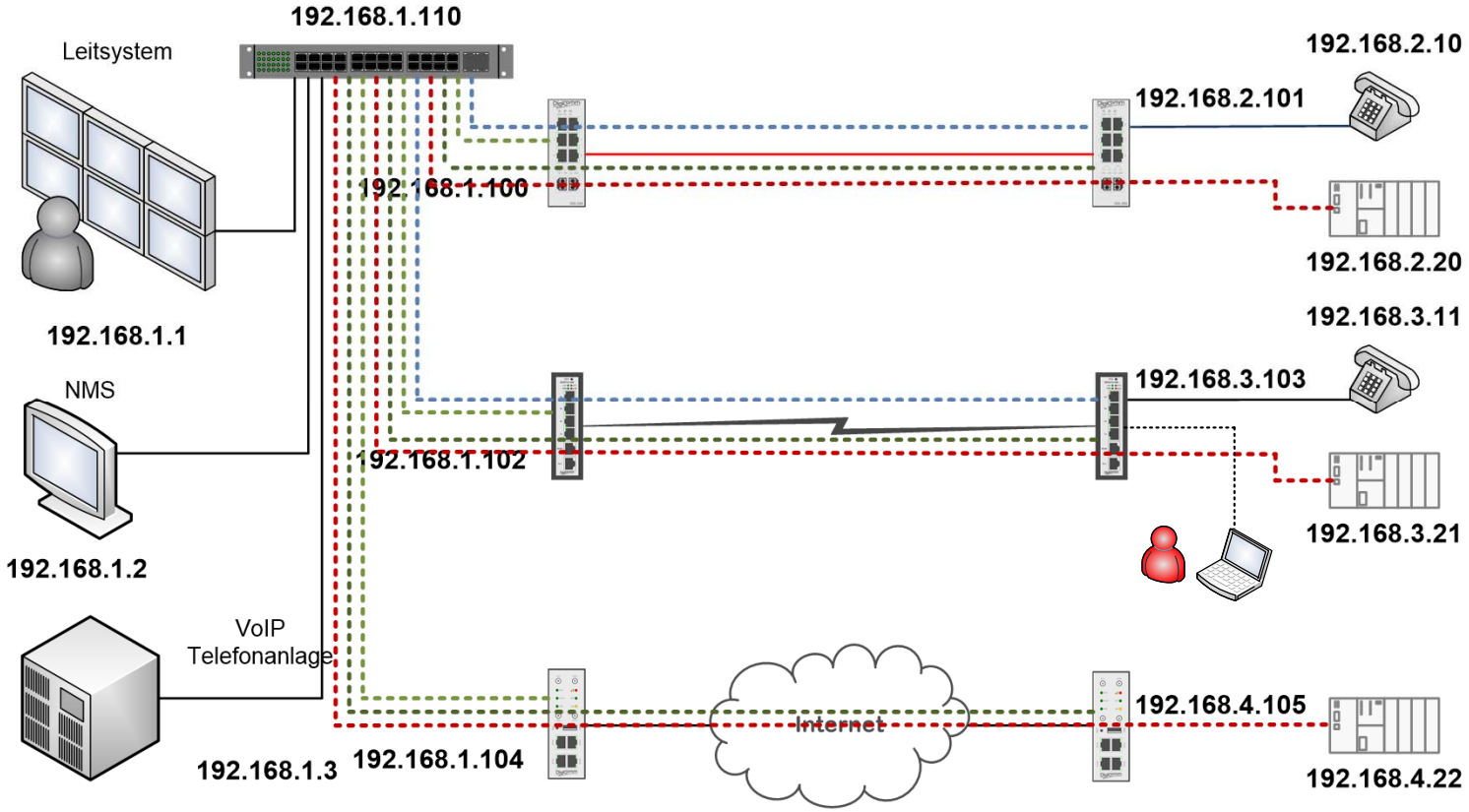
Kommunikationsnetze Anwendungen

Sicherheit durch VPN Tunnel = IPsec

- Komplex in der Handhabung
- Kompliziertes Subnetting
- Sicherheit vergleichbar mit Open VPN
- Gutes VLAN Handling
- Verschiedene Dialekte
- Wird von vielen Herstellern unterstützt

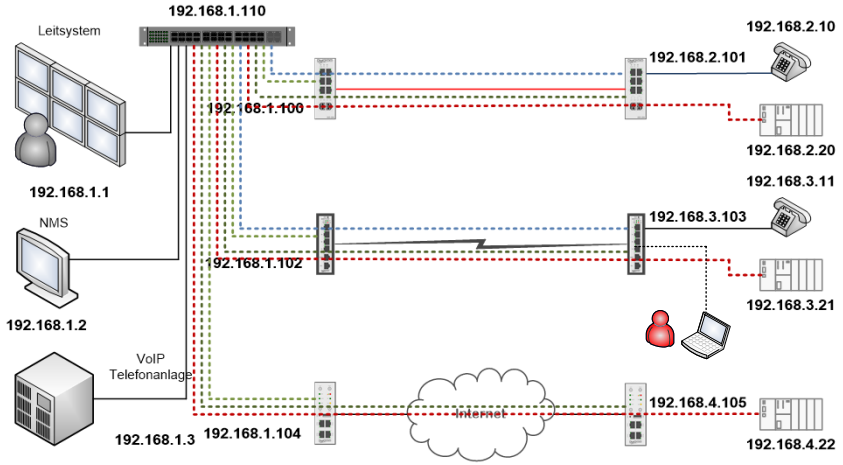
Kommunikationsnetze Anwendungen

Layer – 3 = Routing & VPN



Kommunikationsnetze Anwendungen

Layer – 3 = Routing & VPN



Voraussetzung für Zugriff

- IP-Adresse, Standardgateway & Subnetzmaske
- VPN-Zertifikat & Username & Passwort

