Google for Education

Google Education – access infrastructure guide

Table of Contents

Google for Education

Google Education – access infrastructure guide

Overview

This document is written to give a guide for building campus internet access (networking) infrastructure that would support cloud services. It walks through various access elements you should consider, standards required for a functional network that can be used to access cloud services, and things to do when deploying the infrastructure. It points you to some solutions available today and partners in various regions of the world that can help deploy a robust network. Lastly it provides a template for developing your action plan.

Disclaimer

Google does not provide technical support for configuring third-party products. In the event of a third-party issue, you should consult your network administrator. GOOGLE ACCEPTS NO RESPONSIBILITY FOR THIRD-PARTY PRODUCTS. You may also contact Google Solutions Providers for consulting services. Links to third-party Web sites are provided for your convenience. The links and their content may change without notice. Please consult the appropriate products' Web sites for the latest configuration and support information.

Elements of access infrastructure

Below are all the areas of an access network that contribute to a successful and robust campus deployment

a. Bandwidth into the campus (including redundancy)
b. Firewalls
c. WAN / inter campus links
d. LAN
    i. Routers
    ii. Switches
    iii. VLANS
    iv. Wired ports
    v. WiFi
        1. AP Radio planning
        2. AP Power
    vi. Access controller(s)
    vii. DHCP
    viii. DNS
e. Network Management software
f. Monitoring software
g. Content filtering
h. Access controls / Security
    i. SSO
    ii. RADIUS

This document covers all the areas above in bold text. The remaining areas are covered in the Google document "Network best practices for large deployments".

Minimum standards for accessing Google cloud services

The table below lists the minimum speed you need per concurrent user for them to have a minimally acceptable experience. In summary

Per concurrent user you will need between 64kbps to 1Mbps depending on what services your users use. Simple formula is:

$TBWx = (\%C * CCUx * SBWx)_1 + (\%C * CCUx * SBWx)_2 + ... + (\%C * CCUx * SBWx)_n$

- TBWx = Total BW at level X of your network
- CCUx = Number of concurrent users at level X of your network
- %C = Percentage of concurrent users using a particular service at level x of your network
- SBWx = Recommended Kbps based on the service (see table below)
- n = number of services being accessed at level x of your network

The user experience will also be greatly affected by latency to Google's servers,

Google Apps Service	12Kbps connection	32Kbps connection	64Kbps connection	128Kbps + connection
Gmail	2 min to load if at all	Initial page 8-20 seconds full load > 1 Min	- full load 2 - 5s	Better than 64kbs
Chat in Gmail	Will not load	> 1 Min to load if ever	Loads in 4 - 10s	Better than 64kbs
Docs / spreadsheet (Open doc)	Will not load	- Initial page 5-20s - full load > 1 Min	4 - 10s	Better than 64kbs
Docs / Spreadsheets (collaborative editing)	Will not load	Noticeably slower for edits to show compared to 64K	Changes showed up quick enough for it to simulate a conversation i.e real time	Better than 64kbs
Site editing	No test	No test	Text page loads in 3 - 5 secs, Editors load about the same Image load of 385KB jpeg file took ~1Min	Text page loads in 2 - 4 secs. Editors load about the same Image load of 385KB jpeg file took ~25secs
Slides			4 - 10 s Speed is just about manageable for editing	better than 64kbps
Hangouts	N/A	N/A	Audio Only : 35kbps up/down	Video : starting at 150kbps up / 500kbps down up to the ideal = 1 Mbps up/down z
Drive			4 - 8 s Speed is just about manageable for loading drive listings	better than 64kbps
Youtube				500kbps and above
Chromebooks & Tablets				200kbps to 512kbps recommended per concurrent user Tablets

Deployment guide

For the Elements of the access network not covered in the Google document "network best practices for large deployments", the table below walks through a deployment guide for small, medium and large networks.

