GÉANT

GÉANT

What is Campus Best Practice?

An important part of the GÉANT project, Campus Best Practice (CBP) aims to address key challenges for European campus networks. The CBP Team does this by organising working groups and providing an evolving and to-the-point set of best-practice documents (BPDs) for the community.

Working methods

The contributing NRENs organise national-level working groups and invite technical staff from the universities to participate. The working groups discuss challenges at hand and agree on common best-practices. The documents are developed in the local language. After national approval the final documents are translated to English and published on www.geant.net

Campus Best Practice documents and reports

Available to download now at
www.geant.net/cbp

Further Information

Go online to learn more about Campus Best Practice and keep up to date with the latest developments

www.geant.net/cbp

www.twitter.com/GEANTnews

www.facebook.com/GEANTnetwork

www.geant.net

DANTE

# Campus Best Practice

connect • communicate • collaborate

The development process for CBP documents

The process of developing national best practice documents (BPDs) starts with a main author (or team of authors) making an initial version of a given new BPD. The working group iterates on this document until consensus is reached. The draft will then be on review at the national level within the higher education (HE) sector before it eventually is approved as a national BPD. The work flow is illustrated in the figure below.

Initial version → **Iterate within working group** → **Draft** → **National approval** → **National Best Practice**
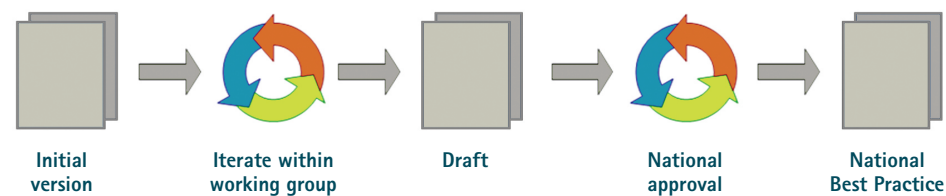
Four NRENs participate in the CBP team: UNINETT (Norway), CESNET (Czech Republic), CSC/FUNET (Finland) and AMRES (Serbia). If you would like to get in touch with a member of the Team email gn3campus@uninett.no

UNINETT   CESNET   CSC   AMRES Akademska mreža Srbije

Six areas of focus

Focus areas are physical infrastructure, campus networking (including IPv6), wireless, network monitoring, real-time communications and security.

Physical Infrastructure

This area addresses the requirements for generic cabling systems on campus, both fibre and twisted pair. The requirements of the infrastructure in telecommunications and server rooms are also dealt with. This includes power supply, ventilation and cooling, and fire protection, as well as general Information and Communications Technology (ICT) room-plan guidelines. Recommendations for building an audio-visual (AV) infrastructure in lecture halls and meeting rooms are also covered.

Campus networking

This area deals with the campus network itself, with the routers and switches as its basic building blocks. Requirements to both Layer 2 and Layer 3 are covered. Recommendations for a redundant design are given. There is a particular emphasis on guidelines for implementing IPv6 on campus. Lightpaths on campus are also dealt with.

Wireless

This area focuses on the wireless infrastructure on campus. Radio planning, design of the wireless network, security considerations, including the implementation of IEEE 802.1X are covered. eduroam requirements and radius setup are dealt with. Cookbooks for controller-based implementations are given. Legal aspects are examined.

Network monitoring

This area focuses on network monitoring of the campus network. General requirements and framework conditions for monitoring are given. NetFlow/ Internet Protocol Flow Information Export (IPFIX) analysis is covered. Security monitoring, anomaly detection and behaviour analysis are also dealt with. Particular considerations for IPv6 monitoring are given. References to a number of open source tools are given, many of which have been developed within the GÉANT community.

Real-time communications

This area recommends infrastructures for real-time communications with an emphasis on open standards, and Session Initiation Protocol (SIP), in particular. The infrastructure itself should be media transparent, coping with voice, video, messaging, document sharing, and presence. Particular focus is given to Voice over IP (VoIP) and IP telephony. Best practices from a number of NRENs in Europe are given. Security concerns are discussed and implemented solutions are recommended. Performance issues are also covered.

Security

This area deals with security considerations for the campus network. A template for a security policy is proposed, based on core principles, as defined in International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC) 27002. An ICT security architecture for higher education is recommended. Traffic filtering technologies are discussed and general applications are recommended. Adoption of digital certificates in a public key infrastructure (PKI) is covered.