Schutzmaßnahmen

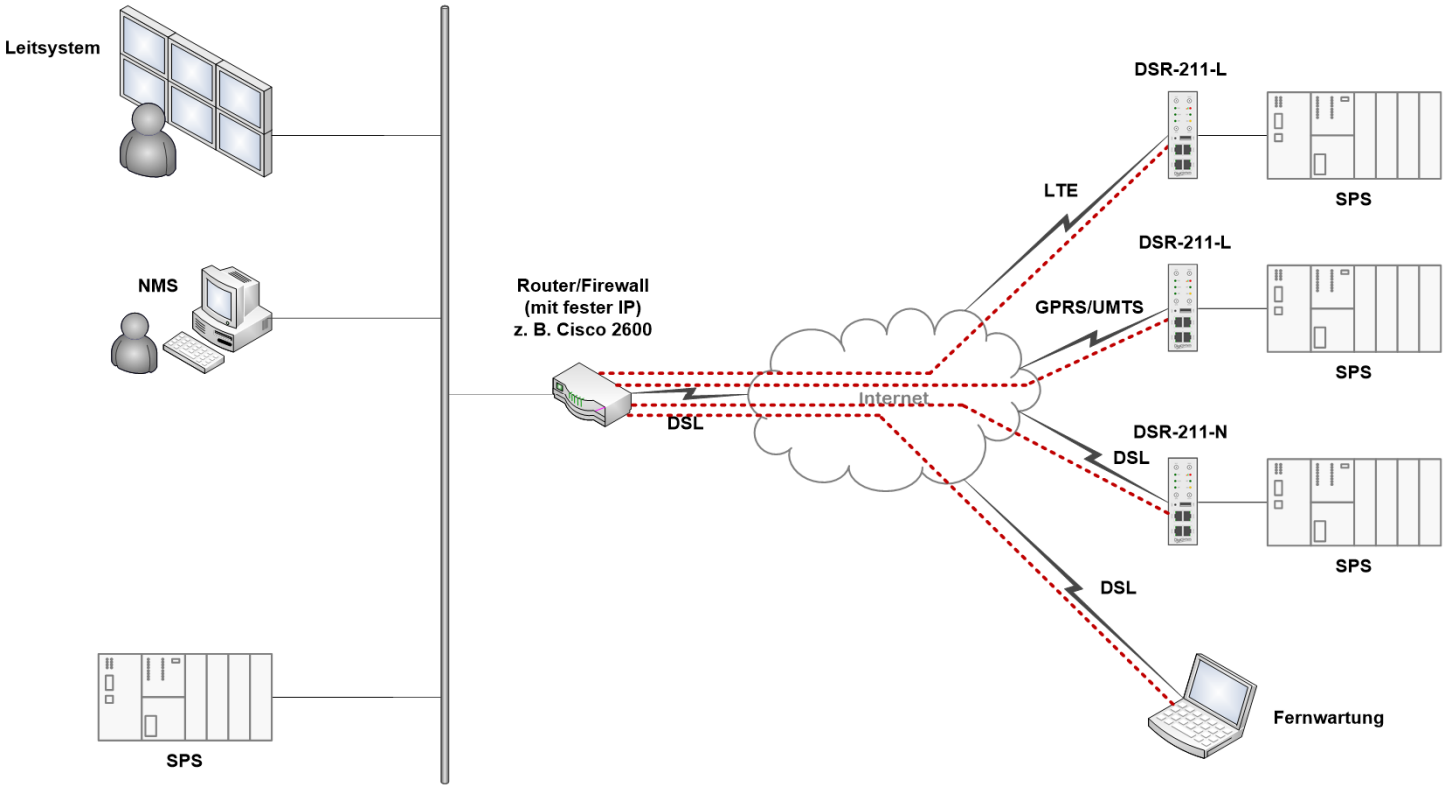
- Nicht genutzte Ports abschalten
- Trennung der Dienste über VPN
- Port-Control nutzen
- MAC- und IP-Filter
- TCP-Ports filtern = nur bestimmte Anwendungen zulassen