Access area	Small network Serving < 500 concurrent users - Total users up to 2000 - 1 or 2 buildings - < 1000 sqMtrs	Medium network Serving 500 - 2000 concurrent users - Total users 2K -> 10K - 3 to 15 buildings - Single campus	large network Serving 2000 - 5000 concurrent users - Total users 10K -> 50K - 16 to 100 buildings - Multiple campuses
Bandwidth into the campus (excluding redundancy) 64kbps, 128kbps or 512kbps per concurrent user	Lowest = 32 Mbps Mid = 64 Mbps High = 256 Mbps	Lowest = 32 Mbps Mid = 256 Mbps High = 1 Gbps	Lowest = 320 Mbps Mid = 640 Mbps High = 2.5 Gbps
Firewalls	If you can live without granular L7 firewall controls you can use your routers ACL for simple allow / deny rules. Else buy a small sized firewall sized appropriately (see sizing elements on the large network box).	If you can live without granular L7 firewall controls you can use your routers ACL for simple allow / deny rules, Else buy a Mid sized firewall sized appropriately (see sizing elements on the large network box).	Typically you will need a large sized firewall, sized for - Network capacity - Connections per second - Concurrent connections - Packets per second - VPN throughput (if required) - IPS throughput (if required) - various other capacity metrics
LAN : Routers	Pick a router that has capacity (CPU, Memory, Backplane...) to: - route your link speed - Has the variety of interfaces you will use now and the near future (T3/E3, GbE Copper or Fiber (SFP's)	Pick a router that has capacity (CPU, Memory, Backplane...) to: - route your link speed - Has the variety of interfaces you will use now and the near future (T3/E3, GbE Copper or Fiber (SFP's)	Pick a router that has capacity (CPU, Memory, Backplane...) to: - route your link speed - Has the variety of interfaces you will use now and the near future (GbE Copper or Fiber (SFP's)
LAN : Switches	Consider the following elements in this article when selecting your switching fabric	Consider the following elements in this article when selecting your switching fabric	Consider the following elements in this article when selecting your switching fabric
LAN : VLANS	In order to reduce the size of your broadcast domains consider using VLAN (see article & simple tutorial) VLAN tagging can also be implemented on wireless traffic as long as the AP's and wireless controllers support it. Also it is recommend that each SSID has its own VLAN.	In order to reduce the size of your broadcast domains consider using VLAN (see article & simple tutorial) VLAN tagging can also be implemented on wireless traffic as long as the AP's and wireless controllers support it. Also it is recommend that each SSID has its own VLAN.	In order to reduce the size of your broadcast domains consider using VLAN (see article & simple tutorial) VLAN tagging can also be implemented on wireless traffic as long as the AP's and wireless controllers support it. Also it is recommend that each SSID has its own VLAN.

continued

Access area	Small network	Medium network	large network
LAN : Wired Ports	Consider if wired network ports are needed and in which areas How many ports per area for users and how many for APs and other devices Cabling - at least CAT 5 (up to 100Mbps)	Consider if wired network ports are needed and in which areas How many ports per area for users and how many for APs and other devices Cabling - at least CAT 5e. Consider fiber if distance between nodes > 100m (up to 1Gbps)	Consider if wired network ports are needed and in which areas How many ports per area for users and how many for APs and other devices Cabling - at least CAT 6. Use fiber to connect campus (up to 10Gbps)
LAN : WiFi : AP radio planning	Radio planning is very important for a successful WiFi deployment. Plan on using multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) It is prefered to use 5Ghz radios the larger your installation gets as they have more channels for channel separation and thus can support more AP radios and thus more users Basic planning steps are referenced in this article In all cases you should use a planning tool, most likely supplied by your equipment vendor	Radio planning is very important for a successful WiFi deployment. Plan on using multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) It is prefered to use 5Ghz radios the larger your installation gets as they have more channels for channel separation and thus can support more AP radios and thus more users Basic planning steps are referenced in this article In all cases you should use a planning tool, most likely supplied by your equipment vendor	Radio planning is very important for a successful WiFi deployment. Plan on using multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) It is prefered to use 5Ghz radios the larger your installation gets as they have more channels for channel separation and thus can support more AP radios and thus more users Basic planning steps are referenced in this article In all cases you should use a planning tool, most likely supplied by your equipment vendor
LAN : WiFi : AP power	Consider Power over Ethernet (PoE) to power your APs and other devices. This way you won't need to have a separate power line/port for each AP, IP phone, camera, etc. PoE: 15.4 W per port. Fine to power APs. Normally not enough to power cameras or IP phones. PoE+: 25.5 W per port. More expensive, but can power phones, cameras and other devices. * Note that your LAN Switches should support the PoE standard you choose. Not always all ports of a switch are PoE capable. You can combine switches of both standards feed different powers to specific areas.	Consider Power over Ethernet (PoE) to power your APs and other devices. This way you won't need to have a separate power line/port for each AP, IP phone, camera, etc. PoE: 15.4 W per port. Fine to power APs. Normally not enough to power cameras or IP phones. PoE+: 25.5 W per port. More expensive, but can power phones, cameras and other devices. * Note that your LAN Switches should support the PoE standard you choose. Not always all ports of a switch are PoE capable. You can combine switches of both standards feed different powers to specific areas.	Consider Power over Ethernet (PoE) to power your APs and other devices. This way you won't need to have a separate power line/port for each AP, IP phone, camera, etc. PoE: 15.4 W per port. Fine to power APs. Normally not enough to power cameras or IP phones. PoE+: 25.5 W per port. More expensive, but can power phones, cameras and other devices. * Note that your LAN Switches should support the PoE standard you choose. Not always all ports of a switch are PoE capable. You can combine switches of both standards feed different powers to specific areas.