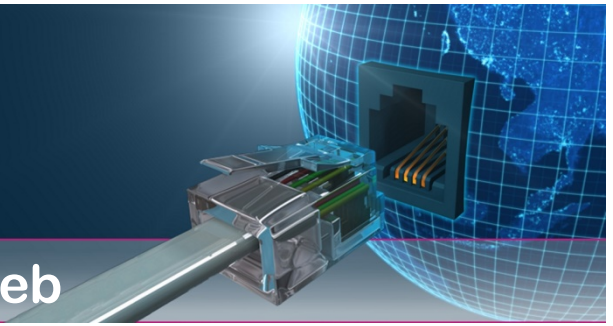
Kommunikationsnetze Anwendungen

VSS-01 – Konzept der DigiComm

Kommunikationsnetze Anwendungen

VSS-01 – Konzept der DigiComm





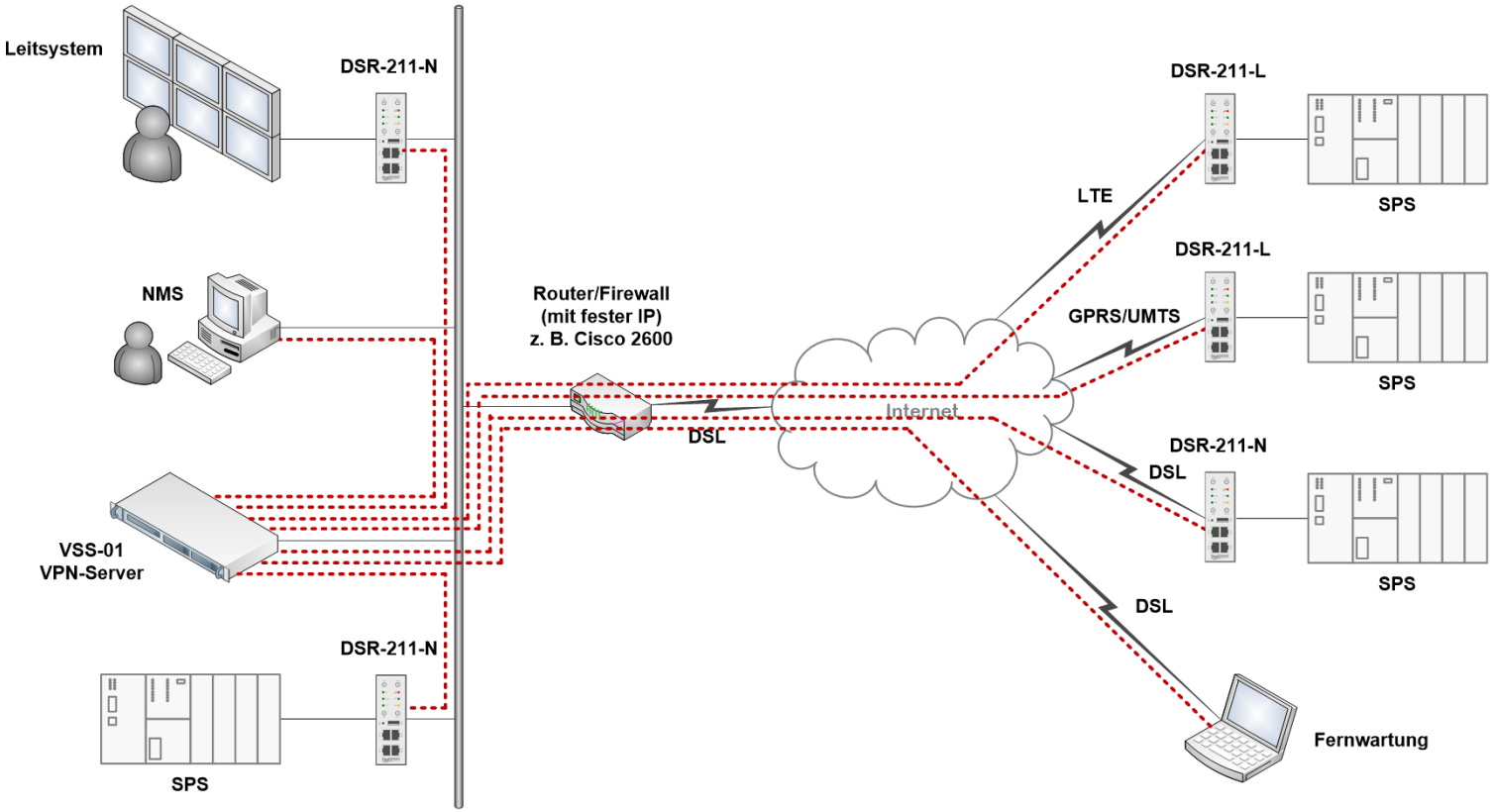
Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01

- Unterschiedliche Größen von 50 bis 2.000 VPN-Verbindungen
- Mit dem Anlegen eines Teilnehmernetzes werden im VSS die Konfigurationsdateien für den Router erzeugt, es ist keine weitere Konfiguration notwendig
- Hohe Sicherheit durch VPN-Verbindungen verbunden mit einer entsprechenden Firewall im VSS und Router
- Gruppen- und Teilnehmerverwaltung über die Web-Oberfläche des VSS

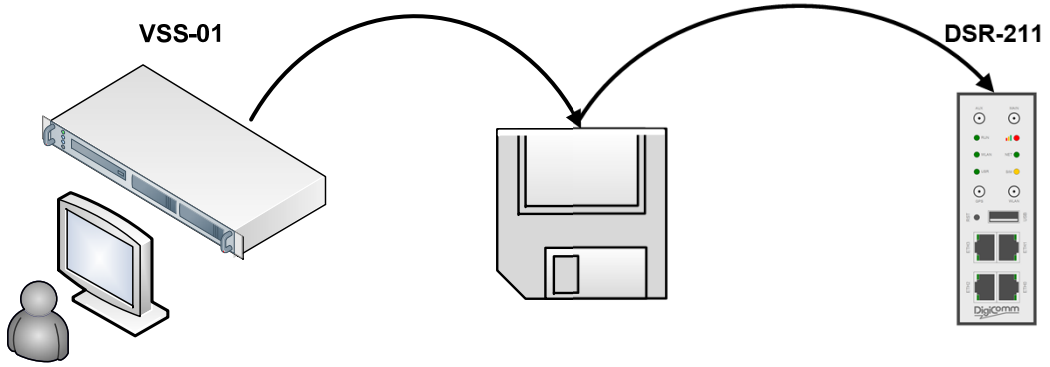
Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01



Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01



1. Schritt
Anlegen einer neuen Station im VSS

2. Schritt
Ausgabe der Konfigdatei für den DSR per Mail oder Download

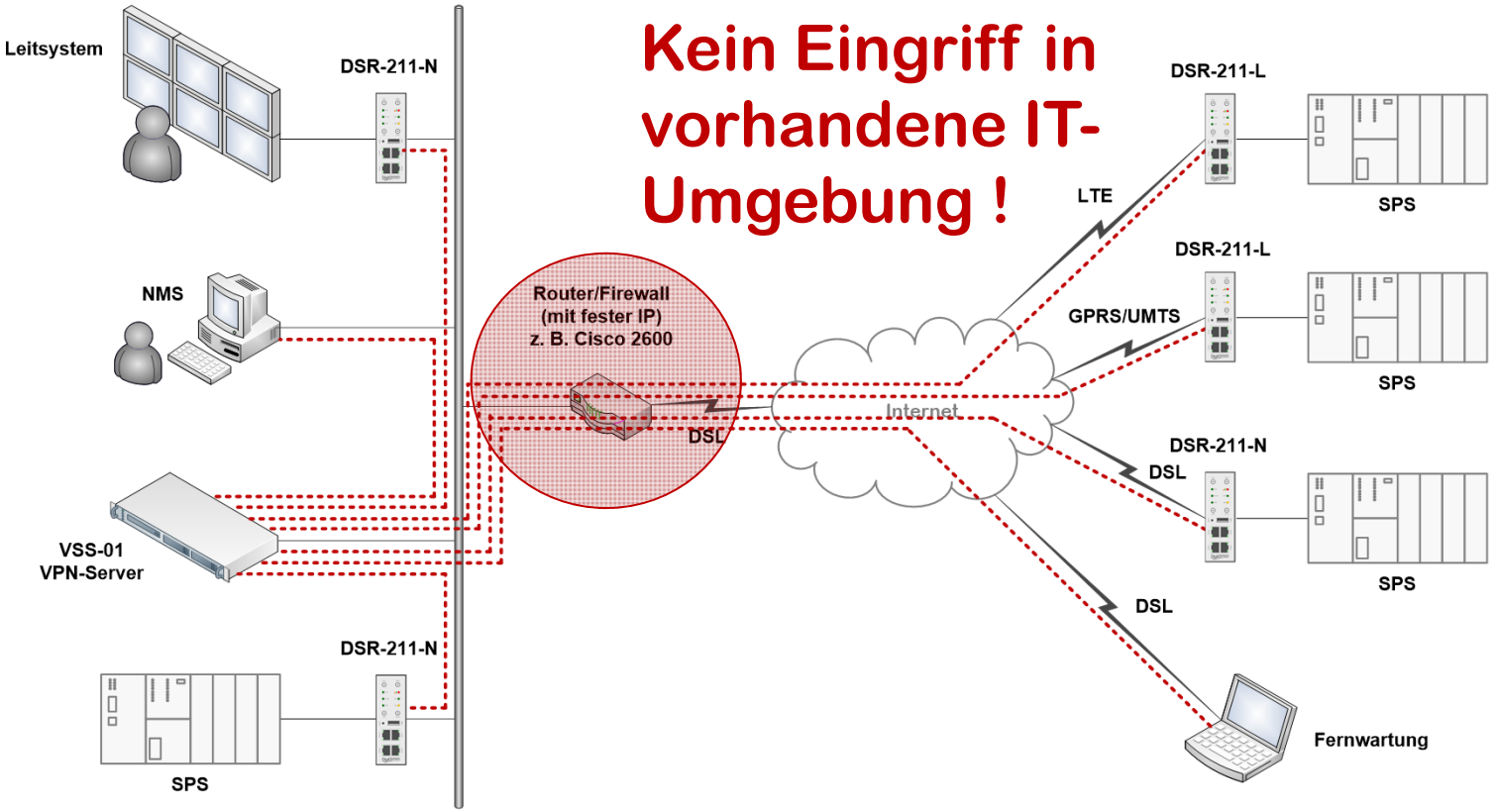
3. Schritt
Einspielen in DSR

FERTIG !

Einfache Konfiguration !

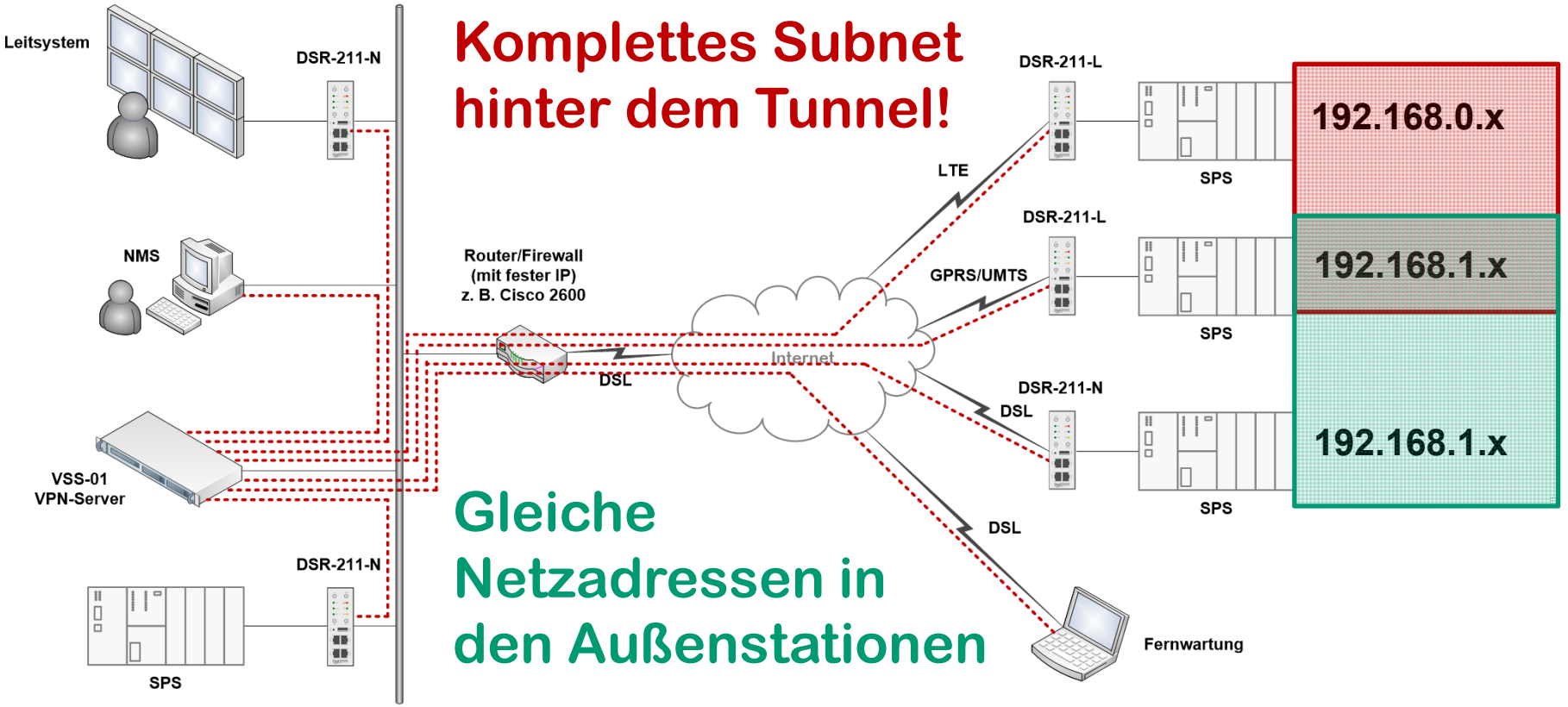
Kommunikationsnetze Anwendungen

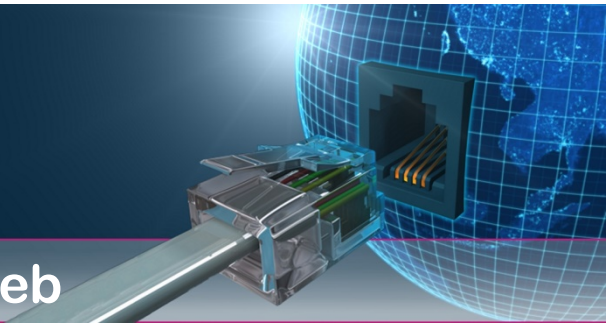
VSS-01 – Security Server VSS-01



Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01





Kommunikationsnetze Anwendungen

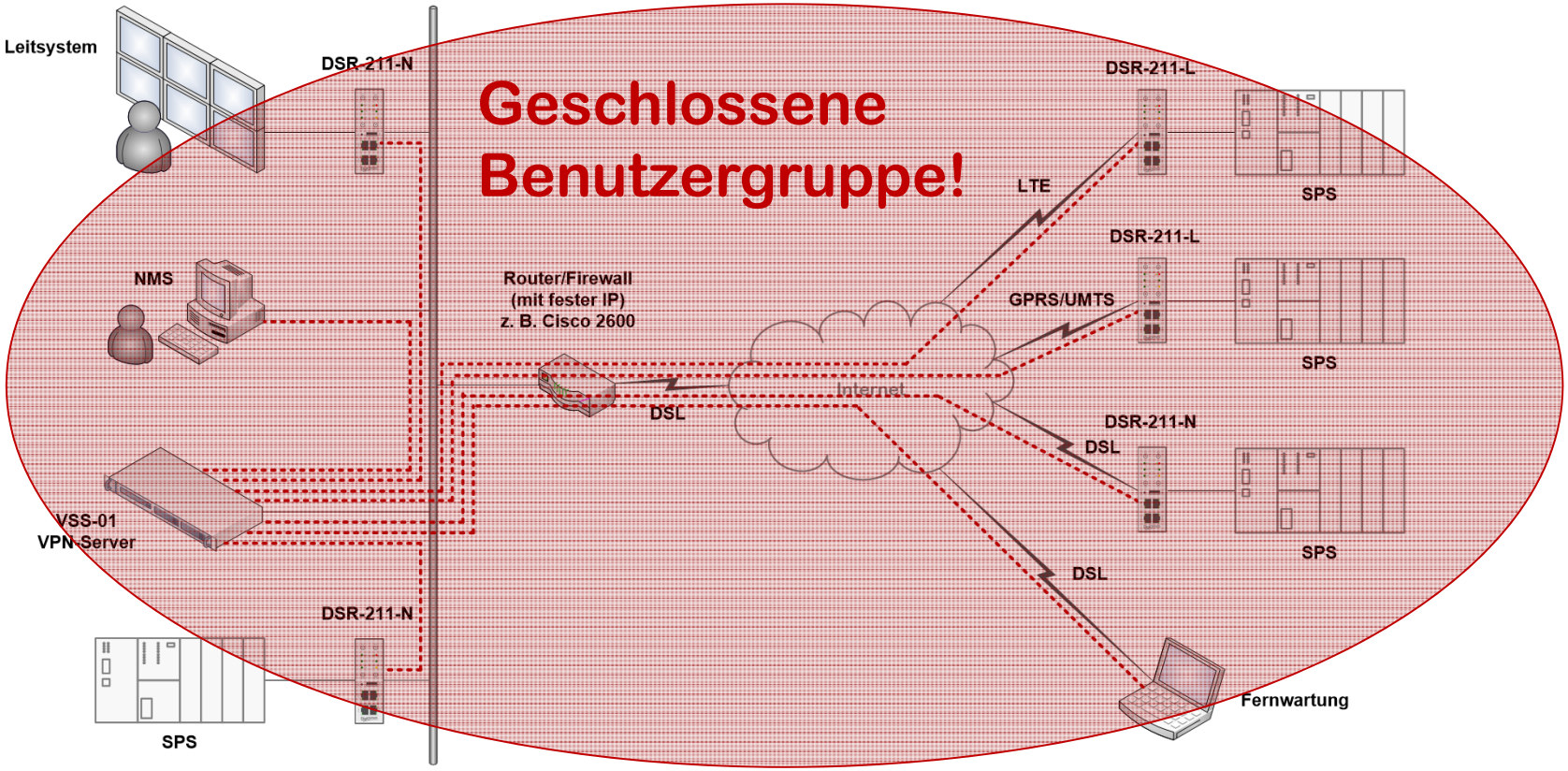
VSS-01 – Security Server VSS-01

Vorteile der SUBNET-Kopplung

- Einfache Inbetriebnahme durch Pingtest zum Router und zu jedem einzelnen Kommunikationspartner des Subnet
- Wenn die Kommunikation zum Router funktioniert, funktioniert auch das ganze Subnet
- Erweiterungsmöglichkeit für später hinzukommende Geräte des Subnets, ohne neue Inbetriebnahme
- Subnetkopplung arbeitet auf Schicht3-Ebene, daher sind alle auf IP basierenden Protokolle anwendbar (TCP, UDP, ICMP…)