continued

Access area	Small network	Medium network	large network
LAN : WiFi Access Controller(s)	For very small networks < 10 access points you may be able to implement without a access controller If you are using an access controller you will have a choice between - SW controller you can install on a PC (e.g ubiquiti Unifi) - An appliance (e.g. Rukus, Mikrotik CCR models) - Cloud controller (e.g. Meraki) In all cases only use the access controller made by and matched to you AP provider. Also if you have a hybrid network with two or more different types of AP's being managed by two or more access controllers ENSURE you contain 1 set of AP's and associated access controller to a contiguous space. DO NOT mix AP's and thus controller functionality in the same physical space as this negates the controllers capabilities / effectiveness	It is likely for a network this size you will have over 10 AP's and thus it is recommended you have an access controller that matches the brand of AP's you deploy. You will have a choice between - SW controller you can install on a PC (e.g ubiquiti Unifi) - An appliance (e.g. Rukus) - Cloud controller (e.g. Meraki) In all cases only use the access controller made by and matched to you AP provider. Also if you have a hybrid network with two or more different types of AP's being managed by two or more access controllers ENSURE you contain 1 set of AP's and associated access controller to a contiguous space. DO NOT mix AP's and thus controller functionality in the same physical space as this negates the controllers capabilities / effectiveness	It is virtually a requirement that you have an access controller that matches the brand of AP's you deploy. You will have a choice between - SW controller you can install on a PC (e.g ubiquiti Unifi) - An appliance (e.g. Rukus) - Cloud controller (e.g. Meraki) In all cases only use the access controller made by and matched to you AP provider. Also if you have a hybrid network with two or more different types of AP's being managed by two or more access controllers ENSURE you contain 1 set of AP's and associated access controller to a contiguous space. DO NOT mix AP's and thus controller functionality in the same physical space as this negates the controllers capabilities / effectiveness