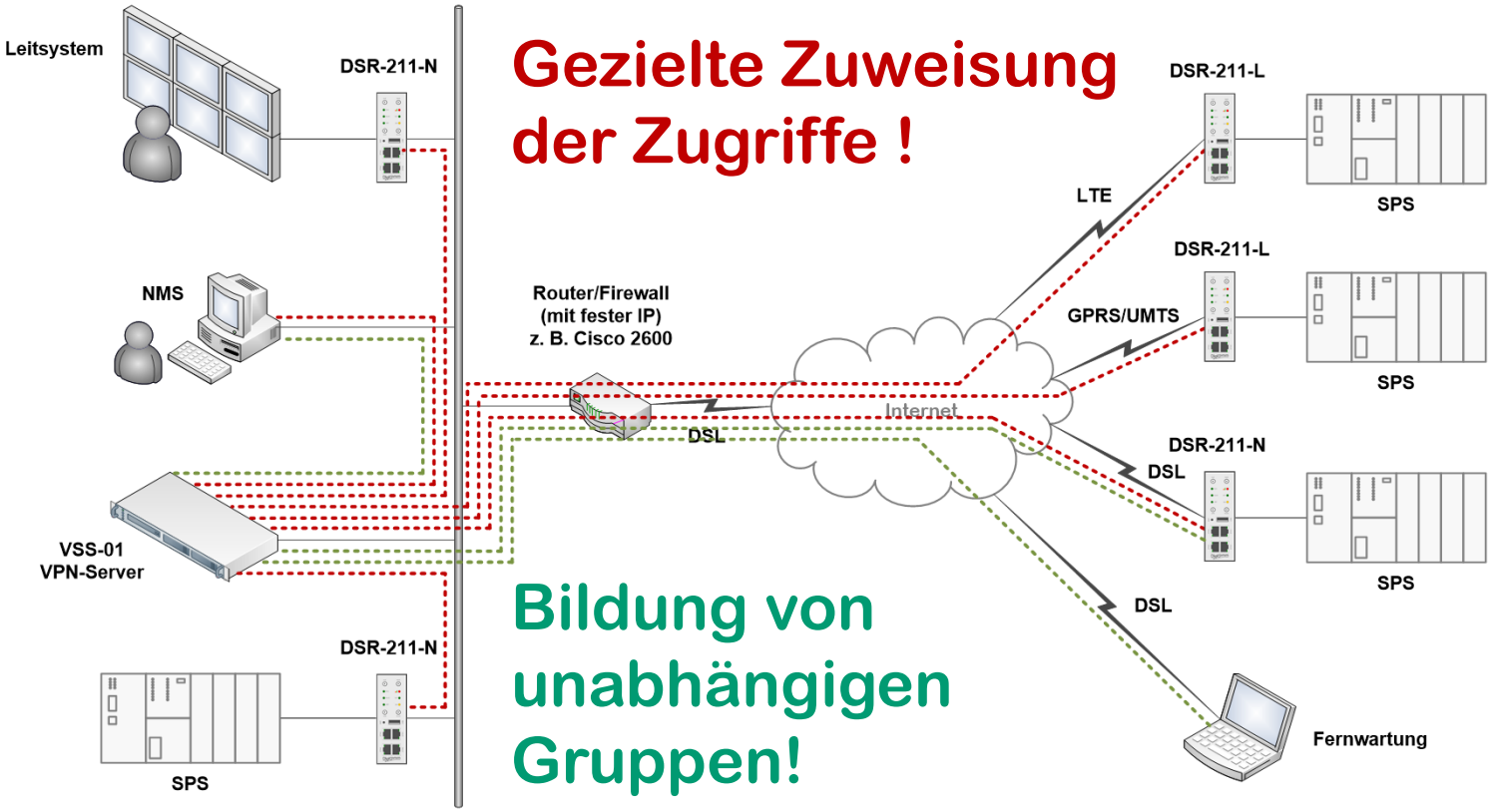
Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01



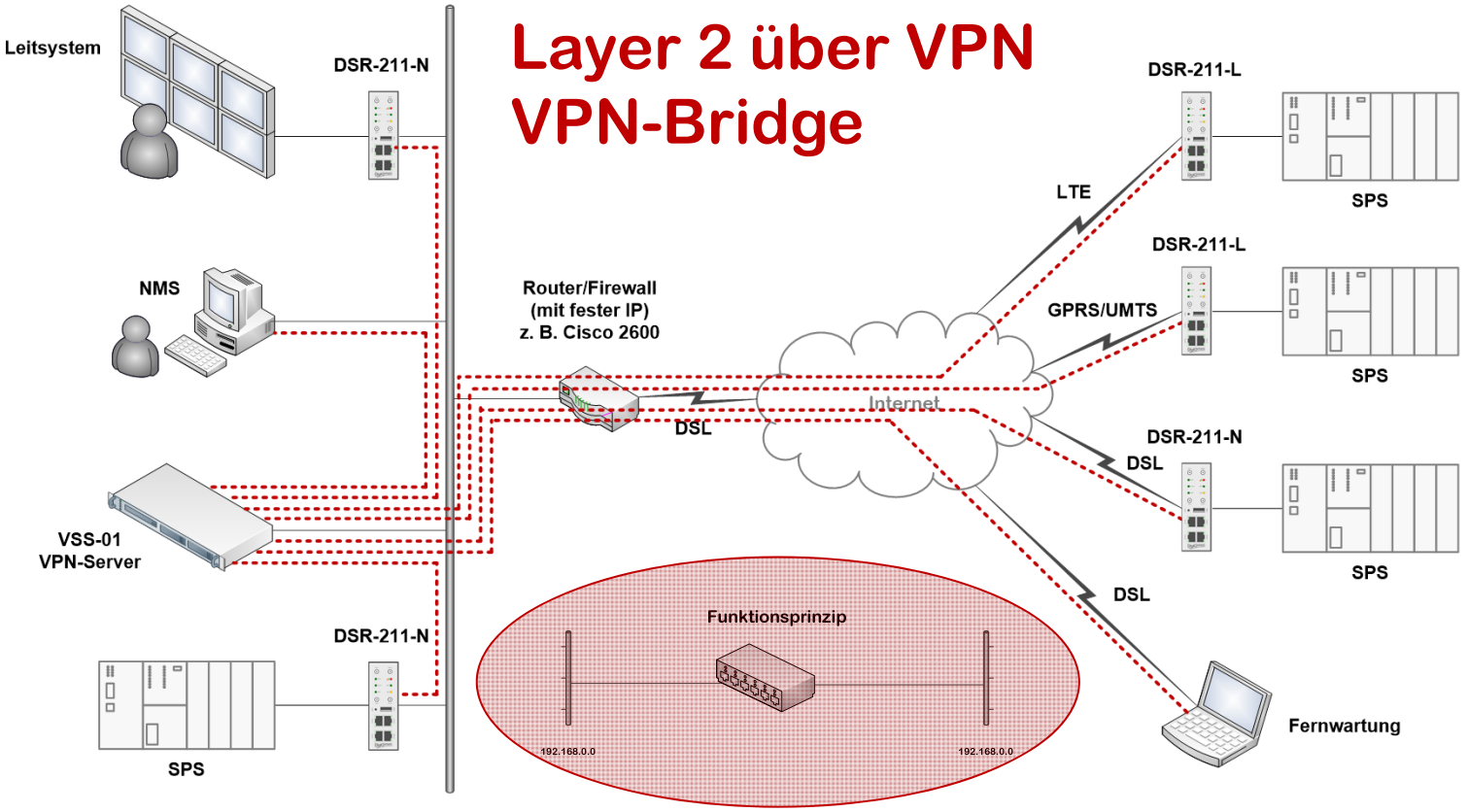
Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01