continued

Access area	Small network	Medium network	large network
LAN DHCP	Use a DHCP server in your network to assign dynamic IP addresses to each device. Most routers and switches have DHCP servers integrated. If yours doesn't have, you can use the DHCP server in a Linux machine (dhcpd). Assign dynamic IP to clients (desktops, laptops, mobile devices, etc.) but assign static IP addresses to servers and routers. Keep a range of IP addresses outside of the DHCP range for these cases. Configure your DHCP so the range of IP addresses that can be issued is large enough to support all clients in the current network + guests + future growth. Consider configuring different IP ranges for wired and wireless clients.	Use a DHCP server in your network to assign dynamic IP addresses to each device. Most routers and switches have DHCP servers integrated. If yours doesn't have, you can use the DHCP server in a Linux machine (dhcpd). Assign dynamic IP to clients (desktops, laptops, mobile devices, etc.) but assign static IP addresses to servers and routers. Keep a range of IP addresses outside of the DHCP range for these cases. Configure your DHCP so the range of IP addresses that can be issued is large enough to support all clients in the current network + guests + future growth. Consider configuring different IP ranges for wired and wireless clients. You can also configure different ranges for each sub-network. For medium networks you can have DHCP redundancy.	Use a DHCP server in your network to assign dynamic IP addresses to each device. Most routers and switches have DHCP servers integrated. If yours doesn't have, you can use the DHCP server in a Linux machine (dhcpd). Assign dynamic IP to clients (desktops, laptops, mobile devices, etc.) but assign static IP addresses to servers and routers. Keep a range of IP addresses outside of the DHCP range for these cases. Configure your DHCP so the range of IP addresses that can be issued is large enough to support all clients in the current network + guests + future growth. Consider configuring different IP ranges for wired and wireless clients. You can also configure different ranges for each sub-network. For large networks you should have DHCP redundancy. If you have lots of guests, you can decrease the lease time.
LAN : DNS	Unless you have < 5 devices (machines, Switches, routers, AP's ....) on your network, you will need internal DNS to resolve machine names. Most DHCP server also have a DNS server making configuration easier for resolving static and dynamic IP's on your internal network For External name resolution (e.g. www.google.com) you should use your ISP DNS or Googles public DNS as per this doc Where possible you should have multiple (redundant) DNS servers to prevent name resolution problems that can make it seem like your whole network is down to your users	You will need internal DNS to resolve machine names. Most DHCP server also have a DNS server making configuration easier for resolving static and dynamic IP's on your internal network For External name resolution (e.g. www.google.com) you should use your ISP DNS or Googles public DNS as per this doc Ensure you have multiple (redundant) DNS servers to prevent name resolution problems that can make it seem like your whole network is down to your users	You will need internal DNS to resolve machine names. Most DHCP server also have a DNS server making configuration easier for resolving static and dynamic IP's on your internal network For External name resolution (e.g. www.google.com) you should use your ISP DNS or Googles public DNS as per this doc Ensure you have multiple (redundant) DNS servers to prevent name resolution problems that can make it seem like your whole network is down to your users

continued

Access area	Small network	Medium network	large network
Network Management software & monitoring SW	A management software will help you manage your network from a single point, many times with a GUI. See the network management tool checklist in this article for considerations. When evaluating these tools, consider which and how many devices you can manage. Spiceworks (free) OpenNMS Cacti MRTG GFI (free) When choosing a network management software, check which features are available for free, and which are paid. Also check is there's a version available for your platform. Most network management solutions also have monitoring functionalities. But you can also find standalone network monitoring software only like Solarwinds (free trial)	For medium and large networks the same network management and monitoring software can be used. Note that the licensing model for some of these paid solutions is based in number of devices managed/monitored. So the larger the network, the more expensive the software license will be.	For medium and large networks the same network management and monitoring software can be used. Note that the licensing model for some of these paid solutions is based in number of devices managed/monitored. So the larger the network, the more expensive the software license will be.
Content filtering	Within an education institution content filtering is a must. To ensure you can block pornography, not expose your organization to legal action for copyright infringement because people are using torrents to download SW and movies, not to mention the bandwidth optimization. Examples of open source web filters is the squidproxy If you use an open source one, or a commercial proxy / filter consider the following: 1) Being able to use a transparent proxy so you dont have to put proxy configurations on all your clients 2) Ensure the proxy can cope with all the internet traffic going through it you don't want it to become a bottleneck. 3) Consider redundancy or machine virtualization so the proxy is not a single point of failure.	Within an education institution content filtering is a must. To ensure you can block pornography, not expose your organization to legal action for copyright infringement because people are using torrents to download SW and movies, not to mention the bandwidth optimization. Examples of open source web filters is the squidproxy If you use an open source one, or a commercial proxy / filter consider the following: 1) Being able to use a transparent proxy so you dont have to put proxy configurations on all your clients 2) Ensure the proxy can cope with all the internet traffic going through it you don't want it to become a bottleneck. 3) Consider redundancy or machine virtualization so the proxy is not a single point of failure.	Within an education institution content filtering is a must. To ensure you can block pornography, not expose your organization to legal action for copyright infringement because people are using torrents to download SW and movies, not to mention the bandwidth optimization. Examples of open source web filters is the squidproxy If you use an open source one, or a commercial proxy / filter consider the following: 1) Being able to use a transparent proxy so you dont have to put proxy configurations on all your clients 2) Ensure the proxy can cope with all the internet traffic going through it you don't want it to become a bottleneck. 3) Consider redundancy or machine virtualization so the proxy is not a single point of failure.