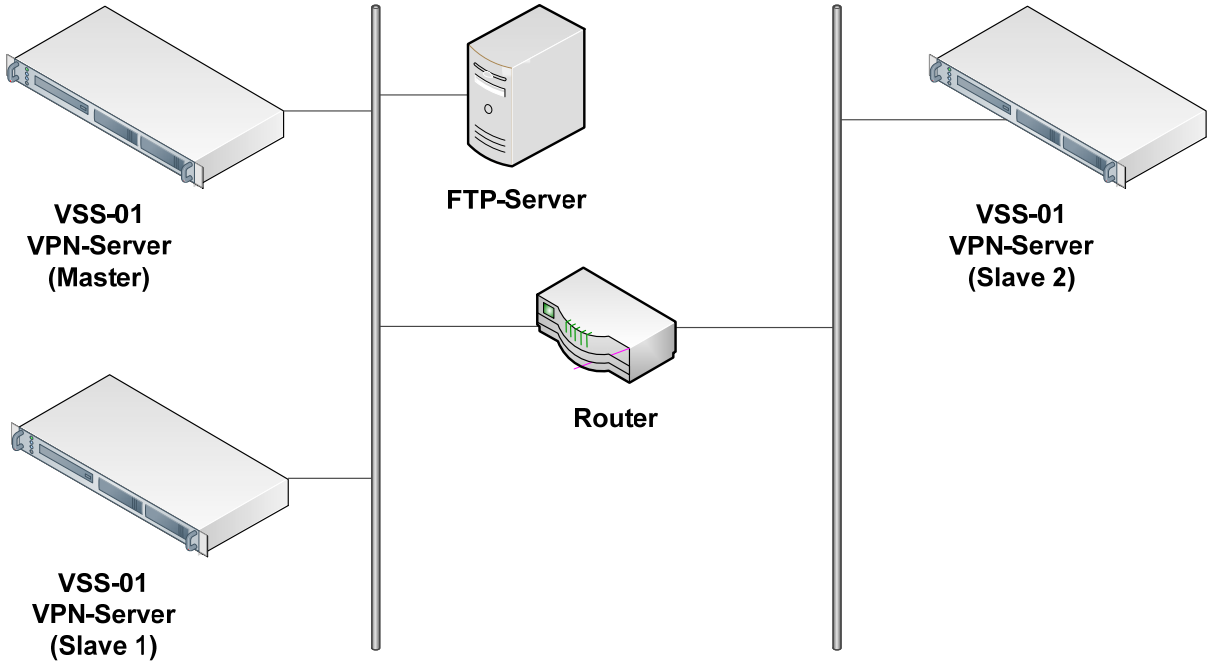
Kommunikationsnetze Anwendungen

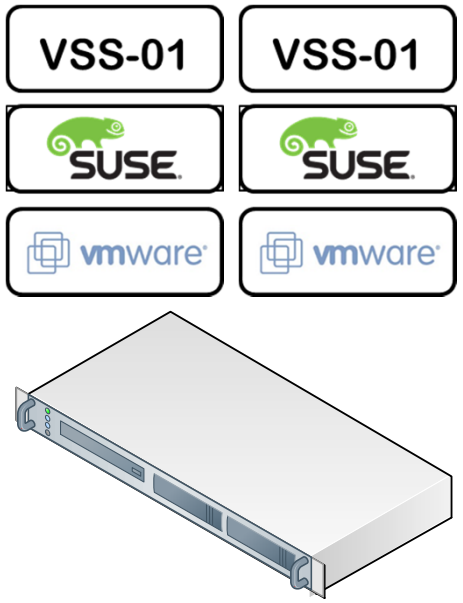
VSS-01 – Security Server VSS-01



Kommunikationsnetze Anwendungen

VSS-01 – Security Server VSS-01 - Redundanz



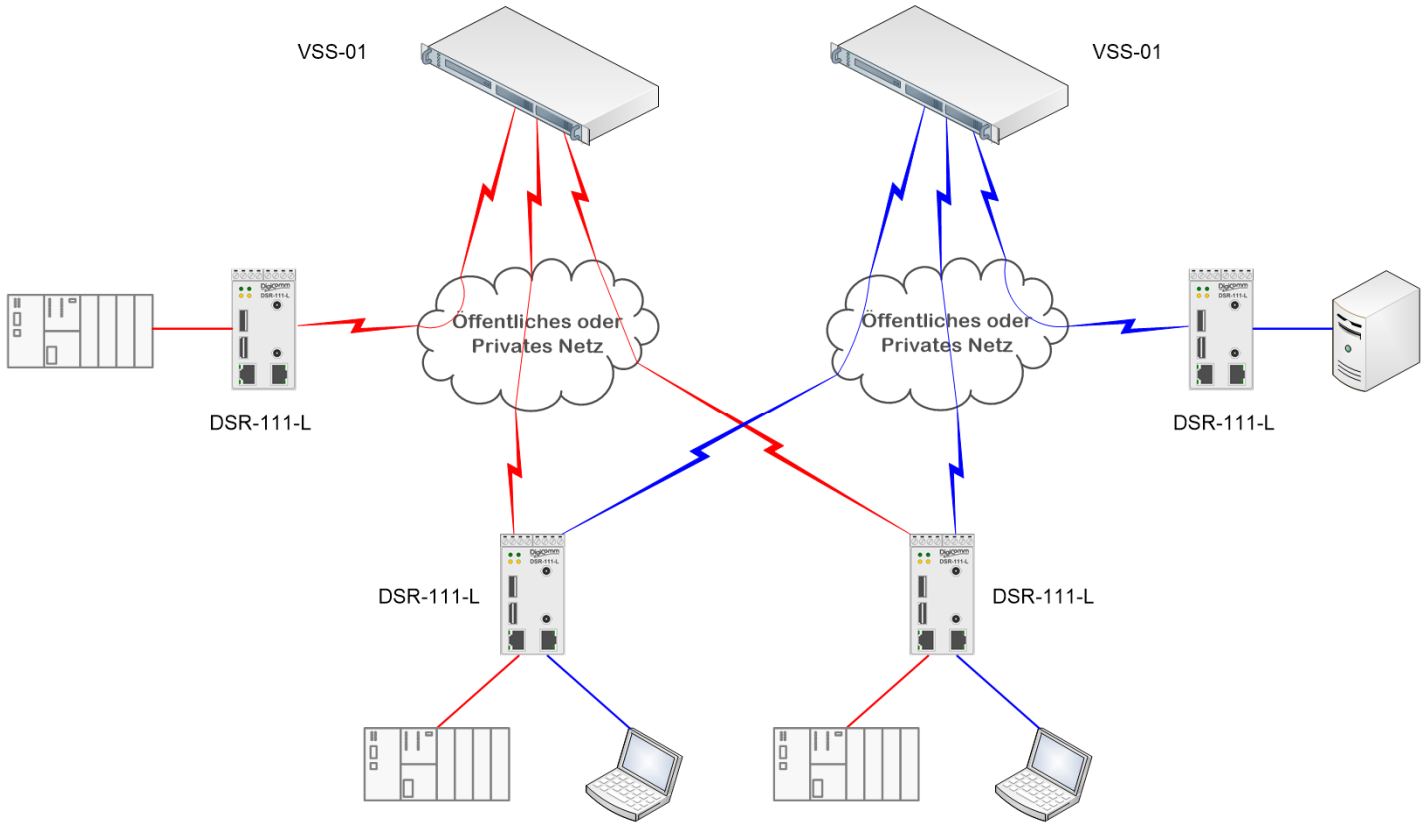


Redundanz mit bis zu drei VSS-01

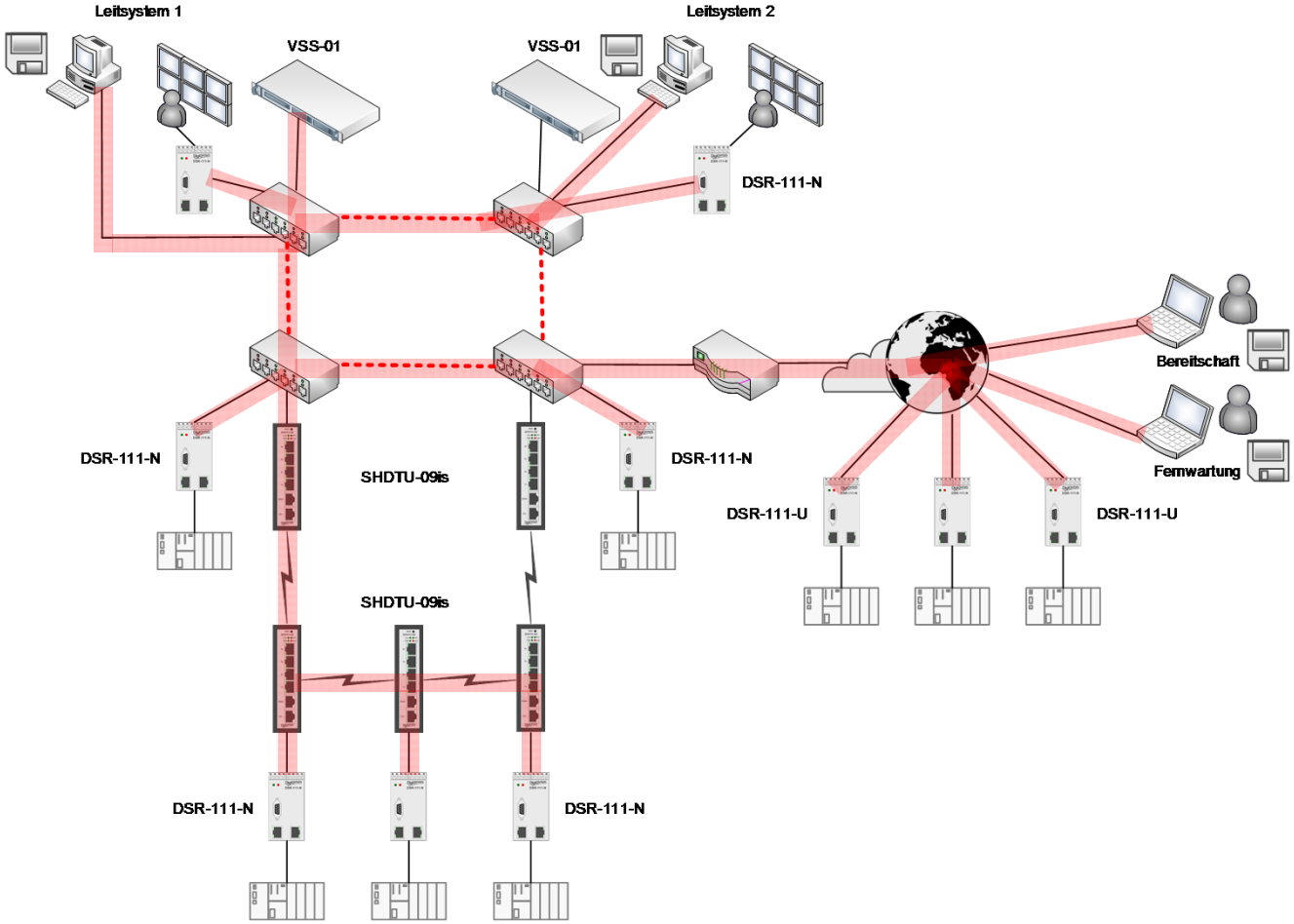
Gehärtetes Betriebssystem

Kommunikationsnetze Anwendungen

VSS-01 – Trennung von Anwendungen über VPN



DigiComm Sicherheitsfeatures



DigiComm Sicherheitsfeatures