continued

Access area	Small network	Medium network	large network
Access controls / Security : Radius / SSO	Access to your network especially WIFi should be controlled. This can be done by using a radius server and configuring WiFi AP's to use your Radius AAA infrastructure for authentication and accounting In order to use the Google credentials for Wifi access (recommended) you will have to redirect the WiFI authentication to a captive portal that redirects to Google login which supports Oauth via such services as Cloudessa	Access to your network especially WIFi should be controlled. This can be done by using a radius server and configuring WiFi AP's to use your Radius AAA infrastructure for authentication and accounting In order to use the Google credentials for Wifi access (recommended) you will have to redirect the WiFI authentication to a captive portal that redirects to Google login which supports Oauth via such services as Cloudessa	Access to your network especially WIFi should be controlled. This can be done by using a radius server and configuring WiFi AP's to use your Radius AAA infrastructure for authentication and accounting In order to use the Google credentials for Wifi access (recommended) you will have to redirect the WiFI authentication to a captive portal that redirects to Google login which supports Oauth via such services as Cloudessa

Very detailed radio planning doc (This is a large document that you can use for reference topics as required)

Possible solutions

The links below are provided AS IS and Google does not warrant or recommend any 3rd party solution over the other. The decision as to which solution best meets the institutions needs is up to the institution.

1. Bandwidth into the campus (including redundancy) , WAN connections and intercampus links
   a. In all cases this will be provided by you local ISP / telco.

2. Firewalls
   a. Checkpoint
   b. McAFee
   c. Juniper
   d. Cisco
   e. Barracuda
   f. MicroTik
   g. Fortinet - fortigate

3. LAN : Routers, Switches
   a. Cisco
   b. Dell
   c. HP
   d. Juniper
   e. Brocade
   f. Netgear
   g. Huawei
   h. ZyXel
   i. Frotinet
   j. MicroTik (router board)
   k. Dlink

4. LAN : WiFi (including access controllers)
   a. Cisco
   b. Ubiquiti
   c. Dell
   d. HP
   e. Juniper
   f. Huawei
   g. ZyXel
   h. MicroTik (Routerboard)
   i. DLink
   j. Fortinet
   k. Aruba
   l. Ruckus
   m. Aerohive
   n. Meru
   o. Xirrus (High Performance)

5. DHCP & DNS
   Most of the Switch products above would also have DHCP / DNS servers built in or standalone options. Others to consider are:

   a. ISC.org
   b. Solarwinds

6. Network Management & Monitoring software
   Most of the Switch products above would also have Management and monitoring software platforms and typically you will use the same manufacturers SW to manage their hardware, although there are some generic SNMP solutions

   a. MRTG (SNMP monitoring) (Free)
   b. Nagios (Generic monitoring)
   c. CACTI
   d. Spiceworks (free)
   e. OpenNMS
   f. GFI (free)
   g. Brocade
   h. Cisco
   i. Juniper
   j. HP
   k. Dell
   l. Huawei
   m. Ubiquiti
   n. Fortinet

7. Content filtering
   a. Squid proxy (Free)
   b. Cisco
   c. Barracuda
   d. Fortinet
   e. MicroTik
   f. Checkpoint
   g. Mcafee

8. Access controls / Security (SSO, RADIUS)
   a. Freeradius (Free)
   b. Zeroshell (Free)
   c. Cloudessa (Cloud based)
   d. Clearbox
   e. MIcrosoft radius server
   f. Aradial

Develop your action plan

1. Scope your network size
   a. Planning horizon for this network (1, 2, 3, 4, 5 ...10 years)
   b. Total number of users and devices
   c. Number of concurrent users, taking in to account light and peak usage times
   d. % of wired and wireless users
   e. other types of applications other than cloud based services that will be running on your network
   f. Discuss and decide on any policy issues, content filtering, who has access when
2. Plan network elements you will be adding / upgrading to meet scope requirements
3. Get internal buy in for scope and plans
4. Get RFP's from vendors (Use this process to educate yourself on the breath of solutions available)
5. Select from Vendor RFP submissions
6. Stakeholder review of Selected solution and purchase go ahead
7. Issue purchase orders
8. Procure equipment and execute deployment (including change management if applicable)
9. Test deployment
10. Fix any issues
11. Go live

WP2051-1408